TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 256, December 1979

ON NATURAL RADII OF p-ADIC CONVERGENCE

BY

B. DWORK AND P. ROBBA

ABSTRACT. We study the radius of p-adic convergence of power series which represent algebraic functions. We apply the p-adic theory of ordinary linear differential equations to show that the radius of convergence is the natural one, provided the degree of the function is less than p. The study of similar questions for solutions of linear differential equations is indicated.

Introduction. It is well known classically that if a power series ξ in one variable represents an algebraic function (resp., a solution of an ordinary linear differential equation with analytic coefficients) then the series ξ converges at least up to the nearest singularity as given by the coefficients of the polynomial equation (resp., differential equation) satisfied by ξ. The example of the binomial expansion

$$\xi = \sum \binom{1/p}{s} \frac{x^s}{s!} = (1 - x)^{-1/p}$$

shows that this is not the case p-adically.

Scott Brown [1] has shown that this p-adic failure to converge in the natural disk cannot occur in the algebraic case if p exceeds a suitable exponential function of n, the degree of ξ. Following methods developed for the p-adic study of linear differential equations [9] we have given a new proof of Brown's result and show furthermore that his exponential function of n may be replaced by n itself. (For a precise statement see Theorem 2.1 below.)

Our result may best be explained in relation to Eisenstein's theorem [4, p. 327] concerning elements of $\mathbf{Q}[[x]]$ which represent algebraic functions. For each prime p of $\mathbf{Q}$ we consider the p-adic Gauss valuation of $\mathbf{Q}(x)$ (the residue class field is the field $\mathbf{F}_p(x)$ of rational functions over the field of p elements). Let K be a finite extension of $\mathbf{Q}(x)$ of degree n. Trivially, this p-adic valuation of $\mathbf{Q}(x)$ is unramified in K for almost all p. This is the main point of Eisenstein's theorem. Trivially again nontame ramification is excluded if p exceeds the degree n of K over $\mathbf{Q}(x)$. This is the basis of the present refinement (3.1.3.1) and (3.1.3.2) of Eisenstein's theorem, since the correct formulation of Brown's theorem is that p-adic failure to converge in

Received by the editors October 24, 1977.
AMS (MOS) subject classifications (1970). Primary 12B40, 34A25.
Key words and phrases. Differential equation, radius of convergence, p-adic.

the natural disk is associated with ramification and indeed can only occur in the event of wild ramification.

For completeness we give yet another proof of Eisenstein's theorem based on Newton's lemma as applied to $\mathbf{Q}((x))$. Here we followed a suggestion of Katz.

Finally we give a brief discussion of the question of nonnatural radii of convergence for solutions of ordinary linear differential equations. Our results are inconclusive.

1. Fields of analytic functions. Let Ω be an algebraically closed field of characteristic zero, complete under a nonarchimedean valuation with residue class field of characteristic p.

We choose an arbitrary "open" disk in Ω, say $D(t, 1^-) = \{x| \, |x - t| < 1\}$ in Ω. Let W be the ring of bounded analytic functions on $D(t, 1^-)$ taking values in Ω. We introduce a valuation

$$\|v\| = \sup_{x \in D(t,1^-)} |v(x)| \tag{1.01}$$

on W. Let M be a field contained by the ring W. Thus $v \in M$ implies that v has neither zero nor pole in $D(t, 1^-)$ and hence [8, 3.3.2]:

$$|v(t)| = |v(x)|, \qquad \forall x \in D(t, 1^-). \tag{1.02}$$

This shows that

$$|v(t)| = \|v\|, \qquad \forall v \in M. \tag{1.03}$$

This remains valid if we replace M by its completion in W. We shall in the following assume M to be complete.

The field M may be imbedded in $\mathbf{O}_t$, the ring of germs of holomorphic functions at t and equation (1.03) is equivalent to the assertion that "$\|v\|$ may be calculated by taking the valuation (in Ω) of the specialization at t of the germ corresponding to v".

If now v is algebraic over the field M, say

$$v^n + a_1 v^{n-1} + \cdots + a_n = 0 \tag{1.04}$$

with each $a_j \in M$ and $a_n \neq 0$, then since all the a_i are analytic at t, the same holds for the solutions. Thus we may view v as an element of $\mathbf{O}_t$ and indeed we may imbed the algebraic closure M^{alg} of M in $\mathbf{O}_t$ and $v \to |v(t)|$ represents a valuation of M^{alg} which extends by (1.03) the valuation of M. Since M is complete this valuation must be the unique valuation of M^{alg} extending the valuation of M. We summarize

1.1 LEMMA. *The field M^{alg} may be imbedded in $\mathbf{O}_t$ and the valuation on M^{alg} may be calculated by applying equation* (1.03) *to elements $v \in M^{\text{alg}}$. In particular $v(t) = 0$ only if v is the zero element.*

We may now state the central lemma of this note.

1.2 LEMMA. *Let M_0 be a complete subfield of W. Let M be an extension of M_0 of degree n prime to p. Then M (as subfield of M_0^{alg} and hence by the previous lemma identified with a subfield of $\mathbf{O}_t$) lies in W, i.e. each element of M converges on the disk $D(t, 1^-)$. This is automatically valid if $p = 0$.*

PROOF. By Ostrowski's defect theorem [7].

$$n = ef\delta \tag{1.2.1}$$

where e is the relative ramification, f is the residue class degree and δ is the defect. Since δ is a power of p, clearly $\delta = 1$ and f is prime to p. This shows that the residue class field $\overline{M}$ of M is a separable extension of $\overline{M}_0$, the residue class field of M_0. Thus we have an inertial subfield T with T over M_0 unramified and M totally and tamely ramified over T. It is enough therefore to consider these two separate cases.

Case 1. M/M_0 unramified. Since $\overline{M}$ is separable over $\overline{M}_0$, we have $\overline{M} = \overline{M}_0(\bar{u})$ and the irreducible monic polynomial $\bar{g}$ for $\bar{u}$ over $\overline{M}_0$ has monic lifting g of same degree and g has root u in M_0^{alg} whose residue class coincides with $\bar{u}$. Furthermore,

$$M = M_0(u). \tag{1.2.2}$$

Since $\bar{g}$ is separable, the roots $u_1, u_2, \ldots, u_n$ of g lie in distinct residue classes in M^{alg}, i.e.,

$$\|u_i - u_j\| = 1 - \delta_{ij} \qquad \forall i, j \tag{1.2.3}$$

and so, by (1.03),

$$|u_i(t) - u_j(t)| = 1 - \delta_{ij} \qquad \forall i, j. \tag{1.2.4}$$

Now $u_1(t), \ldots, u_n(t)$ are the n roots of $g(t, y)$, i.e.,

$$g(t, y) = \prod_{i=1}^{n} (y - u_i(t)) \tag{1.2.5}$$

and so

$$g_y(t, u_1(t)) = \prod_{i=2}^{n} |u_1(t) - u_i(t)|. \tag{1.2.6}$$

Thus by (1.2.4) we have

$$\begin{aligned} g(t, u_1(t)) &= 0, \\ |g_y(t, u_1(t))| &= 1. \end{aligned} \tag{1.2.7}$$

Fix $r < 1$, view $g(x, y)$ as polynomial in y with coefficients in W_t^r, the ring of bounded analytic functions on $D(t, r^-)$. Letting $\| \ \|_r$ denote the supremum norm on this disk,

$$\begin{aligned} \|g(x, u_1(t))\|_r &\leqslant r < 1, \\ \|g_y(x, u_1(t))\|_r &= 1. \end{aligned} \tag{1.2.8}$$

Thus we view $v_0 = u_1(t)$ as an approximate solution in W_t^r of the equation

$$g(x, y) = 0 \tag{1.2.9}$$

and we define recursively

$$v_{s+1} = v_s - g(x, v_s)/g_y(x, v_s) \tag{1.2.10}$$

and show that $\| g_y(x, v_s)\|_r = 1$ for all s and that the limit $v_s = v$, an element of W_t^r which satisfies the equation

$$g(x, v) = 0, \qquad v(t) = u_1(t). \tag{1.2.11}$$

These conditions uniquely characterize v and hence letting $r \to 1$, we conclude that u_1 $(= v)$ converges in $D(t, 1^-)$ as asserted.

Case 2. M/M_0 totally and tamely ramified (we do not assume that M_0 is discretely valuated).

It is well known [**10**, p. 64] that M is a radical extension of M_0, i.e., there exists a sequence of fields

$$M = M_v \supset M_{v-1} \supset \cdots \supset M_0 \tag{1.2.12}$$

such that for $i = 0, 1, \ldots, v - 1$, there exist $\beta_i \in M_i$ and n_i divisor of n for which

$$M_{i+1} = M_i\big((\beta_i)^{1/n_i}\big). \tag{1.2.13}$$

Thus we may reduce to the case in which

$$M = M_0(b^{1/n}) = M_0\big[b^{1/n}\big] \tag{1.2.13}'$$

with $b \in M_0$.

We use (1.02) to conclude that $b(x)/b(t)$ is an element of W bounded by 1 on $D(t, 1^-)$ and taking the value 1 at $x = t$. Thus $z = b(x)/b(t) - 1$ is represented by a power series in $(x - t)$ with no constant term and coefficients bounded by unity. Consequently,

$$|z(x)| \leqslant r \qquad \forall x \in D(t, r^-). \tag{1.2.14}$$

On the other hand, $1/n \in \mathbf{Z}_p$ since $p \nmid n$ and hence the series

$$(1 + z)^{1/n} = \sum_{s=0} \binom{1/n}{s} z^s \tag{1.2.15}$$

converges for $|z| < 1$. Writing

$$(b)^{1/n} = (b(t))^{1/n}(1 + z)^{1/n} \tag{1.2.16}$$

it is now clear from (1.2.13)′ that M lies in W.

2. Theorem of Brown. Our object is to describe the p-adic radius of convergence of a series representing an algebraic function. Following Brown we proceed with a little more generality.

2.1 THEOREM. *Let K be a field of characteristic zero with nonarchimedean valuation and residue class field of characteristic p. Let*

$$f(y) = A_0 y^n + \cdots + A_n \in K[[x]][y] \tag{2.1.1}$$

be a polynomial in y of degree n with coefficients $A_j \in K[[x]]$ and which lie in the ring H of functions analytic on $D(0, 1^+)$ $(= \{x \mid |x| < 1\})$. Suppose f and f_y are relatively prime in $H[y]$ and that at each $x_0 \in D(0, 1^-)$ (except possibly at $x_0 = 0$) the equation

$$f(y) = 0 \tag{2.2}$$

has n distinct locally analytic solutions. Then the solutions of (2.2) at $x = 0$ are of the form

$$y = x^{-m/c}\xi(x^{1/c}) \tag{2.3}$$

where $m \in \mathbf{N}$, c is a positive integral divisor of $n!$ and ξ is a power series with coefficients algebraic over K. The point is that the radius of convergence of ξ is at least unity if p is either zero or strictly greater than the degree n.

Notes. (1) The result is independent of the choice of the extension of the valuation of K to the valuation of K^{alg}.

(2) There is no need to assume that the A_j lie in H; convergence and boundedness in $D(0, 1^-)$ are sufficient as it is enough to show that $\xi \in (D(0, r^-))$ for each $r < 1$.

(3) Regardless of p, if ξ converges on $D(0, r^-)$ $(r < 1)$ then ξ is bounded on $D(0, r^-)$. In general, a function y algebraic over H is bounded on its domain of convergence. Thus, in particular, if ξ converges on $D(0, 1^-)$ then it is bounded there.

PROOF. We view f as a polynomial in y with coefficients in $K^{\text{alg}}((x))$. Let c be the degree of the splitting field of f over this field. Then c divides $n!$ and the spitting field is, in fact, $K^{\text{alg}}((x^{1/c}))$. This explains the form of (2.3).

We imbed the field K in a complete field Ω containing an element t whose residue class is transcendental over $\overline{K}$, the residue class field of K. The restrictions to $D(t, 1^-)$ of the coefficients $A_0, \ldots, A_m$ generate over $\mathbf{Q}$ a subfield of the ring W of analytic bounded functions on $D(t, 1^-)$. We take M_0 to be the completion of that field under the valuation of W (§1). We apply Lemma 1.2, noting that f need not be irreducible over M but that its irreducible factors have degrees strictly less than p. We conclude that the solutions at t of (2.2) lie in W.

We will use a previously employed procedure [9, Lemma 4.25] to transfer this information to the origin. We replace x by x^c and y by $x^r y$ where r is a sufficiently large integer. With these changes, each solution at t of (2.2) remains in W but now we are sure that at each $x_0 \in D(0, 1^-)$ (including $x_0 = 0$) equation (2.2) has n distinct analytic solutions.

If y is an arbitrary solution of (2.2) then the derivation d/dx of the quotient field H_0 of H may be extended to the field $H(y)$ and indeed, letting $\mathbf{X} = (1, y, \ldots, y^{n-1})$, we have

$$\frac{d\mathbf{X}}{dx} = \mathbf{X}G \tag{2.4}$$

where G is an $n \times n$ matrix with coefficients in H_0; the singularities of the coefficients in $D(0, 1^-)$ lie among the zeros of $A_0\Delta$ (Δ = discriminant of $f(y)$) in $D(0, 1^-)$.

We deduce from (2.4) that for each $s \in \mathbf{N}$ there exist G_s, an $n \times n$ matrix with coefficients in H_0 and singularities in $D(0, 1^-)$ among the zeros of $A_0\Delta$, such that

$$\frac{1}{s!}\frac{d^s\mathbf{X}}{dx^s} = \mathbf{X}G_s. \tag{2.5}$$

Since (2.2) has n solutions in W, equation (2.4) has a solution matrix at t which lies in W. It follows that

$$|G_s|_{\text{gauss}} = O(1) \quad \text{as } s \to \infty. \tag{2.6}$$

The symbol on the left denotes the supremum of the values assumed at t by the coefficients of G_s.

By hypothesis for each $x_0 \in D(0, 1^-)$ there exists a locally analytic solution matrix V (depending upon x_0) of (2.4). Thus

$$\frac{1}{s!}\frac{d^sV}{dx^s} = VG_s$$

which shows that VG_s is analytic at x_0. But $(\det V)V^{-1}$ is also analytic and hence

$$\det V \cdot G_s \text{ is analytic at } x_0. \tag{2.7}$$

Now $\det V$ is the wronskian with logarithmic derivative equal to the trace of G. This shows that $(\det V)(x_0) = 0$ for only a finite set of $x_0 \in D(0, 1^-)$ and that the zeros are of uniformly bounded order. It follows that there exists a fixed polynomial $P \in K[x]$ such that PG_s has no pole in $D(0, 1^-)$ for any $s \in N$.

Fix $b \in D(0, 1^-)$, such that $P(b) \neq 0$. By the maximum principle, $P(b)G_s(b)$ is coefficient-wise bounded by $|P(t)|\,|G_s|_{\text{gauss}} = O(1)$. A solution matrix of (2.4) at b is given by

$$\sum G_s(b)(x - b)^s \tag{2.8}$$

which clearly converges for $x \in D(b, 1^-) = D(0, 1^-)$. The theorem of Brown now follows, taking into account that we have changed the exponent c in equation (2.3).

3. Theorem of Eisenstein

3.1 THEOREM. *Let $f \in \mathbf{Z}[x, y]$ be a polynomial of degree n with coefficients in $\mathbf{Z}[x]$,*

$$f(x, y) = A_0 y^n + A_1 y^{n-1} + \cdots + A_0 \tag{3.1.0}$$

with Δ ($\in \mathbf{Z}[x]$) as discriminant. Let S be the set of zeros of $A_0\Delta$ other than $x = 0$. For each prime p, let $d_p(0, S)$ be the distance between the origin and the set S, the distance to be measured in any valuation of $\mathbf{Q}^{\text{alg}}$ extending p. Let

$$\xi = \sum_{j=0}^{\infty} b_j x^j \in \mathbf{Q}[[x]] \tag{3.1.1}$$

be a formal solution of

$$f(x, \xi) = 0. \tag{3.1.2}$$

There exist integers m, m_0 such that

$$m_0 b_j m^j \in \mathbf{Z} \tag{3.1.3}$$

for all $j \in \mathbf{N}$. We may choose m such that its prime divisors satisfy one of the two conditions

$$p < n, \tag{3.1.3.1}$$

$$d_p(0, S) < 1. \tag{3.1.3.2}$$

(*These restrictions on m seem to be new.*)

PROOF. It follows from Brown's theorem that ξ converges p-adically in $D(0, 1^-)$ unless p satisfies conditions (3.1.3.1), (3.1.3.2). In any case ξ has at each p a nontrivial radius of convergence (for example, by Clark [2], as the solution of a linear differential equation with rational exponents). Thus we may choose m with prime factors as indicated such that

$$\xi(mx) \text{ converges in } D(0, 1^-) \text{ for every } p. \tag{3.1.4}$$

It only remains to choose m_0 such that

$$m_0\xi(mx) \text{ is bounded } p\text{-adically by 1 in } D(0, 1^-) \text{ for each } p. \tag{3.1.5}$$

To prove this, it is simplest to suppose that f has been transformed so that (3.1.4) holds with $m = 1$. For almost all p we have

$$|A_0|_{\text{gauss}} = 1, \ |A_j|_{\text{gauss}} < 1 \qquad (j = 1, 2, \ldots, n).$$

It follows that, for $x \in D(0, 1^-)$, $|A_j(x)| < 1$ $(j = 1, 2, \ldots, n)$ and that $|A_0(x)| \to 1$ as $|x| \to 1$ from below. By (3.1.0) it follows easily that $|\xi(x)|$ approaches an upper bound less than or equal to 1 as $|x| \to 1$. This shows that ξ is bounded by 1 on $D(0, 1^-)$ for almost all p. It is bounded on $D(0, 1^-)$ at the remaining primes and hence equation (3.1.5) follows for a suitable choice of m_0. This completes the proof.

Of course this does not characterize algebraic functions. The example

$F(\frac{1}{2}, \frac{1}{2}; 1; X)$ shows that radii of convergence cannot characterize such functions. Christol [3] has studied (and characterized) algebraic elements (i.e. uniform limits on $D(0, 1^-)$ of algebraic functions). The same example shows that a power series may represent an algebraic element for almost all p without representing an algebraic function.

Notes. (3.2) One may obtain (3.1.4) (without any interpretation of the divisors of m) by noting that, for almost all p, $\Delta(t)$ is a p-adic unit and hence for almost all p if z is algebraic over $\mathbf{Q}(t)$ and $f(t, z) = 0$ then $f_y(t, z)$ is a p-adic unit. By Newton's lemma this implies that the solutions of $f(x, y) = 0$ at t converge in $D(t, 1^-)$ for almost all p. This then gives a proof of Eisenstein's theorem without using Brown's theorem.

(3.3) A different proof of (3.1.4) may be based upon the existence of Frobenius structure "for differential equations arising from algebraic geometry". The essential principles may be found in Katz's article [6, Proposition 3.1].

(3.4) For p satisfying (3.1.3.1), (3.1.3.2) one may find upper bounds for the power of p which divides m. Such bounds would be based upon the ramification of the p-adic gauss valuation of $\mathbf{Q}(x)$ in the splitting field of f over $\mathbf{Q}(X)$. (see §§6, 7).

(3.5) We state without proof the generalization of (3.1) to the case of an algebraic number field K.

Let f (given by (3.1.0)) lie in $K[x, y]$. Let $\Delta \in K[x]$ be the discriminant. Let S ($\subset Q^{\mathrm{alg}} = K^{\mathrm{alg}}$) be the set of zeros of $A_0\Delta$, excluding $x = 0$. For each prime $\mathfrak{p}$ of K, let $d_{\mathfrak{p}}(0, S)$ denote the distance between the origin and the set S measured in any valuation of K^{alg} extending $\mathfrak{p}$. Let ξ as given by (3.1.1) lie in $K[[x]]$ and be a formal solution of 3.1.2. Then

$$\text{for almost all } \mathfrak{p}, \quad \mathrm{ord}_{\mathfrak{p}} b_j \geqslant 0 \quad \text{for all } j \in \mathbf{N}, \tag{3.5.1}$$

$$\text{for fixed } \mathfrak{p}, \quad \mathrm{ord}_{\mathfrak{p}} b_j = O(1) \quad \text{as } j \to \infty, \tag{3.5.2}$$

unless either

$$\mathfrak{p} \text{ divides } p, \quad p \text{ rational prime}, p \leqslant n, \tag{3.5.2.1}$$

$$d_{\mathfrak{p}}(0, S) < 1, \tag{3.5.2.2}$$

$$\text{for arbitrary } \mathfrak{p}, \quad (\mathrm{ord}_{\mathfrak{p}} b_j)/j = O(1) \quad \text{as } j \to \infty. \tag{3.5.3}$$

4. Proof of Eisenstein's theorem based on Newton's lemma. Let f be as in §3 and let ξ satisfy (3.1.1), (3.1.2). We may assume that

$$f_y(x, \xi) = b_0 x^s + (x^{s+1}), \qquad b_0 \neq 0, \tag{4.1}$$

but we may not assume that

$$f_y(0, a_0) \neq 0.$$

We choose

$$\eta_0 = a_0 + a_1 x + \cdots + a_{2s} x^{2s} \equiv \xi \bmod x^{2s+1}. \tag{4.2}$$

Replacing x by mx if necessary, we may assume that $a_0, a_1, \ldots, a_{2s} \in \mathbf{Z}$. We now have

$$\begin{aligned} f(x, \eta_0) &\equiv 0 \bmod x^{2s+1}, \\ f_y(x, \eta_0) &\equiv b_0 x^s \bmod x^{s+1}, \qquad b_0 \neq 0. \end{aligned} \tag{4.3}$$

Hence by Newton's lemma for $\mathbf{Q}((x))$ we know that $f(y) = 0$ has a unique solution ξ satisfying (4.2) and that this solution is the limit (in the x-adic topology) of the sequence η_j constructed recursively (starting with η_0) by

$$\eta_{j+1} = \eta_j - f(x, \eta_j)/f_y(x, \eta_j).$$

Clearly $f_y(x, \eta_j) \equiv b_0 x^s (x^{s+1})$ and by induction one shows that only powers of b_0 appear as denominators in the series representation of η_j. Furthermore, one checks that the coefficient of x^{s+j} has at worst b_0^j in the denominator. This completes our sketch of a proof of the usual form of Eisenstein's theorem.

Note. If we exclude (3.5.2), then the extension of Eisenstein's theorem to algebraic number fields indicated in (3.5) above may be obtained by the argument of this section.

5. Linear differential equations. Let

$$l = D^n + a_1 D^{n-1} + \cdots + a_n \qquad (D = d/dx)$$

be a linear differential operator whose coefficients a_i are bounded analytic functions on $D(0, 1^-)$. Let $l\xi = 0$, ξ a germ of analytic function at the origin. We are interested in the case in which ξ fails to converge in $D(0, 1^-)$. The example $\exp X$ suggests a false conjecture.

5.0 False Conjecture. The solution ξ is, for each $r < 1$, algebraic over the ring $W_0^{r,0}$ of functions analytic and bounded on $D(0, r^-)$.

5.1 Lemma. *The conjecture is true for* $n = 1$.

Proof. $l = D + a_1$. Let

$$-a_1 = \sum_{j=0}^{\infty} b_j X^j, \qquad \operatorname{ord} b_j \geqslant \gamma_0, \qquad \forall j \in \mathbf{N}. \tag{5.1.1}$$

If ξ is a solution then

$$\xi^{p^r} = \exp p^r \sum_{j=0}^{\infty} \frac{1}{j+1} b_j X^{j+1}. \tag{5.1.2}$$

We recall that there exists $\gamma > 0$ such that

$$\operatorname{ord} j < \gamma \log j \qquad \forall j \in \mathbf{N}. \tag{5.1.3}$$

We consider the disk

$$\operatorname{ord} x > \varepsilon > 0 \tag{5.1.4}$$

and calculate

$$\operatorname*{Inf}_{j\in\mathbf{N}} (j\varepsilon - \operatorname{ord} j) \geqslant \operatorname*{Inf}_{j>1} (j\varepsilon - \gamma \log j) \geqslant \gamma(1 + \log \varepsilon/\gamma).$$

For each ε we may choose ν such that

$$\gamma_0 + \nu + \gamma(1 + \log \varepsilon/\gamma) > \frac{1}{p-1}$$

and so ξ^{p^ν} converges on the disk (5.1.4).

5.2 LEMMA. *The conjecture is false for* $n = 2$.

PROOF. We again [5, §7] consider the confluent hypergeometric series

$$\varphi(a, c, x) = \sum \frac{(a)_s}{(c)_s} \frac{x^s}{s!}. \tag{5.2.1}$$

Letting $c = 1/p^\nu$, we consider $\varphi(a, c, c(1-x))$ which satisfies the linear differential equation

$$L_{a,\nu} = p^\nu(1-x)D^2 - xD - a. \tag{5.2.2}$$

There is a unique formal solution $x^{-a}V$ where

$$V = \sum_{m=0}^{\infty} (-x)^{-m} B_m (a)_m, \tag{5.2.3}$$

the B_m being given by the generating function

$$(1 + p^\nu z)^{-1-a} \exp(-z + p^{-\nu} \log(1 + p^\nu z)) = \sum_{m=0}^{\infty} B_m z^m. \tag{5.2.4}$$

It follows that, for a fixed $|a| = 1$ (a not necessarily in $\mathbf{Z}_p$) and with suitable ν, there exists $\varepsilon > 0$ such that V converges for

$$|x| > 1 - \varepsilon. \tag{5.2.5}$$

We choose a real number r and a point b such that

$$1 > r > |b| > 1 - \varepsilon. \tag{5.2.6}$$

Since $L_{a,\nu}$ has no singularity in $D(b, 1^-)$, the solution

$$\xi = x^{-a}V \tag{5.2.7}$$

at b is conjecturally algebraic over $W_b^{r,0}$ (= ring of functions analytic and bounded in $D(b, r^-)$). Let Γ be the annulus

$$\Gamma = \{x | 1 - \varepsilon < |x| < r\} \tag{5.2.8}$$

and let W_Γ denote the ring of bounded analytic functions on Γ. Clearly $W_\Gamma \supset W_b^{r,0}$ and hence conjecturally ξ is algebraic over W_Γ. However $V \in W_\Gamma$ and so the conjecture implies that x^{-a} is algebraic over W_Δ.

We show that this cannot be true if $a \notin \mathbf{Q}$. Let $\eta = x^a$ and consider the irreducible monic polynomial for x^{-a} over the quotient field of W_Γ. We write this in the form

$$B_0\eta^s + B_1\eta^{s-1} + \cdots + B_{s-1}\eta + 1 = 0. \tag{5.2.9}$$

There exists a possibly smaller annulus Γ_1 such that each $B_j \in W_{\Gamma_1}$. By definition

$$x\frac{d\eta}{dx} = a\eta \tag{5.2.10}$$

and hence

$$(xB_0' + saB_0)\eta^s + \cdots + (xB_{s-1}' + aB_{s-1})\eta = 0. \tag{5.2.11}$$

Since s is minimal in (5.2.9),

$$xB_0' = -saB_0, \tag{5.2.12}$$

but since $B_0 \in W_{\Gamma_1}$, B_0 may be represented by a nontrivial Laurent series, and hence $sa \in \mathbf{Z}$, i.e., $a \in \mathbf{Q}$ as asserted.

It is not clear that a counterexample is given by this example with $a \in \mathbf{Q} \cap \mathbf{Z}_p$.

6. Wild ramification. Our object is to examine Lemma 1.2 in the case of wild ramification. Thus we again let M_0 be a field of functions analytic on a disk $D(t, 1^-)$, complete under the natural valuation provided by the supremum norm. We consider a totally ramified extension M of degree $q = p^c$. We introduce two hypotheses:

(6.01) the valuation of M_0 is discrete;

(6.02) there exists a chain of intermediate fields $M_0 \subset M_1 \subset \cdots \subset M_c = M$ such that $\deg M_i/M_{i-1} = p$ for $i = 1, 2, \ldots, c$.

6.1 Lemma. *If M is a totally ramified extension of M_0 of degree p^c satisfying conditions* (6.01), (6.02) *then each element of M converges in the set*

$$\operatorname{ord}(x - t) > c + 1/(p - 1). \tag{6.1.1}$$

To carry out an induction proof we introduce a slightly stronger statement.

6.2 Lemma. *For each nonzero element θ of the field M (of Lemma* 6.1*) and for* $\operatorname{ord}(x - t) > c + 1/(p - 1)$ *we have*

$$\operatorname{ord}(\theta(x) - \theta(t)) \geqslant \operatorname{ord}(x - t) + \operatorname{ord}\theta(t) - c \tag{6.2.1}$$

Proof. The assertion is trivial for $c = 0$ and so it is sufficient to suppose both lemmas valid for M and to consider M', a ramified extension of M of degree p. We verify the corresponding assertions for M'.

Let e be the ramification of M, i.e., if w is prime element of M then $\operatorname{ord} w = 1/e$, it being understood that $\operatorname{ord} p = 1$.

Let u be a prime element of M' so $M' = M(u)$ and u is root of an

Eisenstein polynomial

$$f(x,y) = f(y) = y^p + A_1 y^{p-1} + \cdots + A_{p-1}y + A_p \in M[y] \quad (6.2.2)$$

where

$$\begin{aligned} &\operatorname{ord} A_p = 1/e, \\ &\operatorname{ord} A_i = l_i/e, \qquad l_i \geqslant 1 \qquad (i = 1, 2, \ldots, p-1). \end{aligned} \quad (6.2.3)$$

We will show that u ($\in \mathbf{O}_t$ by Lemma 1.1) satisfies the conditions

$$u \text{ converges for } \operatorname{ord}(x-t) > c + 1 + \frac{1}{p-1}. \quad (6.2.4.1)$$

$$\operatorname{ord}(u(x) - u(t)) \geqslant \operatorname{ord}(x-t) - (c+1) + \frac{1}{pe} \quad (6.2.4.2)$$

(x being as in (6.2.4.1)).

For $\eta \in M'$ we have

$$\eta = \sum_{j=0}^{p-1} G_j u^j \quad (6.2.5)$$

with $G_j \in M$ ($j = 0, 1, \ldots, p-1$) and

$$\operatorname{ord} \eta(t) \leqslant \operatorname{ord} G_j(t) + j \operatorname{ord} u(t). \quad (6.2.6)$$

The proof of Lemma 6.1 would follow from (6.2.5), (6.2.4.1) and the induction hypothesis for M. The proof of Lemma 6.2 would follow from (6.2.5), (6.2.6), (6.2.4.2) and the induction hypothesis for M. Thus it is enough to verify (6.2.4.1), (6.2.4.2).

We write $u(t) = \xi \in \Omega$. Hence,

$$f(t, \xi) = 0. \quad (6.2.7)$$

We write

$$f(x, \xi + z) = z^p + B_{p-1}z^{p-1} + \cdots + B_1 z + B_0. \quad (6.2.8)$$

The left side is the same as

$$f(x, \xi + z) - f(t, \xi) = (z + \xi)^p - \xi^p + \sum_{i=0}^{p-1} \left\{ A_{p-i}(x)(\xi + z)^i - A_{p-i}(t)\xi^i \right\}$$

and so

$$B_0 = A_p(x) - A_p(t) + \sum_{i=1}^{p-1} \xi^i (A_{p-i}(x) - A_{p-i}(t)). \quad (6.2.9.1)$$

$$B_1 = p\xi^{p-1} + \sum_{i=1}^{p-1} A_{p-i}(x) i \xi^{i-1}, \quad (6.2.9.2)$$

$$B_i = \binom{p}{i}\xi^{p-i} + \sum_{s=i}^{p-1} A_{p-s}(x)\binom{s}{i}\xi^{s-i} \qquad (i = 2, 3, \ldots, p-1). \quad (6.2.9.3)$$

The verification consists of two parts. We fix x such that

$$\operatorname{ord}(x - t) > c + 1 + \frac{1}{p-1}; \tag{6.2.10}$$

we consider the convex closure (Newton polygon) of the points $\{i, \operatorname{ord} B_i(x)\}$ ($B_p = 1$). We show that the first side joins the first two points, i.e., $(0, \operatorname{ord} B_0(x))$, $(1, \operatorname{ord} B_1(x))$, that all the other points lie strictly above this first side and that the first side has negative slope. In particular we will show

$$\operatorname{ord} B_0(x) - \operatorname{ord} B_1(x) \geqslant \operatorname{ord}(x - t) - (c + 1) + 1/pe. \tag{6.2.11}$$

The equation of the line joining the first two points is

$$Y = \operatorname{ord} B_0(x) + X(\operatorname{ord} B_1(x) - \operatorname{ord} B_0(x))$$

and so we assert that subject to (6.2.10); we have

$$\operatorname{ord} B_i(x) > \operatorname{ord} B_0(x) + i(\operatorname{ord} B_1(x) - \operatorname{ord} B_0(x)) \qquad (i = 2, 3, \ldots, p). \tag{6.2.12}$$

From (6.2.9.1), (6.2.10) and the induction hypothesis for M we have

$$\operatorname{ord} B_0(x) \geqslant \frac{1}{e} + \operatorname{ord}(x - t) - c > \frac{1}{e} + 1 + \frac{1}{p-1}. \tag{6.2.13}$$

Likewise from (6.2.9.2) we have

$$\operatorname{ord} B_1(x) = \operatorname{Inf}\left(1 + \frac{p-1}{pe}, \inf_{i=1}^{p-1}\left[\frac{(i-1)}{pe} + \operatorname{ord} i + \operatorname{ord} A_{p-i}(t)\right]\right). \tag{6.2.14}$$

(Of course ord $i = 0$ in this equation, we retain this term as well as the $\operatorname{ord}\binom{s}{i}$ term in (6.2.16.2) below to indicate in (6.2.16.2)′ the difficulty in treating an extension of degree p^c without intermediate fields.)

It follows from (6.2.13) that to prove (6.2.12) it is enough to show that

$$\operatorname{ord} B_i(x) \geqslant i \operatorname{ord} B_1(x) - (i-1)\left[\frac{1}{e} + 1 + \frac{1}{p-1}\right], \qquad (2 \leqslant i \leqslant p). \tag{6.2.15}$$

It follows from (6.2.9.3) that (6.2.15) is valid for $2 \leqslant i < p$ if both

$$1 + \frac{p-i}{pe} \geqslant i \operatorname{ord} B_1(x) - (i-1)\left[\frac{1}{e} + 1 + \frac{1}{p-1}\right], \qquad (2 \leqslant i \leqslant p-1), \tag{6.2.16.1}$$

and

$$\operatorname{ord}\binom{s}{i} + \operatorname{ord} A_{p-s}(t) + \frac{s-i}{pe} \geqslant i \operatorname{ord} B_1(x) - (i-1)\left[\frac{1}{e} + 1 + \frac{1}{p-1}\right], \quad \forall 2 \leqslant i \leqslant s \leqslant p-1. \tag{6.2.16.2}$$

To verify (6.2.15) for $i = p$, we need

$$(p-1)\left(1+\frac{1}{e}+\frac{1}{p-1}\right) > p \operatorname{ord} B_1(x). \tag{6.2.16.3}$$

It follows from equation (6.2.14) that

$$\operatorname{ord} B_1(x) \leqslant 1+\frac{p-1}{pe} = \frac{p-1}{p}\left(1+\frac{1}{p-1}+\frac{1}{e}\right), \tag{6.2.17.1}$$

$$\operatorname{ord} B_1(x) \leqslant \frac{s-1}{pe} + \operatorname{ord} A_{p-s} + \operatorname{ord} s, \qquad 2 \leqslant s \leqslant p-1. \tag{6.2.17.2}$$

By means of this last relation, equation (6.2.16.2) is certainly valid if

$$0 > (i-1)\left[\operatorname{ord} B_1(x) - \left(1+\frac{p-1}{pe}\right)\right] - \frac{i-1}{p-1} + \operatorname{ord} s - \operatorname{ord}\binom{s}{i},$$
$$2 \leqslant i \leqslant s \leqslant p-1. \tag{6.2.16.2)'}$$

Equations (6.2.16.1), (6.2.16.2)', (6.2.16.3) are all direct consequences of (6.2.17.1). This completes the verification of (6.2.15) and hence of (6.2.12).

Note. In equation (6.2.16.2)', $\operatorname{ord} s = 0 = \operatorname{ord}\binom{s}{i}$. The purpose of condition (6.02) is to make it possible to discard these terms.

Finally equation (6.2.11) follows directly from equations (6.2.13) and (6.2.17.1).

We have thus shown that for each x in the disk (6.2.4.1) the Newton polygon for (6.2.8) has a distinguished first side of projected length one and of predicted slope. The lemma follows without difficulty.

7. Inseparable residue class field. To discuss this topic briefly we put ourselves in the induction part of the proofs of §6.

LEMMA. *Let M be a field of analytic functions on the disk* $\operatorname{ord}(x-t) > c + 1/(p-1)$ *with the property that for each x in the disk and each $\theta \in M$, $\theta \neq 0$, we have*

$$\operatorname{ord}(\theta(x)-\theta(t)) \geqslant \operatorname{ord}(x-t) - c + \operatorname{ord}\theta(t).$$

We further assume that M has discrete valuation. Let M' be an extension of M of degree p with residue class degree p but with $\overline{M}'$ inseparable over $\overline{M}$. Then M' is a field of functions analytic on the disk $\operatorname{ord}(x-t) > c + 1 + 1/(p-1)$ *and for each nonzero $v \in M'$ and each x in this disk we have*

$$\operatorname{ord} v(x) - v(t) \geqslant \operatorname{ord}(x-t) - c - 1 + \operatorname{ord} v(t).$$

PROOF. We know that $M' = M(u)$ where $\bar{u}$ is root of an inseparable polynomial $Y^p + \overline{A}_p = 0$ over $\overline{M}$. Thus u is root of polynomial (6.2.2) but now $\operatorname{ord} A_p(t) = 0$ (instead of $1/e$ as in (6.2.3)). We again set $\xi = u(t)$ and we now have $\operatorname{ord}\xi = 0$. We may prove the lemma by repeating all the calcula-

tions in §6 starting with (6.2.4). We find that at each step we must drop the terms in $1/e$. (The only exception is in the expression for ord A_i, (6.2.3).) The key relations (6.2.6), (6.2.14) no longer depend on distinctness of cosets of the valuation group, but rather on the fact that $\overline{M}' = \overline{M}(\overline{u})$. This completes our discussion of the proof of this lemma.

COROLLARY. *Lemma* 6.1 *remains valid with the words "totally ramified" removed, i.e., M is an extension of M_0 containing no proper intermediate field tamely ramified over M and which satisfies* (6.01), (6.02).

REFERENCES

1. S. Brown, *Bounds of transfer principles for algebraically closed and complete discretely valued fields*, Mem. Amer. Math. Soc. **15** (1978), no. 204.

2. D. Clark, *A note on the p-adic convergence of solutions of linear differential equations*, Proc. Amer. Math. Soc. **17** (1966), 262–269.

3. G. Christol, *Eléments algébriques*, Groupe de Travail d'Analyse Ultra-métrique, (1re année: 1973/74), Exp. No. 14, Secrétariat Mathématique, Paris, 1975.

4. P. Dienes, *The Taylor series*, Dover, New York, 1957.

5. B. Dwork and P. Robba, *On ordinary linear p-adic differential equations*, Trans. Amer. Math. Soc. **231** (1977), 1–46.

6. N. Katz, *Travaux de Dwork*, Séminaire Bourbaki (1971/1972, Exposés Nos. 400–417), Lecture Notes in Math., vol. 317, Springer-Verlag, Berlin and New York, 1973, Exposé 409, pp. 167–200.

7. A. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper*, Math. Z. **39** (1934), 269–404.

8. P. Robba, *Fonctions analytiques sur les corps valués ultrametriques complets*, Prolongement Analytique et Algèbres de Banach Ultramétriques, Astérisque no. 10, Soc. Math. France, Paris, 1973, pp. 109–220.

9. _____, *On the index of p-adic differential operators*. I, Ann. of Math. **101** (1975), 280–316.

10. O. Schilling, *The theory of valuations*, Math. Surveys, no. 4, Amer. Math. Soc., Providence, R. I., 1950.

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08540

DEPARTEMENT DE MATHEMATIQUE, UNIVERSITE DE PARIS, XI PARIS 91400, ORSAY, FRANCE