Rodolphe RICHARD
On $\pi$-exponentials II: Closed formula for the index

<http://jtnb.cedram.org/item?id=JTNB_2016__28_2_539_0>
On $\pi$-exponentials II: Closed formula for the index

par Rodolphe Richard


Abstract. This article pursues the series, initiated by [17], dedicated to Pulita’s $\pi$-exponentials and $p$-adic differential equations of rank one with coefficient a polynomial in a ultrametric extension of the field of $p$-adic numbers. We complement [17] with a closed formula for the index. In particular this answers one problem studied in [15]. We also answer a question [21, §2.4] of Robba on the comparison from rational cohomology toward Dwork cohomology (i.e. rigid cohomology on a disk with coefficient). We also indicate a procedure to palliate the lack of isomorphy of this comparison. We establish by the way a characterisation of soluble equations up to equivalence on the dagger algebra. An appendix determine the polynomial complexity of the derived algorithm.

This paper deals with rank one isocrystals over the rigid affine line in characteristic $p > 0$. This corresponds to the datum of an ordinary linear...
differential equation of order one, over a disk of radius $1 + \varepsilon$ for unspecified $\varepsilon > 0$.

Such equations have been actively studied since Bernard Dwork, [7], and Philippe Robba [20], [22], and more recently by Bruno Chiarelotto [1], Daniele Chinellato [3], Gilles Christol [4], Richard Crew [6], Laurent Garnier [9], Shigeki Matsuda [14], Andrea Pulita [16], [2].

This class of isocrystals are investigated because they constitute a family of handy examples where essentially all interesting phenomena arises explicitly.

However explicit computations were quite involved since the paper of Pulita who obtained a systematic description of isomorphism classes of these equations in term of Witt vectors (following an original unexploited idea of Robba also used by Dwork, Chinellato, Matsuda).

**General notations.** Fix a prime $p$ and a ultrametric field extension $K$ of $\mathbb{Q}_p$, and write $|-|$ for its absolute value. An element $x$ of $K$ is a (ultrametric) integer of $K$ if $|x| \leq 1$. We denote $R$ the ring of integers of $K$, and $\kappa$ its residue field.

(characteristic 0) $K \leftarrow R \rightarrow \kappa$ (characteristic $p$)

1. **Results**

1.1. **Problem.** For any $L(T)$ in $K[T]$ we consider the differential equation

$$y' = L(T) \cdot y. \tag{1.1}$$

Let $P(T)$ be given by: $P(0) = 0$ and $P'(T) = L(T)$, so that the series

$$e(T) = \exp(P(T)) \tag{1.2}$$

is defined in $K[[T]]$ and is a solution of (1.1).

We may refer indifferently to a differential equation like (1.1) through the equation (1.1) itself, the corresponding polynomial $P(T)$, or the corresponding series $e(T)$.

1.1.1. Denote $O^\dagger \subseteq K[[T]]$ the sub-algebra of “overconvergent” series: convergent series with unspecified radius of convergence $> 1$. We consider (1.1) as a differential equation over $O^\dagger$.

One says that (1.1)

- is trivial if $e(T)$ has radius $> 1$, and, more generally,
- is soluble if $e(T)$ has radius $\geq 1$ (radius 1 is included).

1.1.2. Given two differential equations such as (1.1), with corresponding series $e_1(T)$ and $e_2(T)$, they are equivalent if the identity $e_1 \cdot O^\dagger = e_2 \cdot O^\dagger$
holds. Equivalently, the series $e_1(T)/e_2(T)$ (which corresponds to the difference$^1$ of the equations) is in $O^!$: its radius of convergence is $> 1$.

1.1.3. We are concerned here with the computation of a numerical invariant, under equivalence 1.1.2, associated with soluble (1.1): its index $\chi \in \mathbb{Z}$ (cf. §1.5). Invariants holding equivalent information are the $p$-adic irregularity of [16, §2.4], the first slope in [4, Definition 2.6], the Swan conductor ([16, Théorème 1.4.4. 4.], see also [2] for a more refined version of the Swan conductor, in the rank one case, which also involves the first slope, and [12] for general differential modules).

**Remark 1.1.** In principle, the determination of the radius of convergence function from [17, §5 (23)] allows us to infer quite directly the slopes and then the index. Nevertheless, formula [17, §5 (23)] is computationally more involved than [17, Théorème 3]. We will obtain here a computationally more direct approach, yielding a more satisfying answer regarding the applications 2.1 and 2.2. We refer to the first article of our series [17] for comparison between the present approach and earlier work of Robba, Matsuda, Pulita on these questions.

1.2. Some notations from [17]. Fix an integer $D \geq \deg(P)$ and write

\[ d = \left\lfloor \log_p(D) \right\rfloor, \quad \text{and} \quad d_i = \left\lfloor \log_p(D/i) \right\rfloor \quad \text{for} \quad 1 \leq i \leq D. \]

We assume that $K$ has a primitive root of unity $\zeta$ of order $p^{d+1}$, and denote

\[ \pi_i = \zeta^{p^{d-i}} - 1 \quad \text{for} \quad 1 \leq i \leq d. \]

(Uniformisers of a tower $\mathbb{Q}_p(\pi_0) \subseteq \ldots \subseteq \mathbb{Q}_p(\pi_d)$ of ramified cyclotomic extensions.)

Write $P(T)$ as $\sum_{i=1}^D a_i \cdot T^i$, let

\[ \tilde{P}(T) = \sum_{i=1}^D a_i \cdot T^i / \pi_{d_i} \]

(1.5)

\[ \tilde{e}(T) = \exp(\tilde{P}(T)) \quad \text{(mod} \quad (T^{D+1})). \]

**Remark 1.2.** The integers (1.3) are the ones which describe the decomposition of the ring of truncated universal Witt vectors of length $D$ into products of rings of $p$-typical Witt vectors, of lengths the $d_i$ (cf. [17, §2.6] and §1.6.2). The uniformisers $\pi_i$, and more general ones, come from the work [16] of Pulita. These ones were already found in [14]. The appendix [17, §C] applies here: everything proceeds without modification with the more general $\pi_i$ of Pulita.

$^1$We mean actually difference on the right-hand side only of (1.1). In terms of differential module of ranks one, the addition of right-hand sides corresponds to $\otimes$ operation, which is a group operation.
1.3. Some results of [17]. This gathers what we need from [17].

**Theorem 1.3** ([17]). The following are equivalent (with notations above):

1. the radius of convergence of $e(T)$ is $\geq 1$ (resp. $> 1$);
2. the coefficients of $e(T)$ are integers (resp. are divisible by $\pi_0$, except maybe for finitely many);
3. the coefficients of $\tilde{e}(T)$ are integers (resp. $\tilde{e}(T)$ reduces to 1 in the quotient $\kappa[T]/(T^{D+1})$).

**Remark 1.4.** Recall this corresponds to the solvability (resp. triviality) of (1.1). We note that, in condition (3), the reduction invoked in the trivial case is meaningful thanks to the integrality expressed in the solvable case.

The solvable case of Theorem 1.3 is namely [17, §2.5 Théorème 2, §2.10 Corollaire 1]. What is left to prove is the triviality case (the “resp.” inside parentheses).

**Proof.** The equivalence of the first two statements in the triviality case follows from [17, Proposition 4]. The equivalence of the first and third statement in the triviality case follows from the formula for the radius of convergence [17, Théorème 3]. $\square$

1.4. Characterisation. In the solvable case, cf. Remark 1.4, we may reduce $\tilde{e}(T)$ into

$$(1.6) \quad \tilde{e}(T) \in \kappa[T]/(T^{D+1}).$$

As a consequence of Theorem 1.3, a soluble (1.1) is characterised by $\tilde{e}(T)$ as follows.

**Proposition 1.5** (Characterisation of differential equations). Consider

- two polynomials $L_1(T)$ and $L_2(T)$ in $\kappa[T]$, each of degree at most $D$;
- the corresponding differential equations, say (1.1)$_1$ and (1.1)$_2$ resp.;
- and the corresponding truncated series $\hat{e}_1(T)$ and $\hat{e}_2(T)$.

Assume solubility of (1.1)$_1$ or (1.1)$_2$. Then (1.1)$_1$ and (1.1)$_2$ are equivalent if and only if

$$(1.7) \quad \hat{e}_1(T) = \hat{e}_2(T).$$

As may be expected we will extract the index form this complete invariant $\hat{e}(T)$.

**Proof.** Solubility is invariant under equivalence; we can assume both (1.1)$_1$ and (1.1)$_2$ are soluble. It suffices to show the equation associated with $L_1(T) - L_2(T)$ is trivial. The associated truncated series is

$$\hat{e}_1(T)/\hat{e}_2(T) \pmod{(T^{D+1})}.$$
It has integral coefficients (recall $1 + TR[[T]]/(T^{D+1})$ is a multiplicative group). The identity (1.7) is equivalent to the triviality of the reduction of $\tilde{e}_1(T)/\tilde{e}_2(T)$ in $\kappa[[T]]/(T^{D+1})$. By Theorem 1.3, this is equivalent to condition (1) of Theorem 1.3. This concludes. \hfill \Box

**Remark 1.6.** Conversely, we may lift a given $\tilde{e}(T)$ to some $\hat{e}(T)$ in $R[[T]]/(T^{D}+1)$, write $\tilde{P}(T)$ the logarithm of the latter, considered as a polynomial, deduce $P(T)$, take its derivative $L(T)$ and get an equation (1.1) which will produce this $\hat{e}(T)$.

**Remark 1.7.** The construction of $\hat{e}(T)$ from (1.1) depends on the choice of $D$. For example, take for $L(T)$ the constant polynomial $\pi_0$, so that $e(T) = \exp(\pi_0 \cdot T)$, which is known to have radius 1.

1. For $D = 1$, one gets $\tilde{P}(T) = T$, and one has
   
   $\tilde{e}(T) = 1 + T \pmod{(T^2)}$
   $\tilde{e}(T) = 1 + T \pmod{(T^2)}$.

2. For $D = p - 1$, one gets $\tilde{P}(T) = T$, and one has
   
   $\tilde{e}(T) = 1 + T + \ldots + T^{p-1}/(p - 1)! \pmod{(T^p)}$
   $\tilde{e}(T) = 1 + T + \ldots + T^{p-1}/(p - 1)! \pmod{(T^p)}$.

3. For $D = p$, one gets $\tilde{P}(T) = \frac{\pi_0}{\pi_1} T$, and one has
   
   $\tilde{e}(T) = 1 + \frac{\pi_0}{\pi_1} T + \ldots + \left(\frac{\pi_0}{\pi_1} T\right)^{p-1} \cdot \frac{1}{(p - 1)!} + \left(\frac{\pi_0}{\pi_1} T\right)^p \cdot \frac{1}{p!} \pmod{(T^{p+1})}$
   $\tilde{e}(T) = 1 + 0 + u \cdot T^p \pmod{(T^{p+1})}$ for the unit $u = -1$ of $\mathbb{Z}/(p)$.

**Remark 1.8** (cf. [16, Introduction]). A famous landmark result is the $p$-adic local monodromy theorem (formerly Crew’s conjecture). The rank one case yields in particular a correspondence between Artin-Schreier-Witt characters of absolute Galois group of a local field in characteristic $p$ and rank one differential equations over the Robba ring. Pulita’s $\pi$-exponential was developed in order to made this correspondence explicit. Given a solvable differential equation (1.1), and some $D$, we constructed a complete invariant $\tilde{e}(T)$. This is a truncated power series, but can be interpreted equivalently as a truncated universal Witt vector, by first theorem of Cartier theory of Witt vectors. Witt motivation for Witt vectors was the classification of cyclic coverings on characteristic zero. The universal Witt vector obtained has a $p$-typical decomposition, and each factor corresponds to some Artin-Schreier-Witt covering, composed with a Kummer covering. Each of this coverings generates by relative rigid cohomology, a degree 1 “$F$-isocrystal” over the affine line in characteristic $p$ with action of $\mathbb{Z}/p^d\mathbb{Z}$ for some $d$. The choice of $\zeta$ determines a character $\chi_{\zeta}$ of $\mathbb{Z}/p^d\mathbb{Z}$ and allows
to consider the $\chi$-equivariant sub-$F$-isocrystal, which is actually of rank 1. It is to be expected that the product of these $F$-isocrystals of rank 1 are realised by the original equation (1.1). Our constructions would provide a computationally accessible exhibition of this correspondence. The details and precise computations for establishing such a fact require lengths in contextualising that should be offered in another article.

1.5. The index $\chi$. We assume the solubility of (1.1). Associated to (1.1) is its index $\chi$.

1.5.1. It is the index of the differential operator\(^2\) in the de Rham complex:

\[(1.8) \quad 0 \to \mathcal{O}^\dagger \xrightarrow{f(T) \mapsto df - L \cdot f \cdot dT} \mathcal{O}^\dagger \cdot dT \to 0\]

namely, the Euler-Poincaré characteristic $\chi = \dim H^0 - \dim H^1$ of the cohomology groups of the complex (1.8). In other words, it is the rigid cohomology of the affine line with coefficient in the differential equation (1.1).

1.5.2. The slope ([4][Definition 2.6 onward]). There is yet another interpretation of this invariant, due to Robba\(^3\). See [4], [22, §9-10] for the notion of a Dwork (or Berkovich) generic point $g_r$ at radius $r \in \mathbb{R}_{\geq 0}$ and more details. We consider the radius of convergence $\text{RoC}(r)$ of (1.1) centered at $g_r$: considering the differential equation given by the coefficient $L(T - g_r)$, it is the radius of convergence of the solution $\exp(P(T - g_r) - P(-g_r))$. Consider the function $\text{RoC}$ viewed in logarithmic abscissa and ordinate:

\[(1.9) \quad v \mapsto \log(\text{RoC}(\exp(v))),\]

It happens to be continuous and piecewise affine: a polygonal line (cf. [17, §5]). Its right derivative at $v = 0$ (the right\(^4\) slope), in the non trivial case\(^5\), is $\chi$.

1.6. Formula for the index. By Proposition 1.5, a soluble (1.1) is characterised by the associated (1.6). One should be able to recover the index from (1.6). For that purpose, we introduce the notation $v_T(-)$ for the valuation associated with $T$. Namely

\[(1.10) \quad v_T(\hat{e}(T) - 1) \text{ is the multiplicity of } 0 \text{ as a root of } \hat{e}(T) - 1,\]

\(^2\)Equivalently, the index of $d : \mathcal{O}^\dagger \cdot e(T) \xrightarrow{f \mapsto df} \mathcal{O}^\dagger \cdot e(T)dT$.

\(^3\)See [19, §1.3 with $a=1$] for a statement with the algebra $\mathcal{H}^+$ of functions converging on the closed disk instead of the dagger algebra, and for the non solvable case. (see also [22, Theorem 10.2.2]) We need to consider the algebra of overconvergent series, instead of $\mathcal{H}^+$, as otherwise, in the solvable case, there is no index (loc. cit.). We refer to the extension [20, §5] of [18] results.

\(^4\)If we parameter the axes with respect to valuations (opposite of $\log$), this is the left slope. Compare the examples from the algorithm joined with [17].

\(^5\)In the trivial case $\chi$ is $h^0 - h^1 = 1 - 0 = 1$, but the slope is zero, as the radius of convergence is constant on the convergence disk. In order to interpret the index $\chi$ as a slope, one introduces a subtlety in the definition of $\text{RoC}$, namely that, at a generic point of radius $r$, the function $\text{RoC}$ is the minimum $\min\{r; \rho\}$ between $r$ and the radius of convergence $\rho$ at this point. Trivial equations will not be of any useful interest here, and we will not need to take this into account.
obviating the case \( \hat{\epsilon}(T) - 1 = 0 \) which corresponds to trivial equations. The algorithm joined to [17] computes \( \hat{\epsilon}(T) \) with some precision. With the slightest extra cost, this allows to exactly deduce \( \hat{\epsilon}(T) \), then \( \nu_T(\hat{\epsilon}(T)) \) and finally (1.12).

1.6.1. \( p \)-typical case. We first treat the \( p \)-typical case. This is the case where

\[
P(T) \in \bigoplus_{i \geq 1} K \cdot T^{p^i}.
\]

**Theorem 1.9** (Closed formula for the index in the \( p \)-typical case). Assume solubility and non triviality\(^6\) of (1.1) and assume (1.11). Then the index of (1.1) is

\[
\chi = 1 - \frac{pd}{\nu_T(\hat{\epsilon} - 1)}.
\]

**Remark 1.10.** As an implied statement: \( \nu_T(\hat{\epsilon} - 1) \) is a power of \( p \). As a corollary: the negative of \( \chi - 1 \), which is the dimension of \( H^1 \), is a power of \( p \).

**Example 1.11.** In the three cases of Remark 1.7, formula (1.12) becomes respectively \( \chi = 1 - p^0/1 \) for (1); \( \chi = 1 - p^0/1 \) for (2); and \( \chi = 1 - p^1/p \) for (3).

1.6.2. \( p \)-typical decomposition. In general we may uniquely write

\[
P(T) = \sum_{1 \leq m \leq D, p \nmid m} P_m(T^m), \text{ where each } P_m \text{ satisfies (1.11)}.
\]

We can correspondingly construct \( e_m(T) := \exp(P_m(T)) \) so that

\[
e(T) = \prod_{1 \leq m \leq D, p \nmid m} e_m(T^m).
\]

We form the corresponding \( \tilde{\epsilon}_m(T) \) and still have

\[
\tilde{\epsilon}(T) = \prod_{1 \leq m \leq D, p \nmid m} \tilde{\epsilon}_m(T^m).
\]

It happens \( \tilde{\epsilon}(T) \) is integral if and only if each factor \( \tilde{\epsilon}_m(T^m) \) is (cf. [17, §X]). Assuming solubility for (1.1), we can consider the corresponding reduction \( \tilde{\epsilon}_m(T^m) \) of \( \tilde{\epsilon}_m(T^m) \) as in (1.6), and still have

\[
\hat{\epsilon}(T) = \prod_{1 \leq m \leq D, p \nmid m} \hat{\epsilon}_m(T^m).
\]

\(^6\)The non-triviality assumption becomes superfluous under the convention that for the null truncated series \( \nu_T(0 (\mod T^{D+1})) = +\infty \), so that the fraction in (1.12) evaluates to 0.
1.6.3. General "global" case. Recall (1.13d), (1.3), (1.10).

**Theorem 1.12** (Closed formula for the index). Assume solubility of (1.1) and consider the decomposition (1.13d). Then the index of (1.1) is

\[
\chi = 1 - \max_{1 \leq m \leq D, p|m} \frac{m \cdot p^d_m}{v_T(\hat{e}_m - 1)}.
\]

2. Applications

2.1. Application to exponential sums. Let us indicate a last interpretation of the index. Given a \( p \)-typical soluble (1.1) one can construct families of exponential sums, which are written down in [15, §2.3], and some generating function, the \( L \)-function, actually an Euler factor, concretely a polynomial of some degree, say \( \Delta \). The thesis [15] investigates these \( L \)-functions. Its first, of two, problems is this degree \( \Delta \), and [15, Ch. 3, cf. Ch. 5] succeeds in providing bounds using Robba formulas by direct computations of radii of convergence.

On the other hand, the trace formula gives a cohomological interpretation of the \( L \)-function, and its degree is \( \dim(H^1) \). It follows that \( \Delta \) is given:

- in the trivial case, by \( \dim(H^1) = 0 \) (but \( \chi = \dim(H^0) = 1 \neq 0 \));
- in the non trivial (but still soluble) case, by \( \dim(H^1) = -\chi \).

More precisely, [15] sums are constructed from a polynomial (Witt) vector \( f(T) = (f_0(T), \ldots, f_m(T)) \), and allegedly associated with the equation (1.1) corresponding to (cf. [15, §2.1])

\[
P(T) = \pi_m \phi_0(f(T)) + \ldots + \pi_0 \phi_m(f(T)),
\]

with \( \phi_i(f) = p^0 \cdot f_0^{p^i} + \ldots + p^i \cdot f_j^{p^0} \).

As a consequence, Theorem 1.12 answers the first problem studied in the reference [15] with the closed formula (1.12). The estimates from [15, end of Ch. 3, cf. Ch. 5] follows from the bound (take \( D = \deg(P) \) in (1.14) or see §2.2 infra)

\[
\chi \geq 1 - \deg(P) \geq 1 - \max\{p^m \deg f_0; \ldots; \deg f_m\}.
\]

The algorithm accompanying [17] allows to compute the right hand side of (1.14).

2.2. Application to comparison. Many ideas here have their roots in Robba’s work (see for instance [22, §13.2,13.3]). We refer to [16, Ch. 1, 1.1.1–1.1.4] for a more historically oriented perspective, and to [17, §0] for relations with [4].

\[\text{Provided one has established the link between Pulita's } \pi \text{-exponentials and the exponential sums written down in [15]. This link is claimed without proof in [15], and it is the subject of a projected article in the series started by [17] and continued here.}\]
2.3. Comparison map. Let us consider the inclusion of de Rham complexes, into (1.8), of

\begin{equation}
0 \to K[T] \xrightarrow{\frac{f(T) - L \cdot f \cdot dT}{df}} K[T] \cdot dT \to 0.
\end{equation}

The cohomology groups of (1.8) are referred sometimes as analytic cohomology, Dwork cohomology or rigid cohomology, etc. For (2.3), one sometimes speaks of rational or algebraic cohomology. We will use [21, §2.4] terminology: Dwork and rational cohomology. The inclusion of complexes induces a comparison map from rational cohomology to Dwork cohomology, say

\begin{equation}
H^0_{\text{rat comparison}} \to H^0 \quad H^1_{\text{rat comparison}} \to H^1
\end{equation}

"easily shown"\(^8\) to be injective and surjective respectively (loc. cit.).

A recurrent difficulty has been that it is not always an isomorphism: For example Boyarsky principle, on variation of cohomology and Gross-Koblitz formula for the \(p\)-adic Gamma function, relies on an interplay between the two cohomology spaces:

- a Frobenius endomorphism which comes from the Dwork cohomology,
- a functional equation which comes from the rational cohomology.

(We refer to [8, 13].)

2.4. Comparison criterion. By injectivity and surjectivity property, the fact that the comparison map is an isomorphism is equivalent to the equality of the dimensions of the Dwork and rational cohomology groups. We precisely computed it for the Dwork cohomology. For the rational cohomology, this is simply given by the degree of the polynomial coefficient \(L(T)\) of (1.1) (cf. [22, 13.4]). We can therefore state the following.

\(^8\)Let us details here the affirmation of Robba. Injectivity: two distinct solutions of (1.1) in \(K[T]\) defines solutions in \(\mathcal{O}\), and stay distinct in \(\mathcal{O}\). Surjectivity is more involved. We use the density of \(K[T]\) in \(\mathcal{O}\), and the continuity of the quotient map from \(\mathcal{O} \cdot e \cdot dT\) to the finite dimensional \(H^1\), with respect to the separated topology on \(H^1\) (which is not a priori the quotient topology). The image of \(K[T] \cdot e \cdot dT\) will then be dense in the finite dimensional \(H^1\), and hence will be \(H^1\) itself. Passing to the quotient we get the desired result. The topology on \(\mathcal{O}\) is that of an inductive limit of Banach spaces.

- The density can be checked on each Banach space separately. It follows for the convergence, with respect to the Gauss norm, of the truncated series towards a power series converging on the closed unit disc.
- The continuity follows from [22, Proposition 7.2.2] and more precisely to the reference [13] to Grothendieck lectures [10].

The author thanks the referee, who provided the reference [5] (which also relies on [10]).
Corollary 2.1. Consider a solvable (1.1), choose $D = \deg(P)$ and let $D = m \cdot p^n$ with $p \nmid m$. The comparison map (2.4) from de Rham cohomology with coefficients in $K[T]$ to cohomology of (1.8) is an isomorphism if and only if (equivalently):

- one has $\chi = 1 - D$;
- the factor $\hat{e}_m(T)$ in (1.13d) has non zero derivative at 0.

Such question was already asked and answered by Robba in [20, resp. §10.6, §10.11], especially about the index [20, §10.7]. The novelty here is easily the criterion given by the easily computable $\hat{e}_m(T)$, and the direct algebraic method (Robba’s method, already algorithmic, already using the exponentials, was recursive).

Let us note that in the special case $p \nmid D$, ie $D = m$ this reduces to an innocuous check, namely that:

$$\text{(2.5) the dominant coefficient } a_D \text{ of } P \text{ satisfies } |a_D| = |\pi_0|. $$

The author thanks the referee for pointing [22, 13.3.1] which already provides a very convenient alternative criterion.

Example 2.2. As an illustration consider the following example. It seems related the conjecture formulated in [13]. Let $P$ be a polynomial with coefficients in $\mathbb{Q}$, and write $D = \deg(P)$. If $p$ is a large enough prime, then we may assume that every coefficient of $P$ is a $p$-adic unit, as well as $D!$. Consider such a $p$, a corresponding $\pi_0$, and the series $e(T) = \exp(\pi_0 \cdot P(T))$.

Then the $p$-typical decomposition corresponds to the monomial decomposition of $P$. For every monomial $a_i T^i$, the series $e_i(T) = \exp(\pi_0 a_i T^i)$ is easily seen to have radius 1, and index $1 - i$. The check (2.5) is satisfied for any $e_i(T)$ and for $e(T)$. We can conclude as follows.

Proposition 2.3. For all but finitely many $p$, the series $\exp(\pi_0 \cdot P(T))$ defines a soluble differential equation with index $1 - D$ and for which the comparison of cohomologies (2.4) is an isomorphism.

For the remaining $p$, the equation may be trivial, not soluble or lack comparison. For the first two issues, the computation of the radius of convergence may help choose a suitable change of variable. For the lack of comparison, the procedure below may apply.

2.5. Factorisation. Without detailing the proof, we mention a complement. Assume for convenience that $\kappa = \mathbb{Z}/(p)$. If $P = a_1 T + a_p T^p + \ldots + a_{pd} T^{pd}$ is a polynomial satisfying (1.11), we define its shift as

$$VP = a_p T + a_{p^2} T^{p^2} + \ldots + a_{pd} T^{pd-1}. $$
Proposition 2.4 (Complement to Corollary 2.1). Assume a solvable (1.1) does not provide comparison isomorphism. Define \( F = V P_m(T^m) - P_m(T^m) \). The decomposition

\[
P = F + (P - F)
\]

is such that

- the term \( F \) defines a trivial differential module;
- the term \( P - F \) has degree \( \leq D - 1 \).

In other words, the equation defined by \( P - F \) is equivalent to the one defined by \( P \) but has strictly lower dimensional rational cohomology.

The only non elementary statement is the triviality of the differential module attached to \( F \). This (mostly)\(^9\) amounts to the existence of a Frobenius structure.

Applied iteratively, this procedure can restore the lack of comparison without changing the Dwork cohomology. We dedicate to yet another future article the consequences of this application to Boyarsky principle. For future reference, we call \( F \) the superfluous factor of degree \( D \).

This is again similar to [22, 13.3.1], and mostly well known to Robba, and its use in the end of the proof of [22, 13.3.2]. More precisely, Our variant, from a computational point of view, may be more satisfactory, as it does not involves taking arbitrary roots \( a_1/d \), as would the original [22, 13.3]. When used recursively, the extensions implied may bring with them a computational weight.

3. Demonstrations

3.1. Products of differential equations and index. Recall that for two non vanishing converging series with distinct radius of convergence, the radius of the product series is the smaller of the two (distinctness is paramount here\(^10\)). A variation of this observation, coupled with the continuity of the function radius of convergence, implies the following.

Lemma 3.1 ([4], [16, Corollary 2.4.8]). Given two polynomials \( L_1 \) and \( L_2 \) whose corresponding equations (1.1) are solvable, but with distinct index \( \chi_1 \) and \( \chi_2 \), the product equation, with coefficient \( L = L_1 + L_2 \), is still solvable and has index \( \min \{ \chi_1; \chi_2 \} \).

\(^9\)The Frobenius structure is the one mentioned at the end of the proof of Lemma 3.2. The mostly refers to the fact that in factorisation (3.5), the factor \( AH(w_m T) \) will be trivial, \( \equiv 1 \) (mod \( (T^d + 1) \)). Actually \( w_m \) is the derivative of \( c_m(T) \) involved in Corollary 2.1.

\(^10\)Starting from a product \( fg \), we apply [23, §6.1.2 Prop. 2] to get \( r_{fg} \geq \min(r_f, r_g) \) and also \( r_f \geq \min(r_{fg}, r_{1/f}) \). Using [23, §6.2.2 Corr. to Th. 1], the nonvanishing yield \( r_{1/f} \geq r_f \). Hence \( r_f \geq \min(r_{fg}, r_{1/f}) \) implies \( r_f \geq \min(r_{fg}, r_f) \) and thus \( r_f \geq r_{fg} \). Conversely \( r_{fg} \geq \min(r_f, r_g) \) implies \( r_{fg} \leq r_f \) and we are done.
We refer to [4] for a detailed explanation, and for these other facts:

(i) For any unit $u$ in $R^\times$ the equations given by $L(T)$ and by $L(u \cdot T)$ share the same index. (There is an obvious isomorphism of de Rham complexes.)

(ii) For any $m$ positive and prime to $p$ (resp. $m = p$), and a soluble equation given by $L(T)$ and of index $\chi$, the derived equation given by $L(T^m)$ is soluble and has index $\chi'$ such that $\chi' - 1 = m \cdot (\chi - 1)$ (resp. $\chi' = \chi$). (cf. [4, Proposition 2.8])

Proof of Theorem 1.12 from Theorem 1.9. The decomposition 1.6.2 induces a corresponding decomposition of (1.1). The equation corresponding to some $P_m(T)$ is eligible for Theorem 1.9: It is trivial or its index has the form $1 - p^i$ for some $i \geq 1$. By the fact (ii) above, the equation corresponding to $P_m(T^m)$ has index $1 - mp^i$.

It follows that each of the non trivial factors of (1.1) have distinct index. By Lemma 3.1 above, the index of (1.1) is the minimum of the index of the factors. This yields (1.14) and concludes. □

3.2. Facts form Witt vectors theory. (cf. [17, §2.6,2.7] and references therein.) For any algebra ring $A$ over the local ring $\mathbb{Z}(p)$, recall: the notation $\Lambda(A) = 1 + TA[[T]]$; that the Artin-Hasse series

(3.1) \[ AH(T) = \exp(T + Tp/p + Tp^2/p^2 + \ldots) = 1 + T + \ldots \]

has coefficients in $\mathbb{Z}(p)$, and defines an element of $\Lambda(A)$. The Artin-Hasse map

(3.2) \[ (w_0, \ldots, w_i, \ldots) \mapsto AH(w_0T) \cdot \ldots \cdot AH(w_iTp^i) \cdot \ldots \]

embeds into $\Lambda(A)$ the ring $W(A)$, of ($p$-typical) Witt vectors with entries in $A$, mapping the unit $(1,0,0,\ldots)$ to (3.1).

If $p$ is not a divisor of zero in $A$, then $A$ embeds in a $\mathbb{Q}$-algebra, hence we can form the logarithm power series, and apply it to series in $\Lambda(A)$. For such $A$, the image of $W(A)$ in $\Lambda(A)$ describes the series in $\Lambda(A)$ whose logarithm belongs to $\prod_{i \geq 0}(\mathbb{Q} \otimes A) \cdot Tp^i$ (compare (1.11)). Every such series uniquely decompose as (3.2).

We denote $W_d(A)$ the ring of truncated Witt vectors $(w_0, \ldots, w_d)$ of length $d + 1$. By quotient, the Artin-Hasse map (3.2) induces an embedding of $W_d(A)$ into the quotient $\Lambda(A)/(1 + T^{D+1})$ (cf. [17, §2.6,2.7]). Every element $e$ in the image factors uniquely as

(3.3) \[ e \equiv AH(w_0T) \cdot \ldots \cdot AH(w_dTp^d) \pmod{(T^{D+1})}, \]

where $(w_0, \ldots, w_d) \in W_d(A)$ is the corresponding truncated Witt vector.
The map (3.2) and decomposition (3.3) are functorial with respect to the $\mathbb{Z}_p$-algebra $A$. In concrete terms, each $w_i$ may theoretically be computed by polynomials over $\mathbb{Z}_p$ in the first $i$ coefficients of the decomposed series ([11, §§9.28, 9.63–9.71, 14.15–14.25]).

3.3. Using §3.2, we finish the proof of our results.

Proof of Theorem 1.9. The property (1.11) on $P(T)$ obviously extends to $\tilde{P}(T)$. Equivalently $\exp(\tilde{P}(T))$ is a $p$-typical series: it belongs to the image of $W(K)$ in $\Lambda(K)$. Consequently, its truncation $\tilde{e}(T) \in \Lambda(K)/(1 + T^{D+1})$ actually comes from $W_d(K)$.

We now use the solvability assumption of Theorem 1.9, interpreted by condition (3) in Theorem 1.3, and conclude $\tilde{e}(T) \in \Lambda(R)/(1 + T^{D+1})$. The decomposition (3.2) is functorial, hence $\tilde{e}(T)$ comes from $W_d(R)$.

By functoriality of the Artin-Hasse map, the reduction map

$$ W_d(R) \xrightarrow{\text{AH map for } R} \Lambda(R)/(1 + T^{D+1}) $$

(3.4) $R \xrightarrow{\text{red}} \kappa$ induces

$$ W_d(\kappa) \xrightarrow{\text{AH map for } \kappa} \Lambda(\kappa)/(1 + T^{D+1}), $$

which is commutative, by functoriality again. The truncated series $\tilde{e}(T)$ has a reduction to characteristic $p$ in $\Lambda(\kappa)/(1 + T^{D+1})$, which, by commutativity, lies in the image of $W_d(\kappa)$. This reduction is by definition $\tilde{e}(T)$ of (1.6). We may apply (3.3) to $\tilde{e}(T)$. This yields the factorisation, over the filed $\kappa$,

$$ \tilde{e}(T) = \text{AH}(w_0 T) \cdot \text{AH}(w_1 T^p) \cdot \ldots \cdot \text{AH}(w_d T^{p^d}). $$

(3.5)

We now use the solvability assumption of Theorem 1.9, interpreted by condition (3) in Theorem 1.3, and conclude $\tilde{e} \not\equiv 1 \pmod{(T^{D+1})}$. Hence at least one of the factors in (3.5) is not $1 \pmod{(T^{D+1})}$, and $k = \min\{i \mid 1 \leq i \leq d, w_i \neq 0\}$ is well defined. As $\text{AH}(T) \equiv 1 + T \pmod{(T^2)}$, we have

$$ \text{AH}(w_i T^{p^i}) = 1 + w_i T^{p^i} \pmod{T^{p^{i+1}}}. $$

From (3.5) and the definition of $k$, it follows that

$$ \tilde{e}(T) - 1 \equiv w_k T^{p^k} \pmod{T^{p^{k+1}}}, \text{ with } w_k \neq 0. $$

We deduce: $v_T(\tilde{e} - 1) = p^k = p^{\min\{0 \leq i \leq d \mid w_i \neq 0\}}$.

The factorisation (3.5) of $\tilde{e}$ corresponds to a factorisation of (1.1) whose factors are uniquely defined up to equivalence §1.1.2, by Remark 1.6: A factor of (1.1) associated with $\text{AH}(w_i T^{p^i})$ is obtained by lifting $\text{AH}(w_i T^{p^i})$ to any series $\tilde{e}_i$ in $\Lambda(R)/(1 + (T^{D+1})$, and using (1.5) backwards.

By Theorem 1.3, a factor $\text{AH}(w_i T^{p^i})$ of (3.5) such that $w_i = 0$ is associated with trivial equations. Otherwise, by Lemma 3.2 below, it may be associated with an equation of index $1 - p^{d-i}$. We note that the non trivial
factors are associated with distinct indices. We may use Lemma 3.1, and conclude the proof:

\[ \chi = \min \{ 1 - p^{d-i} \mid 0 \leq i \leq d, \ w_i \neq 0 \} = 1 - p^{d-k} = \frac{p^d}{v_T(\tilde{e} - 1)} . \]

Lemma 3.2. For any \( \lambda \) in \( \kappa^\times \) and any \( 0 \leq i \leq d \), there is a solvable differential equation (1.1) of index \( 1 - p^{d-i} \) such that

\[ \tilde{e}(T) = AH(\lambda T^{p^i}). \]

Proof. Thanks to remark (i) of § 3.1, we may assume \( \lambda = 1 \), maybe considering an extension \( \kappa(\lambda^{1/p^i}) \) of \( \kappa \). Let us denote (the “\( \pi \)-exponentials” of [16], cf. [17, §B], [22, 13.2.1])

\[ e_k(T) = \exp \left( \pi_k T + \ldots + \pi_0 T^{p^k}/p^k \right) . \]

(These exponentials and their properties, were systematically studied by Pulita. There were already proved to exists in the work of Robba, see for instance [20, §10.8, §10.12]. Matsuda already gave some explicit exponentials of such kind.)

Recall (3.1) and (1.5). An equation satisfying (3.6) is the one such that

\[ e(T) = e_{d-i}(T^{p^i}) . \]

Pulita proved that \( e(T) = e_{d-i}(T^{p^i}) \) defines a solvable equation of index \( 1 - p^{d-i} \) ([16], or [22, 13.3.1] together with the solvability in [17, §2.5]). From (ii) in §3.1, the same holds for \( e_{d-i}(T^p) \), for \( e_{d-i}(T^{p^2}) \ldots \) and for \( e_{d-i}(T^{p^i}) \). This concludes the proof. (Actually these equations have a Frobenius structure, cf. [16], which make them equivalent to each other.)

Remark 3.3. The decomposition (3.3) is classical in Witt vectors theory, at least since Cartier. We applied it to \( \tilde{e}(T) \). It applies equally to \( \tilde{e}(T) \). Its counterpart for the series \( e(T) \) itself is a decomposition into \( \pi \)-exponentials, and it is due to Pulita. In a sense, we exhibit and retrieve here Pulita’s decomposition as a Cartier dual of decomposition (3.3).

Remark 3.4. Globalisation of Remark 3.3. Combining the \( p \)-typical decomposition and \( \pi \)-exponential decomposition yield, for \( \tilde{e}(T) \) in \( \Lambda(\kappa)/(1 + T^{D+1}) \) a factorisation

\[ \tilde{e}(T) = \prod_{1 \leq n = mp^i \leq D} AH(u_n T^n) \]
which is unique\textsuperscript{11}. In terms of the nullity of the $u_i$, we recover the index as (3.8)

$$\chi = 1 - \max \left\{ m \cdot p^\left\lfloor \log_p(D/n) \right\rfloor \mid 1 \leq n \leq D, \, u_n \neq 0, \, n = mp^e, \, p \nmid m \right\}.$$ 

**Appendix A. Polynomial complexity**

Together with [17] is an algorithm which computes $\tilde{e}(T)$ form $P(T)$. We discuss here two points which were left untouched: the $p$-adic precision required; and the complexity. The main computational operation is $\tilde{P}(T) \mapsto \tilde{e}(T)$.

**Remark A.1.** The following has benefited discussions with Jan Tuitman.

**A.1. Complexity.** Let us write $\tilde{L}(T) = \sum_{i=0}^{D-1} c_i T^i$ the derivative of $\tilde{P}(T)$. In order to compute $\tilde{e}(T)$ we do solve the differential equation $y' = \tilde{L} \cdot y$ in $K(\zeta)[T]/(T^{D+1})$. Writing $\tilde{e}(T) = \sum_{i=0}^{D} b_i T^i/i!$, one has $b_0 = 1$ and the recurrence relation of order $D$,

$$b_{i+1} = \sum_{k=0}^{D-1} c_k \cdot b_{i-k}, \quad \text{(with } b_i = 0 \text{ for } i < 0)$$

which it will suffice to apply $D - 1$ times. This amounts to $D - 1$ summation of a total of the triangular $D(D - 1)/2$ number of products, all to the required precision. This amounts to $O(D^2)$ pairwise products and additions.

Assume

$$\text{(A.2) precision is } O(p^a) \text{ and ramification index is } e.$$ 

Assuming pairwise products and addition in a polynomial time $O((ae)^\eta)$, this gets a complexity

$$\text{(A.3) } O(D^2(ae)^\eta).$$

We usually have $e = O(D)$ and $a = O(D)$ (see below). For a quasi-linear exponent $\eta$, we get a quasi-quartic complexity. This is yet to multiply with the complexity of the residue field operations underlying our product and additions. (dependence in $p$ and the residual degree).

**A.2. Precision.** The truncated series $\tilde{e}(T)$ has finitely many $p$-adic coefficients, all of which have infinitely many $p$-adic digits, provided elements of the field $K$ allows representation by digits.

\textsuperscript{11}Unicity holds for any series $AH(T)$ such that $v_T(AH(T) - 1) = 1$. For the series $1 - T$ the $u_i$ are the universal Witt vector coordinates. But for (3.8), this is important to choose the $p$-typical $AH(T)$. 
A.2.1. Ramification. We will assume that $K$ is a finite extension of $\mathbb{Q}_p$: it hence has finite residue field, of finite degree $f_K$ over $\mathbb{Z}/(p)$, and finite ramification index $e_K$. The working field is the ramified cyclotomic extension $K(\zeta)$, with same residue field, but may have ramification index $e$ from $p^d \cdot \frac{p-1}{p} \geq D \frac{p-1}{p}$ up to $e_K \cdot p^d \cdot \frac{p-1}{p} \leq e_K \cdot D$. In order to distinguish between the complexity originating form $K$ and from $D$, we do not assume that $\zeta$ belongs to $K$.

\begin{equation}
(A.4) \quad e = \Omega(D) \text{ for a given } K \text{ and } p, \text{ and } e = O(D) \text{ for a given } K.
\end{equation}

A.2.2. Wanted precision. We still need to decide up to which precision we want to compute the coefficients of $\tilde{e}(T)$. We want enough precision to determine the radius of convergence through formula [17, Théorème 3 (14)], and, in the soluble case, for computing $\hat{e}(T)$. We will ask for enough precision in order to compute the first digit of the coefficients of $\tilde{e}(T)$ achieving the maximum in the radius formula. In the solvable case, these are the coefficients reducing to non zero coefficients of $\tilde{e}(T)$.

A.2.3. Preparation. It is easy to obtain the smallest $k$ such that $\tilde{P}(\pi_d^k T)$ has integer coefficients. In terms of the normalised $p$-adic valuation $v_p$,

$$k = \left\lceil \min v_p(\tilde{a}_i)/(i \cdot v_p(\pi_d)) \right\rceil \text{ where } \tilde{P} = \sum_{i=1}^{D} \tilde{a}_i T^i.$$ 

We will use the substitution of $T$ by $\pi_d^k T$. This way, by integrality of $\tilde{P}$ the recurrence relations (A.1) will always be computed in $R$. Moreover, by the minimality condition, we obtain in the same time, the Gauss norm lower bound

\begin{equation}
(A.5) \quad \|P\| \geq \|\pi_d\|^{D-1} > \|p\pi_0\| = |p|^{p/(p-1)}.
\end{equation}

Such substitution is likely to destroy the solvability property. Before reducing $\tilde{e}(T)$ to compute $\hat{e}(T)$, we must not forget to substitute back the variable. Assuming this substitution, we will be able to express compute uniformly our need in precision in terms of absolute precision.

A.2.4. Minoration. Identifying $\tilde{P}(T)$ with a truncated series in the quotient $K(\zeta)[T]/(T^{D+1})$, we compute the transformation $\exp : \tilde{P}(T) \mapsto \tilde{e}(T)$ from $K(\zeta)[T]/(T^{D+1})$ to itself. This is a polynomial operation: we may substitute exp with the truncated power series

$$1 + \tilde{P} + \tilde{P}^2/2 + \ldots + \tilde{P}^D/D!,$$

whose truncation gives $\tilde{e}(T)$.

We get back $\tilde{P}(T)$ from $\tilde{e}(T)$ by applying the truncated power series of $\log(1-X)$ to $1-\tilde{e}(T)$. Assuming $\|X\| \leq \|\pi_0\|$ we have $\|\log(1-X)\| = \|X\|$
for the untruncated power series, hence
\[ \| \tilde{P} \| \leq \| \log(1 - \tilde{e}) \| = \| \tilde{e} \|. \]
Together with (A.5), this yields
\[ (A.6) \quad \| \tilde{e} \| > |p\pi_0|. \]

A.2.5. Minimal radius. We seek to apply the formula for the radius. We know that at least one coefficient of \( \tilde{e} \) is at least \( |p\pi_0| \) in absolute value. In the least favourable case, this is the coefficient of degree 1, and we need to compute the coefficient of degree \( D \) up to precision \( O((p\pi_0)^D) \) in order to use [17, Théorème 3]. Finally let us note that the coefficients of \( \tilde{e} \) are not the \( c_i \) from (A.1) but are the \( c_i/i! \). This involves an extra \( |i!| \) factor in precision for computing \( c_i \). We recall \( 1/|D!| \leq 1/|\pi_0|^D \). In the end, an absolute precision \( O(p^a) \) is sufficient, with
\[ a = D \cdot (1 + 2\nu_p(\pi_0)) = D \cdot \frac{p + 1}{p - 1} = O(D). \]

References


Rodolphe Richard
Witte de Withlaan 17,
2253XS Voorchoten, Nederland
E-mail: rodolphe.richard@normalesup.org