Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 344 (2007) 187–190
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Algebraic Geometry/Ordinary Differential Equations

Algebraic properties of a class of p-adic exponentials

Daniele Chinellato

Dip. di Matematica, Via Trieste 63, 35121 Padova, Italy

Received 11 May 2006; accepted after revision 4 December 2006

Presented by Michel Raynaud

Abstract

In this Note we give an algebraic construction of a class of p-adic exponentials of Artin–Hasse type which are convergent in the disk $\mathrm{D}^{-}(0,1)$. Moreover we have a control for the field of coefficients of power series that defines such functions. Such objects were used by Christol and Robba to calculate the irregularity of a rank 1 p-adic differential operator, under the restriction of *spherical completeness* for the field of coefficients, and recently by Pulita, in order to classify the same equations. ***To cite this article: D. Chinellato, C. R. Acad. Sci. Paris, Ser. I 344 (2007).***

Résumé

Propriétés algébriques d'une classe d'exponentielles. Dans cette Note nous donnons une construction algébrique d'une classe d'exponentielles p-adiques du type d'Artin–Hasse qui sont convergentes dans le disque $\mathrm{D}^{-}(0,1)$. Nous avons d'ailleurs un contrôle des coefficients de la série entière qui définit de telles fonctions. De tels objets ont été employés par Christol et Robba pour calculer l'irrégularité d'un opérateur différentiel p-adique d'ordre 1, sous la restriction que le champ des coefficients soit sphériquement complet, et récemment par Pulita, afin de classifier les mêmes équations. ***Pour citer cet article : D. Chinellato, C. R. Acad. Sci. Paris, Ser. I 344 (2007).***

0. Introduction

In this Note we find a family of p-adic exponentials of Artin–Hasse type which are convergent in the disk $\mathrm{D}^{-}(0,1)$. More precisely our main result is the following:

Theorem 0.1 *(Main theorem). Let T be a complete unramified extension of $\mathbb{Q}_p$ with perfect residue field of char $p>0$, and let $P(t)\in\mathcal{O}_T[t]$ be an Eisenstein polynomial of degree $e\leqslant p-1$. Then there exists a sequence $(\alpha_0,\alpha_1,\dots)\in(\mathcal{O}_{\overline{T}})^{\mathbb{N}}$ such that the following assertions hold for all natural numbers $n\geqslant 0$:*

(i) *The exponential*

$$E_n(x) := \exp\left(\frac{\alpha_0}{p^n}x^{p^n} + \frac{\alpha_1}{p^{n-1}}x^{p^{n-1}} + \cdots + \alpha_n x\right) \tag{1}$$

E-mail address: chinel@math.unipd.it (D. Chinellato).

doi:10.1016/j.crma.2006.12.001

belongs to $1 + x\mathcal{O}_{K_n}[\![x]\!]$, *where* $K_n := T(\alpha_0, \ldots, \alpha_n)$.

(ii) α_0 *is a root of* $P(t)$, *and inductively* α_n *verifies* $Q^{\sigma^{-n}}(\alpha_n) = \alpha_{n-1}$, *where* $Q := t^{p-e} \cdot P(t)$, σ *is the Frobenius of* T, *and* $Q^{\sigma}(t)$ *is the polynomial obtained by applying* σ *to the coefficients of* $Q(t)$.

(iii) *The extension* K_n/T *is totally ramified for all* $n \geqslant 0$.

(iv) α_n *has* p*-adic valuation* $v_p(\alpha_n) = 1/ep^n$. *Hence* $[K_n : K_{n-1}] = p$, *for all* $n \geqslant 1$, *while* $[K_0 : T] = e$.

The interest of this theorem is that such p-adic exponentials are solutions of rank one solvable differential equations and led P. Robba to obtain an explicit computation of the index of the associated differential operators (cf. [10, §10], [3, §13]). The existence of the α_i's was first proved by Robba in [10, Lemme 10.8] and [3, Théorème 13.2.1], but his method was highly non-explicit and required working in a spherically complete and algebraically closed field.

This problem was pointed out us by B. Dwork [5], and we obtained our result in 1994 under his direction. This Note was not published before, because, in 1994, this statement had already been proved by S. Matsuda (cf. [8, Lemma 1.5]) in the particular case in which $T = \mathbb{Q}_p$, $Q(t) = (1+t)^p - 1$, and $p > 2$. Note that for $P(t) = t^{p-1} - p$, α_0 is the π used by Dwork in the construction of his $\theta(t)$ (cf. [6, Ch II §6], [4, Introduction]). Until recently it seemed to us that the existence of a new and more general proof was not really interesting. But recently A. Pulita in [9] has actually shown how these exponentials, and in particular the proof we give, is crucial in the classification of rank one p-adic differential equations.

1. Notations

If K is a p-adic field we denote by v_p the valuation normalized by $v_p(p) = 1$, by $\mathcal{O}_K$ the ring of integers and by $\overline{K}$ an algebraic closure of K. If A is a ring we denote by $\mathbb{W}(A)$ the ring of Witt vectors on A relative to the prime p (cf. [2]). Let A be a ring, the *phantom map* is the ring homomorphism $w : \mathbb{W}(A) \to A^{\mathbb{N}}$ defined by $\boldsymbol{a} = (a_0, a_1, \ldots) \mapsto w(\boldsymbol{a}) = (w_0(\boldsymbol{a}), w_1(\boldsymbol{a}), \ldots)$, where w_k is defined by $w_k(\boldsymbol{a}) := \sum_{i=0}^{k} p^i \cdot a_i^{p^{k-i}}$.

Remark 1. If the multiplication by p is injective (resp. bijective), then the phantom map is *injective* (resp. bijective) (cf. [2, Lemme 3, §1, n° 2]).

2. Proof of the main theorem

We split the proof into two parts: first we reduce the *existence* of the sequence $(\alpha_n)_{n\in\mathbb{N}}$ to that of a suitable sequence $(\boldsymbol{a}_n)_{n\in\mathbb{N}}$ of Witt vectors, then we construct the sequence $(\boldsymbol{a}_n)_{n\in\mathbb{N}}$ in (many) *effective ways*.

2.1. Reduction to a Witt vector problem

The following lemma provides a criterion for the integrality of certain formal series [2, §1 Ex. 58/c]:

Lemma 2.1. *Let* $\mathbb{Z}_{(p)} := \mathbb{Z}_p \cap \mathbb{Q}$, *and let* A *be a* $\mathbb{Z}_{(p)}$*-algebra of characteristic zero. Let* $\mathbb{Q}(A) := A[1/p]$ *and let* $(w_0, w_1, \ldots) \in A^{\mathbb{N}}$. *Let* $f(x)$ *the formal series defined by*

$$f(x) := \exp\left(\sum_{k=0}^{\infty} w_k \frac{x^{p^k}}{p^k}\right) \in 1 + x\mathbb{Q}(A)[\![x]\!]. \tag{2}$$

Then the following are equivalent:

(i) $f(x) \in 1 + xA[\![x]\!]$;

(ii) *There exists a Witt vector* $\boldsymbol{a} = (a_0, a_1, \ldots) \in \mathbb{W}(A)$ *such that* $w(\boldsymbol{a}) = (w_0, w_1, \ldots)$.

Proof. Assume the existence of $\boldsymbol{a}$. Let $E(x) := \exp(\sum_{k=1}^{\infty} \frac{x^{p^k}}{p^k})$ be the *Artin–Hasse exponential*. Then one can easily check that $\exp(\sum_{k=0}^{\infty} w_k \frac{x^{p^k}}{p^k}) = \prod_{i\geqslant 0} E(a_i \cdot x^{p^i})$. Since $E(a_k x^{p^k}) \in 1 + xA[\![x]\!]$ for all $a \in A$, we have $f(x) \in 1 +$

$xA[\![x]\!]$. Assume now that $f(x) \in 1 + xA[\![x]\!]$. By [6, Ch II Lemma 1.5] and [1, Ch IV §4.10], there exists a unique sequence $\boldsymbol{b} = (b_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ such that

$$f(x) = \prod_{k=1}^{\infty}\bigl(1 - b_k x^k\bigr)^{-1} = \exp\circ\log\left(\prod_{k=1}^{\infty}\bigl(1 - b_k x^k\bigr)^{-1}\right) = \exp\left(-\sum_{k=1}^{\infty}\log\bigl(1 - b_k x^k\bigr)^{-1}\right)$$
$$= \exp\left(\sum_{r,k=1}^{\infty}\frac{b_k^r}{r}x^{r\cdot k}\right) = \exp\left(\sum_{n=1}^{\infty}\left(\frac{\Phi_n(\boldsymbol{b})}{n}\right)x^n\right) \quad \text{where } \Phi_n(\boldsymbol{b}) = \sum_{\substack{r\mid n\\ 1\leqslant r\leqslant n}} r\cdot b_r^{n/r}. \tag{3}$$

By comparing the last exponential in (3) with $f(x)$ we get $\Phi_n(\boldsymbol{b}) = w_k$ if $n = p^k$ and 0 otherwise. Let $a_k = b_{p^k} \in A$ for all k. Then the Witt vector $\boldsymbol{a} := (a_n)_{n\in\mathbb{N}}$ satisfies the requirements of Lemma 2.1. □

Definition 2.2. For all sequences $\boldsymbol{w} = (w_0, w_1, \ldots) \in A^{\mathbb{N}}$, we set $\boldsymbol{w}_n = (w_n, w_{n-1}, \ldots, w_1, w_0, 0, 0, \ldots)$.

Remark 2. By Lemma 2.1 the assertion (i) of the main Theorem 0.1 is equivalent to the following assertion:

There exists a sequence $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots) \in \mathcal{O}_{\overline{T}}^{\mathbb{N}}$ and a family of Witt vectors $\boldsymbol{a}_n \in \mathbb{W}(\mathcal{O}_{\overline{T}})$, $n \geqslant 0$, such that, for all $n \geqslant 0$, one has

$$w(\boldsymbol{a}_n) = \boldsymbol{\alpha}_n. \tag{4}$$

In other words, for all $n \geqslant 0$, the phantom vector of $\boldsymbol{a}_n$ is $(\alpha_n, \alpha_{n-1}, \ldots, \alpha_0, 0, 0, \ldots)$.

The proof of Theorem 0.1 is therefore reduced to *defining* a (not unique) sequence $\alpha_n \in \mathcal{O}_{\overline{T}}$ such that Eqs. (4) with data $\boldsymbol{\alpha}_n$ and unknown $\boldsymbol{a}_n \in \mathbb{W}(\mathcal{O}_{\overline{T}})$ are satisfied.

2.2. Second part of the proof: definition of the sequence $(\alpha_0, \alpha_1, \ldots) \in A^{\mathbb{N}}$

We denote by σ both the Frobenius homomorphism $\sigma : x \mapsto x^p$ on the residue field of T and its unique lifting to T defined by $a^\sigma \equiv a^p \bmod p\mathcal{O}_T$. We also denote by σ the extension to $\mathcal{O}_T[t]$ given by the following: $\sum a_i t^i \mapsto \sum a_i^\sigma t^i : \mathcal{O}_T[t]y \to \mathcal{O}_T[t]$. Let $P(t) \in \mathcal{O}_T[t]$ be an Eisenstein polynomial of degree $e \leqslant p-1$, we set

$$Q(t) := t^{p-e}\cdot P(t). \tag{5}$$

Definition 2.3 *(Definition of the sequence $\alpha_n \in A^{\mathbb{N}}$).* Let α_n be inductively defined as follows:

(i) α_0 is an arbitrary root of $P(t)$, then $v_p(\alpha_0) = 1/e$ and put $K_0 = T(\alpha_0)$;
(ii) Suppose $(\alpha_i)_{i\leqslant n-1}$ and $(K_i)_{0\leqslant i\leqslant n-1}$ have already been defined so that $K_i := K_{i-1}(\alpha_i)$ and $v_p(\alpha_i) = 1/ep^i$, for all $i \leqslant n-1$. Let $P_n(t)$ be the following Eisenstein polynomial of degree p:

$$P_n(t) := Q^{\sigma^{-n}}(t) - \alpha_{n-1}, \quad n \geqslant 1. \tag{6}$$

We define α_n as an arbitrary root of $P_n(t) \in \mathcal{O}_{K_{n-1}}[t]$, then $v_p(\alpha_n) = 1/ep^n$ and put $K_n := K_{n-1}(\alpha_n)$.

2.2.1. Construction of the sequence $\boldsymbol{a}_n$

The construction is based on the following lemma, which provides the existence of certain Witt vectors with prescribed phantom vector:

Lemma 2.4. ([7, Ch 7 Prop 4.12], [2, §1 Ex. 14]) *Let A be a p-torsion-free ring and let $\Phi : A \to A$ be a lifting of the Frobenius endomorphism on A/pA, namely $\Phi(x) \equiv x^p \bmod pA$. Let $\Phi^0 := \mathrm{Id}_A$ and $\Phi^n = \Phi\circ\Phi^{n-1}$. Then there exists a unique ring morphism $\boldsymbol{s}_\Phi : A \to \mathbb{W}(A)$ satisfying*

$$F\circ\boldsymbol{s}_\Phi = \boldsymbol{s}_\Phi\circ\Phi, \tag{7}$$

where $F : \mathbb{W}(A) \to \mathbb{W}(A)$ is the canonical Frobenius homomorphism. Moreover $\boldsymbol{s}_\Phi$ is injective, and for all $n \in \mathbb{N}$, and all $x \in A$ one has

$$w_n\bigl(\boldsymbol{s}_\Phi(x)\bigr) = \Phi^n(x). \tag{8}$$

Now we apply Lemma 2.4 with $A = \mathcal{O}_T[t]$ to solve Eqs. (4) in $\mathbb{W}(\mathcal{O}_T[t])$. Then we *specialize* the indeterminate t to the values α_n to obtain a sequence of Witt vectors satisfying the relations (4). To do this, for all $n \geqslant 0$, we call Φ_n the Frobenius on $\mathcal{O}_T[t]$ sending $g(t) \mapsto g^{\sigma}(Q^{\sigma^{-n}}(t))$:

$$\Phi_n : \mathcal{O}_T[t] \to \mathcal{O}_T[t]. \tag{9}$$

Lemma 2.5. *For all $n \in \mathbb{N}$ the pair $(\mathcal{O}_T[t], \Phi_n)$ satisfies the assumptions of Lemma* 2.4.

Now fix $g(t) = t$. For each $n \in \mathbb{N}$, let $\boldsymbol{s}_n(t) := s_{\Phi_n}(t) = (s_{n,0}(t), s_{n,1}(t), \ldots) \in \mathbb{W}(\mathcal{O}_T[t])$ be the unique Witt vector satisfying $w_k(\boldsymbol{s}_n(t)) = \Phi_n^k(t)$. In other words $\boldsymbol{s}_n(t)$ is the unique Witt vector having

$$\big(t, \Phi_n(t), \Phi_n^2(t), \ldots\big) \in A^{\mathbb{N}} \tag{10}$$

as phantom vector. The existence and uniqueness of $\boldsymbol{s}_n(t)$ is guaranteed by Lemma 2.4.

Now specialize the variable t to α_n, and put

$$\boldsymbol{a}_n := \boldsymbol{s}_n(\alpha_n) \in \mathbb{W}(\mathcal{O}_{K_n}), \tag{11}$$

in order that the phantom components of $\boldsymbol{a}_n$ be $(\alpha_n, \Phi_n(t)|_{t=\alpha_n}, \Phi_n^2(t)|_{t=\alpha_n}, \ldots, \Phi_n^n(t)|_{t=\alpha_n}, 0, 0, \ldots)$. Hence, by Definition 2.3, one has $Q^{\sigma^{-n}}(\alpha_n) = \alpha_{n-1}$, $Q^{\sigma^{-n+1}}(\alpha_{n-1}) = \alpha_{n-2}, \ldots, Q(\alpha_0) = 0$ and so:

$$\Phi_n^k(t)|_{t=\alpha_n} = \big(Q^{\sigma^{-n+k-1}} \circ \cdots \circ Q^{\sigma^{-n+2}} \circ Q^{\sigma^{-n+1}} \circ Q^{\sigma^{-n}}\big)(\alpha_n) = \begin{cases} \alpha_{n-k} & \text{if } k \leqslant n, \\ 0 & \text{if } k > n. \end{cases} \tag{12}$$

Then we can conclude that the sequence $\boldsymbol{a}_n$ satisfies $w(\boldsymbol{a}_n) = \boldsymbol{\alpha}_n$ (cf. Definition 2.2) with the property required by Theorem 0.1. This completes the proof of the main theorem.

Acknowledgements

I wish to thank Dr. Andrea Pulita and Prof. Bruno Chiarellotto for their encouragement, many suggestions and carefully proofreading of this note. I also thank the referee for pointing out mistakes and giving useful comments.

References

[1] N. Bourbaki, Elements of Mathematics, Algebra II, Springer-Verlag, 1990.
[2] N. Bourbaki, Eléments de Mathématiques, Chapitre IX, Algèbre Commutative, Masson, 1983.
[3] G. Christol, P. Robba, Equations différentielles p-adiques, Hermann, 1994.
[4] B. Dwork, Generalized Hypergeometric Functions, Clarendon Press, 1990.
[5] B. Dwork, Manuscript.
[6] B. Dwork, G. Gerotto, F.J. Sullivan, An Introduction to G-Functions, Annals of Mathematics Studies, vol. 133, Princeton Univ. Press, 1994.
[7] M. Lazard, Commutative Formal Groups, Lecture Notes in Mathematics, vol. 443, Springer-Verlag, 1975.
[8] S. Matsuda, Local Indices of p-adic differential operators corresponding to Artin–Schreier–Witt coverings, Duke Math. J. 77 (1995) 607–625.
[9] A. Pulita, Rank one solvable p-adic differential equations and finite Abelian characters via Lubin–Tate groups, Math. Ann., in press.
[10] P. Robba, Indice d'un opérateur différentiel p-adique IV. Cas de systèmes, Ann. Inst. Fourier 35 (1985) 13–55.