Glasgow Math. J. **47** (2005) 319–326.
doi:10.1017/S0017089505002533. Printed in the United Kingdom

ON THE p-ADIC BINOMIAL SERIES AND A FORMAL ANALOGUE OF HILBERT'S THEOREM 90

PAVLOS TZERMIAS

Department of Mathematics, University of Tennessee, Knoxville, TN 37996-1300, USA
e-mail: tzermias@math.utk.edu

(Received 3 August, 2004; accepted 11 March, 2005)

Abstract. We strengthen a characterization of the p-adic binomial series and a special case of a formal analogue of Hilbert's Theorem 90 for p-adic power series.

2000 *Mathematics Subject Classification.* 12J25, 13F25, 11S99.

1. Introduction. Let R be a complete discrete valuation ring with field of fractions K and residue field k. Denote by v the valuation on R. We assume that we are in the unequal characteristic case; i.e. K has characteristic zero and k has characteristic $p > 0$. We also assume that k is perfect. The natural injection $\mathbb{Z} \to R$ extends by continuity to an injection $\mathbb{Z}_p \to R$. Let $e = v(p)$. It is well known (see [**7**, Section II.5]) that K is a totally ramified extension of degree e of the field of fractions of the ring of Witt vectors of k.

Let $\overline{K}$ be a fixed algebraic closure of K and let $|\cdot|$ denote the absolute value on $\overline{K}$. We denote by μ_∞ (resp. μ_{p^∞}, μ_{p^l}) the set of roots of unity (resp. p-power roots of unity, p^l-th roots of unity) in $\overline{K}$. Let $t_1, \ldots, t_n$ be independent variables and let $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ be a diagonal matrix with diagonal entries a_i, for $i = 1, \ldots, n$. The ideal generated by $t_1, \ldots, t_n$ in $R[[t_1, \ldots, t_n]]$ is denoted by $(t_1, \ldots, t_n)R[[t_1, \ldots, t_n]]$. Let $F(t_1, \ldots, t_n) \in 1 + (t_1, \ldots, t_n)R[[t_1, \ldots, t_n]]$. Note that, as $|\zeta - 1| < 1$ for $\zeta \in \mu_{p^\infty}$, the power series F induces a function $(\mu_{p^\infty})^n \to \overline{K}^\times$ given by

$$(\zeta_1, \ldots, \zeta_n) \mapsto F(\zeta_1 - 1, \ldots, \zeta_n - 1),$$

for all $(\zeta_1, \ldots, \zeta_n) \in (\mu_{p^\infty})^n$. By a result of Loeser (see Théorème A.1 in [**6**]), we have the following result.

THEOREM 1.1. *(Loeser) Let the notation be as above. Suppose that for all integers $f \geq 1$ and for all $(\zeta_1, \ldots, \zeta_n) \in (\mu_{p^\infty})^n$ such that $\zeta_i^{a_i^f} = \zeta_i$, for $i = 1, \ldots, n$, we have*

$$\prod_{i=0}^{f-1} F\left(\zeta_1^{a_1^i} - 1, \ldots, \zeta_n^{a_n^i} - 1\right) \in \mu_\infty.$$

Then there exist $b_1, \ldots, b_n \in \mathbb{Z}_p$ and a unit $G(t_1, \ldots, t_n) \in R[[t_1, \ldots, t_n]]$ such that

$$F(t_1, \ldots, t_n) = \frac{G((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1)}{G(t_1, \ldots, t_n)} \prod_{i=1}^{n} (1+t_i)^{b_i}.$$

We stated Theorem 1.1 for diagonal matrices A in $\mathrm{GL}_n(\mathbb{Z}_p)$. As Loeser points out in [**6**], one can replace "diagonal" by "diagonalizable" and, after an appropriate change of variables, the result is still valid. It is easy to see that the converse of Theorem 1.1 is also true. Theorem 1.1 generalizes a result of Anderson [**2**], which in turn is an extension of a theorem of Coleman [**3**]. The latter theorem affirmatively answered a question of Deligne, a special case of which was settled by Adolphson [**1**]. As explained in Remark 2.2 below, Theorem 1.1 bears a formal similarity to a recent result of Dubickas and Smyth [**4**] extending the classical Hilbert's Theorem 90 to the non-cyclic case.

In the unramified case (i.e. the case $e = 1$), a crucial ingredient in Loeser's, Anderson's and Coleman's proofs is the Dieudonné-Dwork lemma on the twisted logarithm homomorphism. Note that in the case $n = 1$ and $a_1 = 1$, Theorem 1.1 can be stated as follows. If a power series $F(t) \in 1 + (t)R[[t]]$ satisfies $F(\zeta - 1) \in \mu_\infty$ for all $\zeta \in \mu_{p^\infty}$, then $F(t)$ is a binomial series. The purpose of this paper is to show that, in the special case where A is a root of unity in $\mathrm{GL}_n(\mathbb{Z}_p)$, the conclusion of Theorem 1.1 remains valid under weaker hypotheses (see Theorems 2.1 and 3.2 below). Our proofs differ from the ones in [**2**], [**3**] and [**6**], in the sense that we do not use the Dieudonné-Dwork lemma, since, given our assumptions, it is not clear how to do so (see Remark 2.3 below). It is not unlikely that similar statements to Theorems 2.1 and 3.2 hold for any diagonal $A \in \mathrm{GL}_n(\mathbb{Z}_p)$, but we have been unable to come up with a successful approach in the general case.

2. The single-variable case.

THEOREM 2.1. *Let $F(t) \in 1 + (t)R[[t]]$.*

(1) *If $F(t)$ satisfies $F(\zeta - 1) \in \mu_\infty$ for infinitely many $\zeta \in \mu_{p^\infty}$, then $F(t)$ is a binomial series; i.e. a series of the form $(1 + t)^b$, for some $b \in \mathbb{Z}_p$.*

(2) *Suppose that a is a primitive f-th root of unity in $\mathbb{Z}_p$, with $a \neq 1$. If $F(t)$ satisfies*

$$\prod_{i=0}^{f-1} F\left(\zeta^{a^i} - 1\right) \in \mu_\infty,$$

for infinitely many $\zeta \in \mu_{p^\infty}$, then there exists $b \in \{0, 1\}$ and a unit $G(t) \in R[[t]]$ such that

$$F(t) = (1 + t)^b \frac{G((1 + t)^a - 1)}{G(t)}.$$

Moreover, $b = 0$, unless $p = 2$ and $F(-2) = -1$.

Proof. (1) Recall that $|\zeta - 1| = 1$, if $\zeta \in \mu_\infty - \mu_{p^\infty}$. For $l \geq 1$, we have that $|\zeta - 1| = p^{-1/\phi(p^l)}$, if $\zeta \in \mu_{p^l} - \mu_{p^{l-1}}$, where ϕ is the Euler function. Note that $|F(\zeta - 1) - 1| \leq |\zeta - 1|$, for all $\zeta \in \mu_{p^\infty}$. Therefore, if $\zeta \in \mu_{p^l} - \mu_{p^{l-1}}$ and $F(\zeta - 1) \in \mu_\infty$, then necessarily $F(\zeta - 1) \in \mu_{p^l}$. Hence, by assumption, we can choose an increasing sequence of positive integers n_i and a sequence of primitive p^{n_i}-th roots of unity ζ_{n_i} such that $F(\zeta_{n_i} - 1) = \zeta_{n_i}^{b_i}$, for an integer $b_i \in \{0, \ldots, p^{n_i} - 1\}$. By compactness of $\mathbb{Z}_p$, we may assume, without loss of generality, that the sequence $b_1, b_2, \ldots$ converges to $b \in \mathbb{Z}_p$. Define a power series $G(t) \in 1 + (t)R[[t]]$ by $G(t) = (1 + t)^{-b}F(t)$. Let r be any positive integer. There is a positive integer $N(r)$ such that $|b_i - b| \leq p^{-r}$; i.e. $b_i - b$ is

https://doi.org/10.1017/S0017089505002533 Published online by Cambridge University Press

divisible by p^r, for all $i \geq N(r)$. If $r \geq n_i$, then $\zeta_{n_i}^{b_i-b} = 1$. Otherwise, $\zeta_{n_i}^{b_i-b}$ is a p^{n_i-r}-th root of unity. Therefore, for all $i \geq N(r)$, we have

$$\left|G\left(\zeta_{n_i}-1\right)-1\right| = \left|\zeta_{n_i}^{-b}F\left(\zeta_{n_i}-1\right)-1\right| = \left|\zeta_{n_i}^{b_i-b}-1\right| \leq \left|\zeta_{n_i}-1\right|^{p^r}.$$

Now write $G(t)-1 = c_1t + c_2t^2 + \cdots$, where $c_j \in R$, for all j. We claim that $|c_j| < 1$, for $j \in \{1, \ldots, p^r-1\}$. If not, there exists a least index $m \leq p^r-1$ such that $|c_m| = 1$. Choose $i \geq N(r)$ such that $p^r \leq \phi(p^{n_i})/e$. Then

$$\left|\sum_{j=1}^{m-1} c_j\left(\zeta_{n_i}-1\right)^j\right| < p^{-1/e},\ \left|c_m\left(\zeta_{n_i}-1\right)^m\right| = p^{-m/\phi(p^{n_i})},\ \left|\sum_{j=m+1}^{\infty} c_j\left(\zeta_{n_i}-1\right)^j\right| < p^{-m/\phi(p^{n_i})}.$$

Therefore, since $m < p^r$, we get

$$|G(\zeta_{n_i}-1)-1| = p^{-m/\phi(p^{n_i})} > p^{-p^r/\phi(p^{n_i})} = |\zeta_{n_i}-1|^{p^r},$$

a contradiction, which proves the claim. Thus, $|c_j| < 1$, for all $j < p^r$. This is true for every positive integer r, so $|c_j| < 1$, for all $j \geq 1$. But then $|G(\zeta_{n_i}-1)-1| < p^{-1/e}$, so $G(\zeta_{n_i}-1)$ is a primitive p^s-th root of unity for some s such that $\phi(p^s) < e$. In other words, the set of values $\{G(\zeta_{n_i}-1) : i = 1, 2, \ldots\}$ if finite. In particular, the power series $G(t)$ takes the same value at infinitely many $\zeta_{n_i}-1$. Since, by the Weierstrass preparation theorem (see [**5**, p. 215]), a non-zero power series with p-integral coefficients can have only finitely many zeros with positive p-adic valuation, it follows that $G(t)$ is constant. But $G(0) = 1$, so that $G(t) = 1$, and this proves that $F(t) = (1+t)^b$.

(2) By part (1), there exists $b \in \mathbb{Z}_p$ such that

$$\prod_{i=0}^{f-1} F\left((1+t)^{a^i}-1\right) = (1+t)^b.$$

The coefficient of t on the left-hand side is a multiple of $1 + a + \cdots + a^{f-1}$ and should equal b. Since $a \neq 1$, $a^f = 1$, it follows that $b = 0$; i.e.

$$\prod_{i=0}^{f-1} F\left((1+t)^{a^i}-1\right) = 1.$$

Note that, at this point, one cannot invoke Theorem 1.1 and finish the proof; the problem is that Theorem 1.1 requires the hypothesis to be satisfied for all f, not just for f equal to the order of a in $\mathbb{Z}_p$. Although there is a way around this problem, we have chosen to follow another approach instead (see also Remark 2.4 below).

As in the usual proof of the classical Hilbert's Theorem 90, define

$$H(t) = 1 + \sum_{i=0}^{f-2}\prod_{j=0}^{i} F\left((1+t)^{a^j}-1\right).$$

The constant coefficient of $H(t)$ equals f; in particular $H(t) \neq 0$.

If $p \neq 2$, then f is relatively prime to p, so that $H(t)$ is a unit in $R[[t]]$. It is now easy to verify that $G(t)F(t) = G((1+t)^a-1)$, where $G(t) = 1/H(t)$.

https://doi.org/10.1017/S0017089505002533 Published online by Cambridge University Press

Now suppose that $p = 2$. Then $f = 2$ and $a = -1$. By the Weierstrass preparation theorem, we may write $H(t) = 2^s r(t)U(t)$, where s is a non-negative integer, $U(t)$ is a unit in $R[[t]]$ and $r(t)$ is a distinguished polynomial. Let $m = \deg(r(t))$. Observe that $r((1+t)^{-1} - 1) = r(-t/(1+t)) = (1+t)^{-m} w(t)$, where $w(t)$ is also a distinguished polynomial of degree m. The equality $H(t) = H((1+t)^{-1} - 1)F(t)$ now gives

$$2^s(1+t)^m r(t)U(t) = 2^s F(t)w(t)U((1+t)^{-1} - 1).$$

By the uniqueness statement in the Weierstrass preparation theorem, it follows that

$$F(t) = (1+t)^m \frac{U(t)}{U((1+t)^{-1} - 1)}.$$

Write $m = 2u + b$, where $u \in \mathbb{Z}_p$ and $b \in \{0, 1\}$. Then

$$F(t) = (1+t)^b \frac{G((1+t)^{-1} - 1)}{G(t)},$$

where $G(t) = (1+t)^{-u}/U(t)$. Now it is clear that $F(-2) = -1$ if and only if $b = 1$, and this completes the proof of Theorem 2.1. □

REMARK 2.2. Let X be the multiplicative group of functions from μ_{p^∞} to $\overline{K}^\times$ induced by power series in $1 + (t)R[[t]]$ in the way described in the Introduction. Also, let Y be the multiplicative group of functions from μ_{p^∞} to the quotient group $\overline{K}^\times/\mu_\infty$ similarly induced by power series in $1 + (t)R[[t]]$. Note that, by Theorem 1.1, Y is isomorphic to the quotient group $(1 + (t)R[[t]])/(1+t)^{\mathbb{Z}_p}$. By the Weierstrass preparation theorem, distinct elements of X can agree on only finitely many $\zeta \in \mu_{p^\infty}$. Theorem 2.1 shows that the same is also true for distinct elements of Y. Also, for the sake of simplicity, consider the case $R = \mathbb{Z}_p$ and $n = 1$. By local class field theory, we can identify $\mathbb{Z}_p^\times$ with $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$. The action of $\mathbb{Z}_p^\times$ on $1 + (t)\mathbb{Z}_p[[t]]$ given by $a \cdot F(t) = F((1+t)^a - 1)$ therefore induces a Galois action of $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ on X and on Y. In this context, Theorem 1.1 bears a formal similarity to the result of Dubickas and Smyth [**4**].

REMARK 2.3. For the Dieudonné-Dwork lemma to be used in the unramified case (as in [**2**], [**3**] and [**6**]) one needs to know that both

$$\prod_{i=0}^{f-1} F\big(\zeta_1^{a_1^i} - 1, \ldots, \zeta_n^{a_n^i} - 1\big) \quad \text{and} \quad \prod_{i=0}^{f-1} F^{\mathrm{Fr}}\big(\zeta_1^{pa_1^i} - 1, \ldots, \zeta_n^{pa_n^i} - 1\big)$$

(where Fr is the arithmetic Frobenius morphism) are in μ_{p^∞} when $\zeta_i^{a_i^f} = \zeta_i$, for all i. If one attempts to replace the hypothesis "for all $(\zeta_1, \ldots, \zeta_n)$" in Theorem 1.1 by "for infinitely many $(\zeta_1, \ldots, \zeta_n)$", it becomes less clear how to use the Dieudonné-Dwork lemma. This is one of the difficulties in trying to extend Theorem 2.1 to the case where a is an arbitrary unit in $\mathbb{Z}_p$. Also, the following easy (and not surprising) example shows that there is no direct way to deduce that if the values of $F(t)$ at $\eta - 1$ have the desired property, then so do the values of $F(t)$ at $\zeta - 1$, where η, ζ are p^m-th, p^l-th roots of unity, respectively, and $m > l$. Let

$$F(t) = 1 + t\frac{(t+1)^{p^m} - 1}{(t+1)^p - 1} \in 1 + t\mathbb{Z}_p[t],$$

https://doi.org/10.1017/S0017089505002533 Published online by Cambridge University Press

where $m \geq 2$. It is clear that $F(\eta - 1) = 1 \in \mu_\infty$, for $\eta \in \mu_{p^m} - \mu_p$. On the other hand, if $\zeta \in \mu_p - \{1\}$, then $F(\zeta - 1) = 1 + p^{m-1}(\zeta - 1)$, so that $0 < |F(\zeta - 1) - 1| < p^{-1}$, which shows that $F(\zeta - 1) \notin \mu_\infty$.

REMARK 2.4. If a is a primitive root of unity of order f in $\mathbb{Z}_p$ and

$$\prod_{i=0}^{f-1} F\left(\zeta^{a^i} - 1\right) = 1,$$

for infinitely many (hence for all) $\zeta \in \mu_{p^\infty}$, it is not true that there exists a unit $G(t)$ in $R[[t]]$ such that $F(t) = G((1 + t)^a - 1)/G(t)$. In other words, the conclusion of Corollary A.7 in [**6**] would be false if, instead of requiring the hypothesis to be satisfied for all $f \geq 1$, we only required that it be satisfied for f equal to the order of a in $\mathbb{Z}_p$. For example, let $p = 2, f = 2, a = -1$ and consider $F(t) = 1 + t$. Then $F(t)F((1 + t)^{-1} - 1) = 1$, but there is no unit $G(t) \in R[[t]]$ such that $F(t) = G((1 + t)^{-1} - 1)/G(t)$, since $F(-2) \neq 1$.

3. The multi-variable case. Theorem 2.1 does not directly extend to the multivariable case, as the following simple example illustrates.

EXAMPLE 3.1. Consider the power series $F(t_1, t_2) = 1 + t_1 - t_2 \in 1 + (t_1, t_2)\mathbb{Z}_p[[t_1, t_2]]$. Then $F(\zeta_1 - 1, \zeta_2 - 1) = 1 \in \mu_\infty$, for infinitely many $(\zeta_1, \zeta_2) \in (\mu_{p^\infty})^2$ (take $\zeta_1 = \zeta_2$). However, $F(t_1, t_2)$ is not of the form $(1 + t_1)^{b_1}(1 + t_2)^{b_2}$, for $b_1, b_2 \in \mathbb{Z}_p$, since $F(0, t_2)$ is not a binomial series.

The above example is hardly surprising; the first and second entries of the chosen infinite set of pairs $(\zeta_1 - 1, \zeta_2 - 1)$ at which F has value 1 are closely related. We shall show that, roughly speaking, this will always be the case for all examples demonstrating the same phenomenon that Example 3.1 does. Part (1) of the following theorem (which, for $n = 1$, reduces to Theorem 2.1) states that a power series in n variables whose values are roots of unity at infinitely many tuples $(\zeta_1 - 1, \ldots, \zeta_n - 1)$ is a product of binomial series in each of its variables, provided that the collection of such tuples is parametrized by n "algebraically unrelated" parameters. The proof of the theorem uses a clever idea of Anderson appearing in the proof of Corollary 3.1.7 in [**2**].

THEOREM 3.2. *Let $F(t_1, \ldots, t_n) \in 1 + (t_1, \ldots, t_n)R[[t_1, \ldots, t_n]]$. Let S be a non-empty set of non-zero tuples in $(\mathbb{Z}_p)^n$, such that for every non-trivial homogeneous polynomial $P(x_1, \ldots, x_n)$ with coefficients in R we have $P(S) \neq \{0\}$. In other words, S satisfies no non-trivial homogeneous algebraic relation with coefficients in R.*

(1) *Suppose that for every $(y_1, \ldots, y_n) \in S$, we have $F(\zeta^{y_1} - 1, \ldots, \zeta^{y_n} - 1) \in \mu_\infty$, for infinitely many $\zeta \in \mu_{p^\infty}$. Then there exist $b_1, \ldots, b_n \in \mathbb{Z}_p$, such that*

$$F(t_1, \ldots, t_n) = \prod_{i=1}^{n} (1 + t_i)^{b_i}.$$

(2) *Let A be a diagonal matrix which is a primitive f-th root of unity in $GL_n(\mathbb{Z}_p)$, with $A \neq I$. Let $a_1, \ldots, a_n$ be the diagonal entries of A. Suppose that for every $(y_1, \ldots, y_n) \in S$, we have*

$$\prod_{i=0}^{f-1} F\left(\zeta^{y_1 a_1^i} - 1, \ldots, \zeta^{y_n a_n^i} - 1\right) \in \mu_\infty,$$

https://doi.org/10.1017/S0017089505002533 Published online by Cambridge University Press

for infinitely many $\zeta \in \mu_{p^\infty}$. *Then there exist* $b_1, \dots, b_n \in \mathbb{Z}_p$ *and a unit* $G(t_1, \dots, t_n) \in R[[t_1, \dots, t_n]]$ *such that*

$$F(t_1, \dots, t_n) = \frac{G((1+t_1)^{a_1} - 1, \dots, (1+t_n)^{a_n} - 1)}{G(t_1, \dots, t_n)} \prod_{i=1}^{n} (1+t_i)^{b_i}.$$

Proof. (1) Let $c_1, \dots, c_n$ be the coefficients of $t_1, \dots, t_n$ in $F(t_1, \dots, t_n)$, respectively. Replacing $F(t_1, \dots, t_n)$ by $(1+t_1)^{-c_1} \dots (1+t_n)^{-c_n} F(t_1, \dots, t_n)$ if necessary, we may assume that $c_1 = \dots = c_n = 0$. It suffices to show that $F(t_1, \dots, t_n)$ is identically equal to 1. Suppose not. We can write

$$F(t_1, \dots, t_n) = 1 + \sum_{j=2}^{\infty} P_j(t_1, \dots, t_n),$$

where $P_j(t_1, \dots, t_n)$ is a homogeneous polynomial of degree j in $t_1, \dots, t_n$ with coefficients in R. By assumption, there exists a least $m \geq 2$ such that $P_m(t_1, \dots, t_n)$ is non-zero. For each $(y_1, \dots, y_n) \in S$, consider the power series

$$H(t) = F((1+t)^{y_1} - 1, \dots, (1+t)^{y_n} - 1) \ \in \ 1 + (t)R[[t]].$$

Note that

$$H(t) \equiv 1 + P_m(y_1, \dots, y_n)\, t^m \pmod{(t)^{m+1} R[[t]]}.$$

By our hypothesis on S, there exists $(y_1, \dots, y_n) \in S$ such that $P_m(y_1, \dots, y_n) \neq 0$. For this choice of $(y_1, \dots, y_n)$, it follows that $H(t)$ is not a binomial series (the coefficient of t equals 0 and the coefficient of t^m is non-zero). On the other hand, by assumption,

$$H(\zeta - 1) = F(\zeta^{y_1} - 1, \dots, \zeta^{y_n} - 1) \in \mu_\infty,$$

for infinitely many $\zeta \in \mu_{p^\infty}$, which is impossible, by Theorem 2.1.

(2) By Part (1), there exist $b_1, \dots, b_p \in \mathbb{Z}_p$ such that

$$\prod_{i=0}^{f-1} F\big((1+t_1)^{a_1^i} - 1, \dots, (1+t_n)^{a_n^i} - 1\big) = \prod_{i=1}^{n} (1+t_i)^{b_i}.$$

For each i, the coefficient of t_i on the left-hand side is a multiple of $1 + a_i + \dots + a_i^{f-1}$ and should equal b_i. If $a_i \neq 1$, then $b_i = 0$ (since $a_i^f = 1$). If $a_i = 1$, then b_i is a multiple of f in $\mathbb{Z}_p$. Set $d_i = b_i/f$, for all i, and define

$$L(t_1, \dots, t_n) = \frac{F(t_1, \dots, t_n)}{(1+t_1)^{d_1} \cdots (1+t_n)^{d_n}}.$$

Then

$$\prod_{i=0}^{f-1} L\big((1+t_1)^{a_1^i} - 1, \dots, (1+t_n)^{a_n^i} - 1\big) = 1.$$

https://doi.org/10.1017/S0017089505002533 Published online by Cambridge University Press

If p is odd, then f is relatively prime to p. Define

$$H(t_1, \ldots, t_n) = 1 + \sum_{i=0}^{f-2} \prod_{j=0}^{i} L\big((1+t_1)^{a_1^j} - 1, \ldots, (1+t_n)^{a_n^j} - 1\big).$$

The constant coefficient of $H(t_1, \ldots, t_n)$ equals f. Therefore $H(t_1, \ldots, t_n)$ is invertible in $R[[t_1, \ldots, t_n]]$. Since $L(t_1, \ldots, t_n)H((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1) = H(t_1, \ldots, t_n)$, it follows that $L(t_1, \ldots, t_n)$ (hence also $F(t_1, \ldots, t_n)$) is of the desired form.

Now suppose that $p = 2$. Then $f = 2$ and $a_i = \pm 1$, for all i. In addition, since $A \neq I$, there exists some i such that $a_i = -1$. Without loss of generality, assume $a_1 = -1$. Write $L(t_1, \ldots, t_n)$ as a power series in t_1:

$$L(t_1, \ldots, t_n) = 1 + \sum_{j=1}^{\infty} g_j(t_2, \ldots, t_n)\, t_1^j,$$

where $g_j(t_2, \ldots, t_n) \in R[[t_2, \ldots, t_n]]$, for all j. Let $\mathcal{M}$ denote the maximal ideal in $R[[t_2, \ldots, t_n]]$. We define a power series $H(t_1, \ldots, t_n)$ as follows.

If for some $j \geq 1$, we have $g_j(t_2, \ldots, t_n) \notin \mathcal{M}$, then

$$H(t_1, \ldots, t_n) = 1 + L(t_1, \ldots, t_n) = 2 + \sum_{j=1}^{\infty} g_j(t_2, \ldots, t_n)\, t_1^j.$$

Otherwise,

$$\begin{aligned} H(t_1, \ldots, t_n) &= (1+t_1) + (1+t_1)^{a_1} L(t_1, \ldots, t_n) \\ &= 2 + g_1(t_2, \ldots, t_n)\, t_1 + (g_2(t_2, \ldots, t_n) - g_1(t_2, \ldots, t_n) + 1)\, t_1^2 + \mathrm{O}(t_1^3). \end{aligned}$$

It easily follows that, in either case, there is some $j \geq 1$ such that the coefficient of t_1^j in the above power series expansion of $H(t_1, \ldots, t_n)$ is not in $\mathcal{M}$. Also,

$$L(t_1, \ldots, t_n)H((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1) = H(t_1, \ldots, t_n).$$

By the general form of the Weierstrass preparation theorem (as stated in [**5**]) for single-variable power series rings over complete local rings it follows that there exists a unit $U(t_1, \ldots, t_n)$ and a distinguished polynomial $r(t_1, \ldots, t_n)$ in $R[[t_2, \ldots, t_n]][t_1]$ such that

$$H(t_1, \ldots, t_n) = r(t_1, \ldots, t_n)U(t_1, \ldots, t_n).$$

If m is the degree of $r(t_1, \ldots, t_n)$ in t_1, it follows that $H((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1)$ equals $(1+t_1)^{-m} w(t_1, \ldots, t_n)U((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1)$, where $w(t_1, \ldots, t_n)$ is also a distinguished polynomial in $R[[t_2, \ldots, t_n]][t_1]$ of degree m in t_1. Therefore, by the uniqueness statement in the Weierstrass preparation theorem (see [**5**, p. 215]), we get that $L(t_1, \ldots, t_n)$ (hence also $F(t_1, \ldots, t_n)$) is of the desired form. □

REFERENCES

1. A. Adolphson, An analogue of Hilbert's Theorem 90, *Proc. Amer. Math. Soc.* **88** (1983), 27–28.

2. G. Anderson, The hyperadelic gamma function, *Invent. Math.* **95** (1989), 63–131.

3. R. Coleman, A formal analogue of Hilbert's Theorem 90, *Proc. Amer. Math. Soc.* **94** (1985), 603–604.

4. A. Dubickas and C. Smyth, Variations on the theme of Hilbert's Theorem 90, *Glasgow Math. J.* **44** (2002), 435–441.

5. S. Lang, *Algebra*, Second Edition (Addison-Wesley, 1984).

6. F. Loeser, Faisceaux pervers, transformations de Mellin et déterminants, *Mém. Soc. Math. Fr.* **66** (1996).

7. J-P. Serre, *Local fields*, Graduate Texts in Math. No. 67 (Springer-Verlag, 1979).