Glasgow Math. J. **57** (2015) 101–105. © Glasgow Mathematical Journal Trust 2014.
doi:10.1017/S0017089514000147.

ADDENDUM

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

PAVLOS TZERMIAS

doi:10.1017/S0017089505002533, Published online by Cambridge University Press, 27 July 2005.

Abstract. The proof of Theorem 3.2 in [1] (P. Tzermias, On the p-adic binomial series and a formal analogue of Hilbert's Theorem 90, *Glasgow Math. J.* **47** (2005), 319–326) contains two opaque claims. The necessary clarifications are provided here.

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

This note owes its existence to the sharp eye of Shashikant B. Mulay (whom the author heartily thanks) who noticed and kindly informed the author that the proof of Theorem 3.2 in [1] needs to address the following two points:

(1) Page 324, line 6: In order to be able to assume that $c_1 = \cdots = c_n = 0$, one needs to know that the coefficients c_i are in $\mathbb{Z}_p$ (not just in R), for all i.

(2) Page 325, line 9: The reason we may assume that the leading coefficient of the power series $L(t_1, \ldots, t_n)$ (when viewed as a power series in t_1 with coefficients in $R[[t_2, \ldots, t_n]]$) equals 1 is not adequately explained.

For the sake of completeness, a revised version of the proof of Theorem 3.2 in [1], which incorporates the required clarifications and justifications, follows:

Proof. (1) We first need the following lemma:

LEMMA 1. *S contains a set T of n K-linearly independent vectors in $(\mathbb{Z}_p)^n$.*

Proof. Suppose not. Let r be the largest number of K-linearly independent vectors in S. Then $r < n$. Fix r such vectors and form the $r \times n$ matrix B with these vectors as its rows. B has rank r, so there exists a non-singular $r \times r$ minor C. Now for each $(y_1, \ldots, y_n) \in S$, the $(r+1) \times n$ matrix formed from B by putting $(y_1, \ldots, y_n)$ as its last row must have rank r also, hence all its $(r+1) \times (r+1)$ minors have zero determinant. Expanding the determinant of an $(r+1) \times (r+1)$ minor having C as a submatrix gives a non-trivial linear polynomial in $y_1, \ldots, y_n$, which is identically 0 on S, contradicting the hypothesis on S. □

Having established Lemma 1, let $c_1, \ldots, c_n$ be the coefficients of $t_1, \ldots, t_n$ in $F(t_1, \ldots, t_n)$ respectively. For each $(y_1, \ldots, y_n) \in T$, consider the power series

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

The coefficient of t in $H(t)$ equals $c_1 y_1 + \cdots + c_n y_n$. Note that

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

for infinitely many $\zeta \in \mu_{p^\infty}$. Therefore, Theorem 2.1 in [1] implies that $H(t) = (1+t)^b$ for some $b \in \mathbb{Z}_p$, hence the coefficient of t in $H(t)$ is in $\mathbb{Z}_p$. The conclusion is that $c_1y_1 + \cdots + c_ny_n \in \mathbb{Z}_p$ for all $(y_1, \ldots, y_n) \in T$. Solving the resulting linear system and using the linear independence of T shows that $c_i \in R \cap \mathbb{Q}_p = \mathbb{Z}_p$ for all i.
Replacing $F(t_1, \ldots, t_n)$ by $(1+t_1)^{-c_1} \cdots (1+t_n)^{-c_n} F(t_1, \ldots, t_n)$ (which also belongs to $1 + (t_1, \ldots, t_n)R[[t_1, \ldots, t_n]]$) if necessary, we may assume that $c_1 = \cdots = c_n = 0$. It suffices to show that $F(t_1, \ldots, t_n)$ is identically equal to 1. Suppose not. We can write

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

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

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

Note that

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

By our hypothesis on S, there exists $(y_1, \ldots, y_n) \in S$ such that $P_m(y_1, \ldots, y_n) \neq 0$. For this choice of $(y_1, \ldots, y_n)$, 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,

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

for infinitely many $\zeta \in \mu_{p^\infty}$, which is impossible, by Theorem 2.1 in [1].

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

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

For each i, the coefficient of t_i on the left-hand side is an R-multiple of $1 + a_i + \cdots + a_i^{f-1}$ 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 an R-multiple of f. Set $d_i = b_i/f$. Then $d_i \in R \cap \mathbb{Q}_p = \mathbb{Z}_p$ for all i. Define

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

Then

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

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

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

https://doi.org/10.1017/S0017089514000147 Published online by Cambridge University Press

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 $a_i = -1$. We need the following lemma.

LEMMA 2. *Let $p = 2$. Consider an n-tuple $(a_1, \ldots, a_n)$, where a_i is an integer of absolute value 1 for all i. Assume that not all a_i equal 1, and let r be an index such that $a_r = -1$. If $Q(t_1, \ldots, t_n) \in 1 + (t_1, \ldots, t_n)R[[t_1, \ldots, t_n]]$ satisfies the conditions*

(1) $Q(t_1, \ldots, t_{r-1}, 0, t_{r+1}, \ldots, t_n) = 1$,

(2) $Q(t_1, \ldots, t_n)\, Q((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1) = 1$,

then there exist a natural number m and a unit $G(t_1, \ldots, t_n)$ in $R[[t_1, \ldots, t_n]]$ such that

$$Q(t_1, \ldots, t_n) = (1+t_r)^m \frac{G((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1)}{G(t_1, \ldots, t_n)}.$$

Proof. Without loss of generality, assume $r = 1$. By condition (1), we may write $Q(t_1, \ldots, t_n)$ as a power series in t_1 in the following manner:

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

where $q_j(t_2, \ldots, t_n) \in R[[t_2, \ldots, t_n]]$, 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 $q_j(t_2, \ldots, t_n) \notin \mathcal{M}$, then

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

Otherwise,

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

$$= 2 + q_1(t_2, \ldots, t_n)\, t_1 + (q_2(t_2, \ldots, t_n) - q_1(t_2, \ldots, t_n) + 1)\, t_1^2 + \mathrm{O}(t_1^3).$$

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, by condition (2),

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

By the general form of the Weierstrass preparation theorem 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, then $H((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1)$ equals $(-1)^m(1+t_1)^{-m}(1+\eta)\, w(t_1, \ldots, t_n)\, U((1+t_1)^{a_1} - 1, \ldots, (1+t_n)^{a_n} - 1)$, 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

https://doi.org/10.1017/S0017089514000147 Published online by Cambridge University Press

t_1 and $\eta \in \mathcal{M}$. Therefore, by the uniqueness statement in the Weierstrass preparation theorem, we get

$$Q(t_1, \ldots, t_n)(-1)^m(1+t_1)^{-m}(1+\eta)\, U((1+t_1)^{a_1}-1, \ldots, (1+t_n)^{a_n}-1) = U(t_1, \ldots, t_n). \qquad (*)$$

Now write

$$U(t_1, \ldots, t_n) = \sum_{j=0}^{\infty} u_j(t_2, \ldots, t_n)\, {t_1}^j,$$

where $u_j(t_2, \ldots, t_n) \in R[[t_2, \ldots, t_n]]$ for all j. Evaluating both sides of $(*)$ at $t_1 = 0$ gives:

$$(-1)^m(1+\eta)\, u_0((1+t_2)^{a_2}-1, \ldots, (1+t_n)^{a_n}-1) = u_0(t_2, \ldots, t_n).$$

Substituting back into $(*)$ gives

$$Q(t_1, \ldots, t_n) = (1+t_1)^m \frac{U(t_1, \ldots, t_n) u_0((1+t_2)^{a_2}-1, \ldots, (1+t_n)^{a_n}-1)}{u_0(t_2, \ldots, t_n) U((1+t_1)^{a_1}-1, \ldots, (1+t_n)^{a_n}-1)}.$$

Setting

$$G(t_1, \ldots, t_n) = \frac{u_0(t_2, \ldots, t_n)}{U(t_1, \ldots, t_n)},$$

it follows that

$$Q(t_1, \ldots, t_n) = (1+t_1)^m \frac{G((1+t_1)^{a_1}-1, \ldots, (1+t_n)^{a_n}-1)}{G(t_1, \ldots, t_n)}.$$

□

Now that Lemma 2 has been proved, let $L(t_1, \ldots, t_n)$ be the power series defined at the beginning of the proof of part (2), namely

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

Without loss of generality, assume that $a_1 = \cdots = a_s = -1$ and $a_{s+1} = \cdots = a_n = 1$. Clearly, $L(t_1, \ldots, t_n)$ satisfies condition (2) but not necessarily condition (1) of Lemma 2. Define the power series

$$P_0(t_1, \ldots, t_n) = L(t_1, \ldots, t_n), \qquad P_1(t_1, \ldots, t_n) = L(0, t_2, \ldots, t_n),$$

$$P_2(t_1, \ldots, t_n) = L(0, 0, t_3, \ldots, t_n), \ldots, \qquad P_s(t_1, \ldots, t_n) = L(0, \ldots, 0, t_{s+1}, \ldots, t_n).$$

All these power series are in $1 + (t_1, \ldots, t_n)R[[t_1, \ldots, t_n]]$. Also, since $L(t_1, \ldots, t_n)$ satisfies condition (2) of Lemma 2, so does $P_i(t_1, \ldots, t_n)$, for all i. In particular, setting $i = s$ gives $P_s(t_1, \ldots, t_n)^2 = 1$, hence $P_s(t_1, \ldots, t_n) = 1$ (because $L(0, \ldots, 0) = 1$). Now for i in $\{1, \ldots, s\}$, define

$$Q_i(t_1, \ldots, t_n) = \frac{P_{i-1}(t_1, \ldots, t_n)}{P_i(t_1, \ldots, t_n)}.$$

https://doi.org/10.1017/S0017089514000147 Published online by Cambridge University Press

Each power series $Q_i(t_1, \ldots, t_n)$ satisfies all the hypotheses of Lemma 2, therefore it is of the form described in Lemma 2. It follows that the product of all $Q_i(t_1, \ldots, t_n)$, which equals $L(t_1, \ldots, t_n)$, is also of the same form and, by definition of $L(t_1, \ldots, t_n)$, the same holds for $F(t_1, \ldots, t_n)$, and this completes the proof. □

REFERENCE

1. P. Tzermias, On the p-adic binomial series and a formal analogue of Hilbert's Theorem 90, *Glasgow Math. J.* **47** (2005), 319–326.

https://doi.org/10.1017/S0017089514000147 Published online by Cambridge University Press