PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 94, Number 4, August 1985

A FORMAL ANALOGUE OF HILBERT'S THEOREM 90

R. COLEMAN

ABSTRACT. We prove a theorem on p-adic analytic functions which formally resembles Hilbert's Theorem 90 and which solves a problem originally proposed by Deligne and considered by Adolphson [A].

Let T denote the standard parameter on $\mathbf{C}_p$ and μ_{p^∞} the p-power roots of unity in $\mathbf{C}_p$. Then the ring of power series $R = \mathbf{Z}_p[[1 - T]]$ may naturally be considered as a ring of functions on μ_{p^∞}. Fix $l \in \mathbf{Z}_p^*$, let T^l denote the function on μ_{p^∞} which takes $\varepsilon \mapsto \varepsilon^l$. Then $T^l \in R$ (see [A]). Consider the following property of a series $F \in R$:

$$(*) \qquad \prod_{i=0}^{f-1} F(\varepsilon^{l^i}) = 1$$

for all $f \in \mathbf{Z}^+$, $\varepsilon \in \mu_{p^\infty}$ such that $\varepsilon^{l^f} = \varepsilon$.

THEOREM. *If F satisfies $(*)$ then there is a $G \in R^*$ such that $G(T)/G(T^l) = F(T)$.*

Note. Adolphson has checked this when l is of finite order in $\mathbf{Z}_p^*$ [A].

Let $F \in R$. Consider the following property:

$$(**) \qquad \sum_{i=0}^{f-1} F(\varepsilon^{l^i}) = 0$$

for all $f \in \mathbf{Z}^+$ and $\varepsilon \in \mu_{p^\infty}$ such that $\varepsilon^{l^f} = \varepsilon$.

PROPOSITION. (i) *If F satisfies $(**)$ then there exists a $G \in R$ satisfying*

$$G(T) - G(T^l) = F(T).$$

(ii) *Moreover, if $F \in (1 - T)^2R$, G may also be taken in $(1 - T)^2R$.*

First we prove a lemma. Let $R_n = R/(1 - T^{p^n})R$. The action $F(T) \mapsto F(T^l)$ for $F \in R$ induces a well-defined action on R_n.

LEMMA. *Suppose $F \in R_n$ such that*

$$(1) \qquad \sum_{i=0}^{f-1} F(T^{l^i}) = 0$$

where $l^f \equiv 1 \bmod p^n$. Then $F(T) = G(T) - G(T^l)$ for some $G \in R_n$.

Received by the editors June 29, 1984 and, in revised form, October 11, 1984.
1980 *Mathematics Subject Classification*. Primary 12B40.

PROOF. Let $S \subseteq \mathbf{Z}$ be a set of representatives of the orbits of multiplication by l on $\mathbf{Z}/p^n\mathbf{Z}$. If $s \in S$, let f_s denote the order of the orbit containing s. Every element $F \in R_n$ has a unique expression of the form

$$F(T) = \sum_{s \in S} \sum_{i=0}^{f_s - 1} b_{s,i} T^{sl^i}$$

where $b_{s,i} \in \mathbf{Z}_p$. If F satisfies (1) then it follows immediately that $\sum_{i=0}^{f_s-1} b_{s,i} = 0$ for $s \in S$. The lemma itself now follows immediately.

PROOF OF PROPOSITION. From the lemma it follows that for each $n \geqslant 0$ we can find a $G_n \in R$ such that

$$H_n(T) = G_n(T) - G_n(T^l) \equiv F(T) \bmod (1 - T^{p^n}).$$

It follows that

$$\lim_{n \to \infty} H_n(T) = F(T). \tag{2}$$

(*Note*. The topology on R is the $(p, 1 - T)$-adic topology.) Let G be a cluster value of the sequence $\{G_n(T)\}$ in R. From (2) it follows that $G(T) - G(T^l) = F(T)$. Finally, we may take $G(1) = 0$ and then (ii) follows by comparing coefficients.

PROOF OF THEOREM. Suppose F satisfies $(*)$. Then $F(1) = 1$. Let

$$H(T) = \log(F(T)) - \log(F(T^p))/p.$$

Then $H(T) \in (1 - T)^2 R$ using the Dieudonné-Dwork lemma and satisfies $(**)$, so there exists a $K(T) \in (1 - T)^2 R$ such that $K(T) - K(T^l) = H(T)$. Set

$$G(T) = \exp\left(\sum_{n=0}^{\infty} \frac{K(T^{p^n})}{p^n} \right).$$

It follows that $G(T) \in R$ again by the Dieudonné-Dwork lemma and $G(T)/G(T^l) = F(T)$.

REFERENCES

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

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720

Current address: Institut Fourier, Université de Grenoble I, Laboratoire de Mathématique Pures, B. P. 74, 38402 Saint-Martin-d'Hères, Cedex France