ALGEBRAIC INDEPENENCE OF CERTAIN FORMAL POWER SERIES (II)

H. Sharif

Department of Mathematics, College of Sciences, Shiraz University, Shiraz 71454, Islamic Republic of Iran

Abstract

We shall extend the results of [5] and prove that if $f=\Sigma_{n\geq 0} a_n x^n \in Z_p[[x]]$ is algebraic over $Q_p(x)$, where $a_0 = 1, f \neq 1$ and if $\lambda_1, \lambda_2, ..., \lambda_n$ are p-adic integers, then $1, \lambda_1, \lambda_2, ..., \lambda_n$ are linearly independent over Q if and only if $(1+x)^{\lambda_1}, (1+x)^{\lambda_2}, ..., (1+x)^{\lambda_n}$ are algebraically independent over $Q_p(x)$ if and only if $f^{\lambda_1}, f^{\lambda_2}, ..., f^{\lambda_n}$ are algebraically independent over $Q_p(x)$.

Introduction

In [5] we generalised Mendes-France and Van der Poorten's recent result (see [4, Theorem]) and we also proved the following theorem:

Theorem 1.1 Suppose that K is a field of characteristic $p>0$ and $f=\Sigma_{n\geq 0} a_n x^n \in K[[x]]$ is algebraic over $K(x)$, where $a_0 = 1$ and $f \neq 1$. Let $\lambda_1, \lambda_2, ..., \lambda_n$ be p-adic integers. Then the following statements are equivalent:

(i) $1, \lambda_1, \lambda_2, ..., \lambda_n$ are linearly independent over Q.

(ii) $(1+x)^{\lambda_1}, (1+x)^{\lambda_2}, ..., (1+x)^{\lambda_n}$ are algebraicially independent over $K(x)$.

(iii) $f^{\lambda_1}, f^{\lambda_2}, ..., f^{\lambda_n}$ are algebraically independent over $K(x)$.

In this paper we shall extend Mendes-France and Van der Poorten's result [4, Theorem] and also Theorem 1.1 over some fields of characteristic zero.

Throughout this paper, p will be prime a number. We shall denote the ring of p-adic integers by Z_p, the field of p-adic integers by Q_p and the Galois Field of order p by F_p. For a field K, $K[[x]]$ will denote the ring of formal power series in x with coefficients in K. We shall write $K((x))$ for the field of fractions of $K[[x]]$.

An element $f \in K((x))$ is said to be an algebraic function over K if f is algebraic over the field of rational functions $K(x)$.

keywords: Field; P-adic integers; Formal power series

Preliminaries

Let p be a prime number. For a p-adic integer $\theta \in Z_p$ we define the formal power series $(1+x)^\theta = \Sigma_{n=0}^{\infty} \binom{\theta}{n} x^n$, where

$$\binom{\theta}{n} = \frac{\theta(\theta-1)(\theta-2)...(\theta-n+1)}{n!}.$$

The following lemma is well-known.

Lemma 2.1 If $\theta \in Z_p$, then $(1+x)^\theta \in Z_p[[x]]$. That is, $\binom{\theta}{n} \in Z_p$ for all $n \in N$.

Proof. See, for example, Koblitz [2].

Remark 2.2 Suppose that f_θ is the reduction $(1+x)^\theta$ modulo the prime p. Since the map $\theta \rightarrow (1+x)$ is a continuous function (with respect to the x-acid metric on $F_p[[x]]$) from Z_p to $F_p[[x]]$, the series

$$f_\theta = (1+x)^\theta = \sum_{n=0}^{\infty} \binom{\theta}{n} x^n \pmod p,$$

as an element of $F_p[[x]]$, can be written in the following form:

$$f_\theta = (1+x)^\theta = (1+x)^{\Sigma_{i=0}^{\infty} \theta_i p^i} = \prod_{i=0}^{\infty} (1+x)^{\theta_i p^i} = \prod_{i=0}^{\infty} (1+x^{p^i})^{\theta_i}.$$

Now for a formal power series $f = 1 + \Sigma_{n=1}^{\infty} a_n x^n$ and $\theta \in Z_p$, we have

$$f^\theta = (1+(f-1))^{\Sigma_{i=0}^{\infty} \theta_i p^i} = \prod_{i=0}^{\infty} \left(1+(f-1)^{p^i}\right)^{\theta_i} = \sum_{n=0}^{\infty} \binom{\theta}{n} (f-1)^\theta,$$

which is an element of $F_p[[x]]$ [4].

$$b\,k^{2(2n+1)}|\mu|^2+|\mu|^2+|\mu|^{1-\frac{1}{n}}p=|\mu|^{1-\frac{1}{n}}\{P+|\mu|^{1+\frac{1}{n}}[1+b\,k^{2(2n+1)}]\}$$
$$\le k\left(a^2-\frac{k^2}{2}\right)$$

It is obvious that for sufficiently small $|\mu|$, we can make the above inequality to be true.

Hence by corollary 1, (16) has a 2ω -periodic solution $x(t)$ that

$$|x(t)|\le|\mu|^{\frac{1}{n}},|x'(t)|\le|\mu|^{\frac{1}{n}}k,|x''(t)|\le|\mu|^{\frac{1}{n}}k^2$$

(A₃) Consider the equation

$$x''+x'+x^3=\frac{1}{8}\,\mathrm{Sin}\,4t \qquad (20)$$

In this example we take $k=1$, $\omega=\frac{\pi}{4}$ and

$$M=\left\{|x'-f(t,x,x',x'')|:t\in(0,\omega],\ |x|\le C,\ |x'|\le Ck,|x''|\le Ck^2\right\}$$
$$\le C^3+\frac{1}{8}.$$

Hence for the condition (2) to be satisfied we must have

$$C^3+\frac{1}{8}\le\frac{1}{2}C.$$

Obviously it is true if we take $C=\frac{1}{2}$. Therefore, by corollary 1, equation (21) has a $\frac{\pi}{2}$ periodic solution for which

$$|x|\le C,|x'|\le Ck,|x''|\le Ck^2.$$

References

1. Cesari, L. Asymptotic Behavior and Stability Problems. 2nd Ed., Academic Press, New York, (1963).
2. Reissig, R. Periodic Solutions of a Third Order Nonlinear Differential Equations. *Ann. Math.* **13**, 139-148; (1971).
3. Mehri, B. and Hamedani, G.G. On the Existence of Periodic Solutions of Nonlinear Second Order Differential Equations *SIAM J. Appl. Math.* **29**; 72-76, (1975).

Results

M. Mendes-France and A.J. Van der Poorten in [4] proved the following theorem:

Theorem 3.1 Suppose that F is a finite field of characteristic $p>0$ and $f=\sum_{n\geq 0} a_n x^n \in F[[x]]$ is algebraic over F, where $a_0=1$ and $f\neq 1$. Let $\lambda \in Z_p$ be a p-adic integer. Then λ is rational if and only if f^{λ} is algebraic over F.

In [5] we generalised this theorem from a finite field to an infinite field of characteristic $p>0$. Now we shall generalise this result over some fields of characteristic zero.

Lemma 3.2 Let $\lambda \in Z_p$ be a p-adic integer and

$$f_\lambda=(1+x)^\lambda \sum_{n=0}^{\infty} \binom{\lambda}{n} x^n \in Z_p[[x]].$$

Then λ is rational if and only if f_λ is algebraic over Q_p.

Proof. Clearly if λ is rational, then $f_\lambda=(1+x)^\lambda$ is algebraic over Q_p. Conversely since f_λ is algebraic over Q_p, there exist elements $a_i(x)$, $i = 0,1,2,\dots, N$ in $Q_p[x]$ (after clearing the denominators), not all zero, such that

$$\sum_{i=0}^{N} a_i(x) f_\lambda^i(x)=0.$$

Let

$$a_i(x)=\sum_{j=0}^{N_i} b_{ij}x^j, \qquad b_{ij}\in Q_p.$$

Since for each $a \in Q_p$ there always exist $b \in Z_p$ such that $a=p^i b$ for some i, we can find $c_{ij} \in Z_p$ such that

$$\sum_{i=0}^{N}\sum_{j} c_{ij} p^{n_{ij}} x^j f_\lambda^i(x)=0.$$

Now multiplying by a suitable power of p, we may assume that not all of the coefficients c_{ij} of $x^j f_\lambda^i$, $i=0,1,2,\dots,N$ have the common factor p, but all in Z_p. We now reduce all the coefficients modulo p and obtain that

$$\sum \bar{c}_{ij} x^j \bar{f}_\lambda^i(x)=0.$$

Therefore, $\bar{f}_\lambda$ is algebraic over F_p and hence λ is rational by Theorem 3.1.

Theorem 3.3 Suppose that $f=\sum_{n\geq 0} a_n x^n \in Z_p[[x]]$ is algebraic over Q_p, where $a_0=1$ and $f\neq 1$. Let $\lambda \in Z_p$. Then λ is rational if and only if f^{λ} is algebraic over $Q_p(x)$.

Proof. Clearly if $\lambda \in Q$ then f^λ is algebraic over Q_p. Conversely, since $a_0=1$, we can change the notation to set $f=\sum_{n\geq 1} a_n x^n$ (that is, we replace f by $f-1$). Now suppose that both f and $(1+f)^\lambda$ are algebraic with $f\neq 0$. Now, if $f_\lambda=(1+x)^\lambda$, then $f_\lambda o f=(1+f)^\lambda$ and f are algebraic and so is f_λ (since f has a right inverse, g say, with $g(x)$ an algebraic formal power series in some fractional power of x). By Lemma 3.2, f_λ being algebraic over Q_p, implies that λ is rational and hence the proof is completed.

More generally, we use the above argument and generalise Theorem 3.3 in the following form:

Theorem 3.4 Suppose that $f=\sum_{n\geq 0} a_n x^n \in Z_p[[x]]$ is algebraic over Q_p, where $a_0=1$ and $f\neq 1$. Let $\lambda_1, \lambda_2, \dots, \lambda_n$ be p-adic integers. Then the following conditions are equivalent:

(i) $1, \lambda_1, \lambda_2, \dots, \lambda_n$ are linearly independent over Q.

(ii) $(1+x)^{\lambda_1}, (1+x)^{\lambda_2}, \dots, (1+x)^{\lambda_n}$ are algebraically independent over $Q_p(x)$.

(iii) $f^{\lambda_1}, f^{\lambda_2}, \dots, f^{\lambda_n}$ are algebraically independent over $Q_p(x)$.

First we need some more lemmas.

Lemma 3.5 Let K be any field. Suppose that

$$f=\sum_{n=1}^{\infty} a_n x^n \in K((x))$$

is an algebraic function, where $a_1\neq 0$ *and* $h_1, h_2, \dots, h_n \in K((x))$ are algebraically dependent over $K(x)$. Then $h_1 o f, h_2 o f, \dots, h_n o f$ are algebraically dependent over $K(x)$.

Proof. See Sharif [5, Lemma 3.3].

We state the following well-known lemma.

Lemma 3.6 Let K be a field and $f=\sum_{n=0}^{\infty} a_n x^n$, $g=\sum_{n=0}^{\infty} b_n x^n$, be the elements of $K[[x]]$. Then the following statements are held:

(i) If f and g are algebraic over K, then so is fog, provided that the formal composition fog is defined.

(ii) Suppose that $a_0=0$ *and* $a_1=0$ (so that the formal compositional inverse f^{-1} exists, with the defining property $fof^{-1}(x)=f^{-1} of (x)=x$). If f is algebraic, then so is f^{-1}.

Proof. See, for example, Stanley [6, p. 178].

We are now in a position to prove Theorem 3.4.

Proof of Theorem 3.4. (i) $\Rightarrow$ (ii) Suppose that $1, \lambda_1, \lambda_2, \dots, \lambda_n$ are linearly independent over Q. Suppose that $f\lambda_1=(1+x)^{\lambda_1}, f\lambda_2=(1+x)^{\lambda_2}, \dots, f\lambda_n=(1+x)^{\lambda_n}$ are algebraically dependent over $Q_p(x)$. Then there exist polynomials $P_{i_1 i_2 \dots i_n}(x) \in Q_p[x]$ (after clearing the denominators), not all zero, such that

$$\sum P_{i_1 i_2 \dots i_n}(x) f_{\lambda_1}^{i_1} f_{\lambda_2}^{i_2} \dots f_{\lambda_n}^{i_n}=0. \quad (3.1)$$

(finite sum). Let

$$P_{i_1 i_2 \dots i_n}(x)=\sum_{j=1}^{N} b_{i_1 i_2 \dots i_n j} x^j, \quad (3.2)$$

where $b_{i_1 i_2 \dots i_n j} \in Q_p$. For each j, we can find $c_{i_1 i_2 \dots i_n j} \in Z_p$ such that $b_{i_1 i_2 \dots i_n j} = p^{n_{i_1 i_2 \dots i_n j}} \times c_{i_1 i_2 \dots i_n j}$. Hence from the equations (3.1) and (3.2) we get

$$\sum\sum_{j=1}^{N} c_{i_1 i_2 \dots i_n j} x^j p^{n_{i_1 i_2 \dots i_n j}} f_{\lambda_1}^{i_1} f_{\lambda_2}^{i_2} \dots f_{\lambda_n}^{i_n} = 0 \quad (3.3)$$

(finite sum). Now multiplying by a suitable power of p, we may assume that not all of the coefficients $c_{i_1 i_2 \dots i_n j}$ of $x^j f_{\lambda_1}^{i_1} f_{\lambda_2}^{i_2} \dots f_{\lambda_n}^{i_n}$ in equation (3.3) have the common factor p, but all belong to Z_p. We now reduce all the coefficients in (3.3) modulo p and obtain the nontrivial equation

$$\sum\sum_{j=1}^{N} \bar{c}_{i_1 i_2 \dots i_n j} x^j \bar{f}_{\lambda_1}^{i_1} \bar{f}_{\lambda_2}^{i_2} \dots \bar{f}_{\lambda_n}^{i_n} = 0$$

(finite sum) Therefore, $\bar{f}_{\lambda_1}, \bar{f}_{\lambda_2}, \dots, \bar{f}_{\lambda_n}$ are algebraically dependent over $F_p(x)$ and hence $1, \lambda_1, \lambda_2, \dots, \lambda_n$ are linearly dependent over Q by Theorem 1.1, which is a contradiction. Thus $f_{\lambda_1}, f_{\lambda_2}, \dots, f_{\lambda_n}$ are algebraically independent over $Q_p(x)$.

(ii) ⇒ (iii) Suppose that $f^{\lambda_1}, f^{\lambda_2}, \dots, f^{\lambda_n}$ are algebraically dependent over $Q_p(x)$. Since $a_0 = 1$ we can change the notation to set $f = \sum_{n=1}^{\infty} a_n x^n$ (that is, we replace f by $f - 1$). Let $f_{\lambda_i} = (1+x)^{\lambda_i}$ for $i = 1, 2, \dots, n$. Then $f_{\lambda_1} of, \dots, f_{\lambda_n}$ of are algebraically dependent over $Q_p(x)$ by assumption. Suppose that $g = \sum_{n \ge 1} b_n x^n$ is the formal compositional inverse of f. Then by Lemma 3.6(ii), g is algebraic over $Q_p(x)$. Hence by Lemma 3.5, since $b_1 \neq 0$ by the choice of f,

$$(f_{\lambda_1} of) og, (f_{\lambda_2} of) og, \dots, (f_{\lambda_n} of) og$$

are algebraically dependent over $Q_p(x)$. That is, $f_{\lambda_1}, f_{\lambda_2}, \dots, f_{\lambda_n}$ are algebraically dependent over $Q_p(x)$, which is a contradiction to the hypothesis.

(iii) ⇒ (i) Suppose that $1, \lambda_1, \lambda_2, \dots, \lambda_n$ are linearly dependent over Q. Then there exist integers $r_1, r_2, \dots, r_n, r_{n+1} = 0$. in Z (after clearing the denominators), not all zero, such that $r_1\lambda_1 + r_2\lambda_2 + \dots + r_n\lambda_n + r_n + 1 = 0$. Thus

$$(f^{\lambda_1})^{r_1} (f^{\lambda_2})^{r_2} \dots (f^{\lambda_n})^{r_n} (f)^{r_{n+1}} = 1.$$

Hence $f^{\lambda_1}, f^{\lambda_2}, \dots, f^{\lambda_n}$ are algebraically dependent over $Q_p(x, f)$. Since f is algebraic over $Q_p(x)$, we get that $f^{\lambda_1}, f^{\lambda_2}, \dots, f^{\lambda_n}$ are algebraically dependent over $Q_p(x)$ (see Van der Waerden [7, Theorem 3, p. 201]), which is a contradiction and hence the proof is completed.

Let K be a perfect field of characteristic $p > 0$. Let K [[x]] be the ring of formal power series in k commuting variables $X = (x_1, x_2, \dots, x_k)$ and K (X) the field of rational functions in X over K. For a p-adic integer $\theta = \sum_{i \ge 0} \theta_i p^i$, where $0 \le \theta_i \le p - 1$ one can define

$$g_\theta = (1 + x_1 + x_2 + \dots + x_k)^\theta = \prod_{i=0}^{\infty} (1 + x_1^{p^i} + x_2^{p^i} + \dots + x_k^{p^i})^{\theta_i}$$

as in Remark 2.2.

Recently, T. Harase informed me that he had proved the following result, which now appears in [1].

Theorem 4.1 For p-adic integers $\lambda_1, \lambda_2, \dots, \lambda_n$ the series $g_{\lambda_1}, g_{\lambda_2}, \dots, g_{\lambda_n}$ of K [[X]] are algebraically independent over K (X) if and only if $1, \lambda_1, \lambda_2, \dots, \lambda_n$ are linearly independent over Z.

Using the following lemma, Theorem 4.1 can be generalised from a perfect field of characteristic $p > 0$ to an arbitrary field of characteristic $p > 0$.

Lemma 4.2 Suppose that K is any field $h_1, h_2, \dots, h_n \in$ K ((X)). If $h_1, h_2, \dots, h_n$ are algebraically dependent over L (X), where L is an extension field of K, then $h_1, h_2, \dots, h_n$ are algebraically dependent over K (X).

Proof. Since $h_1, h_2, \dots, h_n$ are algebraically dependent over L (X), there exist polynomials $a_{i_1 i_2 \dots i_n}$ in L (X) (after clearing the denominators), not all zero, such that

$$\sum_{i_j=0}^{N_j} a_{i_1 i_2 \dots i_n}(X) h_1^{i_1} h_2^{i_2} \dots h_n^{i_n} = 0. \quad (4.1)$$

For each n-tuple $(i_1, i_2, \dots, i_n)$, $i_j = 0, 1, 2, \dots, N_j$ and $j = 1, 2, \dots, n$ we have

$$a_{i_1, i_2, \dots, i_n}(X) = \sum_t b_{i_1 i_2 \dots i_n t} X^t$$

(a finite sum) and from above there exists the coefficient $b_{i_1 i_2 \dots i_n v} \in L$ which is non-zero.

Let $b_{i_1 i_2 \dots i_n v}$ be the first element of a basis B for L over K. Define a K-linear map

$$\phi : L \to K$$

such that if $x \in B$, then

$$\phi(x) = \begin{cases} 1 & \text{if } x = b_{i_1 i_2 \dots i_n v}, \\ 0 & \text{otherwise} \end{cases}$$

Hence, if we denote $\phi(x)$ by $\bar{x}$ then from (4.1) we get

$$\sum_{i_j=0}^{N_j} \bar{a}_{i_1 i_2 \dots i_n}(X) h_1^{i_1} h_2^{i_2} \dots h_n^{i_n} = 0,$$

where the finite sum

$$\bar{a}_{i_1 i_2 \dots i_n}(X) = \sum_t \bar{b}_{i_1 i_2 \dots i_n t} X^t$$

is a non-zero element of K [X] for some $(i_1 i_2, \dots, i_n)$, by the choice of ϕ. Therefore, $h_1 h_2, \dots, h_n$ are algebraically depen-

dent over K(X) and hence the proof is completed.
Therefore, we have the following theorem.

Theorem 4.3 Let L be a field of characteristic p>0. For p-adic integers $\lambda_1\lambda_2, \dots, \lambda_n$, the series $g_{\lambda_1}, g_{\lambda_2}, \dots, g_{\lambda_n}$ of L[[X]] are algebraically independent over L(X) if and only if $1, \lambda_1, \lambda_2, \dots, \lambda_n$ are linearly independent over Z.

By the method which was used in section 3, one can extend Theorem 4.3 from a field of characteristic $p > 0$ to some fields of characteristic zero.
That is,

Theorem 4.4 Suppose that $\lambda_1, \lambda_2, \dots, \lambda_n$ are p-adic integers. Then $1, \lambda_1, \lambda_2, \dots, \lambda_n$ are linearly independent over Q if and only if $g_{\lambda_1}, g_{\lambda_2}, \dots, g_{\lambda_n}$, the elements of Z_p[[X]], are algebraically independent over $Q_p(X)$.

Acknowledgements

The author would like to thank the Research Center of Shiraz University for its financial support Grant No. 68-SC-556-294.

References

1 Harase, T. Algebraic Dependence of Formal Power Series, LNM, no. 1434, pp. 133-137.
2 Koblitz, N. P-adic Analysis; A Short Course on Recent Work, Cambridge U.P.; LMS Lecture Note series 46, p. 3 (1980).
3 Mahler, K. Lectures on Diophantine Approximations, Ann Arbor, Michigan, (1961).
4 Mendes-France, M. and Van der Poorten, Automata and the Arithmetic of Formal Power Series, *Acta Arith.* **46**, pp. 211-214, (1986).
5 Sharif, H. Algebraic Independence of Certain Formal Power Series (I), *J. Sci. I. R. Iran* (to appear).
6 Stanley, R.P. Differentiably Finite Power Series, *Europ. J. Combinatorics* 1, pp. 175-188, (1980).
7 Van der Waerden, B.L. *Modern Algebra*, Vol.I, Frederick Ungar, New York, (1966).