Vol.2,No.1,2
Winter&Spring,1991

ALGEBRAIC INDEPENDENCE OF CERTAIN FORMAL POWER SERIES (I)

H. Sharif
Department of Mathematics, Faculty of Science , Shiraz University, Shiraz, Islamic Republic of Iran

Abstract

We give a proof of the generalisation of Mendes-France and Van der Poorten's recent result over an arbitrary field of positive characteristic and then by extending a result of Carlitz, we shall introduce a class of algebraically independent series.

Introduction

In 1986, M. Mendes-France and A. J. Van der Poorten [5] showed that if $f=\sum_{n=0}^{\infty} a_n x^n \varepsilon F[[x]]$ is algebraic, where F is a finite field of characteristic p>0, $a_0=1$ and $f\neq 1$ and if λ is a p-adic integer, then f^{λ} is algebraic if, and only if λ is rational. One can generalise this result from a finite field to an infinite field of characteristic p>0. However, we shall generalise this result and prove the following theorem:

Theorem A. Suppose that K is a field of characteristic p>0. Suppose that $f=\sum_{n\geq 0} a_n x^n \varepsilon K[[x]]$ is algebraic over K, where $a_0=1$ and $a_1\neq 0$. Let $\lambda_1, \lambda_2, ..., \lambda_n$ be p-adic integers. Then the following conditions 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 algebraically independent over K(x).

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

Throughout this paper, p will be a prime number. We shall denote the ring of p-adic integers by z_p, and the Galois Field of order p by F_p.

Keywords: Field, P-adic Integer, Formal Power Series, Algebraic Independence

2. Preliminaries.

Let p be a prime. Every p-adic integer $\theta \varepsilon z_p$ (not necessarily rational*) has a unique p-adic expansion $\theta = \sum_{i=0}^{\infty} \theta_i p^i$, where $\theta_i \varepsilon z$ and $0\leq\theta_i\leq p-1$. We define for any $\theta \varepsilon z_p$ the formal power series

$$(1+x)^{\theta} = \sum_{n=0}^{\infty} \binom{\theta}{n} x^n, \qquad (2.1)$$

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

We state the following well-known lemma.

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

Proof. For example, see **Koblitz** [4, p.3].

Remark 2.2. Suppose now that f_θ is the reduction of $(1+x)^{\theta}$ modulo the prime p. Since the map $\theta \longrightarrow f_\theta$ is a continuous function (with respect to the x-adic metric on $F_p[[x]]$) from z_p to $F_p[[x]]$), for a formal

(*) A p-adic integer may be an irrational number. For example, $\theta = \sum_{n=0}^{\infty} p^{n!}$ is an irrational (in fact transcendental) p-adic integer in z_p.

power series $f = 1+\sum_{n=1}^{\infty} a_n x^n$ and $\theta \varepsilon z_p$. we have

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

which is an element of $F_p[[x]]$ (see [5]).

Let K be a field. $K[[x]]$ will denote the ring of formal power series in x with coefficients in K, that is,

$f \varepsilon K[[x]]$ if $f = \sum_{n=0}^{\infty} a_n x^n$, where $a_n \varepsilon K$.

We shall write K((x)) for the field of fractions of $K[[x]]$.

An element f ε K((x)) is said to be an algebraic series over K if F is algebraic over the field of rational functions K(x).

3. Results

M. Mendes-France and A. J. Van der Poorten in [5], in analogy with the Gelfond-Schneider theorem conjectured and later, with a slight modification, proved the following theorem.

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

One can generalise this theorem from a finite field to an infinite field of characteristic p>0 by use of the following lemma:

Lemma 3.2. Suppose that K is any field. If h ε K((x)) is an algebraic function over L, where L is an extension field of K, then h is an algebraic function over K.

Proof. See Sharif-Woodcock [6, Theorem 6.1, p.401] for the case of several variables.

More generally, we intend to extend Theorem 3. 1 and prove Theorem A. (*) First we need some more lemmas.

Lemma 3.3. Let K be any field. Suppose that $f = \sum_{n=1}^{\infty} a_n x^n \varepsilon K((x))$ is an algebraic series, wher $a_1 \neq 0$ and $h_1 h_2, \dots, h_n \varepsilon K((x))$ are algebraically dependent over K(x). Then h_1 of, h_2 of,...,h_n of are algebraically dependent over K(x).

Proof. Since $a_0 = 0$, the formal composition h_i of exists for i = 1, 2,..., n.

Now since $h_1, h_2, \dots, h_n$ are algebraically dependent over K(x), there exist elements $\alpha_{i_1 i_2 \dots i_n}$ in K(x), not all zero, such that

$$\sum_{1\leq j\leq n}\ \sum_{1\leq i_j \leq N_j} \alpha_{i_1 i_2 \dots i_n}(x) h_1^{i_1} h_2^{i_2} \dots h_n^{i_n} = 0$$

Hence

$$\sum_{i_j=1}^{N_j} \alpha_{i_1 i_2 \dots i_n}(f)(h_1 \text{ of})^{i_1}(h_n \text{ of})^{i_2} \dots (h_n \text{ of})^{i_n} = 0 \quad (3.1)$$

$j = 1,2,\dots,n$

Equation (3.1) is non-trivial, since otherwise, if g is the compositional inverse of f (which in fact exists as $a_0 = 0$ and $a_1 \neq 0$), then composing g with (3.1) we get the equation

$$\sum_{i_j=1}^{N_j} \alpha_{i_1 i_2 \dots i_n}(x) h_1^{i_1} h_2^{i_2} \dots h_n^{i_n} \doteq 0$$

$j = 1,2,\dots,n$

is trivial, which is a contradiction. Therefore, h_1 of, h_2 of,...,h_n of are algebraically dependent over K (x,f). Since f is algebraic, h_1 of, h_2 of,...,h_n of are algebraically dependent over K(x) (see Van derWaerden [7, Theorem 3, p. 201])

The following lemma is a generalisation of Lemma 3.2 to the case of several functions.

Lemma 3.4. Suppose that K is any field. Suppose that $h_1 h_2, \dots, h_n \varepsilon K((x))$. 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

(*) M. Mendes-France has informed me that he, J.P. Allouche and A. J. Van der Poorten have independently proved this Theorem over a finite field, by a somewhat different method. Their proof has now appeared in [1].

$$\sum_{i_j=0}^{N_j} a_{i_1 i_2 \ldots i_n}(x) h_1^{i_1} h_2^{i_2} \ldots h_n^{i_n} = 0$$

$j = 1,2,\ldots,n$

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

$$a_{i_1 i_2 \ldots i_n}(x) = \sum_j b_{i_1 i_2 \ldots i_n j} x^j$$

(a finite sum) and from the above there exists some coefficient $b_{i_1 i_2 \ldots i_n k} \varepsilon L$ which is non-zero. Let $b_{i_1 i_2 \ldots i_n k}$ be the first element of a basis B for L over K. Define a K-linear map ϕ: $L \longrightarrow K$ such that if $\beta \varepsilon B$ then

$$\phi(\beta) = \begin{cases} 1 & \text{if } \beta = b_{i_1 i_2 \ldots i_n k,} \\ 0 & \text{otherwise.} \end{cases}$$

Hence, if we denote $\phi(\beta)$ by $\bar{\beta}$ then from (3.2) we get

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

$j = 1,2,\ldots,n$

where the finite sum

$$\bar{a}_{i_1 i_2 \ldots i_n}(x) = \sum_j \bar{b}_{i_1 i_2 \ldots i_n j} x^j$$

is a non-zero element of K[x] for some $(i_1,i_2,\ldots,i_n)$, by the choice of ϕ.

Therefore, $h_1,h_2,\ldots,h_n$ are algebraically dependent over K(x) and hence the proof is complete.

Note. The above theorem can be generalised to the case of several vairables.

In [6] we introduced a splitting process for series over a perfect field and defined associated semi-linear operators on the field of fractions of the ring of formal power series. We state the following lemma whose proof (in the case of several variables) can be found in [6].

Lemma 3.5. Let K be a perfect field of characteristic p>0. If $f \varepsilon K[[x]]$ (respectively K((x))), then f can be written uniquely as $f = \sum_{i=0}^{p-1} x^i f_i^p$ for some $f_i \varepsilon K[[x]]$ (respectively K((x))).

Now for $i \varepsilon \{0,1,2,\ldots,p-1\}$ define $E_i: K((x)) \longrightarrow K((x))$ by $E_i(f) = f_i$. For $f \varepsilon K((x))$, by Lemma 3.5 we have

$$f = \sum_{i=0}^{p-1} x^i (E_i(f))^p. \quad (3.3)$$

Remark 3.6: Let α be a p-adic integer and $\sum_{i=0}^{\infty} \alpha_i p^i$ be the p-adic expansion of α in z_p. Let $f_\alpha = (1+x)^\alpha \varepsilon F_p[[x]]$. Then

$$f_\alpha = (1+x)^\alpha = (1+x)^{\alpha_0}\left[(1+x)^{\frac{\alpha-\alpha_0}{p}}\right]^p.$$

Hence by Lemma 3.5 and equation (3.3), we have

$$E_i(f_\alpha) = \binom{\alpha_0}{i}(1+x)^{\frac{\alpha-\alpha_0}{p}}$$

for $i = 0,1,2,\ldots,p-1$.

First we prove the following lemma.

Lemma 3.7. Suppose that $\theta_1,\theta_2,\ldots,\theta_n \varepsilon z_p$. If $1,\theta_1,\theta_2,\ldots,\theta_n$ are linearly independent over Q, then $f_{\theta_1}, f_{\theta_2},\ldots,f_{\theta_n}$ are algebraically independent over $F_p(x)$.

Proof. Suppose that $f_{\theta_1}, f_{\theta_2},\ldots,f_{\theta_n}$ are algebraically dependent over $F_p(x)$. Then there exist polynomials (after clearing the denominators) $p_{i_1 i_2 \ldots i_n}(x)$ in $F_p[x]$, not all zero, such that

$$\sum_{i_j=0}^{N_j} p_{i_1 i_2 \ldots i_n}(x) f_{\theta_1}^{i_1} f_{\theta_2}^{i_2} \ldots f_{\theta_n}^{i_n} = 0. \quad (3.4)$$

$j = 1,2,\ldots,n$

By a change of variable let $P_{i_1 i_2 \ldots i_n}(x)$ be a polynomial in (1+x),

$$p_{i_1 i_2 \ldots i_n}(x) = \sum_{i_{n+1}=0}^{N_{n+1}} a_{i_1 i_2 \ldots i_{n+1}} (1+x)^{i_{n+1}}$$

$$= \sum_{i_{n+1}=0}^{N_{n+1}} a_{i_1 i_2 \ldots i_{n+1}} f_{i_{n+1}}$$

say, where $a_{i_1 i_2 \ldots i_{n+1}} \varepsilon F_p$ and some $a_{i_1 i_2 \ldots i_{n+1}} \neq 0$. Hence from the above equation and equation (3.4) as $f_\alpha = (1+x)^\alpha$ we get

$$\sum_{i_j=0}^{N_j} a_{i_1 i_2 \ldots i_{n+1}} f_{i_1\theta_1 + i_2\theta_2 + i_n\theta_n + i_{n+1}} = 0. \quad (3.5)$$

$j = 1,2,\ldots,n+1$

Let

$$\theta_\gamma = i_1\theta_1 + i_2\theta_2 + \ldots + i_n\theta_n + i_{n+1},$$

where $\gamma = (i_1,i_2,\ldots,i_{n+1})$. Then from (3.5) we can write

$$\sum_{\gamma} a_\gamma f_{\theta_\gamma} = 0 \qquad (3.6)$$

(a finite sum). Let r,r>1 be the number of non-zero terms in (3.6). Since $1,\theta_1,\theta_2,...,\theta_n$ are linearly independent over Q, $\theta_\gamma \neq \theta_\sigma$ for $\gamma \neq \sigma$. Suppose that we choose an equation of the form (3.6) with r minimal.

Now for the p-adic integer

$$\alpha = \sum_{\iota=0}^{\infty} \alpha_\iota p^i$$

define

$$T(\alpha) = \sum_{i=0}^{\infty} \alpha_\iota + 1^{p^i}$$

Then we have

$$\alpha = \alpha_0 + pT(\alpha). \qquad (3.7)$$

Suppose that $\theta_\gamma(0) = n_{0,\gamma}$ is the coefficient of p^O in the p-adic expansion of the p-adic integer

$$\theta_\gamma = \sum_{\kappa=0}^{\infty} n_{k,\gamma} p^k. \qquad (3.8)$$

Suppose that the $\theta_\gamma(0)$ are equal. Using (3.7), as $\theta_\gamma \neq \theta_\sigma$, we have that $T(\theta_\gamma) \neq T(\theta_\sigma)$. Hence from (3.6) we get

$$\sum a_\gamma f_{T(\theta_\gamma)} = 0. \qquad (3.9)$$

Equivalently, applying E_0 to (3.6) by Remark 3.6 we get (3.9). Now, by applying E_0 to (3.6) repeatedly, without loss of generality, we can assume that the $\theta_\gamma(0)$ are not all equal. For, in (3.8), as $\theta_\gamma \neq \theta_\sigma$, we have $n_{k,\gamma} \neq n_{k,\sigma}$ for some k.

Now suppose that $\lambda = \max \theta_\gamma(0)$. Hence there exist γ, σ such that $\theta_\gamma(0) = \lambda$ and $\theta_\sigma(0) < \lambda$. By Remark 3.6 we have

$$E_\lambda\left((1+x)^{\theta_\gamma}\right) = \begin{pmatrix} \theta_\gamma(0) \\ \lambda \end{pmatrix} (1+x)^{T(\theta_\gamma)} = (1+x)^{T(\theta_\gamma)}$$

and

$$E_\gamma (1+x)^{\theta_\sigma} = \begin{pmatrix} \theta_\sigma(0) \\ \lambda \end{pmatrix} (1+x)^{T(\theta_\sigma)} = 0.$$

Hence by applying E_λ to (3.6) we get

$$\sum_{\substack{\gamma \\ \theta_\gamma(0)=\lambda}} a_\gamma f_{T(\theta_\gamma)} = 0, \qquad (3.10)$$

which is non-trivial and shorter than (3.6). Moreover, from (3.7) we have

$$T(\theta_\gamma) \neq T(\theta_\sigma)$$

if $\theta_\gamma(0) \neq \theta_\sigma(0)$ for $\gamma \neq \delta$ Hence we have a similar equation to (3.6) of length <r, which is a contradiction. Therefore, $f_{\theta_1}, f_{\theta_2}, \ldots, f_{\theta_n}$ are algebraically independent over $F_p(x)$ and hence the proof is complete.

We are now in a position to prove Theorem A.

Proof of Theorem A. (i) implies (ii) Suppose that $1,\lambda_1,\lambda_2,...,\lambda_n$ are linearly independent over Q. If $(1+x)^{\lambda_1}, (1+x)^{\lambda_2},..., (1+x)^{\lambda_n}$ are algebraically dependent over K(x), then by Lemma 3.4, they are also algebraically dependent over $F_p(x)$ which is a contradiction by Lemma 3.7.

(ii) implies (iii) Suppose that $f^{\lambda_1}, f^{\lambda_2}, \ldots, f^{\lambda_n}$ are algebraically dependent over K (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

$$f_{\lambda_i}(x) = (1+x)^{\lambda_i}$$

for i = 1,2,3,...,n. Then

$$f_{\lambda_1} of, f_{\lambda_2} of, \ldots, f_{\lambda_n} of$$

are algebraically dependent over K (x) by assumption. Suppose that $g = \sum_{n\geq 1} b_n x^n$ is the formal compositional inverse of f. Then g is algebraic over K. Hence by Lemma 3.3, since $b_1 \neq 0$ by the choice of f,

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

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

(iii) implies (i) Suppose that $1,\lambda_1,\lambda_2,..., \lambda_n$ are linearly dependent over Z. Then there exist $1,\lambda_1,\lambda_2,..., \lambda_n, r_{n+1}$ not all zero, such that

$$r_1\lambda_1 + r_2\lambda_2 + \ldots + r_n\lambda_n + r_{n+1} = 0.$$

Thus

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

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

4. Some Further Results.

In this section F will denote the Galois Field of order p, p prime and $f = \sum_{n=0}^{\infty} x^{q^n - 1}$, where $q = p^s$.

L. Carlitz in [2] conjectured that the expansion

$$\left(\sum_{n=0}^{\infty} x^{q^n-1}\right)^{\theta} = \sum_{n=0}^{\infty} \binom{\theta+nq}{n} x^{n(q-1)},$$

where θ is an arbitrary rational number with denominator prime to p, holds over F. Later, in [3] he proved this conjecture:

Theorem 4.1. Let $\theta \varepsilon Q$ with denominator prime to p. Then

$$f^{\theta} = \sum_{n\geq 0} \binom{\theta+nq}{n} x^{n(q-1)}.$$

We shall show that this expansion does hold over F for any p-adic integer $\theta \varepsilon z_p$. Then, we shall introduce a class of a lgebraically independent series.

Note that $f = \sum_{n=0}^{\infty} x^{q^n-1} = 1 + \sum_{n=1}^{\infty} x^{q^n-1}$.

Hence for $\theta \varepsilon z_p$, f^{θ}, as an element of $F[[x]]$ is well-defined (see Remark 2.2).

Theorem 4.2. Let $\theta \varepsilon z_p$. Then

$$f^{\theta} = \sum_{n\geq 0} \binom{\theta+nq}{n} x^{n(q-1)}$$

Proof.

$$f^{\theta} = \left[1 + \sum_{n\geq 1} x^{q^n-1}\right]^{\theta} = \left[1 + x^{q-1} \sum_{n\geq 0} x^{q(q^n-1)}\right]^{\theta}$$

$$= \sum_{i\geq 0} \binom{\theta}{i} x^{i(q-1)} \left(\sum_{n\geq 0} x^{q(q^n-1)}\right)^{i}$$

(by equation (2.1))

$$= \sum_{i\geq 0} \binom{\theta}{i} x^{i(q-1)} \sum_{n\geq 0} \binom{i+nq}{n} x^{nq(q-1)}$$

(by Theorem 4.1, as $i \varepsilon N$)

$$= \sum_{t\geq 0} x^{t(q-1)} \sum_{i+nq=t} \binom{\theta}{i}\binom{t}{n} = \sum_{t\geq 0} x^{t(q-1)} \sum_{t\geq nq} \binom{\theta}{t-nq}\binom{t}{n}.$$

Hence we must show that

$$\sum_{t\geq nq} \binom{\theta}{t-nq}\binom{t}{n} = \binom{\theta+tq}{t}.$$

Consider

$$\sum_{t\geq 0} \sum_{n=0}^{\mathrm{Min}(t/q,m)} \binom{\theta}{t-nq}\binom{m}{n} x^{t} = \sum_{n=0}^{m} \binom{m}{n} x^{nq} \sum_{t=0}^{\infty} \binom{\theta}{t} x^{t}$$

$$= \sum_{n=0}^{m} \binom{m}{n} x^{nq} (1+x)^{\theta} = (1+x^q)^m (1+x)^{\theta} = (1+x)^{qm} (1+x)^{\theta} = (1+x)^{qm+\theta}$$

$$= \sum_{t\geq 0} \binom{\theta+qm}{t} x^{t} \pmod p.$$

Hence $\sum_{n=0}^{\mathrm{Min}(t/q,m)} \binom{\theta}{t-nq}\binom{m}{n} = \binom{\theta+qm}{t}$.

Substituting m = t, we get $\sum_{nq\leq t} \binom{\theta}{t-nq}\binom{t}{n} = \binom{\theta+qt}{t}$ as required.

Note. If $f = \sum_{n\geq 0} x^{q^n-1}$, then $(xf)^q = \sum_{n\geq 1} x^{q^n} = xf - x$.

Hence f is an algebraic series over F.

Corollary 4.3. Let $\theta \varepsilon z_p$. Then the series $\sum_{n=0}^{\infty} \binom{\theta+nq}{n} x^{n(q-1)}$ is algebraic over F if, and only if, θ is rational.

Corollary 4.4. Let K be a field of characteristic p>0. Let $\theta_1, \theta_2, ..., \theta_n$ be p-adic integers. Then the set $\{1, \theta_1, \theta_2, ..., \theta_m\}$ is linearly independent over Q if, and only if, $\{\sum_{n=0}^{\infty} \binom{\theta_i+nq}{n} x^{n(q-1)}\}_{i=1}^{m}$ is a set of algebraically independent series over K (x).

Acknowledgements

The author would like to express his gratitude to Dr C.F. Woodcock and to thank the Research center of Shiraz University for its financial support. # 68-556-294

References

1. J.P. Allouche, M. Mendes-France and A.J. Van der Poorten Independance algebraique de certaines series formelles. *Bull Soc. Math. France* **116** no. 3 449-454(1989).
2. L Carlitz, Some congruences involving sums of binomia coefficients. *Duke Math. J.*. **27** 77-79 (1960).
3. L. Carlitz, On the power series expansion of certain function over a field of characteristic p. *Indian J. Math.* **29** 159-16 (1987).
4. N. Koblitz, p-adic analysis, a short course on recent worl (Cambridge U.P.; LMS Lecture Note series **46**, 1980).
5. M. Mendes-France and A.J. Van der Poorten, Automata and th

arithmetic of formal power series, Acta Arith. **46** 211-214 (1986).

6. H. Sharif and C.F. Woodcock, Algebraic functions over a field of positive characteristic and Hadamard products, J. London Math. Soc. (2) **37** 395-408 (1988).
7. B.L. Van der Waerde, Modern Algebra Vol I (Frederick Ungar, New York, 1966).