ISRAEL JOURNAL OF MATHEMATICS, Vol. 63, No. 3, 1988

ALGEBRAIC ELEMENTS IN FORMAL POWER SERIES RINGS

BY

TAKASHI HARASE

Department of Mathematics, Tokyo Institute of Technology, Oh-okayama, Meguro-ku, Tokyo 152, Japan

Dedicated to the memory of Chiyo Harase

ABSTRACT

We obtain a theorem giving a condition for algebraicity of an element in a formal power series field of characteristic $p > 0$. Using it many results can be proved, for example, the "theorem of the diagonal" of Furstenberg is deduced as an easy corollary.

Introduction

Let p be a prime number and q be some power of p. If k is a field of characteristic p, $k[[\boldsymbol{x}]]$ will denote the formal power series ring with coefficients in k and indeterminates $\boldsymbol{x} = (x_1, \ldots, x_m)$. $k((\boldsymbol{x}))$ will denote the quotient (or fraction) field of $k[[\boldsymbol{x}]]$. We consider the elements in $k((\boldsymbol{x}))$ which are algebraic over $k(\boldsymbol{x})$. About those elements there are several well-known results. The first is the following theorem of Christol et al. in [1].

THEOREM 1. *If k is a finite field of q elements, then an element f in $k[[x]]$ is algebraic over $k(x)$ if and only if f is q-recognizable.*

But in fact they proved the following:

THEOREM 1′. *An element f in $k((x))$ is algebraic over $k(x)$ if and only if f is contained in an A-stable finite* subset *of $k((x))$.*

('A-stable' will be defined in Section 1, Definition 2.)

The second result concerns diagonal map D. Let t be an indeterminate over k. Then D is a (infinite) k-linear map from $k[[\boldsymbol{x}]]$ to $k[[t]]$ defined by

Received May 2, 1988

$$D(x_1^{n_1}, \ldots, x_m^{n_m}) = t^n \quad (\text{if } n_1 = \cdots = n_m = n) \quad \text{or } 0 \quad (\text{otherwise}).$$

The following famous theorem was proved by Furstenberg [4] in the rational case and, in general, more recently by Deligne [2]:

THEOREM 2. *If an element f in $k[[\boldsymbol{x}]]$ is algebraic over $k(\boldsymbol{x})$, then $D(f)$ is also algebraic over $k(t)$.*

The third are the problems concerning the products of Hadamard, Hurwitz and Lamperti (cf. Fliess [3], Furstenberg [4] and Section 2).

In this paper we generalize Theorem 1′ and prove:

THEOREM 0. *Let k be a perfect field of characteristic $p > 0$, and f be an element in $k((\boldsymbol{x}))$. Then f is algebraic over $k(\boldsymbol{x})$ if and only if f is contained in an A-stable finite k-vector subspace of $k((\boldsymbol{x}))$.*

This Theorem 0 is 'fundamental' for formal power series fields of characteristic $p > 0$. Using Theorem 0, we can prove all known results mentioned above, and much more. For example, we deduce Theorem 2 easily as Corollary 1 of the Theorem, and as Corollary 2 we generalize Theorem A in [4], that is, Hadamard products of algebraic elements in $k[[\boldsymbol{x}]]$ are also algebraic. Further, in Section 2 we generalize the Corollary 2 and prove that Lamperti products of algebraic elements in $k[[x]]$ are also algebraic. Though this is proved for a single invariant x, it is clear that the method of the proof is applicable for sequences of several indeterminates $\boldsymbol{x}$.

Section 1

Let k be a field of characteristic $p > 0$ and q some power of p.

NOTATION. In general we denote by $\boldsymbol{n}$ an integer vector $(n_1, \ldots, n_m)$, that is, a vector of dimension m with integer coordinates. For integer vector $\boldsymbol{n}$, $|\boldsymbol{n}|$ denotes $\max_{1 \leqq i \leqq m}(|n_i|)$. Let R be the set of integer vectors $\boldsymbol{r} = (r_1, \ldots, r_m)$ with conditions $0 \leqq r_i < q$. For integer vectors $\boldsymbol{n}$, $\boldsymbol{n}'$ we shall write $\boldsymbol{n} \leqq \boldsymbol{n}'$ if and only if we have $n_i \leqq n_i'$ for $i = 1, \ldots, m$. We denote $\boldsymbol{n} + \boldsymbol{n}'$ for $(n_1 + n_1', \ldots, n_m + n_m')$, and so for $\boldsymbol{r}$ in R, $q\boldsymbol{n} + \boldsymbol{r} = (q \cdot n_1 + r_1, \ldots, q \cdot n_m + r_m)$. For an integer vector $\boldsymbol{n}$, $a_{n_1, \ldots, n_m}$ and $x_1^{n_1} \cdots x_m^{n_m}$ will be abbreviated to $a_{\boldsymbol{n}}$ and $\boldsymbol{x}^{\boldsymbol{n}}$ respectively. For a polynomial f in $k[\boldsymbol{x}]$, $\deg(f)$ is defined to be $\max_{1 \leqq i \leqq m}(\deg_{x_i}(f))$.

Every element of $k((\boldsymbol{x}))$ is expressed (not uniquely) as a quotient f/g^q of power series f, g where

$$f = \sum_{0 \leq n} a_n x^n \qquad \text{and} \qquad g = \sum_{0 \leq n} b_n x^n.$$

Here $\mathbf{0}$ is the integer vector $(0, \ldots, 0)$, and a_n, b_n are elements of k.

We set $K = k((x)) = Q(k[[x]])$, and denote by H the algebraic closure of $k(x)$ in K. As is well known, H is the fraction field of the henselean ring $k\langle\langle x \rangle\rangle$ ($H = Q(k\langle\langle x \rangle\rangle)$ cf. [5]).

DEFINITION 1. Let k be a perfect field. For each element r in R we define A_r, the (infinite) additive endomorphism of $k[[x]]$, by

$$A_r(f) = \sum_{0 \leq n} (a_{qn+r})^{1/q} x^n.$$

A_r can be uniquely extended to the (infinite) additive endomorphism of $k((x))$ by

$$A_r(f/g^q) = (1/g)A_r(f).$$

REMARK. The endomorphisms A_r satisfy the following equalities for elements f, g in $k((x))$:

(a) $A_r(g \cdot f^q) = A_r(g) \cdot f$,

(b) $f = \Sigma_r x^r [A_r(f)]^q$.

DEFINITION 2. Let k be a perfect field. We shall say that a subset M in $k((x))$ is A-stable if, for each element r in R, M contains $A_r(f)$ with f.

'Theorem 0' in the introduction is contained in the following and this is a generalization of Theorem 1 in [1].

THEOREM 0′. *The following conditions are equivalent for a perfect field k:*

(a) *f is contained in H.*

(b) *f is contained in an A-stable $k(x)$-finite submodule M of K.*

(c) *f is contained in an A-stable k-finite subspace V of K.*

PROOF. (c)$\Rightarrow$(b): Let $f_1, \ldots, f_m$ be the basis of V. Denoting by M the $k(x)$-submodule of $k((x))$ generated by f_i, we prove that M is A-stable. Let $g = c_1 f_1 + \cdots + c_m f_m$ be an element of M. The coefficients c_i are elements of $k(x)$ and they are quotients of elements a_i, b_i in $k[x]$. For the sake of simplicity we write a, b, c, f for a_i, b_i, c_i, f_i. Then it is sufficient to prove that $A_r((a/b)f)$ is contained in M.

Let $N = \max(\deg(a), \deg(b))$; then $\deg(a \cdot b^{q-1}) \leq qN$, and we can write, with elements $a_{s,n}$ in k,

$$a \cdot b^{q-1} = \sum_{s,n}{}' a_{s,n} x^s \cdot x^{qn}$$

where the summation is over s in R and $|n| \leqq N$. Using this notation, we have

$$A_r(cf) = A_r((a/b)f) = A_r((ab^{q-1})/b^q)f)$$
$$= \sum_{s,n}{}' ((a_{s,n})^{1/q}/b)x^n A_r(x^s f).$$

Now by the following Lemma, $A_r(x^s f)) = x^e \cdot A_{s'}(f)$ $(s + s' = q \cdot e + r)$. And they are contained in M, therefore $A_r(cf)$ is contained in M.

Lemma 1. *Let s' be an element of R and n be an integer vector, then for $g = x^{qn+s'}$, $A_r(x^s g) = (d \cdot x^e) \cdot A_{s'}(g)$ where $s' + s = qe + r'$ and $d = 1$ (if $r = r'$) or 0 (otherwise).*

Proof. We have $x^s g = x^{qn+(s'+s)} = x^{q(n+e)+r'}$. If $r \neq r'$ then clearly $A_r(x^s g) = 0$, and if $r = r'$ then $A_r(x^s g) = x^{n+e} = A_{s'}(g)x^e$.

The following two arguments are dependent on [1], Sections 6, 7 but the meaning of the symbols is slightly different.

(a)⟹(c) (cf. [1], Sections 6, 7): Let f be an element of H. Then f^{q^i} $(0 \leqq i)$ generate a finite $k(x)$ submodule of $k((x))$; so f satisfies an equation

$$\sum_{i=0}^{u} a_i \cdot f^{q^i} = 0 \qquad (u \text{ a positive integer})$$

with a_i in $k[x]$.

Claim. We may assume $a_0 \neq 0$.

Proof of Claim. If $a_0 = 0$ then we have

$$\sum_{i=j}^{u} a_i \cdot f^{q^i} = 0$$

with $a_j \neq 0$. As

$$a_j = \sum_r x^r \cdot [A_r(a_j)]^q \neq 0$$

there is an element l in R such that $A_l(a_j) \neq 0$. Now

$$0 = A_l\left(\sum_{i=j}^{u} a_i \cdot f^{q^i}\right)$$

$$= \sum_{i=j}^{u} A_l(a_i) \cdot f^{q^{i-1}}.$$

By denoting $a_i' = A_l(a_{i+1})$ $(j - 1 \leqq i \leqq s - 1)$ we have

$$\sum_{i=j-1}^{u-1} a_i' \cdot f^{q^i} = 0 \qquad (a_{j-1}' \neq 0).$$

After finite repetition we get the form with $a_0 \neq 0$.

Let $g = f/a_0$, then by setting $b_i = -a_i \cdot a_0^{q^i - 2}$ it clearly follows that

$$g = \sum_{i=1}^{u} b_i g^{q^i}.$$

Let $L = \max(\deg(a_0), \deg(b_i))$ and V be the k-vector subspace of $k((x))$ spanned by $x^{\boldsymbol{s}} \cdot g^{q^i}$ with $|\boldsymbol{s}| \leqq L$ and $i \leqq u$. Then clearly V is finite, A-stable and contains f.

(b)$\Rightarrow$(a) (cf. [1], Section 6): Let M be a finite $k(\boldsymbol{x})$-submodule of K. Let M' be the $k(\boldsymbol{x})$-submodule of K generated by the q-th power of elements of M. Then clearly we have $\dim_{k(\boldsymbol{x})}(M') \leqq \dim_{k(\boldsymbol{x})}(M)$). On the other hand, for every element f in M, $A_{\boldsymbol{r}}(f)$ is contained in M. As M' contains $[A_{\boldsymbol{r}}(f)]^q$, it also contains f, because by Remark (a)

$$f = \sum_{\boldsymbol{r}} \boldsymbol{x}^{\boldsymbol{r}} [A_{\boldsymbol{r}}(f)]^q.$$

As we find that M' contains M and they have the same finite dimension, we have $M = M'$. For every element f in M, M contains f^{q^i}, so that f is algebraic over $k(\boldsymbol{x})$. q.e.d.

Let k' be a subfield of the perfect field k, and k be algebraic over k'. Then it is clear that an element f in $k'((\boldsymbol{x}))$ is algebraic over $k'(\boldsymbol{x})$ if and only if f is contained in H. So we may eliminate the perfectness assumption of k.

As previously mentioned, D denotes the diagonal map from $k((\boldsymbol{x}))$ to $k((t))$.

Corollary 1 (Theorem of Furstenberg and Deligne, cf. [2], [4]). *If an element f in $k[[\boldsymbol{x}]]$ is algebraic over $k(\boldsymbol{x})$, then $D(f)$ is algebraic over $k(t)$.*

Proof. f is contained in an A-stable finite k-subspace M in K, and $D(M)$

is also a finite k-space in $k((t))$. Setting $\boldsymbol{e}=(1,\ldots,1)$ we have $A_r(D(f))=D(A_{r\cdot\boldsymbol{e}}(f))$, so $D(M)$ is also A-stable.

Let f, g be elements in K; then $f*g$ is defined by

$$f*g=\sum_{0\leq n} a_n\cdot b_n\cdot \boldsymbol{x}^n$$

(Hadamard product, cf. Section 2) where

$$f=\sum_{0\leq n} a_n\boldsymbol{x}^n \qquad\text{and}\qquad g=\sum_{0\leq n} b_n\boldsymbol{x}^n.$$

Then we have a generalization of Theorem A in [3] as:

COROLLARY 2. *Let f, g be elements of $k[[\boldsymbol{x}]]$ and algebraic over $k(\boldsymbol{x})$. Then $f*g$ is also algebraic.*

PROOF. Let V be an A-stable finite k-subspace containing f and g. If $f_1,\ldots,f_n$ form the basis of V, then f_i*f_j generate an A-stable finite k-vector subspace which contains $f*g$.

Section 2

Let f, g be elements of $k[[x]]$. The following pairings of $k[[x]]$ are known as the Hadamard product and Hurwitz product, respectively:

$$f*g=\sum_{0\leq n} a_nb_nx^n,$$

$$f(H)g=\sum_{0\leq n}\left(\sum_{k=0}^{n} {}_nC_k a_k b_{n-k}\right)x^n,$$

where

$$f=\sum_{0\leq n} a_nx^n,\qquad g=\sum_{0\leq n} b_nx^n,$$

and

$${}_nC_k=n!/[(n-k)!\,k!].$$

Lamperti generalized those products by

$$f(L)g=\sum_{0\leq n} c_nx^n,$$

where

$$c_n=\sum_{i+j+k=n}\frac{n!}{i!\,j!\,k!}a^ib^jc^ka_{i+k}b_{j+k}$$

and a, b and c are elements in k.

The cases of Hadamard and Hurwitz are obtained from the Lamperti product, respectively, by setting $a = b = 0, c = 1$ and $a = b = 1, c = 0$. If f and g are algebraic and f or g is rational (i.e. contained in $k(x)$), then it is known that $f(L)g$ is algebraic for characteristic $p \geqq 0$ (cf. [3]).

By using Theorem 0 we prove:

COROLLARY 3. *Let k be a field of characteristic $p > 0$. If f, g are elements of $k[[x]]$ and algebraic over $k(x)$, then $f(L)g$ is also algebraic.*

PROOF. We can assume without loss of generality that k is perfect. As the pairing (L) is bilinear, it is sufficient to prove the following proposition.

PROPOSITION. *Let ${}_rC_{s,t} = (r!)/[s!\,t!\,(r-s-t)!]$. Then*

$$A_r(f(L)g) = \sum_{0 \leqq s,t \leqq s+t \leqq r} {}_rC_{s,t}\, a^{s/q} b^{t/q} c^{(r-s-t)/q} \cdot (A_{r-t}(f)(L)A_{r-s}(g)).$$

The following lemma is necessary for the proof of the Proposition.

LEMMA 2. *In the field of characteristic $p > 0$, it follows that*

$$\begin{aligned} {}_nC_{m,l} &= {}_rC_{s,t} \cdot {}_{n'}C_{m',l'} \quad (\text{if } n = qn' + r,\ m = qm' + s,\ l = ql' + t, \\ &\qquad\qquad 0 \leqq s + t \leqq r,\ 0 \leqq m' + l' \leqq n'), \\ &= 0 \qquad\qquad (\text{otherwise}). \end{aligned}$$

PROOF OF LEMMA 2. Now, ${}_nC_{m,l}$ is the coefficient of X^mY^l in the expansion of $(1 + X + Y)^{qn'+r}$. But we have in our context

$$(1 + X + Y)^{qn'+r} = (1 + X + Y)^r(1 + X^q + Y^q)^{n'}.$$

PROOF OF THE PROPOSITION. By setting $G(n; i, j) = a^ib^jc^{n-i-j}$, we have

$$\begin{aligned} f(L)g &= \sum_{i+j+k=n} \frac{n!}{i!\,j!\,k!} a^ib^jc^ka_{i+k}b_{j+k}x^n \\ &= \sum_{C(n,n-m,n-l)} {}_nC_{n-m,n-l}\, a^{n-m}b^{n-l}c^{l+m-n}a_lb_mx^n \\ &= \sum_{C(n,n-m,n-l)} {}_nC_{n-m,n-l}\, G(n; n-m, n-l)a_lb_mx^n \\ &= (*), \end{aligned}$$

where $\Sigma_{C(n,m,l)}$ denotes summation over integers with $0 \leqq l,\ m \leqq l + m \leqq n$.

By Lemma 2 and using substitutions $n = qn' + r$, $n - m = qm' + s$, $n - l = ql' + t$, $n' - m' = m''$ and $n' - l' = l''$, we have

$$(*) = \sum_{C(r,s,t)} {}_rC_{s,t} \sum_{C(n',m',l')} {}_{n'}C_{m',l'} G(qn' + r; qm' + s, ql' + t)$$

$$\cdot\, a_{q(n'-l')+(r-t)} b_{q(n'-m')+(r-s)} x^{qn'+r}$$

$$= \sum_{C(r,s,t)} {}_rC_{s,t} G(r; s, t) \sum_{C(n',n'-m'',n'-l'')} {}_{n'}C_{n'-m'',n'-l''}$$

$$\cdot\, G(n', n' - m'', n' - l'')^q a_{ql''+(r-t)} b_{qm''+(r-s)} x^{qn'+r}.$$

Now it is clear that

$$A_r(f(L)g) = \sum_{s,t} {}_rC_{s,t} G(r; s, t)^{1/q} \sum_{C(n',n'-m'',n'-l'')} {}_{n'}C_{n'-m'',n'-l''}$$

$$\cdot\, G(n', n' - m'', n' - l'')(a_{ql''+(r-t)})^{1/q}(b_{qm''+(r-s)})^{1/q} x^{n'}$$

$$= \sum_{s,t} {}_rC_{s,t} G(r; s, t)^{1/q} \cdot (A_{r-t}(f)(L)A_{r-s}(g)).$$

q.e.d.

REFERENCES

1. G. Christol, T. Kamae, M. Mendes-France et G. Rauzy, *Suites algebraiques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), 401–419.

2. P. Deligne, *Integration sur un cycle evanescent*, Invent. Math. **76** (1983), 129–143.

3. M. Fliess, *Sur divers products de series formelles*, Bull. Soc. Math. France **102** (1974), 181–191.

4. H. Furstenberg, *Algebraic functions over finite fields*, J. Algebra **7** (1967), 271–277.

5. H. Kurke, G. Pfister und M. Roczen, *Henselsche Ring und algebraische Geometrie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1975.

6. M. Mendes-France and A. J. Van der Poorten, *Automata and the arithmetic of formal power series*, Acta Arithmetica **46** (1986), 211–214.