ISRAEL JOURNAL OF MATHEMATICS, Vol. 67, No. 1, 1989

ALGEBRAIC ELEMENTS IN FORMAL POWER SERIES RINGS II

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

ABSTRACT
We obtain explicit formulae for degrees on diagonals, Hadamard products and Lamperti products.

§0. Introduction

We obtained in [6] a theorem giving a condition for algebraicity of an element in a formal power series field of positive characteristic. Prof. J.-P. Allouche and Prof. G. Christol pointed out to me the existence of the works of H. Sharif and C. Woodcock [9] and J. Denif & L. Lipshitz [3]. They use almost the same idea as we do. But we found our formulation contains some quantitative aspects. In this short note, we present by our methods the explicit formulae for degrees on diagonals and products of Hadamard and Lamperti. This seems to be an answer to the question of Sharif–Woodcock and Deligne (cf. [9] p. 402, [2] 3.7). It is remarkable that the formulae for degrees on the products of Hadamard and Lamperti are the same.

§1. In this paper we use all notations and definitions in [6] freely. But for a polynomial $a = a(\boldsymbol{x})$ in $k[\boldsymbol{x}]$ we denote size(a) for $\max_{0 \leq i \leq m}[\deg_{x_i}(a)]$. We also say an element f in $K = k((\boldsymbol{x}))$ is algebraic of degree (at most) d and size s if and only if f is a root of a non-trivial polynomial over $k[\boldsymbol{x}]$ which has degree at most d and has sizes of coefficients at most s.

Recall the following theorem in [6].

Received October 30, 1988

THEOREM 0′. *The following conditions are equivalent for a perfect field* k:
(a) f *is contained in* H *(i.e. algebraic over* $k(\boldsymbol{x})$*).*
(b) f *is contained in an* A*-stable* $k(\boldsymbol{x})$*-finite submodule* M *of* K.
(c) f *is contained in an* A*-stable* k*-finite subspace* V *of* K.

And we recall also the following remarks from the proof of the theorem:
(1) $\dim_k(V) \geqq \dim_{k(\boldsymbol{x})}(M)$,
(2) M contains all q^i-th powers of f,
(3) if f satisfies a non-trivial equation

$$a_d f^{q^d} + a_{d-1} f^{q^{d-1}} + \cdots + a_0 f = 0$$

with coefficients a_i in $k[\boldsymbol{x}]$ and $\operatorname{size}(a_i) \leqq c$, then $\dim_k(V) \leqq d \cdot ((q^{d-2} + 1)c + 1)^m$.

The following elementary lemma is useful.

LEMMA. *If* f *is an algebraic element in* $k((\boldsymbol{x}))$ *with degree* d *and size* s, *then* f *satisfies the following non-trivial equation over* $k[\boldsymbol{x}]$:

$$(*) \qquad c_d f^{q^d} + c_{d-1} f^{q^{d-1}} + \cdots + c_0 f = 0, \qquad \operatorname{size}(c_j) \leqq c,$$

where, denoting w *the smallest integer with* $q^w \geqq d$,

$$c = s[(q^{d+1} - 1)/(q-1) - q^{-w}(d^2 - 1)].$$

PROOF OF LEMMA. Let $G(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0$ be the non-trivial polynomial of f in $k[\boldsymbol{x}][X]$ with $\operatorname{size}(a_i) \leqq s$. Let

$$H(X) = b_e X^e + b_{e-1} X^{e-1} + \cdots + b_0$$

with $e \geqq d$ and $\operatorname{size}(b_j) \leqq z$. Then we have with coefficients in $k[\boldsymbol{x}]$,

$$a_d H(f) = a_d(b_e f^e + b_{e-1} f^{e-1} + \cdots + b_0) - b_e f^{e-d}(a_d f^d + \cdots + a_0)$$
$$= b_{e-1}^{(1)} f^{e-1} + b_{e-2}^{(1)} f^{e-2} + \cdots + b_0^{(1)},$$
$$\operatorname{size}(b_i^{(1)}) \leqq s + z,$$
$$a_d^2 H(f) = a_d(b_{e-1}^{(1)} f^{e-1} + b_{e-2}^{(1)} f^{e-2} + \cdots + b_0^{(1)})$$
$$- b_{e-1}^{(1)} f^{e-d-1}(a_d f^d + \cdots + a_0)$$
$$= b_{e-2}^{(2)} f^{e-2} + \cdots + b_0^{(2)},$$
$$\operatorname{size}(b_i^{(2)}) \leqq 2s + z,$$

and in general

$$a_d^v H(f) = b_{e-v}^{(v)} f^{e-v} + b_{e-v-1}^{(v)} f^{e-v-1} + \cdots + b_0^{(v)},$$

$$\mathrm{size}(b_i^{(v)}) \leqq vs + z.$$

Finally we have for $v = e - d + 1$

$$a_d^{e-d+1} H(f) = b_{d-1}^{(e-d+1)} f^{d-1} + \cdots + b_0^{(e-d+1)},$$

$$\mathrm{size}(b_i^{(e-d+1)}) \leqq (e - d + 1)s + z.$$

For the above-mentioned w and for $u = 0, \ldots, d$ considering $H(f) = f^{q^{u+w}}$, we obtain the following $d + 1$ equations:

$$a_d^{q^{u+w}} f^{q^{u+w}} = c_{d-1} f^{d-1} + \cdots + c_0^{(u)}, \qquad \mathrm{size}(c_j^{(u)}) \leqq s(q^{u+w} - d + 1).$$

By eliminating $f^{d-1}, \ldots, f, 1$ from the $d + 1$ equations we obtain the non-trivial equation

$$c_d f^{q^{d+w}} + c_{d-1} f^{q^{d-1+w}} + \cdots + c_0 f^{q^w} = 0.$$

Here

$$\mathrm{size}(c_i) \leqq \sum_{u=0}^{d} (q^{u+w} - d + 1)s = sq^w(1 - q^{d+1})/(1 - q) - s(d^2 - 1).$$

But after some w-times of successive applications of A_r, the equation takes on the form (*) of the lemma with

$$\mathrm{size}(c_i) \leqq c = s(1 - q^{d+1})/(1 - q) - sq^{-w}(d^2 - 1). \qquad \text{q.e.d.}$$

§2. In this section we take $q = p$. The following is the main result of this paper, and the quantitative version of Corollaries 1, 2 and 3 in [6].

THEOREM. *Let f and g be elements in $k[[\mathbf{x}]] = k[[x_1, \ldots, x_m]]$.*

(a) *If f is an algebraic element in $k((\mathbf{x}))$ of degree d and size s, then the diagonal $D(f)$ is algebraic of degree at most*

$$\exp[\log(p)\cdot d(s(p^{d-2} + 1)(p^{d+1} - 1)/(p - 1) - s(p^{d-2} + 1)p^{-w}(d^2 - 1) + 1)^m]$$

where w is the smallest integer with $p^w \geqq d$.

(b) *If f (resp. g) is algebraic of degree d_1 (resp. d_2) and size s_1 (resp. s_2) then the Hadamard product $f * g$ is algebraic of degree at most*

$$\exp[\log(p)\cdot d_1 d_2 (s_1(p^{d_1-2} + 1)(p^{d_1+1} - 1)/(p - 1) - s_1(p^{d_1-2} + 1)p^{-w_1}(d_1^2 - 1) + 1)^m$$

$$\cdot (s_2(p^{d_2-2} + 1)(p^{d_2+1} - 1)/(p - 1) - s_2(p^{d_2+2} + 1)p^{-w_2}(d_2^2 - 1) + 1)^m],$$

where, for $i = 1, 2$, w_i is the smallest integer with $p^{w_i} \geqq d_i$.

(c) *For $m = 1$ and with the same assumption as in* (b), *the Lamperti product $f(L)g$ is algebraic of degree at most*

$$\exp[\log(p)\cdot d_1 d_2 (s_1(p^{d_1-2}+1)(p^{d_1+1}-1)/(p-1) - s_1(p^{d_1-2}+1)p^{-w_1}(d_2^2-1)+1)$$
$$\cdot(s_2(p^{d_2-2}+1)(p^{d_2+1}-1)/(p-1) - s_2(p^{d_2-2}+1)p^{-w_2}(d_2^2-1)+1)],$$

where, for $i = 1, 2$, w_i is the smallest integer with $p^{w_i} \geqq d_i$.

PROOF OF THE THEOREM. (a) *Diagonal case*. Let f be an algebraic element in $k((\boldsymbol{x}))$ with degree d and size s. Then by the lemma and (3), f satisfies the equality (*) and f is contained in an A-stable finite k-space V of $\dim_k(V) \leqq e = d((p^{d-2}+1)c+1)^m$. So diagonal $g = D(f)$ is contained in the A-stable k-space $D(V)$ of dimension at most e. By (1), (2) $D(f)$ is algebraic of degree at most p^e.

(b) *Hadamard product*. Let f (resp. g) be an algebraic element in $k((\boldsymbol{x}))$ with degree d_1 (resp. d_2) and size s_1 (resp. s_2). Then f (resp. g) is contained in an A-stable k-space V_1 (resp. V_2) of dimension at most

$$e_1 = d_1((p^{d_1-2}+1)c_1+1)^m \qquad (\text{resp. } e_2 = d_2((p^{d_2-2}+1)c_2+1)^m.$$

Let $f_1, \ldots, f_{n_1}$ ($n_1 \leqq e_1$) (resp. $g_1, \ldots, g_{n_2}$ ($n_2 \leqq e_2$)) be basis of V_1 (resp. V_2). Then, it was proved in [6] that $f_i * g_j$ span A-stable k-space which contains $f*g$ and has dimension at most $e_1 e_2$. By (1), (2) the degree of $f*g$ is at most $p^{e_1 e_2}$.

(c) *Lamperti product*. Though the product of Lamperti can be generalized by an obvious way to several indeterminates, the formulation is rather complicated. So we consider here the case of a single indeterminate (cf. [6] Corollary 3). Let f (resp. g) be an algebraic element in $k(x)$ with degree d_1 (resp. d_2) and size s_1 (resp. s_2), then $f(L)g$ is contained in an A-stable k-space of degree at most $e_1 e_2$. By (1), (2) we deduce that the degree of $f(L)g$ is less than $p^{e_1 e_2}$.

Here for $i = 1.2$

$$e_i = d_i((p^{d_i-2}+1)c_i+1), \qquad c_i = s_i[(p^{d_i+1}-1)/(p-1) - p^{-w_i}(d_i^2-1)],$$

and w_i is the smallest integer with $p^{w_i} \geqq d_i$. q.e.d.

REFERENCES

1. G. Christol, T. Kamae, M. Mendes-France et G. Rauzy, *Suites algébraiques, 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. J. Denef and L. Lipshitz, *Algebraic power series and diagonals*, J. Number Theory **26** (1987), 46–67.

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

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

6. T. Harase, *Algebraic elements in formal power series rings*, Isr. J. Math., **63** (1988), 281–288.

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

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

9. H. Sharif and C. Woodcock, *Algebraic functions over a field of positive characteristic and Hadamard products*, J. London Math. Soc. (2) **37** (1988), 395–403.