JOURNAL OF NUMBER THEORY **26**, 46–67 (1987)

Algebraic Power Series and Diagonals

J. DENEF

University of Leuven, Celestijnenlaan 200, B-3030 Heverlee, Belgium

AND

L. LIPSHITZ*

Purdue University, West Lafayette, Indiana 47907

Communicated by D. J. Lewis

Received September 4, 1985

We extend some results of Christol and Furstenberg to the case of several variables: (1) A power series in several variables over the p-adic integers $\mathbb{Z}_p$ is congruent mod p^s to an algebraic power series if and only if its coefficients satisfy certain congruences mod p^s. (2) Any algebraic power series in m variables over a field K can be written as the diagonal of a rational power series in $2m$ variables. We also give an elementary proof of a result of Deligne: The diagonal of an algebraic power series in several variables, over a field of nonzero characteristic is algebraic. Moreover we show that the diagonal of an algebraic power series over $\mathbb{Z}_p$ is algebraic mod p^s, for every s. We also obtain other related results. © 1987 Academic Press, Inc.

1. INTRODUCTION

We prove several results about algebraic power series and diagonals of algebraic power series. If R is an integral domain, then $R[[x]]$ denotes the ring of formal power series in the variables $x = (x_1, ..., x_m)$ over R. We call a power series $y(x) \in R[[x]]$ algebraic if it is algebraic over $R[x]$. Section 2 contains a lemma that we use repeatedly in the rest of the paper. In Section 3 we prove the following (Theorem 3.1):

If $y(x) = \sum a_v x^v$ is an algebraic power series $(x = (x_1, ..., x_m)$, $v = (v_1, ..., v_m))$ with the $a_v \in \mathbb{Z}_p$, the p-adic integers, then for any $s > 0$ there

* The friendly hospitality and support of the University of Leuven and the support of the N.S.F. are gratefully acknowledged.

0022-314X/87 $3.00

is an $e \in \mathbb{N}$ such that for each $i = (i_1, ..., i_m)$, with $0 \leqslant i_j < p^e$, there is an $e' < e$ and an $i' = (i'_1, ..., i'_m)$, with $0 \leqslant i'_j < p^{e'}$, such that for all v

$$a_{p^e v + i} \equiv a_{p^{e'} v + i'} \bmod p^s.$$

(Here $p^e v + i = (p^e v_1 + i_1, ..., p^e v_m + i_m)$.) Conversely if the $a_v \in \mathbb{Z}_p$ satisfy such a set of congruences then there is an algebraic power series $y = \sum \tilde{a}_v x^v \in \mathbb{Z}_p[[x]]$ with $\tilde{a}_v \equiv a_v$ modulo p^s. The case $s = 1$ of this theorem is contained in Christol, Kamae, Mendes-France, and Rauzy [C-K], and the case $m = 1$ is proved in Christol [Ch1] by somewhat different methods (see Remark 6.6). Recently Christol [Ch2] has extended the case $m = 1$ to nondiscrete valuation rings. In [C-K] the theorem is proved that if F is a finite field then $y(x_1) = \sum a_n x_1^n \in F[[x_1]]$ is algebraic if and only if the function $n \mapsto a_n$ can be computed by a finite machine. The generalization of this theorem to power series modulo p^s is immediate from Theorem 3.1 by using the method of [C-K]. For the sake of completeness we provide details in Section 4. If $y(x) = \sum a_{v_1 \cdots v_m} x_1^{v_1} \cdots x_m^{v_m}$ then the diagonal $I_{x_1 x_2}(y)$ is defined by $I_{x_1 x_2}(y) = \sum a_{v_1 v_1 v_3 \cdots v_m} x_1^{v_1} x_3^{v_3} \cdots x_m^{v_m}$. We define the other diagonals $I_{x_i x_j}$ similarly. By a diagonal we mean any composition of these diagonals. In Furstenberg [Fu] it is shown that (a) if $y(x)$ is a rational function $\in F[[x]]$, where F is a field of characteristic $p \neq 0$, then any diagonal of y is an algebraic function and (b) if $y(x_1)$ is an algebraic function in $K[[x_1]]$ (K any field) then there is a rational function $R(x_1, x_2) \in K[[x_1, x_2]]$ such that $y(x_1) = I_{x_1 x_2}(R)$. In Deligne [D1] it is shown that (c) if F is a field of characteristic $p \neq 0$ and $y(x_1, ..., x_m) \in F[[x_1, ..., x_m]]$ is algebraic then any diagonal of y is also algebraic, and (d) if $y \in \mathbb{Z}[[x_1, ..., x_m]]$ is algebraic then for almost all p, and for all s, the diagonal of y modulo p^s is algebraic. In Section 5 we reprove (c) and also show that if R is a complete discrete valuation ring with uniformizing parameter π and residue class field of characteristic $p \neq 0$, and if $y \in R[[x_1, ..., x_m]]$ is algebraic, then for any diagonal $I(y)$ and any $s \in \mathbb{N}$ there is an algebraic power series $\tilde{y} \in R[[x_1, ..., x_m]]$ such that $I(y) \equiv \tilde{y}$ modulo π^s. In Section 6 we extend (b) to the case of algebraic power series in several variables over a local Noetherian integral domain A which is not pathological: If $y(x_1, ..., x_m) \in A[[x_1, ..., x_m]]$ is algebraic, then there is a rational power series R of $2m$ variables so that y is a diagonal of R. We also give an application of this theorem (Remark 6.6). In Section 7 we show that power series $\sum a_n x_1^n \in \mathbb{Z}_p[[x_1]]$ with the a_n defined by a recursion of the form $a_n = F(n)\, a_{n-1}$, where $F(n)$ is a rational function over $\mathbb{Q}$ all of whose zeros and poles belong to $\mathbb{Q}$, are algebraic modulo p^s for all s.

We would like to thank B. Dwork for stimulating conversations, G. Christol for sending us valuable information and L. Van Hamme for bringing reference [C-K] to our attention.

2. A Useful Lemma

First we introduce some notation. F is a perfect field of characteristic $p \neq 0$; $x = (x_1, \ldots, x_m)$ and $F[[x]]$ is the ring of formal power series in $x_1, \ldots, x_m$ over F. Let $S = \{\alpha = (\alpha(1), \ldots, \alpha(m)) \colon 0 \leqslant \alpha(i) < p \text{ for } i = 1, \ldots, m\}$. We shall denote elements of S by the letters α, β, or γ, sometimes with subscripts. Note that for any $y \in F[[x]]$ there exist unique $y_\alpha(x) \in F[[x]]$ for $\alpha \in S$ such that $y(x) = \sum_{\alpha \in S} x^\alpha y_\alpha^p(x)$. (Here $x^\alpha = x_1^{\alpha(1)} \cdots x_m^{\alpha(m)}$,) We can iterate this so that $y(x) = \sum_{\alpha, \beta \in S} x^{\alpha + p\beta} y_{\alpha\beta}^{p^2}(x)$ and so on, where $p\beta = (p\beta(1), \ldots, p\beta(m))$. If $y(x) = \sum_\nu a_\nu x^\nu$ where $\nu = (\nu_1, \ldots, \nu_m)$ is a multi-index then $y_\alpha(x) = \sum_\nu a_{p\nu + \alpha}^{1/p} x^\nu$, where $p\nu + \alpha = (p\nu_1 + \alpha(1), \ldots, p\nu_m + \alpha(m))$. $y_{\alpha\beta}(x) = \sum_\nu a_{p^2\nu + \alpha + p\beta}^{1/p^2} x^\nu$ and so on. If F is the p element field then we have $y_\alpha(x) = \sum_\nu a_{p\nu + \alpha} x^\nu$ and so on. Suppose now that $y(x) \in F[[x]]$ is algebraic (i.e., is algebraic over $F[x]$). Then $y(x)$ satisfies an equation of the form $\sum_{i=r}^s g_i(x)\, y^{p^i} = 0$ with the $g_i(x) \in F[x]$ and $g_r(x) \neq 0$. (Because $F(x)(y)$ is a finite dimensional vector space over $F(x)$.) We claim that we can always take $r = 0$. Indeed, suppose $r > 0$: Since F is perfect we can write $g_i(x) = \sum_{\alpha \in S} g_{i\alpha}^p(x)\, x^\alpha$. Hence we have $\sum_{\alpha \in S} \sum_{i=r}^s (g_{i\alpha}^p\, y^{p^i})\, x^\alpha = 0$ which is equivalent to the p^m equations $\sum_{i=r}^s g_{i\alpha}\, y^{p^{i-1}} = 0$. For at least one α we have that $g_{r\alpha} \neq 0$ and hence y satisfies an equation of the above form with r replaced by $r - 1$. Hence we have that if $y(x)$ is algebraic then it satisfies an equation of the form

$$f(x)\, y = \sum_{i=1}^{s} f_i(x)\, y^{p^i} = L(y^p, \ldots, y^{p^s}) \tag{1}$$

where $f(x) \neq 0$ and L is linear over $F[x]$. In the rest of the paper we shall make repeated use of the following Lemma. Part (ii) in the case $m = 1$, occurs in [C-K].

2.1. Lemma. (i) *Let $y(x) \in F[[x]]$ be algebraic. Then for e large enough we have that for every $(\alpha_1, \ldots, \alpha_e) \in S^e$ there is an F linear combination $M_{\alpha_1 \cdots \alpha_e}(\ldots, y_{\beta_1 \cdots \beta_{e'}}, \ldots)$ of the $y_{\beta_1 \cdots \beta_{e'}}$ with $e' < e$ such that*

$$y_{\alpha_1 \cdots \alpha_e} = M_{\alpha_1 \cdots \alpha_e}(\ldots, y_{\beta_1 \cdots \beta_{e'}}, \ldots).$$

(ii) *If, in addition, F is a finite field then we have that for e large enough and each $(\alpha_1, \ldots, \alpha_e) \in S^e$ there is an $e' < e$ and $(\beta_1, \ldots, \beta_{e'}) \in S^{e'}$ such that*

$$y_{\alpha_1 \cdots \alpha_e} = y_{\beta_1 \cdots \beta_{e'}}.$$

Proof. y satisfies an equation of the form (1) above. Letting $y = \sum_{\alpha \in S} y_\alpha^p x^\alpha$ and substituting into (1) we get

$$\sum_{\alpha \in S} f(x)\, y_\alpha^p x^\alpha = L(y^p, \ldots, y^{p^s}). \tag{2}$$

Multiply (2) by f^{p-1} and express $f^{p-1}(x)\,L$ in the p-basis $\{x^\alpha\}$ to get

$$\sum_{\alpha\in S} f^p(x)\,y_\alpha^p x^\alpha = f^{p-1}(x)\,L(y^p,\ldots,y^{p^s}) = \sum_{\alpha\in S} L_\alpha^p(y,\ldots,y^{p^{s-1}})\,x^\alpha. \tag{3}$$

Hence we have the p^m equations

$$f(x)\,y_\alpha = L_\alpha(y,\ldots,y^{p^{s-1}}). \tag{4}$$

Suppose now that $\deg_x(f)=N$ and $\deg_x(L)=K$ where "$\deg_x$" means the total degree in x. Then

$$\deg_x(f^{p-1}(x)\,L(y^p,\ldots,y^{p^s})) = K+(p-1)\,N$$

and

$$\deg_x(L_\alpha) \leqslant \frac{K+(p-1)\,N}{p}.$$

Multiply (4) by $f^{p-1}(x)$ and substitute from (1) for $f(x)\,y$ to get

$$\begin{aligned} f^p(x)\,y_\alpha &= f^{p-2}(x)\,L_\alpha(f(x)\,y, f(x)\,y^p,\ldots) \\ &= f^{p-2}(x)\,L_\alpha(L(y^p,\ldots,y^{p^s}), f(x)\,y^p,\ldots). \end{aligned} \tag{5}$$

Set $y_\alpha = \sum_\beta y_{\alpha\beta}^p x^\beta$, where $\beta=(\beta_1,\ldots,\beta_m)$ with $0\leqslant\beta_i<p$, substitute into (5) and write the new equation in the p-basis $\{x^\beta\}$ to get

$$\sum_\beta (f^p(x)\,y_{\alpha\beta}^p)\,x^\beta = \sum_\beta (L_{\alpha\beta}(y,\ldots,y^{p^{s-1}}))^p\,x^\beta. \tag{6}$$

Equating the coefficients of x^β and taking pth roots we have

$$f(x)\,y_{\alpha\beta} = L_{\alpha\beta}(y,\ldots,y^{p^{s-1}}). \tag{7}$$

The $\deg_x$ of the right-hand side of (5) is $\leqslant(A/p)+A$ where $A=(p-1)\,N+K$, so $\deg_x(L_{\alpha\beta})\leqslant(A/p^2)+(A/p)$. Iterating this procedure we get that

$$f(x)\,y_{\alpha\beta\gamma\cdots} = L_{\alpha\beta\gamma\cdots}(y,\ldots,y^{p^{s-1}}), \tag{8}$$

where $\deg_x(L_{\alpha\beta\gamma\cdots})\leqslant(A/p)+(A/p^2)+(A/p^3)+\cdots=A/(p-1)$. Note that $L_{\alpha\beta\gamma\cdots}$ is linear in y, $y^p,\ldots,y^{p^{s-1}}$, with degree in x bounded by $A/(p-1)$. These polynomials lie in a finite dimensional vector space over F. Hence for e large enough we have that

$$y_{\alpha_1\alpha_2\cdots\alpha_e} = M_{\alpha_1\cdots\alpha_e}(\ldots,y_{\beta_1\cdots\beta_{e'}},\ldots),$$

where $M_{\alpha_1 \cdots \alpha_e}$ is an F linear combination of the $y_{\beta_1 \cdots \beta_{e'}}$, for $e' < e$. In the case that F is a finite field the set of all possible $L_{\alpha\beta\gamma\cdots}(y, y^p, ..., y^{p^{s-1}})$ is finite and so (ii) follows. Q.E.D.

2.2. *Remark.* Note that if $e' < e$ then each $y_{\beta_1 \cdots \beta_e}$ is an $F[x]$ linear combination of the $y^{p^{e-e'}}_{\beta_1 \cdots \beta_{e'}}$, and that the coefficient of $y^{p^{e-e'}}_{\beta_1 \cdots \beta_{e'}}$ is a polynomial in x of degree less than $p^{e-e'}$. Hence it follows that for e large enough the $y_{\alpha_1 \cdots \alpha_e}$ satisfy a system of equations of the form

$$y_{\alpha_1 \cdots \alpha_e} = \tilde{L}_{\alpha_1 \cdots \alpha_e}(..., y^p_{\beta_1 \cdots \beta_e}, y^{p^2}_{\beta_1 \cdots \beta_e}, ...), \tag{9}$$

i.e., each $y_{\alpha_1 \cdots \alpha_e}$ is an $F[x]$ linear combination of the $y^p_{\beta_1 \cdots \beta_e}$, $y^{p^2}_{\beta_1 \cdots \beta_e}, ...,$ $y^{p^e}_{\beta_1 \cdots \beta_e}$, and the coefficient of $y^{p^i}_{\beta_1 \cdots \beta_e}$ is of degree less than p^i. The Jacobian of this system of equations (in the unknowns $y_{\alpha_1 \cdots \alpha_e}$) is 1. Hence the $y_{\alpha_1 \cdots \alpha_e}$ are all algebraic. (see, e.g., [La, p. 268]). Further it follows that if R is a complete discrete valuation ring with prime $\mathfrak{p}$ such that $R/\mathfrak{p} = F$ then there are $\bar{y}_{\alpha_1 \cdots \alpha_e}(x) \in R[[x]]$, all algebraic, such that $\bar{y}_{\alpha_1 \cdots \alpha_e} \equiv y_{\alpha_1 \cdots \alpha_e}$ modulo $\mathfrak{p}$. This is merely a variant of Hensel's Lemma. For the sake of completeness we include a proof. We must show that if we have a system of equations

$$f_i(Y_1, ..., Y_k) = 0, \qquad i = 1, ..., k$$

with the $f_i \in R[[x]][Y_1, ..., Y_k]$ and a $\bar{y} = (\bar{y}_1, ..., \bar{y}_k) \in R[[x]]^k$ such that

$$f_i(\bar{y}) \equiv 0 \mod \mathfrak{p}R[[x]]$$

and

$$\det\left(\frac{\partial f_i}{\partial y_j}\right)(\bar{y}) \equiv 1 \mod \mathfrak{p}R[[x]]$$

then there is a $\tilde{y} \in R[[x]]^k$ satisfying $f_i(\tilde{y}) = 0$ and $y_i \equiv \tilde{y}_i \mod \mathfrak{p}R[[x]]$ for $i = 1, ..., k$. It is sufficient to show that there exist $\bar{z}_i \in R[[x]]^k$ such that if $y = \bar{y} + \sum_{i=1}^n \mathfrak{p}^i \bar{z}_i$ then $f_i(y) \equiv 0 \mod \mathfrak{p}^{n+1}$. Suppose that $\bar{z}_1, ..., \bar{z}_n$ have been shown to exist. Let $\bar{\bar{y}} = \bar{y} + \sum_{i=1}^n \mathfrak{p}^i \bar{z}_i$ and let $y = \bar{\bar{y}} + \mathfrak{p}^{n+1} z$. Then, writing f for $(f_1, ..., f_k)$, we have by Taylor's Theorem that $f(y) = f(\bar{\bar{y}} + \mathfrak{p}^{n+1} z) = f(\bar{\bar{y}}) + (\partial f/\partial y)(\bar{\bar{y}})\, \mathfrak{p}^{n+1} z + \mathfrak{p}^{2n+2} H(z)$ where $(\partial f/\partial y) = (\partial f_i/\partial y_j)_{i,j=1,...,k}$ and $H(z)$ has entries from $R[[x]][z]$. Now $f(\bar{\bar{y}}) = \mathfrak{p}^{n+1} L$ for some vector L with entries from $R[[x]]$. Hence we must see that z can be chosen so that $\mathfrak{p}^{n+1} L + \mathfrak{p}^{n+1} (\partial f/\partial y)(\bar{\bar{y}})\, z \equiv 0 \mod \mathfrak{p}^{n+2}$, i.e., that there is a z such that $L + (\partial f/\partial y)(\bar{\bar{y}})\, z \equiv 0 \mod \mathfrak{p}$. Since $\det(\partial f/\partial y)(\bar{\bar{y}}) \equiv 1 \mod \mathfrak{p}$ there is a matrix A with entries from $R[[x]]$ such that $A(\partial f/\partial y)(\bar{\bar{y}}) = I$, the identity matrix, and hence we can choose $\bar{z}_{n+1} = -AL$.

3. Algebraic Power Series mod p^s

The main result of this section is

3.1. Theorem. (i) *Let $f(x)=\sum_\nu a_\nu x^\nu \in \mathbb{Z}_p[[x]]$, $x=(x_1,\ldots,x_m)$, be algebraic. Let $s\in\mathbb{N}_0$. Then there exists an $e\in\mathbb{N}_0$ such that for all $j<p^e$, there exist $e'<e$ and $j'<p^{e'}$ such that*

$$a_{p^e\nu+j}\equiv a_{p^{e'}\nu+j'} \mod p^s, \tag{1}$$

for all ν. Here ν, j, j' are multi-indices $\in\mathbb{N}^m$, and e, $e'\in\mathbb{N}$. By $j=(j_1,\ldots,j_m)<p^e$ we mean $j_1<p^e,\ldots,j_m<p^e$, etc.

(ii) *The converse is also true: Let $f(x)=\sum_\nu a_\nu x^n\in\mathbb{Z}_p[[x]]$, and let $s\in\mathbb{N}_0$. Suppose that there exists an $e\in\mathbb{N}_0$ such that for all $j<p^e$, there exist $e'<e$ and $j'<p^{e'}$ satisfying* (1). *Then there exists an algebraic $g(x)\in\mathbb{Z}_p[[x]]$ such that $f(x)\equiv g(x)$ mod p^s.*

Remark. The case $s=1$ is contained in [C-K]. The case $m=1$ is proved in [Ch1] and [Ch2]. To prove 3.1(i) we shall first prove 3.1(ii). First we introduce some more notation.

3.2. *Notation.* Let K be any field and $f(x)\in K[[x]]$. Let $\alpha_1,\ldots,\alpha_e\in S$, with S as in Section 2. We define $\hat{f}_{\alpha_1\cdots\alpha_e}(x)\in K[[x]]$ by

$$f(x)=\sum_{\alpha_1,\ldots,\alpha_e\in S} x^{\alpha_1+p\alpha_2+\cdots+p^{e-1}\alpha_e}\hat{f}_{\alpha_1\cdots\alpha_e}(x^{p^e}).$$

If K is the p element field F_p, then $\hat{f}_{\alpha_1\cdots\alpha_e}(x)=f_{\alpha_1\cdots\alpha_e}$, where $f_{\alpha_1\cdots\alpha_e}$ is as defined in Section 2.

Note that the νth coefficient of $\hat{f}_{\alpha_1\cdots\alpha_e}(x)$ is equal to the

$$(p^e\nu+\alpha_1+\alpha_2 p+\cdots+\alpha_e p^{e-1})\text{th} \tag{1}$$

coefficient of $f(x)$.

Proof of Theorem 3.1(ii). From 3.1(1) and 3.2(1) it follows that for all $\alpha_1,\ldots,\alpha_e\in S$ there exist $e'<e$ and $\alpha'_1,\ldots,\alpha'_{e'}\in S$ such that

$$\hat{f}_{\alpha_1\cdots\alpha_e}(x)\equiv\hat{f}_{\alpha'_1\cdots\alpha'_{e'}}(x) \qquad \mod p^s,$$

and hence

$$\hat{f}_{\alpha_1\cdots\alpha_e}(x)\equiv L(\ldots,\hat{f}_{\beta_1\cdots\beta_e}(x^{p^{e-e'}}),\ldots) \mod p^s, \tag{1}$$

where L is a linear polynomial without constant term (depending on

$\alpha_1, \ldots, \alpha_e)$ over $\mathbb{Z}[x]$, and where the $\beta_1, \ldots, \beta_e$ run over all elements of S. If $s = 1$, then (1) is equivalent to

$$\hat{f}_{\alpha_1 \cdots \alpha_e}(x) \equiv L(\ldots, (\hat{f}_{\beta_1 \cdots \beta_e}(x))^{p^{e'-e}}, \ldots) \quad \bmod p. \tag{2}$$

Since the Jacobian of the system (2) is congruent to 1 mod p, it follows that the $\hat{f}_{\alpha_1 \cdots \alpha_e}$, (and hence also f), are algebraic mod p, and can be lifted to an algebraic power series over $\mathbb{Z}_p$ (see Remark 2.2). We will prove by induction on s that the $\hat{f}_{\alpha_1 \cdots \alpha_e}$ (and hence also f), are the reductions mod p^s of algebraic power series $g^{(\alpha_1 \cdots \alpha_e)}(x) \in \mathbb{Z}_p[[x]]$. Let $s > 1$. By the induction hypothesis there exist algebraic power series $h^{(\alpha_1 \cdots \alpha_e)}(x) \in \mathbb{Z}_p[[x]]$ such that

$$\hat{f}_{\alpha_1 \cdots \alpha_e}(x) \equiv h^{(\alpha_1 \cdots \alpha_e)}(x) \quad \bmod p^{s-1}$$

Set

$$\hat{f}_{\alpha_1 \cdots \alpha_e}(x) = h^{(\alpha_1 \cdots \alpha_e)}(x) + p^{s-1} \Delta^{(\alpha_1 \cdots \alpha_e)}(x).$$

From (1) it follows that

$$\Delta^{(\alpha_1 \cdots \alpha_e)}(x) \equiv L(\ldots, \Delta^{(\beta_1 \cdots \beta_e)}(x^{p^{e-e'}}), \ldots) + R^{(\alpha_1 \cdots \alpha_e)}(x) \qquad \bmod p,$$

and hence

$$\Delta^{(\alpha_1 \cdots \alpha_e)}(x) \equiv L(\ldots, (\Delta^{(\beta_1 \cdots \beta_e)}(x))^{p^{e-e'}}, \ldots) + R^{(\alpha_1 \cdots \alpha_e)}(x) \quad \bmod p, \tag{3}$$

where

$$R^{(\alpha_1 \cdots \alpha_e)}(x) = p^{-s+1}[-h^{(\alpha_1 \cdots \alpha_e)}(x) + L(\ldots, h^{(\beta_1 \cdots \beta_e)}(x^{p^{e-e'}}), \ldots)].$$

Note that $R^{(\alpha_1 \cdots \alpha_e)}(x) \in \mathbb{Z}_p[[x]]$ is algebraic. The system (3), in the unknowns $\Delta^{(\alpha_1 \cdots \alpha_e)}(x)$, has Jacobian congruent to 1 mod p. Thus Hensel's Lemma implies that there exist algebraic power series $\tilde{\Delta}^{(\alpha_1 \cdots \alpha_e)}(x) \in \mathbb{Z}_p[[x]]$ such that

$$\tilde{\Delta}^{(\alpha_1 \cdots \alpha_e)}(x) \equiv \Delta^{(\alpha_1 \cdots \alpha_e)}(x) \quad \bmod p.$$

The Theorem 3.1(ii) now follows from

$$\hat{f}_{\alpha_1 \cdots \alpha_e}(x) \equiv h^{(\alpha_1 \cdots \alpha_e)}(x) + p^{s-1} \tilde{\Delta}^{(\alpha_1 \cdots \alpha_e)}(x) \quad \bmod p^s. \qquad \text{Q.E.D.}$$

Next we turn to the proof of 3.1(i), but first we need some notation and some lemmas.

3.3. *Notation.* If $a\in\mathbb{Z}$, then $\bar{a}\in F_p$ denotes the residue class of a mod p. Let θ be the map $F_p\to\mathbb{Z}_p\colon \bar{i}\mapsto i$ for $i=0, 1,\dots, p-1$. This map induces (coefficientwise) a map $\theta\colon F_p[[x]]\to\mathbb{Z}_p[[x]]$. Let $\sum_\nu a_\nu x^\nu\in\mathbb{Z}_p[[x]]$. The ith p-adic digit of a_ν will be denoted by $a_\nu(i)$. Thus $a_\nu(i)\in\{0, 1,\dots, p-1\}$ and $a_\nu=\sum_{i=0}^{\infty} a_\nu(i)\, p^i$.

3.4. Lemma. *Let $f(x)\in F_p[[x]]$ be algebraic. Let $s\in\mathbb{N}_0$. Then there exists an algebraic power series $g(x)\in\mathbb{Z}_p[[x]]$ such that*

$$\theta(f(x))\equiv g(x)\quad \bmod p^s.$$

Proof. Let $f(x)=\sum_\nu c_\nu x^\nu$, with $c_\nu\in F_p$. From Lemma 2.1(ii) it follows (see 3.2(1)) that there exists an $e\in\mathbb{N}_0$ such that for every $j<p^e$ there exist an $e'<e$ and $j'<p^{e'}$ such that

$$c_{\nu p^e+j}=c_{\nu p^{e'}+j'},$$

for all $\nu\in\mathbb{N}^m$. But this also implies that

$$\theta(c_{\nu p^e+j})=\theta(c_{\nu p^{e'}+j'}).$$

The lemma follows now by applying 3.1(ii) to $\sum_\nu \theta(c_\nu)\, x^\nu$. Q.E.D.

Remark. In general $\theta(f(x))$ is not algebraic. For example, $f(x)=\sum x^{p^n}\in F_p[[x]]$ is algebraic but $\theta(f(x))$ is not algebraic since every algebraic function satisfies a homogeneous, linear differential equation, and hence, if it is not a polynomial, there is a bound on the number of successive Taylor coefficients which can be all zero.

3.5. Proposition. *Let $\sum_\nu a_\nu x^\nu\in\mathbb{Z}_p[[x]]$ be algebraic. Let $i\in\mathbb{N}$. Then $\sum_\nu \overline{a_\nu(i)}\, x^\nu\in F_p[[x]]$ is algebraic.*

Proof. It is clear that $\sum_\nu \overline{a_\nu(0)}\, x^\nu=\sum_\nu \bar{a}_\nu x^\nu\in F_p[[x]]$ is algebraic, since $\sum_\nu a_\nu x^\nu$ is algebraic. For $i>0$, the proof is by induction on i. Note that

$$\sum_\nu \overline{a_\nu(i)}\, x^\nu=\overline{p^{-i}h(x)},$$

where

$$h(x)=\sum_\nu a_\nu x^\nu-\theta\left(\sum_\nu \overline{a_\nu(0)}\, x^\nu\right)-p\theta\left(\sum_\nu \overline{a_\nu(1)}\, x^\nu\right)$$
$$-\cdots-p^{i-1}\theta\left(\sum_\nu \overline{a_\nu(i-1)}\, x^\nu\right).$$

By the induction hypothesis and Lemma 3.4, there exists an algebraic power series $g(x) \in \mathbb{Z}_p[[x]]$ such that

$$h(x) \equiv g(x) \mod p^{i+1}.$$

Hence $\sum_v \overline{a_v(i)}\, x^v = \overline{p^{-i}g(x)}$ is algebraic, since $p^{-i}g(x) \in \mathbb{Z}_p[[x]]$ is algebraic. Q.E.D.

Proof of Theorem 3.1(i). It is sufficient to prove that

$$\overline{a_{p^e v+j}(i)} = \overline{a_{p^{e'} v+j'}(i)} \qquad \text{for } i = 0, 1, \ldots, s-1. \tag{1}$$

From Proposition 3.5 it follows that

$$y^{(i)} \overset{\text{def}}{=} \sum_v \overline{a_v(i)}\, x^v \in F_p[[x]]$$

is algebraic. From Lemma 2.1 it follows that, for each i, the set of all $y^{(i)}_{\alpha_1\alpha_2\alpha_3\cdots}$, for all possible $\alpha_1, \alpha_3, \alpha_3, \ldots \in S$ is finite. Hence the set of all s-tuples

$$(y^{(0)}_{\alpha_1\alpha_2\alpha_3\cdots}, y^{(1)}_{\alpha_1\alpha_2\alpha_3\cdots}, \ldots, y^{(s-1)}_{\alpha_1\alpha_2\alpha_3\cdots})$$

is finite. Hence there exists an $e \in \mathbb{N}_0$ such that for all $\alpha_1, \ldots, \alpha_e \in S$ there exist $e' < e$ and $\alpha'_1, \ldots, \alpha'_e \in S$ such that

$$y^{(i)}_{\alpha_1\alpha_2\cdots\alpha_e} = y^{(i)}_{\alpha'_1\cdots\alpha'_{e'}} \qquad \text{for } i = 0, 1, \ldots, s-1. \tag{2}$$

Formula (1) now follows from (2) and 3.2(1). Q.E.D.

Remark. The results which we have proved for F_p and $\mathbb{Z}_p$ remain true, with essentially the same proofs, for any finite field F_q ($q = p^n$) and any complete discrete valuation ring R, of characteristic zero, with prime $\mathfrak{p}$ and $R/(\mathfrak{p}) = F_q$.

4. Finite Machines

We recall that a finite machine M consists of the following. (i) A finite set $\mathcal{S}$ of (internal) states, one of which is the initial state, (ii) A finite alphabet, $\mathcal{I}$, of inputs, (iii) A finite alphabet $\mathcal{O}$ of outputs, (iv) A transition function $t: \mathcal{S} \times \mathcal{I} \to \mathcal{S}$ and an output function $o: \mathcal{S} \to \mathcal{O}$. The machine, starting in the initial state, is fed a sequence $i_1, i_2, \ldots$, from $\mathcal{I}$. At the jth stage it is in internal state s, it "reads" input i_j, enters the internal state $s' = t(s, i_j)$ and displays output $o(s')$.

We shall also want to consider machines with m inputs $i_{j1}, i_{j2}, \ldots$, for each

$j = 1, \dots, m$. At each stage it will read one "digit" from each input. We can always reduce such a machine to one with only one input by interweaving the inputs $i_{11}, i_{21}, \dots, i_{m1}, i_{12}, \dots$. For more information about finite machines the reader is referred to [Mi].

The machines we shall consider will have $\mathscr{I} = \{0, 1, 2, \dots, p-1\}$, so that an input $i_1, i_2, \dots$, can be considered as a natural number $\sum_j i_j p^{j-1}$. $\mathscr{O}$ will be the elements of $\mathbb{Z}/p^s$. Hence for each input $v \in \mathbb{N}^m$, in p-adic notation, the machine M produces an $a_v \in \mathbb{Z}/p^s$. We shall say that the sequence $\{a_v\}$ is generated by M.

4.1. Theorem. *The sequence $a_v \in \mathbb{Z}_p/p^s$, $v = (v_1, \dots, v_m) \in \mathbb{N}^m$ is generated by a finite machine if and only if there is an algebraic power series $y(x) = \sum \tilde{a}_v x^v \in \mathbb{Z}_p[[x]]$ such that $\tilde{a}_v \equiv a_v \bmod p^s$.*

Proof. Suppose that the a_v are generated by a finite machine M. Choose e so large that for every $s \in \mathscr{S}$ if M ever enters state s then it does so on an input of length less than e. This means that for each $i = (i_1, \dots, i_m)$ with $0 \leqslant i_j < p^e$ there is an $e' < e$ and an $i' = (i'_1, \dots, i'_m)$ with $0 \leqslant i'_j < p^{e'}$ such that $a_{p^e v + i} = a_{p^{e'} v + i'}$ for all v (i.e., M is in the same state after e stages starting with input i as it is after e' stages starting with input i'). The existence of $y(x)$ now follows immediately from Theorem 3.1(ii).

Conversely suppose that there is an algebraic power series $y(x) = \sum \tilde{a}_v x^v \in \mathbb{Z}_p[[x]]$ with $\tilde{a}_v \equiv a_v \bmod p^s$. From Theorem 3.1(i) we have that for e large enough and for every $i = (i_1, \dots, i_m)$ with $0 \leqslant i_j < p^e$ for $j = 1, \dots, m$ there is an $e' < e$ and an $i' = (i'_1, \dots, i'_m)$ with $0 \leqslant i'_j < p^{e'}$ for $j = 1, \dots, m$ such that

$$\tilde{a}_{p^e v + i} \equiv \tilde{a}_{p^{e'} v + i'} \quad \bmod p^s.$$

We equip our machine with a table of all the values of the $\tilde{a}_{i'} \bmod p^s$ for $i' = (i'_1, \dots, i'_m)$ with $0 \leqslant i'_j < p^{e'}$. We compute as follows. Given v write $v = p^e \bar{v} + i$. Use the above congruence to replace v by $v' = p^{e'} \bar{v} + i'$. Use the table to display $\bar{a}_{i'}$ and iterate. Q.E.D.

Remark. The same result is true if we replace $\mathbb{Z}_p$ by any complete discrete valuation ring R of characteristic zero, with prime $\mathfrak{p}$ such that $R/(\mathfrak{p}) = F$, for any finite field F. The only changes necessary in the proof are notational.

5. Diagonals of Algebraic Power Series

In this section we shall prove two results about the diagonals of algebraic power series. Theorem 5.1 gives an elementary proof of a result of

Deligne [D1, p. 129], and Theorem 5.2 is a strengthening of [D1, 3.8]. We apply Theorem 5.2 to give an analogue of Proposition 3.5 for "Teichmüller digits" (Theorem 5.5).

Throughout this section $x=(x_1,\ldots,x_m)$. If $y(x)=\sum a_{\nu_1\cdots\nu_m}x_1^{\nu_1}\cdots x_m^{\nu_m}$ then $I_{x_1x_2}(y)=\sum a_{\nu_1\nu_1\nu_3\cdots\nu_m}x_1^{\nu_1}x_3^{\nu_3}\cdots x_m^{\nu_m}$. The other diagonals $I_{x_ix_j}$ are defined similarly. By a diagonal we mean any composition of the $I_{x_ix_j}$. We shall also need the nondiagonals $J_{x_ix_j}(y)=\sum_{\nu_i>\nu_j}a_{\nu_1\cdots\nu_m}x_1^{\nu_1}\cdots x_m^{\nu_m}$.

5.1. Proposition. *Let F be a field of characteristic $p\neq 0$, let $x=(x_1,\ldots,x_m)$ and let $y(x)\in F[[x]]$ be algebraic. Let I be any composition of the $I_{x_ix_j}$'s* and the $J_{x_ix_j}$'s. Then $I(y)$ is algebraic.

Proof. We may suppose that F is perfect. It is sufficient to prove the proposition for $I=I_{x_ix_j}$ and for $J=J_{x_ix_j}$. We know from the remark following Lemma 2.1 that for e large enough the $y_{\alpha_1\cdots\alpha_e}$, for $(\alpha_1,\ldots,\alpha_e)\in S^e$, satisfy a system of equations of the form

$$y_{\alpha_1\cdots\alpha_e}=L_{\alpha_1\cdots\alpha_e}(\ldots y^{p}_{\beta_1\cdots\beta_e},\ldots,y^{p^2}_{\beta_1\cdots\beta_e},\ldots),\tag{1}$$

where $L_{\alpha_1\cdots\alpha_e}$ is a linear combination over $F[x]$ of the $y^{p}_{\beta_1\cdots\beta_e}$, $y^{p^2}_{\beta_1\cdots\beta_e},\ldots,y^{p^e}_{\beta_1\cdots\beta_e}$, and the coefficient of $y^{p^i}_{\beta_1\cdots\beta_e}$ has degree less than p^i. Hence we have for each $\alpha_1\cdots\alpha_e$ that

$$y_{\alpha_1\cdots\alpha_e}=\sum q_{\beta_1\cdots\beta_e i}(x)\,y^{p^i}_{\beta_1\cdots\beta_e},\tag{2}$$

where $i\geqslant 1$ and the degree of $q_{\beta_1\cdots\beta_e i}(x) is<p^i$. Note that $I(qy^{p^i}_{\beta_1\cdots\beta_e})=I(q)$ $I(y^{p^i}_{\beta_1\cdots\beta_e})=I(q)(I(y_{\beta_1\cdots\beta_e}))^{p^i}$, where we have written q instead of $q_{\beta_1\cdots\beta_e i}$. Hence applying I to the system (2) we get a system of the form

$$I(y_{\alpha_1\cdots\alpha_e})=\sum I(q_{\beta_1\cdots\beta_e i})(I(y_{\beta_1\cdots\beta_e}))^{p^i}$$

with i always $\geqslant 1$. Since the Jacobian of this system, in the unknowns $I(y_{\alpha_1\cdots\alpha_e})$ is 1 we have that all the $I(y_{\alpha_1\cdots\alpha_e})$ are algebraic. Since $y=\sum x^{\alpha_1+p\alpha_2+\cdots+p^{e-1}\alpha_e}y^{p^e}_{\alpha_1\cdots\alpha_e}$ we have that $I(y)=\sum I(x^{\alpha_1+p\alpha_2+\cdots+p^{e-1}\alpha_e})$ $(I(y_{\alpha_1\cdots\alpha_e}))^{p^e}$ and hence that $I(y)$ is algebraic.

Next let J be any one of the $J_{x_ix_j}$ and let I be the corresponding $I_{x_ix_j}$. Note that $J(qy^{p^i}_{\beta_1\cdots\beta_e})=q(J(y_{\beta_1\cdots\beta_e}))^{p^i}+J(q)(I(y_{\beta_1\cdots\beta_e}))^{p^i}$, where again q denotes $q_{\beta_1\cdots\beta_e i}(x)$ which has degree $<p^i$. Hence if we apply J to (2), we see by the previous argument, and the fact that the $I(y_{\beta_1\cdots\beta_e})$ are algebraic, that all $J(y_{\alpha_1\cdots\alpha_e})$ are algebraic. Since $J(y)=J(\sum x^{\alpha_1+p\alpha_2+\cdots+p^{e-1}\alpha_e}y^{p^e}_{\alpha_1\cdots\alpha_e})=\sum x^{\alpha_1+p\alpha_2+\cdots+p^{e-1}\alpha_e}(J(y_{\alpha_1\cdots\alpha_e}))^{p^e}+$ $\sum J(x^{\alpha_1+p\alpha_2+\cdots+p^{e-1}\alpha_e})(I(y_{\alpha_1\cdots\alpha_e}))^{p^e}$, we see that $J(y)$ is algebraic. Q.E.D.

Next let R be a complete discrete valuation ring of characteristic zero, with uniformizing parameter π such that $R/(\pi)=F$ is a field of characteristic $p\neq 0$.

5.2. Theorem. *Let $f(x) \in R[[x]]$ be algebraic and let $s \in \mathbb{N}$. Let I be any diagonal. Then there exists an algebraic power series $g(x) \in R[[x]]$ such that $I(f) \equiv g \bmod \pi^s$.*

5.3. Lemma. *Let $f(x) \in R[[x]]$ be algebraic. Then there exist* algebraic *power series*

$$g(x_1, x_3, \dots, x_m) \in R[[x_1, x_3, \dots, x_m]],$$
$$h(x) \in R[[x]],$$

such that

$$f(x) \equiv g(x_1 x_2, x_3, \dots, x_m) + h(x) \mod \pi$$

and

$$I_{x_1 x_2}(h) = 0.$$

Proof. $\overline{I_{x_1 x_2}(f)} = I_{x_1 x_2}(\bar{f}) \in F[[x_1, x_3, \dots, x_m]]$ is algebraic, and hence is the reduction $\bmod \pi$ of an algebraic power series $g(x_1, x_3, \dots, x_m) \in R[[x_1, x_3, \dots, x_m]]$. We have $I_{x_1 x_2}(f) \equiv g \bmod \pi$. Let $J_{x_1 x_2}$ be as before. $\overline{J_{x_1 x_2}(f)} = J_{x_1 x_2}(\bar{f}) =^{\text{def}} w_0(x) \in F[[x]]$ is algebraic. Note that $w_0(x)$ can be written as

$$w_0(x) = x_1 u_0(x_1, x_1 x_2, x_3, \dots, x_m) \qquad \text{with} \quad u_0 \in F[[x]].$$

Since $w_0(x)$ is algebraic, also $u_0(x)$ is algebraic. Hence $u_0(x)$ is the reduction $\bmod \pi$ of an *algebraic* power series $u(x) \in R[[x]]$. Thus $\bar{u}(x) = u_0(x)$, and $\overline{J_{x_1 x_2}(f)} = w_0(x) = x_1 \bar{u}(x_1, x_1 x_2, x_3, \dots, x_m)$. Hence $J_{x_1 x_2}(f) \equiv x_1 u(x_1, x_1 x_2, x_3, \dots, x_m) \bmod \pi$. Analogously there exists an algebraic power series $v(x) \in R[[x]]$ such that

$$J_{x_2 x_1}(f) \equiv x_2 v(x_1 x_2, x_2, x_3, \dots, x_m) \mod \pi.$$

Now take $h(x) =^{\text{def}} x_1 u(x_1, x_1 x_2, x_3, \dots, x_m) + x_2 v(x_1 x_2, x_2, x_3, \dots, x_m)$.

Q.E.D.

Proof of Theorem 5.2. It is sufficient to prove the theorem for the diagonal operator $I_{x_1 x_2}$. From the previous lemma the existence of algebraic power series $g_1 \in R[[x_1, x_3, x_4, \dots, x_m]]$ and $h_1 \in R[[x]]$ follows such that

$$f(x) \equiv g_1(x_1 x_2, x_3, \dots) + h_1(x) \mod \pi \qquad \text{and} \qquad I_{x_1 x_2}(h_1) = 0.$$

Let $f_1(x) =^{\text{def}} (1/\pi)(f(x) - g(x_1 x_2, x_3, \dots) - h(x)) \in R[[x]]$. Applying the lemma to $f_1(x)$ and so on, we obtain algebraic power series $g_2, g_3, \ldots, g_s \in R[[x_1, x_3, \ldots, x_m]]$ and $h_2, h_3, \ldots, h_s \in R[[x]]$ such that

$$\begin{aligned} f(x) \equiv g_1(x_1x_2, x_3, \ldots) + h_1(x) + \pi \cdot g_2(x_1x_2, x_3, \ldots) + \pi h_2(x) \\ + \cdots + \pi^{s-1} g_s(x_1x_2, x_3, \ldots) + \pi^{s-1} h_s(x) \mod \pi^s, \end{aligned}$$

and $I_{x_1x_2}(h_i) = 0$. Hence

$$I_{x_1x_2}(f(x)) \equiv g_1 + \pi g_2 + \cdots + \pi^{s-1} g_s \mod \pi^s. \qquad \text{Q.E.D.}$$

5.4. Corollary. *Let* $f(x) = \sum a_\nu x^\nu \in R[[x]]$ *and* $g(x) = \sum b_\nu x^\nu \in R[[x]]$ *be algebraic. Let* $h(x) = \sum_\nu a_\nu b_\nu x^\nu$ *be the Hadamard product of* f *and* g. *Let* $s \in \mathbb{N}_0$. *Then there exists an algebraic power series* $r(x) \in R[[x]]$ *such that* $r(x) \equiv h(x) \mod \pi^s$.

Proof. This follows from Theorem 5.2 and

$$I_{x_1 y_1} I_{x_2 y_2} \cdots I_{x_m y_m}(f(x)\, g(y)) = h(x). \qquad \text{Q.E.D.}$$

Remark. Theorem 5.2 in the case that $R/(\pi)$ is a finite field follows immediately from the results of Section 4. The use of the results of Section 4 can be replaced by an application of the diagonal to a system of equations of the form (1) in the proof of 3.1(ii) and an argument like the proof of Theorem 3.1(ii).

Next we use Theorem 5.2 to prove an analogue of Proposition 3.5 for "Teichmüller digits." Let R be a complete discrete valuation ring of characteristic zero, with uniformizing parameter π such that $R/(\pi) = F$ is a *perfect* field of characteristic $p \neq 0$. Then there exists a unique homomorphism γ of the *multiplicative* group of F into the group of units of R such that $\overline{\gamma(z)} = z$ for all $z \in F$, where the overbar denotes reduction mod(π), see, e.g., [Gr, p. 71]. The element $\gamma(z)$ is called the Teichmüller representative of z. If $c \in R$ is such that $\bar{c} = z^{p^{-n}}$, then $c^{p^n} \equiv \gamma(z) \mod \pi^{n+1}$. Every element $a \in R$ can be written in a unique way as

$$a = a(0) + a(1)\,\pi + a(2)\,\pi^2 + \cdots + a(i)\,\pi^i + \cdots,$$

where each $a(i) \in R$ is the Teichmüller representative of some element in F. We call $a(i)$ the ith Teichmüller digit of a. If $f(x) = \sum_\nu a_\nu x^\nu \in F[[x]]$, then we define $\gamma(f(x)) = \sum_\nu \gamma(a_\nu)\, x^\nu \in R[[x]]$, where we take $\gamma(\bar{0}) = 0$. With these notations we have

5.5 Theorem. *Let* $f(x) = \sum_\nu a_\nu x^\nu \in R[[x]]$ *and let* $s \in \mathbb{N}_0$. *Then* $f(x)$ *is congruent* $\mod \pi^s$ *to an algebraic power series in* $R[[x]]$ *if and only if* $\sum_\nu \overline{a_\nu(i)}\, x^\nu \in F[[x]]$ *is algebraic for* $i = 0, 1, \ldots, s-1$.

Proof. The theorem follows from Lemma 5.6 below, by using the same argument as in Proposition 3.5. Q.E.D.

5.6. LEMMA. *Let $f(x) \in F[[x]]$ be algebraic. Let $s \in \mathbb{N}_0$. Then there exists an algebraic power series $g(x) \in R[[x]]$ such that*

$$\gamma(f(x)) \equiv g(x) \mod \pi^s.$$

Proof. Write $f(x) = \sum_\nu a_\nu x^\nu$, with $a_\nu \in F$. Let $b_\nu = a_\nu^{p^{-(s-1)}}$. Then $\sum_\nu b_\nu x^\nu$ is algebraic, since it equals

$$(f(x^{p^{s-1}}))^{p^{-(s-1)}}.$$

From Remark 2.2 it follows that there exists an algebraic power series $\sum_\nu c_\nu x^\nu \in R[[x]]$ such that $\bar{c}_\nu = b_\nu = a_\nu^{p^{-(s-1)}}$. From Corollary 5.4 it follows that there exists an algebraic power series $g(x) \in R[[x]]$ such that

$$g(x) \equiv \sum_\nu c_\nu^{p^{s-1}} x^\nu \mod \pi^s$$

The lemma now follows from the congruence $\gamma(a_\nu) \equiv c_\nu^{p^{s-1}} \mod \pi^s$. Q.E.D.

6. REPRESENTATION OF ALGEBRAIC POWER SERIES AS DIAGONALS OF RATIONAL POWER SERIES

In this section we prove (Theorem 6.2) that any algebraic power series in any number of variables over an excellent local integral domain A can be written as a diagonal of a power series over A which is rational. The special case of algebraic power series in one variable over a field is contained in [Fu]. In Remark 6.6. we show how this representation can be used to give a short proof of the result in Section 3, following Christol's approach [Ch1].

Roughly speaking, an excellent ring is a Noetherian commutative ring which is not "pathological". For the definition of excellent ring we refer to [Ma, p. 258]. We recall that

(i) $\mathbb{Z}$, any field k, and any complete local Noetherian ring are excellent.

(ii) If A is an excellent ring, then any finitely generated A-algebra is excellent.

(iii) Any localization of an excellent ring is excellent.

(iv) A discrete valuation ring R is excellent if and only if the fraction field of its completion is separable over the fraction field of R.

(v) An excellent ring is Noetherian.

6.1. *Notation.* Let A be any integral domain. Let $x=(x_1,..., x_m)$ be as usual, and let y be one variable. Let

$$f(x, y)=\sum_{i_1,...,i_m,j} a_{i_1,i_2,...,i_m,j}x_1^{i_1}\cdots x_m^{i_m}y^j \in A[[x, y]].$$

We use the following notation

$$\mathscr{D}(f(x, y))=\sum_{j=i_1+i_2+\cdots+i_m} a_{i_1,i_2,...,i_m,j}x_1^{i_1}\cdots x_m^{i_m}.$$

6.2. THEOREM. *Let A be any excellent local integral domain, and let $x=(x_1,..., x_m)$ as usual. Let $f(x)\in A[[x]]$ be an algebraic power series. Then we have*:

(i) *There exists a power series $R(x, y)\in A[[x, y]]$, with y one variable, that represents a rational function of x, y, such that $f(x)=\mathscr{D}(R(x, y))$.*

(ii) *There exists a power series $S(x, u)\in A[[x, u]]$, $u=(u_1,..., u_m)$, that represents a rational function of x and u, such that*

$$f(x)=I_{x_1u_1}I_{x_2u_2}\cdots I_{x_mu_m}S(x, u).$$

Proof of 6.2(i). Let $\mathfrak{m}$ be the unique maximal ideal of A, let (x) be the prime ideal of $A[x]$ generated by $x_1, x_2,..., x_m$, and let $(\mathfrak{m}, x)$ be the maximal ideal of $A[x]$ generated by $\mathfrak{m}$ and (x).

We denote the localization of $A[x]$ with respect to the maximal ideal $(\mathfrak{m}, x)$ by $A[x]_{(\mathfrak{m},x)}$. We will use the notion of *Henselization* of a pair (R, I) consisting of a ring R and an ideal I of R, see [Ra, p. 124 Definition 4]. Let the pair $(A\{x\}, (x))$ be the Henselization of the pair $(A[x]_{(\mathfrak{m},x)}, (x))$. Thus $(A\{x\}, (x))$ is an Henselian pair although in general $A\{x\}$ is not an Henselian ring. We have $A\{x\}\subset A[[x]]$. Since A is excellent, the fibers of $\text{Spec}(A[[x]]\rightarrow\text{Spec}(A[x]_{(\mathfrak{m},x)})$ are geometrically regular [Ma, Sect. 34.C]. Hence, from [Ra, p. 127, Corollary 1] (and the faithfully flatness of $A[[x]]$ over $A\{x\}$), follows that $A\{x\}$ is algebraically closed in $A[[x]]$. In the special case that A is a field or a complete discrete valuation ring, the claim that $A\{x\}$ is algebraically closed in $A[[x]]$ also follows directly from Artin's Approximation Theorem [Ar]. Now, let $f(x)\in A[[x]]$ be any algebraic power series. Thus we have $f(x)\in A\{x\}$. From the construction of the Henselization $A\{x\}$ as a direct limit of certain étale extensions of $A[x]_{(\mathfrak{m},x)}$, see [Ra, p. 125, Theorem 2], it easily follows that there exists a subring B of $A[[x]]$ which is finitely generated over $A[x]$ and étale over $A[x]$ at $(\mathfrak{m}, x)\cap B$, such that $f\in B$. (For simplicity we use $(\mathfrak{m}, x)$ to denote $(\mathfrak{m}, x)A[[x]]$.) Next, we use the fact [Ra, p. 51, Theorem 1] that any étale extension is *locally* a standard étale extension. (Because we have this only locally, we need A to be local). Hence

$$B_{(\mathfrak{m},x)\cap B} = (A[x][\varphi])_{(\mathfrak{m},x)\cap A[x][\varphi]}, \tag{1}$$

where $\varphi \in A[[x]]$ satisfies an equation $P(x, \varphi) = 0$, with $P(x, y) \in A[x, y]$, (y one variable), and

$$\frac{\partial P}{\partial y}(x, \varphi) \notin (\mathfrak{m}, x). \tag{2}$$

Without loss of generality we may suppose that $\varphi(0) = 0$. Then (2) implies that $(\partial P/\partial y)(0, 0) \notin \mathfrak{m}$. From (1) it follows that

$$f(x) = \frac{a_0(x) + a_1(x)\,\varphi(x) + \cdots + a_r(x)\,\varphi(x)^r}{b_0(x) + b_1(x)\,\varphi(x) + \cdots + a_s(x)\,\varphi(x)^s}, \tag{3}$$

with $a_i(x)$, $b_i(x) \in A[x]$ and $b_0(0) \notin \mathfrak{m}$. Let

$$W(x, y) = \frac{a_0(x) + a_1(x)\,y + \cdots + a_r(x)\,y^r}{b_0(x) + b_1(x)\,y + \cdots + a_s(x)\,y^s} \in A[[x, y]],$$

and let

$$R(x, y) = y W(xy, y) \frac{\partial P}{\partial y}(xy, y)/P(xy, y),$$

(here xy denotes $(x_1 y, x_2 y, \ldots, x_m y)$). Note that $R(x, y)$ represents a rational function of x, y.

From Lemma 6.3(i), it follows that $R(x, y) \in A[[x, y]]$. Moreover, from Lemma 6.3(ii), and by expanding $W(x, y)$ in a power series in x, y and using the additivity of $\mathcal{D}$, it follows that

$$\mathcal{D}(R(x, y)) = W(x, \varphi(x)) = f(x). \qquad \text{Q.E.D.}$$

6.3. Lemma. *Let A be an integral domain. Let $x = (x_1, \ldots, x_m)$, and let y be one variable. Let $P(x, y) \in A[x, y]$ and suppose that $(\partial P/\partial y)(0, 0)$ is a unit in A. Let $\varphi(x) \in A[[x]]$ and suppose that $P(x, \varphi(x)) = 0$ and $\varphi(0) = 0$. Then we have*:

(i) $y(\partial P/\partial y)(xy, y)/P(xy, y) \in A[[x, y]]$,

(*here xy denotes $(x_1 y, x_2 y, \ldots, x_m y)$.*).

(ii) *If $i \in \mathbb{N}^m$, $j \in \mathbb{N}$, then*

$$\mathcal{D}\left(y(xy)^i y^j \frac{\partial P}{\partial y}(xy, y)/P(xy, y)\right) = x^i \varphi(x)^j.$$

Proof. We apply the method of [Fu, Proposition 2]. Write

$$P(x, y) = (y - \varphi(x))\, Q(x, y),$$

with $Q(x, y) \in A[[x]][y]$. We have

$$\frac{\partial P}{\partial y} = Q + (y - \varphi(x))\, \frac{\partial Q}{\partial y} \tag{1}$$

and

$$\frac{1}{P}\, \frac{\partial P}{\partial y} = \frac{1}{y - \varphi(x)} + \frac{1}{Q}\, \frac{\partial Q}{\partial y}. \tag{2}$$

From (1) and $\varphi(0) = 0$, it follows that $Q(0, 0)$ is a unit, since $(\partial P/\partial y)(0, 0)$ is a unit. Hence $(1/Q)(\partial Q/\partial y) \in A[[x, y]]$. Note that

$$\frac{y}{y - \varphi(xy)} = \frac{1}{1 - y^{-1}\varphi(xy)} \in A[[x, y]].$$

This proves (i). Next we have that

$$\mathscr{D}\Big(y(xy)^i\, y^j\, \frac{\partial Q}{\partial y}\, (xy, y)/Q(xy, y)\Big) = 0, \tag{3}$$

because $\mathscr{D}$ is applied to a power series of the form $y\theta(xy, y)$, with $\theta \in A[[x, y]]$. Moreover

$$\begin{aligned}\mathscr{D}\, \frac{(xy)^i\, y^{j+1}}{y - \varphi(xy)} &= \mathscr{D}((xy)^i\, y^j(1 - y^{-1}\varphi(xy))^{-1})\\ &= \mathscr{D}\Big((xy)^i \sum_{n=0}^{\infty} y^{j-n}\varphi(xy)^n\Big)\\ &= \mathscr{D}((xy)^i\, \varphi(xy)^j) = x^i\varphi(x)^j.\end{aligned}$$

The Lemma now follows from (2) and (3). Q.E.D.

Proof of 6.2(ii). By Theorem 6.2(i), there exists a rational function $R(x, y) \in A[[x, y]]$, such that $f(x) = \mathscr{D}(R(x, y))$. As before, y is one variable. Write

$$R(x, y) = \sum a_{ij} x^i y^j,$$

where i is a multi index. Define

$$R_1(x, u_1, v_1)$$
$$= \frac{u_1 R(x, u_1) - v_1 R(x, v_1)}{u_1 - v_1} = \sum_{j = k_1 + l_1} a_{ij} x^i u_1^{k_1} v_1^{l_1},$$

$$R_2(x, u_1, u_2, v_2)$$
$$= \frac{u_2 R_1(x, u_1, u_2) - v_2 R_1(x, u_1, v_2)}{u_2 - v_2} = \sum_{j = k_1 + k_2 + l_2} a_{ij} x^i u_1^{k_1} u_2^{k_2} v_2^{l_2},$$

$$\vdots$$

$$R_{m-1}(x, u_1, \ldots, u_{m-2}, u_{m-1}, v_{m-1})$$
$$= \frac{u_{m-1} R_{m-2}(x, u_1, \ldots, u_{m-2}, u_{m-1}) - v_{m-1} R_{m-2}(x, u_1, \ldots, u_{m-2}, v_{m-1})}{u_{m-1} - v_{m-1}}$$
$$= \sum_{j = k_1 + \cdots + k_{m-1} + l_{m-1}} a_{ij} x^i u_1^{k_1} u_2^{k_2} \cdots u_{m-1}^{k_{m-1}} v_{m-1}^{l_{m-1}}.$$

We have

$$I_{x_1 u_1} I_{x_2 u_2} \cdots I_{x_{m-1} u_{m-1}} I_{x_m v_{m-1}} (R_{m-1}) = \mathscr{D}(R(x, y)).$$

Since $f(x) = \mathscr{D}(R(x, y))$, this proves Theorem 6.2(ii). Q.E.D.

6.3. *Remark.* If A is a Noetherian integral domain, then every power series $f(x) \in A[[x]]$, $x = (x_1, \ldots, x_m)$, which represents a rational function, can be written as

$$f(x) = P(x)/Q(x) \quad \text{with } P(x), Q(x) \in A[x] \quad \text{and} \quad Q(0) = 1. \tag{1}$$

This follows from the fact that $A[[x]]$ is faithfully flat over the ring of power series of the form (1), see [Ma, Sect. 24, p. 172]. However, this is not generally true when A is not Noetherian.

6.4. *Remark.* The converse of Theorem 6.2(i) is also true. Let $x = (x_1, \ldots, x_m)$ and let y be one variable. If $f(x, y)$ is a power series which represents a rational function, then $\mathscr{D}(f)$ is algebraic. Indeed

$$I_{ty} f(xt, y) = \mathscr{D}(f)(xt),$$

and I_{ty} of a rational power series (t one variable, y one variable) is algebraic, see [Fu].

Remark. The converse of Theorem 6.2(ii) is not true. Indeed it is known [Fu, p. 273] that there exists a rational power series $f(x, y, u)$ over $\mathbb{C}$ in three variables such that $I_{xy} I_{yu} f$ is not algebraic. But

$$I_{xy} I_{zu} f(x, yz, u) = (I_{xy} I_{yu} f)(xz).$$

6.6. *Remark.* Christol [Ch1] proves the case $m = 1$ of Theorem 3.1 by using the case $m = 1$, A a field, (due to Furstenberg [Fu]) of Theorem 6.2. In this remark we show how Theorem 3.1 follows by the same argument from Theorem 6.2. Moreover we can simplify Christol's argument by taking for A the ring $\mathbb{Z}_p$ instead of a field. Note, however, that the proof of Theorem 6.2 is not elementary, while that of Theorem 3.1 given above is.

Proof of Theorem 3.1(i). Let $f \in \mathbb{Z}_p[[x_1, ..., x_m]]$ be algebraic. Let $x = (x_1, ..., x_m, x_{m+1}, ..., x_{2m})$. From Theorem 6.2 and Remark 6.3 it follows that we can write

$$f = I(P/Q), \qquad \text{where} \quad I = I_{x_1 x_{m+1}} I_{x_2 x_{m+2}} \cdots I_{x_m x_{2m}}$$

and $P(x)$, $Q(x) \in \mathbb{Z}_p[x]$, $Q(0) = 1$. Let $\varphi: \mathbb{Z}_p[[x]] \to \mathbb{Z}_p[[x]]$ be defined by $\varphi(\sum_\nu a_\nu x^\nu) = \sum_\nu a_\nu x^{p\nu}$. For $r = (r_1, ..., r_{2m})$, $0 \leqslant r_i < p$, let $\psi_r(\sum_\nu a_\nu x^\nu) = \sum_\nu a_{p\nu + r} x^\nu$. Let $s \in \mathbb{N}$ be fixed.

Let V be the $\mathbb{Z}_p/(p^s)$ module of all $F/Q^{p^s} \bmod p^s$, where $F \in \mathbb{Z}_p[x]$ has degree $\leqslant d$, where d will be chosen later. Note that $Q^p \equiv \varphi(Q) \bmod p$, and hence that $Q^{p^s} \equiv (\varphi(Q))^{p^{s-1}} \bmod p^s$. Indeed if $a \equiv b \bmod p$, then $a^{p^n} \equiv b^{p^n} \bmod p^{n+1}$. Note also that $\psi_r(g\varphi(h)) = \psi_r(g)\, h$ and that $(\varphi(Q))^{p^{s-1}} = \varphi(Q^{p^{s-1}})$. Hence

$$\begin{aligned} \psi_r(F/Q^{p^s}) &\equiv \psi_r(F/\varphi(Q^{p^{s-1}})) \quad \bmod p^s \\ &\equiv \psi_r(F)/Q^{p^{s-1}} \equiv \psi_r(F)\, Q/Q^{p^s}. \end{aligned}$$

Choose $d \geqslant \deg P + p^s \deg Q$. Then, since $\deg \psi_r(F) \leqslant (1/p) \deg F$, we see that V is closed under all the ψ_r and that $P/Q \bmod p^s$ is an element of V. Notice that V is finite. Let IV be the image of V under the diagonal map I. Clearly $f \bmod p^s$ is an element of IV and IV is closed under ψ_v for all $v = (r_1, ..., r_m)$, since $I\psi_{(v,v)} = \psi_v I$. Theorem 3.1(i) follows directly from this and the finiteness of IV. Q.E.D.

Proof of Theorem 3.1(ii). Suppose that the Taylor coefficients of $f(x) \in \mathbb{Z}_p[[x_1, ..., x_m]]$ satisfy congruences of the form (1) of Theorem 3.1. By Remark 2.2 there is an algebraic $g \in \mathbb{Z}_p[[x_1, ..., x_m]]$ such that $f \equiv g \bmod p$. Applying Theorem 3.1(i) to g it follows easily that $(1/p)(f - g)$ satisfies a set of congruences of the form (1) of Theorem 3.1 with p^s replaced by p^{s-1}. Hence by induction there is an algebraic $h \in \mathbb{Z}_p[[x]]$ such that $(1/p)(f - g) \equiv h \bmod p^{s-1}$. Then $f \equiv g + ph \bmod p^s$. Q.E.D.

7. Some Particular Recursions

Let the $a_n \in \mathbb{Z}_p$, $n \in \mathbb{N}$, satisfy $a_n = F(n)\, a_{n-1}$ where $F(n) = f(n)/g(n)$, $f(n) = \prod_{i=1}^{m} (\alpha_i n + \beta_i)$, $g(n) = \prod_{i=1}^{m} (\gamma_i n + \delta_i)$, where the α_i, β_i, γ_i, $\delta_i \in \mathbb{Z}$ and $(\alpha_i, p) = (\gamma_i, p) = 1$.

7.1. Theorem. *With the above notation let $y(x) = \sum a_n x^n$ and let $s \in \mathbb{N}$. Then there is an algebraic power series $\bar{y}(x) \in \mathbb{Z}_p[[x]]$ such that $y(x) \equiv \bar{y}(x) \bmod p^s$.*

Proof. Let $0 \leqslant j < p$. Iterating the above recursion formula p times we have that

$$\begin{aligned} a_{pk+j} &= F(pk+j)\, F(pk+j-1) \cdots F(pk+j-p+1)\, a_{p(k-1)+j} \\ &= \left(\prod_{r=j-p+1}^{j} F(pk+r) \right) a_{p(k-1)+j} \\ &= \left(\prod_{i=1}^{m} \prod_{r=j-p+1}^{j} \frac{\alpha_i pk + (\alpha_i r + \beta_i)}{\gamma_i pk + (\gamma_i r + \delta_i)} \right) a_{p(k-1)+j}. \end{aligned}$$

Now for each i exactly one of the terms $\alpha_i r + \beta_i$ is divisible by p. Let it be equal to $\beta_i' p$. Similarly for each i exactly one of the $\gamma_i r + \delta_i$ is divisible by p. Let it be equal to $\delta_i' p$. Cancelling the p's we get

$$a_{pk+j} = \left(\prod_{i=1}^{m} \frac{\alpha_i k + \beta_i'}{\gamma_i k + \delta_i'} \right) \cdot \frac{u_0 + u_1(k)\, p + u_2(k)\, p^2 + \cdots}{v_0 + v_1(k)\, p + v_2(k)\, p^2 + \cdots}\, a_{p(k-1)+j}, \qquad (1)$$

where we have collected into the second factor all the factors not divisible by p. Notice that u_0 and v_0 are $\not\equiv \bmod p$ and the $u_i(k)$, $v_i(k) \in \mathbb{Z}[k]$. Let $u(k) = u_0 + u_1(k)\, p + \cdots$ and $v(k) = v_0 + v_1(k)\, p + \cdots$. Then for every value of $k \in \mathbb{N}$, $u(k)$ and $v(k)$ are p-adic units. Note that for every $k \in \mathbb{N}$ we have $k^{p^{s-1}(p-1)+s} \equiv k^s \bmod p^s$. Reducing $u(k)$ and $v(k)$ modulo p^s and using the above congruence we see that there are polynomials $\bar{u}(k)$ and $\bar{v}(k)$ of degree $< p^{s-1}(p-1)+s$ with coefficients from the set $\{0, 1, ..., p^s - 1\}$ such that for all $k \in \mathbb{N}$ we have $u(k) \equiv \bar{u}(k)$ and $v(k) \equiv \bar{v}(k)$ modulo p^s. Let $R_{1j} = \bar{u}(k)/\bar{v}(k)$. Hence we have that if the $\tilde{a}_{pk+j}$ are determined by the recursion formula $\tilde{a}_{pk+j} = \prod_{i=1}^{m} (\alpha_i k + \beta_i')/(\gamma_i k + \delta_i')\, R_{1j}(k)\, \tilde{a}_{p(k-1)+j}$, and the initial condition $\tilde{a}_j \equiv a_j \bmod p^{\operatorname{ord}(a_j)+s}$, where $\operatorname{ord}(a_j)$ is the p-adic order of a_j, then $\tilde{a}_{pk+j} \equiv a_{pk+j} \bmod p^s$ for all k. Iterating the above procedure we get for every e and every j with $0 \leqslant j < p^e$ that there exist β_{iej}, $\delta_{iej} \in \mathbb{Z}$ and rational functions $R_{ej}(k)$ with numerators and denominators of degrees

$<p^{s-1}(p-1)+s$ and coefficients from $\{0, 1, \ldots, p^s-1\}$ such that if the $\tilde{a}_{p^ek+j}$ satisfy the recursion formula

$$\tilde{a}_{p^ek+j} = \left(\prod_i \frac{\alpha_i k+\beta_{iej}}{\gamma_i k+\delta_{iej}}\right) R_{ej}(k)\, \tilde{a}_{p^e(k-1)+j} \tag{2}$$

and initial condition

$$\tilde{a}_j \equiv a_j \bmod p^{\operatorname{ord}(a_j)+s} \tag{3}$$

then $\tilde{a}_{p^ek+j} \equiv a_{p^ek+j} \bmod p^s$ for all $k \in \mathbb{N}$. Now let $A \in \mathbb{N}$ be such that $|\alpha_i|$, $|\beta_i|$, $|\gamma_i|$, $|\delta_i| \leqslant A$ for all i. Notice that $|\beta_i'| = |(\alpha_i r+\beta_i)/p| \leqslant (|\alpha_i|\,(p-1)+|\beta_i|)/p$ since $j-p+1 \leqslant r \leqslant j$ and $0 \leqslant j < p$. Hence $|\beta_i'| \leqslant A$. Similarly $|\delta_i'| \leqslant A$. Hence, by induction $|\beta_{iej}| \leqslant A$ and $|\delta_{iej}| \leqslant A$ for all i, e, j. This shows that there are only finitely many different recursion formulas (2). If e, j and e', j' are such that the corresponding recursion formulas (2) are actually the same, and if a_j, a_j', satisfy $\operatorname{ord}(a_j)+s \leqslant \operatorname{ord}(a_j')$, then, since all the $a_n \in \mathbb{Z}_p$, we must have that $\tilde{a}_{p^{e'}k+j'} \equiv 0 \bmod p^s$ for all k. Now consider the above procedure of determining recursion formulas (2) and initial conditions (3). The first time a particular recursion formula F occurs, let its initial condition be a_F. We can note $\operatorname{ord}(a_F)+s = v_F$ say. If this recursion formula F occurs again in the procedure we know that the corresponding sequence of the $\tilde{a}_{p^ek+j} \bmod p^s$, $k = 0, 1, 2, \ldots$, is determined by the recursion formula F and $\tilde{a}_j \bmod p^{v_F+s}$. Hence we see that there are only a finite number of different sequences $\tilde{a}_{p^ek+j} \bmod p^s$. Hence for e large enough we will have that for every j with $0 \leqslant j < p^e$ there is an $e' < e$ and a j' with $0 \leqslant j' < p^{e'}$, such that $a_{p^ek+j} \equiv a_{p^{e'}k+j'} \bmod p^s$, for all k. From Theorem 3.1(ii) we now have immediately that there is an algebraic power series $\bar{y}(x) = \sum \bar{a}_n x^n \in \mathbb{Z}_p[[x]]$ with $\bar{a}_n \equiv a_n \bmod p^s$, for all $n \in \mathbb{N}$. Q.E.D.

Remarks. (i) In the above proof we could have considered recursions of the form $a_n = (f(n)\,h(n)/g(n)\,k(n))\,a_{n-1}$, with the $f(n)$, $g(n)$ as above and the $h(n)$, $k(n) \in \mathbb{Z}[n]$ such that $h(n)$, $k(n)$ are units in $\mathbb{Z}_p$ for all $n \in \mathbb{N}$.

(ii) If one allows $f(n)$ to have a zero in $\mathbb{Z}_p \backslash \mathbb{Q}$ then $y(x)$ need not be algebraic. Indeed, for $\alpha \in \mathbb{Z}_p \backslash \mathbb{Q}$, the power series $(1-x)^\alpha \in F_p[[x]]$ is not algebraic, see [Ch2, Sect. 9 Example 1] or [M-V].

(iii) Christol and Dwork have informed us that Theorem 7.1 can also be proved (at least for almost all p), by using the theory of differential equations with strong Frobenius structure.

References

[Ar] M. Artin, Algebraic approximation of structures over complete local rings, *Inst. Hautes Etudes Sci. Publ. Math.* **36** (1968), 23–58.

[Ch] G. Christol, Eléments analytiques uniformes et multiformes, Sèminaire Delange–Pisot–Poitou (Théorie des nombres) 1973/1974, No. 6.

[Ch2] G. Christol, Fonctions et éléments algébriques, *Pacific J. Math.* **125** (1986), 1–37.

[C-K] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, Suites Algébriques, Automates et Substitutions, *Bull. Soc. Math. France* **108** (1980), 401–409.

[D1] P. Deligne, Intégration sur un cycle évanescant, *Invent. Math.* **76** (1984), 129–143.

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

[Gr] M. Greenberg, "Lectures on forms in many variables," Benjamin, New York, 1969.

[La] S. Lang, "Algebra," Addison–Wesley, Reading, Mass., 1965.

[Ma] Matsumura, "Commutative Algebra," Benjamin, New York, 1970.

[M-V] M. Mendès-France and A. van der Poorten, Automata and the arithmetic of formal power series, preprint.

[Mi] M. Minsky, Computation: Finite and infinite machines, Prentice–Hall, Englewood Cliffs, N.J., 1967.

[Ra] M. Raynaud, "Anneaux Locaux Henséliens," Lecture Notes in Mathematics, No. 169, Springer-Verlag, Berlin, 1970.