Journal of Pure and Applied Algebra 29 (1983) 93-97
North-Holland

AUTOMORPHISMS OF POLYNOMIAL AND POWER SERIES RINGS

Pekka NOUSIAINEN
Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

Moss E. SWEEDLER*
Department of Mathematics, Cornell University, Ithaca, NY 14853, USA

Communicated by H. Bass
Received 8 November 1982

1980 AMS(MOS)SCN: Primary 13B10; Secondary 13F20, 13F25.

Key words and phrases: Jacobian matrix, Jacobian conjecture, Inversion formula, Locally nilpotent derivation, Locally finite derivation.

1. Introduction

Our main results are inversion formulas for automorphisms of a power series ring (2.1, 2.5) and a characterization of automorphisms of a polynomial ring in characteristic zero (3.3). We use:

1.1. Notations. k is a commutative ring and $X=(X_1,\dots,X_n)$ is a set of indeterminates, $k[X]=k[X_1,\dots,X_n]$ and $k[[X]]=k[[X_1,\dots,X_n]]$ are the polynomial and power series rings over k.

A k-algebra endomorphism φ of $k[X]$ is given by $X_i\to f_i$ $(1\le i\le n)$ for some set of n polynomials $f=(f_1,\dots,f_n)$ in $k[X]$. If $\tau\in \mathrm{Aut}_k\, k[X]$ is the translation defined by $X_i\to X_i-f_i(0)$ $(1\le i\le n)$, then $\varphi\tau$ is defined by $X_i\to f_i-f_i(0)$ $(1\le i\le n)$. Hence there is no essential loss of generality in assuming that φ *preserves the origin*, i.e., that $f_1,\dots,f_n$ have no constant terms. In the case of power series, a k-algebra endomorphism φ of $k[[X]]$ is given by $X_i\to f_i$ $(1\le i\le n)$ for some set of n power series $f=(f_1,\dots,f_n)$ in $k[[X]]$ with no constant terms. Hence, if φ is an endomorphism of $k[X]$ preserving the origin then φ is also an endomorphism of $k[[X]]$.

1.2. Definition. Let $\varphi\in \mathrm{End}_k\, k[X]$ (resp. $\varphi\in\mathrm{End}_k\, k[[X]]$) be an endomorphism given by $X_i\to f_i$ $(1\le i\le n)$. Then the *Jacobian* of φ is the $n\times n$ matrix

*Supported by the John Simon Guggenheim Memorial Foundation.

$$\mathrm{Jac}(\varphi)=\mathrm{Jac}(f)=(\partial f_j/\partial X_i)$$

over $k[X]$ (resp. over $k[[X]]$).

A simple computation gives:

1.3. Lemma. (i) *Let* 1 *denote the identity map of* $k[X]$ *(resp. of* $k[[X]]$*). Then* $\mathrm{Jac}(1)=I$.

(ii) *If* φ *and* ψ *are two endomorphisms of* $k[X]$ *(resp. of* $k[[X]]$*), then* $\mathrm{Jac}(\varphi\psi)=\mathrm{Jac}(\varphi)\mathrm{Jac}(\psi)^{\varphi}$, *where* $\mathrm{Jac}(\psi)^{\varphi}$ *denotes* φ *applied entrywise to* $\mathrm{Jac}(\psi)$. □

By 1.3, if φ is invertible, then so is $\mathrm{Jac}(\varphi)$. The converse is not true in general. A long-standing open problem is:

1.4. Jacobian Conjecture. If k contains the field $\mathbf{Q}$ of rational numbers and φ is an endomorphism of $k[X]$ with $\mathrm{Jac}(\varphi)$ invertible, then φ is an automorphism of $k[X]$. □

In 3.3 we give necessary and sufficient conditions under which 1.4 is true. These conditions are expressed in terms of certain derivations $d_1,\dots,d_n$ of $k[X]$ introduced in the next section (2.3). We refer to [1] for a survey of the Jacobian Conjecture.

2. The inversion formula

We use the notations 1.1. Given a multi-index $\alpha=(\alpha_1,\dots,\alpha_n)$ of non-negative integers, define

$$(\partial/\partial X)^{(\alpha)}=\frac{1}{\alpha!}(\partial/\partial X)^{\alpha}=\frac{1}{\alpha_1!\cdots\alpha_n!}(\partial/\partial X_1)^{\alpha_1}\cdots(\partial/\partial X_n)^{\alpha_n}.$$

As an operator, $(1/j!)(\partial/\partial X_i)^j$ is defined by

$$\frac{1}{j!}(\partial/\partial X_i)^j(X_1^{m_1}\cdots X_n^{m_n})=\binom{m_i}{j}X_1^{m_1}\cdots X_{i-1}^{m_{i-1}}X_i^{m_i-j}X_{i+1}^{m_{i+1}}\cdots X_n^{m_n}.$$

Hence this makes sense over any commutative ring k. The $(\partial/\partial X)^{(\alpha)}$ are *higher derivations* of $k[X]$ (resp. of $k[[X]]$), i.e., they satisfy the rule

$$(\partial/\partial X)^{(\alpha)}(uv)=\sum_{\beta+\gamma=\alpha}(\partial/\partial X)^{(\beta)}(u)(\partial/\partial X)^{(\gamma)}(v).$$

This is essentially the familiar Leibniz rule from Calculus.

2.1. Inversion Formula. *Let* φ *be an automorphism of* $k[[X]]$ *given by* $X_i\to f_i$ $(1\le i\le n)$. *If* $\alpha=(\alpha_1,\dots,\alpha_n)$ *is a multi-index of non-negative integers, define* $d^{(\alpha)}=\varphi(\partial/\partial X)^{(\alpha)}\varphi^{-1}$. *Then* φ^{-1} *is given by*

$$\varphi^{-1}(u)=\sum_{\alpha}(X-f)^{\alpha}d^{(\alpha)}(u) \tag{2.2}$$

where $(X-f)^{\alpha}=(X_1-f_1)^{\alpha_1}\cdots(X_n-f_n)^{\alpha_n}$.

Proof. Define $\psi(u)$ to be the right-hand side of (2.2). Then ψ is a well-defined k-linear map $k[[X]]\to k[[X]]$. Since the $(\partial/\partial X)^{(\alpha)}$ are higher derivations of $k[[X]]$, so are the $d^{(\alpha)}$. This implies that ψ is a k-algebra endomorphism of $k[[X]]$. For $1\le i\le n$ we have

$$\psi\varphi(X_i)=\sum_{\alpha}(X-f)^{\alpha}\varphi(\partial/\partial X)^{(\alpha)}(X_i)=f_i+(X_i-f_i)=X_i.$$

Hence $\psi\varphi=1$. □

Now suppose that φ is an endomorphism of $k[X]$ (resp. of $k[[X]]$) with $\operatorname{Jac}(\varphi)$ invertible. We define derivations $d_1,\dots,d_n$ of $k[X]$ (resp. of $k[[X]]$) by the matrix equation

$$\begin{pmatrix} d_1\\ \vdots \\ d_n\end{pmatrix}=\operatorname{Jac}(\varphi)^{-1}\begin{pmatrix}\partial/\partial X_1\\ \vdots\\ \partial/\partial X_n\end{pmatrix}. \tag{2.3}$$

2.4. Proposition. (i) *$d_1,\dots,d_n$ are uniquely characterized by the property that d_i is equal to $\partial/\partial f_i$ on $k[f]$ (resp. on $k[[f]]$) for $1\le i\le n$.*

(ii) *$d_1,\dots,d_n$ commute.*

(iii) *If φ is an automorphism, then $d_i=\varphi(\partial/\partial X_i)\varphi^{-1}$.*

Proof. As a module, the set of derivations of $k[X]$ (resp. of $k[[X]]$) is generated by $\partial/\partial X_1,\dots,\partial/\partial X_n$. Since $\operatorname{Jac}(\varphi)$ is invertible, it is also generated by $d_1,\dots,d_n$. It is clear from the definition that $d_if_j=\delta_{ij}$. Hence d_i restricts to $\partial/\partial f_i$. If d is a derivation such that $df_1=\cdots=df_n=0$, then writing $d=\sum a_id_i$ we see that $d=0$. We use this to prove the remaining claims. If d_i,d_i' both restrict to $\partial/\partial f_i$ then $d=d_i-d_i'=0$. Given i and j, the commutator $d=[d_i,d_j]=d_id_j-d_jd_i=0$. Finally, if φ is an automorphism then $d=d_i-\varphi(\partial/\partial X_i)\varphi^{-1}=0$. □

We conclude this section with:

2.5. Characteristic Zero Inversion Theorem. *Assume that k contains the field $\mathbb{Q}$ of rational numbers. Let φ be an endomorphism of $k[[X]]$ with $\operatorname{Jac}(\varphi)$ invertible. Then φ is an automorphism of $k[[X]]$ and φ^{-1} is given by the formula* (2.2), *where*

$$d^{(\alpha)}=\varphi(\partial/\partial X)^{(\alpha)}\varphi^{-1}=\frac{1}{\alpha!}\,d^{\alpha}=\frac{1}{\alpha_1!\cdots\alpha_n!}\,d_1^{\alpha_1}\cdots d_n^{\alpha_n}.$$

Proof. Let $d^{(\alpha)}=(1/\alpha!)d^{\alpha}$. Then the $d^{(\alpha)}$ are higher derivations of $k[[X]]$. Define

$\psi(u)$ to be the right-hand side of (2.2). Then ψ is an endomorphism of $k[[X]]$, and using 2.4(i), (ii) we see that $\psi\varphi = 1$. In order to show that $\varphi\psi = 1$ it suffices to show that $\varphi\psi \equiv 1 \bmod ((X))^m$ for $m \geq 0$, where $((X))$ is the ideal generated by $X_1, \ldots, X_n$. This is clear since $\psi\varphi \equiv 1 \bmod ((X))^m$ and $k[[X]]/((X))^m$ is a finitely generated free k-module. Finally, $d^{(\alpha)} = \varphi(\partial/\partial X)^{(\alpha)}\varphi^{-1}$ by 2.4(iii). □

3. Local nilpotence and local finiteness

This section contains a criterion for the invertibility of an endomorphism φ of $k[X]$ in characteristic zero.

3.1. Definition. Let k be a commutative ring and let d be a derivation of $k[X]$. Then $\mathrm{Ker}(d)$, $\mathrm{Nil}(d)$, $\mathrm{Fin}(d) \subseteq k[X]$ and defined by

(i) $z \in \mathrm{Ker}(d)$ iff $d(z) = 0$.

(ii) $z \in \mathrm{Nil}(d)$ iff there is an integer $m \geq 0$ such that $d^m(z) = 0$.

(iii) $z \in \mathrm{Fin}(d)$ iff there is a finitely generated k-module $M \subseteq k[X]$ such that $z \in M$ and M is *d-invariant* (i.e., $dM \subseteq M$).

We say that d is *locally nilpotent* if $\mathrm{Nil}(d) = k[X]$ and *locally finite* if $\mathrm{Fin}(d) = k[X]$.

3.2. Lemma. $\mathrm{Ker}(d) \subseteq \mathrm{Nil}(d) \subseteq \mathrm{Fin}(d)$ *are subalgebras of* $k[X]$.

Proof. The inclusions are obvious. The formula

$$d^m(z_1 z_2) = \sum_{i+j=m} \binom{m}{i} d^i(z_1) d^j(z_2)$$

implies that $\mathrm{Ker}(d)$ and $\mathrm{Nil}(d)$ are subalgebras. If M_1, M_2 are finitely generated and d-invariant, then so are $M_1 + M_2$ and $M_1 M_2 = \{\sum a z_1 z_2 \mid a \in k, z_1 \in M_1, z_2 \in M_2\}$. Hence $\mathrm{Fin}(d)$ is a subalgebra. □

3.3. Theorem. *Suppose that k contains the field* $\mathbf{Q}$ *of rational numbers, and let* φ *be an endomorphism of* $k[X]$ *with* $\mathrm{Jac}(\varphi)$ *invertible. Define derivations* $d_1, \ldots, d_n$ *of* $k[X]$ *by* (2.3). *Then the following are equivalent:*

(i) φ *is invertible.*

(ii) $d_1, \ldots, d_n$ *are locally nilpotent.*

(iii) $d_1, \ldots, d_n$ *are locally finite.*

Proof. Replacing φ by $\varphi\tau$ for a suitable translation $\tau \in \mathrm{Aut}_k\, k[X]$ we can assume that φ preserves the origin. By 2.5, φ is an automorphism of $k[[X]]$. If $\varphi \in \mathrm{Aut}_k\, k[X]$ then $d_i^m = \varphi(\partial/\partial X_i)^m \varphi^{-1}$ (2.4(iii)) shows that d_i is locally nilpotent. Conversely, if the d_i are locally nilpotent then φ^{-1} takes $k[X]$ to $k[X]$ by (2.2). Hence (i) and (ii) are equivalent.

It is clear that (ii) implies (iii). The rest of this section is devoted to the proof of the converse. Assume (iii). By 3.2, a derivation d is locally finite if $X_1, \ldots, X_n \in \mathrm{Fin}(d)$. Using this it is easy to reduce to the case where k is a finitely generated $\mathbf{Q}$-algebra. Let k have nilradical N, and write $k/N = k_1 \times \cdots \times k_r$ where the k_i are domains. Then for each i, $\mathrm{Jac}(\varphi)$ is invertible over k_i and $d_1, \ldots, d_n$ are locally finite over k_i.

3.4. Lemma. *If φ is invertible over each k_i, then φ is invertible over k.*

Proof. If $k_i[f] = k_i[X]$ for each i, then $N(k[X]/k[f]) = k[X]/k[f]$. Since N is nilpotent, $k[X] = k[f]$.

Hence we can assume that k is a domain. By enlarging k we can further reduce to the case where k is an algebraically closed field of characteristic 0.

3.5. Lemma. *Let k be a field of characteristic* 0. *If d is a derivation of $k[X]$, $z \in k[X]$, and $dz = \lambda z$ for some $0 \neq \lambda \in \mathrm{Ker}(d)$ then z is transcendental over* $\mathrm{Nil}(d)$.

Proof. Assume the contrary. Let $a_r z^r + \cdots + a_0 = 0$ be an algebraic equation with $a_r, \ldots, a_0 \in \mathrm{Nil}(d)$ and r minimal. Applying d to this equation gives

$$(da_r + r\lambda a_r)z^r + \cdots + (da_1 + \lambda a_1)z + da_0 = 0.$$

Since $a_0 \in \mathrm{Nil}(d)$, applying d repeatedly we can assume that $a_0 \neq 0$, $da_0 = 0$. Then also $da_i + i\lambda a_i = 0$ by the minimality of r. Since $a_r \in \mathrm{Nil}(d)$, there is m such that $0 = d^m a_r = (-1)^m r^m \lambda^m a_r$, a contradiction.

We now complete the proof of 3.3 by showing that $d_1, \ldots, d_n$ are locally nilpotent. Let $d = d_i$. Suppose M is a finite-dimensional k-vector space such that $dM \subseteq M$. By linear algebra, in order to show that the linear map $d|M$ on M is nilpotent, it suffices to show that the eigenvalues of $d|M$ are zero. Suppose $z \in M$ is an eigenvector of $d|M$, say $dz = \lambda z$ where $\lambda \in k$. Since $k[X]$ is algebraic over $k[f]$ and $k[f] \subseteq \mathrm{Nil}(d)$, z is algebraic over $\mathrm{Nil}(d)$. Then by (3.5), $\lambda = 0$. □

The equivalence of (i) and (ii) in 3.3 also follows directly from the following fact: If d is a derivation in characteristic zero and $d(z) = 1$, then $\mathrm{Nil}(d) = \mathrm{Ker}(d)[z]$. This fact has been noted by several people, see e.g. [2] and [3].

References

[1] H. Bass, E.H. Connell and D. Wright, The Jacobian Conjecture: Reduction of degree and formal expansion of the inverse, Bull. Amer. Math. Soc. 7 (1982) 287–330.

[2] M. Razar, Polynomial maps with constant Jacobian, Israel J. Math. 32 (1979) 97–106.

[3] D. Wright, On the Jacobian Conjecture, Illinois J. Math. 25 (1981) 423–440.