Pacific Journal of Mathematics

CANONICAL FORMS FOR LOCAL DERIVATIONS

Maxwell Alexander Rosenlicht

Vol. 42, No. 3 March 1972

PACIFIC JOURNAL OF MATHEMATICS
Vol. 42, No. 3, 1972

CANONICAL FORMS FOR LOCAL DERIVATIONS

MAXWELL ROSENLICHT

Consider a field k, the formal power series field $k((x))$ in one variable over k, and a derivation D of $k((x))$ that maps k into itself. We wish to replace x by another generator y of $k((x))$ so that Dy has a particularly simple expression as a function of y. This is accomplished subject to certain restrictions on the differential field k, some deductions are drawn, and there are extensions to the analogous problem for power series rings in several variables.

We first consider a derivation D on a noetherian local ring R. If M is the maximal ideal of R, then for any $N = 1, 2, \cdots$ we have $DM^N \subset M^{N-1}$. Thus D is automatically continuous in the natural topological ring structure of R, where a basis for the neighborhoods of zero are the various powers of M.

THEOREM 1. *Let R be a complete noetherian local ring containing $\boldsymbol{Q}$, M the maximal ideal of R and D a derivation of R such that $DM \not\subset M$. Then M has a set of generators $y_1, \cdots, y_n$ such that $Dy_1 = \cdots = Dy_n = 1$.*

There is an element $x \in M$ such that $Dx \notin M$. For any other element $y \in M$, either Dy or $D(x + y)$ is not in M. Since x and y generate the same ideal in R as do x and $x + y$, it follows that M is generated by those of its elements x for which $Dx \notin M$, that is, for which Dx is a unit in R. Now if $x \in M$ and $Dx \notin M$, we have $D(x/Dx) - 1 = xD(1/Dx) \in M$, so that M is generated by those of its elements x satisfying $Dx - 1 \in M$. Since R is noetherian, a finite number of such x's, say $x_1, \cdots, x_n$, will generate M. If we have elements $y_1, \cdots, y_n \in M$ such that $x_i - y_i \in M^2$ for each $i = 1, \cdots, n$ then $y_1, \cdots, y_n$ also generate M, and we shall be done with the proof if we can find such $y_1, \cdots, y_n$ such that $Dy_1 = \cdots = Dy_n = 1$. To do this, we shall show by a successive approximation process that $x_1, \cdots, x_n$ may be replaced by elements which differ from these by elements in successively higher powers of M in such a way that the new $Dx_1 - 1, \cdots, Dx_n - 1$ also belong to high powers of M, and we shall then let each $y_i, i = 1, \cdots, n$, be the limit of the sequence of x_i's thus obtained. Specifically, we are reduced to showing that if $x_1, \cdots, x_n$ generate M and $N \geqq 1$ is an integer such that for each $i = 1, \cdots, n$ we have $Dx_i - 1 \in M^N$, then there exist $z_1, \cdots, z_n \in M^{N+1}$ such that each $D(x_i + z_i) - 1 \in M^{N+1}$. Since $DM^{N+1} \subset M^N$, it suffices to show that the R-module homomorphism induced by D

$$\sum_{\substack{i_1,\cdots,i_n \geqq 0 \\ i_1+\cdots+i_n=N+1}} Rx_1^{i_1}\cdots x_n^{i_n} \longrightarrow M^N/M^{N+1} ,$$

according to which $x_1^{i_1}\cdots x_n^{i_n}$ is mapped into

$$i_1 x_1^{i_1-1}x_2^{i_2}\cdots x_n^{i_n} + \cdots + i_n x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}x_n^{i_n-1} + M^{N+1} ,$$

is surjective. To do this it suffices to show that if $X_1, \cdots, X_n$ are indeterminates then the $\boldsymbol{Q}$-linear map δ from the vector space of forms of degree $N+1$ in $\boldsymbol{Q}[X_1, \cdots, X_n]$ into forms of degree N that is given by

$$\delta(X_1^{i_1}\cdots X_n^{i_n}) = X_1^{i_1}\cdots X_n^{i_n}\left(\frac{i_1}{X_1} + \cdots + \frac{i_n}{X_n}\right)$$

is surjective. For this, we order the set of monomials $X_1^{i_1}\cdots X_n^{i_n}$ of degree N in $\boldsymbol{Q}[X_1, \cdots, X_n]$ lexicographically, setting $X_1^{i_1}\cdots X_n^{i_n} < X_1^{j_1}\cdots X_n^{j_n}$ if, for the smallest $p = 1, \cdots, n$ such that $i_p \neq j_p$, we have $i_p < j_p$. That δ is surjective follows immediately from the remark that if $i_1, \cdots, i_n \geqq 0$, $i_1 + \cdots + i_n = N$, and $q = 1, \cdots, n$ is the largest integer such that $i_q \neq 0$, then $X_1^{i_1}\cdots X_n^{i_n}$ differs from $\delta(X_1^{i_1}\cdots X_n^{i_n}X_q/(i_q+1))$ by a linear combination of monomials that are less than $X_1^{i_1}\cdots X_n^{i_n}$.

COROLLARY. *Under the same conditions as above, there exist generators* $y, z_1, \cdots, z_{n-1}$ *of* M *such that* $Dy = 1$ *and* $Dz_1 = \cdots = Dz_{n-1} = 0$.

To prove this, just set $y = y_1$, $z_1 = y_2 - y_1, \cdots, z_{n-1} = y_n - y_1$.

The case of greatest interest for Theorem 1 is that of a formal power series ring $k[[x_1, \cdots, x_n]]$ in indeterminates $x_1, \cdots, x_n$ over a field k of characteristic zero and a derivation D on this ring that sends k into itself but does not send the maximal ideal M of the ring into itself. Since any set of generators of the maximal ideal M of a noetherian local ring R contains a minimal set of generators, in number $\dim_{R/M} M/M^2$, we see that in the present case new generators $y, z_1, \cdots, z_{n-1}$ may be chosen for M such that our differential ring is the formal power series ring $k[[y, z_1, \cdots, z_{n-1}]]$, with the derivation extended from k by means of $Dy = 1$, $Dz_1 = \cdots = Dz_{n-1} = 0$. We ask what the constants of this ring are, that is, what are the elements to which application of D gives 0? Any element of $k[[y, z_1, \cdots, z_{n-1}]]$ can be uniquely written $\sum_{i=0}^{\infty} f_i(z)y^i$, wher eeach $f_i(z) \in k[[z_1, \cdots, z_{n-1}]]$. Note that D maps $k[[z_1, \cdots, z_{n-1}]]$ into itself and is obtained simply by applying D to the coefficients of the power series, these coefficients being elements of k. We have

$$D\sum_{i=0}^{\infty} f_i(z)y^i = \sum_{i=0}^{\infty}((Df_i(z))y^i + if_i(z)y^{i-1})$$
$$= \sum_{i=0}^{\infty}(Df_i(z) + (i+1)f_{i+1}(z))y^i .$$

Therefore we get $\sum_{i=0}^{\infty} f_i(z)y_i$ constant if and only if for each $i \geqq 0$ we have $Df_i(z) + (i+1)f_{i+1}(z) = 0$. In other words, the constants of $k[[y, z_1, \cdots, z_{n-1}]]$ are the elements of the form

$$\sum_{i=0}^{\infty}(-1)^i\frac{D^i f(z)}{i!}y^i ,$$

for arbitrary $f(z) \in k[[z_1, \cdots, z_{n-1}]]$. The generators $y, z_1, \cdots, z_{n-1}$ of the maximal ideal of $k[[y, z_1, \cdots, z_{n-1}]]$ are of course not unique, but may be altered by adding to each of $y, z_1, \cdots, z_{n-1}$ a constant in M, that is an element of the above form, with $f(z)$ having no term of degree zero, provided the new elements we obtain have their linear terms linearly independent over k.

To prove the next theorem, we shall have to restrict ourselves to differential fields with certain special properties. For this purpose, let us consider briefly an arbitrary ordinary differential field k and a *system of n first order linear differential equations in n unknowns over k*, that is, a system of equations $Dy_i = \sum_{j=1}^{n} a_{ij}y_j + b_i$, $i = 1, \cdots, n$, where each $a_{ij}, b_i \in k$. By a *solution* of this system we of course mean an n-tuple $(y_1, \cdots, y_n)$ of elements of some differential extension field of k satisfying these equations. The totality of solutions in k (that is, solutions with component functions in k), if any, is got as usual by adding to a particular solution an arbitrary solution of the corresponding system of homogeneous differential equations $Dy_i = \sum_{j=1}^{n} a_{ij}y_j$, $i = 1, \cdots, n$, and, as usual, the solutions of the homogeneous system form a vector space over the subfield of constants of k. That this vector space is of dimension at most n is an immediate consequence of the following result.

LEMMA. *Let a_{ij}, $i, j = 1, \cdots, n$, be elements of the differential field k. Then any solutions in k of the system of n first order homogeneous differential equations in n unknowns $Dy_i = \sum_{j=1}^{n} a_{ij}y_j$, $i = 1, \cdots, n$, that are linearly dependent over k are linearly dependent over the subfield of constants of k.*

For suppose that the solutions $z_1 = (y_{11}, \cdots, y_{1n}), \cdots, z_m = (y_{m1}, \cdots, y_{mn})$, with each $y_{ij} \in k$, are linearly dependent over k. We must show that $z_1, \cdots, z_m$ are linearly dependent over the subfield of constants of k. We may suppose that no proper subset of $z_1, \cdots, z_m$ is linearly dependent over k. Choose $c_1, \cdots, c_m \in k$ such that $c_1z_1 + \cdots + c_mz_m =$

0 and suppose, as we may, that $c_1 = 1$. For $i = 1, \cdots, n$ we have $\sum_{p=1}^{m} c_p y_{pi} = 0$, so that

$$\begin{aligned}\sum_{p=1}^{m} c_p D y_{pi} &= \sum_{p=1}^{m} c_p \sum_{j=1}^{n} a_{ij} y_{pj} \\ &= \sum_{j=1}^{n} a_{ij} \sum_{p=1}^{m} c_p y_{pj} \\ &= 0\,.\end{aligned}$$

Therefore

$$\begin{aligned}0 &= D \sum_{p=1}^{m} c_p y_{pi} \\ &= \sum_{p=1}^{m} (Dc_p) y_{pi} + \sum_{p=1}^{m} c_p D y_{pi} \\ &= \sum_{p=1}^{m} (Dc_p) y_{pi}\,.\end{aligned}$$

Since $c_1 = 1$, we have $\sum_{p=2}^{m} (Dc_p) y_{pi} = 0$ for $i = 1, \cdots, n$, or $\sum_{p=2}^{m} (Dc_p) z_p = 0$. Since $z_2, \cdots, z_m$ are linearly independent over k, we have $Dc_p = 0$ for $p = 2, \cdots, m$. Hence $c_1, \cdots, c_m$ are constant. Recalling that $\sum_{p=1}^{m} c_p z_p = 0$ completes the proof.

We say that the system of equations $Dy_i = \sum_{j=1}^{n} a_{ij} y_j + b_i$, $i = 1, \cdots, n$, *has a full set of solutions in* k if it has a particular solution in k and if the corresponding system of homogeneous equations $Dy_i = \sum_{j=1}^{n} a_{ij} y_j$, $i = 1, \cdots, n$, has n solutions in k that are linearly independent (over k or over its subfield of constants). It is worth mentioning the following result, which we shall not use, a result that is an easy consequence of standard facts: The system of equations $Dy_i = \sum_{j=1}^{n} a_{ij} y_j + b_i$, $i = 1, \cdots, n$, with coefficients a_{ij}, b_i in the differential field k, has a full set of solutions in some finitely generated differential extension field of k whose subfield of constants is algebraic over that of k.

THEOREM 2. *Let R be a complete noetherian local ring containing $\boldsymbol{Q}$, M the maximal ideal of R, and D a derivation on R such that $DM \subset M$. Let the differential field $k = R/M$ be such that any system of n first order linear differential equations in n unknowns with coefficients in k has a full set of solutions in k, where $n = \dim_k M/M^2$. Then M has a set of generators $y_1, \cdots, y_n$ such that $Dy_1 = \cdots = Dy_n = 0$.*

The derivation on k is of course that induced by D via the natural surjection $R \to k$. We denote this derivation on k, somewhat incorrectly, by the same letter D. For any $N = 1, 2, \cdots$ we have $DM^N \subset M^N$.

The map D on M induces a map Δ on the k-vector space M/M^2, with $\Delta(m + M^2) = Dm + M^2$ for any $m \in M$. The operator Δ is not k-linear, but it is additive, and it satisfies the relation $\Delta(ax) = (Da)x + a(\Delta x)$ for all $a \in k$, $x \in M/M^2$. Fix a k-basis $\alpha_1, \cdots, \alpha_n$ of M/M^2. Then there exist $a_{ij} \in k$, $i, j = 1, \cdots, n$, such that for each $i = 1, \cdots, n$ we have $\Delta\alpha_i = \sum_{j=1}^n a_{ij}\alpha_j$. For any $u_1, \cdots, u_n \in k$ we have

$$\begin{aligned}\Delta\Big(\sum_{i=1}^n u_i\alpha_i\Big) &= \sum_{i=1}^n \Big((Du_i)\alpha_i + u_i\sum_{j=1}^n a_{ij}\alpha_j\Big) \\ &= \sum_{i=1}^n \Big(Du_i + \sum_{j=1}^n a_{ji}u_j\Big)\alpha_i \,.\end{aligned}$$

By our assumptions on k, there exist n-tuples of elements of k, say $(u_{11}, \cdots, u_{1n}), \cdots, (u_{n1}, \cdots, u_{nn})$, linearly independent over k, such that for each $i, p = 1, \cdots, n$ we have $Du_{pi} + \sum_{j=1}^n a_{ji}u_{pj} = 0$. If we let $\xi_p = \sum_{i=1}^n u_{pi}\alpha_i$, $p = 1, \cdots, n$, then we get $\Delta\xi_1 = \cdots = \Delta\xi_n = 0$ and $\xi_1, \cdots, \xi_n$ is a k-basis of M/M^2. Now choose $x_1, \cdots, x_n \in M$ such that $\xi_i = x_i + M^2$, $i = 1, \cdots, n$. Then $x_1, \cdots, x_n$ is a set of generators for M and $Dx_1, \cdots, Dx_n \in M^2$. We have to show that $x_1, \cdots, x_n$ can be modified so that we still have $\xi_i = x_i + M^2$, $i = 1, \cdots, n$, and in addition have the stronger relations $Dx_1 = \cdots = Dx_n = 0$. To do this it suffices to prove, in virtue of the usual successive approximation argument and the completeness of R, that if $N = 2, 3, \cdots$ and $x_1, \cdots, x_n$ is a set of generators of M such that $Dx_1, \cdots, Dx_n \in M^N$, then there exist $z_1, \cdots, z_n \in M^N$ such that $D(x_1 + z_1), \cdots, D(x_n + z_n) \in M^{N+1}$. To prove this, for each $i = 1, \cdots, n$ write

$$Dx_i = \sum_{\substack{i_1,\cdots,i_n \geqq 0 \\ i_1+\cdots+i_n=N}} a_{ii_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}\,,$$

for certain $a_{ii_1\cdots i_n} \in R$, and try setting

$$z_i = \sum_{\substack{i_1,\cdots,i_n \geqq 0 \\ i_1+\cdots+in=N}} b_{ii_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}\,,$$

with the $b_{ii_1\cdots i_n}$'s elements of R to be determined. Since for each $i = 1, \cdots, n$

$$Dz_i = \sum_{\substack{i_1\cdots,i_n \geqq 0 \\ i_1+\cdots+i_n=N}} (Db_{ii_1\cdots i_n})x_1^{i_1}\cdots x_n^{i_n} \qquad (\text{mod } M^{N+1})\,,$$

we will have $D(x_1 + z_1), \cdots, D(x_n + z_n)$ all in M^{N+1} if, for each $ii_1 \cdots i_n$, we have $a_{ii_1\cdots i_n} + Db_{ii_1\cdots i_n} \in M$. Passing from R to $R/M = k$, we are reduced to the problem of finding elements of k with prescribed derivatives. But that this is always possible is a consequence of the assumption made on k (special case of first order linear differential equations where each $a_{ij} = 0$), except in the case $n = 0$, where the theorem is vacuous.

The case of greatest interest for Theorem 2 is, as for Theorem 1, that of a formal power series ring $k[[x_1, \cdots, x_n]]$ over a field k of characteristic zero in indeterminates $x_1, \cdots, x_n$ and a derivation D on this ring that sends k into itself and each x_i into a power series with no term of degree zero. If the differential field k satisfies the appropriate condition on the solvability of systems of linear differential equations, then new variables $y_1, \cdots, y_n$ may be found such that $k[[x_1, \cdots, x_n]] = k[[y_1, \cdots, y_n]]$ and $Dy_1 = \cdots = Dy_n = 0$. It is easy to compute the subring of constants of this ring. We in fact do this for a slightly more general case, where the variables $y_1, \cdots, y_n$ may satisfy certain analytic relations.

PROPOSITION. *Let k be a differential field and let R be a differential extension ring of k which is a complete noetherian local ring containing nonunits $y_1, \cdots, y_n$ such that $R = k + Ry_1 + \cdots + Ry_n$ and $Dy_1 = \cdots = Dy_n = 0$. Then the constants of R are just the subring $C[[y_1, \cdots, y_n]]$, where C is the subfield of constants of k.*

Clearly each formal power series in $y_1, \cdots, y_n$ with coefficients in C is a constant. Suppose conversely that $x = \sum_{i_1,\cdots,i_n \geqq 0} a_{i_1\cdots i_n} y_1^{i_1} \cdots y_n^{i_n}$, with each $a_{i_1\cdots i_n}$ in k, is such that $Dx = 0$. We would like to know that this power series representation for x has the property that for each $N = 1, 2, 3, \cdots$, if we consider the various $i_1, \cdots, i_n \geqq 0$ such that $i_1 + \cdots + i_n = N$ and $a_{i_1\cdots i_n} \neq 0$, then the various elements $y_1^{i_1} \cdots y_n^{i_n} \in M^N$ are actually linearly independent over k modulo M^{N+1}. This property of the representation of our given x is not necessarily true to begin with, but working successively with $N = 1, N = 2, \cdots$ we can modify the $a_{i_1\cdots i_n}$'s so as to make this property valid. This being so, we can prove by induction on $N = 0, 1, 2, \cdots$ that all the coefficients $a_{i_1\cdots i_n}$ of the power series representation of x are in C, as follows. This fact is clear for $N = 0$, and if for a certain $N > 0$ we know that each nonzero $a_{i_1\cdots i_n}$ is a constant whenever $i_1 + \cdots + i_n < N$, then the congruence

$$Dx \equiv \sum_{i_1+\cdots+i_n=N} (Da_{i_1\cdots i_n}) y_1^{i_1} \cdots y_n^{i_n} \qquad (\text{mod } M^{N+1})$$

shows that $Da_{i_1\cdots i_n} = 0$ if $i_1 + \cdots + i_n = N$. Thus each $a_{i_1\cdots i_n}$ is in C.

A rather stringent condition is imposed on k in the statement of Theorem 2. That some such condition is necessary can be seen from the example of the formal power series ring $R = k[[x]]$, where the differential field k contains an element a that is not of the form $-Db/b$ for any $b \in k$ and the derivation D on k is extended to R by setting $Dx = ax$. Any other generator of the ideal Rx is of the form $y = b_1x + b_2x^2 + \cdots$, with $b_1, b_2, \cdots \in k, b_1 \neq 0$, and if $Dy = 0$ we get $Db_1 + b_1a = 0$, which is impossible. Or we may obtain a similar counterexample, verified by a similar argument, by supposing k to contain an element a which is not the derivative of any element of k and then extending the derivation D on k to one on $k[[x]]$ by setting $Dx = ax^2$.

The remainder of this paper will consider extensions of the derivation on a differential field k of characteristic zero to the formal power series field $k((x))$, the field of quotients of the formal power series ring in one variable $k[[x]]$. We begin with a number of well-known remarks. First of all, $k((x))$ has a natural topological field structure, depending only on its field structure and inducing the usual topology on $k[[x]]$, since the maximal ideal $k[[x]]x$ of $k[[x]]$ can be characterized as the set of all $u \in k((x))$ such that, given any $v \in k((x))$, there exists an integer $n > 0$ such that $1 + u^nv$ has an mth root in $k((x))$ for an infinite number of positive integers m, and $k[[x]]$ is the set of all elements of $k((x))$ not having a reciprocal in $k[[x]]x$. Any nonzero $u \in k((x))$ has an *order*, denoted $\operatorname{ord} u$, which is that integer m such that we can write $u = \sum_{n \geq m} a_nx^n$, with each $a_n \in k$ and $a_m \neq 0$, and $\operatorname{ord} u$ does not depend on x. The element x which, together with k, "generates" $k((x))$ is certainly not unique, since it can be replaced by any other element of order one. The field k is of course determined to within isomorphism as the field $k[[x]]/k[[x]]x$, but k is not necessarily determined as a subfield of $k((x))$; for example if $k = k_0(a)$, where k_0 is a subfield of k and a is transcendental over k_0, then $k_0(a + x)$ could replace k.

We shall be interested in derivations of $k((x))$ that map k into itself and are continuous. Such a derivation is given by

$$D(\sum_{n \geq m} a_nx^n) = \sum_{n \geq m} ((Da_n)x^n + na_nx^{n-1}Dx) ,$$

for any $\{a_n\}_{n \geq m} \subset k$. The derivation D is completely determined by its action on k and the knowledge of Dx, which can be an arbitrary element of $k((x))$. If we note that for any such D the set $\{\operatorname{ord} Du - \operatorname{ord} u : u \in k((x)), u \neq 0, Du \neq 0\}$ is bounded from below, we see that there exist derivations D of $k((x))$ that map k into itself and are *not* continuous, got for example by taking a transcendence basis $\{u_\alpha\}_{\alpha \in A}$ for $k((x))$ over k and defining each Du_α to be some specific element of $k((x))$, subject to the condition that the set $\{\operatorname{ord} Du_\alpha - \operatorname{ord} u_\alpha\}_{\alpha \in A}$ is not bounded from below. (We remark that we use here the well-known fact that $k((x))$ has infinite transcendence degree over k. This can be shown by a cardinality argument if k is at most countable and then easily extended to any k, but it may be worth mentioning that an easy differential-algebraic proof of this fact can be based on the well-known and elementary result that if k is a differential field of characteristic zero and K a differential extension field of k having the same subfield of constants, then elements of K whose derivatives are in k are algebraically dependent over k if and only if a linear combination of them with constant coefficients not all zero is in k. For using the continuous derivation D on $k((x))$ that is given by $Dk = 0$, $Dx = 1$, we see that the power series for $\{\log(1 + ax)\}_{a \in k, a \neq 0}$ are algebraically independent over the subfield $k(x)$ of $k((x))$ since no nontrivial linear combination with coefficients in k of their derivatives $\{a/(1 + ax)\}$ is the derivative of an element of $k(x)$. Or we may use the well-known result that if k and K are as above then elements of K whose logarithmic derivatives are in k are algebraically dependent over k if and only if a nontrivial power product of these elements is in k to show that the power series for $e^x, e^{x^2}, e^{x^3}, \cdots$ are algebraically independent over $k(x)$.)

The following two theorems concern the classification of continuous derivations of $k((x))$ that map k into itself. The analogous problem for derivations of the field of quotients $k((x_1, \cdots, x_n))$ of the formal power series ring $k[[x_1, \cdots, x_n]]$, where $Dx_1, \cdots, Dx_n$ are quite arbitrary, seems considerably more difficult. Note the slight overlap (the case $r = 0$) of the next result with Theorem 1.

THEOREM 3. *Let k be a field of characteristic zero, D a continuous derivation of the formal power series field $k((x))$ that maps k into itself and does not send the maximal ideal of $k[[x]]$ into itself. Then there exists a unique nonnegative integer r and an element $y \in k((x))$ of order one (so that $k((x)) = k((y))$) such that $Dy = ay^{-r}$, for some nonzero $a \in k$. The element a is unique to within multiplication by $(r + 1)^{\text{th}}$ powers of nonzero elements of k, and for given a the element y is unique to within multiplication by an $(r + 1)^{\text{th}}$ root of unity in k.*

We must have $\operatorname{ord} Dx \leqq 0$, for otherwise $D(k[[x]]x) \subset k[[x]]x$. Hence we can write $Dx = ax^{-r}(1 + \sum_{n=1}^{\infty} a_n x^n)$, with r a nonnegative integer and $a, a_1, a_2, \cdots \in k$, $a \neq 0$. The $k[[x]]$-module generated by $D(k[[x]])$ is $k[[x]]x^{-r}$, proving that r is unique. Any element $y \in k((x))$ of order one is of the form $y = bx(1 + \sum_{n=1}^{\infty} b_n x^n)$, with $b, b_1, b_2, \cdots \in k$, $b \neq 0$. The leading term of the power series for Dy is bax^{-r}, so that $Dy - b^{r+1}ay^{-r} \in k[[x]]x^{1-r} = k[[y]]y^{1-r}$. Thus the transition from x to y multiplies a by b^{r+1}. It is now immediate that the existence of a special $y \in k((x))$ with the property prescribed in the statement of the theorem and also the uniqueness statements about a and y will all be known if it can be shown that there exist unique $b_1, b_2, \cdots \in k$ such that if $y = x(1 + \sum_{n=1}^{\infty} b_n x^n)$ then $Dy = ay^{-r}$. For this particular y we have

$$\begin{aligned} Dy &= D\Big(x + \sum_{n=1}^{\infty} b_n x^{n+1}\Big) \\ &= \sum_{n=1}^{\infty} (Db_n) x^{n+1} + \Big(1 + \sum_{n=1}^{\infty} (n+1) b_n x^n\Big) a x^{-r} \Big(1 + \sum_{n=1}^{\infty} a_n x^n\Big) , \end{aligned}$$

which we want to equal

$$ay^{-r} = ax^{-r}\Big[1 - \Big(\sum_{n=1}^{\infty} b_n x^n\Big) + \Big(\sum_{n=1}^{\infty} b_n x^n\Big)^2 - \cdots\Big]^r .$$

The condition we need is therefore

$$\begin{aligned} &a^{-1} \sum_{n=1}^{\infty} (Db_n) x^{n+r+1} + \Big(1 + \sum_{n=1}^{\infty} (n+1) b_n x^n\Big)\Big(1 + \sum_{n=1}^{\infty} a_n x^n\Big) \\ &= \Big[1 - \Big(\sum_{n=1}^{\infty} b_n x^n\Big) + \Big(\sum_{n=1}^{\infty} b_n x^n\Big)^2 - \cdots\Big]^r . \end{aligned}$$

Both sides of this last equation have constant term 1. For any integer $m > 0$, the coefficient of x^m on the left is $a^{-1}Db_{m-r-1} + (m + 1)b_m + mb_{m-1}a_1 + \cdots + 2b_1 a_{m-1} + a_m$ (understanding b_n to be 0 if $n < 1$), while the coefficient of x^m on the right hand side is $- rb_m +$ (a specific polynomial in $b_1, \cdots, b_{m-1}$ with integer coefficients). Therefore by letting $m = 1, 2, 3, \cdots$ we successively find $b_1, b_2, \cdots \in k$ such that $Dy = ay^{-r}$, and we see that these $b_1, b_2, \cdots$ are unique.

COROLLARY. *If y is as above, the constants of $k((x)) = k((y))$ are precisely the elements of the form*

$$c - \frac{a^{-1}Dc}{r+1} y^{r+1} + \frac{(a^{-1}D)^2 c}{(r+1)^2 2!} y^{2(r+1)} - \frac{(a^{-1}D)^3 c}{(r+1)^3 3!} y^{3(r+1)} + \cdots, c \in k .$$

For any subset $\{c_n\}_{n \in Z}$ of k such that $c_n = 0$ if n is sufficiently small, we have

$$\begin{aligned} D(\textstyle\sum c_n y^n) &= \textstyle\sum ((Dc_n) y^n + n c_n a y^{n-1-r}) \\ &= \textstyle\sum (Dc_{n-r-1} + nac_n) y^{n-r-1} . \end{aligned}$$

Therefore for $\sum c_n y^n$ to be constant it is necessary and sufficient that $Dc_{n-r-1} + nac_n = 0$ for all n, that is that $c_n = - Dc_{n-r-1}/(na)$ if $n \neq 0$ and c_{-r-1} be a constant of k. Therefore we must have $c_n = 0$ if $n < 0$ or $n \not\equiv 0(\mathrm{mod}\,(r + 1))$, and the corollary follows directly, with $c = c_0$.

If we have a derivation of $k((x))$ that sends both the field k and the maximal ideal of $k[[x]]$ into themselves, then this derivation is automatically continuous and is the extension to $k((x))$ of a derivation of $k[[x]]$. Theorem 2 is directly applicable if the differential equations $Dy = ay$ and $Dy = a$ have solutions in k for any $a \in k$. For a quite general differential field k, where this condition is not necessarily satisfied, nothing much can be said. However, complete information is also available in the special but important case in which the derivation on k is trivial.

THEOREM 4. *Let k be a field of characteristic zero, D a nonzero derivation of the formal power series ring in one variable $k[[x]]$ that is trivial on k and maps the maximal ideal of $k[[x]]$ into itself. For any $y \in k[[x]]$ of order one we can write $Dy = y^r/\sum_{n=0}^{\infty} a_n y^n$, with $r \geqq 1$ an integer, $a_0, a_1, \cdots \in k$, and $a_0 \neq 0$. Here r and a_{r-1} are uniquely determined by D, independent of the choice of y, and a_0 is determined to within multiplication by the $(r-1)^{\text{th}}$ power of a nonzero element of k. If $r > 1$ then y can be chosen such that $Dy = y^r/(a + cy^{r-1})$, with $a, c \in k$. If $r = 1$ then y can be chosen such that $Dy = y/a$ with $a \in k$, and here y is unique to within multiplication by a nonzero element of k.*

Let us write $Dx = x^r/\sum_{n=0}^{\infty} \alpha_n x^n$, with r an integer and $\alpha_0, \alpha_1, \cdots \in k$, $\alpha_0 \neq 0$. Then any $y \in k[[x]]$ of order one is of the form $y = bx(1 + \sum_{n=1}^{\infty} b_n x^n)$ with $b, b_1, b_2, \cdots \in k$, $b \neq 0$. Since $y \equiv bx \pmod{k[[x]]x^2}$ we have $Dy \equiv \alpha_0^{-1} b^{1-r} y^r \pmod{k[[x]]x^{r+1}}$, which shows that Dy is of the form $Dy = y^r/\sum_{n=0}^{\infty} a_n y^n$, with $a_0, a_1, \cdots \in k$, $a_0 = \alpha_0 b^{r-1}$. In particular, r is unique. Since D maps $k[[x]]x$ into itself, we have $r \geqq 1$. In the special case where $y = bx$, we verify immediately that $a_n = \alpha_n b^{r-n-1}$, $n = 0, 1, 2, \cdots$. To complete the proof of the theorem it suffices to show that if we restrict ourselves to the case $b = 1$, that is $y = x(1 + \sum_{n=1}^{\infty} b_n x^n)$, then $a_{r-1} = \alpha_{r-1}$ and, furthermore, that there exist certain $b_1, b_2, \cdots \in k$, unique if $r = 1$, such that we have $a_n = 0$ for all $n \neq 0, r-1$. Working out Dy in two ways we get

$$Dy = \frac{y^r}{\sum_{n=0}^{\infty} a_n y^n} = \left(1 + \sum_{n=1}^{\infty} (n+1) b_n x^n\right) \frac{x^r}{\sum_{n=0}^{\infty} \alpha_n x^n},$$

so that the α_n's and a_n's are related by the identity

$$\sum_{n=0}^{\infty} \alpha_n x^n = \frac{\left(1 + \sum_{n=1}^{\infty} (n+1) b_n x^n\right)\left(\sum_{n=0}^{\infty} a_n x^n \left(1 + \sum_{N=1}^{\infty} b_N x^N\right)^n\right)}{\left(1 + \sum_{n=1}^{\infty} b_n x^n\right)^r}.$$

Comparison of terms of degree zero gives $a_0 = \alpha_0$, which we already know. To show that $a_{r-1} = \alpha_{r-1}$ it suffices to show that for each integer $m = 0, 1, 2, \cdots$ the coefficient of x^{r-1} in the power series expansion of

$$\left(1 + \sum_{n=1}^{\infty} (n+1) b_n x^n\right) x^m \left(1 + \sum_{N=1}^{\infty} b_N x^N\right)^{m-r} \text{is 1 if } m = r-1 ,$$

otherwise 0. But this last power series is $x^r y^{m-r} y'$, where $'$ refers to formal differentiation with respect to x. If $m \neq r-1$ this power series is $x^r (y^{m-r+1})'/(m-r+1)$, and the coefficient of x^{r-1} must be zero since the derivative with respect to x of a formal power series in x has no term in x^{-1}. On the other hand if $m = r-1$ the coefficient of x^{r-1} in $x^n y'/y$ is clearly 1. So it remains only to show that by a suitable choice of $b_1, b_2, \cdots$, unique if $r = 1$, we can get all a_n's except a_0 and a_{r-1} to be zero. Now for any integer $m > 0$ the coefficient of x^m in the right hand side of the last displayed equation is

$$a_m + (\text{a specific polynomial in } a_0, \cdots, a_{m-1}, b_1, \cdots, b_{m-1} \\ \text{with integer coefficients}) + (m+1-r) b_m$$

and this should equal α_m. Letting $m = 1, 2, \cdots, r-2$ we successively get the values of $b_1, \cdots, b_{r-2}$ for which $a_1 = \cdots = a_{m-2} = 0$, and they are unique. We already know that $a_{r-1} = \alpha_{r-1}$. We can now choose b_{r-1} to be an arbitrary element of k, except in the case $r = 1$ where there is no b_{r-1} to worry about, and we then successively get unique $b_r, b_{r+1}, \cdots$ in k such that $a_r = a_{r+1} = \cdots = 0$. This completes the proof. Note that if $r > 1$, then for fixed $a_0, a_{r-1} \in k$ with $a_0 \neq 0$ there are many possibilities for our y of order one such that $Dy = y^r/(a_0 + a_{r-1} y^{r-1})$, all given by replacing y by $\gamma y(1 + \sum_{n=r-1}^{\infty} b_n y^n)$, with γ any $(r-1)^{\text{th}}$ root of unity in k, b_{r-1} an arbitrary element of k, and b_r, $b_{r+1}, \cdots$ polynomial functions of b_{r-1}.

In the last theorem, and also in Theorem 3 if it happens that $Dk = 0$, we can write $D = f(x) d/dx$, with $f(x) \in k((x))$. In the duality between the one dimensional vector spaces over $k((x))$ of continuous k-derivations and k-differentials of $k((x))$, the basis for the space of differentials that is dual to the basis D for the space of derivations is $dx/f(x)$. We have therefore also derived canonical forms for the nonzero k-differentials of $k((x))$, and these are of the type $y^r dy/a$ for $r \geqq 0$, $a\,dy/y$, and $((a/y^r) + (c/y))dy$ for $r > 1$, with $a, c \in k, a \neq 0$. Note that the invariance of a_{r-1} is simply the invariance of the residue of $dx/f(x)$. Note also that in these cases the constant subfield of $k((x))$ for the derivation D is the same as that for the derivation d/dx, which is just k.

One can verify that if the k of Theorem 3 or 4 is the field of complex numbers (with trivial derivation) and the derivation D on $k((x))$ is such that Dx is a convergent power series in x, then the y of order one for which Dy is in canonical form can be chosen to be a convergent power series in x. The analogous comment applies to the application of Theorem 1 to the formal power series ring $k[[x_1, \cdots, x_n]]$: if $Dx_1, \cdots, Dx_n$ are convergent power series, we can get $y_1, \cdots, y_n$ to be convergent power series in $x_1, \cdots, x_n$.

Received April 3, 1972. Research supported by National Science Foundation grant number GP-20532A.

UNIVERSITY OF CALIFORNIA, BERKELEY

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. The editorial "we" must not be used in the synopsis, and items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. **39**. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is \$8.00; single issues, \$3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$4.00 per volume; single issues \$1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics

Vol. 42, No. 3 March, 1972

Catherine Bandle, *Extensions of an inequality by Pólya and Schiffer for vibrating membranes* 543
S. J. Bernau, *Topologies on structure spaces of lattice groups* 557
Woodrow Wilson Bledsoe and Charles Edward Wilks, *On Borel product measures* 569
Eggert Briem and Murali Rao, *Normpreserving extensions in subspaces of $C(X)$* 581
Alan Seymour Cover, *Generalized continuation* 589
Larry Jean Cummings, *Transformations of symmetric tensors* 603
Peter Michael Curran, *Cohomology of finitely presented groups* 615
James B. Derr and N. P. Mukherjee, *Generalized quasicenter and hyperquasicenter of a finite group* 621
Erik Maurice Ellentuck, *Universal cosimple isols* 629
Benny Dan Evans, *Boundary respecting maps of 3-mainfolds* 639
David F. Fraser, *A probabilistic method for the rate of convergence to the Dirichlet problem* 657
Raymond Taylor Hoobler, *Cohomology in the finite topology and Brauer groups* 667
Louis Roberts Hunt, *Locally holomorphic sets and the Levi form* 681
B. T. Y. Kwee, *On absolute de la Vallée Poussin summability* 689
Gérard Lallement, *On nilpotency and residual finiteness in semigroups* 693
George Edward Lang, *Evaluation subgroups of factor spaces* 701
Andy R. Magid, *A separably closed ring with nonzero torsion pic* 711
Billy E. Rhoades, *Commutants of some Hausdorff matrices* 715
Maxwell Alexander Rosenlicht, *Canonical forms for local derivations* 721
Cedric Felix Schubert, *On a conjecture of L. B. Page* 733
Reinhard Schultz, *Composition constructions on diffeomorphisms of $S^p \times S^q$* 739
J. P. Singhal and H. M. (Hari Mohan) Srivastava, *A class of bilateral generating functions for certain classical polynomials* 755
Richard Alan Slocum, *Using brick partitionings to establish conditions which insure that a Peano continuum is a 2-cell, a 2-sphere or an annulus* 763
James F. Smith, *The p-classes of an H^*-algebra* 777
Jack Williamson, *Meromorphic functions with negative zeros and positive poles and a theorem of Teichmuller* 795
William Robin Zame, *Algebras of analytic functions in the plane* 811