DERIVATIONS AND EMBEDDINGS OF A FIELD IN ITS POWER SERIES RING, II

Nickolas Heerema

1. INTRODUCTION

Let F be a field of characteristic zero, and let π be a derivation on F with values in F. Let F[[x]] be the power series ring in x over F. The mapping

$$a \to \sum_{i=0}^{\infty} \frac{\pi^i(a)\, x^i}{i!} \qquad (a \in F)$$

is an isomorphism of F into F[[x]]. The familiar relation

$$\pi^n(ab) = \sum_{i=0}^{n} C_{n,i}\, \pi^i(a)\, \pi^{n-i}(b)$$

assures that products are preserved. The above example of an embedding of F in F[[x]] is a special case of a theorem of the author's [2, Theorem 4'] which exhibits a biunique correspondence between embeddings of F in $F[[x_1, \cdots, x_n]]$ and sequences of derivations of F into F. The object here is to generalize this result to the case with characteristic p (Theorem 1). The generalization is then used to investigate the question of extending an embedding.

We begin with some definitions. The symbol $F[[x_1, \cdots, x_n]]$ represents the power series ring in n variables $x_1, \cdots, x_n$ over F. Let ξ denote the natural map of $F[[x_1, \cdots, x_n]]$ onto F as residue field. An embedding of F in $F[[x_1, \cdots, x_n]]$ is a field $F' = \phi(F)$, where ϕ is an isomorphism of F into $F[[x_1, \cdots, x_n]]$ such that $\xi\phi$ maps onto all of F. This is equivalent to the condition that ϕ can be extended to an automorphism on $F[[x_1, \cdots, x_n]]$.

Roman capital letters I and J will always denote n-tuples of non-negative integers, $\mathscr{I}^*$ the set of all such n-tuples, and $\mathscr{I}$ the set of all such n-tuples save $Q = (0, \cdots, 0)$.

An *embedding sequence of* F is a set of mappings $\{\bar{\pi}_I\}_{\mathscr{I}}$ whose domain is F, whose range is a commutative ring R containing F, and which satisfy the following conditions for all $I \in \mathscr{I}$ and all a and b in F.

(1) $$\bar{\pi}_I(a + b) = \bar{\pi}_I(a) + \bar{\pi}_I(b)\,,$$

(2) $$\bar{\pi}_I(ab) = \sum_{J \leq I} \bar{\pi}_J(a)\, \bar{\pi}_{I-J}(b)\,.$$

Here, $J \leq I$ if each component of J is less than or equal to the corresponding component of I. The n-tuple I - J is obtained by component-wise subtraction, and $\bar{\pi}_Q$ is

Received September 28, 1960.

This research was supported by N.S.F. Grant G-11292.

the identity map. Henceforth, mappings said to be *on* F are those with F as range and domain, whereas mappings *of* F, as above, have domain F and range R.

Given an embedding $F' = \phi(F)$, where

$$\phi(a) = \sum_{I \in \mathscr{I}^*} a_I x^I \qquad (x^I = x_1^{i_1} \cdots x_n^{i_n}, \text{ where } I = i_1, \cdots, i_n),$$

then the sequence of mappings $\{\bar{\pi}_I\}_{\mathscr{I}}$, where $\bar{\pi}_I(a_Q) = a_I$, is an embedding sequence on F. Conversely, given an embedding sequence $\{\bar{\pi}_I\}_{\mathscr{I}}$ on F, the mapping ϕ given by $\phi(a) = \Sigma_{I \in \mathscr{I}^*} \bar{\pi}_I(a) x^I$ is an isomorphism of F into $F[[x_1, \cdots, x_n]]$. This correspondence between embeddings and embedding sequences is biunique.

H. Hasse and F. K. Schmidt [1] first noted the connection between embedding sequences, which they called differentiations, and isomorphisms. In an adjunct to [1], Schmidt proves Theorems 2 and 3 of the present paper, on the extension of an embedding sequence of F to one of F(t), for the case $n = 1$, by an approach entirely different from that used here.

If F has characteristic zero and $\{\pi_I\}_{\mathscr{I}}$ is a sequence of derivations on F, then the mappings $\bar{\pi}_I$ of an embedding sequence on F can be obtained as simply described symmetric polynomials with rational coefficients in those π_J for which $J \leq I$. Similar functions of the $\bar{\pi}_I$ also yield the original derivations [2, Relations (5') and (7')]. The case where the characteristic is p is quite different. Here there exists no similar functional relationship between derivations and embedding mappings. This fact can be demonstrated by assuming $n = 1$, $p = 3$, and attempting to describe $\bar{\pi}_3$ in terms of π_1, π_2, and a third derivation.

2. EMBEDDINGS OF F IN $F[[x_1, \cdots, x_n]]$

The symbol $[j, I]$ represents the set of all ordered partitions of I into j summands from $\mathscr{I}^*$, $|I|$ denotes the largest integer in I, and kI (k an integer) represents the n-tuple obtained by multiplying each component of I by k. Throughout this section we assume that F has characteristic p.

LEMMA 1. *If* $\{\bar{\pi}_I\}_{\mathscr{I}}$ *is an embedding sequence on* F, *then for all* I *and* J *in* $\mathscr{I}$ *such that* $|J| < p$, *we have*

$$\bar{\pi}_{pI}(a^p) = [\bar{\pi}_I(a)]^p \tag{3}$$

and

$$\bar{\pi}_{pI+J}(a^p) = 0. \tag{4}$$

Proof. By condition 2, we have

$$\pi_{pI+J}(a^p) = \sum_{(I_1, \cdots, I_p) \in [p, pI+J]} \bar{\pi}_{I_1}(a) \cdots \bar{\pi}_{I_p}(a). \tag{5}$$

Each term on the right side of (5) occurs $(r_1, \overset{p}{\cdots}, r_p)$ times, where the r_i represents the multiplicities of the distinct I_j occurring in $I_1, \cdots, I_p$. Clearly, if $J \neq Q$, p divides $(r_1, \overset{p}{\cdots}, r_p)$; and if $J = Q$, the only term with non-zero coefficient is $[\bar{\pi}_I(a)]^p$, in which case the coefficient is one.

Let S be a p-basis for F. (For a discussion of p-bases and derivations, see [3].) Let $\mathcal{F}$ represent the set of all functions f whose domain is the cartesian product of $\mathcal{I}$ and S and whose range is R. It is well known that there exists one and only one derivation of F with prescribed images for the elements of a p-basis. Thus, with each $f \in \mathcal{F}$ there is associated a biuniquely determined sequence of derivations $\{\pi_I\}_{\mathcal{I}}$ given by the condition $\pi_I(e) = f(I, e)$ for all e in S. In the proof of Theorem 1, we shall show that f also biuniquely determines an embedding sequence $\{\bar{\pi}_I\}_{\mathcal{I}}$ by the condition $\bar{\pi}_I(e) = f(I, e)$ for all e in S.

THEOREM 1. *Let* $\{\pi_I\}_{\mathcal{I}}$ *be a sequence of derivations of the field* F *and let* S *be a* p-*basis for* F. *There exists a unique embedding sequence* $\{\bar{\pi}_I\}_{\mathcal{I}} = \mathcal{E}\{\pi_I\}_{\mathcal{I}}$ *of* F *which satisfies the condition*

$$\bar{\pi}_I(e) = \pi_I(e) \tag{6}$$

for all $e \in S$ *and* $I \in \mathcal{I}$. *Moreover, the mapping* $\mathcal{E}$ *is a one-to-one correspondence between the set of all sequences of derivations of* F *and the set of all embedding sequences of* F.

Proof. If the sum of the integers in I is 1, then $\bar{\pi}_I$ is a derivation. Proceeding by induction, we assume the theorem to hold for sequences $\{\pi_I\}_{I<J}$ and sequences $\{\bar{\pi}_I\}_{I<J}$.

Let $\bar{\pi}_J$ be defined on F^p, the subfield of p^{th} powers in F, by (3) or (4), whichever applies. Conditions (1) and (2) are then satisfied by $\{\bar{\pi}_I\}_{I\leq J}$ on F^p. Let $\bar{\pi}_J(e) = \pi_J(e)$ for all e in S. If $a = a_1^p e_1^{n_1} \cdots e_1^{n_s}$, where the e_i are different elements of S and $0 \leq n_i < p$ for each i, we define

$$\bar{\pi}_J(a) = \sum_{(I_0,\cdots,I_r)\in[r+1,J]} \pi_{I_0}(a_1^p)\,\pi_{I_1}(e_1)\cdots\pi_{I_r}(e_s), \tag{7}$$

where $r = n_1 + \cdots + n_s$ and each e_i appears n_i times in the product. The representation of a in the above form is unique except for insertion or deletion of factors e_i^0; such factors do not change the right side of (7). Thus the definition is unambiguous.

CONTENTION 1. *Relation* (2) *holds for* a *as above and* $b = b_1^p e_1^{m_1} \cdots e_s^{m_s}$, *where* $n_i + m_i < p$, *for* $i = 1, \cdots, s$.

This is easily verified because of the structure of the right side of (7) and the induction assumption.

CONTENTION 2. *Equation* (7) *remains valid even if the conditions* $n_i < p$ *are dropped.*

Proof of Contention 2. From Contention 1 it can be seen that Contention 2 will follow if we can prove that, for each e in S and each $m = pq + n$ with $0 \leq n < p$, we have

$$\bar{\pi}_J(e^{pq+n}) = \sum_{(I_1,\cdots,I_m)\in[m,J]} \bar{\pi}_{I_1}(e)\cdots\bar{\pi}_{I_m}(e); \tag{8}$$

that is, we must show that

(9) $$\sum_{(I_0,\cdots,I_n)\in[n+1,J]} \bar{\pi}_{I_0}(e^{qp})\,\pi_{I_1}(e)\cdots\bar{\pi}_{I_n}(e)$$

equals the right side of (8). But $\bar{\pi}_{I_0}(e^{qp})$ was defined by (3) or (4) in the case $I_0 = J$; and by the inductive assumption, $\bar{\pi}_{I_0}$ satisfies (2) when $I_0 < J$. By the proof of formulas (3) and (4) (when $I_0 = J$) or by the generalization of (2) to products of more factors (when $I_0 < J$), we see that

(10) $$\bar{\pi}_{I_0}(e^{qp}) = \sum_{(I_1,\cdots,I_{qp})\in[qp,I_0]} \bar{\pi}_{I_1}(e)\cdots\bar{\pi}_{I_{qp}}(e)\,.$$

Substitution of (10) into (9) gives the right side of (8), thus proving Contention 2.

It now follows easily that (2) holds for *all* monomials a and b. Define $\bar{\pi}_J$ for sums of monomials by (1). This proves the existence of at least one $\bar{\pi}_J$ satisfying the conditions of Theorem 1. But (7) is a consequence of (2), and the definition of $\bar{\pi}_J(a_1^p)$ follows from Lemma 1; therefore $\bar{\pi}_J$ is unique. This completes the proof of Theorem 1. (The author is indebted to the referee for suggesting a simplification of the original proof.)

3. EXTENSIONS OF EMBEDDINGS

Given an embedding of F in $F[[x_1, \cdots, x_n]]$, in how many ways can we extend this embedding to an embedding of a simple extension $F' = F(t)$ in $F'[[x_1, \cdots, x_n]]$? This question is answered in terms of embedding sequences by the following. Let t be an element in some containing field of F.

THEOREM 2. *If* t *is transcendental over* F *and* $\{u_I\}_{\mathcal{J}}$ *is any set of elements in in* F(t) *indexed as indicated, then there exists one and only one extension of a given embedding sequence* $\{\bar{\pi}_I\}_{\mathcal{J}}$ *on* F *to an embedding sequence* $\{\bar{\pi}_I'\}_{\mathcal{J}}$ *on* F(t) *such that* $\bar{\pi}_I'(t) = u$.

Proof. Clearly, if the extension $\{\bar{\pi}_I'\}_{\mathcal{J}}$ exists, it is unique. If F has characteristic p, the existence of $\{\bar{\pi}_I'\}_{\mathcal{J}}$ follows from Theorem 1 and the fact that the adjunction of t to a p-basis S of F yields a p-basis for F(t).

If F has characteristic zero, we observe, using the notation of [1], that each derivation π_I' of the sequence $D'\{\bar{\pi}_I'\}_{\mathcal{J}}$ is an extension of the corresponding derivation π_I in the sequence $D'\{\bar{\pi}_I\}_{\mathcal{J}}$. Next we observe the well-known fact that if $u \in F(t)$ and π is a derivation on F, there exists one and only one extension π' of π to F(t) such that $\pi'(t) = u$. We extend π_I by choosing $\pi'(t)$ to be

$$u_I - \sum_{(r,I):r>1} [\pi']_{(r,I)}(t)\,.$$

The resulting sequence of derivations $\{\pi_I'\}_{\mathcal{J}}$ on F(t) yields an embedding sequence $\mathcal{E}'\{\pi_I'\}_{\mathcal{J}}$ with the desired properties.

THEOREM 3. *If* F(t) *is a separable algebraic extension of* F, *an embedding sequence* $\{\bar{\pi}_I\}_{\mathcal{J}}$ *on* F *can be extended, and in only one way, to an embedding sequence* $\{\bar{\pi}_I'\}_{\mathcal{J}}$ *on* F(t).

Proof. If F has characteristic p, the result follows from the fact that if S is a p-basis for F it is also a p-basis for F(t). If F has characteristic zero, we appeal to the fact that a derivation π on F has one and only one extension to F(t).

THEOREM 4. *If* F *has characteristic* p *and* t *is a root of the irreducible equation* $x^p - a = 0$ *over* F, *an embedding sequence* $\{\bar{\pi}_I\}_{\mathcal{J}}$ *on* F *can be extended to an embedding sequence* $\{\bar{\pi}_I{}'\}_{\mathcal{J}}$ *on* F(t) *if and only if* $\bar{\pi}_{pI}(a) \in F^p(a)$ *for all* I *and* $\bar{\pi}_J(a) = 0$ *for all* J *not of the form* pI. *If these conditions are fulfilled, the extension is unique and*

$$\bar{\pi}_I{}'(t) = [\bar{\pi}_{pI}(a)]^{1/p}. \tag{11}$$

Proof. The "only if" portion of the theorem follows directly from Lemma 1, as does condition (11) if the extension exists.

Thus, assuming that $\bar{\pi}_I(a)$ satisfies the conditions of the theorem, we define $\{\bar{\pi}_I{}'\}_{\mathcal{J}}$ on F(t) as follows.

a) $$\bar{\pi}_I{}'(c) = \bar{\pi}_I(c) \quad \text{for } c \text{ in } F.$$

b) $$\bar{\pi}_I{}'(t^r) = [\bar{\pi}_{pI}(a^r)]^{1/p} \quad \text{for } 0 < r < p.$$

c) $$\bar{\pi}_I{}'(ct^r) = \sum_{J \leq I} \bar{\pi}_J{}'(c)\,\bar{\pi}_{I'-J}(t^r) \quad \text{for } c \text{ in } F \text{ and } 0 < r < p.$$

d) $$\bar{\pi}_I{}'(c_0 + c_1 t + \cdots + c_{p-1}t^{p-1}) = \bar{\pi}_I{}'(c_0) + \bar{\pi}_I{}'(c_1 t) + \cdots + \bar{\pi}_I{}'(c_{p-1}t^{p-1}) \quad \text{for } c_i \text{ in } F.$$

The mapping $\bar{\pi}_I{}'$ as defined is a single-valued additive mapping of F(t) into F(t). we need to verify condition (2). First we note that, for positive integers r and s less than p,

$$\begin{aligned}\sum_{J \leq I} \bar{\pi}_{I'}(t^r)\,\bar{\pi}_{I'-J}(t^s) &= \sum_{J \leq I} [\bar{\pi}_{pJ}(a^r)]^{1/p}[\bar{\pi}_{p(I-J)}(a^s)]^{1/p} \\ &= \sum_{pJ \leq pI} [\bar{\pi}_{pJ}(a^r)\,\bar{\pi}_{p(I-J)}(a^s)]^{1/p} = [\bar{\pi}_{pI}(a^{r+s})]^{1/p}.\end{aligned} \tag{12}$$

If $r + s < p$, then (12) is equal to $\pi_I(t^{r+s})$. If $r + s = p + k$, then (12) is

$$\sum_{pJ \leq pI} [\pi_{pJ}(a^p)]^{1/p}[\pi_{p(I-J)}(a^k)]^{1/p} = \sum_{J \leq I} \bar{\pi}_J(a)\,\bar{\pi}_{I-J}(t^k) = \bar{\pi}_I(at^k).$$

From these observations it follows directly that condition (2) is satisfied by the sequence of mappings $\{\bar{\pi}_I{}'\}_{\mathcal{J}}$ on F(t). The uniqueness of the extended embedding sequence is immediate.

We conclude with a proposition which follows from Theorems 2 and 3, by a standard proof based on Zorn's Lemma.

COROLLARY. *If* K *is separably generated over* F, *then every embedding sequence on* F *can be extended to an embedding sequence on* K.

REFERENCES

1. H. Hasse and F. K. Schmidt, *Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten,* J. Reine Angew. Math. 177 (1937), 215-237.

2. N. Heerema, *Derivations and embeddings of a field in its power series ring,* Proc. Amer. Math. Soc. 11 (1960), 188-194.

3. O. Zariski and P. Samuel, *Commutative algebra,* vol. 1, Van Nostrand, Princeton, 1958.

Florida State University