TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 180, June 1973

HIGHER DERIVATIONS AND FIELD EXTENSIONS

BY

R. L. DAVIS

ABSTRACT. Let K be a field having prime characteristic p. The following conditions on a subfield k of K are equivalent: (i) $\bigcap_n K^{p^n}(k) = k$ and K/k is separable. (ii) k is the field of constants of an infinite higher derivation defined in K. (iii) k is the field of constants of a set of infinite higher derivations defined in K. If K/k is separably generated and k is algebraically closed in K, then k is the field of constants of an infinite higher derivation in K. If K/k is finitely generated then k is the field of constants of an infinite higher derivation in K if and only if K/k is regular.

Introduction. The relationship between field extensions and derivations was investigated by Baer [1] in 1927. Baer obtained a characterization of those subfields k of the field K that are the fields of constants of derivations defined in K. In the prime characteristic case it was found that k is the field of constants of a nonzero derivation defined in K if and only if K/k is a purely inseparable extension having exponent one. Later Weisfield [7] generalized this result to finite higher derivations and purely inseparable extensions having higher exponent. The works of Weisfield [7] and Sweedler [6] yield the following: Let K be a field having prime characteristic. The following conditions on a subfield k of K are equivalent:

(i) K/k is a purely inseparable modular extension with finite exponent.

(ii) k is the field of constants of a finite higher derivation in K.

(iii) k is the field of constants of a set of finite higher derivations in K.

The purpose of this paper is to extend the above results to infinite higher derivations. The following is obtained: Let K be a field having prime characteristic p. The following conditions on a subfield k of K are equivalent:

(i) K/k is separable and $\bigcap_n K^{p^n}(k) = k$.

(ii) k is the field of constants of an infinite higher derivation in K.

(iii) k is the field of constants of a set of infinite higher derivations in K.

A few comments should be made concerning the theory for characteristic zero fields. Baer [1] showed that in this case the subfields of K which are fields of constants of derivations in K are precisely those subfields algebraically closed in K. These subfields are also the fields of constants of the finite and infinite higher derivations in K.

Received by the editors February 22, 1971.

AMS (MOS) subject classifications (1970). Primary 12F10, 12F15.

Key words and phrases. Higher derivation, separable extension, separably generated, regular extension, p-basis.

Preliminaries. All fields considered have prime characteristic p. Separable will mean separable in the linear disjoint sense. Let K be a field.

Definition. An infinite higher derivation in K is a sequence of additive mappings (d_i) of K into itself such that, for all x and y in K and $n = 0, 1, 2, \cdots$

$$d_n(xy) = \sum \{d_i(x)d_j(y) | \; i + j = n\}$$

and d_0 is the identity mapping of K.

The field of constants of a derivation is its kernel and the field of constants of a higher derivation (d_i) is the intersection of the kernels of the d_i for $i \geq 1$. If k is a subfield of the field of constants of the derivation d in K, d is said to be a derivation in K over k. The notation $\mathrm{Der}\,(K/k)$ is adopted for the collection of derivations in K over k and $H(K/k)$ is adopted for the analogous collection of infinite higher derivations in K.

The following results will be needed repeatedly in this paper.

Theorem A [3, p. 181]. *Let S be a p-basis for the field extension K/k and $f\colon S \longrightarrow K$ an arbitrary function. Then there exists a unique derivation d in K over k such that $d(s) = f(s)$ for each $s \in A$.*

Theorem B [2, Theorem 1]. *Let S be a p-basis for the separable field extension K/k and $f\colon \{1, 2, \cdots\} \times S \longrightarrow K$ an arbitrary function. Then there exists a unique higher derivation (d_i) in K over k such that, for each $s \in S$ and $i \in \{1, 2, \cdots\}$, $d_i(s) = f(i, s)$.*

Theorem C [7, p. 436]. *Let (d_i) be a higher derivation in K. Then for each $a \in K$:* (i) $d_{pj}(a^p) = (d_j(a))^p$ *for each $j \geq 1$ and* (ii) $d_j(a^p) = 0$ *if p does not divide j.*

Main result.

Lemma 1. *Let K be a purely trancendental extension of k. Then there exists $d \in \mathrm{Der}\,(K)$ having $k(K^p)$ as field of constants and $(d_i) \in H(K)$ with field of constants k.*

Proof. Let S be a transcendency basis for K/k with $K = k(S)$. If $S = \{s_1, \cdots, s_n\}$ is finite, let $s_0 = 1$ and define $d(s_i) = (s_0 \cdots s_{i-1})^{-1}$ for $1 \leq i \leq n$. Since S is a p-basis for K/k, this defines a unique derivation d in K over k [Theorem A]. Let $0 < m < n$ and $e^{(m)}$ denote the restriction of d to $k(K^p)(s_0, \cdots, s_m)$. We induct on m to show that the field of constants of $e^{(m)}$ is $k(K^p)$ and $(s_0 \cdots s_m)^{-1} \notin \mathrm{Im}\,(e^{(m)})$. If $m = 0$, then the result is clearly true since $e^{(0)}$ is the zero derivation in $k(K^p)$. Thus assume the result for m with $0 < m < n$.

Suppose there are $A_i \in k(K^p)(s_0, \cdots, s_m)$ such that

(1)
$$e^{(m+1)}\left(\sum_0^{p-1} A_i s_{m+1}^i\right) = \sum_0^{p-1} e^{(m)}(A_i) s_{m+1} + \sum_1^{p-1} iA_i s_{m+1}^{i-1} (s_0 \cdots s_m)^{-1} = 0.$$

If $A_i \neq 0$ for some $i \geq 1$, then there exists a $j \geq 0$ such that $A_j \neq 0$ and $e^{(m)}(A_j) = 0$. From (1) we have

(2)
$$e^{(m)}(-A_{j-1}/jA_j) = (s_0 \cdots s_m)^{-1}.$$

This contradicts the induction hypothesis. Thus $A_i = 0$ for each $i \geq 1$ and $A_0 \in k(K^p)$ follows from the induction hypothesis.

Now suppose there are $B_i \in k(K^p)(s_0, \cdots, s_m)$ such that

(3)
$$e^{(m+1)}\left(\sum_0^{p-1} B_i s_{m+1}^i\right) = \sum_0^{p-2} (e^{(m)}(B_i) + B_{i+1}(i+1)(s_0 \cdots s_m)^{-1}) s_{m+1}^i + e^{(m)}(B_{p-1}) s_{m+1}^{p-1} = (s_0 \cdots s_{m+1})^{-1}$$

or

(4)
$$\sum_0^{p-2} (e^{(m)}(B_i) + B_{i+1}(i+1)(s_0 \cdots s_m)^{-1}) s_{m+1}^{i+1} + e^{(m+1)}(B_{p-1} s_{m+1}^p) = (s_0 \cdots s_m)^{-1}.$$

Consequently, $e^{(m)}(B_{p-1} s_{m+1}^p) = (s_0 \cdots s_m)^{-1}$ and this is a contradiction of the induction hypothesis.

If $S = \{s_\alpha\}$ is infinite, well-order it so that there is no last element. Define $d(s_\alpha) = s_{\alpha+1}$ for each $s_\alpha \in S$. This defines a unique derivation in K over k [Theorem A].

Let $A_i \in k(K^p)$ $(\{s \in S \mid s < s_\alpha\})$ and suppose

(5)
$$d\left(\sum_0^{p-1} A_i s_\alpha^i\right) = \sum_0^{p-1} d(A_i) s_\alpha^i + \sum_1^{p-1} iA_i s_\alpha^{i-1} s_{\alpha+1} = 0.$$

Necessarily, $\Sigma_1^{p-1}\, iA_i s_\alpha^{i-1} = 0$ and from this it follows that $A_1 = \cdots = A_{p-1} = 0$. Iteration of the process yields that $A_0 \in k(K^p)$. Thus the field of constants of d is $k(K^p)$.

Since the action of a higher derivation is completely determined by its action on a p-basis [Theorem B], there exists a higher derivation $(d_i) \in H(K/k)$ with $d_1 = d$. Theorem C is used to show that for each $i \geq 1$, the restriction of d_{p^i} to $K^{p^i}(k)$ is a derivation. Since $d_{p^i}(x^{p^i}) = d(x)^{p^i}$ for each $x \in K$, we see that d_{p^i} operates on S^{p^i} in exactly the same manner d operates on S. Since S^{p^i} is a transcendency basis for $K^{p^i}(k)/k$ with $K^{p^i}(k) = k(S^{p^i})$, the field of constants of the restriction of d_{p^i} to $K^{p^i}(k)$ is $K^{p^{i+1}}(k)$. Thus the field of constants of (d_i) is $\bigcap_n K^{p^n}(k) = \bigcap_n k(S^{p^n}) = k$.

Theorem 1. *The following conditions on a subfield k of K are equivalent.*

(i) *K/k is separable and $\bigcap_n K^{p^n}(k) = k$.*

(ii) *k is the field of constants of a higher derivation in K.*

(iii) *k is the field of constants of a set of higher derivations in K.*

Proof. (i) implies (ii). Let S be a p-basis for K/k and T be a p-basis for k. Since $S \cup T$ is a p-basis for K, it is algebraically independent over K_0, the maximal perfect subfield of K. The existence of an $(e_i) \in H(K_0(S \cup T))$ with field of constants $K_0(T)$ is guaranteed by Lemma 1. In the proof of Lemma 1 it was shown that (e_i) can be chosen such that the field of constants of the restriction of e_{p^j} to $K_0(S^{p^j} \cup T)$ is $K_0(S^{p^{j+1}} \cup T)$ for each $j \geq 0$. Take (d_i) to be the unique higher derivation in K agreeing with (e_i) on $S \cup T$. Since (d_i) acts trivially on T, k is a subfield of the field of constants of (d_i). Let U be a linear basis for $K/K_0(S \cup T)$. We note that U^p and hence U^{p^n} for any n is a linear basis for $K/K_0(S \cup T)$. It is easily verified that K^p and $K_0(S \cup T)$ are linearly disjoint over $K_0(S^p \cup T^p)$. Thus U^p is linearly independent over $K_0(S)$ and is a linear basis for $K^p(S \cup T) = K$ over $K_0(S \cup T)$.

Let $x \in K$ and assume $d_i(x) = 0$ for all $i \geq 1$. We show that $x \in K^{p^n}(k)$ for each n and consequently $x \in k$. Fix $n \geq 1$ and let $\{A_i\} \subseteq U$ and $\{a_i\} \subseteq K_0(S \cup T)$ be such that $x = \sum a_i A_i^{p^n}$. For each $1 \leq j < n$ we have

$$d_{p^j}(x) = \sum d_{p^j}(a_i) A_i^{p^n} = \sum e_{p^j}(a_i) A_i^{p^n} = 0. \tag{6}$$

As a consequence of the fact that each $e_{p^j}(a_i) = 0$ we have that each $a_i \in K_0(S^{p^n} \cup T)$ and hence $x \in K^{p^n}(k)$. It now follows that the field of constants of (d_i) is k.

(ii) implies (iii) is clear.

(iii) implies (i). Let H denote a set of higher derivations and suppose k is the field of constants of H. We first show that $\bigcap_n K^{p^n}(k) = k$. Let $x \in K^{p^n}(k)$ and $(d_i) \in H$. Fix $j \geq 1$ and let $p^g > j$. Since $x \in K^{p^g}(k)$, there are A and B in $K^{p^g}[k]$ such that $xB = A$ and $B \neq 0$. We apply d_j to both sides and use Theorem C to obtain that $d_j(x) = 0$.

Now we need to show that K^p and k are linearly disjoint over k^p. If this were not the case, then there would exist a minimal subset of k which is linearly independent over k^p and linearly dependent over K^p. Thus suppose $\{A_i\}$ is such a minimal subset. Then

$$\sum_1^n a_i^p A_i = 0, \quad \{a_i\} \subseteq K, \quad \text{each } a_i \neq 0, \ n > 1. \tag{7}$$

Without loss of generality we may assume $a_1 = 1$ and $a_2 \notin k$. There exists a $(d_i) \in H$ and $j > 0$ such that $d_j(a_2) \neq 0$.

$$d_{pj}\left(A_1 + \sum_2^n a_i^p A_i\right) = \sum_2^n (d_j(a_i))^p A_i = 0. \tag{8}$$

The minimal nature of n is contradicted by (8). Thus K/k is a separable field extension.

Theorem 2. *If K/k is separably generated and k is algebraically closed in K, then there exists an infinite higher derivation in K having field of constants k.*

Proof. Let S be a separating transcendency basis for K/k. An application of Theorem 1 to the field extension $k(S)/k$ yields the existence of a higher derivation (d_i) defined on $k(S)$ having k as field of constants. Since S is a p-basis for K, there is a unique extension of (d_i) to K/k [Theorem B]. We now show that the field of constants of this extension is k. Suppose s is an element of the field of constants of (d_i). Let $f(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_0$ denote the minimal polynomial of s over $k(S)$. If each $f_i \in k$, then s is algebraic over k and we are finished. So suppose some $f_i \notin k$. Thus there exists $q > 0$ such that $d_q(f_i) \neq 0$. We may assume q to be minimal and that $d_j(f_g) = 0$ for each g and each $j < q$.

$$d_q(f(s)) = d_q\left(s^m + \sum_0^{m-1} f_i s^i\right) = \sum_0^{m-1} d_q(f_i)s^i = 0. \tag{9}$$

The polynomial $\sum_0^{m-1} d_q(f_i)x^i$ is nonzero and has degree less than that of the minimal polynomial of s. This is a contradiction. Thus each $f_i \in k$ and hence $s \in k$.

Corollary 1. *If K/k is separably generated and k is algebraically closed in K, then $\bigcap_n K^{p^n}(k) = k$.*

Recall that a field extension K/k is said to be regular if K and $\bar{k}$ are linearly disjoint over k. Regularity is equivalent to K/k being a separable extension and k being algebraically closed in K [4, p. 56]. Thus we have

Corollary 2. *Let K/k be finitely generated. Then k is the field of constants of a higher derivation in K if and only if the extension K/k is regular.*

The following example due to Mac Lane [5] illustrates that the converse of

Theorem 2 is false. Let k be a perfect field and let $T = \{t_0, t_1, \cdots\}$ be algebraically independent over k, define $Y = \{y_2, y_3, \cdots\}$ by $y_n^p = t_{n-2} + t_{n-1}t_n^p$, $n \geq 2$, and let $K = k(T)(Y)$. Then K/k is a separable extension having $\bigcap_n K^{p^n}(k) = k$; however, K/k is not separably generated.

REFERENCES

1. R. Baer, *Algebraische Theorie der differentierbaren Runktionenkorper*. I, S.-B. Heidelberg. Akad. 1927, 15–32.

2. N. Heerema, *Derivations and embeddings of a field in its power series ring*. II, Michigan Math. J. 8 (1961), 129–134. MR 25 #69.

3. N. Jacobson, *Lectures in abstract algebra*. Vol. 3: *Theory of fields and Galois theory*, Van Nostrand, Princeton, N. J., 1964. MR 30 #3087.

4. S. Lang, *Introduction to algebraic geometry*, Interscience, New York, 1958. MR 20 #7021.

5. S. Mac Lane, *Steinitz field towers for modular fields*, Trans. Amer. Math. Soc. 46 (1939), 23–45. MR 1, 3.

6. M. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) 87 (1968), 401–410. MR 36 #6391.

7. M. Weisfeld, *Purely inseparable extensions and higher derivations*, Trans. Amer. Math. Soc. 116 (1965), 435–449. MR 33 #122.

DEPARTMENT OF MATHEMATICS, LOUISIANA STATE UNIVERSITY, BATON ROUGE, LOUISIANA 70803