ITERATIVE HIGHER DERIVATIONS IN FIELDS OF PRIME CHARACTERISTIC

Fredric Zerla

1. INTRODUCTION

Let K be a field having prime characteristic p. The sequence

$$\Pi = \{\pi_i\} \qquad (i = 0, 1, 2, \cdots)$$

of endomorphisms of (K, +), the additive group of K, is called a *higher derivation in* K if and only if π_0 is the identity endomorphism I of (K, +), and if

$$\pi_i(ab) = \sum \{\pi_{i-j}(a)\pi_j(b) \mid 0 \leq j \leq i\}$$

for all a, b $\in$ K. If, in addition, Π satisfies for each a $\in$ K the relation

$$\pi_i \pi_j(a) = \binom{i+j}{i} \pi_{i+j}(a),$$

then Π is called an *iterative higher derivation on* K. F. K. Schmidt [2, Theorems 12 and 13, pp. 235-237] obtained a characterization of all iterative higher derivations in a field K that is separably generated with transcendence degree 1 over a field k. He required k to be contained in the field of constants of Π. The major problem proposed in this paper is to characterize all iterative higher derivations in an arbitrary field K of prime characteristic, by means of a generalization of Schmidt's theorems. It will be shown that in a certain sense each iterative higher derivation is a derivation with respect to an element; this eliminates the need for the cumbersome chain-rule developed by Schmidt. We shall also show that many properties of a higher derivation Π are demonstrated in the action of Π on a p-basis of K, and we shall extend Schmidt's approximation method to arbitrary fields of prime characteristic. Finally, under the restriction that K is finitely and separably generated over a countable field k, we shall characterize the subfields H of K ($k \subseteq H \subseteq K$) that can be the field of constants of an iterative higher derivation on K. They are the algebraically closed subfields over which K is separable.

2. PRELIMINARY RESULTS

In accordance with Schmidt's definition, let $\Pi = \{\pi_i\}$ (i = 0, 1, 2, $\cdots$) be an iterative higher derivation on a field K of prime characteristic p. We assume that not each of the π_i is the zero map on K; then, without loss of generality, we can assume the existence of an x in K for which $\pi_1(x) \neq 0$ [2, p. 277]. This convention

Received December 22, 1967.

This paper is a condensation of the author's doctoral dissertation, Florida State University, Tallahassee, Florida, 1967, directed by Professor Nickolas Heerema. The primary portions of this paper were written while the author was a National Science Foundation Cooperative Graduate Fellow.

will be used throughout this paper. Following Weisfeld [10], we define a sequence of subfields $K_1, K_2, \cdots$ of K by

$$K_i = \{x \in K \mid \pi_1(x) = \cdots = \pi_{p^{i-1}}(x) = 0\}.$$

The field $K_\infty = \bigcap_{i=1}^\infty K_i$ is called the *field of constants* of Π. Since we have assumed the existence of an $x \in K$ for which $\pi_1(x) \neq 0$, the field K is not K_1, so that $K = K_0 \supset K_1$. Furthermore, for $i = 0, 1, 2, \cdots$, $x^{p^i} \in K_i$ but $x^{p^i} \notin K_{i+1}$. The sequence therefore has the form

$$K = K_0 \supset K_1 \supset K_2 \supset \cdots \supset K_\infty, \tag{2.1}$$

where the inclusions are strict. From the requirement that Π be iterative, we see by induction that $\pi_\nu(x) = \pi_1^\nu(x)/\nu!$ for $\nu < p$ and $x \in K$. However, if $\nu \geq p$ and ν is divisible by a higher power of p than is μ, then (again because Π is iterative) $\pi_{\nu-\mu}\pi_\mu(x) = 0$. Also, Weisfeld [10, p. 437] has shown that if

$$n = n_0 + n_1 p^1 + n_2 p^2 + \cdots + n_m p^m$$

is the p-adic representation of the positive integer n, then

$$\pi_n(x) = \frac{\pi_1^{n_0}\pi_p^{n_1}\cdots\pi_{p^m}^{n_m}(x)}{n_0!\,n_1!\cdots n_m!} \tag{2.2}$$

and

$$\pi_{p^i}\pi_{p^j}(x) = \pi_{p^j}\pi_{p^i}(x), \tag{2.3}$$

for all $x \in K$ and all nonnegative integers i and j. It follows from (2.2) and (2.3) that if Π is an iterative higher derivation on a field K of prime characteristic p, then Π is determined by its components $\pi_1, \pi_p, \pi_{p^2}, \cdots, \pi_{p^n}, \cdots$. We shall also use the easily established fact that

$$(\pi_{p^i})^p = 0 \qquad (i = 0, 1, 2, \cdots). \tag{2.4}$$

If $x \in K_i$, then $\pi_{p^{i-1}}(x) = 0$, and also (see [10, p. 436]) $[\pi_{p^{i-1}}(x)]^p = \pi_{p^i}(x^p) = 0$; hence $x^p \in K_{i+1}$. Therefore K_i has exponent at most 1 over K_{i+1}. Also, π_{p^i} induces a derivation τ_i on K_i with constant field K_{i+1}, for $i = 0, 1, 2, \cdots$. From (2.4) we see that $\tau_i^p = 0$; together with [6, p. 218] and the fact that $K_i \supset K_{i+1}$ for $i = 0, 1, 2, \cdots$, this implies that $[K_i : K_{i+1}] = p$ for $i = 0, 1, 2, \cdots$.

LEMMA 1. *There exists an element* $y \in K$ *for which* $\pi_1(y) = 1$.

Proof. There is an element $x \in K$ for which $\pi_1(x) \neq 0$, so that $x \notin K_1$; since

$$\pi_1\pi_{p-1}(x) = p\pi_p(x) = 0,$$

we conclude that $\pi_{p-1}(x) \in K_1$. Thus there is an i $(0 \leq i < p-1)$ for which $\pi_i(x) \notin K_1$, but $\pi_{i+1}(x) \in K_1$. Let $a = \pi_1\pi_i(x)$. Then $a \in K_1$ and $a \neq 0$. Thus

$$\pi_1[\pi_i(x)/a] = 1,$$

which establishes the existence of the required $y \in K$.

If K is an extension field of a field k of prime characteristic p, then K is defined to be a *separable extension* of k if and only if K and $k^{p^{-1}}$ are linearly disjoint over k.

LEMMA 2. K *is a separable extension of* K_∞.

Proof. Let X be a set of elements of K that are linearly independent over K_∞. Let $\{x_1, \cdots, x_n\}$ be any finite subset of X. Assume that

$$a_1^p x_1 + \cdots + a_m^p x_m = 0 \tag{2.5}$$

is an expression of linear dependence over K where $a_i \neq 0$ and $a_i \in K$ for $i = 1, 2, \cdots, m$. Furthermore, assume that (possibly with a reordering) $\{x_1, \cdots, x_m\}$ is the minimal subset of $\{x_1, \cdots, x_n\}$ for such an expression. Note that if $a_1 \in K_r$, then

$$\pi_{p^r}(a_1^p) = [\pi_{p^{r-1}}(a_1)]^p = 0,$$

so that in

$$\pi_{p^r}(a_1^p)x_1 + \cdots + \pi_{p^r}(a_m^p)x_m = \pi_{p^{r-1}}(a_1)^p x_1 + \cdots + \pi_{p^{r-1}}(a_m)^p x_m = 0$$

the first coefficient is zero. Thus, by the minimality of the representation (2.5), $\pi_{p^{r-1}}(a_i) = 0$ for $i = 2, \cdots, m$. Now, since $a_1^p \neq 0$, we can divide both sides of (2.5) by a_1^p to obtain the relation

$$x_1 + b_2^p x_2 + \cdots + b_m^p x_m = 0,$$

where $b_i = a_i/a_1 \in K$ for $i = 2, \cdots, m$. For each natural number r, $\pi_{p^r}(1) = 0$, and therefore $\pi_{p^r}(b_j) = 0$ for all r and for $j = 2, \cdots, m$. Therefore, $b_j \in \bar{K}$ for $j = 2, \cdots, m$. But this is a contradiction of the linear independence of the set $\{x_1, \cdots, x_n\}$ over K_∞. Therefore, K/K_∞ is separable. ∎

LEMMA 3. K_∞ *is algebraically closed in* K.

Proof. Schmidt [2, Theorem 7, p. 230] has shown that a higher derivation Π on a field F can be extended to a separable algebraic extension $F(x)$ in exactly one way. In particular, the zero higher derivation on F can be extended only to the zero higher derivation on $F(x)$. Thus, if $x \in K$ is separably algebraic over K_∞, then, since Π restricted to K_∞ is the zero higher derivation, $\pi_i(x) = 0$ for $i = 1, 2, \cdots$. This implies $x \in K_\infty$. Also, if $x \in K$ is inseparable over K_∞, then some power of x, say x^{p^r}, is separably algebraic over K. Thus, for $i = 0, 1, 2, \cdots$,

$$\pi_{p^i}(x)^{p^r} = \pi_{p^{i+r}}(x^{p^r}) = 0,$$

which implies that $\pi_{p^i}(x) = 0$. Thus, $x \in K_\infty$, which then is algebraically closed in K. ∎

LEMMA 4. $K^{p^\infty} \subseteq K_\infty$.

Proof. If $x \in K^{p^\infty}$, then for each natural number i the p^ith root y_i belongs to K^{p^∞}. Thus, for each r, $\pi_{p^r}(x) = \pi_{p^r}(y^{p^i})$. For $i > r$,

$$\pi_{p^r}(x) = \pi_{p^r}(y^{p^i}) = [\pi_1(y^{p^{i-r}})]^{p^r} = 0,$$

since the pth power of any element in K belongs to K_1. Thus, for each r, $\pi_{p^r}(x) = 0$, so that $x \in K_\infty$, and $K^{p^\infty} \subseteq K_\infty$. ∎

3. A GENERALIZATION OF SCHMIDT'S THEOREM

In this section we extend Schmidt's theorem [2, Theorem 13, p. 237] to arbitrary fields of prime characteristic p. Let K be a field of prime characteristic p, and let S be a p-basis of K.

LEMMA 5. *A higher derivation* Π *on* K *is iterative on* K *if and only if* Π *is iterative on a* p-*basis* S *of* K.

Proof. If Π is iterative on K, then it is obviously iterative on the subset S. Conversely, if Π is a higher derivation on K that is iterative on each $s \in S$, then one can compute easily that Π is iterative on the subring A generated by S. Thus

$$\pi_0, \cdots, \pi_{p^n-1} \text{ is iterative on } K_n[A] \supseteq K^{p^n}[S] = K. \quad ∎$$

The following theorem was obtained by N. Heerema [4, Theorem 1, p. 131].

LEMMA 6. *If* $T = \{\tau_i\}$ $(i = 1, 2, \cdots)$ *is a set of functions* $\tau_i\colon S \to K$, *then there exists a unique higher derivation* Π *on* K *such that* $\pi_i(s) = \tau_i(s)$ *for each* $s \in S$.

In particular, for each p-basis $\{t, S\}$ of K there is a unique iterative higher derivation $D = \{D^{(i)}\}$ for $i = 0, 1, 2, \cdots$, defined by

$$D^{(1)}(t) = 1, \qquad D^{(i)}(t) = 0 \text{ for } i > 1, \qquad D^{(j)}(s) = 0 \text{ for } j \geq 1 \text{ and } s \in S.$$

We call D *the derivation with respect to* t *along* S, and we denote it by $D = D_{(t,S)} = \{D^{(i)}_{(t,S)}\}$, for $i = 0, 1, 2, \cdots$.

Let K be an extension field of the field k that is separably generated in one indeterminant over k. In [2], Schmidt developed a process for approximating a given iterative higher derivation in K for which the elements of k are constants. For this he constructed a sequence of iterative higher derivations, each being a derivation with respect to a separating element. We shall now show that an iterative higher derivation Π in an arbitrary field K of prime characteristic p can be approximated by a sequence of iterative higher derivations, each of which is of type $D_{(t,S)}$ for some p-basis $\{t, S\}$ of K.

Definition 1. Two p-bases $\{t, T\}$ and $\{s, S\}$ of K are n-*equivalent*, for a fixed nonnegative integer n, if

$$K^{p^n}(T) = K^{p^n}(S) \quad \text{and} \quad t - s \in K^{p^n}(T) = K^{p^n}(S).$$

Remark. If two p-bases $\{t, T\}$ and $\{s, S\}$ of K are n-equivalent, then it is seen directly that

$$D^{p^i}_{(t,T)}(x) = D^{p^i}_{(s,S)}(x) \qquad (0 \le i < n),$$

where $x \in \{t, T\}$; hence, by Lemma 6,

$$D^{p^i}_{(t,T)} = D^{p^i}_{(s,S)} \qquad (0 \le i < n).$$

We make the following definition for notational convenience

Definition 2. Let m be a nonnegative integer. Two higher derivations Π and T on K are *m-equivalent* if $\pi_i = \tau_i$ for $1 \le i < p^m$.

THEOREM 1. *Let* $\{t_n, S_n\}$ $(n = 0, 1, 2, \cdots)$ *be a sequence of* p*-bases of* K *such that* $\{t_m, S_m\}$ *and* $\{t_{m+1}, S_{m+1}\}$ *are* m*-equivalent for* $m = 0, 1, 2, \cdots$, *let* Π *be defined so that* π_0 *is the identity mapping on* K, *and let*

$$\pi_i = D^{(i)}_{(t_n, S_n)} \quad \textit{for } p^n \le i < p^{n+1};$$

then Π *is an iterative higher derivation on* K.

Proof. We note that if i and j are natural numbers such that $i < j$, then $\{t_i, S_i\}$ and $\{t_j, S_j\}$ are i-equivalent. Thus

$$D^{(r)}_{(t_i, S_i)} = D^{(r)}_{(t_j, S_j)} \qquad \text{for } r < p^i.$$

This implies that

$$\pi_r = D^{(r)}_{(t_j, S_j)} \qquad \text{for } r < p^j. \tag{3.1}$$

Because (3.1) is true for each natural number r, and since π_0 is the identity map on K, the conclusion follows.

THEOREM 2. *If* K *is a field of prime characteristic* p, *and* Π *is an iterative higher derivation defined on* K, *then there exists a sequence* $\{t_i, S_i\}$ $(i = 0, 1, 2, \cdots)$ *of* p*-bases of* K *with the property that* $\{t_i, S_i\}$ *and* $\{t_{i+1}, S_{i+1}\}$ *are* i*-equivalent and*

$$\pi_j(y) = D^{(j)}_{(t_m, S_m)}(y) \quad \textit{for } y \in K \textit{ and } p^m \le j < p^{m+1}.$$

Proof. Since π_1 is assumed to be nontrivial, Lemma 1 allows us to find an element t_0 of K such that $\pi_1(t_0) = 1$. As in Section 2, denote the subfields of constants of the various π_{p^i} by

$$K \supset K_1 \supset K_2 \supset \cdots \supset K_i \supset \cdots \supset \bigcap_{n=1}^{\infty} K_n = K_\infty.$$

Now $t_0^p \in K_1$, because $\pi_1(t_0^p) = 0$, but $t_0 \notin K_1$. Therefore, because $[K : K_1] = p$, $K = K_1(t_0)$. It follows that t_0^p may be extended to a p-basis $\{t_0^p, S_0\}$ for K_1; $\{t_0, S_0\}$ will then be a p-basis for K. Now, since $\pi_i(x) = D^{(i)}_{(t_0, S_0)}(x)$ for $x \in K$ and $1 \le i < p$, Π is 1-equivalent to $D_{(t_0, S_0)}$.

Now assume that $\{t_n, S_n\}$ is a p-basis of K for which Π is n-equivalent to $D_{(t_n, S_n)}$. This means that

$$\pi_1(t_n) = 1 \quad \text{and} \quad \pi_i(t_n) = 0 \qquad \text{for } 2 \le i < p^n,$$

and that $\pi_j(s) = 0$ for all $s \in S_n$ and $1 \leq j < p^n$. Therefore $S_n \subset K_n$ and $t_n^{p^n} \in K_n$. Also,

$$\pi_{p^i}\pi_{p^n}(t_n) = \pi_{p^n}\pi_{p^i}(t_n) = 0 \quad \text{for } 0 \leq i < n,$$

so that $\pi_{p^n}(t_n) \in K_n = K_{n+1}(t_n^{p^n})$.

For some $b_i \in K_{n+1}$,

$$\pi_{p^n}(t_n) = b_{p-1}\, t_n^{p^n(p-1)} + \cdots + b_0 .$$

This implies that

$$b_{p-1} = \pi_{p^n(p-1)}\, \pi_{p^n}(t_n) = \binom{p^{n+1}}{p^n} \pi_{p^{n+1}}(t_n) = 0,$$

so that

$$\pi_{p^n}(t_n) = b_{p-2}\, t_n^{p^n(p-2)} + \cdots + b_0 .$$

If we write

$$v = -\frac{b_{p-2}}{p-1}\, t_n^{p^n(p-1)} - \cdots - b_0 t_n^{p^n},$$

then

$$\pi_{p^i}(t_n + v) = \delta_{0,i} \quad \text{for } 0 \leq i < n+1 .$$

Thus $(t_n + v)^{p^{n-1}} \notin K_n$ and $(t_n + v)^{p^n} \in K_n$, and therefore $\{(t_n + v)^{p^n}\}$ may be extended to a p-basis $\{(t_n + v)^{p^n}, S_{n+1}\}$ for K_n. Then $\{t_n + v, S_{n+1}\}$ is a p-basis for K, and Π is $(n+1)$-equivalent to $D_{(t_n+v,\, S_{n+1})}$, as was required.

Furthermore, we see that

$$K^{p^n}(S_n) \subseteq K_n, \qquad K^{p^n}(S_n, t_n) = K, \qquad t_n^{p^n} \in K^{p^n};$$

therefore $[K : K^{p^n}(S_n)] = p^n$. Now the fact that $[K : K_n] = p^n$ implies $K^{p^n}(S_n) = K_n$. Similarly, $S_{n+1} \subset K_n$, so that $K^{p^n}(S_{n+1}) \subset K_n$. Again

$$K^{p^n}(S_{n+1}, t_{n+1}) = K \quad \text{and} \quad t_{n+1}^{p^n} \in K^{p^n};$$

therefore $[K : K^{p^n}(S_{n+1})] = p^n$, which implies $K^{p^n}(S_{n+1}) = K$. Now, because

$$K^{p^n}(S_n) = K^{p^n}(S_{n+1}) \quad \text{and} \quad t_n - t_{n+1} = t_n - (t_n - v) = v \in K_n,$$

we conclude that $\{t_n, S_n\}$ and $\{t_{n+1}, S_{n+1}\}$ are n-equivalent p-bases.

The following is a consequence of Theorems 1 and 2.

COROLLARY (Schmidt's Theorem). *Let* K *be a field of prime characteristic* p, *separably generated with transcendence degree* 1 *over a subfield* k, *and let* S *be a* *p-basis of* k. *If* Π *is an iterative higher derivation on* K *whose field of constants* K_∞ *contains* k, *then there exists a sequence* $\{t_i\}$ $(i = 0, 1, 2, \cdots)$ *of elements of* K *with the properties that, for each* i, $\{t_i\}$ *is a separating transcendence basis of* K *over* k, $t_{i+1} - t_i \in k(K^{p^i})$, *and* Π *is* i-*equivalent to* $D_{(t_i, S)}$.

Conversely, let $\{t_j\}$ $(j = 1, 2, \cdots)$ *be a sequence of separating transcendence bases of* K *over* k *with the property that*

$$t_{j+1} - t_j \in k(K^{p^j}),$$

and let S *be any* p-*basis for* k. *Then the mappings* $\Pi = \{\pi_j\}$ *on* K *defined by the conditions*

a) π_0 *is the identity mapping for* K, b) Π *is* j-*equivalent to* $D_{(t_j, S)}$

is an iterative high derivation on K *whose field of constants contains* k.

Proof. Under our hypotheses, S_i may be chosen to be S for all i, $K^{p^i}(S) = k(K^{p^i})$, and t is a separating transcendence basis for K over k if and only if $\{t, S\}$ is a p-basis for K.

4. SUBFIELDS OF CONSTANTS

The present section is concerned with the problem of determining which subfields of K are possible fields of constants of an iterative higher derivation Π on K. We restrict our attention to the case where K is finitely generated over a countable subfield k. By Lemma 2, we may assume that K is separably generated over k. Thus

$$K = k(u_1, u_2, \cdots, u_n, \theta),$$

where $u_1, \cdots, u_n$ is a separating transcendence basis, θ is a primitive element, and k is countable. Since Schmidt's Theorem covers the case $n = 1$, we assume $n > 1$. Set

$$S = K - kK^p.$$

Since S is countable, we can well-order it by putting its elements into a one-to-one correspondence with the natural numbers: $S = \{y_1, y_2, y_3, \cdots\}$. We shall construct a sequence of subfields of K,

$$K = K_0 \supset K_1 \supset K_2 \supset \cdots \supset K_m \supset \cdots$$

such that for each $m = 0, 1, 2, \cdots$,

a) $[K_m : K_{m+1}] = p$, b) $K_{m+1}(u_1^{p^m}) = K_m$, c) $y_i \notin K_{m+1}$ for $1 \leq i < m+1$.

We shall then extend $\{u_1^{p^m}\}$ to a p-basis $\{u_1^{p^m}, v_2, \cdots, v_n\}$ of K_m relative to k. Then $\{u_1, v_2, \cdots, v_n\}$ is a p-basis of K relative to k. The sequence of p-bases generated in this manner will have the properties of the sequence of p-bases in the hypothesis of Theorem 1 (with $t_m = u_1$), and therefore they will define an iterative higher derivation Π on K. It will be shown that the field of constants of Π is the algebraic closure of k in K.

Assume now that K_m has been determined so that

$$x_i \notin K_m \ (i = 1, \cdots, m-1), \qquad u_1^{p^{m-1}} \notin K_m, \qquad K_m(u_1^{p^i}) = K_i, \qquad [K_{m-1} : K_m] = p.$$

We now proceed to determine K_{m+1}. Let $x_m \in S$ be the first element of S that is also in K_m. Clearly, x_m is beyond x_{m-1} in the ordering of S. We now verify the existence of a p-independent set $\{w_2, \cdots, w_n\}$ in K_m over k for which

$$u_1^{p^m} \notin kK_m^p(w_2, \cdots, w_n) \quad \text{and} \quad x_m \notin kK_m^p(w_2, \cdots, w_n).$$

If u_1^p and x_m are p-dependent over k as elements of K_m, then $x_m \in kK_m^p(u_1^{p^m})$. There is a p-independent set $\{w_2, \cdots, w_n\}$ in K_m over k such that $\{u_1^{p^m}, w_2, \cdots, w_n\}$ forms a p-basis for K_m over k. Also, $x_m \notin kK_m^p(w_2, \cdots, w_n)$.

Assume now that $u_1^{p^m}$ and x_m are p-independent over k as elements of K_m, and let $b = u_1^{p^m} x_m$. Then $\{b, x_m\}$ is also a p-independent set over k with respect to K_m. For, otherwise, the polynomial over kK_m^p exhibiting the p-dependence of b and x_m would also exhibit the p-dependence of x_m and $u_1^{p^m}$, contrary to the hypothesis that these are p-independent. Clearly,

$$u_1^{p^m} \in kK_m^p(b, x_m) \quad \text{and} \quad x_m \in kK_m^p(b, u_1^{p^m});$$

but by the p-independence of the sets $\{b, x_m\}$ and $\{b, u_1^{p^m}\}$ over k with respect to K_m, neither $u_1^{p^m}$ nor x_m can belong to $kK_m^p(b)$. The set $\{b, x_m\}$ can be extended to a p-basis $\{b, x_m, w_3, \cdots, w_n\}$ of K_m with respect to k. Then

$$x_m \notin kK_m^p(b, w_3, \cdots, w_n) \quad \text{and} \quad u_1^{p^m} \notin kK_m^p(b, w_3, \cdots, w_n).$$

We set $b = w_2$.

In either case, set $K_{m+1} = kK_m^p(w_2, \cdots, w_n)$. Then

$$K_{m+1}(u_1^{p^m}) = K_m, \qquad u_1^{p^{m+1}} \in K_{m+1}, \qquad x_m \notin K_{m+1}.$$

It is also obvious that $\{u_1, w_2, \cdots, w_n\}$ is a p-basis for K over k.

This process yields a sequence of p-bases $\{u_1, S_n\}$ $(n = 1, 2, \cdots)$ that satisfy the hypotheses of Theorem 1. Let Π be the corresponding iterative higher derivation on K whose existence is assured by this theorem, and let K be its subfield of constants. By construction, $S \cap K_\infty = \emptyset$, so that $K_\infty \subseteq kK^p$. Thus $k \subseteq K_\infty \subseteq kK^p \subseteq K$. Since K is separable over K_∞ (by Lemma 2), each p-basis of K over K_∞ is also a separating transcendence basis of K over K_∞. But $kK^p \subseteq K_\infty K^p \subseteq kK^p$, so that $K_\infty K^p = kK^p$. Thus any p-basis of K over K_∞ is also a p-basis of K over k. A p-basis (and hence a separating transcendence basis of K over K_∞) must have n elements, where n is the transcendence degree of K over k. Therefore K_∞ is algebraic over k, and in fact it is the algebraic closure of k in K.

We can now prove a fairly general theorem on fields of constants of iterative high derivations.

THEOREM 3. *Let* k *be a countable field of prime characteristic* p, *and let* K *be a finitely generated extension of* k. *A subfield* H *of* K *over* k *is the field of constants of an iterative higher derivation* Π *on* K *if and only if* H *is algebraically closed in* K *and* K *is separable over* H.

Proof. (The author is indebted to Mr. William Heinzer for suggesting this proof.). K_∞, the field of constants of Π, is by Lemma 3 algebraically closed in K. For each subfield H, it is therefore sufficient to consider the algebraic closure H' of H in K. Now, if K is separable over H', the methods of this section show that H' is the field of constants of an iterative higher derivation. Conversely, if H' is a constant field of an iterative higher derivation Π, then K is separable over H', by Lemma 2, and H' is algebraically closed in K.

REFERENCES

1. H. Hasse, *Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik.* J. Reine Angew. Math. 175 (1936), 50-54.
2. 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.
3. N. Heerema, *Derivations and embeddings of a field in its power series ring.* Proc. Amer. Math. Soc. 11 (1960), 183-194.
4. ———, *Derivations and embeddings of a field in its power series ring, II.* Michigan Math. J. 8 (1961), 129-134.
5. ———, *Derivations on* p-*adic fields.* Trans. Amer. Math. Soc. 102 (1962), 346-351.
6. N. Jacobson, *Abstract derivations and Lie algebras.* Trans. Amer. Math. Soc. 42 (1937), 206-224.
7. ———, *Lectures in abstract algebra.* Vol. III: *Theory of fields and Galois theory.* D. Van Nostrand Co., Princeton, N. J., 1963.
8. S. Mac Lane, *Modular fields, I. Separating transcendence bases.* Duke Math. J. 5 (1939), 372-393.
9. D. Teichmüller, *Differentialrechnung bei Charakteristik* p. J. Reine Angew. Math. 175 (1936), 89-99.
10. M. Weisfeld, *Purely inseparable extensions and higher derivations.* Trans. Amer. Math. Soc. 116 (1965), 435-449.
11. O. Zariski and P. Samuel, *Commutative algebra,* Vol. 1. D. Van Nostrand Co., Princeton, N. J., 1958.

University of South Florida
Tampa, Florida 33620