J. Sci. Hiroshima Univ. Ser. A-I
32 (1968), 167-171

Some Remarks on Higher Derivations of Finite Rank in a Field of a Positive Characteristic

Hiroshi Yanagihara

(Received February 22, 1968)

In this short note we give a generalization of an approximation theorem on iterated higher derivations given by F. K. Schmidt in a paper [2] (see Satz 14). Our generalization is done by determining all the iterated higher derivations of finite rank in any field K of a positive characteristic p. The following result on a derivation d in K will play an essential role in the proof: if we have $d^p=0$, then $d^{p-1}(\alpha)=0$ if and only if $\alpha=d(\beta)$ for some β in K *). We shall give a proof of this fact using the Jacobson-Bourbaki's theorem which asserts the existence of a $1-1$ correspondence between subfields of finite codimension in a field K and certain subrings of the ring $\mathcal{L}(K)$ of endomorphisms of the additive group $(K, +)$. Lastly we shall be concerned with conditions for a purely inseparable extension K of finite degree over a field k to be a tensor product of simple extensions over k. These conditions will be given in terms of higher derivations in K.

§**1.** Let K be a field and $\mathcal{L}(K)$ the set of additive homomorphisms of K into itself. $\mathcal{L}(K)$ is considered naturally as a vector space over K. Then a sequence $\{d_i\}_{i=0,1,\dots,m}$ of elements in $\mathcal{L}(K)$ is called *a higher derivation in K of rank m* if the following conditions are satisfied: (i) *d_0 is the identity of K*, (ii) *$d_j(ab)=\sum_{i=0}^{j} d_i(a)d_{j-i}(b)$, $j=0, 1, \cdots, m$, holds for any elements a, b in K.* A higher derivation $\{d_i\}$ is called *iterated* if it satisfies one more condition (iii) *$d_i d_j=\binom{i+j}{i}d_{i+j}$ for $i+j\leqq m$ and $d_i d_j=0$ for $i+j>m$.* Let k be the subset of the elements α in K such that $d_i(\alpha)=0$ for $i\geqq 1$. Then k is a subfield of K and we call it *the constant field* of $\{d_i\}$. In the following we treat only iterated higher derivations in a field of a positive characteristic p. In this case we can easily see that a section $\{d_i\}_{i=0,1,\dots,p^e-1}$ of $\{d_i\}$ for $p^e-1\leqq m$ is also an iterated higher derivation of rank p^e-1 in K, since we have $\binom{i+j}{i}\equiv 0$ (mod p) for $0\leqq i$, $j\leqq p^e-1$, $i+j\geqq p^e$. The following three lemmas are known.

Lemma 1. *Let $\{d_i\}_{i=0,1,\dots,m}$ be a higher derivation in K such that $d_1\neq 0$. Then we have $d_i\neq 0$ for any i and these $m+1$ elements $d_0, \cdots, d_m$ are linearly independent over K.*

---

*) F. K. Schmidt proved this result in a special case where K is an algebraic function field of one variable. The method of his proof is function theoretical.

This is Excercise 7 of §9, Chapter IV in [1] and is proved, using the above equality (ii), in the exactly same way as the Dedekind's Theorem (Theorem 3 of §3, Chapter I in [1]).

LEMMA 2. *Let $\{d_i\}$ be an iterated higher derivation of finite rank m in a field K of a positive characteristic p such that $d_1 \neq 0$, and let k be the constant field of $\{d_i\}$. Then K is a simple and purely inseparable extension of degree $m+1$ over k and hence m is equal to p^e-1 for some integer e.*

PROOF. By Theorem 20 of Chapter IV in [1], K is a purely inseparable extension of exponent e where $p^{e-1} \leqq m < p^e$ and an element x in K has exponent e over k if and only if $d_1(x) \neq 0$. On the other hand, the subspace $Kd_0 + \cdots + Kd_m$ of $\mathscr{L}(K)$ is a subring satisfying the condition of the Jacobson-Bourbaki Theorem (Theorem 2 of Chapter I in [1]) since $\{d_i\}$ is iterated. This means, by Lemma 1, that K is of degree $m+1$ over k and hence K is a simple extension of degree $p^e = m+1$.

LEMMA 3. *Let K be a simple and purely inseparable extension of degree p^e over k and let x be a primitive element of K over k. Then there exists exactly one iterated higher derivation $\{d_i\}$ of rank p^e-1 in K with constant field k such that $d_1(x)=1$ and $d_i(x)=0$ for $i \geqq 2$.*

For the proof, see §9 of Chapter IV in [1].

We denote by $\{d_{xi}\}$ this uniquely determined derivation by a primitive element x. Then it is easy to see that $d_{xi}(x^m) = \binom{m}{i} x^{m-i}$ if $m \geqq i$ and $d_{xi}(x^m)=0$ if $m < i$.

§**2**. Now we show that every iterated higher derivation of finite rank in K with constant field k is $\{d_{xi}\}$ for some primitive element x of K over k. Let K be a simple and purely inseparable extension of degree p^e over k and $\{d_i\}$ an iterated higher derivation of rank p^e-1 in K over k such that $d_1 \neq 0$. Then we have

LEMMA 4. *Let K_j be the set of elements α in K such that $d_i(\alpha)=0$ for $i=1, 2, \cdots, p^j-1$. Then K_j is equal to kK^{p^j}.*

PROOF. It is clear that K_j contains kK^{p^j}. Let x be a primitive element of K over k. Then x^{p^j} is in K_j but $x^{p^{j-1}}$ is not in K_j since $d_{p^{j-1}}(x^{p^{j-1}}) = (d_1(x))^{p^{j-1}} \neq 0$, and hence we have $K_{j-1} \supsetneqq K_j$ for $e \geqq j \geqq 1$. On the other hand we have $k(x^{p^j}) = kK^{p^j}$ and hence $[kK^{p^j} : k] = p^j$. This means that $K_j = kK^{p^j}$.

For our purpose the following proposition is basic.

PROPOSITION 1. *Let d be a derivation in a field of a positive characteristic p such that $d^p=0$. Then the set of the elements y in K such that $d^{p-1}(y)=0$ coincides with the set of all elements $d(x)$ for $x \in K$.*

PROOF. Put $d_i = \frac{1}{i!} d^i$ for $i=1, 2, \cdots, p-1$ and let d_0 be the identity mapping of K. Then we can easily see that $\{d_i\}$ is an iterated higher derivation of rank $p-1$. Let K_1 be the constant field of $\{d_i\}$. Then K is of degree p over K_1 by Lemma 2. Let V be the set of elements $d_1(x)$ for $x \in K$. It is easy to see that V is a linear subspace of K over K_1 and K_1 is the kernel of the mapping d_1 of K onto V, since α is in K_1 if and only if $d(\alpha)=d_1(\alpha)=0$. Hence V is of dimension $p-1$ over K_1. Let W be the set of the elements x in K such that $d^{p-1}(x)=(p-1)!d_{p-1}(x)=0$. Then W is a linear subspace of K over K_1 and contains V by the assumption $d^p=0$. Therefore W is equal to K or to V, since $\dim_K V=\dim_K K-1$. By Lemma 1, $d_0, d_1, \cdots, d_{p-1}$ are linearly independent over K_1 as vectors in $\mathfrak{L}(K)$ and hence there exists an element γ in K such that $d_{p-1}(\gamma)\neq 0$. This means that $V=W$.

Now we can show the following Theorem from Proposition 1 in the same way as Satz 12 from Satz 11 in [2].

THEOREM. *Let K be a field of a positive characteristic p and $\{d_i\}$ an iterated higher derivation of finite rank in K with constant field K such that $d_1 \neq 0$. Then there exists a primitive element x of K over k such that $\{d_i\}$ is equal to $\{d_{xi}\}$.*

An outline of our proof is as follows: it is sufficient to find x in K such that $d_1(x)=1$ and $d_i(x)=0$ for $i \geqq 2$, since we have $K=k(x)$ for such x by Lemma 2. We can find x_j such that $d_1(x_j)=1$ and $d_i(x_j)=0$ for $2 \leqq i < p^j$ by induction on j. In fact this is trivial for $j=1$. We put $r=-d_{p^j}(x_j)$ if there exists an x_j satisfying the condition. Then we can see that r is in $K_j=kK^{p^j}$ and put $r=r_1^{p^j}c_1+\cdots+r_h p^j c_k$ where $c_1, \cdots, c_h$ are in k and linearly independent over K^{p^j}. Then we can see $d_{p^{j+1}-p^j}(r)=(d_{p-1}(r_1))^{p^j}c_1+\cdots+(d_{p-1}(r_h))^{p^j}c_h=0$ for $j \leqq e-1$. This means that $d_{p-1}(r_i)=0$ and hence we have $d_1(\alpha_i)=r_i$ for some $\alpha_1, \cdots, \alpha_h$ in K by Proposition 1. Put $x_{j+1}=x_j+\alpha_1^{p^j}c_1+\cdots+\alpha_h^{p^j}c_h$ and we see that x_{j+1} satisfies $d_1(x_{j+1})=1$ and $d_i(x_{j+1})=0$ for $2 \leqq i < p^{j+1}$.

REMARK 1. It is easy to see that Satz 14 in [2] follows from the above theorem.

REMARK 2. Let $\{d_i\}$ be an iterated higher derivation of infinite rank in a field K and let K_j be the constant field of the section $\{d_i\}_{i \leq p^j-1}$ of $\{d_i\}$. Then the constant field k of $\{d_i\}$ is $\bigcap_{j=1} K_j$. If K is an algebraic function field of one variable over k, we know that the constant field K_j of $\{d_i\}_{i \leq p^j-1}$ is kK^{p^j} (cf. Satz 10 in [2]). In general cases, using the idea of the proof of Theorem, we see that $K_j=kK^{p^j}$ for all j if $K_1=kK^p$. In fact assume that $K_j \neq kK^{p^j}$ for some $j \geqq 2$. Let x be an element in K_j but in kK^{p^j}. If x is in $kK^{p^{t-1}}$ but not in kK^{p^t} $(t \leqq j)$, we have $x=c_1 r_1^{p^{t-1}}+\cdots+c_h r_h^{p^{t-1}}$ for some $r_1, \cdots, r_h$ in K where $c_1, \cdots, c_h$ are in k and linearly independent over $K^{p^{t-1}}$. Since x is in K_j, we have $d_{p^{t-1}}(x)=c_1(d_1(r_1))^{p^{t-1}}+\cdots+c_h(d_1(r_h))^{p^{t-1}}=0$ and hence $d_1(r_i)=0$ for all i.

This means that r_i is in $K_1=kK^p$ and hence x is in kK^{p^t}. This is a contradiction.

As a consequence of Theorem we have the following

PROPOSITION 2. *Let K be a field of a positive characteristic p and E a subfield of K. Suppose that there exists an iterated higher derivation $\{d_i\}$ of finite rank p^e-1 in E with constant field k. Then $\{d_i\}$ can be extended to an iterated higher derivation in K if and only if there exists a subfield F of K containing k such that K is the tensor product of E and F over k.*

PROOF. We may assume that $d_1\neq 0$. Then there exists an element x in F such that $d_1(x)=1$ and $d_i(x)=0$ for $i\geqq 2$ by Theorem. If $\{d_i\}$ is extended to $\{\bar{d}_i\}$ in K, let F be the constant field of $\{\bar{d}_i\}$. Then we have $[K: F]=[E: k]=p^e$, $K=F(x)$ and $E=k(x)$ by Lemma 2. This means that $K=EF$, and that E and F are linearly disjoint over k. Conversely assume that $K=EF$ and that E and F are linearly disjoint over k. Since $E=k(x)$, $K=F(x)$ is purely inseparable extension of degree p^e over F and hence there exists an iterated higher derivation $\{\bar{d}_i\}$ of rank p^e-1 in K with constant field F such that $\bar{d}_1(x)=1$ and $\bar{d}_i(x)=0$ for $i\geqq 2$ by Lemma 3. It is easy to see that $\{\bar{d}_i\}$ is an extension of $\{d_i\}$.

§3. Let K be a purely inseparable extension of finite degree over a field k. Then it is known that if K is a tensor product of simple extensions over k, then k is an intersection of constant fields of iterated higher derivations in K (cf. §9 of Chapter IV in [1]), but in general k is not an intersection of constant fields of iterated higher derivations in K. For an example let K be a purely inseparable extension of degree p^3 over k such that K is not a tensor product of simple extensions over k. There exists such an extension. (See Exercise 6 of §9, Chapter IV in [1].) Then K has exponent 2 and contains only one subfield F of K over k which is of degree p over k. Then F is contained in the constant field of any iterated higher derivation in K over k, since the exponent of K over k is two.

Now we give a sufficient condition for an extension K over k to be a tensor product of simple, purely inseparable extensions over k.

PROPOSITION 3. *Let K be a purely inseparable extension of exponent e over k which is an intersection of constant fields of iterated higher derivations in K. Then K is a tensor product of a simple extension $k(x)$ of degree p^e and a subfield E over k.*

PROOF. Let x be an element of K whose exponent over k is e. Since $x^{p^{e-1}}$ is not in k, there exists an iterated higher derivation $\{d_i\}$ in K whose constant field E contains k but not $x^{p^{e-1}}$. Then K is a simple extension over E whose degree is at most p^e. Hence we have $K=E(x)=k(x)E$ and $[K: E]$

$=p^e$. This means that K is the tensor product of $k(x)$ and E over k.

COROLLARY. *Assume that K/k satisfies the same condition as Proposition 3. Then K is a tensor product of simple extensions over k if the degree of K over k is at most of p^{e+2}.*

PROOF. Since a purely inseparable extension of degree p^2 is a simple extension or a tensor product of two simple extensions of degree p over k, this is a direct consequence of Proposition 3.

REMARK 3. Assume that $[K: k]\leqq p^4$. Then k is an intersection of constant fields of iterated higher derivations in K if and only if K is a tensor product of simple purely inseparable extensions over k. However the author does not know any example for $[K: k]=p^5$ such that K is not a tensor product of simple extensions over k which is an intersection of constant fields of iterated higher derivations in K.

REMARK 4. Let K be a purely inseparable extensions of finite degree. If K and any subfield of K containing k satisfy the assumptios in Proposition 3, K is a tensor product of simple extensions over k.

Added in Proof. After this paper was completed, Prof. E. Abe kindly communicated to me that M. E. Sweedler obtained the following result: a purely inseparable extension K of finite exponent over a field k is a tensar product of simple extensions over k if and only if there are higher derivations of K over k relative to which k is the field of constants. (Annals of Math. vol. 87, No. 3).

References

[1] N. Jacobson, "*Lectures in Abstract Alqebra*," Vol. III-Theory of Fields and Galois Theory, Van Nostrand, (1964).

[2] H. Hasse-F. K. Schmidt, "*Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten*," J. reine u. angw. Math. Vol. 177, pp. 215-137 (1937).

Department of Mathematics
Faculty of Science
Hiroshima University