PURELY INSEPARABLE EXTENSIONS AND HIGHER DERIVATIONS(1)

BY
MORRIS WEISFELD

I. Let F be a field having prime characteristic p and C be a subfield. An element x of F is called purely inseparable if $x \notin C$ and $x^{p^e} \in C$ for some positive integer e; the least positive integer e such that $x^{p^e} \in C$ is called the exponent of x over C. F is a purely inseparable extension of C if every element of F not in C is purely inseparable over C. The maximum of the set of exponents of the purely inseparable elements of F, if it exists, is called the exponent of F over C.

In 1927 R. Baer studied the relationship between derivations and purely inseparable extensions having exponent one over the base field. In this paper a generalization of Baer's results to purely inseparable extensions having any exponent over the base field is studied.

Of prime importance in this study is the notion due to H. Hasse and F. K. Schmidt of a higher derivation.

Let A be a ring with an identity.

The sequence

$$D = \{ D^{(r)} \mid 0 \leqq r < m \}$$

of endomorphisms of $(A, +)$, the additive group of A, is called a higher derivation in A if and only if $D^{(0)} = I$, the identity endomorphism of $(A, +)$ and(2)

$$D^{(r)}(xy) = \sum \{ D^{(r-j)}(x) D^{(j)}(y) \mid 0 \leqq j \leqq r \}. \tag{1}$$

If $k = \max\{r \mid D^{(r)} \neq 0,\ 0 \leqq r < m\}$ exists, k is called the rank of D (0 is the zero endomorphism). If $m < \infty$, D is called finite. An element x of A is called a D-constant if and only if $D^{(r)}(x) = 0$ for all r such that $0 < r < m$. The set of D-constants of A is a subring which is closed with respect to taking multiplicative inverses.

Let F be a purely inseparable extension of C. A subset B of F is called a sub-basis of F over C if and only if $B \cap C = \emptyset$, $F = C(B)$, and, for any

Received by the editors January 10, 1963.

(1) This paper originated in the author's doctoral dissertation, Yale University, New Haven, Conn., 1954. Cf. also *A note on purely inseparable extensions*, Bull. Amer. Math. Soc. **60** (1954), p. 336. The primary portions of this paper, except for revisions, were written when the author was a Fund for the Advancement of Education Teaching Intern at the University of Chicago.

(2) $\sum\{\ \}$ denotes the sum of the elements of the indicated set.

finite subset $\{b_1, \cdots, b_n\}$ of B, the canonical homomorphism of the tensor product $C(b_1) \otimes C(b_2) \otimes \cdots \otimes C(b_n)$ into F is a monomorphism.

The main result is the following: Let F be a field having prime characteristic p and C be a subfield of F. Then, there exists a nontrivial finite higher derivation in F having C as its subfield of constants if and only if F is a purely inseparable extension of C having an exponent and a subbasis over C[3].

II. In this section some implications of the existence of a higher derivation in a field will be drawn.

Let F be a field having prime characteristic p and $D = \{D^{(r)} \mid 0 \leqq r < m\}$ be a higher derivation in F. Then, if $m < \infty$,

$$x \to x + D^{(1)}(x)\, Y + \cdots + D^{(m-1)}(x)\, Y^{m-1}$$

is a monomorphism of F into the algebra $F[Y]/(Y^m F[Y])$ over F, and if $m = \infty$,

$$x \to x + D^{(1)}(x)\, Y + \cdots + D^{(r)}(x)\, Y^r + \cdots$$

is a monomorphism of F into the algebra of formal power series in the indeterminate Y over F. Using the fact that the pth power map is an endomorphism in these rings, one finds:

$$\begin{aligned} &D^{(r)}(x^{p^f}) = (D^{(j)}(x))^{p^f} \quad \text{if } r = jp^f \text{ for some } j, \\ &D^{(r)}(x^{p^f}) = 0 \quad \text{if } r \neq jp^f \text{ for any } j. \end{aligned} \tag{2}$$

THEOREM 1. *Let F be a field having prime characteristic p, $D = \{D^{(r)} \mid 0 \leqq r < m\}$ be a higher derivation in F, and C be the subfield of D-constants.*

Suppose D has finite positive rank k. If $x \in F$ and $x \notin C$, let s be the least positive integer such that $D^{(s)}(x) \neq 0$, and e be the least integer such that $k/s < p^e$. Then, x is purely inseparable over C, and e is the exponent of x over C. Hence, if q is the least positive integer for which $D^{(q)} \neq 0$ and r is the least integer such that $k/q < p^r$, then F is a purely inseparable extension of C having exponent r over C. Moreover, D is finite and $m - 1 < qp^r$.

If $m = \infty$, then D does not have finite positive rank, and F does not contain any purely inseparable elements over C.

Proof. It is claimed that $x^{p^e} \in C$. By (2) $D^{(r)}(x^{p^e}) = 0$ if p^e does not divide r. If $r = jp^e$, where $1 \leqq j < s$ then, since $D^{(j)}(x) = 0$ by hypothesis, (2) shows that $D^{(r)}(x^{p^e}) = 0$. Finally, if $r = jp^e$ and $j \geqq s$, then $jp^e > k$, and hence, $D^{(jp^e)}$, if it is defined, is identically zero. Thus, $x^{p^e} \in C$, that is, x is purely inseparable over C. If for some $f < e$, $x^{p^f} \in C$, then, since $p^f \leqq k/s$ (according to the definition of e), $D^{(sp^f)}$ is defined. (2) gives $D^{(sp^f)}(x^{p^f}) = (D^{(s)}(x))^{p^f}$ and, on the other hand, $x^{p^f} \in C$ implies $D^{(sp^f)}(x^{p^f}) = 0$.

(3) The author thanks G. Hochschild, N. Jacobson, S. MacLane, and W. H. Mills.

These statements imply that $D^{(s)}(x) = 0$ contrary to the choice of s. Hence, the exponent of x over C is precisely e.

Now, suppose that $D^{(qp^r)}$ is defined. Then, $x^{p^r} \in C$ implies that $D^{(qp^r)}(x^{p^r}) = 0$, and (2) gives $D^{(qp^r)}(x^{p^r}) = (D^{(q)}(x))^{p^r}$ so that $D^{(q)}(x) = 0$ for all $x \in F$. The latter statement contradicts the choice of q. Hence m must be finite and $m - 1 < qp^r$.

The first statement of the last paragraph of the theorem is a restatement of what has been just demonstrated. The final statement follows from the fact that if any element $x \in F$ satisfies $x^{p^f} \in C$, then, since $D^{(jp^f)}$ is defined for all j, $D^{(j)}(x) = 0$ for all j, that is, $x \in C$.

III. Iterative higher derivations are defined, and their relation to purely inseparable extensions is characterized in this section.

A higher derivation $D = \{D^{(j)} \mid 0 \leqq j < m\}$ is called iterative if and only if

$$\binom{i+j}{i} D^{(i+j)} = D^{(i)}D^{(j)} \quad \text{for all } i,j \text{ such that } 0 \leqq i,j,\ i+j < m. \tag{3}$$

Suppose F is a field of prime characteristic p. Let D be an iterative higher derivation in F.

(3) yields, in particular

$$\binom{jp^i}{p^i} D^{(jp^i)} = D^{((j-1)p^i)} D^{(p^i)}.$$

In a field of prime characteristic p, the identity $(1+x)^{jp^i} = (1+x^{p^i})^j$ holds. Hence,

$$\binom{jp^i}{p^i}$$

is congruent to $j \bmod p$, and the above may be written $jD^{(jp^i)} = D^{((j-1)p^i)}D^{(p^i)}$. By induction on j, one finds that $(jp^i)!/(p^i!)^j$ is congruent to $j! \bmod p$, and that $j!D^{(jp^i)} = (D^{(p^i)})^j$. Now, one shows by induction on n that if $r = j_0 + j_1 p + \cdots + j_n p^n$ with $0 \leqq j_k < p$, then,

$$j_0!\, j_1! \cdots j_n!\, D^{(r)} = (D^{(1)})^{j_0} (D^{(p)})^{j_1} \cdots (D^{(p^n)})^{j_n}. \tag{4}$$

The coefficient on the sinister side of (4) is not zero. Thus, if $D^{(p^i)} = 0$, $0 \leqq r \leqq n$, then, $D^{(r)} = 0$ for all r such that $0 < r < p^{n+1}$. If D is not trivial, if follows that the smallest $q > 0$ for which $D^{(q)} \neq 0$ has the form p^s.

Suppose that D also has finite rank k. Let $r+1$ be the least integer such that $k < p^{r+1}$ and C be the subfield of D-constants. Set $F_0 = F$ and, for $i = 0, \cdots, r$, define F_{i+1} to be the set of all $x \in F$ such that $D^{(1)}(x)$, $D^{(2)}(x), \cdots, D^{(p^i)}(x)$ are all equal to zero. Then, each F_i is a subfield of F_{i-1}, and one has

$$F = F_0 = \cdots = F_s \supset F_{s+1} \supset \cdots \supset F_r \supset F_{r+1} = C.$$

According to (2), $(D^{(p^{i-1})}(x))^p = D^{(p^i)}(x^p)$. Hence, if $x \in F_i$, $x^p \in F_{i+1}$ and F_i has, at most, exponent 1 over F_{i+1}. On the other hand, according to Theorem 1, F has at least exponent $r+1-s$ over C. Hence, $F_i \neq F_{i+1}$, that is, F_i has exponent one over F_{i+1} for $i = s, \cdots, r$, and F has exponent $r+1-s$ over C.

$D^{(p^i)}$ induces a derivation T_i on F_i with constant field F_{i+1} where $i = 1, \cdots, r$. Moreover, $T_i \neq 0$ for $i = s, \cdots, r$. According to (4), $(D^{(p^{i-1})})^p = p!D^{(p^i)} = 0$. Therefore, $T_i^p = 0$ for $i = s, \cdots, r-1$, and F_i has dimension less than or equal to p over F_{i+1} for $i = s, \cdots, r-1$ [4, p. 218]. The preceding results show that the dimension cannot be less than p. Hence, F_i has dimension p over F_{i+1} for $i = s, \cdots, r-1$.

Since F has exponent $r+1-s$ over C, there is an $x \in F = F_0$ such that $x^{p^t} \in F_{s+t}$, but $x^{p^t} \notin F_{s+t+1}$ where $t = 0, 1, \cdots, r-s$. Hence, $F = F_r(x)$, $x^{p^{r-s}} \in F_r$, but $x^{p^{r-s}} \notin C$. Since F_r has exponent 1 over C, one can find a set A of elements of F_r such that $A \cup \{x^{p^{r-s}}\}$ is a sub-basis for F_r. Then $A \cup \{x\}$ is clearly a sub-basis for F.

Baer showed that for any purely inseparable extension having exponent one over C, there is a derivation taking the value 1 for an arbitrarily chosen element not in C and having C as its constant subfield.

Suppose that F has a sub-basis of the form $\{x\} \cup A$, where x has exponent $e > 1$ over C and the elements of A have exponent one over C. Then, $B = C(x^{p^{e-1}}, A)$ has exponent one and sub-basis $\{x^{p^{e-1}}\} \cup A$ over C. Thus, there exists a derivation D^* in B such that $D^*(x^{p^{e-1}}) = 1$, and C is the subfield of D^*-constants.

Let t be the coset of X in the ring $F[X]/X^{p^e}F[X] = F(t)$. Then, $t^{p^e} = 0$, and $\phi\colon b \to b + D^*(b)t^{p^{e-1}}$ is a C-monomorphism of B into $F(t)$. Since $D^*(x^{p^{e-1}}) = 1$ and $(x+t)^{p^{e-1}} = x^{p^{e-1}} + t^{p^{e-1}}$, it is clear that ϕ can be uniquely extended to a C-monomorphism of $F = B(x)$ into $F(t)$ such that $\phi(x) = x + t$. This monomorphism ϕ gives rise to a higher derivation D by writing for each $u \in F$

$$\phi(u) = u + D^{(1)}(u)t + \cdots + D^{(j)}(u)t^j + \cdots + D^{(p^{e-1})}(u)t^{p^{e-1}}.$$

It is clear from the definition of ϕ that the restrictions of D to B and $C(x)$ respectively are iterative. Now, one can compute directly that if

$$D^{(i)}D^{(j)}(a_k) = \binom{i+j}{i} D^{(i+j)}(a_k), \quad k = 1, 2,$$

then,

$$D^{(i)}D^{(j)}(a_1a_2) = \binom{i+j}{i} D^{(i+j)}(a_1a_2).$$

Hence, one concludes that D is iterative.

It remains to show that C is the subfield of D-constants. Suppose that $g(x^{p^i}) = \sum\{a_j x^{jp^i} | 0 \leqq j < p^{e-i}\}$, where $a_j \in C(A)$ and $0 \leqq i \leqq e$ is a D-constant. If $i < e - 1$, since $D^{(p^i)}(a) = 0$ for all $a \in C(A)$, one has

$$0 = D^{(p^i)}(g(x^{p^i})) = \sum a_j D^{(p^i)}(x^{jp^i}) = \sum j a_j x^{(j-1)p^i}.$$

Thus, if p does not divide j, $a_j = 0$. Hence, $g(x^{p^i}) = h(x^{p^{i+1}})$. Carrying out this procedure for $i = 0, \cdots, e - 2$ yields the fact that all D-constants must lie in B. By the definition of D they are D^*-constants, and so they lie in C.

These results can be summed up as follows:

THEOREM 2. *A purely inseparable extension F of C has a sub-basis of the form $\{x\} \cup A$, where the exponent of x over C is arbitrary and the elements of A have exponent one over C, if and only if there exists a finite iterative higher derivation in F having C as its subfield of constants.*

IV. Two basic theorems on purely inseparable extensions and higher derivations are proved in this section. Theorem 3 is concerned with the existence of subfields of a purely inseparable extension which are maximal with respect to set inclusion among subfields having a sub-basis. The characterizing property is not directly amenable to the use of Zorn's lemma, and so the proof is not trivial. Sufficient conditions are given; the question of necessary and sufficient conditions is open. This theorem is applied to the proof of Theorem 4 which states that the existence of a higher derivation implies that the purely inseparable extension has to have a sub-basis. In general, even finite extensions of exponent greater than one are not so benign as to be a tensor product of simple purely inseparable extensions.

The following notation is used: $A^r = \{a^r | a \in A\}$.

Let L be a field having prime characteristic p and M be a subfield of L. For any subset S of L, A is called a p-free subset of S relative to M if and only if $a^p \in M$, $a \in S$ and $a \notin M(A - \{a\})$ for any $a \in A$. Note that A is p-free relative to M if and only if

(i) $A^p \subseteq M$,

(ii) the monomials of the form $a_1^{k_1} \cdots a_n^{k_n}$ with $a_i \in A$ and $0 \leqq k_i < p$ are linearly independent over M.

Evidently, condition (i) is necessary. If it is satisfied, each element $a \in A$ is a root of a polynomial of the form $X^p - m$ with $m \in M$. Also, $X^p - m$ is reducible over $M(A - \{a\})$ if and only if there is a $y \in M(A - \{a\})$ such that $y^p = m = a^p$, that is, if and only if $a = y \in M(A - \{a\})$. Hence, (ii) is true if and only if $a \notin M(A - \{a\})$ for any $a \in A$.

The p-free subsets of S relative to M which are maximal with respect to

set inclusion among such sets are called maximal p-free subsets of S relative to M. An application of Zorn's lemma yields the result that any p-free subset of S relative to M can be extended to a maximal p-free subset of S relative to M. By a proof analogous to that of Chevalley([4]) for vector spaces, one can show that all maximal p-free subsets of S relative to M have the same cardinality.

Now, suppose F is a purely inseparable extension having exponent e over C. Let $B_e^{p^{e-1}}$ be a maximal p-free subset of $F^{p^{e-1}}$ relative to C. Clearly $F^{p^{e-1}} \subseteq F^{p^{e-2}}$. Extend $B_e^{p^{e-1}}$ to a maximal p-free subset A_{e-1} of $F^{p^{e-2}}$ relative to C. Define B_{e-1} by the conditions: $B_{e-1}^{p^{e-2}} \cup B_e^{p^{e-1}} = A_{e-1}$, $B_{e-1}^{p^{e-2}} \cap B_e^{p^{e-1}} = \emptyset$. In general, let A_{e-i} be an extension of A_{e-i+1} to a maximal p-free subset of $F^{p^{e-i-1}}$ relative to C, where $i = 1, \cdots, e-1$. Define B_{e-i} by the conditions: $B_{e-i}^{p^{e-i-1}} \cup A_{e-i+1} = A_{e-i}$ and $B_{e-i}^{p^{e-i-1}} \cap A_{e-i+1} = \emptyset$. Set $B = B_e \cup B_{e-1} \cup \cdots \cup B_1$. It is claimed that B is a sub-basis for $C(B)$.

In order to prove the last statement, first well-order B so that if $x \in B_i$ and $y \in B_j$ with $i < j$, then $y < x$. Suppose u is the least element, $u \in B_e$ since F has exponent e over C. One has $u^{p^{e-1}} \notin C$. Hence, $\{u\}$ is a sub-basis for $C(u)$.

Now, let u be an arbitrary element of B, and let $A_u = \{x \mid x \in B \text{ and } x < u\}$. Assume that A_u is a sub-basis for $C(A_u)$. Suppose that $u \in B_r$. Then, $u^{p^r} = c \in C$ and $u^{p^{r-1}} \notin C(B_e^{p^{e-1}} \cup \cdots \cup B_{r+1}^{p^r} \cup (B_r - \{u\})^{p^{r-1}})$. It is readily shown that these facts imply that $x^{p^r} - c$ is irreducible over $C(A_u)$, and hence, that $A_u \cup \{u\}$ is a sub-basis for $C(A_u, u)$. By induction, B is a sub-basis for $C(B)$.

It is further claimed that $C(B)$ is maximal with respect to set inclusion among subfields of F having a sub-basis over C.

Suppose that L is a subfield of F having a sub-basis E over C and containing $C(B)$. Let E_i be the subset of E consisting of the elements having exponent i over C, where $i = 1, \cdots, e$. Let B be well-ordered as before. It will be shown that B is a sub-basis for L, and therefore, $L = C(B)$. The method consists of generating a new sub-basis for L, starting with replacing E_e by B_e and stepping down in exponent. Each step has the same proof.

Suppose that L has a sub-basis, call it E, again such that $E_e = B_e, \cdots, E_{r+1} = B_{r+1}$. If $B_r = \emptyset$, then $A_r = B_e^{p^{e-1}} \cup \cdots \cup B_{r+1}^{p^r}$ is a maximal p-free subset of $F^{p^{r-1}}$ relative to C. If E_r were not empty, then since $E_r^{p^r} \subseteq C$, $A_r \cup E_r^{p^{r-1}}$ cannot be a p-free subset of F relative to C. This fact would contradict the hypothesis that E is a sub-basis. Hence, $B_r = \emptyset$ implies that $E_r = \emptyset$. Now, suppose that $B_r \neq \emptyset$. Let u be the least element of B_r that

([4]) S. Lefschetz, *Algebraic topology*, Amer. Math. Soc. Colloq. Publ. Vol. 27, Amer. Math. Soc., Providence, R. I., 1942; p. 73.

does not belong to E_r. Set $A_u = \{w | w \in B \text{ and } w < u\}$. Then, A_u contains $B_{r+1} = E_{r+1}, \cdots, B_e = E_e$.

One can write

$$u = \sum a_{i_1 \cdots i_n} v_1^{i_1} \cdots v_n^{i_n},$$

where $v_1, \cdots, v_n \in E_r$, $v_1, \cdots, v_n \notin A_u$ and $a_{i_1, \cdots, i_n} \in C(E_1, \cdots, E_{r-1}, A_u)$.

If all the exponents i_s were divisible by p, then $u^{p^{r-1}}$ would be in $C(A_u^{p^{r-1}})$, and this statement would contradict the fact that the subset $A_u \cup \{u\}$ of B is a sub-basis over C. Hence, there is a nonzero term in the expression for u in which the exponent i_s of v_s is not divisible by p. It follows that $u^{p^{r-1}} \notin C(E - \{v_s\})$, since $A_u \subset E$ and E is a sub-basis. Hence, u is of degree p^r over $C(E - \{v_s\})$.

One can write

$$u^i = \sum \{a_{ij} v_s^j | \ 0 \leqq j < p^r\},$$

where $a_{ij} \in C(E - \{v_s\})$ and $i = 0, \cdots, p^r - 1$. Since the elements $1, u, \cdots, u^{p^r} - 1$ are linearly independent over $C(E - \{v_s\})$, the determinant formed from the coefficients a_{ij} is not zero. Therefore,

$$v_s \in C((E - \{v_s\}) \cup \{u\}).$$

Now, it is clear that if E' is the set $(E - \{v_s\}) \cup \{u\}$, then E' is still a sub-basis for L over C, $E_j' = E_j = B_j$ for $j > r$, and E_j' contains all $w \in B$ such that $w \leqq u$. By induction and the maximum properties of B, it follows that one can replace E with a new sub-basis E^* such that $E_j^* = B_j$ for all $j \geqq r$. Now, an induction on r shows that B is still a sub-basis for L over C, i.e., that $L = C(B)$.

It is clear that B has the following property: every element of F having exponent s over C is either in $C(B_e \cup B_{e-1} \cup \cdots \cup B_s)$ or has exponent less than s over $C(B_e \cup B_{e-1} \cup \cdots \cup B_s)$.

The cardinal number of B is the cardinal number of A_1, a maximal p-free subset of F relative to C. If L is a subfield of F having a sub-basis E over C and also maximal with respect to set inclusion, then $E^* = E_e^{p^{e-1}} \cup E_e^{p^{e-2}} \cup \cdots \cup E_1$, where E_j consists of those elements of a sub-basis E of L having exponent j over C is readily shown to be a maximal p-free subset of F relative to C. That E^* is p-free is clear since E is a sub-basis. If E^* were not maximal p-free then one could find an $x \in F$, $x \notin L$ such that $E^* \cup \{x\}$ was p-free. But then $L(x)$ properly contains L and has the sub-basis $E^* \cup \{x\}$ which contradicts the maximality of L. Therefore the cardinality of the sub-basis of any subfield of F maximal among subfields of F having a sub-basis over C is unique.

These results are summed up in the following theorem.

THEOREM 3. *Let F be a purely inseparable extension having exponent e over C. Then, among the subfields of F having a sub-basis over C there is a maximal subfield with respect to set inclusion. A sub-basis B of such a maximal subfield can be chosen so that any element of F having exponent s over C either belongs to $C(B_e \cup B_{e-1} \cup \cdots \cup B_s)$ or has exponent less than s over $C(B_e \cup B_{e-1} \cup \cdots \cup B_s)$ where B_i consists of the elements of B having exponent i over C. The cardinal number of a sub-basis of such a maximal subfield is unique.*

Consider the following purely inseparable extension: $C(u_1, u_2, \cdots)$ where $u_1^p \in C$ and $u_{i+1}^p = u_i$ for $i = 1, 2, \cdots$. Every subfield is contained in some subfield of the increasing sequence,

$$C(u_1) \subset C(u_2) \subset \cdots \subset C(u_n) \subset \cdots.$$

Thus, the only candidate for maximality is $C(u_1, u_2, \cdots)$ itself. Given any two elements $x, y \in C(u_1, u_2, \cdots)$, there is a u_n such that $x = \sum a_i u_n^i$ and $y = \sum b_j u_n^j$. It follows that x and y cannot form a sub-basis because u_n can be eliminated and either x or y can be expressed in terms of the other. Since no single element generates the field, it fails to have the desired maximal subfield. This example shows that F must have an additional condition besides pure inseparability over C in order that the conclusion of Theorem 3 hold.

THEOREM 4. *Let F be a purely inseparable extension having exponent e over C and D be a higher derivation in F having C as its subfield of constants. Then F has a sub-basis over C.*

Proof. Suppose that K is a subfield of F maximal among subfields of F having a sub-basis over C. The maximality of K implies that K contains all elements of F having exponent one over C. Suppose that K contains all elements of F of exponent less than r over C where $r > 1$. It will be shown that K contains all elements of exponent r over C. Consequently, by induction, K would equal F.

Let B be a sub-basis for K over C such that every element of F having exponent s over C either belongs to $C(B_e \cup B_{e-1} \cup \cdots \cup B_s)$ or has exponent less than s over $C(B_e \cup B_{e-1} \cup \cdots \cup B_s)$ where B_i is the set of elements of B having exponent i over C.

Suppose that $u \in F$ has exponent r over C and that $u \notin K$. Let u be a root of $X^{p^r} - c$. Then, $X^{p^r} - c$ is reducible over $C(B_e \cup B_{e-1} \cup \cdots \cup B_r)$, and one can write

$$u^{p^s} = a_1 v_1^{p^s} + \cdots + a_n v_n^{p^s}, \tag{5}$$

where $a_j \in C$, $v_j \in K$, $s < r$, s is the smallest exponent for which a relation

(5) holds and n is chosen so that this relation has the smallest number of terms. Clearly, $s \geqq 1$; otherwise, $u \in K$. It is claimed that $n > 1$; otherwise u/v_1 has exponent s over C and so, because K contains all elements of exponent $s < r$ over C, u/v_1 is in K, which puts u in K.

Since K contains all elements of F having exponent one over C, $K^p \cap C = F^p \cap C$. Hence, if all the $a_j \in F^p$, then they belong to K^p. But then, by taking pth roots in (5), one could reduce s by 1 and contradict the minimality of s. Thus, not all the a_j are in F^p. Suppose that $\{a_1, \cdots, a_k\}$ is a maximal p-free subset of $\{a_1, \cdots, a_n\}$ relative to K^p and that $\{a_1, \cdots, a_j\}$ is a maximal p-free subset of $\{a_1, \cdots, a_k\}$ relative to F^p. $j < k$ because if one expresses $a_{k+1}, \cdots, a_n$ in terms of $a_1, \cdots, a_k$ in (5), one finds that $a_1, \cdots, a_k$ are not p-free relative to F^p. Thus, one can write

$$(6) \qquad a_{j+1} = \sum \{ y^p_{i_1 \cdots i_j} a_1^{i_1} \cdots a_j^{i_j} \mid y_{i_1 \cdots i_j} \in F, 0 \leqq i_n < p, n = 1, \cdots, j \}.$$

Not all the $y_{i_1 \cdots i_j}$ can have exponent one over C because they would then be in K and violate the p-freedom of $a_1, \cdots, a_{j+1}$ relative to K^p. Let g be the least positive integer for which there is a coefficient $y_{i_1 \cdots i_j}$ such that $D^{(g)}(y_{i_1 \cdots i_j}) \neq 0$. According to Theorem 1, $D^{(gp)}$ must be defined. Applying $D^{(gp)}$ to (6) yields

$$0 = \sum (D^{(g)}(y_{i_1 \cdots i_j}))^p a_1^{i_1} \cdots a_j^{i_j}.$$

This relation is not trivial and violates the p-freedom of $a_1, \cdots, a_j$ relative to F^p. Therefore, K must contain all elements of F having exponent r over C.

Thus, a higher derivation with the requisite properties cannot exist in F unless F has a sub-basis over C.

V. In this section a theorem on extending higher derivations and an existence theorem are proved.

While a proof of the existence theorem could be obtained, perhaps, more directly, it was the author's desire to obtain a direct generalization of the theorem due to Baer for the case of purely inseparable extensions of exponent one. Baer made use of the fact that a nonintegrable element of K, that is, an element that does not belong to the range of the given derivation in K, could be used to extend the derivation to an extension of K. Considering the sequence of mappings involved in defining higher derivations, the question of how to define the nonintegrability of a single element, at first glance, appears to be almost meaningless. But this is not the case. By studying the problem of making extensions of higher derivations, a sensible notion of nonintegrability can be attained.

The notion of nonintegrability for a derivation can be formulated as follows: If D is a derivation in K, and C is the subfield of D-constants, then a nonzero element of K is nonintegrable if and only if the equation

$$D(x) = c\alpha, \qquad c \in C$$

has a solution in K only when $c = 0$. This definition will correspond to nonintegrability of order zero in the general case. In general, let K be a field of prime characteristic p, $D = \{ D^{(j)} \mid 0 \leqq j \leqq m \}$ be a higher derivation in K, and C be the subfield of D-constants. A nonzero element $\alpha \in K$ is called nonintegrable of order s in K if and only if the following condition holds: If the set of equations

$$D^{(jp^s)}(x) = c_j \alpha^j \quad \text{for all } j \text{ such that } 0 < jp^s < m,$$

$$D^{(r)}(x) = 0 \quad \text{for the remaining indices } r \text{ with } 0 < r < m,$$

where $c_j \in C$, has a solution $x \in K$, then $c_j = 0$ for all j such that $0 < jp^s < m$.

The extension theorem can now be stated.

THEOREM 5. *Let F be a field of prime characteristic p, K be a subfield of F, $D_0 = \{ D_0^{(n)} \mid 0 \leqq n < m \}$ a higher derivation in K, C be the subfield of D_0-constants and $p^{r-1} < m < p^r$, $r \geqq 1$. Let $t \in F$ be a root of $X^{p^e} - c$, $c \in C$, $e \leqq r$, where $X^{p^e} - c$ is irreducible over K. Let $\alpha \in K$ be nonintegrable of order $r - e$ in K.*

Then there exists a higher derivation $D = \{ D^{(n)} \mid 0 \leqq n < m \}$ in $K(t)$ with the following properties:

(1) *$D^{(n)}(x) = D_0^{(n)}(x)$ for all $x \in K$ and all n, $0 \leqq n < m$;*

(2) *C is the subfield of D-constants;*

(3) *$\alpha^{p^{s-r+e}} t^{p^e - 1}$ is nonintegrable of order $s \geqq r - e$ in $K(t)$.*

Proof. The first step consists in defining D so that requirement (1) is fulfilled. One proceeds by defining a higher derivation $D_1 = \{ D_1^{(n)} \mid 0 \leqq n < m \}$ in the polynomial ring $K[X]$ as follows:

$$D_1^{(n)}(y) = D_0^{(n)}(y) \quad \text{for all } y \in K \text{ and all } n,\ 0 \leqq n < m;$$

$$D_1^{(p^{r-e})}(X) = \alpha;$$

$$D_1^{(j)}(X) = 0 \quad \text{for all } j,\ 0 < j < p^r,\ j \neq p^{r-e}.$$

It is convenient in carrying out the computations to set $\binom{g}{h} = 0$ if $g < h$ and to set $D_1^{(n)}$ formally equal to zero for all integers distinct from $0, 1, 2, \cdots, m - 1$. The latter convention must be used with care in order that no extra relations are imposed. Note that with this convention and the proviso that $0 \leqq k < m$, one can write formula (1) as follows:

$$D^{(k)}(xy) = \sum \{ D^{(k-j)}(x) D^{(j)}(y) \mid 0 \leqq j < \infty \} \tag{7}$$

for any higher derivation $D = \{ D^{(j)} \mid 0 \leqq j < m \}$.

If Y is a formal variable, X has the representation D_1: $X \to X + \alpha Y^{p^{r-e}}$. For $i \geqq 0$,

$$X^{kp^i} \to (X + \alpha Y^{p^{r-e}})^{kp^i} = (X^{p^i} + \alpha^{p^i} Y^{p^{r-e+i}})^k$$

$$= X^{kp^i} + \binom{k}{1} X^{(k-1)p^i} \alpha^{p^i} Y^{p^{r-e+i}} + \cdots + \alpha^{kp^i} Y^{kp^{r-e+i}}.$$

Thus

$$(8) \quad D_1^{(n)}(X^{kp^i}) = \begin{cases} \binom{k}{q} X^{(k-q)p^i} \alpha^{qp^i} \text{ when } n = qp^{r-e+i} < m, \\ 0 \text{ for the remaining indices } n \text{ such that } 0 < n < m. \end{cases}$$

Since $X^{p^e} - c$ is irreducible over K, $K(t)$ is isomorphic to

$$K[X]/(X^{p^e} - c)K[X].$$

One finds that $X^{p^e} - c$ is a D_1-constant, and, consequently, that the ideal $(X^{p^e} - c)K[X]$ is invariant under D_1. Hence D_1 induces in the natural way a higher derivation $D = \{D^{(j)} \mid 0 \leqq j < m\}$ in $K(t)$. Here t corresponds to the coset of X. Note that formula (8) holds for X replaced by t and D_1 replaced by D.

From the construction it is clear that assertion (1) of the theorem is valid.

Next one calculates the image of any element of $K(t)$ under D.

Suppose that

$$(9) \qquad g(t^{p^i}) = \sum \{a_k t^{kp^i} \mid 0 \leqq k \leqq f\},$$

where $a_k \in K$ for all k, $0 \leqq i < e$, and f is the largest integer such that $fp^i < p^e$.

For $0 < n < m$, by applying formulas (7) and (8),

$$D^{(n)}(a_k t^{kp^i}) = \sum \{D^{(n-j)}(a_k) D^{(j)}(t^{kp^i}) \mid j \geqq 0\}$$

$$= \sum \left\{ D^{(n-qp^{r-e+i})}(a) t^{(k-q)p^i} \binom{k}{q} \alpha^{qp^i} \mid q \geqq 0 \right\}.$$

One can alter the last sum to $0 \leqq q \leqq f$ because $(f+1)p^{i-e+r} \geqq p^r$ and $n < m \leqq p^r$ and hence the terms that are dropped are zero by the previously given convention. Thus, for $0 < n < m$

$$D^{(n)}(g(t^{p^i})) = \sum \left\{ \sum \left\{ D^{(n-qp^{r-e+i})}(a_k) t^{(k-q)p^i} \binom{k}{q} \alpha^{qp^i} \mid 0 \leqq q \leqq f \right\} \mid 0 \leqq k \leqq f \right\}.$$

Since

$$\binom{k}{q} = 0 \quad \text{if } k < q,$$

the last sum can be changed to $q \leqq k \leqq f$. Finally, by setting $k - q = h$, one obtains

$$D^{(n)}(g(t^{p^i}))$$

$$(10)\qquad = \sum \left\{ \sum \binom{q+h}{q} \left\{ D^{(n-qp^{r-e+i})}(a_{q+h}) t^{hp^i} \alpha^{qp^i} \mid 0 \leqq q \leqq f-h \right\} \mid 0 \leqq h \leqq f \right\}$$

The proof of assertion (2) rests on the following lemma:

LEMMA. *Let g satisfy conditions* (9) *and $D^{(n)}(g(t^{p^i})) = 0$ for all n, $0 < n < m$. Then $g(t^{p^i}) = h(t^{p^{i+1}})$, where h is a polynomial in $t^{p^{i+1}}$ of degree less than p^e with coefficients in K.*

Using formulas (10) and the hypotheses of the lemma, one obtains the following sequence of equations:

$$D^{(n)}(a_f) = 0 \quad (\text{from } h = f);$$

$$D^{(n)}(a_{f-1}) + \binom{f}{1} D^{(n-p^{r-e+i})}(a_f) \alpha^{p^i} = 0 \quad (\text{from } h = f-1);$$

$$\cdots$$

$$D^{(n)}(a_{f-w}) + \binom{f-w+1}{1} D^{(n-p^{r-e+i})}(a_{f-w+1}) \alpha^{p^i} +$$

$$\cdots \quad + \binom{f-w+u}{u} D^{(n-up^{r-e+i})}(a_{f-w+u}) \alpha^{up^i} +$$

$$\cdots \quad + \binom{f}{w} D^{(n-up^{r-e+i})}(a_f) \alpha^{up^i} = 0 \quad (\text{from } h = f-w);$$

$$\cdots$$

$$D^{(n)}(a_0) + D^{(n-p^{r-e+i})}(a_1) \alpha^{p^i} + \cdots + D^{(n-fp^{r-e+i})}(a_f) \alpha^{fp^i} = 0$$

$$(\text{from } h = 0); \quad \text{for all } n,\ 0 < n < m.$$

The first equation of (11) gives $D^{(n)}(a_f) = 0$ for all n, $0 < n < m$. Since $a_f \in K$, these conditions imply that $a_f \in C$. The second equation of (11) can be written as follows: $D^{(n)}(a_{f-1}) = 0$ for all $n \neq p^{r-e+i}$, $0 < n < m$ (either by convention or hypothesis)

$$D^{(p^{r-e+i})}(a_{f-1}) = -\binom{f}{1} a_f \alpha^{p^i}.$$

Setting

$$j = p^i, \quad s = r - e, \quad c_j = -\binom{f}{1} a_f,$$

and applying the hypothesis on α and the definition of nonintegrability of order $r - e$ to α, one obtains $fa_f = 0$. Hence, either p divides f or $a_f = 0$. In any case, $D^{(n)}(a_{f-1}) = 0$ for all n, $0 < n < m$ and since $a_{f-1} \in K$, $a_{f-1} \in C$.

At this point one proceeds by induction. Suppose that $a_v = 0$ or p divides v for $v = f, f-1, \cdots, f-w+2$ and $a_v \in C$ for $v = f, f-1, \cdots, f-w+1$. It will be shown that $a_{f-w+1} = 0$ or p divides $f-w+1$ and that $a_{f-w} \in C$. Equations (11), the hypotheses of the lemma, the convention, and the inductive hypotheses yield the following equations:

$$D^{(n)}(a_{f-w}) = 0 \quad \text{for } n \neq up^{r-e+i}, \qquad u = 1, \cdots, w,\ 0 < n < m,$$

$$D^{(up^{r-e+i})}(a_{f-w}) = -\binom{f-w+u}{u} a_{f-w+u}\alpha^{up^i}, \qquad u = 1, \cdots, w.$$

Setting

$$j = up^i,\ c_j = -\binom{f-w+u}{u} a_{f-w+u} \text{ and } s = r-e,$$

and applying the hypothesis on a definition of nonintegrability of order $r-e$ to α yields the following result in particular $(u = 1)$, $(f-w+1)a_{f-w+1} = 0$. Thus either $a_{f-w+1} = 0$ or $f-w+1$ is divisible by p. Moreover, one has $D^{(n)}(a_{f-w}) = 0$ for all n, $0 < n < m$ and $a_{f-w} \in K$. Hence $a_{f-w} \in C$.

Thus applying induction, one can state that $a_v = 0$ or p divides v for all v, $0 \leqq v \leqq f$. This fact implies that $g(t^{p^i}) = h(t^{p^{i+1}})$ with h satisfying the conditions of the lemma.

Assertion (2) is proved by repeated application of the lemma until i reaches e. In that case $g(t^{p^i}) \in K$ and being a D-constant in K, it must belong to C. Finally assertion (3) will be proved.

Suppose that $x = \sum \{a_k t^k \mid 0 \leqq k < p^e\}$ is a solution of the system of equations

$$D^{(jp^s)}(x) = c_j(\alpha^{p^{s-r+e}} t^{p^{e-1}})^j = c_j \alpha^{jp^{s-r+e}} c^{j-1} t^{p^e-j},$$

$$c_j \in C, \text{ and all } j \text{ such that } 0 < jp^s < m, \tag{12}$$

$$D^{(n)}(x) = 0 \quad \text{for all other indices } n \text{ with } 0 < n < m.$$

Formula (10) with $i = 0$ and $f = p^e - 1$ can be applied to the sinister side of (12) and one obtains the following system of equations, for each j such that $0 < jp^s < m$,

$$\begin{aligned} &D^{(jp^s)}(a_{p^e-j}) + \binom{p^e-j+1}{1} D^{(jp^s-p^{r-e})}(a_{p^e+1})\alpha + \\ &\qquad \cdots + \binom{p^e-1}{j-1} D^{(jp^s-(j-1)p^{r-e})}(a_{p^e-1}) = c^{j-1}c_j\alpha^{jp^{s-r+e}}, \\ &D^{(n)}(a_{p^e-w}) + \binom{p^e-w+1}{1} D^{(n-p^{r-e})}(a_{p^e-w+1})\alpha + \\ &\qquad \cdots + \binom{p^e-1}{w-1} D^{(n-(w-1)p^{r-e})}(a_{p^e-1})\alpha^{w-1} = 0 \end{aligned} \tag{13}$$

whenever $n \neq jp^s$ or $w \neq j$, $0 < n < m$, $0 \leqq w \leqq p^e - 1$.

Taking $w = 1$ in the system (13), one gets

$$D^{(n)}(a_{p^e-1}) = 0, \quad n \neq p^s,\ 0 < n < m,$$

$$D^{(p^s)}(a_{p^e-1}) = c_1\alpha^{p^{s-r+e}} = D^{(p^{s-r+e}p^{r-e})}(a_{p^e-1}).$$

The definition of nonintegrability of order $r - e$ and the hypothesis on α can be applied to yield $c_1 = 0$. One also obtains $a_{p^e-1} \in C$. One proceeds by induction. Suppose that $c_1, \cdots, c_{j-1}$ are all zero and $a_{p^e-1}, \cdots, a_{p^e-j+1}$ all belong to C. Then equations (13) yield (taking into account $s \geqq r - e$)

$$D^{(jp^s)}(a_{p^e-j}) = D^{(jp^{s-r+e}p^{r-e})}(a_{p^e-j}) = c^{j-1}c_j\alpha^{jp^{s-r+e}},$$

$$D^{(up^{r-e})}(a_{p^e-j}) = -\binom{p^e - j + u}{u} a_{p^e-j+u}\alpha^u, \quad u = 1, \cdots, j-1, \tag{14}$$

$$D^{(n)}(a_{p^e-j}) = 0 \quad \text{for all other indices } n \text{ with } 0 < n < m.$$

Applying the hypothesis of the nonintegrability of order $r - e$ in K of α and the definition of nonintegrability, one finds all dexter sides of (14) are zero. In particular since c and α are not zero, $c_j = 0$. Moreover $a_{p^e-j} \in C$. Applying induction, one obtains that all the c_j in equations (12) are zero and this fact is exactly what is required to prove assertion (3).

Finally an existence theorem is proved.

THEOREM 6. *Let F be a purely inseparable extension of C having exponent r and a sub-basis A over C. Then, there exists a higher derivation $D = \{D^{(j)} \mid 0 \leqq j < m\}$, $p^{r-1} < m < p^r$, in F such that C is the subfield of D-constants.*

Proof. Let q be the least integer such that the set B' of elements of A having exponent $\geqq q$ is finite. Let B be the complement of B' in A. B is either empty or infinite. If B is infinite, one can well-order B so that $u \in B$ has a successor u' whose exponent over C is not less than the exponent of u over C. Define a higher derivation

$$D_0 = \{D_0^{(n)} \mid 0 \leqq n < m\} \quad \text{in } C(B) \text{ as follows:}$$

$$D_0^{(n)}(x) = 0 \quad \text{for all } x \in C \text{ and all } n,\ 0 < n < m,$$

$$D_0^{(p^{r-e})}(u) = uu' \quad \text{if } u \in B \text{ has exponent } e \text{ over } C,$$

$$D_0^{(n)}(u) = 0 \quad \text{for all other indices } n,\ 0 < n < m.$$

One finds

$$D_0^{(jp^{r-e})}(u^i) = \binom{i}{j} u^i(u')^j$$

for any $u \in B$ having exponent e over C.

Suppose $x \in C(B)$ is a D_0-constant and $x \notin C$. Write

$$x = \sum \{a_i u^i \mid 0 \leqq i < p^e\},$$

where u is the largest element of B appearing nontrivially ($a_1, \cdots, a_{p^e-1}$ independent of u and not all zero) and u has exponent e over C. Then

$$D_0^{(kp^{r-e})}(x) = \sum \left\{ \sum \left\{ D_0^{(k-j)p^{r-e}}(a_i) \binom{i}{j} u^i (u')^j \mid 0 \leqq j \leqq k \right\} \mid 0 \leqq i < p^e \right\} = 0.$$

The coefficients a_i are independent of u and u', and u' has exponent not less than e. Hence the powers $u^i(u')^j$, $0 \leqq i, j \leqq p^e$ are linearly independent over the field $C(B - \{u, u'\})$. Setting $j = 1$ and $k = 1$ gives $ia_i = 0$ for all i not divisible by p. $j = p$ and $k = p$ give $\binom{i}{p} a_i = 0$. Hence $a_i = 0$ for all i not divisible by p^2. And so on. Therefore, $a_i = 0$ for all $i \neq 0$. Hence, u appears trivially which is a contradiction. Therefore, if $x \in C(B)$ is a D_0-constant, then $x \in C$.

Next it will be shown that 1 is nonintegrable of order 0 in $C(B)$; that is, it will be shown that if the equations

$$D_0^{(n)}(x) = c_n \in C,\ 0 < n < p^r$$

have a solution $x \in C(B)$, then $c_n = 0$ for all n. It follows from the definition of $D_0^{(n)}$ that $D_0^{(n)}(x) = 0$ or $D_0^{(n)}(x) \notin C$ for $x \in C(B)$ (one gets zero or one does not lower degrees of monomials). Therefore, 1 is nonintegrable of order zero.

To complete the construction, if $q > r$, set $D = D_0$. Otherwise, let $B' = \{u_1, \cdots, u_m\}$, where $r = e_1 \geqq e_2 \geqq \cdots \geqq e_m$, e_i being the exponent of u_i over C. One extends D_0 to $C(B \cup \{u_i\})$, then to $C(B \cup \{u_1, u_2\})$, and so on, by means of Theorem 5.

References

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ. Vol. 24, Amer. Math. Soc., Providence, R. I., 1939.

2. R. Baer, *Algebraische Theorie der Differentierbaren Funktionkörper* I, S.-B. Heidelberger Akad. Wiss. (1927), 15-32.

3. H. Hasse and F. K. Schmidt, *Noch eine Begrundung der Theorie der hoheren Differential quotienten in einem algebraischen Funktionkörper eine Unbestimmten*, J. Reine Angew. Math. **177** (1937), 215-237.

4. N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. **42** (1937), 206-224.

5. ———, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. Vol. 37, Amer. Math. Soc., Providence, R. I., 1956.

Aerospace Corporation,
San Bernardino, California