TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 198, 1974

AN INTERMEDIATE THEORY FOR A PURELY INSEPARABLE GALOIS THEORY[1]

BY
JAMES K. DEVENEY

ABSTRACT. Let K be a finite dimensional purely inseparable modular extension of F, and let L be an intermediate field. This paper is concerned with an intermediate theory for the Galois theory of purely inseparable extensions using higher derivations [4]. If L is a Galois intermediate field and M is the field of constants of all higher derivations on L over F, we prove that every higher derivation on L over F extends to K if and only if $K = L \otimes_M J$ for some field J. Similar to classical Galois theory the distinguished intermediate fields are those which are left invariant under a standard generating set for the group of all rank t higher derivations on K over F. We prove: L is distinguished if and only if L is M-homogeneous (4.9).

I. Introduction. This paper is concerned with an intermediate theory for the Galois theory of purely inseparable extensions using higher derivations [4]. In classical Galois theory, if G is a full group of automorphisms on a field C with field of constants E, then an intermediate field D is distinguished if and only if it is invariant under G. Moreover, all automorphisms on D over E can be extended to C. Let K be a finite dimensional purely inseparable modular extension of F, and let L be an intermediate field. We prove: (1) the only intermediate fields invariant under all higher derivations on K over F are of the form $F(K^{p^n})$ for some n; (2) if L is a Galois intermediate field (i.e., the field of constants of a group of higher derivations on K over F) and M is the field of constants of all higher derivations on L over F, then every higher derivation on L over F extends to K if and only if $K = L \otimes_M J$ for some field J. Combining (1) and (2) shows that the only intermediate fields with properties completely analogous to the classical case are K and F. Considering the Dedekind independence theorem for automorphisms and [7, Theorem 19, p. 186] a natural alternative is to define the distinguished intermediate fields to be those which are left invariant under a standard generating set for the group of all higher derivations on K over F. If L is a distinguished intermediate field, then K is modular over L and L is modular over F. We provide an example which shows the converse does not hold. Two conditions equivalent to being distinguished are established: (1) There exists a subbase $\{x_1, \dots, x_n\}$ for K over F such that $\{x_i^{p^{e_i}}, \dots, x_n^{p^{e_n}}\}$ is a subbase for L over

Presented to the Society, November 16, 1973; received by the editors June 27, 1973.
AMS (MOS) subject classifications (1970). Primary 12F15.
Key words and phrases. Higher derivation, iterative higher derivation, dual basis, M-homogeneous intermediate fields.
[1] This work was supported in part by the Committee on Faculty Research Support administered by Dr. Nickolas Heerema.

F for some $e_1, \ldots, e_n$; (2) There exists $T = T_1 \cup \cdots \cup T_n$ a subbase for K over F, the elements of T_i being of exponent i over F, such that $L = L \cap F(T_1) \otimes \cdots \otimes L \cap F(T_n)$ and $F(T_i)$ is modular over $L \cap F(T_i)$ for all i.

II. Definitions and preliminary results. Throughout this paper, K will be a field of characteristic $p \neq 0, 2$. A rank t higher derivation on K is a sequence $d = \{d_i \mid 0 \leq i < t+1\}$ of additive maps of K into K such that $d_r(ab) = \sum \{d_i(a)d_j(b) \mid i+j = r\}$ and d_0 is the identity map. The set $H^t(K)$ of all rank t higher derivations on K is a group with respect to the composition $d \circ e = f$ where $f_j = \sum \{d_m e_n \mid m+n = j\}$ [1, Theorem 1, p. 33]. The field of constants of a subset $G \subseteq H^t(K)$ is $\{a \in K \mid d_i(a) = 0, i > 0, (d_i) \in G\}$. $H_F^t(K)$ will denote the group of all rank t higher derivations on K whose field of constants contains the subfield F.

(2.1) [2, Theorem 1]. Let B be a p-basis for K and let $f\colon Z \times B \to K$ be an arbitrary function. There is a unique $(d_i) \in H^\infty(K)$ such that for each $b \in B$ and $i \in Z$, $d_i(b) = f(i, b)$.

A higher derivation d in $H^\infty(K)$ is called iterative of index q, or simply iterative, if $\binom{i}{j}d_{qi} = d_{qi}d_{q(i-j)}$ for all i and $j \leq i$, whereas $d_m = 0$ if $q \nmid m$. If $d \in H^\infty(K)$ is iterative of index q, and a is in K, then $ad = e$ where $e_{qi} = a^i d_{qi}$, and $e_j = 0$ if $q \nmid j$. It is clear that ad is a higher derivation. A finite rank higher derivation ($t < \infty$) is iterative if it is the first $t+1$ maps of an infinite iterative higher derivation. Given $d \in H_F^t(K)$ of index q, $V(d) = e \in H_F^t(K)$ where $e_{(q+1)i} = d_{qi}$ for $(q+1)i \leq t$ and $e_j = 0$ if $(q+1) \nmid j, j \leq t$.

Throughout the remainder of this paper, K will be a finite dimensional purely inseparable modular extension of F of exponent n, and $p^{n-1} \leq t < \infty$. Since K is modular over F, $K = F(x_1) \otimes \cdots \otimes F(x_n)$. Any such elements $x_1, \ldots, x_n$ is called a subbase for K over F.

(2.2) [3, p. 436]. Let $(d_i) \in H^t(K)$ and $a \in K$. Then $d_{ip}(a^p) = (d_i(a))^p$ and if p and j are relatively prime, then $d_j(a^p) = 0$.

(2.3) [4, Lemma 3.7]. Let K be a purely inseparable modular extension of F, and let N be a subbase for K over F. Then there exists a subset S of F such that $N \cup S$ is a p-basis for K.

(2.4) **Definition.** Let $\{x_{1,1}, \ldots, x_{1,j_1}, \ldots x_{n,1}, \ldots, x_{n,j_n}\}$ be a subbase for K over F where $x_{i,e}$ is of exponent i over F. Let $A = \{d^{i,e} \mid 1 \leq i \leq n, 1 \leq e \leq j_i\}$ be the set of rank t higher derivations on K over F defined by

$$d^{i,e}_{[t/p^i]+1}(x_{r,s}) = \delta_{((i,e),(r,s))},$$

where $[t/p^i]$ is the greatest integer less than or equal to t/p^i.

$$d^{i,e}_\alpha(x_{r,s}) = 0, \qquad 1 \leq i, r \leq n, 1 \leq e \leq j_i, \quad 1 \leq s \leq j_r, \alpha \neq [t/p^i]+1.$$

Then A is a standard set of generators for $H_F^t(K)$ and $\{x_{i,e} \mid 1 \leq i \leq n, 1 \leq e \leq j_i\}$ is called a dual base for A.

For later use, we now list some properties of A which follow from [4, §VI]. Let the first nonzero map (of subscript > 0) of $d^{i,e}$ be $d^{i,e}_{z_{i,e}}$.

(2.5) **Observations.** (a) A is abelian, i.e., all maps which appear in elements of A commute, and each $d^{i,e}$ is iterative of index $z_{i,e}$.

(b) $\{x^{p^r}_{r+1,1}, \ldots, x^{p^r}_{n,j_n}\}$ is a subbase for $F(K^{p^r})$ over F.

(c) $$\{d^{r+1,1}_{z_{r+1,1}p^r}|_{F(K^{p^r})}, \ldots, d^{n,j_n}_{z_{n,j_n}p^r}|_{F(K^{p^r})}\}$$

is a vector space basis over $F(K^{p^r})$ for the space of all derivations on $F(K^{p^r})$ over $F(K^{p^{r+1}})$ and hence these maps have field of constants $F(K^{p^{r+1}})$.

(d) $d^{i,e}_{z_{i,e}p^r}(x^{p^r}_{k,s}) = \delta_{((i,e),(k,s))}, \qquad r+1 \leq i, k \leq n, 1 \leq e \leq j_i, 1 \leq s \leq j_k.$

III. Invariant subfields and extensions of higher derivations.

(3.1) **Theorem.** *Let L be a subfield of K containing F. Then L is invariant under $H^t_F(K)$ if and only if $L = F(K^{p^r})$ for some nonnegative integer r.*

Proof. Assume $L = F(K^{p^r})$, and let $(d_i) \in H^t_F(K)$. If $x \in L$, then

$$x = \sum \{a_i b_i^{p^r} \mid a_i \in F, b_i \in K, 1 \leq i \leq s\}, \quad d_j(x) = \sum \{a_i d_j(b_i^{p^r})\}.$$

If $p^r \nmid j$, then by (2.2) $d_j(x) = 0 \in L$. If $p^r \mid j$, then $d_j(x) = \sum \{a_i(d_{j/p^r}(b_i))^{p^r}\} \in F(K^{p^r}) = L$. Since d_j was arbitrary, L is invariant under $H^t_F(K)$.

Conversely, assume L is invariant under $H^t_F(K)$. Assume $L \subseteq F(K^{p^r})$ and $L \nsubseteq F(K^{p^{r+1}})$ (otherwise $L = F = F(K^{p^n})$). Let $x \in L \backslash F(K^{p^{r+1}})$, and let A be a standard generating set for $H^t_F(K)$. In view of (2.5)c, there exists $d^{i,j} \in A$ such that $d^{i,j}_{z_{i,j}p^r}(x) \neq 0$. For any $a \in K$, $ad^{i,j}$ has $z_{i,j}p^r$ map $a^{p^r} d^{i,j}_{z_{i,j}p^r}$. Since L is invariant under $H^t_F(K)$, for any $a \in K$, $a^{p^r} d^{i,j}_{z_{i,j}p^r}(x) \in L$. Thus $K^{p^r} \subseteq L$ and thus $L = F(K^{p^r})$.

A subfield L of K containing F will be called Galois if K is modular over L, i.e., L is the field of constants of a group of rank t higher derivation on K over F. We now wish to determine which Galois intermediate fields L have the property that every rank t higher derivation on L over F can be extended to K. We will need the following result.

(3.2) **Theorem** [6, Proposition 3.3, p. 94]. *Let $K \supseteq L \supseteq F$ be fields and assume K is modular over L of exponent e. The following conditions are equivalent.*

(1) *There exists an intermediate field J of K/F such that $K = L \otimes_F J$ and J/F is modular.*

(2) *There exists a subbase $B = B_1 \cup \cdots \cup B_e$ of K over L such that $B_i^{p^i} \subseteq (K^{p^i} \cap F)((L(B_{i+1}, \ldots, B_n))^{p^i})$.*

(3.3) **Lemma.** *Let L be a subfield of K containing F, and assume L is modular over F and that every rank t higher derivation on L over F can be extended to K. Let $x \in K$ such that $x^{p^i} \in F(L^{p^i})$. Then $x^{p^i} \in (K^{p^i} \cap F)(L^{p^i})$.*

Proof. If $x^{p^i} \in F$, the result is obvious. Hence assume $x^{p^i} \in F(L^{p^r}) \backslash F(L^{p^{r+1}})$,

$r \geq i$. Let $T = \{x_{i,e} \mid 1 \leq i \leq n, 1 \leq e \leq j_i\}$ be a subbase for L over F, and let A have T as dual base. Write

$$(*) \qquad x^{p^i} = \sum_{s=1}^{m} a_s (x_{r+1,1}^{p^r})^{t_{s,r+1,1}} \cdots (x_{n,j_n}^{p^r})^{t_{s,n,j_n}}$$

where $a_s \in F$, $0 \leq t_{s,j,e} < p^{j-r}$, and at least one $t_{s,i,e}$ is not divisible by p (see (2.5)b).

To show $x^{p^i} \in (K^{p^i} \cap F)(L^{p^i})$ it suffices to show each $a_i \in K^{p^i}$. Proof is by induction on m. If $m = 1$, $a_1 \in K^{p^i}$. Assume the result for $m - 1$. By induction it suffices to show some a_i is in K^{p^i}. Since every higher derivation on L over F can be extended to K, and K^{p^i} is invariant under all higher derivations on K (2.2), any map in any higher derivation on L over F must map x^{p^i} into K^{p^i}. We will show some a_s is in K^{p^i} by induction on the total exponent of $(*)$ (i.e., $\sum t_{s,\alpha,\beta}$). If the total exponent is 1, then $m = 1$ and the result follows. Since $x^{p^i} \in F(L^{p^r})\backslash F(L^{p^{r+1}})$, in view of (2.5)c, some $d^{i,e}_{z_{i,e}p^r}(x^{p^i}) \neq 0$. Applying $d^{i,e}_{z_{i,e}p^r}$ to $(*)$ yields a nonzero element of K^{p^i} of lower total exponent with nonzero coefficients of the form wa_s, $w \in Z/(p)$. If $d^{i,e}_{z_{i,e}p^r}(x^{p^i}) \notin F$, then by induction some wa_s, hence some a_s, is in K^{p^i} and the result follows. If $d^{i,e}_{z_{i,e}p^r}(x^{p^i}) \in F$, then since

$$(x_{r+1,1}^{p^r})^{t_{s,r+1,1}} \cdots (x_{n,j_n}^{p^r})^{t_{s,n,j_n}}, \qquad 0 \leq t_{s,i,e} < p^{i-r}$$

is a vector space basis for $F(L^{p^r})$ over F, in view of (2.5)d, $d^{i,e}_{z_{i,e}p^r}(x^{p^i}) = a_s$ for some s. Thus once again some a_s is in K^{p^i} and the result is established.

(3.4) **Theorem.** *Let L be a Galois subfield of K containing F and assume L is modular over F. Then every rank t higher derivation on L over F extends to K if and only if there exists a field J, $K \supseteq J \supseteq F$, J is modular over F and $K = L \otimes_F J$.*

Proof. If $K = L \otimes_F J$, then every rank t higher derivation on L over F can be extended to K by acting trivially on J.

Assume now that every rank t higher derivation on L over F can be extended to K. Let $B = B_1 \cup \cdots \cup B_n$ be a subbase for K over L where B_i is of exponent i over L. We claim $B_r^{p^r} \subseteq F(L^{p^r})$. Let A be a standard set of generators of $H_F^t(L)$ with dual basis $\{x_{i,e} \mid 1 \leq i \leq n, 1 \leq e \leq j_i\}$. In view of (2.5)c, $F(L^{p^r})$ is the field of constants of the set of maps $S = \{d^{i,e}_{z_{i,e}p^{c_i}} \mid 1 \leq i \leq n, 1 \leq e \leq j_i,$ $0 \leq c_i < \min(i, r)\}$. Thus it suffices to show x^{p^r} is annihilated by all maps in S. If $p \nmid z_{i,e}$, since $d^{i,e}$ can be extended to K,

$$d^{i,e}_{z_{i,e}p^{c_i}}(x^{p^r}) = 0, \qquad 0 \leqslant c_i < \min(i, r)$$

(2.2). If $p \mid z_{i,e}$, consider $V(d^{i,e})$ (see §II). We claim $(z_{i,e} + 1)p^{c_i} \leq t$ if $0 \leq c_i < \min(i, r)$ (unless $t = 1$, in which case the result is obvious). For if not, $(z_{i,e} + 1)p^{i-1} > t$, hence $z_{i,e} + 1 > t/p^{i-1}$ and $z_{i,e/p} + 1/p > t/p^i$, a contradiction to the definition of $z_{i,e}$ (2.4). Since $p \nmid (z_{i,e} + 1)$, we see again $d^{i,e}_{z_{i,e}p^{c_i}}(x^{p^r}) = 0$, $0 \leq c_i < \min(i, r)$. Thus $x^{p^r} \in F(L^{p^r})$, and $B_r^{p^r} \subseteq F(L^{p^r})$. By Lemma 3.3,

$$B_r^{p^r} \subseteq (K^{p^r} \cap F)(L^{p^r}) \subseteq (K^{p^r} \cap F)((L(B_{r+1}, \ldots, B_n))^{p^r}).$$

The result now follows from (3.2).

(3.5) **Corollary.** *Let L be a Galois subfield of K containing F. Let M be the field of constants of all rank t higher derivations on L over F. Then every rank t higher derivation on L over F extends to K if and only if there exists a field J, $K \supseteq J \supseteq M$, J is modular over M and $K = L \otimes_M J$.*

Proof. Since K is modular over L, and every rank t higher derivation on L over F extends to K, K is modular over M. Applying (3.4) to the chain of fields $K \supseteq L \supseteq M$ yields the result.

(3.6) **Corollary.** *Let L be a subfield of K containing F. Then L is invariant under $H_F^t(K)$ and every rank t higher derivation on L over F extends to K if and only if $L = F$ or $L = K$.*

Proof. Apply (3.1) and (3.5), (3.1) showing K is modular over L.

IV. **An intermediate theory.** Assume E is a normal separable extension of H. In classical Galois theory, the distinguished intermediate subfields D are characterized by being invariant under the group of automorphisms of E over H. They also possess the property that the Galois group of E over H when restricted to D is the Galois group of D over H.

As usual, let K be a finite dimensional purely inseparable modular extension of F and let L be an intermediate field such that K is modular over L. In view of (3.1) the requirement that L be invariant under $H_F^t(K)$ is much too restrictive. Considering the Dedekind independence theorem for automorphisms, (2.5)c, and [7, Theorem 19, p. 186], a natural alternative to this condition is that there exists a standard generating set for $H_F^t(K)$ which leaves L invariant. As we shall see, this invariance condition gives rise to an interesting intermediate theory. We observe that if L is invariant under a standard generating set for $H_F^t(K)$, then the restriction of that set to L will have field of constants F, and hence L must be modular over F. Moreover, since the higher derivations $d^{i,j}$ in a standard for $H_F^t(K)$ are iterative, $d^{i,e}|_L$ we will have first nonzero map $d_{z_{i,j}p^r}$ for some r, and will be iterative of index $z_{i,j}p^r$. In this section we will characterize such intermediate fields L.

(4.1) **Definition.** Let L be a Galois subfield of K containing F. Then L is distinguished if and only if there exists a standard generating set for $H_F^t(K)$ which leaves L invariant.

We will begin by examining the simplest type of modular extension. Recall $[K: F] < \infty$.

(4.2) **Definition.** Let K be a modular extension of F. Then K is an equiexponential modular extension of F if and only if there exists a subbase $\{x_1, \ldots, x_n\}$ for K over F such that each x_i has exponent r over F for some fixed integer r.

(4.3) **Lemma.** *A modular extension K of F is equiexponential if and only if every relative p-base for K over F is also a subbase for K over F.*

Proof. If K is an equiexponential modular extension of F, then since a subbase is a relative p-base of minimal total exponent, any relative p-base will be a subbase. Conversely, assume K is not equiexponential over F and let $\{x_{1,1},\ldots,x_{n,j_n}\}$ be a subbase. Then $\{x_{1,1}-x_{n,j_n},\ldots,x_{n,j_{n-1}}-x_{n,j_n},x_{n,j_n}\}$ is a relative p-base for K over F, and is not of minimal total exponent, and hence is not a subbase for K over F.

(4.4) **Theorem.** *Assume K is an equiexponential modular extension of F. If L is an intermediate such that K is modular over L, then L is modular over F.*

Proof. Let the exponent of K over F be n, and let $\{x_1,\ldots,x_s\}$ be a subbase for K over L. By (2.3), there exists a set $T\subset L$ such that $T\cup\{x_1,\ldots,x_s\}$ is a p-basis for K. Since $\{x_1,\ldots,x_s\}$ is relatively p-independent in K over L, it is relatively p-independent in K over F. Thus $\{x_1,\ldots,x_s\}$ can be completed to a relative p-basis for K over F with elements from T. Let $\{x_1,\ldots,x_s,Y_1,\ldots,Y_r\}$ be such a relative p-basis. Since K is equiexponential modular over F, $\{x_1,\ldots,x_s,Y_1,\ldots,Y_r\}$ is also a subbase for K over F. Let $\{x_1,\ldots,x_t\}$ be of exponent n over L, and let x_j be of exponent e_j over L, $t+1\leq j\leq s$. By a degree argument, we observe $L=F(x_{t+1}^{p^{e_{t+1}}},\ldots,x_s^{p^{e_s}},Y_1,\ldots,Y_r)$, and since $\{x_1,\ldots,x_s,Y_1,\ldots,Y_r\}$ is a subbase for K over F, $\{x_{t+1}^{p^{e_{t+1}}},\ldots,Y_r\}$ is a subbase for L over F. Thus L is modular over F.

(4.5) **Corollary.** *Assume K is an equiexponential modular extension of F, and L is an intermediate field such that K is modular over L. Then there exists a subbase $\{x_1,\ldots,x_n\}$ for K over F such that $\{x_s^{p^{e_s}},\ldots,x_n^{p^{e_n}}\}$ is a subbase for L over F for some $e_s,\ldots,e_n$.*

(4.6) **Example.** The converse of Theorem (4.4) does not hold. Consider the following chain of fields where P is a perfect field (char $P\neq 0$), and x,y,z are algebraically independent over P.

$$K=P(x,y^px+z^p,z^{p^2}),\quad L=P(x^{p^2},y^{p^2},z^{p^2}),\quad F=P(x^{p^2},y^{p^3},z^{p^2}).$$

Elementary calculations show K is equiexponential modular over F, and L is modular over F. However, K is not modular over L.

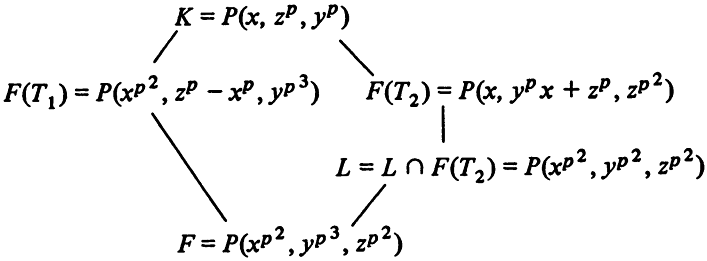
(4.7) **Definition.** Let K be a modular extension of F, and let L be a Galois intermediate field. Then L is homogeneous with respect to K if and only if there exists $T=T_1\cup\cdots\cup T_n$ a subbase for K over F where $F(T_i)$ is equiexponential modular over F, and such that $L=L\cap F(T_1)\otimes\cdots\otimes L\cap F(T_n)$.

(4.8) **Proposition.** *Let K be a modular extension of F and let L be a homogeneous intermediate field. Then L is modular over F if and only if $L\cap F(T_i)$ is modular over F for all i.*

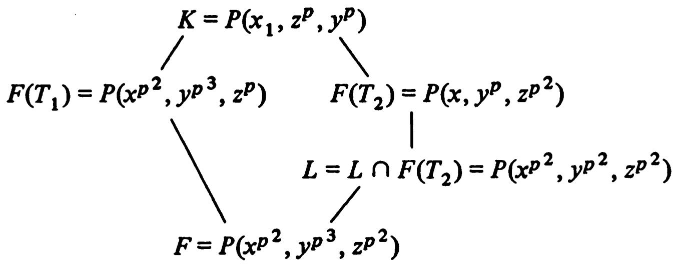
Proof. Assume L is modular over F, and let $(L\cap F(T_i))^*$ be the unique minimal extension of $L \cap F(T_i)$ which is modular over F. Since both L and $F(T_i)$ are modular over F, $(L \cap F(T_i))^* \subseteq L \cap F(T_i)$, and hence $(L \cap F(T_i))^* = L \cap F(T_i)$. The converse follows since a tensor product of tensor products is a tensor product.

(4.9) **Definition.** Let K be a modular extension of F, and let L be an intermediate field. Then L is M-homogeneous if and only if there exists a subbase $T = T_1 \cup \cdots \cup T_n$ of K over F such that $L = L \cap F(T_1) \otimes \cdots \otimes L \cap F(T_n)$ and $F(T_i)$ is modular over $L \cap F(T_i)$ for all i.

(4.10) **Example.** L may be M-homogeneous for some subbases of K over F, and only homogeneous for others. Let P be a perfect field, and x, y, z algebraically independent over P. In the following diagram with $T_1 = \{z^p - x^p\}$ and $T_2 = \{x, y^p x + z^p\}$, L is homogeneous but $F(T_2)$ is not modular over $L \cap F(T_2)$.



However, if we set $T_1 = \{z^p\}$ and $T_2 = \{x, y^p\}$, the following diagram shows L is M-homogeneous.



Conjecture. L is homogeneous if and only if L is M-homogeneous.

(4.11) **Proposition.** *Let K be a modular extension of F, and let L be an M-homogeneous intermediate field. Then L is also modular over F.*

Proof. By assumption, $F(T_i)$ is modular over $L \cap F(T_i)$ for all i. By (4.4), $L \cap F(T_i)$ is modular over F for all i, and hence L is modular over F (4.8).

(4.12) **Theorem.** *Assume K is a modular extension of F and L is a Galois intermediate field. Then L is distinguished if and only if L is M-homogeneous.*

Proof. Assume L is distinguished and let A be a standard generating set for $H_F^t(K)$ which leaves L invariant. Let $T = T_1 \cup \cdots \cup T_n$ be a dual base for A.

We claim $L = L \cap F(T_1) \otimes \cdots \otimes L \cap F(T_n)$. Let $A = A_1 \cup \cdots \cup A_n$ where the field of constants of A_i if $F(T_1) \otimes \cdots \otimes \widehat{F(T_i)} \otimes \cdots \otimes F(T_n)$. Let $A_i = \{d^{i,1}, \ldots, d^{i,j_i}\}$ and let $d^{i,s} \mid L$ have first nonzero map $r_{i,s}$. Let $\overline{A_i} = \{d_c^{i,s} \mid 1 \leq s \leq j_i, 0 \leq c < r_{i,s}\}$. Then the field of constants of $\overline{A_i}$ is of the form $F(T_1) \otimes \cdots \otimes H_i \otimes \cdots \otimes F(T_n)$. Since L is the field of constants of $\bigcup \overline{A_i}$,

$$L = \bigcap \{F(T_1) \otimes \cdots \otimes H_i \otimes \cdots \otimes F(T_n) \mid 1 \leq i \leq n\} = H_1 \otimes \cdots \otimes H_n.$$

Thus L is homogeneous and since $\overline{A_i}|_{F(T_i)}$ has H_i as field of constants, L is M-homogeneous.

Conversely, assume L is M-homogeneous and let $L = L_1 \otimes \cdots \otimes L_n$. Then since $F(T_i)$ is modular over L_i, and $F(T_i)$ is equiexponential modular over F, in view of Corollary (4.3), there exists $T'_i = \{x_{i,1}, \ldots, x_{i,j_i}\}$ such that $\{x_{i,s}^{p^{e_{i,s}}}, \ldots, x_{i,j_i}^{p^{e_{i,j_i}}}\}$ (possibly renumbering) is a subbase for L_i over F. Thus if we let A be the standard generating set for $H_F^t(K)$ with T'_i as dual basis, elementary calculations show L is invariant under A.

(4.13) **Corollary.** *Assume K is a modular extension of F, and L is a Galois subfield. The following are equivalent.*

(1) *L is distinguished.*

(2) *L is M-homogeneous.*

(3) *There exists a subbase $\{x_1, \ldots, x_n\}$ for K over F such that $\{x_1^{p^{e_1}}, \ldots, x_n^{p^{e_n}}\}$ is a subbase for L over F for some $e_1, \ldots, e_n$.*

We have seen (4.11) that the class of distinguished intermediate fields is contained in $\{L \mid K$ is modular over L and L is modular over $F\}$. We close with an example to show this containment may be proper.

Let P be a perfect field (char $P \neq 0$) and let x, y be algebraically independent over P. Consider the following chain of fields.

$$K = P(x,y), \quad L = P(x - y^{p^2}, x^p), \quad F = P(x^p, y^{p^4}).$$

Elementary calculations show all extensions are modular. Since K is generated over L by a single element y, if L is homogeneous, then $K = L \otimes_F L'$ for some L'. But since L is of exponent 2 over F, this is impossible. Thus L is not homogeneous, and hence not distinguished.

References

1. N. Heerema, *Convergent higher derivations on local rings*, Trans. Amer. Math. Soc. **132** (1968), 31–44. MR **36** #6406.

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

3. F. Zerla, *Iterative higher derivations in fields of prime characteristic*, Michigan Math. J. **15** (1968), 407–415. MR **39** #185.

4. N. Heerema and J. Deveney, *Galois theory for fields K/k finitely generated*, Trans. Amer. Math. Soc. 189 (1974), 263–274.

5. R. Davis, *A Galois theory for a class of purely inseparable field extensions*, Dissertation, Florida State University, Tallahassee, Fla.

6. J. N. Mordeson and B. Vinograde, *Structure of arbitrary purely inseparable extension fields*, Lecture Notes in Math., vol. 173, Springer-Verlag, Berlin and New York, 1970. MR **43** #1952.

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

DEPARTMENT OF MATHEMATICS, FLORIDA STATE UNIVERSITY, TALLAHASSEE, FLORIDA 32306

Current address: Department of Mathematics, Kansas State University, Manhattan, Kansas 66502