ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 9, Number 3, Summer 1979

INVARIANCE IN INSEPARABLE GALOIS THEORY

JAMES K. DEVENEY[1] AND JOHN N. MORDESON

ABSTRACT. Let L be a normal, modular extension of a field K of characteristic $p \neq 0$, and let $K(L^{p^r})/K$ be separable for some nonnegative integer r. This paper is concerned with the intermediate theory for the Galois theory of inseparable extensions developed by N. Heerema. A new characterization of the distinguished subfields for the purely inseparable case in terms of linear disjointness properties is used to incorporate the purely inseparable intermediate theory as a special case of the inseparable theory developed here.

1. **Introduction.** Let L be a field of characteristic $p \neq 0$. In [3], Heerema develops a Galois theory for inseparable field extensions which includes both the Krull infinite Galois theory and the purely inseparable, finite higher derivation theory. The groups used in this correspondence are subgroups of the group A of automorphisms of the local ring $L[\bar{x}] = L[x]/x^{p^e+1}L[x]$ such that $f(\bar{x}) = \bar{x}$ where x is an indeterminant over L, e is a nonnegative integer, $x^{p^e+1}L[x]$ is the ideal generated in $L[x]$ by x^{p^e+1}, and $\bar{x}$ is the coset $x + x^{p^e+1}L[x]$. For a subgroup G of A, set $G_L = \{f \in G \mid f(L) \subseteq L\}$, $G_0 = \{f \in G \mid f(c) - c \in \bar{x}\, L[\bar{x}]$ for all $c \in L\}$, and $L^G = \{c \in L \mid f(c) = c$ for all $f \in G\}$. For K a subfield of L, let $G^K = \{f \in G \mid f(c) = c$ for all $c \in K\}$. If $\mathfrak{D}$ denotes the group of all rank p^e higher derivations on L, there is an isomorphism $\Delta(\mathfrak{D}) = A_0$ given in [3, Proposition 2.1, p. 194]. Basically, if G is a Galois subgroup of A, then G_L can be considered as a classical group of automorphisms of L, and L is a normal separable extension of L^{G_L}; G_0 can be considered as a group of higher derivations on L via the isomorphism Δ, and L is purely inseparable modular extension of L^{G_0}; and moreover, $L = L^{G_L} \otimes_{L^G} L^{G_0}$.

Throughout this paper, K will be a given Galois subfield of L with Galois group G, and we will let $L^{G_0} = S$, $L^{G_L} = J$ and $\Delta(\mathfrak{D}^S) = G_0$. Moreover, we will assume $[L : S] < \infty$ in order to apply the Galois theory of [4]. In particular, S is normal over K and is the maximal separable extension of K in L, and J is a finite dimensional purely inseparable modular extension of K (as is L/S).

The purely inseparable Galois theory of higher derivations developed

Received by the editors on Octoberl, 1976 and in revised form on April 7, 1977.

[1]Supported by the Grants-In-Aid Program for Faculty of Virginia Commonwealth University.

AMS (MOS) *subject classification*: Primary 12F15, Secondary 12A55.

Key Words and Phrases: Higher derivations, normal field extension, modular field extension.

in [4] occurs as a special case of the inseparable theory when $S = K$, $[L:S] < \infty$. In [1] it is shown that the only intermediate fields F of L/S which satisfy the property that if S is Galois in F, then F is invariant under $\mathfrak{D}^s$ are those of the form $S(L^{p^r})$. This defect is circumvented in [1] by defining an intermediate field F of L/S to be distinguished when it is left invariant under a standard generating set for $\mathfrak{D}^s$. In [2] it is shown that F is distinguished if and only if F is homogeneous [1, Definition 4.7, p. 292] and that F is homogeneous if and only if there is a subbase $\{x_1, \cdots, x_r\}$ for L over S such that

$$\{x_1^{p^{n_1}}, \cdots, x_s^{p^{n_s}}\}, \ (s \leqq r)$$

is a subbase for F over S. Clearly if F is homogeneous, then L/F and F/S are modular. In this paper, the concept of distinguished intermediate fields for the inseparable Galois theory is developed. A new characterization for the purely inseparable case in terms of linear disjointness properties is used to incorporate the purely inseparable intermediate theory as a special case of inseparable theory developed here. Of course any defect which appears in the purely inseparable Galois theory will also appear in the inseparable Galois theory. Theorem 2 circumvents the problem concerning distinguished intermediate fields for the inseparable case in a similar manner to what is done in [1] for the purely inseparable case. Theorem 3 examines the question of when every intermediate field is distinguished.

2. **Intermediate Theory.** Before developing an intermediate theory for Heerema's inseparable Galois theory, we first derive a new characterization for the purely inseparable case (i.e., $G = G_0$).

LEMMA 1 (REPLACEMENT LEMMA). *Assume L/K is purely inseparable modular of exponent n. Let $T_n \cup T_{n-1} \cup \cdots \cup T_1$ be a subbase for L/K where the elements of T_i are of exponent i over K. Let $\{b_1, \cdots, b_r\} \subset L$ be such that $[b_1^{p^i}, \cdots, b_r^{p^i}\}$ is relatively p-independent in $K^{p^{-s}} \cap L$ over $(K^{p^{-s+1}} \cap L)\,(L^{p^{i+1}} \cap K^{p^{-s}})$. Then there exists $T'_{s+i} \supseteq \{b_1, \cdots, b_r\}$ such that $T_n \cup \cdots \cup T_{s+i+1} \cup T'_{s+i} \cup \cdots T_1$ is also a subbase for L/K.*

PROOF. We shall use the construction of a subbase given by Sweedler in [7, p. 402]. T_n is a relative p-basis for L over $K^{p^{-n+1}} \cap L$. Since $T_n \cup \cdots \cup T_1$ is assumed to be a subbase for L/K, we can proceed to the stage of constructing a relative p-basis for $K^{p^{-(i+s)}} \cap L$ over $K^{p^{-(i+s)+1}} \cap L$. Since L/K is modular, $T_n^{p^{n-(i+s)}} \cup \cdots \cup T_{i+s+1}^p$ is p-independent here [7, Theorem 1, p. 403], and in fact is a relative p-basis for $(K^{p^{-(i+s)+1}} \cap L)\,(L^p \cap K^{p^{-(i+s)}})$ over $K^{p^{-(i+s)+1}} \cap L$. The set $\{b_1, \cdots, b_r\}$ is in $K^{p^{-(i+s)}} \cap L$ since $\{b_1^{p^i}, \cdots, b_r^{p^i}\} \subset K^{p^{-s}} \cap L$. Moreover, it is p-independent over $(K^{p^{-(i+s)+1}} \cap L)\,(L^p \cap K^{p^{-(i+s)}})$. For if not, there exists a non-trivial relation among the monomials $\{\prod b_1^{n_1} \cdots b_r^{n_r} \mid 0 \leqq n_i < p\}$ with coefficients in $(K^{p^{-(i+s)+1}} \cap L)\,(L^p \cap K^{p^{-(i+s)}})$. Raising this relation to the p^i power would give a non-trivial relation among $\{\prod (b_1^{p^i})^{n_1} \cdots (b_r^{p^i})^{n_r} \mid 0 \leqq n_i < p\}$ with coefficients in $(K^{p^{-s+1}} \cap L)\,(L^{p^{i+1}} \cap K^{p^{-s}})$, contrary to assumption. Thus, $\{b_1, \cdots, b_r\}$ can be completed to a relative p-basis T'_{s+i} for $K^{p^{-(i+s)}} \cap L$ over $(K^{p^{-(i+s)+1}} \cap L)\,(L^p \cap K^{p^{-(i+s)}})$. Thus $T_n \cup \cdots \cup T'_{i+s}$ is part of a subbase for L/K. In constructing a relative p-basis for $K^{p^{-h}} \cap L$ over $K^{p^{-h+1}} \cap L$ *where* $h < i + s$, $T_n^{p^{n-h}} \cup \cdots \cup T'^{\,p^{(i+s)-h}}_{i+s} \cup \cdots \cup T_{h+1}^{p}$ will be a relative p-basis for $(K^{p^{-h+1}} \cap L)\,(L^p \cap K^{p^{-h}})$ over $K^{p^{-h+1}} \cap L$, and hence can be completed to a relative p-basis with T_h. This establishes the lemma.

We note that as a corollary of the replacement lemma, the complete set of elements of a given exponent from some subbase may be used in any other subbase.

LEMMA 2 (SHIFT LEMMA). *Assume $L \supseteq M \supseteq K$ where L is purely inseparable modular of exponent n over K. If*

(1) $K^{p^{-r}} \cap L$ *and* M *are linearly disjoint over* $K^{p^{-r}} \cap M$ *for all* r, *and*

(2) $(K^{p^{-r}} \cap L)\,(L^{p^{i+1}} \cap K^{p^{-r-1}})$ *and* $(K^{p^{-r}} \cap L)\,(L^{p^i} \cap K^{p^{-r-1}} \cap M)$ *are linearly disjoint over* $(K^{p^{-r}} \cap L)\,(L^{p^{i+1}} \cap K^{p^{-r-1}} \cap M)$ *for all* i *and* r,

then any relative p-basis for $(K^{p^{-r}} \cap M)\,(L^{p^i} \cap K^{p^{-r-1}} \cap M)$ *over* $(K^{p^r} \cap M)\,(L^{p^{i+1}} \cap K^{p^{-r-1}} \cap M)$ *remains p-independent over* $(K^{p^{-r}} \cap L)\,(L^{p^{i+1}} \cap K^{p^{-r-1}})$.

PROOF. This result follows by applying the standard theorem on linear disjointness to the diagram of fields below.

$$\begin{tikzcd}[arrows=dash]
(K^{p^{-r}} \cap L)(L^{p^{i+1}} \cap K^{p^{-r-1}}) \arrow[ddr] & & (K^{p^{-r}} \cap L)(L^{p^i} \cap K^{p^{-r-1}} \cap M) \arrow[ddl] \arrow[dr] & & M \arrow[dl] \\
& & & (K^{p^{-r}} \cap M)(L^{p^i} \cap K^{p^{-r-1}} \cap M) \arrow[ddl] & \\
& (K^{p^{-r}} \cap L)(L^{p^{i+1}} \cap K^{p^{-r-1}} \cap M) \arrow[dl] \arrow[dr] & & & \\
K^{p^{-r}} \cap L \arrow[dr] & & (K^{p^{-r}} \cap M)(L^{p^{i+1}} \cap K^{p^{-r-1}} \cap M) \arrow[dl] & & \\
& (K^{p^{-r}} \cap M) & & &
\end{tikzcd}$$

THEOREM 1. *Assume* $L \supseteq M \supseteq K$ *where* L *is purely inseparable modular of exponent* n *over* K. *Then there is a subbase* B *of* L *over* K *and a subset* B' *of* B *such that* $C = \{b^{p^r} \mid b \in B', r$ *is the exponent of* b *over* $M\}$ *is a subbase of* M *over* K *if and only if*

(1) $K^{p^{-r}} \cap L$ *and* M *are linearly disjoint over* $K^{p^{-r}} \cap M$ *for all* r;

(2) $(K^{p^{-r}} \cap L)(L^{p^{i+1}} \cap K^{p^{-r-1}})$ *and* $(K^{p^{-r}} \cap L)(L^{p^i} \cap K^{p^{-r-1}} \cap M)$ *are linearly disjoint over* $(K^{p^{-r}} \cap L)(L^{p^{i+1}} \cap K^{p^{-r-1}} \cap M)$ *for all* r, i.

PROOF. Assume conditions (1) and (2) are satisfied. Then M is modular over K [8, Proposition 1.4, p. 41]. The idea of the proof is to simultaneously construct subbases for L/K and M/K with the desired property. Once again, we will use Sweedler's method.

STAGE 1. Let A_n be a relative p-basis for M over $K^{p^{-n+1}} \cap M$. By assumption (1), A_n remains p-independent over $K^{p^{-n+1}} \cap L$ and hence can be completed to a relative p-basis for $K^{p^{-n}} \cap L = L$ over $K^{p^{-n+1}} \cap L$ with $B_{n,1}$. The elements of $B_{n,1}$ may be changed later.

STAGE 2. We want to construct a relative p-basis for $K^{p^{-n+1}} \cap M$ over $K^{p^{-n+2}} \cap M$. Consider $(K^{p^{-n+2}} \cap M)(L^p \cap K^{p^{-n+1}} \cap M)/(K^{p^{-n+2}} \cap M)$. $A_n{}^p$ is p-independent here since L/K is modular. This set can be completed to a relative p-basis with elements of L^p, called $C_{n,1}{}^p$. By the Shift Lemma, $A_n{}^p \cup C_{n,1}{}^p$ is p-independent in $(K^{p^{-n+2}} \cap L)(L^p \cap K^{p^{-n+1}})$ over $K^{p^{-n+2}} \cap L = (K^{p^{-n+2}} \cap M)(L^{p^2} \cap K^{p^{-n+1}} \cap M)$, and hence by the Relacement Lemma, we can replace $A_n \cup B_{n,1}$ with $A_n \cup C_{n,1} \cup B_{n,2}$. Let A_{n-1} be a relative p-basis for $K^{p^{-n+1}} \cap M$ over $(K^{p^{-n+2}} \cap M)(L^p \cap K^{p^{-n+1}} \cap M)$. By the Shift Lemma, A_{n-1} is p-independent in $K^{p^{-n+1}} \cap L$ over $(K^{p^{-n+2}} \cap L)(L^p \cap K^{p^{-n+1}})$, and hence $A_n{}^p \cup C_{n,1}{}^p \cup B_{n,2}{}^p \cup A_{n-1}$ is p-independent over $K^{p^{-n+2}} \cap L$ and can be completed to a relative p-basis for $K^{p^{-n+1}} \cap L$ over $K^{p^{-n+2}} \cap L$ with $B_{n-1,1}$. Thus we now have $T_n = A_n \cup C_{n,1} \cup B_{n,2}$, $T_{n-1} = A_{n-1} \cup B_{n-1,1}$ as part of a subbase for L/K and $T'_n = A_n$, $T'_{n-1} = C_{n,1}{}^p \cup A_{n-1}$ as part of a subbase for M/K.

We now assume that after the completion of stage $(i-1)$ we have constructed partial subbases

$$T_r = A_r \cup C_{r,1} \cup \cdots \cup C_{r,i-n+r-2} \cup B_{r,i-n+r-1}$$

and

$$T'_r = A_r \cup C_{n,n-r}{}^{p^{n-r}} \cup \cdots \cup C_{r-1,1}{}^p,$$

$n \geqq r \geqq n-i+2$.

STAGE i. We want to construct a relative p-basis for $K^{p^{-n+i-1}} \cap M$ over $K^{p^{-n+i}} \cap M$. This is done in i steps via the intermediate fields

$(K^{p^{-n+i}} \cap M)$ $(L^{p^j} \cap K^{p^{-n+i-1}} \cap M)/(K^{p^{-n+i}} \cap M)$ $(L^{p^{j+1}} \cap K^{p^{-n+i-1}} \cap M)$, $i-1 \geqq j \geqq 0$, and is done in descending order of j. For $j > 0$, $A_{n-(i-1-j)}{}^{p^j} \cup C_{n-(i-1-j),1}{}^{p^j} \cup \cdots \cup C_{n-(i-1-j),j-1}{}^{p^j}$ is p-independent here since it is part of a subbase of L/K and hence is p-independent over $(K^{p^{-n+1}} \cap L)$ $(L^{p^{j+1}} \cap K^{p^{-n+i-1}})$. Complete this to a relative p-basis with elements of L^{p^j}, called $C_{n-(i-1-j),j}{}^{p^j}$. Using the Shift and Replacement Lemmas, we can replace $B_{n-(i-1-j),j}$ with $C_{n-(i-1-j),j} \cup B_{n-(i-1-j),j+1}$. When $j = 0$, we want to construct a relative p-basis for $K^{p^{-n+i-1}} \cap M$ over $(K^{p^{-n+i}} \cap M)$ $(L^p \cap K^{p^{-n+i-1}} \cap M)$. Note that we have already shown $T_r'^{p^{-n+i-1}}$, $n \geqq r \geqq n-i+2$, is p-independent in $(K^{p^{-n+i}} \cap M)$ $(L^p \cap K^{p^{-n+i-1}} \cap M)$ over $K^{p^{-n+i}} \cap M$, and that we have already added some "new" elements to these. Thus when we choose any p-basis for $K^{p^{-n+i-1}} \cap M$ over $(K^{p^{-n+i}} \cap M)$ $(L^p \cap K^{p^{-n+i-1}} \cap M)$, called A_{n-i+1}, we have constructed $T'_{n-i+1} = C_{n,i-1}{}^{p^{i-1}} \cup \cdots \cup C_{n-(i-2),1}{}^{p} \cup A_{n-i+1}$ as part of a subbase for M/K. By assumption, A_{n-i+1} remains p-independent in $K^{p^{-n+i-1}} \cap L$ over $(K^{p^{-n+i}} \cap L)$ $(L^p \cap K^{p^{-n+i-1}})$. Since $\cup\{T_r^{p^{r-(n-i+1)}} \mid n \geqq r \geqq n-i+2\}$ is a relative p-basis for $(K^{p^{-n+1}} \cap L)$ $(L^p \cap K^{p^{-n+i-1}})$ over $K^{p^{-n+i}} \cap L$, we can find $B_{n-i+1,1}$ so that $A_{n-i+1} \cup B_{n-i+1,1} \cup \{T_r^{p^{r-(n-i+1)}} \mid n \geqq r \geqq n-i+2\}$ is a relative p-basis for $K^{p^{-n+i-1}} \cap L$ over $K^{p^{-n+i}} \cap L$, i.e., we can choose $T_{n-i+1} = A_{n-i+1} \cup B_{n-i+1,1}$. Since L/K is of bounded exponent n, the desired subbases are constructed in a finite number of stages. The proof of the converse is straightforward.

DEFINITION. As usual let K be a Galois subfield of L. Let $G = A^K$ and let $\mathscr{H} = \{x_{11}, \cdots, x_{1j_1}, \cdots, x_{n1}, \cdots, x_{nj_n}\}$ be a subbase for L/S where x_{ij} has exponent i over S. Let $\mathscr{H}^J = \{d^{ij} \mid 1 \leqq i \leqq n, 1 \leqq j \leqq j_i\}$ be the set of rank p^e higher derivations defined on L by

$$d_u^{ij}(x_{rs}) = \begin{cases} \delta_{(i,j)\cdot(r,s)} & \text{if } u = [p^{e-i}] + 1 \\ 0 & \text{otherwise,} \end{cases}$$

where $[p^{e-1}]$ is the greatest integer less than or equal to p^{e-i}, and $\delta_{(i,j),(r,s)} = 1$ if $i = r$, $j = s$, and is 0 otherwise. Let $H^J = \Delta(\mathscr{H}^J)$. Then $G_L H^J = [\sigma\Delta(d^{ij}) \mid \sigma \in G_L, \Delta(d^{ij}) \in H^J\}$ is called a *standard generating set* for G with respect to $\mathscr{H}$. An intermediate field F is *distinguished* if and only if $F[\bar{x}]$ is invariant under some standard generating set.

Clearly $n \leqq e+1$ and $\Delta(d^{ij}) \in G_0$. Also $[p^{e-i}] = p^{e-i}$ if $i \leqq e$ and $[p^{e-i}] = 0$ if $i = e+1$.

The case when $G = G_0$ is the intermediate theory developed in [1]. In view of [1, Corollary 4.13, p. 294], the linear disjointness conditions of Theorem 1 yields a new characterization of the distinguished subfields in this case. We now derive a characterization of the distinguished subfields for the inseparable Galois theory.

THEOREM 2. *Let K be a Galois subfield of L such that $[L:S]<\infty$. Let $G=A^K$ and let F be a Galois intermediate field of L/K. The following are equivalent.*

(1) *F/K is normal and $F\cap J$ is homogeneous in J/K.*

(2) *$F[\bar{x}]$ is invariant under a standard generating set for G.*

(3) *F/K is normal and SF is homogeneous in L/S.*

PROOF. (1) $\Rightarrow$ (2). Let $\mathscr{H}=\{x_{11},\cdots,x_{1j_1},\cdots,x_{n1},\cdots,x_{nj_n}\}$ be a subbase of J/K such that for $k_1\leqq j_1,\cdots,k_n\leqq j_n$,

$$\mathscr{X}=\{x_{11}{}^{p^{e_{11}}},\cdots,x_{1k_1}{}^{p^{e_{1k_1}}},\cdots,x_{n_1}{}^{p^{e_{n_1}}},\cdots,x_{nk_n}{}^{p^{e_{nk_n}}}\}$$

is a subbase of $(F\cap J)/K$. Let G_LH^J be a standard generating set for G with respect to $\mathscr{H}$ and $\sigma f^{ij}\in G_LH^J$ where $f^{ij}=\Delta(d^{ij})$. Since $\mathscr{X}$ generates F over $S\cap F$, it suffices to show $\sigma f^{ij}(x_{rs}{}^{p^{e_{rs}}})\in F[\bar{x}]$ and $\sigma f^{ij}(s)\in F$ where $s\in S\cap F$. Clearly $\sigma f^{ij}(s)\in S\cap F$ since f^{ij} is the identity on S and $(S\cap F)/K$ is necessarily normal. Now

$$f^{ij}(x_{rs}{}^{p^{e_{rs}}})=\sum_{u=0}^{p^e}\bar{x}^u\,d_u{}^{ij}(x_{rs}{}^{p^{e_{rs}}})$$

$$=x_{rs}{}^{p^{e_{rs}}}+\sum_{u=1}^{p^e}\bar{x}^u\,d_u{}^{ij}(x_{rs}{}^{p^{e_{rs}}})$$

and $d_u{}^{ij}(x_{rs}{}^{p^{e_{rs}}})=d_t{}^{ij}(x_{rs})^{p^{e_{rs}}}$ if $u=tp^{e_{rs}}$ for some t, $d_u{}^{ij}(x_{rs}{}^{p^{e_{rs}}})=0$ otherwise. Suppose $u=tp^{e_{rs}}$ for some t. Then $d_t{}^{ij}(x_{rs})=\sigma_{(i,j),(r,s)}$ if $t=[p^{e-i}]+1$ and $d_t{}^{ij}(x_{rs})=0$ otherwise. Therefore,

$$f^{ij}(x_{rs}{}^{p^{e_{rs}}})=x_{rs}{}^{p^{e_{rs}}}+\bar{x}^{([p^{e-i}]+1)p^{e_{rs}}}\delta_{(i,j),(r,s)}.$$

Thus, $\sigma f^{ij}(x_{rs}{}^{p^{e_{rs}}})\in(F\cap J)[\bar{x}]$ since σ is the identity on $J[\bar{x}]$.

(2) $\Rightarrow$ (3). Let G_LH^J be the standard generating set. Since the identity map is in G_L, $F[\bar{x}]$ is invariant under H^J. Thus $F[\bar{x}]$ is invariant under G_L. Since L is also invariant under G_L, $F[\bar{x}]\cap L=F$ is invariant under G_L and F/K is normal. Since $F[\bar{x}]$ is invariant under H^J and clearly every element of H^J is the identity on S, $SF[\bar{x}]$ is invariant under H^J. Thus SF is invariant under $\Delta^{-1}(H^J)$ which is a standard generating set for L/S in the sense of [1]. Thus, SF is homogeneous in L/S.

(3) $\Rightarrow$ (1). We show $F\cap J=M$ satisfies conditions (1) and (2) of Theorem 1. To show (1), we need to prove that $K^{p^{-r}}\cap J$ and M are linearly disjoint over $K^{p^{-r}}\cap M$. However, a basis for $K^{p^{-r}}\cap J$ over $K^{p^{-r}}\cap M$ is a basis for $S^{p^{-r}}\cap L$ over $S^{p^{-r}}\cap SF$, and since SF is homogeneous in L/S, by Theorem 1, this set will be independent over SF hence over M.

To show (2), since SF is homogeneous in L/S, we have that $(S^{p^{-r}}\cap$

$L)$ $(L^{p^{i+1}} \cap S^{p^{-r-1}})$ and $(S^{p^{-r}} \cap L)$ $(L^{p^i} \cap S^{p^{-r-1}} \cap SF)$ are linearly disjoint over $(S^{p^{-r}} \cap L)$ $(L^{p^{i+1}} \cap S^{p^{-r-1}} \cap SF)$. We first note that $S^{p^{-r}} \cap L = S(K^{p^{-r}} \cap J)$ and that $S = S^{p^{i+1}} \otimes_{K^{p^{i+1}}} K$. Thus we get

$$
\begin{aligned}
&(S^{p^{-r}} \cap L)\ (L^{p^{i+1}} \cap S^{p^{-r-1}} \cap SF)\\
&\quad = S(K^{p^{-r}} \cap J)\ ((S^{p^{i+1}} \otimes_{K^{p^{i+1}}} J^{p^{i+1}})\\
&\qquad \cap (S(K^{p^{-r-1}} \cap J \cap F)))\\
&\quad = S(K^{p^{-r}} \cap J)\ ((S^{p^{i+1}} \otimes_{K^{p^{i+1}}} J^{p^{i+1}})\\
&\qquad \cap (S^{p^{i+1}} \otimes_{K^{p^{i+1}}} K \otimes_K K^{p^{-r-1}} \cap M))\\
&\quad = S(K^{p^{-r}} \cap J)\ ((S^{p^{i+1}} \otimes_{K^{p^{i+1}}} J^{p^{i+1}})\\
&\qquad \cap (S^{p^{i+1}} \otimes_{K^{p^{i+1}}} K^{p^{-r-1}} \cap M))\\
&\quad = S(K^{p^{-r}} \cap J)\ (S^{p^{i+1}} \otimes_{K^{p^{i+1}}} (J^{p^{i+1}} \cap K^{p^{-r-1}} \cap M))\\
&\quad = S(K^{p^{-r}} \cap J)\ (S^{p^{i+1}} (J^{p^{i+1}} \cap K^{p^{-r-1}} \cap M))\\
&\quad = S(K^{p^{-r}} \cap J)\ (J^{p^{i+1}} \cap K^{p^{-r-1}} \cap M).
\end{aligned}
$$

Similarly, $(S^{p^{-r}} \cap L)$ $(L^{p^{i+1}} \cap S^{p^{-r-1}}) = S(K^{p^{-r}} \cap J)$ $(J^{p^{i+1}} \cap K^{p^{-r-1}})$ and $(S^{p^{-r}} \cap L)$ $(L^{p^i} \cap S^{p^{-r-1}} \cap F) = S(K^{p^{-r}} \cap J)$ $(J^{p^i} \cap K^{p^{-r-1}} \cap M)$. We need to show $(K^{p^{-r}} \cap J)$ $(J^{p^{i+1}} \cap K^{p^{-r-1}})$ and $(K^{p^{-r}} \cap J)$ $(J^{p^i} \cap K^{p^{-r-1}} \cap M)$ are linearly disjoint over $(K^{p^{-r}} \cap J)$ $(J^{p^{i+1}} \cap K^{p^{-r-1}} \cap M)$. But since S and J are linearly disjoint over K, a basis for $(K^{p^{-r}} \cap J)$ $(J^{p^i} \cap K^{p^{-r-1}} \cap M)$ over $(K^{p^{-r}} \cap J)$ $(J^{p^{i+1}} \cap K^{p^{-r-1}} \cap M)$ will be a basis for $S(K^{p^{-r}} \cap J)$ $(J^{p^i} \cap K^{p^{-r-1}} \cap M)$ over $S(K^{p^{-r}} \cap J)$ $(J^{p^{i+1}} \cap K^{p^{-r-1}} \cap M)$ and will thus be independent over $S(K^{p^{-r}} \cap J)$ $(J^{p^{i+1}} \cap K^{p^{-r-1}})$ and hence certainly over the subfield $(K^{p^{-r}} \cap J)$ $(J^{p^{i+1}} \cap K^{p^{-r-1}})$. Thus $M = F \cap J$ satisfies (1) and (2) of Theorem 1, and $F \cap J$ is homogeneous in J/K.

COROLLARY 1. *Let K be a Galois subfield of L. Let $G = A^K$, $S = L^{G_0}$ and $J = L^{G_L}$. Let F be a Galois intermediate field. Then F is distinguished if and only if $F = S_1 \otimes_K J_1$ where S_1 is normal separable over K and there exists a subbase $\{x_1, \cdots, x_n\}$ for J over K such that $\{x_1^{p^{n_1}}, \cdots, x_s^{p^{n_s}}\}$ is a subbase of J_1 over K, $s \leqq n$.*

In view of Theorem 2 and its corollary, if a Galois intermediate field F of L/K is to be distinguished, then its purely inseparable part $(F \cap J)$ must be homogeneous in J/K. We now wish to determine necessary and sufficient conditions for every intermediate field to be distinguished. Let L/S denote a purely inseparable modular extension of bounded exponent. If $[S : S^p] \leqq p^2$, then every subbase of L/S has no more than two elements.

THEOREM 3. *Every intermediate field of L/S is homogeneous if and only if either*

(1) $L^p \subseteq S$, *or*

(2) L/S *is simple, or*

(3) $[S : S^p] \leqq p^2$ *and if L/S has a subbase of two elements with exponents $e_1 \geqq e_2$ over S, then $e_1 - 1 \leqq e_2$, or*

(4) L/S *has a subbase of two elements with exponents* 2,1 *over S.*

PROOF. Suppose every intermediate field of L/S is homogeneous. Then for every intermediate field F of L/S, L/F and F/S are modular. Thus either (1) $L^p \subseteq S$, or (2) L/S is simple, or (3) $[S : S^p] \leqq p^2$, or (4) L/S has a subbase of two elements one of which has exponent 1 over S. ([5, Corollary to Theorem 4]).

Suppose (1) and (2) do not hold. Then L/S has a subbase of two elements. Suppose the exponents of these elements over S are $e_1 \geqq e_2$ with $e_1 - 1 > e_2$. Let $\{m_1, m_2\}$ be a subbase of L/S with exponents e_1, e_2, respectively. Set $F = S(m_2 - m_1{}^p)$. Then F/S has exponent $e_1 - 1 > e_2$. Since F is also homogeneous, there exists a subbase $\{t_1, t_2\}$ of L/S with exponents e_1, e_2, respectively, such that $F = (F \cap S(t_1)) \otimes_S (F \cap S(t_2)) = S(t_1{}^p)$. Thus $F \subseteq (L^p)$ which is clearly impossible. Hence, $e_1 - 1 \leqq e_2$.

Conversely, if (1) or (2) hold, the converse is immediate. Suppose (4) holds. Let F be an intermediate field of L/S such that $L \neq F \neq S$. Then either $F = S(c)$ where c has exponent 2 or 1 over S, or $F = S(c_1, c_2)$ where $\{c_1, c_2\}$ is a minimal generating set of F/S and $F^p \subseteq S$. If $F = S(c)$ and c has exponent 2 over S, then clearly F is homogeneous since $\{c\}$ can be extended to a subbase of L/S. Suppose c has exponent 1 over S. If $\{c\}$ cannot be extended to a subbase of L/S, then for all $t \in L$ such that t has exponent 2 over S, $c \in S(t)$. For any such t, $F = S(t^p)$ so F is homogeneous. If $F = S(c_1, c_2)$, then $F = S^{p^{-1}} \cap L$ so $F = S(t_1{}^p, t_2)$ where $\{t_1, t_2\}$ is a subbase of L/S with exponents 2, 1 over S, respectively. Thus F is homogeneous. Suppose (3) holds and L/S is not simple. If $\{t_1, t_2\}$ is an equi-exponential subbase of L/S, then $F = F \cap S(t_1, t_2)$ so F is homogeneous. Suppose L/S has a subbase whose elements have exponents $e_1, e_1 - 1$ over S. Since $[S : S^p] = p^2$, $L^{p^{e_1-1}} \supseteq S$. Suppose $F = S(c_1, c_2)$ where $\{c_1, c_2\}$ is a subbase with exponents $e_1{}', e_2{}'$ over S, respectively. If either $c_1{}^{p^{-e_1+e_1'}}$ or $c_2{}^{p^{-e_1+e_2'}} \in L$, say $c_1{}^{p^{-e_1+e_1'}} \in L$, then $\{c_1{}^{p^{-e_1+e_1'}}, c_2{}^{p^{-e_1+1+e_2'}}\}$ is a subbase of L/S. Hence F is homogeneous. Suppose $c_1{}^{p^{-e_1+e_2'}}$ and $c_2{}^{p^{-e_1+e_2'}}$ are not in L. Then $c_1{}' = c_1{}^{p^{-e_1+1+e_1'}}$ and $c_2{}' = c_2{}^{p^{-e_1+1+e_2'}} \in S^{p^{-e_1+1}} \cap L$ since $L \supseteq S^{p^{-e_1+1}}$. Now $c_1{}', c_2{}' \notin S(L^p) = L^p$. Thus both $c_1{}'$ and $c_2{}'$ are in a subbase of L/S. Suppose $e_1{}' \geqq e_2{}'$. Let $\{t, c_1{}'\}$ be a subbase of L/S with exponents e_1, $e_1 - 1$, respectively. Then $S(c_2{}', c_1{}') = S^{p^{-e_1+1}} \cap L = S(t^p, c_1{}')$ so $S(c_c{}^{p^{e_2'-e_1'}}, c_1) = S(t^{p^{e_1-e_1'}}, c_1)$. Thus $F = S(c_2, c_1) =$

$S(t^{p^{e_1-e_2'}}, c_1)$. Hence F is homogeneous. The result follows by symmetry for $e_2' \geqq e_1'$. Suppose $F = S(c)$ where c has exponent e' over S. Then $c^{p^{-e_1+e'}} \in L$ or $c^{p^{-e_1+1+e'}} \in (S^{p^{-e_1+1}} \cap L) - S(L^p)$. This either $c^{p^{-e_1+e'}}$ or $c^{p^{-e_1+1+e'}}$ is in a subbase of L/S so F is homogeneous.

References

1. J. Deveney, *An intermediate theory for a purely inseparable Galois theory,* Trans. Amer. Math. Soc. **198** (1974), 287–295.

2. ———, *Pure subfields of purely inseparable field extensions,* Canad. J. Math. **28** (1976), 1162–1166.

3. N. Heerema, *A Galois theory for inseparable field extensions,* Trans. Amer. Math. Soc. **154** (1971), 193–200.

4. N. Heerema and J. Deveney, *Galois theory for fields K/k finitely generated,* Trans. Amer. Math. Soc. **189** (1974), 263–274. MR **48** #8462.

5. J. Mordeson, *On a Galois theory for inseparable field extensions,* Trans. Amer. Math. Soc. **214** (1975), 337–347.

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

7. M. Sweedler, *Structure of inseparable extensions,* Annals of Math. **87** (1968), 401–410; correction, ibid (2) **89** (1969), 206–207. MR **36** #6391; **38** #4451.

8. W. Waterhouse, *The structure of inseparable field extensions,* Trans. Amer. Math. Soc. **211** (1975), 39–56.

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

Virginia Commonwealth University, Richmond, Virginia 23284

Creighton University, Omaha, Nebraska 68131