TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 214, 1975

ON A GALOIS THEORY FOR INSEPARABLE FIELD EXTENSIONS

BY

JOHN N. MORDESON

ABSTRACT. Heerema has developed a Galois theory for fields L of characteristic $p \neq 0$ in which the Galois subfields K are those for which L/K is normal, modular and, for some nonnegative integer e, $K(L^{p^{e+1}})/K$ is separable. The related automorphism groups G are subgroups of a particular group A of automorphisms on $L[x]/x^{p^e+1}L[x]$ where x is an indeterminate over L. For $H \subseteq G$ Galois subgroups of A, we give a necessary and sufficient condition for H to be G-invariant. An extension of a result of the classical Galois theory is also given as is a necessary and sufficient condition for every intermediate field of L/K to be Galois where K is a Galois subfield of L.

Let L be a field of characteristic $p \neq 0$. In [4], Heerema exhibits an automorphism group invariant field correspondence on L which incorporates both the Krull infinite Galois theory and the purely inseparable, finite higher derivation theory [1]. The associated automorphism groups are subgroups of the group A of all automorphisms f 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 indeterminate over L, e is a nonnegative integer, $x^{p^e+1}L[x]$ is the ideal in $L[x]$ generated by x^{p^e+1}, and $\bar{x}$ is the coset $x + x^{p^e+1}L[x]$.

In this paper we determine further properties concerning this correspondence. We use the following notation: For G a subgroup of A, $G_L = \{f \in G \mid f(L) \subseteq L\}$, $G_0 = \{f \in G \mid f(a) - a \in \bar{x}L[\bar{x}]$ for all $a \in L\}$, and $L^G = \{a \in L \mid f(a) = a$ for all $f \in G\}$. For K a subfield of L, $G^K = \{f \in G \mid f(a) = a$ for all $a \in K\}$.

For subgroups $H \subseteq G$ of A which are Galois [4, Definition 3.6, p. 197], we give a necessary and sufficient condition (Theorem 1) for H to be G-invariant [4, Definition 3.9, p. 198]. This result extends [4, Corollary 4.4, p. 200]. We then give a natural extension of a result of the classical Galois theory (Theorem 2), namely that if H is G-invariant and $H_0 = G_0$, then the quotient group G/H is isomorphic to G_H where G_H is the group of all automorphisms of $L^H[\bar{x}]$ which are the identity on $L^G[\bar{x}]$.

For K a subfield of L such that L/K is algebraic, we say that L/K splits and write $L = S \otimes_K J$ if and only if L is the field composite of S and J over K where

Received by the editors December 3, 1974.

AMS (MOS) subject classifications (1970). Primary 12F15; Secondary 12A55.

Key words and phrases. Higher derivations, normal field extension, modular field extension, purely inseparable field extension. Galois theory.

S is the maximal separable intermediate field of L/K and J is the maximal purely inseparable intermediate field of L/K. For K Galois ([4, Definition 3.7, p. 197], [4, Theorem 3.1, p. 196]), we give some necessary and sufficient conditions for every Galois intermediate field of L/K to split over K (Theorem 3). This result is then applied to the invariance of H_0 in G_L where $H \subseteq G$ are Galois subgroups of A (Corollary to Theorem 3).

For a purely inseparable field extension J/K, we give a necessary and sufficient condition for J/F to have a modular base for every intermediate field F (Theorem 4). This result describes a necessary and sufficient condition for every intermediate field of L/K to be Galois where K is a Galois subfield of L (Proposition 4).

For K a subfield of L such that L/K is algebraic and L/K splits, say $L = S \otimes_K J$, the splitting is called nontrivial when $S \supset K$ and $J \supset K$ where $\supset$ denotes strict inclusion. If F is an intermediate field of L/K, we use the notation SF to denote the field composite of S and F over $S \cap F$. We often use the fact that a subfield K of L is Galois if and only if $L = S \otimes_K J$ where S/K is normal and J/K is modular with exponent $\leqslant e + 1$ [4, Theorem 3.1, p. 196]. Definitions of modlar and modular base can be found in [9, p. 401] or [8, Definition 1.57, p. 53; Definition 1.21, p. 14]. If J/K is a purely inseparable field extension of bounded exponent, then J/K is modular if and only if J/K has a modular base ([9, Theorem 1, p. 403] or [8, Proposition 1.56, p. 50]).

1. **Group invariance.** Let $\mathcal{H}$ denote the group of all rank p^e higher derivations on L where the group operation on $\mathcal{H}$ is defined in [4, p. 194]. We let Δ denote the isomorphism of $\mathcal{H}$ onto A_0 defined in [4, Proposition 2.1, p. 194]. For K a subfield of L, $\mathcal{H}^K = \{d \in \mathcal{H} | d_i(a) = 0, i = 1, \ldots, p^e, \text{ for all } a \in K\}$ where we use the notation $d = \{d_0, d_1, \ldots, d_{p^e}\}$ for $d \in \mathcal{H}$.

THEOREM 1. *Let $H \subseteq G$ be Galois subgroups of A and let S denote the maximal separable intermediate field of L/L^G. Then H is G-invariant if and only if either $L^H \subseteq S$ and H_L is G_L-invariant, or $L^H \supseteq S$, L^H/L^G splits, and H_0 is G_0-invariant.*

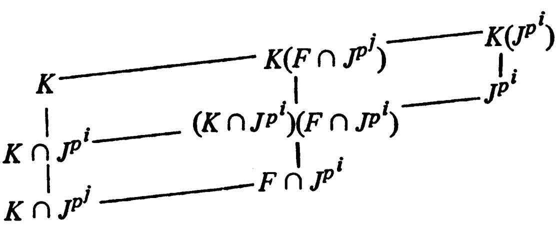
Our proof of Theorem 1 uses the fact that there does not exist a purely inseparable modular field extension J/K of bounded exponent with an intermediate field F such that $J \supset F \supset K$, J/F is modular, and for every modular base M of J/K every $m \in M$ has the same exponent over F that it has over K. The following lemmas show that such a field extension does not exist. However we note in the following example that such a field extension exists if we drop the requirement that J/F be modular.

EXAMPLE 1. Let $K = P(x, y, z)$, $J = K(z^{p^{-2}}, z^{p^{-2}}x^{p^{-1}} + y^{p^{-2}})$, and $F =$

$K(y^{p^{-1}})$ where P is a perfect field of characteristic $p \neq 0$ and x, y, z are algebraically independent indeterminates over P. Then for every modular base M of J/K every $m \in M$ has the same exponent over F that it has over K. Let $\{m_1, m_2\}$ be a modular base J/K. Then both m_1 and m_2 have exponent 2 over K. Suppose that m_2 has exponent 1 over F. Then $F = K(m_2^p)$. Thus $\{m_1, m_2\}$ is a modular base of J/F contrary to the fact that J/F is not modular.

LEMMA 1. *Let J/K be a field extension and F an intermediate field of J/K. If J/K and J/F are modular, then $J/K(F \cap J^{p^j})$ is modular for $j = 0, 1, \ldots$.*

PROOF. Let j be a fixed nonnegative integer. Suppose i is an integer such that $i \geqslant j$. Then $F \cap J^{p^i} = F \cap J^{p^j} \cap J^{p^i} \subseteq K(F \cap J^{p^j}) \cap J^{p^i} \subseteq F \cap J^{p^i}$. Thus $K(F \cap J^{p^j}) \cap J^{p^i} = F \cap J^{p^i}$. Since also $F \supseteq K(F \cap J^{p^j})$ and J/F is modular, $K(F \cap J^{p^j})$ and J^{p^i} are linearly disjoint over $F \cap J^{p^i}$. Now suppose $i < j$. That $K(F \cap J^{p^j})$ and J^{p^i} are linearly disjoint over $(K \cap J^{p^i})(F \cap J^{p^j})$ follows from the following diagram, the modularity of J/K, and [5, Lemma, p. 162].



Q.E.D.

LEMMA 2. *Let J/K be a purely inseparable field extension with bounded exponent n and let F^* be an intermediate field of J/K such that F^*/K has exponent $\leqslant 1$. If J/K and J/F^* are modular and if for every modular base M of J/K every $m \in M$ has the same exponent over F^* that it has over K, then $F^* = K$.*

PROOF. Since F^*/K has exponent $\leqslant 1$, $F^* \cap J^{p^i} \subseteq K(K^{p^{-1}} \cap J^{p^i})$ for $i = 0, 1, \ldots, n$. There does not exist $a \in F^* \cap J^{p^i} - K(K^{p^{-1}} \cap J^{p^{i+1}})$ (set difference) else $a^{p^{-i}} \in K^{p^{-i-1}} \cap J - K^{p^{-i}}(K^{p^{-i-1}} \cap J^p)$ so $a^{p^{-i}} \in K^{p^{-i-1}} \cap J - (K^{p^{-i}} \cap J)(K^{p^{-i-1}} \cap J^p)$. Thus $a^{p^{-i}}$ is in a modular base of J/K [8, Proposition 1.55 (c), p. 49] and has exponent $i + 1$ over K and exponent i over F^*, contrary to the hypothesis. Hence $F^* \cap J^{p^i} \subseteq K(K^{p^{-1}} \cap J^{p^{i+1}})$, $i = 0, 1, \ldots, n$. Since J/K is modular, K and $F^* \cap J^{p^i}$ are linearly disjoint over $K \cap J^{p^i}$, $i = 0, 1, \ldots$. Also since J/F^* is modular, F^* and $K(J^{p^{i+1}})$ are linearly disjoint over $K(F^* \cap J^{p^{i+1}})$, $i = 0, 1, \ldots$, by [8, Lemma 1.60 (a), p. 55]. We have just seen that $F^* \cap J^{p^i} \subseteq K(K^{p^{-1}} \cap J^{p^{i+1}}) \subseteq K(J^{p^{i+1}})$ so $K(F^* \cap J^{p^i}) \subseteq K(J^{p^{i+1}})$, $i = 0, 1, \ldots, n$. Since $K(F^* \cap J^{p^{i+1}}) \subseteq K(F^* \cap J^{p^i}) \subseteq K(J^{p^{i+1}})$, we have that $K(F^* \cap J^{p^i}) = K(F^* \cap J^{p^{i+1}})$ for $i = 0, 1, \ldots, n$. Thus $F^* =$

$K(F^* \cap J^p) = \cdots = K(F^* \cap J^{p^n}) \subseteq K$ so $F^* = K$. Q.E.D.

LEMMA 3. *Let J/K be a purely inseparable field extension of bounded exponent n and let F be an intermediate field of J/K. If J/K and J/F are modular and if for every modular base M of J/K every $m \in M$ has the same exponent over F that it has over K, then $F = K$.*

PROOF. Suppose $F \supset K$. Clearly every modular base of J/K has the same property concerning exponents over any intermediate field of F/K. Since $F = K(F \cap J^{p^0}) \not\subseteq K$ and $K(F \cap J^{p^n}) \subseteq K$, there exists a nonnegative integer i such that $K(F \cap J^{p^i}) \not\subseteq K$ and $K(F \cap J^{p^{i+1}}) \subseteq K$. Set $F^* = K(F \cap J^{p^i})$. Then F^*/K has exponent 1 and J/F^* is modular by Lemma 1. By Lemma 2, $F^* = K$ which contradicts the assumption that $F \supset K$. Thus $F = K$. Q.E.D.

We also make use of the following lemma in the proof of Theorem 1.

LEMMA 4. *Suppose F/K is an algebraic field extension such that $F = S \otimes_K J$ where S is the maximal separable intermediate field and J is the maximal purely inseparable intermediate field. Then the following conditions are equivalent:*

(1) *F/K is modular.*

(2) *F/S is modular.*

(3) *J/K is modular.*

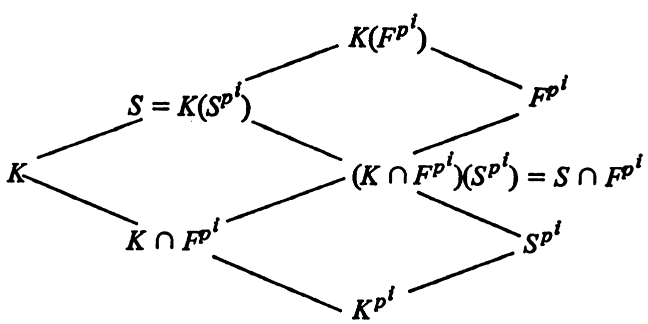
PROOF. We first show that $(K \cap F^{p^i})(S^{p^i}) = S \cap F^{p^i}$, $i = 1, 2, \ldots$. We have

$$K \cap F^{p^i} = (K \otimes_{K^{p^i}} 1) \cap (J^{p^i} \otimes_{K^{p^i}} S^{p^i}) = (K \cap J^{p^i}) \otimes_{K^{p^i}} 1 = K \cap J^{p^i},$$

$$S \cap F^{p^i} = (K \otimes_{K^{p^i}} S^{p^i}) \cap (J^{p^i} \otimes_{K^{p^i}} S^{p^i})$$

$$= (K \cap J^{p^i}) \otimes_{K^{p^i}} S^{p^i} = (K \cap J^{p^i})(S^{p^i}).$$

Thus $(K \cap F^{p^i})(S^{p^i}) = (K \cap J^{p^i})(S^{p^i}) = S \cap F^{p^i}$, $i = 1, 2, \ldots$. That (1) and (2) are equivalent is now apparent from the following diagram and [5, Lemma, p. 162].



That (1) and (3) are equivalent follows from [8, Lemma 1.61(c), p. 56]. Q.E.D.

PROOF OF THEOREM 1. If L/L^G is either separable or purely inseparable, then the theorem is trivially true. Hence suppose L/L^G is inseparable but not purely inseparable. Let J denote the maximal purely inseparable intermediate field of L/L^G. Assume H is G-invariant. Then L^H/L^G is normal by [4, Corollary 4.4, p. 200] so L^H/L^G splits. Also H_0 is G_0-invariant and H_L is G_L-invariant. Suppose $L^H \not\subseteq S$ and $L^H \not\supseteq S$. Since $L^H \not\subseteq S$, $L^H \cap J \supset L^G$. Since H is Galois, L^HJ is modular over L^H by [4, Theorem 3.1, p. 196]. Thus $J/(L^H \cap J)$ is modular by Lemma 4. By Lemma 3, there exists a modular base M of J/L^G and an element m of M such that m has exponent n over L^G and exponent t over $L^H \cap J$ with $n > t$. There exists a subset X of L^G such that $X \cup M$ is a p-base of J. Since L/J is separable algebraic, $X \cup M$ is a p-base of L. Set $B = X \cup M$ and $C = \{b^{p^i} | b \in B$ and i is the exponent of b over $L^G\}$. By [8, Proposition 1.22, p. 14], C is a p-base of L^G. Since $L^H \not\supseteq S$, $S \supset L^H \cap S$. Let $s \in S - L^H \cap S$. Let q be an integer such that $p^{e-n} < q \leqslant p^{e-n+1}$. Then there exists $d = \{d_0, d_1, \ldots, d_{p^e}\} \in H$ such that $d_i(m) = 0$, $i = 1, \ldots, q-1$, $d_q(m) = s$, and $d_i(b) = 0$ $(i = 1, \ldots, p^e)$ for all $b \in B - \{m\}$. For all $c \in C - \{m^{p^n}\}$, $d_i(c) = 0$ for $i = 1, \ldots, p^e$. Now $d_i(m^{p^n}) = (d_j(m))^{p^n}$ if $i = jp^n$ for some j and $d_i(m^{p^n}) = 0$ otherwise by [10, p. 436]. Consider those i such that $i = jp^n$. Then $1 \leqslant j \leqslant p^{e-n} < q$ whence $d_i(m^{p^n}) = 0$. Thus $d \in H^{L^G}$. Since $s \notin L^H$, there exists $h_1 \in H_L$ such that $h_1(s) = s' \in S$ with $s' \neq s$. Now $p^{e-n+t} < qp^t \leqslant p^{e-n+t+1} \leqslant p^e$ so d_{qp^t} is defined. Also $m^{p^t} \in L^H \cap J$, $m^{p^t} \notin L^G$, and $d_{qp^t}(m^{p^t}) = (d_q(m))^{p^t} = s^{p^t}$. For any integer i such that $1 \leqslant i < qp^t$, we have that $d_i(m^{p^t}) = (d_j(m))^{p^t}$ if $i = jp^t$ for some j and $d_i(m^{p^t}) = 0$ otherwise. For those i such that $i = jp^t$, $jp^t < qp^t$ so $j < q$. Thus $d_i(m^{p^t}) = 0$ when $1 \leqslant i < qp^t$. We now obtain a contradiction by showing that H is not G-invariant. Thus either $L^H \subseteq S$ or $L^H \supseteq S$. We show that H is not G-invariant by showing that $h_1g_0(m^{p^t}) \neq g_0(m^{p^t})$ where $g_0 = \Delta(d)$. In the following we use the fact that h_1 is the identity on J. Now

$$h_1g_0(m^{p^t}) = h_1\left(m^{p^t} + \bar{x}^{qp^t}s^{p^t} + \sum_{i=qp^t+1}^{p^e} \bar{x}^i d_i(m^{p^t})\right)$$

$$= m^{p^t} + \bar{x}^{qp^t}s'^{p^t} + \sum_{i=qp^t+1}^{p^e} \bar{x}^i h_1 d_i(m^{p^t}).$$

Clearly $h_1g_0(m^{p^t}) \neq g_0(m^{p^t})$ since $\{1, \bar{x}, \ldots, \bar{x}^{p^e}\}$ is linearly independent over L and $s^{p^t} \neq s'^{p^t}$.

Conversely, suppose $L^H \subseteq S$ and H_L is G_L-invariant. Let $g \in G$ and $h \in H$. Then, by [4, Proposition 2.4, p. 195], $g = g_1g_0$ and $h = h_1h_0$ for unique $g_1 \in G_L$, $g_0 \in G_0$, $h_1 \in H_L$, $h_0 \in H_0$. Let $s \in L^H$. Since $g_1(s) \in S$, $g_1^{-1}h_1g_1(s) \in S$, and g_0, h_0 are identities on S, it follows easily that $g^{-1}hg(s) = s$. Thus $g^{-1}hg \in H$ so H is

G-invariant. Now suppose $L^H \supseteq S$, L^H/L^G splits, and H_0 is G_0-invariant. Since $L^H \supseteq S$, we have that H_L consists only of the identity map. Since L^H/L^G splits, we have that H_0 is G_L-invariant by [4, Theorem 4.2, p. 199]. Thus if $g = g_1 g_0 \in G$ and $h = h_0 \in H = H_0$ where $g_1 \in G_L$ and $g_0 \in G_0$, we have $g^{-1}hg = g_0^{-1}h_0' g_0$ for some $h_0' \in H_0$. Thus $g^{-1}hg \in H_0 = H$ since H_0 is G_0-invariant. Hence H is G-invariant. Q.E.D.

2. **Quotient groups.** Let $H \subseteq G$ be Galois subgroups of A. Let G_H denote the group of all automorphisms g_H for $L^H[\bar{x}] = L^H[x]/x^{p^e+1}L^H[x]$ such that $g_H(\bar{x}) = \bar{x}$ and g_H is the identity on L^G. If H is G-invariant, then $H_0 = G_0$ or $H_0 = H$ by Theorem 1. In this section, S denotes the maximal separable intermediate field of L/L^G and J denotes the maximal purely inseparable intermediate field of L/L^G.

THEOREM 2. *Let $H \subseteq G$ be Galois subgroups of A. If H is G-invariant and $H_0 = G_0$, then $G/H \cong G_H$.*

PROOF. Define the mapping Φ on G by, for all $g \in G$, $\Phi(g)$ is the restriction of g to $L^H[\bar{x}]$. Since H is G-invariant and $H_0 = G_0$, $L^G \subseteq L^H \subseteq S$ and, L^H/L^G is normal. Let $g = g_1 g_0 \in G$ where $g_1 \in G_1, g_0 \in G_0$. Since $L^H \subseteq S$, g_0 is the identity on $L^H[\bar{x}]$. Since L^H/L^G is normal, $g_1(L^H) = L^H$. Thus $g(L^H) = L^H$ so $g(L^H[\bar{x}]) = L^H[\bar{x}]$. Hence Φ maps G into G_H and it follows easily that Φ is a homomorphism. Let $g_H \in G_H$. Since $L^H \subseteq S$, $g_H(L^H) = L^H$. Since L^H/L^G is normal, the restriction of g_H to L^H can be extended to an automorphism of S. This extension can be extended to an element g_H^* of G by requiring it to be the identity on $J[\bar{x}]$. Thus for all $g_H \in G_H$, $g_H^* \in G$ and $\Phi(g_H^*) = g_H$. Hence Φ maps G onto G_H. Since every element of H is the identity on $L^H[\bar{x}]$, $H \subseteq \operatorname{Ker} \Phi$. Since H is Galois, $H = \{f \in A \mid f(a) = a \text{ for all } a \in L^H\}$. Thus since every $f \in \operatorname{Ker} \Phi$ is the identity on L^H, $f \in H$ so $\operatorname{Ker} \Phi \subseteq H$. Therefore $H = \operatorname{Ker} \Phi$ whence $G/H \cong G_H$. Q.E.D.

The following example shows that if $H \subseteq G$ are Galois subgroups of A such that H is G-invariant, then it is not necessarily the case that $L^H[\bar{x}] = \{q(\bar{x}) \in L^H[\bar{x}] \mid h(q(\bar{x})) = q(\bar{x}) \text{ for all } h \in H\}$ even though $L^H = \{a \in L \mid h(a) = a \text{ for all } h \in H\}$.

EXAMPLE 2. Let $L = P(u, v)$ and $K = P(u^p, v^p)$ where P is a perfect field of characteristic $p \neq 0$ and u, v are algebraically independent indeterminates over P. Let $\mathcal{H}$ be the group of all rank p^e higher derivations on L with $e = 0$. Set $G = \Delta(\mathcal{H}^K)$ and $H = \Delta(\mathcal{H}^{K(u)})$. Let $d = \{d_0, d_1\} \in \mathcal{H}^{K(u)}$ and set $h = \Delta(d)$. Then $h(u + \bar{x}v) = u + \bar{x}d_1(u) + \bar{x}v + \bar{x}^2 d_1(v) = u + \bar{x}v$. However $u + \bar{x}v \notin L^H[\bar{x}] = K(u)[\bar{x}]$. This example also shows that $\mathcal{H}^{L^H}$ can be $\mathcal{H}^{L^G}$-invariant without L^H being invariant under every $d \in \mathcal{H}^{L^G}$. Let $d = \{d_0, d_1\} \in \mathcal{H}^{L^G}$ be such that $d_1(u) = v$. Then L^H is not invariant under d. However for all $d = \{d_0, d_1\} \in \mathcal{H}L^G$ and for all $d' = \{d'_0, d'_1\} \in \mathcal{H}L^H$, $d^{-1}d'd = \{d'_0, -d'_1\} \in \mathcal{H}L^H$ so $\mathcal{H}L^H$ is $\mathcal{H}L^G$-invariant.

In view of Example 2 and [2, Corollary 3.6], the existence of a theorem corresponding to Theorem 2 for the case $H_0 = H$ is unlikely. However we do have the following partial results.

PROPOSITION 1. *Let $H \subseteq G$ be Galois subgroups of A. If H is G-invariant and $H_0 = H$, then $G_L \cong (G_H)_{L^H}$.*

PROOF. Define the mapping Φ on G_L by, for all $g_1 \in G_L$, $\Phi(g_1)$ is the restriction of g_1 to $L^H[\bar{x}]$. For $g_1 \in G_L$, g_1 is the identity on J and $g_1(S) = S$. Thus $g_1(L^H[\bar{x}]) = L^H[\bar{x}]$. Hence it is clear that Φ is a homomorphism of G_L into $(G_H)_{L^H}$. Let $g_H \in (G_H)_{L^H}$. Then g_H is the identity on $L^H \cap J$ since $L^H = S \otimes_{L^G} (L^H \cap J)$. Now g_H has a unique extension g_H^* to an element of G_L, namely g_H^* is the identity on $J[\bar{x}]$. The existence of the extension implies Φ maps G_L onto $(G_H)_{L^H}$ while the unicity of the extension implies that Φ is one-one. Q.E.D.

Let $G' = \{g \in G | g(L^H[\bar{x}]) = L^H[\bar{x}]\}$ where $H \subseteq G$ are Galois subgroups of A. Then G' is a subgroup of G and $H \subseteq G'$.

PROPOSITION 2. *Let $H \subseteq G$ be Galois subgroups of A such that H is G-invariant and $H_0 = H$. If $L = L^H \otimes_S J'$ for some intermediate field J' of L/S such that L^H/S and J'/S are modular, then $G'/H \cong G_H$.*

PROOF. Define the mapping Φ on G' by for all $g' \in G'$, $\Phi(g')$ is the restriction of g' to $L^H[\bar{x}]$. Since $L = L^H \otimes_S J'$ with L^H/S and J'/S modular, every element in G_H has an extension to an element of G' by [2, Theorem 3.4]. The remainder of the proof follows in an entirely similar manner to that of Theorem 2. Q.E.D.

3. **Splitting.** An exceptional field extension is one which is inseparable but has no elements (except those in the base field) which are purely inseparable over the base field ([3], [7]). A reliable field extension is one which is generated by every relative p-base [7].

We let S denote the maximal separable intermediate field and J the maximal purely inseparable intermediate field of the field extension F/K in the following lemma.

LEMMA 5. *Let F/K be an inseparable but not purely inseparable algebraic field extension such that $F = S \otimes_K J$ where J/K has a modular base. Then there exists an intermediate field of F/K over which F is modular and which is an exceptional and reliable extension of K if and only if $(K^{p^{-1}} \cap J)/K$ is not simple.*

PROOF. If such an intermediate field exists, then $(K^{p^{-1}} \cap J)/K$ is not simple by [7, Theorem 4, p. 46]. Conversely, suppose $(K^{p^{-1}} \cap J)/K$ is not simple. Then J/K is not simple. Let M be a modular base of J/K and let u, v be distinct elements of M. Let n, t denote the exponents of u, v over K, respectively. Suppose $n \geqslant t$. Let $s \in S - K$. Set $E = K(su^{p^{n-t}} + v)$. Now $s \in E$, $E/K(s)$ is simple, and $K(s)$ is the maximal separable intermediate field of E/K. Either $E \cap J \supset K$ or $E \cap J = K$. If $E \cap J \supset K$, then $K(s^{p^{t-1}}u^{p^{n-1}} + v^{p^{t-1}})/K$ splits as can be seen by a simple degree argument. However this is impossible since, by [7, Theorem 4, p. 47], $K(s^{p^{t-1}}u^{p^{n-1}} + v^{p^{t-1}})/K$ is exceptional. Thus $E \cap J = K$ so E/K is exceptional. A similar argument shows that E does not split nontrivially over any intermediate field of $K(s)/K$. Hence by the comments preceding [7, Theorem 1, p. 44], E does not split nontrivially over any intermediate field. Thus E/K is reliable by [7, Theorem 1, p. 44]. Since $v \in E(u)$, $M - \{v\}$ is a modular base of JE/E. Since also $F = SE \otimes_E JE$, F/E is modular. Q.E.D.

THEOREM 3. *Suppose K is a Galois subfield of L. Then the following conditions are equivalent.*

(1) *Every Galois intermediate field of L/K splits over K.*

(2) *Every intermediate field of L/K splits over K.*

(3) *Every intermediate field of L/K is Galois and splits over K.*

(4) *Every intermediate field of L/K is Galois, splits over K, and is modular over K.*

(5) *L/S is simple where S is the maximal separable intermediate field of L/K.*

PROOF. That (4) implies (3), (3) implies (2), and (2) implies (1) is immediate.

(5) implies (4): Let F be an intermediate field of L/K. Since K is a Galois subfield of L, L/K splits. Thus L/F splits, i.e., $L = SF \otimes_F JF$ where J is the maximal purely inseparable intermediate field of L/K. Since L/S is simple, JF/F is simple whence modular. Since also SF/F is normal, F is Galois. If F is an intermediate field of S/K or J/K, then F/K splits trivially. Suppose F/K is inseparable but not purely inseparable. Since L/S is simple, J/K is simple. Hence $(K^{p^{-1}} \cap J)/K$ is simple. Thus F/K is not exceptional by [3, Theorem 6, p. 546]. Let J' be the maximal purely inseparable intermediate field of F/K. Either F/K splits or F/J' is exceptional. However F/J' is not exceptional or else L/J' contains exceptional extensions of J' which is impossible since $(J'^{p^{-1}} \cap J)/J'$ is simple. Thus F/K splits. Since L/S is simple, J'/K is simple whence F/K is modular.

(1) implies (5): Since L/K splits, L splits over every intermediate field. Thus any intermediate field over which L is modular is Galois. Thus by (1) every intermediate field over which L is modular splits over K. Hence $(K^{p^{-1}} \cap J)/K$ is

simple by Lemma 5. Since K is Galois, J/K is modular. Thus J/K whence L/S is simple. Q.E.D.

COROLLARY. *Suppose G is a Galois subgroup of A. Then L/S is simple where S is the maximal separable intermediate field of L/L^G if and only if for every subgroup H of G which is Galois, H_0 is G_L-invariant.*

PROOF. Suppose L/S is simple. Then L^H/L^G splits by Theorem 3. Hence by [4, Theorem 4.2, p. 199], H_0 is G_L-invariant. Conversely, suppose H_0 is G_L-invariant for every subgroup of G which is Galois. Then by [4, Theorem 4.2, p. 199], L^H/L^G splits for every subgroup H of G which is Galois. Let F be any Galois intermediate field of L/L^G. Then A^F is a Galois subgroup of G and $L^{A^F} = F$. Hence F/K splits. Thus L/S is simple by Theorem 3. Q.E.D.

4. **Galois subfields.** Let J/K be a purely inseparable field extension. If J/K has a modular base, then J/K is modular [8, Proposition 1.23, p. 16].

PROPOSITION 3. *Suppose J/K is a purely inseparable field extension. Then every intermediate field of J/K has a modular base over K if and only if $J^p \subseteq K$, or J/K is simple, or J/K has a modular base consisting of two elements.*

PROOF. Suppose every intermediate field of J/K has a modular base over K. Suppose J/K does not have exponent 1 or J/K is not simple. Then if M is a modular base of J/K, M consists of at least two elements one of which has exponent $\geqslant 2$ over K, say m_1. Suppose M has two other elements, say m_2, m_3, with exponents n, t over K, respectively. Then $K(m_1, m_1 m_2^{p^{n-1}} + m_3^{p^{t-1}})$ is an intermediate field of J/K which does not have a modular base over K, a contradiction. Thus M consists of exactly two elements. The converse follows by [8, Proposition 2.5, p. 76]. Q.E.D.

LEMMA 6. *Suppose J/K is a purely inseparable field extension.*

(1) *If $[K : K^p] = p^2$, then J/K is modular.*

(2) *If J/K has a modular base and J/F is modular for every intermediate field F, then J/K has a bounded exponent.*

PROOF. (1) Clearly $K^{p^{-i}}/K$ has a modular base consisting of two elements, $i = 1, 2, \ldots$. By Proposition 3, $(K^{p^{-i}} \cap J)/K$ has a modular base, $i = 1, 2, \ldots$. By [6, Lemma 2, p. 336], $J = \bigcup_{i=1}^{\infty}(K^{p^{-i}} \cap J)$ is modular over K.

(2) Suppose J/K does not have bounded exponent. Let M be a modular base of J/K. There exists $m_i \in M$ such that m_i has exponent e_i over K with $e_i < e_{i+1}$, $i = 0, 1, \ldots$. Set $F = K(M')(m_1^{p^2}, m_2^{p^2}, -m_1^p m_0 + m_2^p)$ where $M' = M - \{m_1, m_2\}$. Then $J = F(m_1, m_2)$. Now $e_2 > e_1 \geqslant 2$ so m_1 and m_2 have exponent 2 over F while m_2 has exponent 1 over $F(m_1)$. Since $m_0, m_1^{p^2}$,

$-m_1^p m_0 + m_2^p$ are p-independent in F, it follows that J/F is not modular ([5, Exercise 6, p. 196] or [8, Example 1.59, p. 55]), a contradiction. Thus J/K has bounded exponent. Q.E.D.

THEOREM 4. *Suppose J/K is a purely inseparable field extension. Then J/F has a modular base for every intermediate field F if and only if* (1) $J^p \subseteq K$, *or* (2) *J/K is simple, or* (3) $[K : K^p] \leqslant p^2$ *and J/K has bounded exponent, or* (4) *J/K has a modular base in which no more than one element has exponent* $\geqslant 2$ *over K.*

PROOF. Suppose J/F has a modular base for every intermediate field F. Suppose further that (1), (2), and (3) do not hold. By (2) of Lemma 6, J/K has a bounded exponent. Since (3) does not hold, $[K : K^p] > p^2$. Let M be a modular base of J/K. Since (1) does not hold, there exists $m_1 \in M$ such that m_1 has exponent $\geqslant 2$ over K. Since (2) does not hold, M has at least two elements. Suppose there exists $m_2 \in M$ such that $m_2 \neq m_1$ and m_2 has exponent $\geqslant 2$ over K. Since $[K : K^p] > p^2$ and M is a modular base of J/K, there exists $m_0 \in J$ such that m_0, $m_1^{p^2}$, $-m_1^p m_0 + m_2^p$ are p-independent in F where $F = K(M')(m_1^{p^2}, m_2^{p^2}, -m_1^p m_0 + m_2^p)$ and $M' = M - \{m_1, m_2\}$. Now as in the proof of (2) of Lemma 6, J/F is not modular, a contradiction. Thus m_1 is the only element of M with exponent $\geqslant 2$ over K.

The converse is immediate if either (1) or (2) holds. Suppose (3) holds. Let F be an intermediate field of J/K. Now $[F : F^p] \leqslant p^2$. Thus J/F is modular by (1) of Lemma 6. Since also J/F has bounded exponent, J/F has a modular base. Suppose (4) holds. Let F be an intermediate field of J/K. If $J^p \subseteq F$, then J/F has a modular base. Suppose $J^p \nsubseteq K$. Let M be a modular base of J/K. Then M contains a relative p-base of J/F, say M'. Since M' is a minimal generating set of J/F and $J^p \nsubseteq F$, M' contains an element m of exponent $\geqslant 2$ over F. By (4) and the fact that $M' \subseteq M$, $(M' - \{m\})^p \subseteq K \subseteq F$. Thus M' is a modular base of J/F. Q.E.D.

Condition (4) of Theorem 4 is equivalent to the existence of a finite iterative higher derivation on J with a field of constants K [10, Theorem 2, p. 439].

COROLLARY. *Suppose J/K is a purely inseparable field extension. Then J/F has a modular base and F/K has a modular base for every intermediate field F if and only if* (1) $J^p \subseteq K$, *or* (2) *J/K is simple, or* (3) $[K : K^p] \leqslant p^2$ *and J/K has bounded exponent, or* (4) *J/K has a modular base consisting of two elements with no more than one element having exponent* $\geqslant 2$ *over K.*

PROOF. Immediate from Proposition 3 and Theorem 4. Q.E.D.

PROPOSITION 4. *Suppose K is a Galois subfield of L. Then every intermediate field of L/K is Galois if and only if L is modular over every intermediate* *field of L/S where S is the maximal separable intermediate field of L/K.*

PROOF. Suppose every intermediate field of L/K is Galois. Let F be an intermediate field of L/S. Then F is Galois so L/F is modular. Conversely, suppose L is modular over every intermediate field of L/S. Let F be an intermediate field of L/K. Since L/K splits, L/F splits, i.e., $L = SF \otimes_F JF$ where J is the maximal purely inseparable intermediate field of L/K. Now L/SF is modular so FJ/F is modular by the equivalence of (2) and (3) of Lemma 4. Since S/K is normal, SF/F is normal. Thus F is Galois. Q.E.D.

REFERENCES

1. R. Davis, *A Galois theory for a class of purely inseparable field extensions* (unpublished notes).

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

3. R. W. Gilmer, Jr. and W. Heinzer, *On the existence of exceptional field extensions*, Bull. Amer. Math. Soc. 74 (1968), 545–547. MR 36 #5107.

4. N. Heerema, *A Galois theory for inseparable field extensions*, Trans. Amer. Math. Soc. 154 (1971), 193–200. MR 42 #4527.

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

6. L. A. Kime, *Purely inseparable, modular extensions of unbounded exponent*, Trans. Amer. Math. Soc. 176 (1973), 335–349. MR 47 #192.

7. J. N. Mordeson and W. W. Shoultz, *p-bases of inseparable field extensions*, Arch. Math. (Basel) 24 (1973), 44–49. MR 47 #6665.

8. 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.

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

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

DEPARTMENT OF MATHEMATICS, CREIGHTON UNIVERSITY, OMAHA, NEBRASKA 68131