TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 154, February 1971

A GALOIS THEORY FOR INSEPARABLE FIELD EXTENSIONS[1]

BY
NICKOLAS HEEREMA

Abstract. A Galois theory is obtained for fields k of characteristic $p\neq 0$ in which the Galois subfields h are those for which k/h is normal, modular, and for some nonnegative integer r, $h(k^{p^{r+1}})/h$ is separable. The related automorphism groups G are subgroups of the group A of automorphisms α on $k[\bar{X}]=k[X]/X^{p^{r+1}}k[X]$, X an indeterminate, such that $\alpha(\bar{X})=\bar{X}$. A subgroup G of A is Galois if and only if G is a semidirect product of subgroups G_k and G_0, where G_k is a Galois group of automorphisms on k (classical separable theory) and G_0 is a Galois group of rank p^r higher derivations on k (Jacobson-Davis purely inseparable theory). Implications of certain invariance conditions on a Galois subgroup of a Galois group are also investigated.

I. **Introduction.** Let k be a field having characteristic $p\neq 0$. The Jacobson Galois correspondence between finite-dimensional restricted p Lie algebras of derivations on k and their fields of constants [6] has been extended recently by R. L. Davis [1], [2] to groups of higher derivations of finite rank and their fields of constants.

In this paper we exhibit an automorphism group invariant field correspondence which incorporates both the Krull infinite Galois theory [7, p. 147] and the purely inseparable theory referred to above. The invariant subfields h are those for which k/h is algebraic, normal, modular (as defined by Sweedler [8, Definition, p. 404]) and the purely inseparable part has finite exponent (Theorem 3.1). The associated automorphism groups are subgroups of the automorphism group of the local ring $k[\bar{X}]$ described below. They can also be described as groups of rank p^r higher derivations as described in §II with the modification that $d^{(0)}$ is an automorphism on k rather than restricting $d^{(0)}$ to be the identity map. The higher derivation approach has the advantage of making unnecessary the introduction of the local ring $k[\bar{X}]$. This seems to be outweighed by the advantage of familiarity of automorphisms and related constructions.

Let $H\subset G$ be Galois groups with invariant fields $k^H\supset k^G$. §IV is concerned with those conditions on H relative to G which are equivalent to k^G being a Galois

Presented to the Society, October 25, 1969 under the title *An extension of classical Galois theory to inseparable fields*; received by the editors March 27, 1970.

AMS 1968 *subject classifications.* Primary 1240; Secondary 1245, 1360.

Key words and phrases. Higher derivations, normal field extension, modular field extension, purely inseparable field extension, semidirect product, linear disjointness, tensor product.

[1] This research was supported by NSF GP-8424.

subfield of k^H. A partial result is obtained (Theorem 4.1). A complete solution awaits an analysis of the above question in the purely inseparable Jacobson-Davis theory.

II. **Definitions and preliminary results.** Let $\bar{X}$ denote the coset of the indeterminate X in the quotient ring $k[\bar{X}]=k[X]/X^{p^r+1}k[X]$, $r\geqq 0$. We will use the following notation.

A: Group of automorphisms α on $k[\bar{X}]$ such that $\alpha(\bar{X}) = \bar{X}$.

For G a subgroup of A,

$$G_k\colon \{\alpha\in G \mid \alpha(k)\subset k\},$$
$$G_0\colon \{\alpha\in G \mid \alpha(a)-a\in \bar{X}k[\bar{X}] \text{ for } a\in k\},$$
$$k^G\colon \{a\in k \mid \alpha(a) = a \text{ for } \alpha \text{ in } G\},$$

and, for h a subfield of k,

$$G^h\colon \{\alpha\in G \mid \alpha(a) = a \text{ for } a\in h\}.$$

For $f(\bar{X})$ in $k[\bar{X}]$ let $\zeta(f(\bar{X}))=f(0)$. Then, for $\alpha\in A$, α^c $(=\zeta\alpha|_k)$ is an automorphism on k. For β an automorphism on k, β^e will denote its unique extension to A. The map $\alpha\rightarrow\alpha^{ce}$ $(=(\alpha^c)^e)$ is a homomorphism of A onto A_k. With a subgroup G of A we associate the groups $G^c=\{\alpha^c \mid \alpha\in G\}$ and $G^{ce}=\{\alpha^{ce} \mid \alpha\in G\}$.

A rank p^r higher derivation on k is a sequence $d=\{d^{(i)} \mid 0\leqq i\leqq p^r\}$ of additive maps of k into k such that $d^{(n)}(ab)=\sum\{d^{(i)}(a)d^{(j)}(b) \mid i+j=n\}$ and $d^{(0)}$ is the identity map. The set $\mathscr{H}$ of all rank p^r higher derivations on k is a group with respect to the composition "$\circ$" where $d\circ e=f$ and $f^{(t)}=\sum\{d^{(i)}e^{(j)} \mid i+j=t\}$ for $t=0,\dots,p^r$ [5, Theorem 1, p. 33].

(2.1) Proposition. *The map $\Delta\colon\mathscr{H}\rightarrow A_0$ given by $\Delta(d)|_k=\sum\{\bar{X}^i d^{(i)} \mid i=0,\dots,p^r\}$ and $\Delta(d)(\bar{X})=\bar{X}$ is an isomorphism of $\mathscr{H}$ with A_0.*

Proof. For $\alpha\in A_0$ and $a\in k$, $\alpha(a)=\sum a_i\bar{X}^i$ with $a_0=a$. For $i=0,\dots,p^r$ let $d^{(i)}(a)=a_i$. Then $d=\{d^{(i)}\}$ is in $\mathscr{H}$ and $\Delta(d)=\alpha$. This and the fact that $\sum\bar{X}^i d^{(i)}$ is an isomorphism for d in $\mathscr{H}$ were essentially observed by Hasse and Schmidt [3]. Also,

$$\begin{aligned}\Delta(d)\Delta(e)|_k &= \sum\{\bar{X}^i d^{(i)}(\bar{X}^j e^{(j)}) \mid 0\leqq i,j\leqq p^r\}\\ &= \sum\{\bar{X}^{(i)}(d\circ e)^{(i)} \mid i=0,\dots,p^r\} = \Delta(d\circ e)|_k.\end{aligned}$$

For $\mathscr{K}$ a subgroup of $\mathscr{H}$ let $k^{\mathscr{K}}=\{a\in k \mid d^{(i)}(a)=0, i>0, d\in\mathscr{K}\}$; $k^{\mathscr{K}}$ is called the field of constants of $\mathscr{K}$. For h a subfield of k let

$$\mathscr{H}^h = \{d\in\mathscr{H} \mid d^{(i)}(a) = 0, i > 0, a\in h\}.$$

The following is an immediate consequence of the definitions involved.

(2.2) Proposition. *For $\mathscr{K}$ a subgroup of $\mathscr{H}$, $k^{\mathscr{K}}=k^{\Delta\mathscr{K}}$, and, for h a subfield of k, $\Delta(\mathscr{H}^h)=A_0^h$.*

A familiar property of higher derivations states that if $d \in \mathscr{H}$ then $d^{(i)}(a^{p^{r+1}})=0$ for $i=1,\ldots,p^r$ [4, Lemma 1, p. 130]. Let $k^\alpha=k^G$ where G is the group generated by α in A. By Propositions 2.1, 2.2 and the above remark we have

(2.3) Proposition. *$k^{p^{r+1}} \subset k^\alpha$ for α in A_0.*

The following three propositions are self evident.

(2.4) Proposition. *Each $\alpha \in A$ has a unique representation as a product $\beta\gamma$, $\beta \in A_k$, $\gamma \in A_0$. In fact, $\beta=\alpha^{ce}$ and thus $\gamma=(\alpha^{ce})^{-1}\alpha$.*

(2.5) Proposition. *$k^\alpha=k^{\alpha^{ce}} \cap k^{(\alpha^{ce})^{-1}\alpha}$.*

(2.6) Corollary. *For G a subgroup of A, let H be the group generated by G^{ce} and G. Then $k^H=k^G=k^{H_k} \cap k^{H_0}$.*

We require the following rather obvious extensions of familiar results. They are proved in Jacobson [7, pp. 49–52] with the assumption that $[k:h]<\infty$.

(2.7) Proposition [7, Lemma, p. 50]. *Let $k \supset m \supset h$ be fields such that, for some positive integer r, $m^{p^r} \subset h$, and k/m is separable algebraic. Then $k=m \otimes_h l$ where l is the separable algebraic closure of h in k.*

Proof. The following argument parallels the proof in Jacobson [7]. Let $\{a_\tau\}=S$ be a basis for k over m. Then

$$a_\tau a_\rho = \sum b_{\tau,\rho,\eta} a_\eta, \qquad b_{\tau,\rho,\eta} \in m,$$

the sum being over a finite subset of S. Also, $a_\tau^{p^r} a_\rho^{p^r} = \sum_1 b_{\tau,\rho,\eta}^{p^r} a_\eta^{p^r}$, and $b_{\tau,\rho,\eta}^{p^r} \in h$. Now $k^{p^r} \subset l$ since $m^{p^r} \subset h$. Hence, $a_\tau^{p^r} \in l$ and S^{p^r} spans both $h[S^{p^r}]$ over h and $m[S^{p^r}]$ over m. It is sufficient to show that S^{p^r} is a basis for l over h and for k over m.

Given b in k, $m(b)=m(b^{p^r})$ since b is separable over m. Now $b=\sum b_\tau a_\tau$, b_τ in m, and $b^{p^r}=\sum b_\tau^{p^r} a_\tau^{p^r}$. Thus $b \in m[b^{p^r}] \subset m[S^{p^r}]$, and b is in the linear span of S^{p^r} over m. Since k is a separable algebraic extension of m, k^p and m are linearly disjoint over m^p. The set S^p is linearly independent over m^p, and hence, over m. By iteration, the set S^{p^r} is linearly independent over m. Thus S^{p^r} is a basis for k over m.

We observed above that $h[S^{p^r}] \subset l$. As above, if b is in l, $b \in h(b^{p^r}) \subset h[S^{p^r}]$. Hence S^{p^r} is a basis for l over h.

(2.8) Proposition. *If k/h is normal and, for some integer r, $k^{p^r} \subset l$, the separable closure of h in k, then $k=l \otimes_h m$ where $m^{p^r} \subset h$.*

The proof of the corresponding result assuming $[k:h]<\infty$ as given in Jacobson [7, Theorem 13, p. 52] also gives (2.8) in view of (2.7).

III. **The Galois correspondence.** We restate the assumption made throughout this paper, namely that k is a field having characteristic $p \neq 0$.

(3.1) Theorem. *Let h be a subfield of a field k such that k/h is algebraic. The following four conditions are equivalent.*

(i) *$h=k^G$ for a subgroup G of A.*

(ii) *k is a normal modular extension of h such that $h(k^{p^{r+1}})/h$ is separable.*

(iii) *There are intermediate fields l and m such that $m^{p^{r+1}}\subset h$, m/h is modular, l/h is normal separable and $k=l\otimes_h m$ (that is, k is generated by l and m, subfields which are linearly disjoint over h).*

(iv) *There are intermediate fields l and m such that l/h is normal separable, m is a tensor product over h of simple purely inseparable extension of h having degree $\leqq p^{r+1}$ and $k=l\otimes_h m$.*

If k satisfied one of (i) *through* (iv) *and $G=A^h$ then $l=k^{G_0}$ and $m=k^{G_k}$ where l and m are given by* (iii) *or* (iv) *above.*

Proof. By Corollary 2.6 we may assume that $G^{ce}\subset G$ and hence that $k^G=k^{G_k}\cap k^{G_0}$. We first prove that k^{G_0} is normal over k^G and is the separable closure of k^G in k. The modularity of k/k^G will follow essentially from certain results due to Sweedler.

(3.2) Lemma. *$\sigma(k^{G_0})=k^{G_0}$ for $\sigma\in G^c$.*

Proof. Suppose to the contrary that for some σ in G^c and a in k^{G_0}, $\sigma(a)=b\notin k^{G_0}$. Choose $\alpha\in G_0$ for which $\alpha(b)\neq b$. Then $\beta=\sigma^{e^{-1}}\alpha\sigma^e$ is in G_0, whereas $\beta(a)\neq a$, which is a contradiction. Thus, $\sigma(k^{G_0})\subset k^{G_0}$ and $\sigma^{-1}(k^{G_0})\subset k^{G_0}$. Hence $\sigma(k^{G_0})=k^{G_0}$.

(3.3) Lemma. *k is a normal extension of k^G.*

Proof. By Lemma 3.2, the restriction to k^{G_0} of α in G^c is an automorphism. Let K be the group of all such automorphisms on k^{G_0}. Since $k^G=k^{G_k}\cap k^{G_0}$, and $G_k=G^{ce}$, the subfield of k^{G_0} invariant under K is k^G. Thus k^{G_0}/k^G is normal separable. By Proposition 2.3 $k^{p^{r+1}}\subset k^{G_0}$ from which we conclude that k^{G_0} is the separable closure of k^G in k.

To complete the proof, let a be in k and let $f(X)$ be its minimum polynomial over k^G. Then for some positive integer e, $f(X)=g(X^e)$ and $g(X)$ is a separable polynomial. Since $g(X)$ has a^{pe} in k^{G_0} as root, $g(X)$ splits over k^{G_0}. Let $g(X)=(X-b_1)\cdots(X-b_t)$ with $a^{pe}=b_1$. Given b_i, there is an α in G^c such that $\alpha(b_1)=b_i$ or $[\alpha(a)]^{pe}=b_i$ and evidently each b_i has a p^eth root in k. It follows that $f(X)$ splits in k which proves the lemma.

The field k^{G_0} is the field of constants of the group $\Delta^{-1}(G_0)$ of higher derivations and thus, by a theorem of Sweedler, k/k^{G_0} is modular [8, Theorem 1, p. 403]. We conclude that k/k^G is modular from the following.

(3.4) Proposition. *Let k be a normal extension of a field h with the property that for some positive integer r, $h(k^{p^r})$ is separable over h. There is a unique extension k' of k, modular over l, the separable closure of h in k. Moreover, k' is modular over h.*

Proof. This result with the added assumption $[k:h]<\infty$ is due to Sweedler [9, Corollary 7, p. 206]. Sweedler's proof with obvious modifications and using (2.8) of this paper where needed suffices to prove the above.

If k/h satisfies (ii) then, by Proposition 2.8, the conditions of (iii) are fulfilled, the modularity of m/h following from a result of Sweedler [8, Lemma 5 (3), p. 407]. The equivalence of (iii) and (iv) is also due to Sweedler [8, Theorem 1, p. 403].

We show that (iv) implies (i) as follows. Let G_1 be the group of extensions to A of the automorphism group of l over h.

(3.5) Proposition. $k^{G_1}=m$.

Proof. Clearly $m\subset k^{G_1}$. If $a\in k^{G_1}$ then, since $h(k^{p^{r+1}})\subset l$, $a^{p^{r+1}}$ is in $l\cap k^{G_1}=h$. Hence a is in m and we have $k^{G_1}=m$.

Let $\mathscr{H}_1$ represent the group of all rank p^r higher derivations of m into m which are trivial on h. Each $d\in\mathscr{H}_1$ has a unique extension to k since k/m is separable algebraic [4, Theorem 3]. Then $\mathscr{H}=\{d \mid d \text{ is an extension to } k \text{ of an element of } \mathscr{H}_1\}$ is a group of rank p^r higher derivations on k with the property $l\subset k^{\mathscr{H}}$. Let G be the subgroup of A generated by G_1 and $\Delta\mathscr{H}$. By Corollary 2.6, $k^G=k^{G_1}\cap k^{G_0}=m\cap k^{\mathscr{H}}=h$.

The last sentence of the theorem remains to be proved. In establishing that (i) implies (ii) it was shown that $k^{G_0}=l$. The proof of (3.5) gives $m=k^{G_k}$.

(3.6) Definition. A subgroup G of A is Galois if $G=A^h$ for a subfield h of k such that k/h is algebraic.

(3.7) Definition. A subfield h of k is Galois if (i) k/h is algebraic and (ii) $h=k^G$ for a subgroup G of A.

Theorem 3.1 identifies those subfields of h which are Galois. The Krull infinite Galois theory asserts that a subgroup G of A_k is Galois if and only if G^c is compact in the finite topology [7, Example 5, p. 151]. R. L. Davis has characterized those subgroups of $\mathscr{H}$ having the form $\mathscr{H}^h$ and hence, via Δ, those subgroups of A_0 which are Galois, with the assumption, however, that $[k:h]<\infty$ [1], [2].

The following result reduces the question of when a subgroup of A is Galois to subgroups of A_0 and A_k.

(3.8) Theorem. *A subgroup G of A is Galois if and only if* (i) $G^{ce}\subset G$ *and* (ii) G^{ce} *and* G^0 *are Galois.*

Proof. The necessity of (i) is clear (see the first sentence of the proof of Theorem 3.1). If G is Galois then in the notation of Theorem 3.1 $G\supset A^l$ and $G\supset A^m$ where $k=l\otimes_{k^G}m$. For α in A^l, α^c is an automorphism on k which is the identity on $k^{p^{r+1}}$ ($k^{p^{r+1}}\subset l$) and hence is the identity on k. Thus, α is in A_0 or $A^l\subset G_0$. By the last sentence of Theorem 3.1 $G_0\subset A^l$ and we have $G_0=A^l$. Also, by Theorem 3.1 $G_k\subset G^m$. Conversely, if α is in A^m then, letting $\beta=\alpha^{ce^{-1}}\alpha$, we have k/k^β is separable algebraic since by (2.5) $m\subset k^\beta$. However, k^β is the field of constants of a finite higher derivation and hence $k=k^\beta$, $\alpha\in A_k$ or $A^m\subset A_k\cap G=G_k$. Hence $G^{ce}=G_k$ $=A^m$ and G^{ce} is Galois.

Suppose; conversely, that G satisfies (i) and (ii). We first show that k/k^G is algebraic. Lemma 3.2 applies since its proof does not require k/k^G to be algebraic. By Lemma 3.2 $G^c|_{k^{G_0}}$ is a group of automorphisms with the property that k^{G_0} is algebraic over its subfield of invariants which is k^G. Since $k^{p^{r+1}} \subset k^{G_0}$ we have k/k^G algebraic. Let $h = k^G$ and $H = A^h$. Then $G \subset H$, $G^c \subset H^c$ and $G^0 \subset H^0$. By Theorem 3.1 $k = m \otimes_h l$, $m = k^{G_k} = k^{H_k}$ and $l = k^{G_0} = k^{H_0}$. But k^{G_k} and k^{H_k} are the fields of invariants of G^c and H^c respectively and, since G^c is Galois, $G^c \supset H^c$ or $G^c = H^c$. Similarly, $G_0 = H_0$ and $G = G^{ce}G_0 = H^{ce}H_0 = H$.

(3.9) Definition. Given subgroups H_1 and H_2 of a group H, we say H_1 is H_2 invariant if for α in H_2, $\alpha^{-1}H_1\alpha \subset H_1$.

We consider the following question. When are two subgroups H of A_k and K of A_0 compatible in the sense that there is a group G in A for which $G_k = H$ and $G_0 = K$? Such a group will exist if and only if KH is such a group and, since K must be an invariant subgroup of G, K and H will be compatible if and only if K is H invariant.

Let $\mathscr{G}$ be the set of groups of automorphisms on k, $\mathscr{D}$ the set of groups of rank p^r higher derivations on k.

(3.10) Definition. A pair $(H, \mathscr{K})$ in $\mathscr{G} \times \mathscr{D}$ is compatible if there is a subgroup G of A such that $G^c = H$ and $G_0 = \Delta(\mathscr{K})$. A pair $(H, \mathscr{K})$ is Galois if it is compatible and $H^e\Delta(\mathscr{K})$ is Galois.

Given $(H, \mathscr{K})$ in $\mathscr{G} \times \mathscr{D}$, $\mathscr{K}$ is invariant under H if given $\sigma \in H$ and $d = \{d^{(i)}\}$ in $\mathscr{K}$ then $\sigma^{-1}\, d\sigma = \{\sigma^{-1}\, d^{(i)}\sigma\}$ is in $\mathscr{K}$. We sum up these remarks with

(3.11) Proposition. *A pair* $(H, \mathscr{K})$ *in* $\mathscr{G} \times \mathscr{D}$ *is compatible if and only if* $\mathscr{K}$ *is* H *invariant. A compatible pair* $(H, \mathscr{K})$ *is Galois if and only if* H^e *and* $\Delta(\mathscr{K})$ *are Galois.*

Proof. The last sentence follows from Theorem 3.8. The rest is a translation of the condition for compatibility of H^e and $\Delta(\mathscr{K})$ stated above.

IV. **The subgroup subfield correspondence.** In this section we consider some of the implications of invariance. Specifically, let $H \subset G$ be Galois subgroups of A. We consider the consequences for k^H/k^G of invariance of H_0 in G_k and of H_k in G_k. The objective of this section is the identification of conditions on H relative to G equivalent to k^H/k^G being Galois. Theorem 4.2 is a partial result in this direction. The discussion following Corollary 4.4 indicates that invariance conditions alone will be insufficient to determine whether or not k^H/k^G is Galois.

(4.1) Theorem. *Let* G *be a Galois subgroup of* A. *Then* G_k *is* G_0 *invariant if and only if* G_k *is* G *or* $\{1\}$.

Proof. If G_k is G_0 invariant then G_k is invariant in G. Hence, since $G_k \cap G_0 = \{1\}$, G is the direct product of G_k and G_0 which means that for $d \in \Delta^{-1}(G_0)$ and α in G_k^c, $\alpha d^{(i)} = d^{(i)}\alpha$, $i = 1, \ldots, p^r$. Using the freedom available in constructing d in $\Delta^{-1}(G_0)$ we will exhibit d and α in G_k which do not commute assuming that G_k and G_0 are nontrivial. By Theorem 3.1(iv), m is a tensor product over $h = k^G$ of purely inseparable extensions $h(x_\tau)$ where p^{n_τ}, the degree of x_τ over h, is such that $n_\tau \leqq r+1$. It follows that the set $S=\{x_\tau^{p^{n_\tau}}\}_\tau$ is a p-independent subset of h and hence of l since separable extensions preserve p-independence. Let $S \cup S_1$ be a p-basis for l. Then $\{x_\tau\} \cup S_1$ is a p-basis for k. We now use the fact that a higher derivation d is determined by its action on a p-basis which action may be arbitrarily prescribed for each map of d [4, Theorem 1, p. 131]. We defined d by the requirement $d^{(i)}(s)=0$ for $s \in \{x_\tau\} \cup S_1$ and $i<p^r$. For $x_1 \in \{x_\tau\}$ we let $d^{p^r}(x_1)=a \in l$, $a \notin m$, and let d^{p^r} map every other element of $\{x_\tau\} \cup S_1$ into 0. Clearly d is trivial on $S \cup S_1$ and hence $\Delta(d)$ is in G_0 since G_0 is Galois. However, $\alpha(a) \neq a$ for some α in G_k and $\alpha d^{(p^r)}(x_1)=\alpha(a) \neq a=d^{(p^r)}(x_1)=d^{p^r}\alpha(x_1)$. Thus, if G_k is G_0 invariant, either G_0 or G_k must be the trivial group.

(4.2) THEOREM. *Let $H \subset G$ be Galois subgroups of A. Let $k=1 \otimes_{k^G} m$ as in Theorem* 3.1. *Then $k^H=l_1 \otimes_{k^G} m_1$ with $l_1 \subset l$ and $m_1 \subset m$ if and only if H_0 is G_k invariant. Moreover, if $k^H=l_1 \otimes_{k^G} m_1$, then $k^{H_0}=l \otimes_{k^G} m_1$, and $k^{H_k}=l_1 \otimes_{k^G} m$.*

Proof. Assume $k^H=l_1 \otimes_{k^G} m_1$. Then $k^{H_0} \supset l \otimes m_1$ and $k^{H_k} \supset l_1 \otimes m$. But, $k=k^{H_0} \otimes_{k^H} k^{H_k}=(l \otimes m_1) \otimes_{k^H} (l_1 \otimes m)$. This in turn means that $k^{H_0}=l \otimes m_1$ and $k^{H_k}=l_1 \otimes m$. If $\alpha \in G_k$ then $\alpha(l) \subset l$ and $\alpha|_m$ is the identity. Hence $\alpha(k^{H_0})=k^{H_0}$, from which it follows that if d is in $\Delta^{-1}(H_0)$ then $\alpha^{-1}\, d\alpha$ is in $\Delta^{-1}(H_0)$ or H_0 is G_k invariant.

Conversely, assume that H_0 is G_k invariant and let $M=G_kH_0$. By Theorem 3.8 G_k and H_0 are Galois. Since $M^{ce}=G_k^{ce}H_0^{ce}=G_k$ and $M_0=H_0$, M is also Galois by Theorem 3.7.

(4.3) LEMMA. *$k^{H_0}=m_1 \otimes_{k^G} l$ where $m_1=k^{H_0} \cap k^{G_k}$ and $k^{H_k}=m \otimes_{k^G} l_1$ where $l_1=k^{H_k} \cap k^{G_0}$.*

Proof of lemma. By the proof of Theorem 3.1 $k^{H_0}=k^{M_0}$ is the separable closure of $k^M=k^{H_0} \cap k^{G_k}=m_1$ in k. However, $l \otimes_{k^G} m_1$ is the separable closure of m_1 in k. We prove this as follows. Let $\{x_\tau\}$ be a basis for $l \otimes m_1$ over m_1 and $\{x_\tau, y_\sigma\}$ a basis over m_1 for the separable closure of m_1 in k. In general, if a field k' is a separable algebraic extension of a field h' and U is a linear basis for k'/h' then $U^p=\{u^p \mid u \in U\}$ is also a basis. Hence $\{x_\tau^{p^{r+1}}, y_\sigma^{p^{r+1}}\}$ is a basis for the separable closure. However, $\{y_\sigma^{p^{r+1}}\} \subset l$ and $\{x_\tau^{p^{r+1}}\}$ spans l over m_1. Thus $\{y_\sigma\}$ is empty and $l \otimes_{k^G} m_1$ is the separable closure of m_1 in k, and $k^{H_0}=l \otimes_{k^G} m_1$.

Considering the remaining equality, we clearly have $k^{H_k} \supset k^{G_k}=m$ and hence $k^{H_k} \supset m \otimes l_1$. To establish equality, let $\{x_\tau\}$ be a basis for l_1/k^G, $\{x_\tau, y_\sigma\}$ for l/k^G and $\{z_\rho\}$ for m/k^G. Assume that $\sum C_{\rho,\sigma}z_\rho y_\sigma$ is in k^{H_k} and not in $m \otimes l_1$ where $C_{\rho,\sigma}$ is in k^G. Then, since $k^{p^{r+1}} \subset k^{G_0}$, we have $\sum C_{\rho,\sigma}^{p^{r+1}} z_\rho^{p^{r+1}} y_\sigma^{p^{r+1}}$ is in $k^{H_k} \cap k^{G_0}=l_1$. But this denies the independence of $\{x_\tau^{p^{r+1}}, y_\sigma^{p^{r+1}}\}$ over k^G, since $z_\rho^{p^{r+1}} \in k^G$. It follows that $k^{H_k}=m \otimes l_1$ and the proof of the lemma is complete. Now $k^H=k^{H_k} \cap k^{H_0}$ $=(m \otimes l_1) \cap (m_1 \otimes l)=m_1 \otimes l_1$.

(4.4) COROLLARY. *If H is an invariant subgroup of G then k^H/k^G is normal.*

Proof. Under the given assumption H_0 is G_k invariant and H_k is G_k invariant. Thus, $H_k|_l$ is an invariant subgroup of $G_k|_l$ having l_1 as its invariant field. It follows that l_1/k^G is normal and hence that k^H/k^G is normal.

It follows from Theorem 4.1 that the converse of the above corollary is not true. If $G=G_kG_0$ and neither G_k nor G_0 is trivial then k^{G_k}/k^G is Galois whereas G_k is not an invariant subgroup of G[2]. The following example illustrates that the purely inseparable theory exhibits the same behavior.

Let k_1 be a field obtained by extending a perfect field by indeterminates x_1 and x_2. Then $\{x_1, x_2\}$ is a p basis for k_0. Let $y_1=x_1^{p^{-2}}$, $y_2=x_2^{p^{-2}}$, and $k=k_0(y_1, y_2)$ $=k_0(y_1) \otimes_{k_0} k_1(y_2)$. Consider the groups $\mathscr{K}\subset\mathscr{H}$ of rank p higher derivations having $k_0(y_1)$ and k_0 as field of constants respectively.

(4.5) $\mathscr{K}$ is not invariant in $\mathscr{H}$.

Proof. Let $d=\{d^{(0)}, \dots, d^{(p)}\}$ and $h=\{h^{(0)}, \dots, h^{(p)}\}$ be higher derivations. Then $h^{-1}=\{h^{(0)}, -h^{(1)}, -h^{(2)}+[h^{(1)}]^2, \dots\}$ [5, Relation (3), p. 53] and $hdh^{-1}=\{d^{(0)}, d^{(1)}, d^{(2)}+[h^{(1)}, d^{(1)}], \dots\}$, where $[h^{(1)}, d^{(1)}]=h^{(1)}d^{(1)}-d^{(1)}h^{(1)}$. We choose $h\in\mathscr{H}$ such that $h^{(1)}(y_1)=y_2$ and $d\in\mathscr{K}$ such that $d^{(1)}(y_2)\neq 0$ (for justification see proof of Theorem 4.1). Then $d^{(2)}+[h^{(1)}d^{(1)}](y_1)=-d^{(1)}h^{(1)}(y_1)\neq 0$ and hdh^{-1} is not in $\mathscr{K}$.

Let $G=\Delta(\mathscr{H})$ and $H=\Delta(\mathscr{K})$. Then $k^G=k_0$, $k^H=k_0(y)$ and k^H/k^G is normal modular, whereas H is not an invariant subgroup of G.

REFERENCES

1. R. L. Davis, *A Galois theory for a class of purely inseparable field extensions*, Dissertation, Florida State University, Tallahassee, Fla., 1969.

2. ———, *A Galois theory for a class of purely inseparable exponent two field extensions*, Bull. Amer. Math. Soc. **75** (1969), 1001–1004. MR **39** #5524.

3. H. Hasse and F. K. Schmidt, *Noch eine Begrundung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten*, J. Reine Angew. Math. **177** (1936), 215–237.

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

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

6. N. Jacobson, *Galois theory of purely inseparable fields of exponent one*, Amer. J. Math. **66** (1944), 645–648. MR **6**, 115.

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

8. M. E. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) **87** (1968), 401–410. MR **36** #6391.

9. ———, *Correction to*: "*Structure of inseparable extensions*", Ann. of Math. (2) **89** (1969), 206–207. MR **38** #4451.

FLORIDA STATE UNIVERSITY,
TALLAHASSEE, FLORIDA 32306

[2] The author is indebted to the referee for this observation.