TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 213, 1975

# A GALOIS THEORY FOR A CLASS OF INSEPARABLE FIELD EXTENSIONS

BY

R. L. DAVIS[1]

ABSTRACT. The structure of the group of rank $n$ higher derivations in a field $K$ is discussed and a characterization of its Galois subgroups is given. This yields a Galois type correspondence between these subgroups and the subfields over which $K$ is purely inseparable, finite dimensional and modular.

**I. Introduction.** The Galois theory due to Jacobson [7] exhibits a one-to-one correspondence between the finite dimensional restricted $p$-Lie subalgebras of the algebra of derivations in the field $K$ and the subfields over which $K$ is finite dimensional and purely inseparable of exponent one. It was conjectured that higher derivations might lead to an extension of the theory to field extensions having higher exponent. The purpose of this paper is to describe such an extension. This is a generalization of the author's exponent two Galois theory [1].

Throughout the development $K$ is a field having odd characteristic $p$. A sequence $\{d_m|0 \leqslant m \leqslant n\}$ of endomorphisms of $(K, +)$ is called a higher derivation in $K$ of rank $n$ if and only if $d_0$ is the identity mapping and $d_i(ab) = \Sigma\ \{d_j(a)d_k(b)|j + k = i\}$. We adopt the notation $(d_m)$ in place of $\{d_m|0 \leqslant m \leqslant n\}$. A group structure for $H^n(K)$, the collection of rank $n$ higher derivations in $K$, is obtained by defining $(d_m)(e_m) = (f_m)$ where $f_i = \Sigma\ \{d_je_k|j + k = i\}$. The field of constants of $(d_m)$ is the intersection of the kernels of the mappings $d_m$, $1 \leqslant m \leqslant n$. We let $H^n(K/k)$ denote the subgroup of $H^n(K)$ consisting of those $(d_m)$ whose fields of constants contain $k$. In this paper we give a characterization of the subgroups $H^n(K/k)$ and thereby obtain a Galois type correspondence between these subgroups of $H^n(K)$ and subfields $k$ over which $K$ is purely inseparable, finite dimensional and modular.

Our approach is to first examine the structure of the group $H^n(K)$ and its subgroups of the form $H^n(K/k)$. Particular attention is given to the upper central series since its factors play a central role in the characterization. Following this we consider the implications of imposing upon an arbitrary subgroup a series of

Presented to the Society, November 21, 1969 under the title *Higher derivations and inseparable Galois theory*; received by the editors August 10, 1972.

*AMS (MOS) subject classifications* (1970). Primary 12F15.

*Key words and phrases.* Higher derivation, purely inseparable, $p$-basis.

[1] This work constitutes a portion of the author's doctoral dissertation at Florida State University.

conditions suggested by the examination of $H^n(K)$. These results are used to assist in the formulation of a technical definition which is used in the subsequent characterization of the groups.

**II. Preliminary results.** We list here a number of results which will be required and discuss the structure of the group $H^n(K)$.

The first result yields the Jacobson Galois theory. An extension of this to the infinite dimensional case can be found in [2], [10].

(2.1) PROPOSITION ([2], [8, p. 186]). *If $D$ is a finite dimensional subspace of* $\operatorname{Der}(K)$ *closed under pth powers and $k$ is the field of constants of $D$, then* $D = \operatorname{Der}(K/k)$ *and* $[K : k] = p^{[D:K]}$.

(2.2) PROPOSITION. *Let $S$ be a subset of* $\operatorname{Der}(K)$ *closed under pth powers and Lie products and $D$ be the K-span of $S$. If $D$ is finite dimensional, then* $D = \operatorname{Der}(K/k)$ *where $k$ is the field of constants of $S$.*

PROOF. We make use of an identity appearing in [9, p. 187] to show that $D$ is closed under $p$th powers and hence by (2.1) is of the desired form. If $a, b \in K$ and $d, e \in S$, then

$$(ad + be)^p = (ad)^p + (be)^p + \sum_{1}^{p-1} s_i(ad, be). \tag{2.3}$$

In this expression $is_i(ad, be)$ is the coefficient of $x^{i-1}$ in

$$[\cdots [ad, \underbrace{xad + be] \cdots xad + be}_{p-1}] \tag{2.4}$$

and $x$ is an indeterminate over the algebra of linear operators on $K$ and [ ; ] denotes Lie product. It is easily shown that $D$ is closed under Lie products and consequently that each term $s_i(ad, be)$ is an element of $D$. According to the formula due to Hochschild: $(ad)^p = a^p d^p + (ad)^{p-1}(a)d$ [8, p. 191], $(ad)^p$ is also an element of $D$. An induction argument shows $(\Sigma_1^n a_i d_i)^p \in D$ whenever $a_i \in K$ and $d_i \in S$ for $1 \leqslant i \leqslant n$. An alternate proof is obtained by essentially reproducing the proof of (2.1).

The next result provides a technique for constructing higher derivations.

(2.5) PROPOSITION [5, THEOREM 1]. *Let $B$ be a p-basis for $K$ and $f$: $\{1, 2, \ldots, n\} \times B \longrightarrow K$ be an arbitrary function. Then there is a unique $(d_m) \in H^n(K)$ such that for each $b \in B$ and $1 \leqslant i \leqslant n$, $d_i(b) = f(i, b)$.*

(2.6) PROPOSITION [11]. *If $K$ is a purely inseparable extension of $k$ having finite exponent, then $K$ is isomorphic to a tensor product over $k$ of simple extensions of $k$ if and only if $k$ is the field of constants of some set of higher derivations defined in $K$.*

The structure of $H^n(K)$ is now considered. A verification that $H^n(K)$ with the composition given in the introduction is a group appears in [4]. The identity $(e_m)$ of the group is given $e_0 = 1$ and $e_i = 0$ for $1 \leqslant i \leqslant n$ and the $i$th mapping of the inverse of $(d_m)$ is given by $\Sigma\{(-1)^r d_{i_1} \cdots d_{i_r} | \Sigma i_j = i\}$. In addition to being a group $H^n(K)$ is closed under a type of scalar multiplication by elements of $K$ given by $a(d_m) = (a^m d_m)$. The following identity for higher derivations will prove useful:

$$(2.7) \qquad d_{pj}(a^p) = d_j(a)^p \quad \text{and} \quad d_i(a^p) = 0 \quad \text{if } i \neq pj \text{ for any } j.$$

An important series of normal subgroups of a group of higher derivations $G$ is defined by: $G_1 = G$ and $G_j = \{(d_m) \in G | d_1 = \cdots = d_{j-1} = 0\}$ for each $2 \leqslant j \leqslant n + 1$. It is shown in (3.1) that for certain subgroups of $H^n(K)$ including those of the form $H^n(K/k)$ this series and the upper central series coincide. For each $1 \leqslant j \leqslant n$ there is a natural injection of $G_j/G_{j+1} = D(G_j)$ into $\mathrm{Der}(K)$. This is given by mapping the coset $(d_m)G_{j+1}$ to $d_j$ which is a derivation. We identify $D(G_j)$ with its image in $\mathrm{Der}(K)$. Let $\langle f; g\rangle = fgf^{-1}g^{-1}$ denote the commutator of two group elements and $[d; e] = de - ed$ denote the Lie product of two derivations. If $(d_m) \in G_j$ and $(e_m) \in G_k$ then $\langle (d_m); (e_m)\rangle \in G_{j+k}$ and has $[d_j; e_k]$ as $j + k$ mapping.

Let $K/k$ be a purely inseparable extension having exponent $n + 1$ and assume $K$ is isomorphic to a tensor product over $k$ of simple extensions of $k$. Thus there are subsets $N_i \subseteq K$ such that $K = \bigotimes_k \{k(a) | a \in \bigcup N_i\}$ and the exponent of each element of $N_i$ over $k$ is $i$.

(2.8) PROPOSITION. *Let $H = H^{p^n}(K/k)$. Then*

$$D(H_{p^i}) = \mathrm{Der}(K/k(N_1) \cdots (N_{n-i})) \quad \textit{for } 0 \leqslant i \leqslant n$$

*and*

$$D(H_{p^i+j}) = D(H_{p^{i+1}}) \quad \textit{for } 0 \leqslant i \leqslant n - 1 \textit{ and } 1 \leqslant j \leqslant p^i(p - 1).$$

PROOF. The following observation is needed to show the existence of $S \subseteq k$ such that $\bigcup N_i \cup S$ is a $p$-basis for $K$: If $T^p \cup S$ is a $p$-independent subset of $k$ then $T \cup S$ is $p$-independent in $k(T)$. The verification of this is routine. Clearly $\bigcup N_i^{p^i}$ is $p$-independent in $k$. Extend $\bigcup N_i^{p^i}$ to a $p$-basis for $k$, $\bigcup N_i^{p^i} \cup S$. The observation is applied to conclude $S \cup N_1 \cup (\bigcup_{i \geqslant 2} N_i^{p^{i-1}})$ is a $p$-independent subset of $k(N_1)(N_2^p) \cdots (N_{n+1}^{p^n})$. Iterate the process to obtain that $\bigcup N_i \cup S$ is $p$-independent in $K$ and hence is a $p$-basis for $K$.

Let $d \in \mathrm{Der}(K/k(N_1) \cdots (N_{n-i}))$. By (2.5) there exists a unique $(d_m) \in H^{p^n}(K)$ satisfying: for each $x \in \bigcup N_i \cup S$, $d_j(x) = 0$ if $j \neq p^i$ and $d_{p^i}(x) = d(x)$. To prove $(d_m) \in H_{p^i}$ it is sufficient to show that it maps the $p$-basis for $k$,

$\bigcup N_j^{p^j} \cup S$, to zero. Let $b^{p^j} \in N_j^{p^j}$ and $1 \leqslant m \leqslant p^n$. If $d_m(b^{p^j})$ is to be nonzero, then (2.7) and the definition of $d_{p^i}$ force $m$ to equal $p^{j+i}$ and $j > n - i$ but this is impossible since $j + i \leqslant n$. This establishes $D(H_{p^i}) \supseteq \mathrm{Der}(K/k(N_1) \cdots (N_{n-i}))$. For the other containment let $a \in k(N_1) \cdots (N_{n-i})$. Then $a^{p^{n-i}} \in k$ and $0 = d_{p^n}(a^{p^{n-i}}) = (d_{p^i}(a))^{p^{n-i}}$ as desired. This same construction technique is used to prove $D(H_{p^i+j}) = \mathrm{Der}(K/k(N_1) \cdots (N_{n-i-1}))$ for $1 \leqslant j \leqslant p^i(p-1)$. The field of constants of $H$ can now be shown easily to be $k$. Let $F$ denote the field of constants of $H$, then $F \subseteq$ field of constants of $D(H_{p^n}) = K^p(k)$. The set $\bigcup \{N_i^p | 2 \leqslant i \leqslant n + 1\} = \{a_j^p\}$ is a $p$-basis for $K^p(k)/k$. There are $(d(i)_m) \in H_{p^{n-1}}$ such that $d(i)_{p^{n-1}}(a_j) = \delta_{ij}$ where $\delta_{ij}$ is the Kronecker delta. The derivations $d(i)_{p^n} | K^p(k)$ form a basis for $\mathrm{Der}(K^p(k)/k)$. Hence $F \subseteq K^{p^2}(k)$ since the field of constants of $\mathrm{Der}(K^p(k)/k)$ is $K^{p^2}(k)$. The procedure can be repeated to obtain $F \subseteq K^{p^{n+1}}(k) = k$.

In general if $G$ is a subset of $H^{p^n}(K)$ and contains $(d_m)$ with $d_1 \neq 0$, then $K$ is purely inseparable over the field of constants of $G$ and the exponent of the extensions is $n + 1$.

III. **The Galois correspondence.** Throughout this section $G$ is a subgroup of $H^{p^n}(K)$ and $F$ is a subfield of $K$ with the property that the restriction of $G$ to $F$ is a subgroup of $H^{p^n}(F)$. We will use $F$ as a matter of convenience; in the subsequent characterization of $H^{p^n}(K/k)$ the role played by $F$ in (3.1)–(3.4) is assumed by $K^{p^i}$ where $0 \leqslant i \leqslant n$. It is also assumed that the restriction of $D(G_1)$ to $F$ is nonzero.

(3.1) PROPOSITION. *If $D(G_1)$ is an $F$-subspace of* Der($K$) *and the restriction mapping of each $D(G_i)$ into* Der($F$) *is injective, then $\{G_i\}$ is the upper central series of $G$.*

PROOF. We show $Z_i = G_{p^n-i+1}$ for $0 \leqslant i \leqslant p^n - 1$ where $Z_i$ is the $i$th term of the upper central series for $G$. Recall $Z_0 = 1$ and $Z_{i+1}$ is taken such that $Z_{i+1}/Z_i$ is the center of $G/Z_i$. Thus assume $Z_j = G_{p^n-j+1}$, $j < p^n - 1$, and let $(d_m) \in Z_{j+1}$ and $b \in F$. Assume $d_s$ is the first nonzero mapping of $(d_m)$ and that $1 \leqslant s \leqslant p^n - j$. Take $(e_m) \in G$ with $e_1 \neq 0$ and $(f_m) \in G$ with $f_1 = be_1$. The coset $(d_m)Z_j$ commutes with both $(e_m)Z_j$ and $(f_m)Z_j$. Therefore $\langle (d_m); (e_m) \rangle$ and $\langle (d_m); (f_m) \rangle \in Z_j = G_{p^n-j+1}$. The $s$ + 1st mappings of these two higher derivations are $[d_s; e_1]$ and $[d_s; f]$. Since $p^n - j + 1 > s + 1$, $[d_s; e_1] = [d_s; f_1] = 0$ and as a direct consequence of this we have the contradiction: $d_s = 0$. Thus $Z_{j+1} \subseteq G_{p^n-j}$. For the containment $G_{p^n-j} \subseteq Z_{j+1}$ let $(d_m) \in G_{p^n-j}$ and $(e_m) \in G$. Then $\langle (e_m); (d_m) \rangle \in G_{p^n-j+1} = Z_j$. Thus the cosets $(d_m)Z_j$ and $(e_m)Z_j$ commute and $(d_m)Z_j$ is in the center of $G/Z_j$ as required.

Notice that in the case in which $F = K$ the condition that $D(G_1)$ be a nonzero subspace of $\mathrm{Der}(K)$ is sufficient to guarantee that $\{G_i\}$ is the upper central series of $G$.

(3.2) Proposition. *If each $D(G_i)$ is an $F$-subspace of* $\mathrm{Der}(K)$, *then $D(G_i) \subseteq D(G_{i+1})$ for $1 \leqslant i \leqslant p^n - 1$. If $G$ is closed under scalar multiplication by elements of $F$, then $D(G_i) \subseteq D(G_{i+1})$ whenever $i$ is relatively prime with $p$.*

Proof. Assume each $D(G_i)$ is an $F$-subspace of $\mathrm{Der}(K)$. In order to prove $D(G_i) \subseteq D(G_{i+1})$ it is necessary to first show that $D(G_1) \subseteq D(G_i)$ for each $i$. Assume $D(G_1) \subseteq D(G_i)$ where $i \geqslant 1$. Let $d \in D(G_1)$ and $a \in F$ such that $d(a) \neq 0$. Since $D(G_i)$ contains $D(G_1)$ which is an $F$-subspace of $\mathrm{Der}(K)$ there exist $(d_m)$, $(f_m)$ in $G$ and $(e_m)$, $(g_m)$ in $G_i$ satisfying $d_1 = d$, $e_i = \tfrac{1}{2}ad(a)^{-1}d$, $f_1 = \tfrac{1}{2}ad$, and $g_i = d(a)^{-1}d$. According to the remark made following (2.7) the higher derivation $\langle (d_m); (e_m)\rangle \langle (g_m); (f_m)\rangle \in G_{i+1}$ and has $[d_1; e_i] + [g_i; f_1]$ as its $i + 1$st mapping. Expanding these Lie products yields $d$. Thus $d \in D(G_{i+1})$.

To show $D(G_i) \subseteq D(G_{i+1})$ let $e \in D(G_i)$, $d \in D(G_1)$ and $b \in F$ such that $d(b) = 1$. There exist $(d_m)$, $(f_m) \in G$ and $(e_m)$, $(g_m) \in G_i$ satisfying $d_1 = d$, $g_i = be$, $f_1 = bd$, and $e_i = e$. The $i + 1$st mapping of $\langle (d_m); (g_m)\rangle \langle (e_m); (f_m)\rangle$ is $[d_1; be_i] + [e_i; bd_1] = e + e(b)d$. Since $D(G_1) \subseteq D(G_{i+1})$ we have $e \in D(G_{i+1})$.

Now we assume $G$ is closed under scalar multiplication by elements of $F$. Since $D(G_1)$ is an $F$-subspace of $\mathrm{Der}(K)$ the argument used to show $D(G_1) \subseteq D(G_i)$ remains valid. In order to show $D(G_i) \subseteq D(G_{i+1})$ let $e \in D(G_i)$, $d \in D(G_1)$ and $b \in F$ such that $d(b) = b^{1-i}/i$. There exist $(d_m)$, $(f_m) \in G$ and $(g_m)$, $(e_m) \in G_i$ with $d_1 = d$, $g_i = b^i e$, $f_1 = b^i d$, and $e_i = e$. The $i + 1$st mapping of $\langle (d_m); (g_m)\rangle \langle (e_m); (f_m)\rangle$ is $[d; b^i e] + [e; b^i d] = e + e(b^i)d$. As before $e \in D(G_{i+1})$ since $D(G_1) \subseteq D(G_{i+1})$.

(3.3) Proposition. *Let $G$ be closed under scalar multiplication by elements of $F$. If $(d_m) \in G$, then $d_i$ is a polynomial in derivations from $D(G_i)$ for $1 \leqslant i < p$ and $d_p$ is a polynomial in derivations from $D(G_p)$ if $d_1 = 0$.*

Proof. From (3.2) we have that $D(G_i) \subseteq D(G_{i+1})$ for $1 \leqslant i \leqslant p - 1$. Let $(d_m) \in G$ have $d_j$ as first nonzero mapping and $1 \leqslant i < p$. If $i = 1$ or $j$, then the conclusion concerning $d_i$ is trivially true. Thus let $i - j > 0$ and induct on $i - j$. Let $r$ be a generator of the multiplicative group of $I/(p)$. The higher derivation $(r^m d_m)(d_m)^{-r^j} \in G_{j+1}$ and has $(r^i - r^j)d_i$ plus a polynomial in $D(G_{i-1})$ as its $i$th mapping. Since $1 \leqslant j < i < p$, $r^i - r^j \neq 0$. The result follows by induction. Now suppose $d_1 = 0$ and let $d_j$ be the first nonzero mapping. The result is trivially true if $j = p$; so assume $2 \leqslant j < p$ and induct on $p - j$. The higher derivation $(r^m d_m)(d_m)^{-r^j} \in G_{j+1}$ and has $(r^p - r^j)d_p$ plus a polynomial in $D(G_{p-1})$

as its $p$th mapping. From this it follows that $d_p$ is a polynomial in mappings from $D(G_p)$.

(3.4) PROPOSITION. *Assume $G$ has the following properties:*

(i) *$G$ is closed under scalar multiplication by elements of $F$,*

(ii) *the restriction mapping of each $D(G_i)$ into* Der$(F)$ *is injective,*

(iii) *$d_{jp}(E) \subseteq E$ for $1 \leqslant j \leqslant p^{n-1}$ and each $(d_m) \in G$ where $E$ is the kernel of $D(G_{p^n})$.*

*Then the mapping $(d_m) \longrightarrow (d_{mp|E})$ is a homomorphism of $G$ into $H^{p^{n-1}}(E)$.*

PROOF. The result will follow readily if it can be shown that for each $(d_m) \in G$, $d_i(E) = 0$ if $p$ fails to divide $i$. Propositions (3.2) and (3.3) show $d_i(E) = 0$ whenever $1 \leqslant i < p$. We assume for each $(d_m) \in G$, $d_j(E) = 0$ whenever $p - 1 \leqslant j < k$ and $j$ is relatively prime to $p$. Suppose $k$ is relatively prime to $p$ (if not, work with $k + 1$ rather then $k$); write $k = pr - s$ with $0 < s < p$. Let $(d_m) \in G$ and $(e_m) \in G_s$ with $0 \neq e_s \in D(G_1)$. Then $(e_m)(d_m)$ has $e_s d_{pr-s}$ plus a mapping that takes $E$ into $E$ as $pr$th map. It must be the case that $e_s d_{pr-s}(E) = 0$ for if not, let $a \in F$ and replace $e_s$ with $ae_s$ by changing the $(e_m)$ being used to conclude $F \subseteq E$ which is a contradiction. If $d_{pr-s}(E) \neq 0$, then a replacement of $(d_m)$ by $(a^m d_m)$ would show $0 = e_s(a^{pr-s}d_{pr-s}(E)) = -sa^{pr-s-1}e_s(a)d_{pr-s}(E)$ and hence $e_s = 0$ which is a contradiction. Thus $d_{pr-s}(E) = 0$ as desired. The verification that the mapping $(d_m) \longrightarrow (d_{mp|E})$ is a homomorphism is elementary.

This homomorphic image of $G$ will be called the collapse of $G$ and is denoted by $CG$.

(3.5) DEFINITION. Let $G$ satisfy the hypothesis of (3.4). We say that $G$ is structured relative to $F$ if each $D(G_i)$ is closed under Lie products and the taking of $p$th powers and $D(G_{p^i+1}) = D(G_{p^{i+1}})$ for $0 \leqslant i \leqslant n - 1$.

Notice that if $G$ is structured, then it possesses all the properties detailed in Propositions (3.1)–(3.4) and the quotient groups of the terms of the upper central series of $G$ will be $F$-subspaces of Der$(K)$. To show this let $a \in F$ and $d \in D(G_{p^i+1})$. Since $D(G_{p^i+1}) = D(G_{p^i+2}) = \cdots = D(G_{p^{i+1}})$ and $G$ is closed under scalar multiplication by elements of $F$, $(a^{-1})^{p^i+1}(a)^{p^i+2}d = ad \in D(G_{p^i+1})$. It follows that each $D(G_j)$ is an $F$-subspace of Der$(K)$.

An inductive characterization of the groups $H^{p^n}(K/k)$ can now be given. We assume the existence of a characterization of the groups $H^{p^{n-1}}(K/k)$ having $[K:k] < \infty$. The Jacobson exponent one Galois theory provides a characterization of the groups $H^1(K/k)$. Let $G$ be a subgroup of $H^{p^n}(K)$ and $S$ denote the subgroup of $H^{p^{n-1}}(K)$ obtained by the deletion of the last $p^n - p^{n-1}$ mappings of all elements of $G$.

(3.6) THEOREM. *$G$ is of the form $H^{p^n}(K/k)$ if:*

(i) *$C^iG$ is structured relative to $K^{p^i}$ for each $0 \leqslant i \leqslant n$.*

(ii) *$D(G_{p^n})$ is finite dimensional.*

(iii) *$S$ satisfies the exponent $n$ Galois theory.*

*Conversely, if $H = H^{p^n}(K/k)$, $[K:k] < \infty$, and $D(H_1) \neq 0$ then $H$ satisfies the above properties.*

PROOF. Let $k$ denote the field of constants of $G$. By the result of Sweedler (2.6), there exist subsets $N_i$ of $K$ for $1 \leqslant i \leqslant n+1$ such that $K = \bigotimes_k \{k(a) | a \in \bigcup N_i\}$ and the exponent of each element of $N_i$ over $k$ is $i$. We first show that $S = H^{p^{n-1}}(K/k(N_1)(N_2^p) \cdots (N_{n+1}^{p^n}))$. Let $a \in N_{j+1}$, then for each $(d_m) \in G$, $0 = d_{ip}(a^{p^{j+1}}) = d_i(a^{p^j})$ for $1 \leqslant i \leqslant p^{n-1}$. Thus we have containment one way. Now let $a$ be an element of the field of constants of $S$. We can write: $a = A_0 + \Sigma_i A_i M_i$ with each $A_i \in k(\bigcup N_i^{p^{i-1}})$ and the $M_i$ distinct nontrivial monomials in elements from $\bigcup N_i$ such that if $n^r$ occurs in $M_i$ and $n \in N_j$, then $0 \leqslant r < p^{j-1}$. Since $a^p \in k$ and each $A_i^p \in k$, we have $a^p = A_0^p$ or $a = A_0 \in k(\bigcup N_i^{p^{i-1}})$. An application of (2.8) shows $D(G_{p^i}) = \mathrm{Der}(K/k(N_1) \cdots (N_{n-i}))$ for $0 \leqslant i \leqslant n-1$ and $[D(G_{p^i}):K] = \Sigma\{\# N_j | n-i+1 \leqslant j \leqslant n+1\}$.

Let $E(i)$ be the field of constants of $D(C^i G_{p^{n-i}})$ for $0 \leqslant i \leqslant n$. It is easily seen that $E(n) = k$. The main part of the theorem proof is devoted to the determination of $E = E(0)$. Ultimately it will be shown that $E = K^p(k)$. To determine $[E:k]$, it is sufficient to evaluate $[E(i):E(i+1)]$ for each $i$ since $[E:k] = \Pi\{[E(i):E(i+1)] | 0 \leqslant i \leqslant n-1\}$. In the development that follows we will see how $[E(i):E(i+1)]$ is determined by the dimension of one of the factor groups of the upper central series of $G$. Recall that $E(i)$-span of $D(C^{i+1}G_{p^{n-i-1}})$ is $\mathrm{Der}(E(i)/E(i+1))$ (2.2) and $[E(i) : E(i+1)] = p^m$ where $m = [\mathrm{Der}(E(i)/E(i+1)):E(i)]$ (2.1). Let $t = p^{n-i-2}+1$ with $0 \leqslant i \leqslant n-2$ and $r = [D(G_t):K]$. We prove $[E(i):E(i+1)] = p^r$ by exhibiting a basis for $D(C^{i+1}G_{t+1}) = D(C^{i+1}G_{p^{n-i-1}})$ over $K^{p^{i+1}}$ consisting of $r$ elements. The term $[E(n-1):E(n)]$ is handled separately.

We begin by showing for $c \in K$, $(e_m) \in G$ with $e_1 \neq 0$, and $1 \leqslant q \leqslant p^{n-i-1}$ there exists a $(g_m) \in G_q$ with $g_q = ce_1$ and $g_{p^{i+1}q}|_{E(i)} = c^{p^{i+1}} e_{p^{i+1}}|_{E(i)}$. This is clearly true for $q = 1$. Assume the result for $q < j$. Let $(g_m)$ and $(h_m) \in G_{j-1}$ have the above property relative to the constants $c$ and $½bc$ respectively where $e_1(b) \neq 0$. A lengthy expansion reveals that

$$(r_m) = \langle (g_m); ((½be_1(b)^{-1})^m e_m)\rangle \langle (e_1(b)^{-m} e_m); (h_m)\rangle \in G_j$$

has the property relative to the constant $c$. Let $(d_m) \in G_t$ and $0 \neq a \in K$. We construct $(f_m) \in G_{t+1}$ such that $f_{t+1} = ad_t$ and the $t+1$st mapping of the image of $(f_m)$ in $C^{i+1}G_{t+1}$ is $a^{p^{i+1}} d_{tp^{i+1}}|_{E(i)}$. Let $(e_m) \in G$ with $e_1(b) = -ab^{-t+1}$ and $(r_m) \in G_{t+1}$ with $r_{t+1} = ce_1$ and $r_{(t+1)p^{i+1}}|_{E(i)} = c^{p^{i+1}} e_{p^{i+1}}|_{E(i)}$ where $c = d_t(b^t)$. Then $(f_m) = \langle (b^m d_m); (e_m)\rangle \langle (b^{tm} e_m); (d_m)\rangle (r_m)$ has the desired property.

To show $[E(i):E(i+1)] = p^r$, let $\{(d(j)_m)\}_j \subseteq G_t$ and $\{n_j\} \subseteq K$ such that $d(j)_t(n_q) = \delta_{jq}$ and $\{d(j)_t\}_j$ is hence a basis for $D(G_t)$. Let $f \in D(C^{i+1}G_{t+1})$ be arbitrary and $(f_m) \in G_{t+1}$ with $f_{(t+1)p^{i+1}}|_{E(i)} = f$. There are $A_i$ in $K$ such that $f_{t+1} = \Sigma A_j d(j)_t$ and there are $(f(j)_m) \in G_{t+1}$ such that $f(j)_{t+1} = A_j d(j)_t$ and $f(j)_{(t+1)p^{i+1}}|_{E(i)} = A_j^{p^{i+1}} d(j)_{(t+1)p^{i+1}}|_{E(i)}$. The higher derivation $(h_m) = (f_m)^{-1}\Pi_j(f(j)_m) \in G_{t+2}$ and

$$0 = h_{(t+2)p^{i+1}}|_{E(i)} = -f_{(t+1)p^{i+1}}|_{E(i)} + \sum A_j^{p^{i+1}} d(j)_{tp^{i+1}}|_{E(i)}.$$

Thus $\{d(j)_{tp^{i+1}}|_{E(i)}\}$ spans $D(C^{i+1}G_{t+1})$ over $K^{p^{i+1}}$ and is linearly independent over $K^{p^{i+1}}$ since $d(j)_{tp^{i+1}}(n_q^{p^{i+1}}) = \delta_{jq}$. This establishes that $[E(i):E(i+1)] = p^r$ where $r = [D(G_{p^{n-i-1}}):K]$ for $0 \leqslant i \leqslant n-2$.

To show $[E(n-1):E(n)] = p^r$ where $r = [D(G_1):K]$ let $\{(d(j)_m)\}_j \subseteq G$ such that $\{d(j)_1\}_j$ is a basis for $D(G_1)$. It will follow that $\{d(j)_{p^n}|_{E(n-1)}\}_j$ is a basis for $D(C^n G_1)$ over $K^{p^n}$.

From what has been proved we have:

$$\begin{aligned}[][E:k] &= \prod [E(i):E(i+1)] = \prod \left( \sum \{\#N_j | n-i+1 \leqslant j \leqslant n+1\} \right) \\ &= \prod [K^{p^{i+1}}(k) : K^{p^{i+2}}(k)] = [K^p(k):k].\end{aligned}$$

Since $K^p(k) \subseteq E$, $E = K^p(k)$.

We approximate an element of $H^{p^n}(K/k)$ by a Cauchy sequence of higher derivations from $G$ in order to show $H^{p^n}(K/k) \subseteq G$. For an arbitrary $(d_m) \in H^{p^n}(K/k)$ there exists an $(e(1)_m) \in G$ such that $d_m = e(1)_m$ for $1 \leqslant m \leqslant p^{n-1}$. Thus $(d_m)(e(1)_m)^{-1} \in H^{p^n}(K/k)_{p^{n-1}+1}$. Assume the existence of $\{(e(q)_m) | 1 \leqslant q \leqslant j\} \subseteq G$ with $(d_m)\Pi(e(q)_m) = (f_m) \in H^{p^n}(K/k)_{p^{n-1}+j}$ where $p^n - p^{n-1} \geqslant j$. Since $f_{p^{n-1}+j} \in \mathrm{Der}(K/k) = D(G_{p^{n-1}+j})$, there exists an $(e(j+1)_m) \in G_{p^{n-1}+j}$ such that $f_{p^{n-1}+j} = -e_{p^{n-1}+j}$. Consequently $(d_m)\Pi(e(q)_m) \in H^{p^n}(K/k)_{p^{n-1}+j+1}$. By induction we construct $(e_m) = \Pi(e(q)_m) \in G$ such that $(e_m) = (d_m)^{-1}$. It then follows that $G = H^{p^n}(K/k)$.

The converse of the theorem is now considered. Let $H = H^{p^n}(K/k)$, $[K:k] < \infty$, and $D(H_1) \neq 0$. It can be assumed that $k$ is the field of constants of $H$. It follows from (2.4) that $K/k$ is a purely inseparable extension having exponent $n+1$ and $K$ is the tensor product over $k$ of simple extensions of $k$. Proposition (2.8) can now be used to show that $G$ satisfies the hypothesis of the theorem.

This theorem provides the desired correspondence. Let $A$ be the collection of subgroups of $H^{p^n}(K)$ satisfying the conditions of (3.5) and let $I$ denote the collection of subfields $k$ of $K$ satisfying:

(1) $[K:k] < \infty$,

(2) $K/k$ is purely inseparable and has exponent $n+1$,

(3) $K$ is a tensor product over $k$ of simple extensions of $k$.

Then the mapping $k \longrightarrow H^{p^n}(K/k)$ of $I$ into $A$ is the inverse of the mapping $G \longrightarrow$ field of constants of $G$ of $A$ into $I$.

## REFERENCES

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

2. M. Gerstenhaber, *On the Galois theory of inseparable extensions*, Bull. Amer. Math. Soc. 70 (1964), 561–566. MR 29 #98.

3. ———, *On infinite inseparable extensions of exponent one*, Bull. Amer. Math. Soc. 71 (1965), 878–881. MR 32 #5645.

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

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

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

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

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

9. ———, *Lie algebras*, Interscience Tracts in Pure and Appl. Math., no. 10, Interscience, New York, 1962. MR 26 #1345.

10. M. Ojanguren and R. Sridharan, *A note on purely inseparable extensions*, Comment. Math. Helv. 44 (1969), 457–461. MR 41 #1708.

11. 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.

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

DEPARTMENT OF MATHEMATICS, UNITED STATES NAVAL ACADEMY, ANNAPOLIS, MARYLAND 21402