HIGHER DERIVATION GALOIS THEORY OF FIELDS

BY

NICKOLAS HEEREMA

ABSTRACT. A Galois correspondence for finitely generated field extensions k/h is presented in the case characteristic $h = p \neq 0$. A field extension k/h is Galois if it is modular and h is separably algebraically closed in k. Galois groups are the direct limit of groups of higher derivations having rank a power of p. Galois groups are characterized in terms of abelian iterative generating sets in a manner which reflects the similarity between the finite rank and infinite rank theories of Heerema and Deveney [9] and gives rise to a theory which encompasses both. Certain intermediate field theorems obtained by Deveney in the finite rank case are extended to the general theory.

I. Introduction. In this paper we bring together two higher derivation Galois theories for fields of characteristic $p \neq 0$ [9]. A higher derivation d of rank n $(0 < n \leqslant \infty)$ on a field k is a set $\{d_i | 0 \leqslant i < n + 1\}$ of additive maps on k which satisfy the Leibniz rule $d_j(ab) = \Sigma\{d_i(a)d_{j-i}(b) | i = 0, \ldots, j\}$ and d_0 is the identity map. An element a in k is a d constant if $d_i(a) = 0$ for $i > 0$. The set of all rank n higher derivations on k is a group with respect to the composition $d \circ e = f$ where $f_j = \Sigma\{d_i e_{j-i} | i = 0, \ldots, j\}$.

Let k be finitely generated over the subfield k_0. $H^\infty(k/k_0)$ and $H^n(k/k_0)$ are respectively the group of infinite rank and the group of rank n higher derivations on K with constant field containing k_0. The field of constants of $H^\infty(k/k_0)$ is the unique minimal intermediate field h such that k/h is separable and h is algebraically closed in k, that is, such that k/h is regular. We refer to h as the regular coclosure of k_0 in k. The field of constants of $H^n(k/k_0)$ is the modular coclosure of $k_0(k^{p^{[n]}})$ in k where $p^{[n]}$ is the least power of p larger than n. k/h is modular if k^{p^n} and h are linearly disjoint over $h \cap k^{p^n}$ for all $n > 0$. This definition is due to Sweedler [13].

In the theories cited previously [9] the authors, following Gerstenhaber and Zaromp [6], characterize $H^\infty(k/k_0)$ and $H^n(k/k_0)$ in terms of abelian sets of generators, the characterizations being similar modulo technicalities. In this paper we, in effect, combine the prior groups by using a direct limit $\overline{H}(k/k_0)$ of the groups $H^{p^n}(k/k_0)$, $n \geqslant 0$. Only higher derivations having rank a power of p are used in order to simplify the details. The resulting Galois correspondence is given in Theorem 5.1. See Gerstenhaber [5, pp. 11, 12] for an application of essentially the same direct limit to deformation theory of rings.

The field of constants h of $H(k/k_0)$ is the constant field of the set of all higher derivations d on k, of arbitrary rank, such that k_0 is in the constant field of d. h is

the unique minimal intermediate field over which k is modular and which is separably algebraically closed in k. Thus h is the separable algebraic closure in k of the modular coclosure t of k_0 in k. Heerema and Tucker [10, Theorem 6] have shown that if $\bar{h} = \bigcup_n (h^{p^{-n}} \cap k)$ then $k = \bar{h} \otimes_h r$ (that is, $\bar{h}$ and r are linearly disjoint over h and $k = \bar{h}r$) where $\bar{h}/h$ is finite, purely inseparable, modular and r/h is regular. Tucker [14] and Deveney and Mordeson [3] have shown how these fields fit in a certain almost canonical lattice of intermediate fields as follows
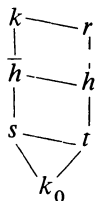
t = modular coclosure of k_0 in k

$\quad = \cap \{l \,|\, k \supset l \supset k_0, k/l \text{ modular}\}$.

s = separable coclosure of k_0 in k.

$\bar{h}$ = regular coclosure of k_0 in k

$\quad$ = algebraic closure of each of s, h, and t in k.

r = any distinguished subfield of k over h.

For details regarding distinguished subfields see Dieudonné [4].

1. k/r, $\bar{h}/h$, and s/t are finite, purely inseparable, modular. $[k : r] = [\bar{h} : h] = [s : t]$.

2. h/t and $\bar{h}/s$ are finite and $[\bar{h} : s] = [h : t]$.

3. s/k_0 is reliable. See Mordeson and Vinograde [12] for definition and basic properties of reliable extensions.

They also show that, as measured by transcendency degree over k_0, h (and hence $\bar{h}$, s, and t) can lie anywhere between k_0 and k. Of the fields in the prior lattice only r is not uniquely determined by k and k_0.

The last section (VI) is concerned with the extension to the present setting of two theorems on intermediate fields due to Deveney [1, Theorems 3.1 and 3.2]. These results are contained in Theorems 6.3 and 6.6.

II. Structure of Galois subfields. Throughout this paper k will be a field of characteristic $p \neq 0$. Sweedler [13, Theorem 1] has shown that k is modular over the constant field h of a set of higher derivations and it is well known that h is separably algebraically closed in k [9, p. 265]. If k/h is finitely generated the converse is also true.

2.1. PROPOSITION. *If k/h is finitely generated the following are equivalent.*

(i) *h is the constant field of a set of higher derivations on k.*

(ii) *k is modular over h and h is separably algebraically closed in k.*

The fact that (ii) implies (i) remains to be shown. By the theorem of Heerema and Tucker [10, Theorem 6] if k/h is modular and separably algebraically closed then $k = \bar{h} \otimes_h r$ where $\bar{h}/h$ is finite, purely inseparable, modular and r/h is finitely generated regular. The field h is the constant field of a set C of higher derivations on $\bar{h}$ [13, Theorem 1] and a set D on r [9, Theorem 4.3]. If $d = \{d_i\}$ is in C then $d' = \{d_i \otimes I\}$, where I is the identity map on r, is a higher derivation on k and $C' = \{d' | d \in C\}$ is readily seen to have r as constant field. Defining D' similarly the set $D' \cup C'$ of higher derivations on k has h as constant field.

Henceforth, all field extensions are assumed to be finitely generated. Subfields satisfying the condition of Proposition 2.1 will be called Galois subfields.

As in the theory of Gerstenhaber and Zaromp [6] and of Heerema and Deveney [9] Galois groups will be characterized in terms of abelian generating sets. For this purpose the following theorems on the structure of Galois extensions are needed. The next result is related to Theorem 7.4 of [9].

2.2. THEOREM. *If h is separably algebraically closed in k then k/h is modular if and only if $k/h(k^{p^n})$ is modular for all n.*

PROOF. We note first that $h = \bigcap_n h(k^{p^n})$ [9, Theorem 7.2]. Tucker has observed that if k/h_α is modular for a collection of subfields $\{h_\alpha\}$ then $k/\bigcap_\alpha h_\alpha$ is modular [14, Corollary 4.2.2]. Hence, $k/h(k^{p^n})$ modular for all n implies k/h modular. Conversely, if k/h is modular and $t < n$ are integers then by transitivity of the linear disjoint property [11, p. 162, Lemma] and the fact that k^{p^t} and h are linearly disjoint over $k^{p^t} \cap h$ we conclude from the following diagram that k^{p^t} and $h(k^{p^n})$ are linearly disjoint over $k^{p^t} \cap h(k^{p^n})$. It follows that k is a modular extension of $h(k^{p^n})$.

$$
\begin{array}{ccc}
k^{p^t} & & \\
| & & \\
h(k^{p^n}) \cap k^{p^t} & - & h(k^{p^n}) \\
| & & | \\
h \cap k^{p^t} & - & h.
\end{array}
$$

A set $\{x_1, \ldots, x_n\} \subset k$ will be called a *tensor basis* for k/h if $k = h(k^{p^t})(x_1) \otimes \cdots \otimes h(k^{p^t})(x_n)$ for all $t \geqslant 1$, tensor product being over $h(k^{p^t})$. Note that if k/h is purely inseparable with finite exponent, a tensor basis for k/h is a subbasis for k/h and conversely [15, p. 435]. As before let $\bar{h}$ be the algebraic closure of h in k.

2.3. THEOREM. *If h is separably algebraically closed in k then h is a Galois subfield if and only if k/h has a tensor basis. The tensor bases of k/h are the sets $S \cup T$ where S is a tensor basis (subbasis) for $\bar{h}/h$ and T is a separating transcendency basis for $k/\bar{h}$.*

PROOF. If k/h has a tensor basis then $k/h(k^{p^n})$ is modular for all n by Sweedler [13, Theorem 1]. Hence by Theorem 2.2 h is Galois. Conversely, assume k/h Galois. Then, $k/\bar{h}$ is separable [10, Lemma 4]. Let T be a separating transcendency basis for $k/\bar{h}$ and let r be the separable algebraic closure of $h(T)$ in k. It is well known that T satisfies the definition of tensor basis for r/h. Since $\bar{h}/h$ is finite, purely inseparable, modular, $\bar{h}$ has a tensor basis S over h [13, Theorem 1]. Since $k = r \otimes_h \bar{h}$ [10, Theorem 6] it follows that $S \cup T$ is a tensor basis for k/h.

It remains to prove that every tensor basis has the prior form. Let X be a tensor basis. Since $\bar{h}(k^p)(X) = k$, X contains a p-basis T for $k/\bar{h}$ and since $k/\bar{h}$ is separable T is a separating transendency basis and hence a tensor basis for $k/\bar{h}$. Let r be the separable algebraic closure of $h(T)$ in k. Then, as before, $k = r \otimes_h \bar{h}$.

2.4. LEMMA. *If x is in $X - T$ then x is purely inseparable algebraic over h and x has the same degree over h as over r.*

PROOF. For m large $k^{p^m} = (\bar{h})^{p^m}(r)^{p^m} \subset r$ and hence $r = h(r^{p^m})(T) \subseteq h(k^{p^m})(T)$ $\subseteq r$. Thus for m large $h(k^{p^m})(T) = r$. Since X is a tensor basis x in $X - T$ has the same degree over $h(k^{p^m})$ as over $h(k^{p^m})(T)$. So for m large, x has the same degree over $h(k^{p^m})$ as over $h(k^{p^{m+i}})$ for all i. It follows that the coefficients of the minimal polynomial of x over $h(k^{p^m})$ are in $h(k^{p^{m+i}})$ for all i and hence are in $\cap_i h(k^{p^{m+i}})$ $= h$ [9, Theorem 7.2]. Clearly x is purely inseparable over h so the lemma is proved.

It remains to prove that $S = X - T$ is a tensor basis for $\bar{h}$ over h. Since X is a tensor basis and for m large, $h(k^{p^m})(T) = r$, we have

$$k = r(S) = \bigotimes_{\substack{r \\ x \in S}} r(x).$$

Since $k = r \otimes_h \bar{h}$, $[k : r] = [\bar{h} : h]$. It follows by degree argument, using Lemma 2.4, that s is a tensor basis for $\bar{h}/h$.

For later use we observe the following. Let $X = S \cup T$ be a tensor basis for k/h as before. If $S = \{x_1, \ldots, x_m\}$ and x_i has degree p^{t_i} over h then $S' = \{x_1^{p^{t_1}}, \ldots, x_m^{p^{t_m}}\}$ is a p-independent subset of h [13, Theorem 1]. Let $P = B \cup S'$ be a p-basis for h ($B \cap S' = \varnothing$). Then $B \cup X$ is a p-basis for k. A higher derivation d on k is completely determined by the action of its maps d_i on $B \cup X$ and that action is free [8, Theorem 9]. Also, d will be trivial on h if and only if $d_i(x) = 0$ for $i > 0$ and x in $S' \cup B$. Thus if d is an infinite higher derivation d will be constant on h if and only if $d_i(x) = 0$ for all $i > 0$ and all x in $B \cup S$. If rank $d = p^n$ then d will be constant on h if and only if $d_j(x) = 0$ for x in B and $j > 0$ and $d_j(x_i) = 0$ for $j < p^{n-t_i}$ and $i = 1, \ldots, m$. The last condition follows from (2.5). See [15, p. 436].

$$\begin{cases} d_{p^t i}(x^{p^t}) = (d_i(x))^{p^t} & \text{for all } i \text{ and } t \geqslant 0. \\ d_j(x^p) = 0 & \text{if } p \nmid j. \end{cases} \tag{2.5}$$

III. The group $\bar{H}(k/k_0)$. Our objective is to construct a group which is, in effect, generated by $\{H^{p^n}(k/k_0)\}_{n>0}$ and $H^\infty(k/k_0)$. This is done by the direct limit construction using the maps $v_{m,n} \colon H^{p^n}(k/k_0) \to H^{p^m}(k/k_0)$ where $m > n$ and $v_{m,n}(d) = f$; $f_{p^{m-n_i}} = d_i$ for $1 \leqslant i \leqslant p^n$, and $f_j = 0$ for $1 < j < p^m$ and $j \nmid p^{m-n}$. The following facts are easily verified.

1. $v_{m,n}(fg) = v_{m,n}(f)v_{m,n}(g)$.
2. $v_{m,n}$ is injective.
3. $v_{r,m}v_{m,n} = v_{r,n}$.

Thus, in particular, $\{H^{p^n}(k/k_0), v_{m,n} | n \geqslant 0, m \geqslant 1\}$ is a directed set of groups. Let $\bar{H}(k/k_0)$ be the direct limit of this system. Let $\bar{d}$ be the element of $\bar{H}(k/k_0)$ containing d. We call $\bar{d}$ the pencil of d. A d in $H^{p^m}(k/k_0)$ is noncontractible if d does not have the form $v_{m,n}(f)$ for some n and f. Note that every $\bar{f}$ contains one and only one noncontractible d. If this d has rank p^n we say $\bar{f}$ has rank p^n. Clearly $\bar{f} = \bar{d} = \{v_{m,n}d | m > n\}$.

A higher derivation d of rank n is the nth section of f if rank $f > n$ and $d_i = f_i$ for $i = 1, \ldots, n$. We say $\bar{d}$ is a section of $\bar{f}$ if each d in $\bar{d}$ is a section of some f' in $\bar{f}$. This is equivalent to the condition d is a section of f given that d and f are noncontractible. We define the extended rank of $\bar{d}$ to be $\sup\{\text{rank } \bar{f} | \bar{d} \text{ is a section of } \bar{f}\}$. Let $\bar{H}^\infty(k/k_0) = \{\bar{d} \in \bar{H}(k/k_0)| \text{ extended rank } \bar{d} = \infty\}$.

3.1. THEOREM. *If $\bar{H}(k/k_0)$ is not the trivial group then $\bar{H}^\infty(k/k_0)$ is the subgroup $\bar{H}(k/\bar{h})$ of $\bar{H}(k/k_0)$ where $\bar{h}$ is the regular coclosure of k_0 in k.*

PROOF. Let $e = \{1, 0\}$ be the rank 1 identity higher derivation. If $\bar{H}(k/k_0) \neq \{\bar{e}\}$ there is a nonzero derivation δ on k/k_0. Then $\bar{d}$ where $d_i = 0$, $1 \leqslant i < p^n - 2$, and $d_{p^n-1} = d_{p^n} = \delta$ is a rank p^n pencil having $\bar{e}$ as a section if $n \geqslant 2$. So, $\bar{e}$ is in $\bar{H}^\infty(k/k_0)$. Let h be the constant field of $\bar{H}(k/k_0)$. Let $S \cup T$ be a tensor basis for k/h as in the discussion following the proof of Theorem 2.3. It follows from (2.5) that if d in $H^{p^n}(k/h)$ is a section of $f \in H^{p^m}(k/h)$ for arbitrary $m > n$ then $d_i(x) = 0$ for any x purely inseparable over h and any $i > 0$. Then d must act trivially on S, $d \in H^{p^n}(k/\bar{h})$ and $\bar{H}^\infty(k/k_0) \subset \bar{H}(k/\bar{h})$. Conversely, $k/\bar{h}$ being separable is thereby a p independence preserving extension. Also, the action of a higher derivation on k is free on a p-basis for k [8, Theorem 9]. It follows that for every $0 \leqslant n < m$ every d in $H^{p^n}(k/\bar{h})$ is the section of an f in $H^{p^n}(k/\bar{h})$ and f can be assumed noncontractible. From these remarks it follows that $\bar{H}^\infty(k/k_0) = \bar{H}(k/\bar{h})$.

IV. Characterization of $\bar{H}(k/h)$. We use the definitions and conventions of Heerema and Deveney [9] with certain modifications. Thus, a set D of higher derivations on k is independent if the set of first nonzero maps (with positive index) of d in D are linearly independent over k. D is abelian if for d, f in D, $d \neq f$, $d_i f_j = f_j d_i$ for all i and j. Iterative higher derivations are assumed to have index 1 or to be normal, which is to say $d_1 \neq 0$. A higher derivation d on k with constant field h is one dimensional if k has a tensor basis over h consisting of a single element, or, equivalently, if $[k: h(k^p)] = p$. Thus every finite iterative higher derivation d is one dimensional [15, p. 438] but if d is infinite it need not have dimension one [16, Theorem 3].

4.1. PROPOSITION. *Let d be an iterative higher derivation on k with constant field h. The following are equivalent.*

(i) *d is one dimensional.*

(ii) *The constant field of the p^nth section of d is $h(k^{p^{n+1}})$ for all $n \geqslant 0$.*

(iii) *The constant field of the p^nth section of d is $h(k^{p^{n+1}})$ for some $n \geqslant 0$.*

PROOF. If d has rank r and $p^n \leqslant r < p^{n+1}$ then $k = h(x)$ and x has degree p^{n+1} over h [15, p. 438]. Hence (i), (ii) and (iii) hold. Assume d infinite. If (i) holds and h_n is the constant field of the p^nth section of d then $[k : h_n] = p^{n+1}$ and $h_n \supseteq h(k^{p^{n+1}})$. But k is by assumption a simple extension of $h(k^{p^{n+1}})$. Hence $h_n = h(k^{p^{n+1}})$. Thus (ii) and hence (iii) holds. If (iii) holds then $[k: h(k^{p^{n+1}})] = p^{n+1}$ since $[k : h_n] = p^{n+1}$. Since k/h is separably generated $[k: h(k^{p^{n+1}})] = p^{(n+1)r}$ where r is the transcendency degree of k/h. Thus (i) holds.

A set $\{x_1, \ldots, x_n\}$ of elements in k is a dual basis A^* of a set $A = \{d^{(1)}, \ldots, d^{(n)}\}$ of finite rank higher derivations on k having constant field h if (i) $k = h(A^*)$ and (ii) for all i and j, $d_1^{(i)}(x_j) = \delta_{i,j}$ and $d_t^{(i)}(x_j) = 0$ if $t > 1$ [9, p. 271].

Let A be a finite set of normal ($d_1 \neq 0$) one dimensional higher derivations and let $A_t = \{d \mid d$ is in A and rank $d \leq p^t$ or d is the p^tth section of f in $A\}$. We note that A is abelian, iterative, or independent if and only if A_t is respectively, abelian, iterative or independent for all $t > 0$. The following is essentially a restatement of Theorem 6.3 of [9, p. 27] in a form which has no restrictions on the ranks of the elements of A.

4.2. THEOREM. *Let A be a finite set of one dimensional higher derivations on k. The following are equivalent.*

(i) *A is an abelian independent set of iterative higher derivations.*

(ii) *A_t has a dual basis A_t^* for all $t > 0$.*

If A satisfies (i) *or* (ii) *then A_t^* is a tensor basis for k over the constant field h_t of A_t. If $A_t = \{d^{(1)}, \ldots, d^{(m)}\}$ and $A_t^* = \{x_1, \ldots, x_m\}$ then the degree of x_i over h_t is p^{t_i+1} where* rank $d^{(i)} = p^{t_i}$. *Also, $k = h_t(x_1) \otimes_{h_t} \cdots \otimes_{h_t} h_t(x_m)$.*

Two observations are called for. The higher derivations in A_t will in general have different ranks in contrast to the set F of the referenced theorem, however the proof of the original theorems does not require the equal rank condition. Since $d_1 \neq 0$ for each d in A the quantity $p(d^{(i)})$ of the original theorem is p^{t_i+1}.

We call a finite set of higher derivations satisfying the conditions of Theorem 4.2 a *standard set of generators*.

The following is concerned with the relationship between dual bases and tensor bases. The next example illustrates the fact that a tensor basis X is a dual basis A_t^* for all t and a suitable standard set of generators A. Let $X = S \cup T$ be a tensor basis for k over a Galois subfield h. Let $S = \{x_1, \ldots, x_n\}$ and assume x_i to have degree p^{t_i+1} over h for $i = 1, \ldots, n$. All elements of $T = \{x_{n+1}, \ldots, x_m\}$ are transcendental over h. As in the discussion following the proof of Theorem 2.3 let $P = B \cup S \cup T$ be a p-basis for k. We construct $A = \{d^{(1)}, \ldots, d^{(m)}\}$ as follows.

(i) $d^{(i)}$ is infinite for $i > n$ and rank $d^{(i)} = p^{t_i}$ for $i \leq n$.

(ii) $d_j^{(i)}(x) = 0$ for $j > 0$, $1 \leq i \leq m$ and $x \in B$.

(iii) $d_1^{(i)}(x_j) = \delta_{i,j}$ for $1 \leq i,j \leq m$.

(iv) $d_t^{(i)}(x_j) = 0$ for $t > 1$ and $1 \leq i,j \leq m$.

By (2.5) $d_j^{(i)}(x_i^{p^{t_i+1}}) = 0$, for $i \leq n$, since $j \leq p_i^{t_i}$. It follows that A acts trivially on a p-basis $B \cup S'$ for h. Then the field of constants of A contains h, and h_t the constant field of A_t contains $h(k^{p^{t+1}})$. It follows that $X = A_t^*$ for all t.

4.3. PROPOSITION. *The constant field of A_t is $h(k^{p^{t+1}})$ and the constant field of A is h.*

PROOF. For future reference we note that the following argument uses the fact that A_t^* is a tensor basis. It does not require that $A_t^* = A_m^*$ for all t and m. Let $A_t = \{f^{(1)}, \ldots, f^{(m)}\}$. Noting that for $i \leq n$ rank $f^{(i)} = p^{s_i}$ where s_i is the minimum of t_i and t and that rank $f^{(i)} = p^t$ otherwise, the result will follow from Theorem 4.2 by a degree argument once it is shown that x_i has degree p^{s_i+1} over $k(h^{p^{t+1}})$ for

$i \leqslant n$ and has degree p^{t+1} otherwise. To that end let r be the separable algebraic closure in k of $h(x_{n+1}, \ldots, x_m)$. Then as in the proof of Theorem 2.3 $k = r \otimes_h \bar{h}$. Also by Theorem 2.3, $\{x_1, \ldots, x_n\}$ is a tensor basis for $\bar{h}/h$. Since $\bar{h} = h(x_1)$ $\otimes_h \cdots \otimes_h h(x_n)$ x_i has degree p^{s_i} over $h(\bar{h})^{p'}$ for $i \leqslant n$. Since $h(k^{p'}) \subset r \otimes_h h(\bar{h}^{p'})$, x_i also has degree p^{s_i} over $h(k^{p'})$. The case $i > n$ is immediate.

Since $h = \cap_t h(k^{p^{t+1}})$ [9, Theorem 7.2] the first clause of Proposition 4.3 leads to the conclusion that the constant field of A is h.

Henceforth A will always designate a standard generating set. We will show that generally, for a given A, there will not be a tensor basis X such that $X = A_t^*$ for all t. Let $A = \{d^{(1)}, \ldots, d^{(m)}\}$ with rank $d^{(i)} = p^{t_i}$ for $i \leqslant n$ and rank $d^{(i)} = \infty$ for $i > n$. Also, $A_F = \{d^{(1)}, \ldots, d^{(n)}\}$ and $A_I = \{d^{(n+1)}, \ldots, d^{(m)}\}$.

4.4. THEOREM. *If h is the constant field of $A = A_F \cup A_I$, then*

(i) $\bar{h}$ *is the constant field of A_I,*

(ii) tr $\deg(k/h) = |A_I|$, *and*

(iii) $A_F|_{\bar{h}}$ *is a standard set of generators having constant field h.*

PROOF. Let h' be the constant field of A_I. Then k/h' is regular and tr $\deg(k/h')$ $= |A_I|$ [9, Theorem 3.2, p. 265]. Since A is abelian h' is invariant under A_I and h is the constant field of the set of higher derivations $A_F|_{h'}$ on h'. If $p^t =$ $\max\{\text{rank } d^{(i)}|_{h'} | i = 1, \ldots, m\}$ then $(h')^{p^{t+1}} \subset h$ by (2.5). Since k/h' is regular and h'/h is algebraic it follows that $h' = \bar{h}$. This proves (i) and (ii).

To verify (iii) it is only necessary to show that $B = \{d_1^{(1)}|_{\bar{h}}, \ldots, d_1^{(n)}|_{\bar{h}}\}$ is an independent set of derivations. If $A_1^* = \{x_1, \ldots, x_m\}$ then by a familiar result the set $\{x_{n+1}, \ldots, x_m\}$ being dual to the set of derivations constant on $\bar{h}$ is p-independent over $\bar{h}$. By (ii) and the fact that $k/\bar{h}$ is separable it follows that $\{x_{n+1}, \ldots, x_m\}$ is a p-basis for $k/\bar{h}$. Since $d_1^{(i)}(x_j) = 0$ for $1 \leqslant i \leqslant n$ and $n < j \leqslant m$ it is clear that a linear dependence among $d_1^{(1)}|_{\bar{h}}, \ldots, d_1^{(n)}|_{\bar{h}}$ also holds if $d_1^{(i)}|_{\bar{h}}$ is replaced by $d_1^{(i)}$ for all i. Thus B is independent. By Theorem 4.2 a p-basis for $\bar{h}/h$ has $|A_F|$ elements.

4.5. COROLLARY. *Let h be the constant field of a standard set of generators A. For all $t \geqslant 0$, $h(k^{p^{t+1}})$ is the constant field of A_t. A dual basis A_t^* is a p-basis for k/h.*

PROOF. For $t > \max\{t_1, \ldots, t_n\}(A_F|_{\bar{h}})_t = (A_F|_{\bar{h}})$ and so by Theorem 4.2 any $(A_F|_{\bar{h}})_t^*$ is a tensor basis for $\bar{h}/h$. Thus a dual basis $A_t^* = \{x_1, \ldots, x_m\}$ can be chosen so that $\{x_1, \ldots, x_n\}$ is a tensor basis for $\bar{h}/h$. Necessarily $\{x_{n+1}, \ldots, x_m\}$ is a p-basis for $k/\bar{h}$, A_t^* is a tensor basis for k/h and the first claim of the corollary follows from the proof of Proposition 4.3. Since h_t in (ii) of Theorem 4.2 is $h(k^{p^{t+1}})$ it follows that any A_t^* is a p-basis for k/h.

Let $\mathfrak{T}$ be the collection of all tensor bases of k/h and for a given A with constant field h let $\mathfrak{D}_t$ be the set of all A_t^*.

4.6. THEOREM. *For all $t \geqslant 0$, $\mathfrak{D}_t \cap \mathfrak{T} \neq \varnothing$. If every d in A has finite rank $\mathfrak{D}_t \subset \mathfrak{T}$ for all t. In general $\cap_t \mathfrak{D}_t = \varnothing$. Each d in A has finite rank if and only if one of the following holds:*

(i) *for t sufficiently large $\mathfrak{D}_t = \mathfrak{D}_{t+1}$ or*

(ii) *for t sufficiently large $\mathfrak{D}_t \subset \mathfrak{T}$ and there is a d in A of finite rank.*

PROOF. We observed that for t large A_t^* can be chosen to be a tensor basis. Since $\mathcal{D}_t \subset \mathcal{D}_s$ for $s < t$ it follows that $\mathcal{D}_t \cap \mathcal{T} \neq \varnothing$ for all t. If $A = A_I$ then k/h is regular and for all t, A_t^* is a separating transcendency basis for k/h and hence a tensor basis, so $\mathcal{D}_t \subset \mathcal{T}$ for all $t \geq 0$. If $A = A_F$ then, as observed in the proof of Corollary 4.5, for t large, $A_t = A_{t+1}$, and $A_t^* \subset \mathcal{T}$. Thus (i) and (ii) hold. On the other hand if $d^{(m)}$ has infinite rank then for a given $A_t^* = \{x_1, \ldots, x_m\}$, $\{x_1, \ldots, x_m + x_m^{p^{t+1}}\}$ is also a dual basis for A_t. However, one of the above must fail to be a dual basis A_{t+1}^* since either $d_{p^{t+1}}^{(m)}(x_m) \neq 0$ or $d_{p^{t+1}}^{(m)}(x_m + x_m^{p^{t+1}}) = [d_1^{(m)}(x_m)]^{p^{t+1}} = 1$ by (2.5). Thus $\mathcal{D}_t \not\subset \mathcal{D}_{t+1}$. Assume in addition that $d^{(1)}$ has finite rank. Then $\{x_1 + x_m^{p^{t+1}}, x_2, \ldots, x_m\}$ is again a dual basis A_t^*, but $A_t^* \not\subset \mathcal{T}$ since $x_1 + x_m^{p^{t+1}}$ is transcendental over h. Thus (i) and (ii) both imply $A = A_F$.

It remains to show that in general $\bigcap_t \mathcal{D}_t = \varnothing$. We use a construction due to F. K. Schmidt [7, Satz 13, p. 237]. Let $k = h(x)$, x an indeterminate, and let $d^{(t)}$ be the rank p^t iterative higher derivation on k/h defined by $d_1^{(t)}(x + x^{p^t}) = 1$, $d_i^{(t)}(x + x^{p^t}) = 0$ for $1 < i \leq p^t$. Let $A = \{d\}$ where d is the infinite iterative one dimensional higher derivation on k/h defined by $d_j = d_j^{(t)}$ for $j < p^t$. If $\bigcap_t \mathcal{D}_t \neq \varnothing$ there is a tensor basis $\{z\}$ which is a dual basis A_t^* for all t. But then $z - x - x^{p^t}$ is in the field of constants $h(x^{p^{t+1}})$ of the p^tth section of d for all t (see Proposition 4.1). Clearly, there is no rational function z in x over h with the above property.

V. The Galois correspondence.
Obtaining a set of generators of a Galois group from a standard set of generators requires the following constructions and definitions. If d has rank t and $q > 0$ is an integer then $v_q(d) = f$ where rank $f = qt$, $f_{qi} = d_i$ and $f_j = 0$ if $q \nmid j$. If $p^m \leq qt$ then $d_{(q,m)}$ is the p^mth section of $v_q(d)$. Given a in k and a higher derivation d, then $ad = \{a^i d_i\}$ is a higher derivation. Given a set D of higher derivations on k, let $(kD)_m$ be the group of rank p^m higher derivations generated by the set of all $(ad)_{(q,m)}$ for $a \in k$, $d \in D$ and any allowable q. $(k\overline{D})$ represents the group of pencils generated by $\{d | d \in (kD)_m$ for some $m \geq 0\}$.

5.1. THEOREM. *Let k/k_0 be finitely generated. A subgroup $\overline{H}$ of $\overline{H}(k/k_0)$ has the form $\overline{H}(k/h)$ if and only if $\overline{H} = (k\overline{A})$ where A is a standard set of generators constant on k_0. Let $\mathcal{F} = \{h | k \supset h \supset k_0$ with k/h Galois$\}$ and $\mathcal{G} = \{(k\overline{A}) | A$ a standard set of generators on k with constant field $k_A \supset k_0\}$. The map $\sigma: \mathcal{F} \to \mathcal{G}$ where $\sigma(h) = \overline{H}(k/h)$ and $\tau: \mathcal{G} \to \mathcal{F}$ where $\tau((k\overline{A})) = k_A$ are inverse bijections.*

PROOF. Given a Galois subfield h by Proposition 4.3 there is a standard generating set A for which $k_A = h$. It remains to show that if A is a standard set of generators then $(k\overline{A}) = \overline{H}(k/k_A)$. Assuming $\overline{d}$ in $\overline{H}(k/k_A)$ to have rank equal to rank$(d) = p^t$ we proceed by induction on $p^t - j + 1$ where d_j is the first nonzero map of d having positive index. Let $A = \{d^{(1)}, \ldots, d^{(m)}\}$ and $A_{t+1}^* = \{x_1, \ldots, x_m\}$. Assume that $d_j(x_1) = \cdots = d_j(x_q) = 0$ and $d_j(x_{q+1}) = -c$ for some $q < m$. Then $f = (cd^{(q+1)})_{(j,t)}$ has rank p^t and $f_j(x_1) = \cdots = f_j(x_q) = 0$ whereas $f_j(x_{q+1}) = c$, f_j being the first nonzero map of f. The first nonzero map of $g = f \circ d$ has index $\geq j$ and $g_j(x_1) = \cdots = g_j(x_{q+1}) = 0$. Repeating this process $m - q - 1$

times if necessary we obtain f in $(kD)_t$ such that rank $(f \circ d) -$ (index of first nonzero map) $< p^t - j$. Invoking the induction hypothesis we have $d \in (kA)_t$ and since t was arbitrary it follows that $(k\overline{A}) \supset \overline{H}(k/k_A)$. Since the reverse inclusion is obvious we have $(k\overline{A}) = \overline{H}(k/k_A)$. The theorem follows.

VI. Intermediate fields. In this section we extend to the present setting the following two theorems due to Deveney.

6.1. THEOREM [1, THEOREM 3.1]. *Let k/h be Galois with $[k:h] < \infty$. An intermediate field l is invariant under all higher derivations on k/h if and only if $l = h(k^{p^t})$ for some t.*

6.2. THEOREM [1, THEOREM 3.2]. *Let k/h be as above and let l be an intermediate field with l/h modular. Every higher derivation on l/h extends to a higher derivation on k/h if and only if there is an intermediate field r modular over h such that $k = l \otimes_h r$.*

6.3. THEOREM. *Let k/h be Galois. An intermediate field l is invariant under $H(k/h)$ the set of all higher derivations of k/h if and only if $l = h(k^{p^n})$ for some $n \geq 0$.*

PROOF. It follows from relation (2.5) that $h(k^{p^m})$ is invariant under $H(k/h)$ for all $m \geq 0$. Assume, conversely, that the intermediate field l is invariant under $H(k/h)$. For any $m > 0$, $k/h(k^{p^m})$ is finite Galois by Theorem 2.2 and by relation (2.5) $l(k^{p^m})$ is invariant under all higher derivations of $k/h(k^{p^m})$. By Theorem 6.1 $l(k^{p^m}) = h(k^{p^{t_m}})$ for some $t_m \leq m$. If $\{t_m\}_{m>0}$ is bounded then for some n, $h(k^{p^n}) = \bigcap_m l(k^{p^m}) = \bar{l}^s$ where $\bar{l}^s$ is the separable algebraic closure of l in k [9, Theorem 7.2]. If not, $\bar{l}^s = \bigcap_m l(k^{p^m}) = \bigcap_m h(k^{p^{t_m}}) = h$ [9, Theorem 7.2] or $l = h$. With the following lemma the proof will be complete.

6.4. LEMMA. *Assume that k/h is not algebraic. If $h(k^{p^n}) \supset l$ and $h(k^{p^n})$ is separable algebraic over l then l is invariant under $H(k/h)$ if and only if $l = h(k^{p^n})$.*

PROOF. Let T be a tensor basis for k/h. Then T^{p^n} contains a p-basis $T_1^{p^n}$ for $h(k^{p^n})/h$. We need the following.

6.5. LEMMA. *A derivation δ on $h(k^{p^n})/h$ such that $\delta(T_1^{p^n}) \subset k^{p^n}$ has the form $d_{p^n}|_{h(k^{p^n})}$ where $d = \{d_i\}$ is in $H(k/h)$ and has rank p^n.*

PROOF. We construct d as follows [6, Theorem 9]. For $t \in T_1$ let $d_1(t) = [\delta(t^{p^n})]^{p^{-n}}$ and let $d_i(t) = 0$ for $1 < i \leq p^n$. Then $d_{p^n}(t^{p^n}) = [d_1(t)]^{p^n} = \delta(t^{p^n})$ and hence $d_{p^n}|_{h(k^{p^n})} = \delta$.

Returning to the proof of Lemma 6.4 assume now that $T_1^{p^n} = \{x_1, \ldots, x_r\}$. We can also assume that x_1 is transcendental over h. If $S = \{s_1, \ldots, s_r\}$ is a p-basis for l/h, then since $h(k^{p^n})/l$ is separable algebraic S is a p-basis for $h(k^{p^n})/h$. Thus for some i, $s_i = g(x_1, \ldots, x_r)$, $g \in h(k^{p^{n+1}})[X_1, \ldots, X_r]$, and $\partial g/\partial x_1 \neq 0$. We can construct a derivation δ on $h(k^{p^n})/h$ such that $\delta(T_1^{p^n}) \subset k^{p^n}$ by choosing $\delta(x_1)$ to be anything in k^{p^n} and requiring $\delta(x_2) = \cdots = \delta(x_r) = 0$. But $\delta(s_i) = (\partial g/\partial x_1)\delta(x_1)$ which is in l by Lemma 6.5. It follows that $k^{p^n} \subset l$ or $l = h(k^{p^n})$.

The following result is similar to Theorem 6.2, however, the hypotheses on l are stronger.

6.6. THEOREM. *Given k/l and l/h Galois, every higher derivation on l/h into k extends to a higher derivation on k if and only if there is a finite purely inseparable modular extension t of h in k such that $l(t) = l \otimes_h t$ and $k/l(t)$ is regular.*

PROOF. Assume l has the above form and let $d = \{d_i\}$ be a higher derivation defined on l into k. Then $d \otimes I = \{d_i \otimes I\}$, where I denotes the identity map on t and is a higher derivation on $l(t)$ into k. Since $k/l(t)$ is p-independence preserving and a higher derivation is determined by its (free) action on a p-basis [6, Theorem 9] it follows that every higher derivation on l into k extends to k.

In proving the converse we observe first that by assumption $k = \bar{h} \otimes_h r$, $l = (\bar{h} \cap l) \otimes_h r_l$ and $k = \bar{l} \otimes_l r^*$ where r/h, r_l/h, and r^*/l are regular extensions and the other tensor factors are finite purely inseparable and modular.

6.7. LEMMA. *The fields r, r^*, and r_l can be chosen so that $r_l \subset r$, with r/r_l separable, and $r^* = l(r)$. Also, $\bar{l} = \bar{h} \otimes_h r_l$.*

PROOF. Since every derivation on l over $\bar{h} \cap l$ extends to k a p-basis T for r_l over h is p-independent in k. Since r_l/h is separable T^{p^t} is a p-basis for $h(r_l^{p^t})$ over h for all t. It follows that T is a p-independent subset of $k/\bar{h}$, $\bar{h}$ being purely inseparable over h. Hence, $T \subset T_1$, where T_1 is a p-basis and hence a separating transcendency basis for $k/\bar{h}$, and as observed earlier r can be chosen to be the separable algebraic closure of $h(T_1)$ in k. For this choice of r, $r_l \subset r$ and r/r_l is separable.

Since $\bar{h}(l) = \bar{h} \otimes_h r_l$ and r/r_l is separably generated it follows that $k = \bar{h} \otimes_h r$ is separably generated over $\bar{h}(l)$. Thus $\bar{l} = \bar{h}(l) = \bar{h} \otimes_h r_l$ and $k = \bar{h}(l)r(l) = \bar{h}(l) \otimes r(l)$.

6.8. LEMMA. *Let l and r be as above with $r^* \subset r$. Every higher derivation on lr/r extends to k.*

PROOF. We observe first that if d and d' are higher derivations of equal rank on k such that $d|_{k_1} = d'|_{k_1}$ for some subfield k_1 of k then k_1 is in the constant field of $d^{-1} \circ d'$. To verify this let $k[\bar{X}] = k[X]/X^{t+1}k[X]$ where $\bar{X} = X + X^{t+1}k[X]$. Each $d \in H^t(k)$ determines an automorphism α_d on $k[\bar{X}]$ given by $\alpha_d(a) = \sum d_i(a)(\bar{X})^i$ and $\alpha_d(\bar{X}) = \bar{X}$. The map $d \to \alpha_d$ is an isomorphism. Thus if $\alpha_d(a) = \alpha_{d'}(a)$ for $a \in k_1$ then $a = \alpha_{d^{-1} \circ d'}(a)$ for $a \in k_1$, that is k_1 is in the constant field of $d^{-1} \circ d'$.

Let d be any higher derivation on lr/r into k and let $d' = d|_l$. By assumption d' extends to a higher derivation d'' on k. Let $d^* = d''|_r$ and let d^{**} be the extension of d^* which is trivial on $\bar{h}$ as in the proof of Theorem 6.6. Then $d^{**-1} \circ d''$ is trivial on r by the above remarks and, by construction of d^{**}, agrees with d'', and hence with d, on l. Thus $d^{**-1} \circ d''$ extends d to k.

Returning to the proof of Theorem 6.6, consider the fields $k \supset (\bar{h} \cap l) \otimes_h r \supset r$. We note that k/r, $k/(\bar{h} \cap l) \otimes_h r$, and $(\bar{h} \cap l) \otimes_h r/r$ are all finite purely inseparable modular. By Lemma 6.8 and Theorem 6.2 there is an extension q of r

which is purely inseparable modular and having the property $k = ((\bar{h} \cap l) \otimes_h r)$ $\otimes_r q$. By associativity of tensor product $k = (\bar{h} \cap l) \otimes_h q$ and $\bar{h} = (\bar{h} \cap l)(t) = (\bar{h} \cap l) \otimes_h t$ where t is the algebraic closure of h in q. In [2, Theorem 4 and its proof] it is shown that in this situation t can be chosen to be modular over h. We have $\bar{l} = \bar{h} \otimes_h r_l = (t \otimes_h \bar{h} \cap l) \otimes_h r_l = t \otimes_h [(\bar{h} \cap l) \otimes_h r_l] = t \otimes_h l$ and $k/\bar{l}$ is regular.

It follows from Theorems 6.3 and 6.6 that there is no proper intermediate field l such that k/l and l/h are Galois; every higher derivation on l/h extends to k and l is invariant under $H(k/h)$.

REFERENCES

1. J. Deveney, *An intermediate theory for a purely inseparable Galois theory*, Trans. Amer. Math. Soc. **198** (1974), 287–296.

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

3. J. Deveney and J. Mordeson, *Subfields and invariants of inseparable field extensions*, Canad. J. Math. **29** (1977), 1304–1311.

4. J. Dieudonné, *Sur les extensions transcendantes separables*, Summa Brasil. Math. (1) **2** (1947), 1 − 20.

5. M. Gerstenhaber, *On the deformation of rings and algebras*. III, Ann. of Math. (1) **88** (1968), 1–34.

6. M. Gerstenhaber and A. Zaromp, *On the Galois theory of purely inseparable field extensions*, Bull. Amer. Math. Soc. **76** (1970), 1011–1014. MR **42** #1806.

7. H. Hasse and R. K. Schmidt, *Noch eine Bergrundung der Theorie der Hoheren Differentialquotienten in einem algebraischen Funktionenkorper einen Unbestimmten*, J. Reine Angew. Math. **177** (1937), 215–237.

8. N. Heerema, *Higher derivations and automorphisms of complete local rings*, Bull. Amer. Math. Soc. **76** (1970), 1212–1225.

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

10. N. Heerema and D. Tucker, *Modular field extensions*, Proc. Amer. Math. Soc. **53** (1975), 301–305.

11. N. Jacobson, *Lectures in abstract algebra*, Vol. III, Van Nostrand, Princeton, N. J., 1963.

12. J. Mordeson and B. Vinograde, *Relatively separated transcendental field extensions*, Arch. Math. **24** (1973), 521–526.

13. M. E. Sweedler, *Structure of inseparable field extensions*, Ann. of Math. (2) **87** (1968), 401–410.

14. D. Tucker, *Finitely generated field extensions*, Dissertation, Florida State University, Tallahassee, Florida, 1975.

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

16. F. Zerla, *Iterative higher derivations in fields of prime characteristic*, Michigan Math. J. **15** (1968), 402–415. MR **39** #185.

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