TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 189, 1974

GALOIS THEORY FOR FIELDS K/k FINITELY GENERATED(1)

BY
NICKOLAS HEEREMA AND JAMES DEVENEY

ABSTRACT. Let K be a field of characteristic $p \neq 0$. A subgroup G of the group $H^t(K)$ of rank t higher derivations ($t \leq \infty$) is Galois if G is the group of all d in $H^t(K)$ having a given subfield h in its field of constants where K is finitely generated over h. We prove: G is Galois if and only if it is the closed group (in the higher derivation topology) generated over K by a finite, abelian, independent normal iterative set F of higher derivations or equivalently, if and only if it is a closed group generated by a normal subset possessing a dual basis. If $t < \infty$ the higher derivation topology is discrete. M. Sweedler has shown that, in this case, h is a Galois subfield if and only if K/h is finite modular and purely inseparable. Also, the characterization of Galois groups for $t < \infty$ is closely related to the Galois theory announced by Gerstenhaber and and Zaromp. In the case $t = \infty$, a subfield h is Galois if and only if K/h is regular. Among the applications made are the following: (1) $\bigcap_n h(K^{p^n})$ is the separable algebraic closure of h in K, and (2) if K/h is algebraically closed, K/h is regular if and only if $K/h(K^{p^n})$ is modular for $n > 0$.

I. **Introduction.** Let K be a field having characteristic $p \neq 0$ and let h be a subfield over which K is finitely generated. This paper is concerned with two related theories. §§I through IV are devoted to a characterization in terms of abelian sets of generators of the group of all infinite higher derivations on K over h. A subfield h of K is the field of constants of a set of infinite higher derivations if and only if K/h is regular. These results are contained in Theorems 4.2, 4.3, and 4.5. §§VI and VII are concerned with the corresponding theory in the case $[K: h] < \infty$. Again, the group of all higher derivations of rank t having a given field of constants is characterized in terms of abelian sets of generators where $t \geq p^{\exp(K/h)-1}$. The finite dimensional theory is similar to, though distinct from, a theory due to Gerstenhaber and Zaromp [10]. Integration of the two theories leads to a number of results connecting modularity, regularity and relative algebraic closure. For example, if K/h is finitely generated then $\bigcap_n h(K^{p^n})$ is the separable algebraic closure of h in K (Theorem 7.2). This extends a result of Dieudonné [11, Proposition 14]. If, in addition, K/h is algebraically closed then K/h is regular if and only if $K/h(K^{p^n})$ is modular for all n (Theorem 7.4).

II. **Definitions and preliminary results.** Throughout this paper, K will be a field of characteristic $p \neq 0$. A rank t higher derivation on K is a sequence d

Presented to the Society, November 25, 1972; received by the editors August 16, 1972.

AMS (MOS) subject classifications (1970). Primary 12F10; Secondary 13B10, 16A72, 16A74.

Key words and phrases. Higher derivation, iterative higher derivation, dual basis, Galois group of higher derivations, independent abelian sets of higher derivations.

(1) This work was supported by NSF GP33027X.

$= \{d_i \mid 0 \le i < t+1\}$ of additive maps of K into K such that $d_r(ab) = \sum \{d_i(a)d_j(b) \mid i+j=r\}$ and d_0 is the identity map. The set $H^t(K)$ of all rank t higher derivations on K is a group with respect to the composition $d \circ e = f$ where $f_j = \sum \{d_m e_n \mid m+n=j\}$ [1, Theorem 1, p. 33]. Note that the first nonzero map (of subscript >0) is a derivation. The field of constants of a subset $G \subset H^t(K)$ is $\{a \in K \mid d_i(a) = 0, i > 0, (d_i) \in G\}$. $H_h^t(K)$ will denote the group of all higher derivations on K whose field of constants contains the subfield h.

From this point until §V we will consider infinite higher derivations ($t = \infty$) only.

The index $i(d)$ of a nonzero higher derivation is either 1 or if d has the property $d_q \ne 0$ and $d_j = 0$ if $q \nmid j$, then $i(d) = q$. We call d in $H^\infty(K)$ iterative of index q, or simply iterative, if $\binom{i}{j} d_{qi} = d_{qj} d_{q(i-j)}$ for all i and $j \le i$, whereas $d_m = 0$ if $q \nmid m$. A complete description of iterative higher derivations has been given by Zerla [3]. If $d \in H^\infty(K)$ has index q, and a is in K, then $ad = e$ where $e_{qi} = a^i d_{qi}$ and $e_j = 0$ if $q \nmid j$. It is clear that ad is a higher derivation. The group generated over k by a subset F of $H^\infty(K)$ is the subgroup generated by $\{ad \mid a \in K, d \in F\}$.

Let $d \in H^\infty(K)$ and let k be the field of constants of d. Then the dimension of d is defined to be the transcendence degree of K over k (i.e., tr.d. (K/k)). A higher derivation is normal if $d_1 \ne 0$. A set $F = \{d^\alpha \mid \alpha \in \Lambda\}$ of higher derivations is abelian if $d_i^\alpha d_j^\beta = d_j^\beta d_i^\alpha$ for all $\alpha, \beta \in \Lambda$, $0 \le i, j < \infty$. A set of nonzero higher derivations on K is independent if the set of first nonzero maps of F with subscript >0 is independent over K. We will need the following.

(2.1) [2, Theorem 1]. Let B be a p-basis for K and let $f\colon Z \times B \to K$ be an arbitrary function. There is a unique $(d_i) \in H^\infty(K)$ such that for each $b \in B$ and $i \in Z$, $d_i(b) = f(i, b)$.

(2.2) [8, p. 436]. Let $(d_i) \in H^\infty(K)$ and $a \in K$. Then $d_{ip}(a^p) = (d_i(a))^p$ and if p and j are relatively prime, then $d_j(a^p) = 0$.

As a simple corollary of (2.2) we have $d_j(a^{p^n}) = 0$ if $p^n \nmid j$. The following theorem can be found in the literature; however a proof is given here for convenience. A field K is a regular extension of a subfield k if K/k is separable and k is algebraically closed in K [5].

(2.3) **Theorem.** *Let k be the field of constants of a set of higher derivations on K. Then K is regular over k.*

Proof. We show first that K is separable over k, i.e., K^p and k are linearly disjoint over k^p. Suppose there exists $\{z_1, \dots, z_n\} \subset k$, independent over k^p and dependent over K^p. Then there exists a relation of minimal length among $\{z_1, \dots, z_n\}$ over K^p, $\sum \{a_i^p z_i \mid 1 \le i \le s\} = 0$ (possibly renumbering) $a_i \in K$, $a_i \ne 0$, $1 \le i \le s$. Without loss of generality we may assume $a_1^p = 1$ and $a_2 \notin k$. Then there exists a map in some higher derivation (d_i) such that $d_j(a_2) \ne 0$. Thus $d_{jp}(\sum \{a_i^p z_i \mid 1 \le i \le s\}) = [d_j(a_2)]^p z_2 + \cdots + [d_j(a_s)]^p z_s = 0$, which yields a nonzero relation of shorter length, a contradiction. Thus K

is separable over k. Suppose $\theta \in K$, and θ is separable algebraic over k. Let $(d_i) \in H_k^\infty(K)$. For a given integer $r > 0$ we choose s so that $r < p^s$. Since θ is separable algebraic over k, $k(\theta) = k(\theta^{p^s})$. Since $p^s > r$, $d_1(\theta^{p^s}) = \cdots = d_r(\theta^{p^s}) = 0$, and hence $k(\theta) = k(\theta^{p^s})$ is contained in the field of constants of $(d_i)_{i=1}^r$. Since r and (d_i) were arbitrary, θ is in k. Hence k is algebraically closed in K.

(2.4) **Theorem** [7, Theorem 15, p. 384]. *Let K be a field obtained by adjoining a finite number of elements to h. If K/h preserves p-independence, then a subset T of K is a separating transcendency basis for K/h if and only if it is a relative p-basis for K/h.*

III. Separating transcendency bases and higher derivations.

(3.1) **Lemma.** *Let $\{k_n \mid 1 \leq n < \infty\}$ and h be subfields of K where $k_j \subseteq k_i$ if $j \geq i$. Then if k_n and h are linearly disjoint for all n, $\bigcap\{k_n \mid 1 \leq n < \infty\}$ and h are linearly disjoint.*

Proof. By [4, Lemma 1.62, p. 57] there exists a unique minimal extension $\bar{k}$ of $\bigcap\{k_n \mid 1 \leq n < \infty\}$ such that $\bar{k}$ and h are linearly disjoint. Since k_n and h are linearly disjoint for all n, $\bar{k} \subseteq k_n$ for all n, and hence $\bar{k} = \bigcap\{k_n \mid 1 \leq n < \infty\}$.

Throughout the rest of this paper h will be a subfield of K such that K is finitely generated over h.

(3.2) **Theorem.** *Let $F = \{d^{(1)}, \ldots, d^{(n)}\}$ be an abelian set of one-dimensional higher derivations in K over h, and let their field of constants be k. Then*

(1) tr.d. $(K/k) \leq n$;

(2) *If F is independent, then* tr.d. $(K/k) = n$.

Proof. (1) We use induction on n. If $n = 1$, the result holds since $d^{(1)}$ is one-dimensional. Let k_{n-1} be the field of constants of $\{d^{(1)}, \ldots, d^{(n-1)}\}$ and k_n the field of constants of $d^{(n)}$. Then tr.d. $(K/k_{n-1}) \leq n - 1$, tr.d. $(K/k_n) = 1$, and $k = k_{n-1} \cap k_n$. All we need to show is tr.d. $(K_{n-1}/k) \leq 1$. It will suffice to show that any subset of k_{n-1} which is algebraically independent over k remains algebraically independent over k_n. We will prove the stronger condition that k_{n-1} and k_n are linearly disjoint. Consider the chain $\{k_{n,i} \mid 1 \leq i < \infty\}$ of subfields of K where $k_{n,i} = \{x \in K \mid d_1^{(n)}(x) = \cdots = d_{p^i-1}^{(n)}(x) = 0\}$. Note that $\bigcap\{k_{n,i} \mid 1 \leq i < \infty\} = k_n$ and $K^{p^{i+1}} \subset k_{n,i}$ by (2.2). We claim $k_{n,i}$ and k_{n-1} are linearly disjoint for all i, $1 \leq i < \infty$. Since $K_{n-1}^{p^{i+1}} \subset k_{n,i}$, we have $k^{p^{i+1}} \subset k_{n,i}$, and hence k_{n-1} is purely inseparable over $k_{n,i} \cap k_{n-1}$. Since $\{d^{(1)}, \ldots, d^{(n)}\}$ is abelian, $\{d^{(1)}|_{k_{n,i}}, \ldots, d^{(n-1)}|_{k_{n,i}}\}$ is a set of higher derivations on $k_{n,i}$, and has field of constants $k_{n,i} \cap k_{n-1}$. Thus by (2.4), $k_{n,i}$ is separable over $k_{n,i} \cap k_{n-1}$, and hence $k_{n,i}$ and k_{n-1} are linearly disjoint [6, Theorem 21, p. 197]. By (3.1), k_n and k_{n-1} are linearly disjoint, and (1) follows.

Now assume $\{d^{(1)}, \ldots, d^{(n)}\}$ is independent. Since we have n independent derivations in K over k and K is separably generated over k, it follows that tr.d. $(K/k) \geq n$ [6, Corollary, p. 179], and hence tr.d. $(K/k) = n$.

(3.3) **Definition.** Let $F = \{d^{(1)}, \ldots, d^{(n)}\}$ be an abelian set of one-dimensional higher derivations in K over h. Let the first nonzero map of $d^{(i)}$ be $d^{(i)}_{r_i}$. Then a subset $S = \{x_1, \ldots, x_n\}$ of K will be called a dual base for $\{d^{(1)}, \ldots, d^{(n)}\}$ if

(1) $d^{(i)}_{r_i}(x_i) = 1,\ 1 \leq i \leq n$,

(2) $d^{(i)}_s(x_j) = 0,\ 1 \leq s < \infty,\ i \neq j$.

In view of (2.4) and (3.2) a dual basis is necessarily a separating transcendency basis for K over the field of constants k of F.

(3.4) **Theorem.** *Let $F = \{d^{(1)}, \ldots, d^{(n)}\}$ be an abelian set of one-dimensional iterative higher derivations on K/h. F is independent if and only if F has a dual basis.*

Proof. Assume F independent. Let k_0 be the field of constants of $\{d^{(1)}, \ldots, d^{(n-1)}\}$. Then, by (3.2), tr.d. $(K/k_0) = n - 1$. If $d^{(n)}_{r_n}|_{k_0} = 0$, then $\{d^{(1)}_{r_1}, \ldots, d^{(n)}_{r_n}\}$ are independent derivations on K/k_0 and it would follow that tr.d. $(K/k_0) \geq n$. Thus $d^{(n)}_{r_n}|_{k_0}$ is a nonzero derivation on k_0 whose pth power is zero and there is an $x_n \in k_0$ such that $d^{(n)}_{r_n}(x_n) = 1$. Let k_1 be the field of constants of $d^{(n)}$ and consider $\bar{F} = \{d^{(2)}|_{k_1}, \ldots, d^{(n)}|_{k_1}\}$. Since F is abelian $\bar{F}$ is an abelian set of iterative higher derivations on k_1. If $\sum \{a_i d^{(i)}_{r_i}|_{k_1} | i = 1, \ldots, n-1; a_i \in k_1\} = 0$ then $\sum \{a_i d^{(i)}_{r_i}|_{k_1(x_n)} | i = 1, \ldots, n-1\} = 0$ and hence $\sum \{a_i d^{(i)}_{r_i} \mid i = 1, \ldots, n - 1\} = 0$ since K is separable algebraic over $k_1(x_n)$. Thus $\bar{F}$ is independent and by the induction hypothesis, has a dual basis $x_1, \ldots, x_{n-1}$. The set $\{x_1, \ldots, x_n\}$ is then a dual basis for F.

IV. The Galois correspondence.

(4.1) **Definition.** Let G be a subgroup of $H^\infty(K)$. The sequence $\{G_j\}$ defined by $G_1 = G$ and. $G_j = \{(d_i) \in G \mid d_1 = d_2 = \cdots = d_{j-1} = 0\}$ for $2 \leq j < \infty$ is called the higher derivation series of G.

It is easily verified that each term in the higher derivation series is a normal subgroup of G and $\bigcap\{G_j \mid j > 0\} = \{e\}$ where e is the identity of G. Using the higher derivation series as a basis of open neighborhoods at e we make G a topological group. Let H^c denote the closure of a subgroup H of G. Given $d \in H^\infty(K)$ of index q, $v(d) = e = \{e_i \mid 0 \leq i < \infty\}$ where $e_{(q+1)i} = d_{qi}$ and $e_j = 0$ if $(q + 1) \nmid j$, it is clear that $v(d)$ is a higher derivation. The v-closure $\bar{v}(F)$ of a set F in $H^\infty(K)$ is $\{v^i(d) \mid d \in F, i \geq 0\}$ where $v^0(d) = d$. We recall the basic assumption that K is a finitely generated extension of the subfield h. A subgroup of $H^\infty_h(K)$ with field of constants k will be called Galois if G is the group of all higher derivations which contain k in their field of constants.

(4.2) **Theorem.** *A subgroup G of $H^\infty_h(K)$ is Galois if and only if G is the closure, $(\bar{v}(F))^c$, of the subgroup generated over K by $\bar{v}(F)$, where F is a finite abelian normal independent set of one-dimensional iterative higher derivations in $H^\infty_h(K)$. If $G = (\bar{v}(F))^c$ has field of constants k, then* tr.d. $(K/k) = |F|$.

Proof. Suppose G is Galois with field of constants k. Let $S = \{x_1, \ldots, x_n\}$ be a separating transcendency basis for K over k, and let P be a p-basis for k. Since

K is a separable extension of k, $P \cup S$ is a p-basis for K. Using (2.1) we describe a set $F = \{d^{(1)}, \ldots, d^{(n)}\}$ of iterative higher derivations [3, Theorem 2] by the conditions

(i) $d_j^{(i)}(x) = 0$ if $x \in S$ and $j > 1$ or $x \in P$ and $j > 0$,

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

Elementary calculations show F to be abelian. Each $d^{(i)}$ is one-dimensional since $k(x_1, \ldots, \hat{x}_i, \ldots, x_n)$ is contained in its field of constants. Thus F is a finite abelian normal independent set of one-dimensional iterative higher derivations in G. We claim that $(\bar{v}(F))^c = G$.

Let (d_i) be in G and have first nonzero map d_t with $d_t(x_i) = a_i$, $i = 1, \ldots, n$. The first nonzero map of $g = \prod \{a_i v^{t-1}(d^{(i)}) \mid i = 1, \ldots, n\}$ is g_t and $g_t = d_t$ since d_t being a derivation is completely determined by $\{d_t(x_i) \mid i = 1, \ldots, n\}$ and $g_t(x_i) = d_t(x_i)$. Thus $g^{-1} \circ d$ is in G_{t+1}. It follows by iteration of this process that, if d is in G and r is any integer, there is a $g \in (\bar{v}(F))$ such that $g_i = d_i$ for $i < r$ or, equivalently, $(\bar{v}(F)) = G \bmod G_r$. Hence $(\bar{v}(F))^c = G$.

Conversely, suppose $G = (\bar{v}(F))^c$ for F as in the theorem. Let $\{x_1, \ldots, x_n\}$ be a dual basis for F and let k be the field of constants of F. Since $\{x_1, \ldots, x_n\}$ is a separating transcendency basis for K/k the above approximation process can be applied to show that $(\bar{v}(F))^c = H_k^\infty(K)$.

(4.3) **Theorem.** *Let $K = h(x_1, \ldots, x_n)$. There exists a unique minimal extension k of h in K such that K/k is regular. k is a subfield of each field k_1, $K \supseteq k_1 \supseteq h$, K/k_1 regular and is the field of constants of $H_h^\infty(K)$.*

Proof. It suffices to show for k, $K \supseteq k \supseteq h$, where K is regular over k, that k is the field of constants of a set of higher derivations in K over h. Let $\{x_1, \ldots, x_n\}$ be a separating transcendency basis for K over k, and let F be as constructed in (4.2). Let k_1 be the field of constants of F. Then $k_1 \supseteq k$. But by (3.2), tr.d. $(K/k_1) = n$, and since k is algebraically closed in K, $k_1 = k$.

Thus if we set $R = \{G \subseteq H^\infty(K) \mid G$ is the closed subgroup generated over K by $\bar{v}(F)$ where F is as in (4.2)$\}$ and $S = \{k \mid K$ is regular and finitely generated over $k\}$, then the maps $g\colon R \to S$, given by $g(G) =$ field of constants of G, and $f\colon S \to R$, given by $f(k) = H_k^\infty(K)$, are inverse bijections.

(4.4) **Definition.** A subfield k of K over which K is finitely generated will be called Galois if K is regular over k. A subgroup G of $H^\infty(K)$ with field of constants k will be called Galois if K is finitely generated over k and $G = H_k^\infty(K)$.

Let G be a Galois subgroup of $H^\infty(K)$. Then a set F of generators for G as in Theorem (4.2) will be called a standard generating set.

(4.5) **Theorem.** *Let h be a Galois subfield of K and let k be an intermediate field. The following are equivalent.*

(1) *k is a Galois subfield of K.*

(2) *There exists $\{d^{(1)}, \ldots, d^{(n)}\}$ a standard set of generators for $H_h^\infty(K)$ such that*

$\{d^{(1)}, \ldots, d^{(t)}\}$, $t \leq n$, has field of constants k. The set $\{d^{(1)}, \ldots, d^{(t)}\}$ is a standard set of generators for $H_k^\infty(K)$.

(3) *k is algebraically closed in K and every d in $H_h^\infty(k)$ can be extended to K.*

Proof. Assume (1). Note that k is regular over h. Let S be a p-basis for h; let $T_1 = \{x_1, \ldots, x_t\}$ be a separating transcendency basis for K over k, and let $T_2 = \{x_{t+1}, \ldots, x_n\}$ be a separating transcendency basis for k over h. Then $T_1 \cup T_2 \cup S$ is a p-basis for K and $T_1 \cup T_2$ is a separating transcendency basis for K over h. Let $\{d^{(1)}, \ldots, d^{(n)}\}$ be as in (4.2). Then $\{d^{(1)}, \ldots, d^{(n)}\}$ is a standard set of generators for $H_h^\infty(K)$ and $\{d^{(1)}, \ldots, d^{(t)}\}$ is a standard set of generators for $H_k^\infty(K)$. Note that $\{d^{(t+1)}|_k, \ldots, d^{(n)}|_k\}$ is a standard set of generators for $H_h^\infty(k)$.

Obviously (2) implies (1) and (2) implies (3). Assume (3). It suffices to show K is separable over k. Let $\{x_1, \ldots, x_s\}$ be a separating transcendency basis for k over h, and let $\{d^{(1)}, \ldots, d^{(s)}\}$ be a standard generating set for $H_h^\infty(k)$. Then $\{d_1^{(1)}, \ldots, d_1^{(s)}\}$ is a basis for $\mathrm{Der}_h(k)$, the space of all derivations on k over h. Since these derivations can be extended to K it follows that every derivation on k extends to K. Thus by [6, Theorem 18, p. 184], K is separable over k, and hence regular over k.

Dropping the algebraically closed assumptions of Theorem (4.5) we have the following.

(4.6) **Theorem.** *Let K/h be finitely generated and separable and let k be an intermediate field. Then K/k is separable if and only if every d in $H_h^\infty(k)$ extends to $H_k^\infty(K)$.*

Proof. Assume k/h separable. Let S be a p-basis for h, T_1 a separating transcendency basis for k/h and T_2 a separating transcendency basis for K/k. Theorem (2.2), the fact that $T_1 \cup S$ is a p-basis for k, and the fact that $T_1 \cup T_2 \cup S$ is a p-basis for K/h together imply that every element of $H_h^\infty(k)$ extends to $H_h^\infty(K)$. To prove the converse one notes that every derivation on k over h is the first nonzero map d_1 of a higher derivation on k over h. This follows from the fact that a p-basis for k over h is a separating transcendency basis for k over h, a p-basis for h extends to a p-basis for k and (3.1). Thus every d in $\mathrm{Der}_h(k)$ extends to K. As in the proof of (4.5) it follows that K/k is separable.

V. Higher derivations of finite rank; preliminaries. The following result on derivations will be used. $K \supset k$ will always be fields of characteristic $p \neq 0$.

(5.1) **Theorem** [10, p. 1011]. *Let $\rho_1, \ldots, \rho_n$ be commuting derivations in K with field of constants k. If they are linearly independent over k, then*

(1) *they are independent over K;*

(2) $[K\colon k] \geq p^n$;

(3) *equality holds if and only if the k-space V_0 spanned by $\rho_1, \ldots, \rho_n$ is closed under the formation of pth powers.*

(5.2) **Proposition.** *Let $F = \{\rho_1, \dots, \rho_n\}$ be derivations on K. The following are equivalent.*

(a) *F is abelian, independent (over K), and has the property $\rho_i^p = 0$, $1 \leq i \leq n$.*

(b) *$K = k(x_1, \dots, x_n)$ where k is the field of constants of F and $\rho_i(x_j) = \delta_{i,j}$, $1 \leq i, j \leq n$. The set $\{x_1, \dots, x_n\}$ is a p-basis for K/k.*

Proof. Assume (a). We use induction on n. If $n = 1$, $[K\colon k] = p$ by (5.1). Since $\rho_1^p = 0$, there is an x_1 in K for which $\rho_1(x_1) = 1$ [3, Lemma 4, p. 408]. Assume the result for $n - 1$, $n > 1$. From (5.1), $[K\colon k] = p^n$. Let k_1 be the field of constants of $\{\rho_1, \dots, \rho_{n-1}\}$ and let $\{y_1, \dots, y_{n-1}\}$ be a p-basis for K/k_1 for which $\rho_i(y_j) = \delta_{i,j}$, $0 \leq i, j \leq n - 1$. Since $\{\rho_1, \dots, \rho_n\}$ is abelian $\rho_n(k_1) \subset k_1$ and since $[K\colon k_1] < p^n$, $\rho_n|_{k_1} \neq 0$ by (5.1). Hence there is an element x_n in k_1 such that $\rho_n(x_n) = 1$. Since $x_n \in k_1$, $\rho_j(x_n) = 0$, $j < n$. Also, $k_1 = k(x_n)$ by (5.1). By commutativity of the ρ_i, $\rho_n(y_j)$ is in k_1, for $j = 1, \dots, n - 1$. Thus, $\rho_n(y_j) = \sum \{a_i x_n^i \mid i = 1, \dots, p - 2, a_i \in k\}$. Note that since $\rho_n^p = 0$, $a_{p-1} = 0$. Then $z = \sum \{a_{i-1} x_n^i / i \mid i = 1, \dots, p - 1\}$ has the property $\rho_n(z) = \rho_n(y_j)$. Choose $x_j = y_j - z$. Since $z \in k_1$, we have $\rho_i(x_j) = \delta_{i,j}$, $1 \leq i, j \leq n$.

Assume (b). Clearly F is independent. The field of constants k_i of ρ_i is $k(x_1, \dots, \hat{x}_i, \dots, x_n)$. Thus $y \in K$ is a polynomial in x_i over k_i of degree $< p$ and $\rho_i^p = 0$. One easily verifies that $\rho_i \rho_j = \rho_j \rho_i$. The set $\{x_1, \dots, x_n\}$ being p-independent [6, Corollary 4, p. 183] is a p-basis for K/k.

The abelian condition in part (a) of (5.2) is essential. A finite independent set of derivations, $\{\rho_1, \dots, \rho_n\}$, on K such that $\rho_i^p = 0$, $1 \leq i \leq n$, need not be abelian. For given distinct subfields k_1, k_2 of K such that $[K\colon k_i] = p$ and K/k_i is purely inseparable, there are independent derivations ρ_1, ρ_2 for which $\rho_i^p = 0$ and which have k_1 and k_2 as respective field of constants. If $\rho_1 \rho_2 = \rho_2 \rho_1$ it would follow that $[K\colon k_1 \cap k_2] = p^2$. A counterexample to this conclusion is easily constructed.

(5.3) **Definition.** A relative p-base for K over k as in (2.4) will be called a dual p-base with respect to $\{\rho_1, \dots, \rho_n\}$.

Using (5.2) we have the following. A finite-dimensional subspace of the K-space Der(K) of derivations on K is Galois if and only if it is generated over K by a set $\{\rho_1, \dots, \rho_n\}$ of commuting independent derivations such that $\rho_i^p = 0$, $1 \leq i \leq n$. This is precisely the type of charaterization which will be established for higher derivations.

Let $d = (d_i)$ be a higher derivation of finite rank t. For $1 \leq s \leq t$, the s-section of d is the higher derivation $e = (d_i \mid i = 0, \dots, s)$. The s-section of a set of higher derivations is the set of s-sections. For $d \neq 0$ in $H^t(K)$, with first nonzero map d_r we define $p(d) = \min\{s \mid p^s \cdot r > t\}$.

Observation. *For $d \in H^t(K)$, $p(d)$ is the exponent of K over the field of constants of d.*

Proof. Let $p(d) = s$. If $d_r(x) \neq 0$ but $d_i = 0$ for $0 < i < r$, then $d_{p^{(s-1)}r}(x^{p^{(s-1)}}) = (d_r(x))^{p^{(s-1)}} \neq 0$. However $d_j(x^{p^s}) = 0, j > 0$, by the remark following (2.2).

We call $d \in H^t(K)$ iterative if d is the tth section of an iterative higher derivation in $H^\infty(K)$. A finite rank iterative d is normal if for some $j > 0$, $i(d)$ is $[t/p^j] + 1$, where $[t/p^j]$ is the greatest integer less than or equal to t/p^j. A normal higher derivation d has minimal index for a given $p(d)$. A finite set F of nonzero higher derivations on K is said to be independent if the set of first nonzero maps of F (of subscript ≥ 1) is independent over K.

In the next proof we will use the fact that if d is iterative and has index q then the restriction of d to the field of constants of its first nonzero map is an iterative higher derivation having index pq (assuming $pq \leq$ rank d).

VI. The finite rank Galois correspondence.

(6.1) **Theorem.** *Let $F = \{d^{(1)}, \ldots, d^{(n)}\}$ be an abelian set of independent iterative members of $H^t(K)$ and let k be the field of constants of F. Then $[K\colon k] = p^{p(d^{(1)})+\cdots+p(d^{(n)})}$.*

Proof is by induction on $p(F) = \max\{p(d^{(i)}) \mid d^{(i)} \in F\}$. If $p(F) = 1$, each $d^{(i)}$ has but one nonzero map with positive subscript and (5.1) applies A counterexample to this conclusion is easily constructed. that if $d = (d_i)$ is iterative of index q then $(d_{qp^j})^p = 0$.)

Hence assume the result holds for $p(F) = j - 1$ or less, and consider the case $p(F) = j$. Let $\{x_1, \ldots, x_n\}$ be a dual basis with respect to the set of first nonzero maps of F, and let k_1 be their field of constants. Then $[K\colon k_1] = p^n$ by (5.1).

By the abelian condition $d_j^{(i)}(k_1) \subset k_1$ for all i and j. Hence $F|_k$ is an abelian set of iterative higher derivations. Also, if $d_{t_i}^{(i)}$ is the first nonzero map of $d^{(i)}$ then, if $pt_i \leq t$ we have, by (2.2), $d_{pt_i}^{(i)}(x_i^p) = (d_{t_i}^{(i)}(x))^p$. Thus $d_{pt_i}^{(i)}|_{k_1}$ is the first nonzero map of $d^{(i)}|_{k_1}$. Let $\bar{F} = \{d^{(b+1)}|_{k_1}, \ldots d^{(n)}|_{k_1}\}$ be the nonzero elements of $F|_{k_1}$. By the above remarks $d_{pt_j}^{(j)}(x_i^p) = \delta_{i,j}$ for $b < i, j \leq n$. It follows that $\bar{F}$ is independent over k_1 and $\{x_{b+1}^p, \ldots, x_n^p\}$ is a p-basis for k_1/k_2, k_2 being the field of constants of the first nonzero maps of $\bar{F}$. By induction,

$$\begin{aligned}[k_1 : k] &= p^{p(d^{(b+1)})-1+\cdots+p(d^{(n)})-1} \\ &= p^{p(d^{(1)})-1+\cdots+p(d^{(n)})-1}\end{aligned}$$

and

$$[K\colon k] = [K\colon k_1][k_1 ; k] = p^{p(d^{(1)})+\cdots+p(d^{(n)})}.$$

(6.2) **Corollary.** *If $d = (d_i)$ is a nonzero finite iterative higher derivation in K with field of constants k, then $[K\colon k] = p^{p(d)}$. If y is any element of K such that $d_{i(d)}(y) \neq 0$, then $K = k(y)$.*

Proof.

$$d_{i(d)p^{p(d)-1}}(y^{p^{p(d)-1}}) = (d_{i(d)}(y))^{p^{p(d)-1}} \neq 0,$$

hence $[k(y): k] \geq p^{p(d)}$ and thus $K = k(y)$.

Let $F = \{d^{(1)}, \ldots, d^{(n)}\}$ be a set of rank t higher derivations on K. $\{x_1, \ldots, x_n\}$ is a dual basis for F if both of the following are true.

(1) $K = k(x_1, \ldots, x_n)$, k the field of constants of F.

(2) $d_{r_i}^{(i)}(x_i) = 1$, where $d_{r_i}^{(i)}$ is the first nonzero map of $d^{(i)}$ and all other maps in F with nonzero subscript take x_i into zero.

(6.3) **Theorem.** *Let $F = \{d^{(1)}, \ldots, d^{(n)}\}$ be a subset of $H^t(K)$. The following are equivalent.*

(a) *F is an abelian set of independent iterative higher derivations.*

(b) *F has a dual basis $\{x_1, \ldots, x_n\}$.*

If $\{x_1, \ldots, x_n\}$ is a dual basis, then $K = k(x_1) \otimes_k \cdots \otimes_k k(x_n)$, $k_i = k(x_1, \ldots, \hat{x}_i, \ldots, x_n)$ is the field of constants of $d^{(i)}$. Also, x_i is purely inseparable over k of exponent $p(d^{(i)})$.

Proof. Assume (a). We use induction on n. If $n = 1$, the result follows from [3, Theorem 2]. Hence assume the result holds for $n - 1$, and let k_1 be the field of constants of $d^{(1)}$. Then $\bar{F} = \{d^{(2)}|_{k_1}, \ldots, d^{(n)}|_{k_1}\}$ is an abelian set of iterative higher derivations on k_1 with field of constants k. Let $\{y_1, \ldots, y_n\}$ be a dual basis with respect to the first nonzero maps, $\{d_{r_i}^{(i)}\}$, of F. Then $K = k_1(y_1)$. If $a_2 d_{r_2}^{(2)}|_{k_1} + \cdots + a_n d_{r_n}^{(n)}|_{k_1} = 0$, then since $d_{r_i}^{(i)}(y_1) = 0$, $i \geq 2$, we have $a_2 d_{r_2}^{(2)} + \cdots + a_n d_{r_n}^{(n)} = 0$. Thus $\bar{F}$ is also independent, and in particular $d_{r_j}^{(j)}|_{k_1} \neq 0$, $2 \leq j \leq n$. Let $\{x_2, \ldots, x_n\}$ be a dual basis for $\bar{F}$. Note that $d_j^{(1)}(x_i) = 0$, $1 \leq j \leq t$, $2 \leq i \leq n$. Now let k_2 be the field of constants of $\{d^{(2)}, \ldots, d^{(n)}\}$. Then as above $d^{(1)}|_{k_2}$ is nonzero with field of constants k and $d_{r_1}^{(1)}|_{k_2} \neq 0$. Hence there exists x_1 in k_2 such that $d_{r_1}^{(1)}(x_1) = 1$ and $d_j^{(1)}(x_1) = 0$, $j \neq r_1$. Then $\{x_1, \ldots, x_n\}$ is a dual basis for F.

Assume (b). Clearly F is independent. By [3, Lemma 5, p. 410] each higher derivation of F is iterative. One easily verifies $d_r^{(i)} d_s^{(j)} = d_s^{(j)} d_r^{(i)}$.

Noting that $d_i^{(j)}(k(x_j)) \subset k(x_j)$, $i \geq 0$, and $d_{r_j}^{(j)}(x_j) = 1$ we conclude that $d^{(j)}|_{k(x_j)}$ is an (iterative) higher derivation and $p(d^{(j)}) = p(d^{(j)}|_{k(x_j)})$. Thus $[k(x_j): k] = p^{p(d^{(j)})}$. Since $K = k(x_1, \ldots, x_n)$ and $[K: k] = p^{p(d^{(1)}) + \cdots + p(d^{(n)})}$ by Theorem 6.1, it follows that $K = k(x_1) \otimes_k \cdots \otimes_k k(x_n)$. Also $k(x_1, \ldots, \hat{x}_j, \ldots, x_n) \subseteq k_j$, the constant field of $d^{(j)}$, and since $[K: k(x_1, \ldots, \hat{x}_j, \ldots, x_n)] = [K: k_j]$ we have $k_j = k(x_1, \ldots, \hat{x}_j, \ldots, x_n)$.

It is shown in Jacobson [6, p. 195] that if $K = k(x_1) \otimes_k \cdots \otimes_k k(x_n)$ and x_i is purely inseparable over k then $\{x_1, \ldots, x_n\}$ is a dual basis.

If d has index q, and a is in K, then $ad = e$ where $e_{qi} = a^i d_{qi}$ and $e_j = 0$ if $q \nmid j$. It is clear that ad is a higher derivation. The group generated over K by a subset F of $H^t(K)$ is the subgroup generated by $\{ad \mid a \in k, d \in F\}$.

Given $d \in H^t(K)$ of index q, $v(d) = e \in H^t(K)$ where $e_{(q+1)i} = d_{qi}$ for $(q+1)i \leq t$ and $e_j = 0$ if $(q+1) \nmid j, j \leq t$. Clearly $v(d)$ is a higher derivation. The v closure $\bar{v}(F)$ of a set F in $H^t(K)$ is $F \cup \{v^i(d) \mid d \in F, i \geq 1\}$. A subgroup G of $H^t(K)$ with field of constants k, $[K: k] < \infty$, will be called Galois if G is the group of all higher derivations in $H^t(K)$ which contain k in their fields of constants.

(6.4) **Theorem.** *A subgroup G of $H^t(K)$ is Galois if and only if G is generated over K by $\bar{v}(F)$ where F is a finite abelian normal independent iterative subset of $H^t(K)$. If G is Galois with field of constants k, and is generated by $\bar{v}(F)$ where $F = \{d^{(1)}, \ldots, d^{(n)}\}$ as above, if $\{x_1, \ldots, x_n\}$ is a dual basis for F, then $K = k(x_1) \otimes_k \cdots \otimes_k k(x_n)$, x_i is purely inseparable of degree $p^{p(d^{(i)})}$ over k and hence $[K: k] = p^{p(d^{(1)}) + \cdots + p(d^{(n)})}$.*

Proof. Suppose G is Galois with field of constants k. Sweedler has shown [9] that $K = k(x_1) \otimes_k \cdots \otimes_k k(x_n)$, the x_i purely inseparable over k. Let $F = \{d^{(1)}, \ldots, d^{(n)}\}$ be a set of higher derivations having $\{x_1, \ldots, x_n\}$ as a dual basis. By the remark following the definition of normality and by (6.3) we can assume that F is an abelian iterative independent normal subset of G. Let $(\bar{v}(F))$ be the subgroup of G generated over K by $\bar{v}(F)$. We claim $(\bar{v}(F)) = G$.

Let d be in G. We will prove $d \in (\bar{v}(F))$ by descending induction on the subscript of the first nonzero map of $d = (d_i)$. Suppose d to be in $G_r = \{d \in G \mid d_1 = \cdots = d_{r-1} = 0\}$. Then d_r is a derivation and is completely determined by $d_r(x_j) = \alpha_j$, $j = 1, \ldots, n$. By the observation following the definition of $p(d)$, x_j has exponent $m_j = p(d^{(j)})$ over k_j and hence over k in view of Theorem 6.3. If $\alpha_j \neq 0$ then $r \geq i(d^{(j)})$ since $d^{(j)}$ is normal. Otherwise we would have $rp^{m_j} \leq t$ and $d_{rp}m_j(x_j^{p^{m_j}}) = d_r(x_j)^{p^{m_j}} \neq 0$ whereas $x_j^{p^{m_j}}$ is in k. Let $e = \prod \{v^{r-i(d^{(j)})}(\alpha_j d^{(j)}) \mid \alpha_j \neq 0\}$. The first nonzero map of e is e_r and $e_r = d_r$. Thus, $d \circ e^{-1}$ is in G_{r+1}. If $r = t$ we have $G_t \subset (\bar{v}(F))$ and, for $r < t$, $G_r \subset G_{r+1}(\bar{v}(F))$. It follows that $G = (\bar{v}(F))$.

Conversely, suppose G is generated by $\bar{v}(F)$ where F is a finite abelian normal independent iterative subset of $H^t(K)$. Then by (6.3), if $\{x_1, \ldots, x_n\}$ is a dual basis for F, $K = k(x_1) \otimes_k \cdots \otimes_k k(x_n)$, and since F is normal, F must be precisely as above; hence G is Galois. The remaining assertions of the theorem are contained in (6.3).

Although the results of Theorem (6.4) are similar to those of [10, Theorem 4, p. 1013], Theorem (6.4) does not follow from Theorem 4 since one cannot determine a priori that F is a standard set of generations.

Suppose $p^n \leq t < p^{n+1}$. If we set $H = \{G \subseteq H^t(K) \mid G$ is generated over K by $\bar{v}(F)$ where F is as in (6.4)$\}$ and $\mathcal{K} = \{k \mid [K: k] < \infty, K^{p^{n+1}} \subseteq k$ and K/k is modular$\}$, then the maps $g: \mathcal{H} \to \mathcal{K}$ given by $g(G) =$ field of constants of G and $f: \mathcal{K} \to \mathcal{H}$ given by $f(k) = H_k^t(K)$ are inverse bijections.

Using (6.3) we can state Theorem (6.4) in part as follows.

(6.5) **Theorem.** *A subgroup of G of $H^t(K)$ is Galois if and only if G is generated over K by $\bar{v}(F)$ where F is a finite normal subset of G possessing a dual basis.*

VII. Regularity vs. modularity.

(7.1) **Theorem.** *Let K/h be finitely generated. If K/h is separable then $K/h(K^{p^n})$ is modular for all $n \geq 0$. If K/h is regular, $h = \bigcap\{h(K^{p^n}) \mid n \geq 1\}$.*

Proof. Let $\{x_1, \ldots, x_s\}$ be a separating transcendency basis for K/h. Let $\{d^{(1)}, \ldots, d^{(s)}\}$ be the standard generating set of $H_h^\infty(K)$ having $\{x_1, \ldots, x_s\}$ as dual basis. If $F = \{\bar{d}^{(i)} \mid 1 \leq i \leq s\}$ where $\bar{d}^{(i)} = \{d_j^{(i)} \mid 0 \leq j \leq p^n\}$ and $k_n = \{x \in K \mid \bar{d}_j^{(i)}(x) = 0, 1 \leq i \leq s, 1 \leq j \leq p^n\}$ then K is modular over k_n [9, Theorem 1, p. 403]. By (2.2), $h(K^{p^{n+1}}) \subset k_n$. By choice of $\{x_1, \ldots, x_s\}$, $k(K^{p^{n+1}})(x_1, \ldots, x_s) = K$. Thus $[K: k(K^{p^{n+1}})] \leq p^{(n+1)s}$. By (6.1), $[K: k_n] = p^{(n+1)s}$. Thus $k_n = k(K^{p^{n+1}})$.

If K/k is regular, k is the field of constants of $H_k^\infty(K)$. Hence $k = \bigcap\{k(K^{p^n}) \mid n \geq 1\}$.

(7.2) **Theorem.** *If K/h is finitely generated then $\bigcap\{h(K^{p^n}) \mid n \geq 1\}$ is the separable algebraic closure of h in K.*

Proof. Let $K = h(x_1, \ldots, x_n)$. If $x_1, \ldots, x_r$ is a transcendency basis for K/h then for some $n \geq 0$, $x_{r+1}^{p^n}, \ldots, x_n^{p^n}$ are separable algebraic over $h(x_1, \ldots, x_r)$. It follows that $h(K^{p^n})/h$ is separable. If x in K is separable algebraic over h then x is in $h(K^{p^n})$ for all n since x is both separable and purely inseparable over $h(K^{p^n})$. Thus h_s, the separable algebraic closure of h in K, is in $\bigcap\{h(K^{p^n}) \mid n \geq 1\}$. Let $\bar{h}$ be the algebraic closure of h in K. As above $\bar{h}(K^{p^m})/\bar{h}$ is separable for some m. Hence $\bar{h}(K^{p^m})/\bar{h}$ is regular and, by (7.1), $\bar{h} = \bigcap\{\bar{h}((\bar{h}(K^{p^m}))^{p^n}) \mid n \geq 1\}$ or $\bar{h} = \bigcap\{\bar{h}(K^{p^n}) \mid n \geq 1\}$. Thus $\bigcap\{h(K^{p^n}) \mid n \geq 1\} \subseteq \bar{h}$. Finally, since for some n, $h(K^{p^n})/h$ is separable, $\bigcap\{h(K^{p^n}) \mid n \geq 1\}/h$ is separable algebraic. Hence $h_s = \bigcap\{h(K^{p^n}) \mid n \geq 1\}$.

(7.3) **Corollary.** *Let K/h be finitely generated. If K/h is separable then $\bigcap\{h(K^{p^n}) \mid n \geq 1\}$ is the algebraic closure of h in K.*

(7.4) **Theorem.** *Let K/h be finitely generated. If h is algebraically closed in K then K/h is regular if and only if $K/h(K^{p^n})$ is modular for all $n \geq 0$.*

Proof. Assume

$K/h(K^{p^n})$ modular for $n \geq 0$. Then K^p and $h(K^{p^n})$ are linearly disjoint for all n and hence, by (3.1), K^p and $\bigcap\{h(K^{p^n}) \mid n \geq 1\}$ are linearly disjoint. Since K/h is algebraically closed $h^p = h \cap K^p$ and $h = \bigcap\{h(K^{p^n}) \mid n \geq 1\}$ by (7.2). Thus K is separable over h. The converse is part of Theorem (7.1).

In §IV we established that for any subfield h for which K/h is finitely generated there is a unique minimal intermediate field h^* such that K/h^* is regular. The fact that h^* need not be the algebraic closure of h in K is illustrated by the following example.

(7.5) **Example** [7, §10, p. 391]. Let P be a perfect field and let z, y, u be algebraically independent over P. If $h = P(y^p, u^p)$ and $K = P(z, y^p, y + zu)$ then K/h is algebraically closed but K is not separable over h. Thus $h^* = K$.

Conjecture. tr.d. $(h^*/h) \leq 1$ *in general.*

From the same reference we have the following.

(7.6) **Corollary.** *Assume K/h finitely generated. If* tr.d. $(h/P) \leq 1$ *where P is the maximal perfect subfield of h, then the regular closure h^* of h in K is the algebraic closure of h in K.*

Proof. [7, Theorem 9(b), p. 378] and [7, Theorem 15, p. 384].

References

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

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

3. F. Zerla, *Iterative higher derivations in fields of prime characteristic*, Michigan Math. J. **15** (1968), 407–415. MR **39** #185.

4. J. 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.

5. A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ., vol. 29, Amer. Math. Soc., Providence, R.I., 1946. MR **9**, 303.

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

7. S. Mac Lane, *Modular fields*. I. *Separating transcendency bases*, Duke Math. J. **5** (1939), 372–393.

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

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

10. 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.

11. J. Dieudonné, *Sur les extensions transcendantes separables*, Summa Brasil. Math. **2** (1947), no. 1, 1–20. MR **10**, 5.

Department of Mathematics, Florida State University, Tallahassee, Florida 32306