A GALOIS THEORY FOR A CLASS OF PURELY INSEPARABLE EXPONENT TWO FIELD EXTENSIONS

BY R. L. DAVIS

Communicated by Murray Gerstenhaber, April 21, 1969

Introduction. A Galois theory for purely inseparable exponent one field extensions was developed by N. Jacobson [2] in 1944. He accomplished this by characterizing the finite dimensional subalgebras $\mathrm{Der}_k(K)$ of $\mathrm{Der}(K)$, where $\mathrm{Der}(K)$ is the Lie algebra of derivations on K, k is a subfield of K, and $\mathrm{Der}_k(K)$ is the subalgebra of $\mathrm{Der}(K)$ consisting of those derivations that are zero on k. It was conjectured that higher derivations might provide an extension of the theory to field extensions of higher exponent. The purpose of this note is to describe such an extension. The author believes that the exponent two case is of sufficient interest to justify its presentation before the general exponent N case is developed. The problem of extending the theory to exponent N appears to be nontrivial; the author's efforts in this area thus far have been unsuccessful.

Let K be a field of characteristic $p \neq 0$ or 2 and let $H^p(K)$ denote the set of all higher derivations of K having length p; that is, sequences of additive mappings (d_i) of K into itself such that for all x and y in K and $n=0, 1, \cdots, p$: $d_n(xy) = \sum\{d_i(x)d_j(y) \mid i+j=n\}$ and d_0 is the identity mapping on K. $H_p(K)$ is a group under $(d_i)(e_i) = (f_i)$ where $f_i = \sum\{d_j e_n \mid j+n=i\}$. $H_p(K)$ is also closed under a type of scalar multiplication by elements of K; this is defined by $a(d_i) = (a^i d_i)$ where $a^i d_i = (a^i)_L d_i$ and $a \in K$. If k is a subfield of K, $H_k^p(K)$ will denote the subset of those (d_i) in $H^p(K)$ with the property that d_i restricted to k is zero for $i=1, 2, \cdots, p$, $H_k^p(K)$ is a subgroup of $H^p(K)$ and is closed under scalar multiplication by elements of K. In the higher derivation setting, Jacobson's result was the characterization of the finitely K-generated subgroups $H_k^1(K)$ of $H^1(K)$.

In this note we give an intrinsic characterization of those subgroups $H_k^p(K)$ of $H_k^p(K)$ having the property that they are finitely K-generated; that is, there is a finite subset S of $H_k^p(K)$ such that the minimal subgroup of $H^p(K)$ containing S and closed under scalar multiplication is $H_k^p(K)$. The result can then be used to provide a Galois type correspondence between these subgroups of $H^p(K)$ and subfields k of K satisfying: $[K:k] < \infty$, exponent of $K/k = 2$, and K is the tensor product of simple extensions of k. Only sketches of proofs are given.

1. **Subgroups of $H^p(K)$ closed under scalar multiplication.** In this section we consider those subgroups G of $H^p(K)$ which have the property that $(a^i d_i) \in G$ whenever $(d_i) \in G$ and $a \in K$. Also the groups considered are required to contain elements (d_i) with $d_1 \neq 0$.

LEMMA 1. *Let $\{Z_i\}$ denote the upper central series for G. There is a natural injection of the group Z_i/Z_{i-1} into* Der(K), *the algebra of derivations on K, for each i.*

PROOF. $Z_i = \{(d_j) \in G \mid d_1 = d_2 = \cdots = d_{p-i} = 0\}$. The mapping from Z_i/Z_{i-1} into Der(K) is $(d_j)Z_{i-1} \to d_{p-i+1}$.

We identify Z_i/Z_{i-1} with its image in Der(K) under the mapping given above.

LEMMA 2. *If $\{Z_i\}$ is the upper central series for G, then $Z_p/Z_{p-1} \subseteq Z_{p-1}/Z_{p-2} \subseteq \cdots \subseteq Z_1/Z_0$.*

PROOF. The assertion follows from two commutator relations for derivations. Let d be a nonzero derivation and let $a \in K$ such that $d(a) \neq 0$. Then $d = [d, \frac{1}{2}ad(a)^{-1}d] - [\frac{1}{2}ad, d(a)^{-1}d]$. If f is a derivation such that $f(b) = -1/ib^{i-1}$ where $2 \leqq i \leqq p-1$, then $[b^i d, f] + [b^i f, d] = d + cf$, $c \in K$.

LEMMA 3. *Let the upper central series for G satisfy $Z_1/Z_0 = Z_{p-1}/Z_{p-2}$, then $(d_i) \in G$ and $1 \leqq j \leqq p-1$ implies that d_j is a polynomial in derivations in Z_{p-1}/Z_{p-2} and $(d_i) \in G$ with $d_1 = 0$ implies that d_p is a polynomial in derivations in Z_{p-1}/Z_{p-2}.*

PROOF. Let m be a generator for the multiplicative group of $I/(p)$. Let $(d_i) \in G$ have d_n with $n < p-1$ as its first nonzero map and let $n < j \leqq p-1$. $(m^i d_i)(d_i)^{-m^n} = (f_i)$, $f_1 = f_2 = \cdots = f_n = 0$, $f_j = (m^j - m^n)d_j + g$ where g is a polynomial in the mappings $d_n, d_{n-1}, \cdots, d_{j-1}$. This together with an inductive argument establishes the first part of the lemma. If $d_1 = 0$ then $n \geqq 2$ and $(m^i d_i)(d_i)^{-m^n} = (g_i)$, $g_1 = g_2 = \cdots = g_n = \theta$, $g_p = (m^p - m^n)d_p + h$ where h is a polynomial in the mappings $d_n, d_{n-1}, \cdots, d_{p-1}$. The second part of the lemma then follows.

2. **Main result.** Let G be a subgroup of $H^p(K)$ closed under scalar multiplication and having an upper central series satisfying: Z_p/Z_{p-1} and Z_{p-1}/Z_{p-2} are finite dimensional subspaces of Der(K) that are closed under pth powers and $Z_1/Z_0 = Z_{p-1}/Z_{p-2}$. The restrictions imposed upon Z_p/Z_{p-1} are the conditions of the exponent one Galois theory. Let k be the field of constants of G; that is, $k = \{x \in K \mid d_i(x) = 0$ for each $(d_i) \in G$ and $1 \leqq i \leqq p\}$. If the exponent of K over k is one and $Z_{p-1}/Z_{p-2} = \cdots = Z_1/Z_0$, then Theorem 19, p. 186 of [3] can

be used to show that $G = H_k^p(K)$. We assume then that the exponent of K over k is two. This is equivalent to assuming that there is a $(d_i) \in G$ with $d_1 \neq 0$. Let F denote the field of constants of Z_{p-1}/Z_{p-2}.

DEFINITION.

$$A(G) = \{f: F \to K \mid f = d_{p|F} \quad \text{for some } (d_i) \in G\},$$

$$P(G) = \{f + g: K \to K \mid f = d_p \quad \text{for some } (d_i) \in G,\ g \in K[Z_1/Z_0] \text{ with } g(0) = 0\}.$$

$A(G)$ is a subset of $\mathrm{Der}(F, K)$ and $P(G)$ is a subset of the ring of endomorphisms of K. Both $A(G)$ and $P(G)$ are closed under addition and scalar multiplication by elements of K^p.

THEOREM 1. *Let G be a subgroup of $H^p(K)$ closed under scalar multiplication and having an upper central series satisfying Z_p/Z_{p-1} and Z_{p-1}/Z_{p-2} are finite dimensional subspaces of* $\mathrm{Der}(K)$ *closed under pth powers and $Z_1/Z_0 = Z_{p-1}/Z_{p-2}$. If $P(G)$ is closed under commutation, then $A(G) \subseteq \mathrm{Der}(F)$ and if in addition $A(G)$ is closed under pth powers, then $G = H_k^p(K)$ where k is the field of constants of G.*

PROOF. $A(G) \subseteq \mathrm{Der}(F)$ follows from noting that if $d \in Z_1/Z_0$ and f is the pth map of an element of G, then $[d, f]\big|_F = 0$. An argument analogous to that used in the proof of Theorem 19, p. 186 of [3] establishes that the algebra of endomorphisms on F generated by $A(G)$ is the set of those endomorphisms of F that are linear over k. A dimension argument can then be used to prove that $F = K^p(k)$ and from this it follows that $G = H_k^p(K)$.

THEOREM 2 (CONVERSE OF THEOREM 1). *If $H_k^p(K)$ is finitely K-generated then the group $G = H_k^p(K)$ satisfies the hypothesis of Theorem* 1.

PROOF. Theorem 1 of [6] and Theorem 1 of [5] are used to determine the structure of $H_k^p(K)$.

THEOREM 3. *If G is a subgroup of $H^p(K)$ satisfying the hypothesis of Theorem* 1, *then the minimal subalgebra of $L(K, K)$, the ring of endomorphisms of K, containing the pth maps of G is $L_k(K)$, the subalgebra of $L(K, K)$ consisting of the endomorphisms which are linear over k.*

3. **Remarks.** If G is a subgroup of $H^p(K)$, let $f(G)$ denote the field of constants of G. Let A be the collection of subgroups of $H^p(K)$ which satisfy the conditions of Theorem 1 and let I be the collection of subfields k of K such that $[K: k] < \infty$, exponent of K over k is two, and K is a tensor product of simple extensions of k. Then the mapping

$k \to H_k^p(K)$ of I into A is the inverse of the mapping $G \to f(G)$ from A into I. Thus we have a Galois type correspondence for a class of finite dimensional exponent two field extensions.

It was not necessary to require that Z_p/Z_{p-1} and Z_{p-1}/Z_{p-2} be subalgebras of Der(K); Gerstenhaber [1] proved that a subspace of Der(K) closed under pth powers is also closed under *commutation.*

Sweedler [6] proved that if k is the field of constants of any set of higher derivations defined on K, then K is a tensor product of simple extensions of k. This fact was used in proving Theorems 1 and 2.

Another contributor in this area, M. Weisfeld [7], has shown that K is a tensor product of simple extensions of k if and only if k is the field of constants of a higher derivation on K.

By working with groups of higher derivations having length p^2, p^3, etc. one should be able to extend these results to higher exponent cases.

References

1. M. Gerstenhaber, *On the Galois theory of inseparable extensions*, Bull. Amer. Math. Soc. **70** (1964), 561–566.

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

3. ———, *Lectures in abstract algebra.* Vol. III, Van Nostrand, Princeton, N. J., 1964.

4. N. Heerema, *Derivations and embeddings of a field in its power series ring*, Proc. Amer. Math. Soc. **11** (1960), 188–194.

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

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

7. M. Weisfeld, *Purely inseparable extensions and higher derivations*, Trans. Amer. Math. Soc. **116** (1965), 435–449.

Florida State University, Tallahassee, Florida 32306