PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 72, Number 2, November 1978

ON GALOIS THEORY USING PENCILS OF HIGHER DERIVATIONS

JAMES K. DEVENEY AND JOHN N. MORDESON

ABSTRACT. Let $L \supset K$ be fields of characteristic $p \neq 0$. Assume K is the field of constants of a group of pencils of higher derivations on L, and hence L is modular over K and K is separably algebraically closed in L. Every intermediate field F which is separably algebraically closed in L and over which L is modular is the field of constants of a group of pencils of higher derivations if and only if $K(L^{p^e})$ has a finite separating transcendence basis over K for some nonnegative integer e. If $p \neq 2, 3$ and $K(L^{p^e})$ does have a finite separating transcendence basis over K, and F is the field of constants of a group of pencils, then the group of L over F is invariant in the group of L over K if and only if $F = K(L^{p^r})$ for some nonnegative integer r.

1. Introduction. Throughout we assume L is a field of characteristic $p \neq 0$. This paper is concerned with the Galois theory of pencils of higher derivations developed by Heerema [5]. Recall that a rank t higher derivation on L is a sequence $d = \{d_i | 0 \leqslant i \leqslant t\}$ of additive maps of L into L such that $d_r(ab) = \Sigma\{d_i(a)d_j(b) | i + j = r\}$ and d_0 is the identity map. The set of all rank t higher derivations forms a group with respect to the composition $d \circ e = f$ where $f_j = \Sigma\{d_m e_n | m + n = j\}$. Let $H(L/K)$ be the set of all higher derivations on L, trivial on K and having rank some power of p. For d in $H(L/K)$, $V(d) = f$ where rank $f = p(\text{rank } d)$, $f_{pi} = d_i$ and $f_i = 0$ if $p \nmid j$. Two higher derivations f and g are equivalent if $g = V^i(f)$ or $f = V^i(g)$ for some i. The equivalence class of d is $\bar{d}$ and is called the pencil of d. The set of all pencils, $\bar{H}(L/K)$, can be given a group structure by defining $\bar{d}\bar{f}$ to be the pencil of $d'f'$ where d' is in $\bar{d}$, f' is in $\bar{f}$ and rank d' = rank f'. Heerema developed the group of pencils in order to incorporate in a single theory the Galois theories of finite and infinite rank higher derivations. However, as indicated by Proposition 1, the group of pencils could also be used to develop a theory for some unbounded exponent purely inseparable modular extensions.

If K is the field of constants of a group of pencils on L, then L/K is modular and K is separably algebraically closed in L. This paper develops criteria for every intermediate field of L/K with these properties to be a field of constants. Necessary and sufficient conditions are shown to be that $K(L^{p^e})$ has a finite separating transcendence basis over K for some nonnegative

Received by the editors April 19, 1977.
AMS (MOS) subject classifications (1970). Primary 12F15.
Key words and phrases. Modular field extension, pencils of higher derivations.

integer e. This provides for an immediate extension of part of the Galois theory in [5]. A characterization of the Galois groups in this more general setting awaits the solution in the bounded exponent infinite dimensional purely inseparable case. §3 develops criteria for a Galois subgroup of a Galois group to be normal.

2. Fields of constants. The following proposition determines which subfields of L are the fields of constants of sets (and hence groups) of pencils of higher derivations. The result parallels that of Davis [1, Theorem 1, p. 50] with the replacement of separable by modular.

PROPOSITION 1. *Let K be a subfield of L. Then K is the field of constants of a set of pencils on L if and only if L/K is modular and $\bigcap_n K(L^{p^n}) = K$.*

PROOF. Suppose K is the field of constants of a set of pencils $\bar{H}$. Let H be the set of all higher derivations d such that $\bar{d} \in \bar{H}$. Then $\bigcap_{d\in H} L^d = K$ where L^d is the field of constants of d. Note that $H = \bigcup_n H_n$ where every element of H_n is of rank p^n. For $d \in H_n$, $L^d \supseteq K(L^{p^{n+1}})$ by [10, p. 436]. Hence

$$K = \bigcap_{d\in H} L^d = \bigcap_n \bigcap_{d\in H_n} L^d \supseteq \bigcap_n K(L^{p^{n+1}}) \supseteq K$$

so $K = \bigcap_n K(L^{p^n})$. Since L is modular over each L^d, L/K is modular [9, Proposition 1.2, p. 40].

Conversely, suppose L/K is modular and $\bigcap_n K(L^{p^n}) = K$. Then $L/K(L^{p^{n+1}})$ is modular for all n and hence, if $H_n(L/K)$ denotes the group of all rank p^n higher derivations on L/K,

$$\bigcap_{d\in H_n(L/K)} L^d = K(L^{p^{n+1}}).$$

Thus

$$\bigcap_{d\in H(L/K)} L^d = \bigcap_n \bigcap_{d\in H_n(L/K)} L^d = \bigcap_n K(L^{p^{n+1}}) = K$$

and K is the field of constants of $H(L/K)$ whence of $\bar{H}(L/K)$.

COROLLARY 2. *The field of constants of the group of all pencils on L is the maximal perfect subfield $\bigcap_n L^{p^n}$ of L.*

PROOF. Since separable extensions are modular, $L/\bigcap_n L^{p^n}$ is modular.

PROPOSITION 3. *Let K be any subfield of L. The field of constants of the group of all pencils on L over K is $\bigcap_n Q^*(L^{p^n})$ where Q^* is the unique minimal intermediate field such that L/Q^* is modular.*

PROOF. The existence of Q^* is established in [4, Theorem 1.1]. Since

$$\bigcap_i \Big(\bigcap_n Q^*(L^{p^n})\Big)(L^{p^i}) = \bigcap_n Q^*(L^{p^n}),$$

$\bigcap_n Q^*(L^{p^n})$ is the field of constants of a set of pencils by Proposition 1.

Moreover, if M is a field of constants, since L/M is modular, $M \supseteq Q^*$ and, hence, $M = \bigcap_n M(L^{p^n}) \supseteq \bigcap_n Q^*(L^{p^n})$.

In view of [4, Theorem 1.6] it would be tempting to conjecture that $\bigcap_n Q^*(L^{p^n})$ is relatively perfect over Q^*. However, examples given by Waterhouse [9] indicate that $\bigcap_n Q^*(L^{p^n})$ can be bounded exponent over Q^*.

The Galois correspondence using pencils developed by Heerema is restricted to the case where L/K is finitely generated. We now determine the most general conditions on L/K so that every intermediate field F which is separably algebraically closed in L and over which L is modular will be a Galois subfield, i.e. the field of constants of a group of pencils.

PROPOSITION 4. *Let L/K be purely inseparable modular. Then every intermediate field F of L/K such that L/F is modular is the field of constants of a group of pencils on L if and only if L/K is of bounded exponent.*

PROOF. If L/K is of bounded exponent, the conclusion is immediate. Suppose F is the field of constants of a set of pencils on L for every F such that L/F is modular. Then by Proposition 1, $F = \bigcap_n F(L^{p^n})$ for every such F. Let B be a maximal pure independent set for L/F. Then $L/F(B)$ is modular and relatively perfect [9, Theorem 2.3, p. 42]. Thus $L = \bigcap_n F(B)(L^{p^n}) = F(B)$. That is, L has a subbasis over every intermediate field F such that L/F is modular. Suppose L/F is modular and of unbounded exponent. Then $L = F(B)$ where B is a subbasis of L/F. Now $B = \bigcup_i B_i$ where every element of B_i is of exponent i over F and for any positive integer n there exists $i > n$ such that $B_i \neq \varnothing$. Let $x_{i_j} \in B$ be such that x_{i_j} has exponent i_j over F, $i_j < i_{j+1}$, $1 \leqslant j < \infty$. Set

$$\hat{F} = F\left(B \setminus \{x_{i_j}\}, x_{i_1} - x_{i_2}^{p^{i_2 - i_1}}, \dots, x_{i_j} - x_{i_{j+1}}^{p^{i_{j+1} - i_j}}, \dots\right).$$

Then

$$L = \hat{F}(x_{i_2}, x_{i_3}, \dots, x_{i_j}, \dots) = \hat{F}(x_{i_3}, \dots, x_{i_j}, \dots) = \dots.$$

The intermediate fields of $L/\hat{F}$ are chained [7, p. 20]. Hence it follows that $L/\hat{F}$ is modular and relatively perfect. However, this is impossible since $L \neq \hat{F}$ and $L/\hat{F}$ must have a subbasis. Hence L/F is of bounded exponent for every intermediate field F such that L/F is modular, in particular, for $F = K$.

The following example is one such that L/K is not modular, every intermediate field F such that L/F is modular is the field of constants of a set of pencils on L, yet L/K is not of bounded exponent. (The proof of Proposition 4 shows that when this happens, L/F is of bounded exponent for every F such that L/F is modular.)

EXAMPLE 5. Let $K = P(z, y, x_1, x_2, \dots, x_n, \dots)$ where P is a perfect field and $z, y, x_1, \dots, x_n, \dots$ are algebraically independent indeterminants over P. Let

$$L = K\left(z^{p^{-2}}x_1^{p^{-1}} + y^{p^{-1}}, \ldots, z^{p^{-n-1}}x_n^{p^{-1}} + y^{p^{-1}}, \ldots\right).$$

Then L/K is reliable [7, Example 1.26(a), p. 20] whence not modular [4, Corollary 2.5]. $K(L^p) = K(z^{p^{-1}}, \ldots, z^{p^{-n}}, \ldots)$. $L/K(L^p)$ is modular so $Q^* \subseteq K(L^p)$ where Q^* is the unique minimal intermediate field of L/K such that L/Q^* is modular. If $Q^* \subset K(L^p)$ (strict inclusion), then $Q^* = K(z^{p^{-n}})$ for some n. Since L/K is reliable, L/Q^* is reliable. Since it is impossible for L/Q^* to be modular, reliable, and of unbounded exponent [4, Corollary 2.5], we must have $Q^* = K(L^p)$. Thus every intermediate field F such that L/F is modular is such that L/F has bounded exponent, in fact, exponent $\leqslant 1$.

THEOREM 6. *Suppose L/K is modular. Then every intermediate field F such that L/F is modular and F is separably algebraically closed in L is the field of constants of a group of pencils on L if and only if $K(L^{p^e})$ has a finite separating transcendence basis over K for some nonnegative integer e.*

PROOF. Suppose the condition holds for every such intermediate field F of L/K. Then the condition holds for every such intermediate field F of L/H^* where H^* is the unique minimal intermediate field such that L/H^* is regular [4]. By [2, Corollary 4.2, p. 397], L/H^* has a finite separating transcendency basis. Since H^*/K is purely inseparable [6, Lemma 4, p. 303] L/K splits [6, Proposition 1, p. 302], say $L = J \otimes_K D$ where D/K has a finite separating transcendence basis and J/K is purely inseparable. Now, L/D is modular and for every intermediate field F of L/D such that L/F is modular, F is the field of constants of a set of pencils on L. Thus by Proposition 4, L/D is of bounded exponent. Thus $K(L^{p^e})$ has a finite separating transcendence basis for some e.

Conversely, suppose $K(L^{p^e})$ has a finite separating transcendence basis over K for some e and let F be an intermediate field such that L/F is modular and F is separably algebraically closed in L. Then $F(L^{p^n})$ has a finite separating transcendence basis over F for some n, hence $L = \bar{F} \otimes_F R$ where R/F is regular and has a finite separating transcendence basis and $\bar{F}/F$ is purely inseparable modular of bounded exponent. Thus F is the field of constants of a set of pencils on L by the proof of [5, Proposition 2.1].

3. Invariant subgroups.

LEMMA 7. *Let K be a Galois subfield of L. Then $\overline{H}(L/K)$ contains an isomorphic image of $H_n(L/K)$, say $\overline{H}_n(L/K)$, and $\overline{H}_n(L/K) \subseteq \overline{H}_{n+1}(L/K)$, $n = 0, 1, \ldots$. Furthermore, $\bigcup_n \overline{H}_n(L/K) = \overline{H}(L/K)$.*

PROOF. Define Φ: $H_n(L/K) \to \overline{H}(L/K)$ by $\Phi(d) = \bar{d}$ for all $d \in H_n(L/K)$. Clearly Φ is a homomorphism. Suppose $\Phi(d) = \Phi(f)$, i.e. $\bar{d} = \bar{f}$. Now d and f have the same rank and since either $v^i(d) = f$ or $v^i(f) = d$ for some i [5], we have $d = f$. That is Φ is 1-1. Let $\bar{f} \in H_n(L/K)$. Then there exists $d \in H_n(L/K)$ such that $\bar{d} = \bar{f}$. Now $v(d) \in H_{n+1}(L/K)$ and

$\bar{f} = \bar{d} = \overline{v(d)} \in \bar{H}_{n+1}(L/K)$, so $\bar{H}_n(L/K) \subseteq \bar{H}_{n+1}(L/K)$. Clearly $\bigcup_n \bar{H}_n(L/K) = \bar{H}(L/K)$.

We note that by Lemma 7 and the definition of multiplication, a subgroup $\bar{H}(L/F)$ of $\bar{H}(L/K)$ will be an invariant subgroup if and only if $H_n(L/F)$ is invariant in $H_n(L/K)$ for all n.

THEOREM 8. *Suppose $p \neq 2, 3$. Let $K \subset F$ be Galois subfields of L such that $K(L^{p^e})$ has a finite separating transcendence basis over K for some e. Then the following conditions are equivalent.*

(1) *$\bar{H}(L/F)$ is $\bar{H}(L/K)$ invariant.*

(2) *$F = K(L^{p^r})$ for some r.*

PROOF. If $F = K(L^{p^r})$, then F is invariant under $\bar{H}(L/K)$ and hence $\bar{H}(L/F)$ is $\bar{H}(L/K)$ invariant.

Assume (1). Let $\bar{F}$ denote the algebraic closure of F in L and we first consider the case $\bar{F} \neq L$. Since $L/\bar{F}$ and $L/\bar{K}$ are regular, $\bar{F}/\bar{K}$ is regular. Also, $L/\bar{F}$ and $\bar{F}/\bar{K}$ have finite separating transcendence bases [8, Theorem 2, p. 419]. Since $\bar{K}/K$ is modular, there exists a p-basis Z of $\bar{K}$ such that $Z \setminus (Z \cap K)$ is a subbasis for $\bar{K}$ over K. Let X be a separating transcendence basis of $\bar{F}/\bar{K}$ and let Y be a separating transcendence basis of $L/\bar{F}$. Then $Z \cup X$ and $Z \cup X \cup Y$ are p-bases of $\bar{F}$ and L, respectively.

Since $\bar{F} \neq L$, $Y \neq \varnothing$. Suppose $X \neq \varnothing$. Let $x_0 \in X$ and $y_0 \in Y$. Let t be the exponent of x_0 over F. Define $d, f \in H_{t+1}(L/K)$ as follows:

$$d_i(z) = 0 \quad \text{for all } z \in Z, i \geqslant 1, \quad f_i(z) = 0 \quad \text{for all } z \in Z, i \geqslant 1,$$
$$d_1(x_0) = y_0, \quad d_i(x_0) = 0, i > 1, \quad f_1(y_0) \neq 0, \quad f_i(y_0) = 0, i > 1,$$
$$d_i(s) = 0 \quad \text{for all } s \in X \cup Y \setminus \{x_0\}, i \geqslant 1,$$
$$f_i(s) = 0 \quad \text{for all } s \in X \cup Y \setminus \{y_0\}, i \geqslant 1.$$

Then $\bar{d} \in \bar{H}(L/K)$ and $\bar{f} \in \bar{H}(L/F)$ by [5]. Since $\bar{H}(L/F)$ is invariant in $\bar{H}(L/K)$, $d^{-1}fd$ restricted to F must be the identity higher derivation, i.e. $fd = d$ when restricted to F. However

$$(fd)_{2p^t}\left(x_0^{p^t}\right) = \sum_{i=0}^{2p^t} f_i d_{2p^t-i}\left(x_0^{p^t}\right) = \left[\sum_{j=0}^{2} f_j d_{2-j}(x_0)\right]^{p^t}$$
$$= d_{2p^t}\left(x_0^{p^t}\right) + \left(f_1(y_0)\right)^{p^t} \neq d_{2p^t}\left(x_0^{p^t}\right).$$

Thus we have a contradiction and, hence, $X = \varnothing$, i.e. $\bar{F} = \bar{K}$ or $F \subseteq \bar{K}$. Since we are assuming $\bar{F} \neq L$, L/F is not purely inseparable. Since $\bar{H}(L/F)$ and, as noted, $\bar{H}(L/K(L^{p^n}))$ are both $\bar{H}(L/K)$ invariant and $L/K(L^{p^n})(F) = L/F(L^{p^n})$ is modular, $\bar{H}(L/K(L^{p^n})(F))$ is $\bar{H}(L/K)$ invariant and hence is invariant in $\bar{H}(L/K(L^{p^n}))$. Thus by [3, Theorem]

$$K(L^{p^n})(F) = K(L^{p^n})(L^{p^r}) = K(L^{p^r})$$

or

$$K(L^{p^n})(F) \subseteq K(L^{p^n})(L^{p^e}) \quad \text{for all } e,$$

i.e. $K(L^{p^n})(F) = K(L^{p^n})$. Moreover, this must be true for all large n. For large n, $K(L^{p^n})$ is separable over K, and since F is purely inseparable over K, for large n, $K(L^{p^{n+1}})(F) \neq K(L^{p^n})(F)$. Thus as n increases, r must increase. But this says F is separable over K and hence $F = K$. Thus under the assumption $\overline{F} \neq L$, we conclude $F = K$, a contradiction.

We now consider the case $\overline{F} = L$. Since L/F is purely inseparable and $K(L^{p^e})$ has a finite separating transcendence basis over K, $K(L^{p^n}) \subseteq F \subseteq L$ for some n. Thus $\overline{H}(L/F)$ is $\overline{H}(L/K(L^{p^n}))$ invariant and $F = K(L^{p^n})(L^{p^r}) = K(L^{p^r})$ for some r by [3, Theorem].

References

1. R. L. Davis, *Higher derivations and field extensions*, Trans. Amer. Math. Soc. **180** (1973), 47–52. MR **47** #6664.

2. J. Deveney, *Fields of constants of infinite higher derivations*, Proc. Amer. Math. Soc. **41** (1973), 394–398. MR **49** #259.

3. J. Deveney and J. Mordeson, *Invariant subgroups of groups of higher derivations*, Proc. Amer. Math. Soc. **68** (1978), 277–280.

4. ______, *Subfields and invariants of inseparable extensions*, Canad. J. Math. **29** (1977), 1304–1311.

5. N. Heerma, *Higher derivation Galois theory of fields* (preprint).

6. N. Heerema and D. Tucker, *Modular field extensions*, Proc. Amer. Math. Soc. **53** (1975), 301–306.

7. J. Mordeson and B. Vinograde, *Structure of arbitrary purely inseparable field extensions*, Lecture Notes in Math., vol. 173, Springer-Verlag, Berlin and New York, 1970. MR **43** #1952.

8. ______, *Separating p-bases and transcendental extension fields*, Proc. Amer. Math. Soc. **31** (1972), 417–422. MR **44** #6655.

9. W. Waterhouse, *The structure of inseparable field extensions*, Trans. Amer. Math. Soc. **211** (1975), 39–56. MR **33** #122.

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

Department of Mathematical Sciences, Virginia Commonwealth University, Richmond, Virginia 23284

Department of Mathematics, Creighton University, Omaha, Nebraska 68131