PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 74, Number 2, May 1979

PENCILS OF HIGHER DERIVATIONS OF ARBITRARY FIELD EXTENSIONS

JAMES K. DEVENEY AND JOHN N. MORDESON

ABSTRACT. Let L be a field of characteristic $p \neq 0$. A subfield K of L is Galois if K is the field of constants of a group of pencils of higher derivations on L. Let $F \supset K$ be Galois subfields of L. Then the group of L over F is a normal subgroup of the group of L over K if and only if $F = K(L^{p^r})$ for some nonnegative integer r. If L/K splits as the tensor product of a purely inseparable extension and a separable extension, then the algebraic closure of K in L, $\overline{K}$, is also Galois in L. Given K, for every Galois extension L of K, $\overline{K}$ is also Galois in L if and only if $[K : K^p] < \infty$.

0. Introduction. Throughout we assume L is a field of characteristic $p \neq 0$. A rank t higher derivation on L is a sequence $d = \{d_i | 0 \leqslant i < t + 1\}$ of additive maps of L into L such that

$$d_r(ab) = \sum \{d_i(a)d_j(b) | i + j = r\}$$

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. Given d in $H(L/K)$, $v(d) = f$ where rank $f = p(\text{rank } d)$, $f_{pi} = d_i$ and $f_j = 0$ 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, $\overline{H}(L/K)$, can be given a group structure by defining $\bar{d}\bar{f}$ to be the pencil of $d'f'$ where $d' \in \bar{d}$, $f' \in \bar{f}$ and rank d' = rank f' [3]. A subfield K of L will be called Galois if K is the field of constants of a group of pencils on L or equivalently if L/K is modular and $\bigcap_i K(L^{p^i}) = K$ [2, Proposition 1]. In §1 it is shown that if $F \supset K$ are Galois subfields of L, then $\overline{H}(L/F)$ is an invariant subgroup of $\overline{H}(L/K)$ if and only if $F = K(L^{p^r})$ for some nonnegative integer r. This generalizes the result given in [2, Theorem 8] for the bounded exponent finite transcendence degree case.

Let $\overline{K}$ denote the algebraic closure of K in L. L/K is said to split when $L = J \otimes_K D$ where J/K is purely inseparable and D/K is separable. §2 examines the question of when $\overline{K}$ is Galois in L, given L/K is Galois. Sufficient conditions are shown to be the splitting of L/K. Moreover, for every Galois extension L of K, $\overline{K}$ is also Galois in L if and only if

Presented to the Society, August 10, 1978 under the title *On pencil Galois theory*; received by the editors March 8, 1978.

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

Key words and phrases. Modular field extension, pencils of higher derivations.

$[K : K^p] < \infty$ (and in this case L/K splits). In view of these results it appeared that $\overline{K}$ being Galois in L was related to L/K splitting. However, an example is constructed with L/K and $L/\overline{K}$ both Galois and yet L/K does not split.

Pencils of higher derivations were originally constructed by Heerema to incorporate into a single theory the Galois theories of finite and infinite rank higher derivations. Basically the infinite higher derivations would be the group of $L/\overline{K}$ ($L/\overline{K}$ being separable). However, in the proof of Theorem 2.2, an example of a Galois extension is constructed with $L/\overline{K}$ being relatively perfect, and hence having no infinite rank higher derivations. Thus in this most general setting some different fields of constants are obtained.

1. Invariant subgroups. Let $F \supset K$ be Galois subfields of L. This section develops necessary and sufficient conditions for $\overline{H}(L/F)$ to be $\overline{H}(L/K)$-invariant.

(1.1) LEMMA. *Suppose L/K is purely inseparable Galois. Let F^* be an intermediate field of L/K such that L/F^* is modular and F^*/K has exponent $\leqslant 1$. If for every maximal pure independent set M of L/K every element of M has the same exponent over F^* that it has over K, then $F^* = K$.*

PROOF. Suppose some c in L has c^{p^i} in F^* but not in $K(K^{p^{-1}} \cap L^{p^{i+1}})$. By modularity,

$$K(K^{p^{-1}} \cap L^{p^{i+1}}) = K(L^{p^{i+1}}) \cap K^{p^{-1}},$$

and hence c^{p^i} is not in $K(L^{p^{i+1}})$. For $j \leqslant i$, c^{p^j} cannot be in $K(L^{p^{j+1}})$. Thus c is pure independent **[9]** and is part of a maximal pure independent set of L/K. But c has exponent $i + 1$ over K and exponent i over F^*, contrary to the hypothesis. Hence

$$F^* \cap L^{p^i} \subseteq K(K^{p^{-1}} \cap L^{p^{i+1}}), \quad i = 0, 1, \ldots.$$

In an entirely similar manner as in the proof of **[7**, Lemma 2, p. 339**]** we obtain $F^* = K(F^* \cap L^p) = \cdots = K(F^* \cap L^{p^i}) = \ldots$. Hence

$$K \subseteq F^* = \bigcap_i K(F^* \cap L^{p^i}) \subseteq \bigcap_i K(L^{p^i}) = K,$$

i.e., $F^* = K$.

(1.2) LEMMA. *Suppose L/K is purely inseparable Galois. Let F be an intermediate field of L/K such that L/F is modular and $F \cap L^{p^n} \subseteq K$ for some nonnegative integer n. If for every maximal pure independent set M of L/K every element of M has the same exponent over F that it has over K, then $F = K$.*

PROOF. The proof is exactly the same as the proof of **[7**, Lemma 3, p. 340**]** with "maximal pure independent set" replacing "modular base" there.

(1.3) THEOREM. *Suppose $p \neq 2$. Let $K \subset F$ be Galois subfields of L. Then $\overline{H}(L/F)$ is $\overline{H}(L/K)$-invariant if and only if $F = K(L^{p^r})$ for some nonnegative integer r.*

PROOF. If $F = K(L^{p^r})$ for some r, then $\overline{H}(L/K)$ leaves F invariant. Hence clearly $\overline{H}(L/F)$ is $\overline{H}(L/K)$-invariant. Conversely, suppose $\overline{H}(L/F)$ is $\overline{H}(L/K)$-invariant. We prove the theorem first for the case $p > 3$. Suppose $\bigcap_i K(F \cap L^{p^j})(L^{p^i}) = F$ for all nonnegative integers j. Then

$$K = \bigcap_j \bigcap_i K(F \cap L^{p^j})(L^{p^i}) = F,$$

a contradiction. Let j be such that $\bigcap_i K(F \cap L^{p^j})(L^{p^i}) \subset F$ and set

$$K_j = \bigcap_i K(F \cap L^{p^j})(L^{p^i}).$$

Then $\bigcap_i K_j(L^{p^i}) = K_j$ and L/K_j is modular [**7**, Lemma 1, p. 339], [**9**, Proposition 1.2(b), p. 40]. Thus K_j is Galois in L and $\overline{H}(L/F)$ is invariant in the smaller group $\overline{H}(L/K_j)$. Now F/K_j is purely inseparable of bounded exponent. By [**8**, Lemma 1.61(c), p. 56], $\overline{F}/K_j$ is modular. Also $F \cap L^{p^n} \subseteq K_j$ for some n, namely $n = j$. Hence $F \cap \overline{F}^{p^n} \subseteq K_j$. By Lemma 1.2, there exists a maximal pure independent set X of $\overline{F}/K_j$ with $x \in X$ such that the exponent t of x over F is less than the exponent s of x over K_j. Let Y be a maximal pure independent set of $\overline{F}/F$. Suppose $\overline{F}/F$ is of unbounded exponent. If $F(Y)/F$ is of bounded exponent, then $\overline{F} = J \otimes_F F(Y)$ for some intermediate field J of $\overline{F}/F$ [**9**, Proposition 2.6, p. 43]. Since Y is necessarily a relative p-basis of $\overline{F}/F$, J/F is relatively perfect. Hence $\bigcap_i F(\overline{F}^{p^i}) = J \supset F$, a contradiction. Thus $F(Y)/F$ is of unbounded exponent. Hence there exists $y \in Y$ such that $u > s$ where u is the exponent of y over F. Hence $u > s > t$. Let e be any positive integer such that $e > u$. Since $L/\overline{F}$ is modular, $L/\overline{F}$ is separable and thus preserves p-independence. It follows that there exists $d = \{d_0, d_1, \ldots, d_{p^e}\} \in H(L/K_j)$ and $d' = \{d'_0, d_1, \ldots, d'_{p^e}\} \in H(L/F)$ with first nonzero maps of positive subscript being q and q' respectively, such that $d_q(x) = y$, $d'_{q'}(y) \neq 0$, $q = p^{e-s} + 1$, $q' = p^{e-u} + 1$.

Since $\overline{H}(L/F)$ is $\overline{H}(L/K_j)$-invariant, $d^{-1}d'd$ restricted to F must be the identity higher derivation, i.e. $d'd = d$ when restricted to F. Suppose $(q + q')p^t \leqslant p^e$. Then

$$\begin{aligned}(d'd)_{(q+q')p^t}(x^{p^t}) &= \sum \left\{ d'_i d_{(q+q')p^t - i}(x^{p^t}) | 0 \leqslant i \leqslant (q + q')p^t \right\} \\ &= \sum \left\{ d'_j \left(d_{q+q'-j}(x)\right)^{p^t} | 0 \leqslant j \leqslant q + q' \right\} \\ &= d_{(q+q')p^t}(x^{p^t}) + d'_{q'}(y)^{p^t} \\ &\neq d_{(q+q')p^t}(x^{p^t}), \quad \text{a contradiction..}\end{aligned}$$

Thus $(q + q')p^t > p^e$, so $p^{e-s} + p^{e-u} + 2 > p^{e-t}$. Hence $p^{-s} + p^{-u} + 2p^{-e} > p^{-t}$. Since we can take e as large as we wish, we have $p^{-s} + p^{-u} \geqslant p^{-t}$ so $p^{t-s} + p^{t-u} \geqslant 1$. Since $s - t \geqslant 1$ and $u - t \geqslant 2$, we have $p^{-1} + p^{-1} > p^{t-s} + p^{t-u}$, i.e., $2 > p$, a contradiction. Thus $\overline{F}/F$ has bounded exponent so L/K_j has finite inseparability exponent. Suppose $\overline{F} \subset L$. Then as in the proof of [**2**, Theorem 8], we obtain $F = K_j$ a contradiction. Hence $\overline{F} = L$.

Thus L/F has bounded exponent so $L \supseteq F \supseteq K(L^{p^n})$ for some n. Now $\overline{H}(L/F)$ is $\overline{H}(L/K(L^{p^n}))$-invariant. Hence $F = K(L^{p^r})$ for some r by [**2**, Theorem 8].

The proof for the case $p = 3$ is exactly the same, once it is noted that [**2**, Theorem 8] is true for $p = 3$. This follows from [**1**, Theorem, p. 277] and in particular [**1**, Lemma, p. 278]. Here, for large e the key inequality becomes $2p^{e-1} + 2p^{t_1} > p^e$. Since t_1 is fixed, large e force $p = 2$.

2. Galois subfields. Let L be a Galois extension of K, i.e., L/K is modular and $\bigcap_i K(L^{p^i}) = K$. Then certainly $\bigcap_i K(\overline{K}^{p^i}) = K$ and since $\overline{K}$ is modular over K, $\overline{K}$ is a Galois extension of K. Moreover $L/\overline{K}$ is separable (hence modular) so $L/\overline{K}$ will be Galois if and only if $\bigcap_i \overline{K}(L^{p^i}) = \overline{K}$. We now investigate conditions which will guarantee $L/\overline{K}$ is Galois.

(2.1) PROPOSITION. *Suppose K is a Galois subfield of L. If L/K splits, then $\overline{K}$ is Galois in L.*

PROOF. $L = S \otimes_K \overline{K}$ where S is an intermediate field of L/K which is separable over K. As noted $L/\overline{K}$ is separable, so it suffices to show $\bigcap_i \overline{K}(L^{p^i}) = \overline{K}$. Now $\bigcap_i \overline{K}(L^{p^i}) = \bigcap_i (K(S^{p^i}) \otimes_K \overline{K}) = \overline{K}$.

(2.2) THEOREM. *Let K be a field. Then $[K : K^p] < \infty$ if and only if for every field extension L/K such that K is Galois in L, $\overline{K}$ is Galois in L.*

PROOF. Suppose $[K : K^p] < \infty$. Let L/K be Galois. Then $\bigcap_i K(\overline{K}^{p^i}) = K$ and since any relative p-basis of $\overline{K}/K$ is finite, we have $\overline{K}/K$ has bounded exponent. By [**5**, Theorem 4, p. 1178], L/K splits and so Proposition 2.1 applies.

Conversely, suppose $[K : K^p] = \infty$. Let $x_1, x_3, \ldots, x_{2n-1}, \ldots$ be p-independent in K. Let

$$L = K\left(z, z^{p^{-1}} + x_1^{p^{-2}}, \ldots, z^{p^{-n}} + x_1^{p^{-n-1}} + x_3^{p^{-n-2}} + \cdots + x_{2n-1}^{p^{-2n}}, \ldots\right)$$

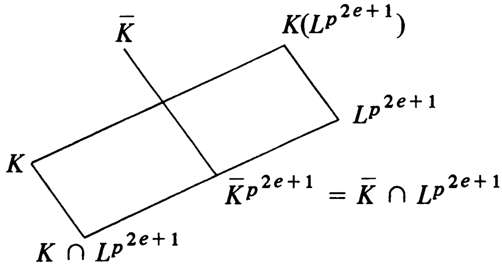
where z is transcendental over K. Then

$$\overline{K} = K\left(x_1^{p^{-1}}, x_3^{p^{-3}}, \ldots, x_{2n-1}^{p^{-2n+1}}, \ldots\right).$$

Since $L/\overline{K}$ is a union of ascending chain of separable extensions of $\overline{K}$, $L/\overline{K}$ is separable. Now $\overline{K}(L^p) = L$ so $\overline{K}$ is not Galois in L. Clearly $\overline{K}/K$ is purely inseparable modular so L/K is modular [**5**, Theorem 1, p. 1117]. Hence in order to show K is Galois in L it suffices to show $\bigcap_i K(L^{p^i}) = K$. Now $\{z^{p^{-n}} + x_1^{p^{-n-1}} + \cdots + x_{2n-1}^{p^{-2n}} | n = 1, 2, \ldots\}$ is a subbasis of $L/K(z)$. Hence $\bigcap_i K(z)(L^{p^i}) = K(z)$. Let $K^* = \bigcap_i K(L^{p^i})$. Since $\bigcap_i K^*(L^{p^i}) = K^*$, K^* is separably algebraically closed in L. Clearly $K^* \subseteq K(z)$. Suppose $K^* \neq K$. Then $K(z)/K^*$ is algebraic and thus $K^* = K(z^{p^e})$ for some nonnegative integer e. Now $z^{p^e} \in K(L^{p^{2e+1}})$. Therefore

$$x_{2e+1}^{p^{-1}} \in K(L^{p^{2e+1}}) \cap \overline{K}.$$

By the separability of $L/\overline{K}$, the modularity of $\overline{K}/K$, [**4**, Lemma p. 162], and the following diagram,



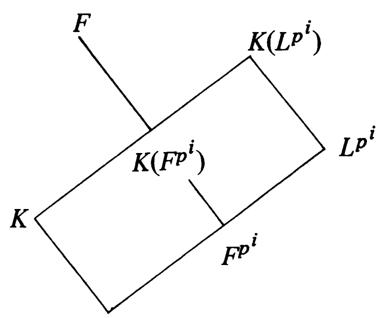
we have $x_{2e+1}^{p^{-1}} \in K(L^{p^{2e+1}}) \cap \bar{K} = K(\bar{K}^{p^{2e+1}})$ which is clearly impossible. Hence $K^* = K$ and K is a Galois subfield of L.

Consider the example constructed in the proof of Theorem 2.2. Heerema [3] originally developed pencils of higher derivations in order to incorporate both the finite and infinite rank higher derivation Galois theories into 1 unified theory. He considered finitely generated modular extensions L/K. In this case $\bar{K}$ would be the field of constants of the group of infinite rank higher derivations (pencils with infinite extended rank in the new theory). However, in the example above, $L/\bar{K}$ is relatively perfect and hence has no infinite higher derivations and yet L/K is Galois. Thus in the nonfinitely generated case a different type of field of constants can occur.

In Proposition 2.1 and Theorem 2.2 the sufficient condition given for $\bar{K}$ to be Galois in L also imply $L/\bar{K}$ splits. We now develop an example to show that L/K and $L/\bar{K}$ being Galois does not imply L/K splits.

(2.3) Proposition. *Let F be an intermediate field of L/K such that L/F is separable Galois and F/K is Galois. Then L/K is Galois.*

Proof. Since L/F is separable and $F/K(F^{p^i})$ is modular, $L/K(F^{p^i})$ is modular, $i = 0, 1, \ldots$. Hence $L/\bigcap_i K(F^{p^i})$ is modular, i.e. L/K is modular [9, Proposition 1.2(b), p. 40]. Thus we have linear disjointness in the following diagram



Hence $F \cap K(L^{p^i}) = K(F^{p^i})$. Clearly $\bigcap_i K(L^{p^i}) \subseteq F$. Thus

$$\bigcap_i K(L^{p^i}) = \bigcap_i K(L^{p^i}) \cap F = \bigcap_i K(F^{p^i}) = K.$$

(2.4) Corollary. *If $L/\bar{K}$ and $\bar{K}/K$ are Galois, then L/K is Galois.*

PROOF. $L/\bar{K}$ is separable since $L/\bar{K}$ is modular and $\bar{K}$ is algebraically closed in L.

(2.5) EXAMPLE. L/K and $L/\bar{K}$ are Galois, yet L/K does not split: Let $K = P(z_1^p, \ldots, z_j^p, \ldots)$ and

$$L = K\left(z_1, \ldots, z_j^{p^{-j+1}}, \ldots\right)\left(y, u_0, \ldots, u_n^{p^{-n}}, \ldots\right)$$

where P is a perfect field, $y, u_0, z_1, \ldots, z_j, \ldots$ are algebraically independent indeterminants over P and $u_n^{p^{-n}} = y^{p^{-1}} + z_n^{p^{-n}} u_{n-1}^{p^{-n}}$, $n = 1, 2, \ldots$. Then $\bar{K} = K(z_1, \ldots, z_j^{p^{-j+1}}, \ldots)$. Now $\bar{K}(y, u_n^{p^{-n}})$, $n = 0, 1, \ldots,$ is an ascending chain of separable extensions of $\bar{K}$ whose union is L. Thus $L/\bar{K}$ is separable and L/K is modular. In order to show L/K and $L/\bar{K}$ are Galois, it suffices to show $L/\bar{K}$ is Galois by Corollary (2.4) since $\bar{K}/K$ is obviously Galois. Let $Z = \{z_i | i = 1, 2, \ldots\}$ and $Z^{p^{-\infty}} = \{z_i^{p^{-j}} | i, j = 1, 2, \ldots\}$. Let $M = L(Z^{p^{-\infty}})$. Then $P(Z^{p^{-\infty}})$ is the maximal perfect subfield of M [6, Lemma 11, p. 392]. Hence

$$\bigcap_i \bar{K}(L^{p^i}) \subseteq \bigcap_i P(Z^{p^{-\infty}})(M^{p^i}) = P(Z^{p^{-\infty}}).$$

Thus $\bigcap_i K(L^{p^i})$ is algebraic over $\bar{K}$ and so is equal to $\bar{K}$. We now show L/K does not split. We first show $\bigcap_i K(y)(L^{p^i}) = K(y, u_0^p)$. Clearly $K(y, u_0^p) \subseteq \bigcap_i K(y)(L^{p^i})$. Now $\{u_0, u_1^{p^{-1}}, \ldots, u_n^{p^{-n}}, \ldots\}$ is a subbasis of $L/K(y, u_0^p)$. Hence

$$\bigcap_i K(y, u_0^p)(L^{p^i}) = K(y, u_0^p).$$

Thus $\bigcap_i K(y)(L^{p^i}) = K(y, u_0^p)$. Suppose L/K does split, say $L = S \otimes_K \bar{K}$, where S is an intermediate field with S/K separable. Let y have exponent t over S. Now $y^{p^t} \notin K = \bigcap_i K(S^{p^i})$. Hence there is a nonnegative integer s such that $y^{p^t} \in K(S^{p^s}), y^{p^t} \notin K(S^{p^{s+1}})$. Suppose $y^{p^{t-1}} \in \bar{K}(S^{p^s})$. Then

$$y^{p^t} \in \left(K(S^{p^{s+1}}) \otimes_K K(\bar{K}^p)\right) \cap \left(K(S^{p^s}) \otimes_K 1\right) = K(S^{p^{s+1}}),$$

a contradiction. Hence y has exponent t over $\bar{K}(S^{p^s})$. Thus $K(S^{p^s})(y)$ and $\bar{K}(S^{p^s})$ are linearly disjoint over $K(S^{p^s})$. Since $K(S^{p^s})$ and $\bar{K}$ are linearly disjoint over K, $K(S^{p^s})(y)$ and $\bar{K}$ are linearly disjoint over K. Since $\bar{K} \supset K^{p^{-1}}$, $K(S^{p^s})(y)$ is separable over K. Let $S' = K(S^{p^s})(y)$. Then $L = K(L^{p^s})(y) = S' \otimes_K \bar{K}$ and $y \in S'$. Since $\{y\}$ must be a relative p-basis of S'/K and S'/K is separable, $S'/K(y)$ is separable. Hence $L = S' \otimes_{K(y)} \bar{K}(y)$. Now

$$K(y, u_0^p) = \bigcap_i K(y)(L^{p^i}) = \bigcap_i \left(K(y)(S'^{p^i}) \otimes_{K(y)} K(y)(\bar{K}^{p^i})\right) = S'.$$

Hence $L = \bar{K}(y, u_0^p)$, a contradiction. Thus L/K does not split.

REFERENCES

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

2. ______, *On Galois theory using pencils of higher derivations*, Proc. Amer. Math. Soc. **72** (1978), 233–238.

3. N. Heerema, *Higher derivation Galois theory of fields*, Trans. Amer. Math. Soc. (to appear).

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

5. H. Kreimer and N. Heerema, *Modularity vs. separability for field extensions*, Canad. J. Math. **27** (1975), 1176–1182.

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

7. J. Mordeson, *On a Galois theory for inseparable field extensions*, Trans. Amer. Math. Soc. **214** (1975), 337–347. MR **52** #5635.

8. 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.

9. W. Waterhouse, *The structure of inseparable field extensions*, Trans. Amer. Math. Soc. **211** (1975), 39–56. MR **52** #359.

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

Department of Mathematics, Creighton University, Omaha, Nebraska 68134