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 \( F = K(L^p) \) 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 \( K \), \( K \) 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 \( d = \{d_i|0 < i < t + 1\} \) of additive maps of \( L \) into \( L \) such that

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

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 \( f_j = \sum \{d_me_n|m + n = j\} \). 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 \( f = p \) (rank \( d \)), \( f_{ji} = d_i \) and \( f_j = 0 \) if \( p \nmid j \). Two higher derivations \( f \) and \( g \) are equivalent if \( g = v'(f) \) or \( f = v'(g) \) for some \( i \). The equivalence class of \( d \) is \( \overline{d} \) and is called the pencil of \( d \). The set of all pencils, \( \overline{H}(L/K) \), can be given a group structure by defining \( \overline{df} \) to be the pencil of \( d'f' \) where \( d' \in \overline{d}, f' \in \overline{f} \) 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 \( \cap \overline{K}(L^p) = K \) [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 \( F = K(L^p) \) for some nonnegative integer \( r \). This generalizes the result given in [2, Theorem 8] for the bounded exponent finite transcendence degree case.

Let \( K \) 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.


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

© 1979 American Mathematical Society

0002-9939/79/0000-0200/$02.75

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
[\mathbb{K} : \mathbb{K^p}] < \infty \text{ (and in this case } L/K \text{ splits). In view of these results it appeared that } \mathbb{K} \text{ being Galois in } L \text{ was related to } L/K \text{ splitting. However, an example is constructed with } L/K \text{ and } L/\overline{K} \text{ both Galois and yet } L/K \text{ 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} \text{ (} L/\overline{K} \text{ being separable). However, in the proof of Theorem 2.2, an example of a Galois extension is constructed with } L/\overline{K} \text{ 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 \supseteq K \text{ be Galois subfields of } L. \text{ This section develops necessary and sufficient conditions for } H(L/F) \text{ to be } H(L/K)-\text{invariant.}

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

Proof. Suppose some } c \text{ in } L \text{ has } c^{p^i} \text{ in } F^* \text{ but not in } K(K^{p^{-1}} \cap L^{p^{i+1}}). \text{ 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} \text{ is not in } K(L^{p^{i+1}}). \text{ For } j < i, c^{p^j} \text{ cannot be in } K(L^{p^{i+1}}). \text{ Thus } c \text{ is pure independent [9] and is part of a maximal pure independent set of } L/K. \text{ But } c \text{ has exponent } i + 1 \text{ over } K \text{ and exponent } i \text{ over } F^*, \text{ 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 \( F^* = K(F^* \cap L^p) = \cdots = K(F^* \cap L^{p^r}) = \ldots. \) 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 \text{ is purely inseparable Galois. Let } F \text{ be an intermediate field of } L/K \text{ such that } L/F \text{ is modular and } F \cap L^{p^r} \subseteq K \text{ for some nonnegative integer } n. \text{ If for every maximal pure independent set } M \text{ of } L/K \text{ every element of } M \text{ has the same exponent over } F \text{ that it has over } K, \text{ 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. \text{ Let } K \subseteq F \text{ be Galois subfields of } L. \text{ Then } H(L/F) \text{ is } H(L/K)-\text{invariant if and only if } F = K(L^{p^r}) \text{ for some nonnegative integer } r.
Proof. If \( F = K(L^p) \) for some \( r \), then \( \bar{H}(L/K) \) leaves \( F \) invariant. Hence clearly \( \bar{H}(L/F) = \bar{H}(L/K) \)-invariant. Conversely, suppose \( \bar{H}(L/F) = \bar{H}(L/K) \)-invariant. We prove the theorem first for the case \( p > 3 \). Suppose \( \bigcap_j K(F \cap L^{p^j})(L^{p^j}) = F \) for all nonnegative integers \( j \). Then

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

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

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

Then \( \bigcap_j K_j(L^{p^j}) = K_j \) 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 \( \bar{H}(L/F) \) is invariant in the smaller group \( \bar{H}(L/K_j) \). Now \( F/K_j \) is purely inseparable of bounded exponent. By [8, Lemma 1.61(c), p. 56], \( F/K_j \) is modular. Also \( F \cap L^{p^n} \subset K_j \) for some \( n \), namely \( n = j \). Hence \( F \cap \bar{F}^{p^r} \subset K_j \). By Lemma 1.2, there exists a maximal pure independent set \( X \) of \( \bar{F}/K_j \) 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 \( \bar{F}/F \). Suppose \( \bar{F}/F \) is of unbounded exponent. If \( F(Y)/F \) is of bounded exponent, then \( \bar{F} = J \otimes_F F(Y) \) for some intermediate field \( J \) of \( \bar{F}/F \) [9, Proposition 2.6, p. 43]. Since \( Y \) is necessarily a relative \( p \)-basis of \( \bar{F}/F, J/F \) is relatively perfect. Hence \( \bigcap_i F(\bar{F}^{p^i}) = J \supset F \), 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 \( L/\bar{F} \) is modular, \( L/\bar{F} \) is separable and thus preserves \( p \)-independence. It follows that there exists \( d = \{d_0, d_1, \ldots, d_{p^r}\} \in H(L/K_j) \) and \( d' = \{d_0', d_1', \ldots, d_{p^r}'\} \in H(L/F) \) 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 \( \bar{H}(L/F) = \bar{H}(L/K_j) \)-invariant, \( d \cdot d' \) restricted to \( F \) must be the identity higher derivation, i.e. \( d' d = d \) when restricted to \( F \). Suppose \( (q + q')p^t < p^e \). Then

\[
(d'd)_{(q+q')p^t}(x^{p^t}) = \sum \left\{ d'_i d_{(q+q')p^t-i}(x^{p^t}) | 0 < i < (q + q')p^t \right\}
= \sum \left\{ d'_j (d_{q+q'-j}(x))^{p^t} | 0 < j < q + q' \right\}
= d_{(q+q')p^t}(x^{p^t}) + d_{q'}(y)^{p^t}
\neq d_{q+q'}(x^{p^t}), \text{ a contradiction}.
\]

Thus \((q + q')p^t > p^e \), so \( p^{e-s} + p^{e-u} + 2 > p^{e-t} \). Hence \( p^{e-s} + p^{e-u} + 2p^{e-t} > p^{e-t} \). Since we can take \( e \) as large as we wish, we have \( p^{e-s} + p^{e-u} > p^{e-t} \) so \( p^{t-s} + p^{t-u} > 1 \). Since \( s - t > 1 \) and \( u - t > 2 \), we have \( p^{t-s} + p^{t-u} > p^{t-s} + p^{t-u} \), i.e., \( 2 > p \), a contradiction. Thus \( \bar{F}/F \) has bounded exponent so \( L/K_j \) has finite inseparability exponent. Suppose \( \bar{F} \subset L \). Then as in the proof of [2, Theorem 8], we obtain \( F = K_j \) a contradiction. Hence \( \bar{F} = L \).
Thus $L/F$ has bounded exponent so $L \supseteq F \supseteq K(L^{p^n})$ for some $n$. Now $\bar{H}(L/F)$ is $\bar{H}(L/K(L^{p^n}))$-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, Lemma, p. 277] and in particular [1, Lemma, p. 278]. Here, for large $e$ the key inequality becomes $2p^{e-1} + 2p^{e-1} > p^e$. Since $\gamma$ 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 $\cap_i K(L^{p^n}) = K$. Then certainly $\cap_i K(\bar{K}(L^{p^n})) = K$ and since $\bar{K}$ is modular over $K$, $\bar{K}$ is a Galois extension of $K$. Moreover $L/\bar{K}$ is separable (hence modular) so $L/\bar{K}$ will be Galois if and only if $\cap_i \bar{K}(L^{p^n}) = \bar{K}$. We now investigate conditions which will guarantee $L/\bar{K}$ is Galois.

(2.1) Proposition. Suppose $K$ is a Galois subfield of $L$. If $L/K$ splits, then $K$ is Galois in $L$.

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

(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 $L$, $K$ is Galois in $L$.

Proof. Suppose $[K : K^p] < \infty$. Let $L/K$ be Galois. Then $\cap_i K(\bar{K}(L^{p^n})) = K$ and since any relative $p$-basis of $\bar{K}/K$ is finite, we have $\bar{K}/K$ 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 $x_1, x_2, \ldots, x_{2^{n-1}}, \ldots$ be $p$-independent in $K$. Let

$L = K\left(z, z^{p^n-1} + x_1^{p^n-2}, \ldots, z^{p^n-1} + x_1^{p^n-2} + x_2^{p^n-3} + \cdots + x_{2n-1}^{p^n-2n} + \ldots\right)$

where $z$ is transcendental over $K$. Then

$\bar{K} = K\left(x_1^{p^n-1}, x_2^{p^n-2}, \ldots, x_{2n-1}^{p^n-2n+1}\right)$.

Since $L/\bar{K}$ is a union of ascending chain of separable extensions of $\bar{K}$, $L/\bar{K}$ is separable. Now $\bar{K}(L^{p^n}) = L$ so $\bar{K}$ is not Galois in $L$. Clearly $\bar{K}/K$ 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 $\cap_i K(L^{p^n}) = K$. Now \(\{z^{p^n} + x_1^{p^n-1} + \cdots + x_{2n-1}^{p^n-2n}|n = 1, 2, \ldots\}\) is a subbasis of $L/K(z)$. Hence $\cap_i K(z)(L^{p^n}) = K(z)$. Let $K^* = \cap_i K(L^{p^n})$. Since $\cap_i K^*(L^{p^n}) = K^*$, $K^*$ is separably algebraically closed in $L$. Clearly $K^* \subseteq K(z)$. Suppose $K^* \neq K$. Then $K(z)/K^*$ is algebraic and thus $K^* = K(z^{p^n})$ for some nonnegative integer $e$. Now $z^{p^e} \in K(L^{2p^{2e+1}})$. Therefore

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

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

```
```

we have \( x_{2e+1}^2 \in K(Lp^{2e+1}) \cap \bar{K} = K(Kp^{2e+1}) \) 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 a 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, \( L/K \) 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 \( L/K \) 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 \( F/K(Kp^i) \) is modular, \( L/K(Kp^i) \) is modular, \( i = 0, 1, \ldots \). Hence \( L/\cap_i K(Kp^i) \) 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 \( F \cap K(Lp^i) = K(Fp^i) \). Clearly \( \cap_i K(Lp^i) \subseteq F \). Thus

\[
\cap_i K(Lp^i) = \cap_i K(Lp^i) \cap F = \cap_i K(Fp^i) = K.
\]

\((2.4)\) Corollary. If \( L/\bar{K} \) and \( \bar{K}/K \) are Galois, then \( L/K \) is Galois.
PROOF. $L/K$ is separable since $L/ar{K}$ is modular and $\bar{K}$ is algebraically closed in $L$.

(2.5) Example. $L/K$ and $L/ar{K}$ are Galois, yet $L/K$ does not split: Let $K = P(z^p, \ldots, z^p)$ and $$L = K(z_1, \ldots, z_i^{p^{-1}}, \ldots)(y, u_0, \ldots, u_i^p, \ldots)$$ where $P$ is a perfect field, $y, u_0, z_1, \ldots, z_i, \ldots$ are algebraically independent indeterminants over $P$ and $u_i^p = y_i^{p^{-1}} + z_i^{p^{n+1}}u_{i-1}^p, n = 1, 2, \ldots$. Then $\bar{K} = K(z_1, \ldots, z_i^{p^{-1}}, \ldots)$. Now $\bar{K}(y, u_0^p), n = 0, 1, \ldots$, is an ascending chain of separable extensions of $K$ 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 $Z^{p^{-1}} = \{z_i^{p^{-1}}| i = 1, 2, \ldots\}$. Then $L = M(Z^{p^{-1}})$.

Let $\bigcap_i \bar{K}(L^{p^i}) \subseteq \bigcap_i P(Z^{p^{-1}})(M^{p^i}) = P(Z^{p^{-1}})$.

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 $\bigcap_i K(y)(L^{p^i}) = K(y, u_0)$. Clearly $K(y, u_0) \subseteq \bigcap_i K(y)(L^{p^i})$. Now $u_0, u_0^{p^{-1}}, \ldots, u_0^{p^{-n}}, \ldots$ is a subbasis of $L/K(y, u_0)$.

Hence

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

Thus $\bigcap_i K(y)(L^{p^i}) = K(y, u_0)$. 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 $y^{p^t} \in K = \bigcap_i K(S^{p^i})$. Hence there is a nonnegative integer $s$ such that $y^{p^t} \in K(S^{p^s}), y^{p^t} \not\in K(S^{p^s+1}).$ Suppose $y^{p^t-1} \in \bar{K}(S^{p^s})$. Then

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

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

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

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

REFERENCES


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

Department of Mathematics, Creighton University, Omaha, Nebraska 68134