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 $K(L^p')$ has a finite separating transcendence basis over $K$ for some nonnegative integer $e$. If $p \neq 2, 3$ and $K(L^p')$ 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 $F = K(L^p')$ 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 $d = \{d_i|0 < i < t\}$ 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 $f_j = \sum d_i e_n| m + n = j$. 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 $f = p(rank \, d)$, $f_{pi} = d_i$ and $f_i = 0$ if $p \mid j$. 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 $\bar{d}$ and is called the pencil of $d$. The set of all pencils, $\bar{H}(L/K)$, can be given a group structure by defining $\bar{d}f'$ to be the pencil of $d'f'$ where $d'$ is in $\bar{d}$, $f'$ is in $\bar{f}$ and rank $d' = \text{rank } f'$. 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 $K(L^p')$ has a finite separating transcendence basis over $K$ for some nonnegative
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 \( \bar{d} \in H \). 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 \( L/k(L^{p^n}) \) 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

\[
\bigcap_i \left( \bigcap_n Q^*(L^{p^n}) \right)(L^{p^n}) = \bigcap_n Q^*(L^{p^n}),
\]

\( \bigcap_n Q^*(L^{p^n}) \) 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, $M = \cap_n M(L^{p^n}) \supseteq \cap_n Q^*(L^{p^n})$.

In view of [4, Theorem 1.6] it would be tempting to conjecture that $\cap_n Q^*(L^{p^n})$ is relatively perfect over $Q^*$. However, examples given by Waterhouse [9] indicate that $\cap_n Q^*(L^{p^n})$ 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, $F = \cap_n F(L^{p^n})$ 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 $L = F(B) = \cup_i B_i$ where every element of $B_i$ is of exponent $i$ over $F$ and for any positive integer $n$ there exists $i > n$ such that $B_i \neq \emptyset$. Let $x_i \in B$ be such that $x_i$ has exponent $i$ over $F$, $i < i_{i+1}$, $1 \leq j < \infty$. Set

$$\hat{F} = F \left( B \setminus \{ x_i \} , x_i - x_i^{p^{n-i}}, \ldots , x_i - x_i^{p^{n+1-i}} , \ldots \right).$$

Then

$$L = \hat{F}(x_i, x_i, \ldots , x_i, \ldots) = \hat{F}(x_i, x_i, \ldots , x_i, \ldots) = \ldots .$$

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 $K = P(z, y, x_1, x_2, \ldots , x_n, \ldots)$ where $P$ is a perfect field and $z, y, x_1, \ldots , x_n, \ldots$ are algebraically independent indeterminants over $P$. Let
\[ L = K \left( z^{p^{-2}} x^{p^{-1}} + y^{p^{-1}}, \ldots, z^{p^{-n}} x^{p^{-1}} + y^{p^{-1}}, \ldots \right). \]

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 \( \leq 1 \).

**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 \( K(L^p) \) 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 transcendence 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 \( K(L^p) \) has a finite separating transcendence basis for some \( e \).

Conversely, suppose \( K(L^p) \) 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 \( F(L^p) \) has a finite separating transcendence basis over \( F \) for some \( n \), hence \( L = F \otimes_F R \) where \( R/F \) is regular and has a finite separating transcendence basis and \( F/F \) 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, \( \bigcup_n H_n(L/K) = \overline{H}(L/K) \).

**Proof.** Define \( \Phi: H_n(L/K) \to \overline{H}(L/K) \) by \( \Phi(d) = \overline{d} \) for all \( d \in H_n(L/K) \). Clearly \( \Phi \) is a homomorphism. Suppose \( \Phi(d) = \Phi(f) \), i.e. \( \overline{d} = \overline{f} \). 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 \( \Phi \) is 1-1. Let \( \overline{f} \in H_n(L/K) \). Then there exists \( d \in H_n(L/K) \) such that \( \overline{d} = \overline{f} \). Now \( v(d) \in H_{n+1}(L/K) \) and
\[ \tilde{f} = \tilde{d} = v(\tilde{d}) \in H_{n+1}(L/K), \text{ so } H_n(L/K) \subseteq H_{n+1}(L/K). \] Clearly \[ \bigcup_n H_n(L/K) = \overline{H}(L/K). \]

We note that by Lemma 7 and the definition of multiplication, a subgroup \( \overline{H}(L/F) \) of \( \overline{H}(L/K) \) 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. \( \overline{H}(L/F) \) is \( \overline{H}(L/K) \) invariant.
2. \( F = K(L^{p^r}) \) for some \( r \).

**Proof.** If \( F = K(L^{p^r}) \), then \( F \) is invariant under \( \overline{H}(L/K) \) and hence \( \overline{H}(L/F) \) is \( \overline{H}(L/K) \) invariant.

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

Since \( \overline{F} \neq L \), \( Y \neq \emptyset \). Suppose \( X \neq \emptyset \). 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:

\[
\begin{align*}
d_i(z) &= 0 \quad \text{for all } z \in Z, i > 1, \quad f_i(z) = 0 \quad \text{for all } z \in Z, i > 1, \\
d_i(x_0) &= y_0, \quad d_i(x_0) = 0, i > 1, \quad f_i(y_0) = 0, i > 1, \\
d_i(s) &= 0 \quad \text{for all } s \in X \cup Y \setminus \{x_0\}, i > 1, \\
f_i(s) &= 0 \quad \text{for all } s \in X \cup Y \setminus \{y_0\}, i > 1.
\end{align*}
\]

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

\[
(fd)_{2p^e}(x_0^p) = \sum_{i=0}^{2p^e} f_i d_{2p^e-i}(x_0^p) = \left[ \sum_{j=0}^{2} f_j d_{2-j}(x_0) \right]^{p^e} = d_{2p^e}(x_0^p).
\]

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

\[
K(L^{p^e})(F) = K(L^{p^e})(L^{p^e}) = K(L^{p^e})
\]

or
$K(L^p)(F) \subseteq K(L^{p^r})(L^p)$ for all $e$,

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

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

References


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

Department of Mathematics, Creighton University, Omaha, Nebraska 68131