INVARIANT SUBGROUPS
OF GROUPS OF HIGHER DERIVATIONS
JAMES K. DEVENEY AND JOHN N. MORDESON

Abstract. Let L be a field of characteristic $p > 3$. A subgroup $G$ of the

group $D$ of all rank $p^r$ higher derivations on $L$ is Galois if $G$ is the group of

each $d$ in $D$ having a given subfield in its field of constants. The field of

constants of $G$ is denoted as $L^G$. The main result states: Let $H \subseteq G$ be

Galois subgroups of $D$. Then $H$ is an invariant subgroup of $G$ if and only if

either $L^H = L^G(L^{p^r})$ for some nonnegative integer $r$, or $L^H \subseteq L^G(L^{p^r})$.

Let $L$ be a field of characteristic $p \neq 0$. A rank $p^r$ higher derivation on $L$ is

a sequence of additive maps $d = \{d_0, d_1, \ldots, d_{p^r}\}$ such that $d_r(ab) = \Sigma (d_r(a)d_r(b))i + j = r$ and $d_0$ is the identity map. Let $D$ be the group of all

rank $p^r$ higher derivations on $L$ where the group operation is defined by

d \circ e = f$ where $f_r = \Sigma (d_r(e))i + j = r$. For $G$ a subset of $D$, its field of

constants is \{ $a \in L | d_r(a) = 0, r > 0, d \in G$ \} and will be denoted by $L^G$. A

subgroup $G$ of $D$ is Galois if it is the group of all higher derivations which are

trivial on $L^G$. For $F$ an intermediate field of $L/L^G$, we let $D^F$ denote the

group of all those $d \in D$ whose field of constants contains $F$. For $H$ and $G$

subgroups, $H$ is $G$-invariant if $d^{-1}d'd \in H$ for all $d' \in H, d \in G$. The

following is the main result.

Theorem. Suppose $p > 3$. Let $H \subseteq G$ be Galois subgroups of $D$. Then $H$ is

$G$-invariant if and only if either $L^H = L^G(L^{p^r})$ for some nonnegative integer $r$, or $L^H \subseteq L^G(L^{p^r})$.

This result can be immediately applied to [3, Theorem 1, p. 338] to give a

necessary and sufficient condition concerning group invariance for the inseparable Galois theory developed by Heerema [2]. For the purely inseparable finite dimensional case, [1, Theorem (3.1), p. 289] shows that $H$ being

$G$-invariant is not equivalent to $L^H$ being invariant under elements of $G$, unless $L$ is of exponent less than $e + 1$ over $L^G$. However, even in this case when $G/H$ acts as a group of higher derivations on $L^H$, it will in general not be a Galois group [1, Theorem (3.4), p. 289], although the field of constants of the restrictions to $L^H$ of $G$ will be $L^G$ [1, 2.5(c), p. 289]. It seems interesting that in the case where $L/L^G$ is of exponent less than $e + 1$, $G$ will have only

Received by the editors April 19, 1977 and, in revised form, August 29, 1977.


Key words and phrases. Purely inseparable field extension, higher derivation, Galois group of

higher derivations.

© American Mathematical Society 1978
a finite number of normal Galois subgroups. We note that $L/L^G$ is modular and hence has a subbasis [4, Theorem 1, p. 403] since $L/L^G$ is of exponent less than or equal to $e + 1$. We frequently use the fact that a higher derivation on $L$ is uniquely determined by its action on a $p$-basis for $L$ [1, (2.1), p. 264]. We also assume $e > 0$, since in the case $e = 0$, $D$ is commutative and the Theorem is obvious.

**Lemma.** Let $H \subseteq G$ be Galois subgroups of $D$. Suppose there exist $m_1$, $m_2$ in $L$ such that $m_1$ is in a subbasis $M_1$ of $L/L^G$, $m_2$ is in a subbasis $M_2$ of $L/L^H$, and $t_1 < \min\{t_1, t_2, e\}$, where $t_1, s_1$ are the exponents of $m_1$ over $L^H$, $L^G$, respectively, and $t_2$ is the exponent of $m_2$ over $L^H$. Suppose $H$ is $G$-invariant. Then $p = 2$ or $p = 3$.

**Proof.** Define $d = \{d_0, \ldots, d_p\}$ and $d' = \{d'_0, \ldots, d'_p\}$ in $D$ as follows:

- $d_i(b) = 0$, $i = 1, \ldots, p^s$, for all $b \in M_1 - \{m_1\}$,
- $d_i(m_1) = 0$, $i = 1, \ldots, q - 1, d_q(m_1) = m_2$,
- $d'_i(b) = 0$, $i = 1, \ldots, p^s$, for all $b \in M_2 - \{m_2\}$,
- $d'_i(m_2) = 0$, $i = 1, \ldots, q - 1, d'_q(m_2) \neq 0$,

where $q = p^{e-s_1} + 1$ if $s_1 < e + 1$ and $q = 1$ if $s_1 = e + 1$, $q' = p^{e-t_1} + 1$ if $t_2 < e + 1$ and $q' = 1$ if $t_2 = e + 1$.

Suppose $t_1 < e + 1$. Then $d'_i(m_2^{p_s}) = (d'_j(m_2))^{p'_j}$ if $i = j p'_j$ for some $j$ and $d'_i(m_2^{p_s}) = 0$ otherwise [6, p. 436]. Suppose $i = j p'_j$ for some $j$. Then $j p'_j \leq p^e$ so $j < p^{e-t_1} < q'$. Thus $d'_i(m_2^{p_s}) = 0$. Hence $d' \in H$. Similarly, $d \in G$ if $s_1 < e + 1$. If $t_2 < e + 1$ or $s_1 = e + 1$, then it follows easily that $d' \in H$ and $d \in G$.

Now $p^{r_i}$ divides both $i$ and $(q + q') p^{r_i} - i$ if and only if $i = r p^{r_i}$, $r = 0, 1, \ldots, q + q'$. Assume $(q + q') p^{r_i} - i$. Then

$$
\sum \left\{ d'_i d_{(q+q') p^{r_i} - i} (m_1^{p^{s_i}}) \right\} = \sum \left\{ (d'_n d_{(q+q') - n} (m_1)) p^{s_i} \right\} = d_{(q+q') p^{r_i}} (m_1^{p^{s_i}}) + (d'_q (d_q (m_1))) p^{s_i} + d'_{(q+q') p^{r_i}} (m_1^{p^{s_i}}).
$$

Since

$$
d'_{(q+q') p^{r_i}} (m_1^{p^{s_i}}) = 0 \quad \text{and} \quad (d'_q (d_q (m_1))) p^{s_i} \neq 0,
$$

we have that $d'd \neq d$ on $L^H$, a contradiction. Thus $(q + q') p^{r_i} > p^e$. A routine solution of this inequality yields $p = 2$ or $p = 3$.

**Proof of the Theorem.** Suppose $L^H = L^G(L^p)$. By [1, Theorem 1, p. 289], $L^H$ is invariant under $G$. Hence, clearly $H$ is $G$-invariant. Suppose $L^H \subseteq L^G(L^p)$. Since the pairs $L^p$, $L^G$ and $L^p$, $L^H$ are linearly disjoint, it follows that there exists a subset $B$ of $L$ such that $L^H = L^G(B^p)$. Let $d' = \{d'_0, \ldots, d'_p\} \in H$ and $d = \{d_0, \ldots, d_p\} \in G$. For any $b \in B$ and $j = 1, \ldots, p^r - 1$,

$$
d_j(b^{p^r}) = 0 \Rightarrow \sum \left\{ d'_i d_{j-i} (b^{p^r}) \right\} \leq \sum \left\{ d_i d_{j-i} (b^{p^r}) \right\} \leq \sum \left\{ d_i d_{j-i} (b^{p^r}) \right\}
$$
INVARIANT SUBGROUPS

since $p^r$ does not divide $j$ [6, p. 436]. Now

$$\sum \{ d_i d_{p-i}(b^{p^r})|0 < i < p^r\} = d_{p^r}(b^{p^r}) + d_{p}(b^{p^r}) = d_{p^r}(b^{p^r}).$$

Thus $d'd = d$ on $L^H$, so $H$ is $G$-invariant.

If $L = L^H$ or $L^H = L^G$, the result is immediate. Hence assume $L \supset L^H \supset L^G$ (strict inclusion). Since $L$ is modular over $L^H$ and $L^G(L^p)$, $L$ is modular over $L^H \cap L^G(L^p)$ [5, Theorem 1.1, p. 39]. Set

$$G' = D^{L^H \cap L^G(L^p)}.$$ 

Then $G'$ is a Galois subgroup of $D$, $L^G' = L^H \cap L^G(L^p)$, $H \subseteq G' \subseteq G$, and $H$ is $G'$-invariant. Suppose $L^H \subseteq L^G(L^p)$. Then $L^G' \subseteq L^H$ and $L^H \supseteq L^G(L^p)$. Let $s$ denote the exponent of $L/L^G$. Suppose for all $m_2$ in $L$ of exponent $s$ over $L^G$, that $m_2^{p^{s-1}} \not\in L^H$. Then for such an $m_2$, $m_2$ has maximal exponent over $L^H$, so $m_2$ is in a subbasis of $L/L^H$. There exists a subbasis of $L/L^G$ which contains an element $m_1$ such that the exponent $t_1$ of $m_1$ over $L^H$ is the exponent $s_1$ of $m_1$ over $L^G$ [3, Lemma 3, p. 340]. Since every element of $L$ with exponent $s$ over $L^G$ also has exponent $s$ over $L^H$, we have $t_1 < s_1 < s = t_2 < e + 1$. Hence $t_1 < e$. Thus by the Lemma, $H$ is not $G'$-invariant, a contradiction. Hence there exists $m$ in $L$ of exponent $s$ over $L^G$ such that $m^{p^{s-1}} \in L^H$. Let $m_1$ be such an element. Then $m_1$ is in a subbasis of $L/L^G$ and the exponent $t_1$ of $m_1$ over $L^H$ is the exponent $s_1$ of $m_1$ over $L^G$. Now $t_1 < e$ and if $t_1 = e$, then

$$m_1^{p^{t_1}} \in L^H \cap L^G(L^p) = L^G,$$

a contradiction. Thus $t_1 < e$. Suppose there exists $m_2$ in $L$ of exponent $s$ over $L^G$ such that $m_2^{p^{s-1}} \not\in L^H$. Then $m_2$ is in a subbasis of $L/L^H$ and $t_1 < s = t_2$. Thus by the Lemma, $H$ is not $G'$-invariant, a contradiction. Hence for all $m_2$ in $L$ of exponent $s$ over $L^G$, $m_2^{p^{s-1}} \in L^H$. Thus $L^G(L^{p^{s-1}}) \subseteq L^H$.

We now conclude the proof by induction on the exponent of $L/L^G$. If the exponent of $L/L^G$ is 0, then the result is immediate. Suppose

$$L^H = L^G(L^p) \text{ or } L^H \subseteq L^G(L^p)$$

whenever $H \subseteq G^*$ are Galois subgroups of $D$ such that $H$ is $G^*$-invariant and the exponent of $L/L^{G^*} < n (n > 1)$. Let $H \subseteq G$ be Galois subgroups of $D$ such that $H$ is $G$-invariant and $L/L^G$ has exponent $n$. If $L^H \subseteq L^G(L^p)$, we have the desired result. Suppose $L^H \subseteq L^G(L^p)$. Let $s$ denote the exponent of $L/(L^H \cap L^G(L^p))$. Then by the preceding paragraph, $L^G(L^{p^{s-1}}) \subseteq L^H$. Now $s - 1 < n$ and $L/L^G(L^{p^{s-1}})$ is modular. Let $G^*$ be the Galois subgroup of $D$ with field of constants $L^G(L^{p^{s-1}})$. Then $H$ is $G^*$-invariant, and by the induction hypotheses,

$$L^H = L^G(L^{p^{r-1}})(L^p)$$

for some $r$, or

$$L^H \subseteq L^G(L^{p^{r-1}})(L^p).$$

Suppose $L^H \subseteq L^G(L^{p^{r-1}})(L^p)$. Since $s - 1 < e + 1$, we have
Suppose $L^H = L^G(L^{p^{r-1}})$. Then $L^H = L^G(L^{p^{r-1}})$ or $L^H = L^G(L^p)$.

In the following example, we show that for small $p$ it is possible for $H$ to be $G$-invariant without $L^H = L^G(L^p)$ for some $r$ or $L^H \subseteq L^G(L^p)$.

Example. Let $L = P(x, y)$ where $P$ is a perfect field of characteristic $p = 2$ or $3$ and $x, y$ are independent indeterminates over $P$. Let $G$ and $H$ be the Galois subgroups of $D$ (with $e = 2$) corresponding to $P(x^p, y^p)$ and $P(x^p, y^p)$, respectively. Since $d_i = 0$ for any $d = (d_0, d_1, \ldots, d_r) \in G$, an easy computation shows $d'd = d$ on $L^H$ for all $d' \in H$.

REFERENCES