ON HIGH ORDER DERIVATIONS OF FIELDS

J. N. MORDESON AND B. VINOGRADE

Abstract. Let $\mathcal{D}(L/K)$ denote the derivation algebra of a field extension $L/K$ of prime characteristic. If $L/K$ is purely inseparable and has an exponent, then every intermediate field $F$ of $L/K$ equals the center of $\mathcal{D}(L/F)$. Here we prove the converse of this statement.

Let $\mathcal{D}_0(L/K)$ denote the derivation algebra of a field extension $L/K$ where $\mathcal{D}_0(L/K)$ is the set of all high order derivations of $L/K$ [3, pp. 1 and 6]. In [4, p. 19, Theorem 3], it is shown that if $L/K$ is purely inseparable and has an exponent, then $F=Z(\mathcal{D}(L/F))$ for every intermediate field $F$ of $L/K$ where $Z(\mathcal{D}(L/F))$ denotes the center of $\mathcal{D}(L/F)$. This result permits a Galois correspondence between the intermediate fields of $L/K$ and closed subrings of $\mathcal{D}(L/K)$ containing $L$. In this note, we show that the converse of this result is true; that is, for an arbitrary field extension $L/K$ of characteristic $p>0$, if $F=Z(\mathcal{D}(L/F))$ for every intermediate field $F$ of $L/K$, then $L/K$ is purely inseparable and has an exponent.

Unless otherwise specified, $L/K$ always denotes a nontrivial field extension of characteristic $p>0$.

Our notation coincides with that in [3] and [4]. The set of $q$th order derivations of $L/K$ into $L$ is denoted by $\mathcal{D}_0(L/K) = \bigcup_{q=1}^{\infty} \mathcal{D}_0^{(q)}(L/K)$. $C_q(L/F)$ denotes the set, $\{x|x \in L$, for all $D \in \mathcal{D}_0^{(q)}(L/F)$, $D(x)=0\}$.

For any intermediate field $F$ of $L/K$, $Z(\mathcal{D}(L/F))$ is an intermediate field of $L/K$ containing $F$ and equals the set $\{x|x \in L$, for all $D \in \mathcal{D}_0(L/F)$, $D(x)=0\}$.

Theorem. The following conditions are equivalent:

1. For every intermediate field $F$ of $L/K$, $F=Z(\mathcal{D}(L/F))$.
2. For every intermediate field $F$ of $L/K$, $F=\bigcap_{i=1}^{\infty} F(L^p)$.
3. For every intermediate field $F$ of $L/K$, every relative $p$-base of $F/K$ is a generating set of $F|K$.
4. $L/K$ is purely inseparable and has an exponent.

Received by the editors July 12, 1971.

AMS 1970 subject classifications. Primary 12F15; Secondary 16A72.

Key words and phrases. High order derivations, field extension, purely inseparable, relative $p$-base.
Proof. (1) $\iff$ (2). This equivalence is immediate once we show that for any $F$, $Z(\mathcal{D}(L/F)) = \bigcap_{i=1}^{\infty} F(L^p)$. Let $x \in \bigcap_{i=1}^{\infty} F(L^p)$. Then, for any $q$ and any $D \in \mathcal{D}_q(L/F)$, $D(x) = 0$ since $F(L^p) \subseteq C_q(L/F)$ by [3, p. 5, Corollary 7.1]. Since $\mathcal{D}_q(L/F) = \bigcup_{q=1}^{\infty} \mathcal{D}_q(L/F)$, we have $x \in Z(\mathcal{D}(L/F))$. Hence $\bigcap_{i=1}^{\infty} F(L^p) \subseteq Z(\mathcal{D}(L/F))$. Let $x \in Z(\mathcal{D}(L/F))$. Then, for any $q$ and any $D \in \mathcal{D}_q(L/F)$, $D(x) = 0$ since $F(L^p) \subseteq C_q(L/F)$ by [3, p. 5, Corollary 7.1]. Since $S > 0(L/F) = \bigcup_{q=1}^{\infty} \mathcal{D}_q(L/F)$, we have $x \in Z(\mathcal{D}(L/F))$. Hence $\bigcap_{i=1}^{\infty} F(L^p) \subseteq Z(\mathcal{D}(L/F))$. Let $x \in Z(\mathcal{D}(L/F))$. If $x \notin \bigcap_{i=1}^{\infty} F(L^p)$, then there exists an $i$ such that $x \notin F(L^p)$. In this case, by [4, p. 18, Theorem 2], there exists $D \in \mathcal{D}_q(L/F)$ (whence $D \in \mathcal{D}_q(L/F)$) such that $D(x) \neq 0$ contrary to the fact that $x \in Z(\mathcal{D}(L/F))$. Thus $x \in \bigcap_{i=1}^{\infty} F(L^p)$ so that $Z(\mathcal{D}(L/F)) \subseteq \bigcap_{i=1}^{\infty} F(L^p)$.

(3) $\iff$ (4). Suppose (3) holds. Let $F$ be any intermediate field of $L/K$ such that $F \supseteq K$ (strict inclusion). Let $M$ be any relative $p$-base of $F/K$. Since $F = K(M)$ and $F \supseteq K$, $M \neq \emptyset$. If $F/K$ is separable, then $M$ is algebraically independent over $K$. In this case, the relative $p$-base $N^{p+1} = \{m^{p+1} | m \in M\}$ of $F/K$ cannot generate $F/K$ else we contradict the algebraic independence of $M$ over $K$. Thus $F/K$ cannot be separable. Hence $L/K$ has no intermediate fields (other than $K$) which are separable over $K$. Thus $L/K$ is purely inseparable. That $L/K$ has an exponent now follows by [1, p. 240, Corollary to Theorem 1] or [2, p. 12, Corollary 1.18]. By [2, p. 2, Corollary 1.6], we have that (4) implies (3).

(2) $\Rightarrow$ (3). Suppose there exists an intermediate field $L'$ of $L/K$ for which there exists a relative $p$-base $M$ such that $L' \supseteq K(M)$. Set $F = K(M)$. Then $L' = F(L^{p^i})$, $i = 1, 2, \ldots$. Thus $L'\in\bigcap_{i=1}^{\infty} L'(L^p) = F(L^p)$, so that $\bigcap_{i=1}^{\infty} F(L^p) = \bigcap_{i=1}^{\infty} L'(L^p) \supseteq L' \supseteq F$, a direct contradiction of (2).

(4) $\Rightarrow$ (2). Immediate. q.e.d.

References


Department of Mathematics, Creighton University, Omaha, Nebraska 68131

Department of Mathematics, Iowa State University, Ames, Iowa 50010