Annals of Mathematics

Determination of the Differentiably Simple Rings with a Minimal Ideal
Author(s): Richard E. Block
Source: *The Annals of Mathematics*, Second Series, Vol. 90, No. 3 (Nov., 1969), pp. 433-459
Published by: Annals of Mathematics
Stable URL: http://www.jstor.org/stable/1970745
Accessed: 07/11/2010 19:03

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/action/showPublisher?publisherCode=annals.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

*Annals of Mathematics* is collaborating with JSTOR to digitize, preserve and extend access to *The Annals of Mathematics.*

STOR®
http://www.jstor.org

# Determination of the differentiably simple rings with a minimal ideal*

By RICHARD E. BLOCK

## 1. Introduction

A central result in ring theory is the Wedderburn-Artin theorem on simple rings: a simple associative ring with DCC on left ideals is a total matrix ring $\Delta_n$ over a division ring $\Delta$. In this paper we consider an analogue of this theorem in which ideals are replaced by differential ideals, these being ideals invariant under all derivations of the ring, and left ideals are replaced by ideals. The main result is a complete determination of the differentiably simple rings with a minimal ideal, in terms of the simple rings. This result (the precise statement will be given shortly) is new even for finite-dimensional associative algebras with a unit. However, the result holds also for completely arbitrary rings, not necessarily associative and not necessarily having a unit element (just differentiably simple with a minimal ideal). In the case of Lie algebras the theorem proves a thirty-year-old conjecture of Zassenhaus. In fact the result leads to the solution of important problems on two very different classes of finite-dimensional non-associative algebras, namely, semisimple Lie algebras (of characteristic $p$) and simple flexible (but not anticommutative) power-associative algebras.

We now give some definitions and notation. If $A$ is a ring and if $D$ is a set of derivations of $A$ (additive mappings $d$ of $A$ into $A$ such that $d(ab) = (da)b + a(db)$ for all $a$, $b$ in $A$) then by a *D-ideal* of $A$ is meant an ideal of $A$ invariant under $D$. The ring is called *D-simple* (*d-simple* if $D$ consists of a single derivation $d$) if $A^2 \neq 0$ and if $A$ has no proper $D$-ideals. Also $A$ is called *differentiably simple* if it is $D$-simple for some set of derivations $D$ of $A$, and hence for the set of *all* derivations of $A$. The same definitions are used for algebras over a ring $K$, the derivations then being assumed to be $K$-linear. Note that when we use the word ring or algebra we do not in general assume, unless stated, that the ring or algebra is associative or has a unit element; however, when we speak of an algebra over a ring, say over $K$, we

* This research was supported by the National Science Foundation under grants GP 5949 through the University of Illinois, GP 6558 through Yale University, and GP 8713 through the University of California, Riverside.

always assume that $K$ is associative with a unit element acting unitally on the algebra.

Jacobson noted (at least in a special case, see [16]) the following class of examples of differentiably simple rings $A$ which are not simple: $A$ is the group ring $SG$ where $S$ is a simple ring of prime characteristic $p$ and $G \neq 1$ is a finite elementary abelian $p$-group (so that $G$ is a direct product of say $n$ copies ($n \geqq 1$) of the cyclic group of order $p$). If $S$ is an algebra over $K$ then $SG$ is also an algebra over $K$. Since the ring or algebra $SG$ depends (up to isomorphism) only on $S$ and $n$, we introduce the notation $S_{[n]}$ for it. We only use this notation when $S$ is simple of prime characteristic. We also let $S_{[0]}$ denote $S$ itself. If $S$ is an algebra over $K$ (so $K = Z$ or $Z_p$ in the ring case) then $S_{[n]}$ may also be written as $S \otimes_K B_{n,p}(K)$ where $B_{n,p}(K)$ denotes the (commutative associative with unit) truncated polynomial algebra $K[X_1, \cdots, X_n]/(X_1^p, \cdots, X_n^p)$ ($p$ the characteristic of $S$). Often one is interested in the case in which $K$ is a field of characteristic $p$, when $B_{n,p}(K)$ is usually just written $B_n(K)$. Note that $S_{[n]}$ *is associative or Lie* etc. *according as S is.*

We now state the most important result of the paper.

MAIN THEOREM. *If $A$ is a differentiably simple ring (or $K$-algebra) with a minimal ideal, then either $A$ is simple or there is a simple ring (or $K$-algebra) $S$ of prime characteristic and a positive integer $n$ such that $A = S_{[n]}$.*

Conversely it is easy to see (and is a special case of results given below) that each $S_{[n]}$ is differentiably simple and has a minimal ideal, in fact a unique minimal ideal. The assumption that $A$ has a minimal ideal cannot be removed, as is shown for example by polynomial and power series rings over a field of characteristic 0.

Posner [11] noted that any differentiably simple ring may be regarded as an algebra over a field (its differential centroid) and so has a characteristic. Three special cases of the theorem above were known. At characteristic 0, where the situation is comparatively uncomplicated, these were due to Posner [11] (the associative case) and Sagle and Winter [15] (the case of finite-dimensional algebras). In the much more complicated characteristic $p$ case, Harper [6] proved the result for finite-dimensional commutative associative algebras over an algebraically closed field $F$ (the result then being $A \cong B_n(F)$), which proved a conjecture of Albert [3]. In the case of finite-dimensional Lie algebras of characteristic $p$ the problem was also studied by Zassenhaus [17] and Seligman [16]. Zassenhaus [17, p. 80] conjectured the result in this case in what we shall show in §6 is an equivalent form.

The above result on the non-simple differentiably simple rings is as mentioned analogous to the Wedderburn-Artin theorem. One aspect of that analogy is that the role of the division rings in that theorem is played here by simple rings, and in the associative case division rings are precisely analogous to simple rings in that they may be characterized as the non-trivial rings with no left ideals. Most of the proof of the Main Theorem (all of it in the characteristic 0 or finite-dimensional associative cases) is valid for a $D$-simple ring $A$ (with minimal ideal) when each operator $d$ in $D$ satisfies a requirement weaker than that of being a derivation, namely $d$ is additive and $[d, t] \in T(A)$ for each $t$ in $T(A)$ where $T(A)$ denotes the ring generated by all right and left multiplications by elements of $A$. We call such an operator $d$ a *quasi-derivation.*

The proof of the Main Theorem occupies §2–§6. The following is an outline of this proof. A key fact proved in §2 is that $A$, as a module for its multiplication algebra, has a composition series with isomorphic factors. Also $A$ has a unique maximal ideal $N$. In §3 it is shown that the centroid $C$ of $A$ is also differentiably simple with a minimal ideal, and that if $C$ contains a subfield $E$ such that $A/N$ is central over $E$ and if $A$ (as an $E$ algebra) contains a subalgebra $S \cong A/N$ with $S + N = A$ then $A \cong S \otimes_E C$; moreover it is essentially shown that such an $S$ exists if $A$ is $d$-simple for some derivation $d$. A proof of the commutative associative case is given in §4, thus determining $C$. In §5 the $d$ used to construct $S$ is shown to exist by proving Theorem 5.2: *if a ring $A$ with a minimal ideal is $D$-simple where $D$ is a set of* (*quasi*)*-derivations closed under addition, commutation and left multiplication by all elements of the centroid then there is a $d$ in $D$ such that $A$ is $d$-simple.* (As a very special case, any differentiably simple ring $A$ with minimal ideal is $d$-simple for some derivation $d$; when $A = B_n(F)$ this gives a result of Albert [3]). In §6 the required field $E$ is constructed, to complete the proof.

In §7 we shall determine the derivation algebra der $S_{[n]}$ of $S_{[n]}$ in terms of der $S$, and give a condition on a set $D$ of derivations of $S_{[n]}$ for $S_{[n]}$ to be $D$-simple.

In §8 we shall consider differentiably semisimple rings and give an analogue of the following Wedderburn-Artin theorem: a semisimple associative ring with DCC on left ideals is a direct sum of simple rings. If $D$ is a set of (quasi)-derivations of a ring $A$ and if $I$ is an ideal of $A$ let $I_D$ denote the (unique) largest $D$-ideal of $A$ contained in $I$. We shall prove in Theorem 8.2 that *if $A$ has* DCC *on ideals and if $A/I$ is a direct sum of simple rings then $A/I_D$ is a direct sum of rings which are $D$-simple* (or more precisely simple with respect to the set of (quasi)-derivations induced on them by $D$). If $A$ is associative and $R$ is the (Jacobson) radical of $A$, then we say that $A$ is $D$-semisimple if $R_D = 0$. As a corollary, *if $A$ is associative and $D$-semisimple with* DCC *on ideals and if $A/R$ has* DCC *on left ideals, then $A$ is a direct sum of $D$-simple rings* (and so is known, in terms of division rings). A similar result holds for alternative rings and a large class of finite-dimensional power-associative rings. We shall also show that this gives a new proof and extension of the theorem of Oehmke [10] that semisimple flexible strictly power-associative algebras are direct sums of simple algebras with a unit. The author has announced elsewhere [4] the determination, by means of the Main Theorem, of the symmetrized algebra $A^+$ for the simple flexible algebras in the finite-dimensional case. At the end of §8 we shall state the generalization of this result to the case of simple flexible rings for which $A^+$ has a minimal ideal.

For (finite-dimensional) Lie algebras of prime characteristic it is not true that $D$-semisimple algebras are direct sums of $D$-simple algebras since it is not even true for semisimple algebras. However in a semisimple Lie algebra $L$ every minimal ideal $I$ is $(\mathrm{ad}_I L)$-simple. This is the basis for the application in §9 of the Main Theorem to obtain a structure theorem for semisimple Lie algebras. The author hopes that ideas connected with the Main Theorem will also prove useful in the determination of the simple Lie algebras.

## 2. Chains of ideals

If $A$ is an algebra over a ring $K$, we denote by $T = T(A)$ the multiplication algebra of $A$, i.e., the (associative) subalgebra of $\mathrm{Hom}_K(A, A)$ (the algebra of all $K$-linear additive mappings of $A$ into $A$) generated by $\{r_x, l_x \mid x \in A\}$ where $r_x$ and $l_x$ are the right and left multiplications $y \mapsto yx$, $y \mapsto xy$, respectively, of $A$ (we do not assume that $1_A \in T$ ($1_A$ the identity operator)). Also we let $C = C(A)$ denote the centroid of $A$, i.e., the centralizer of $T$ in $\mathrm{Hom}_K(A, A)$. If $A^2 = A$ then $C$ is commutative (and associative with 1). If $D$ is a set of derivations of $A$, the *$D$-centroid* of $A$ (*differential centroid* if $D = \mathrm{der}\, A$ (the derivation algebra)) is defined to be the centralizer of $D$ in $C$. If $A$ is $D$-simple then the $D$-centroid is a field; the proof is the same as the usual one for the centroid of a simple algebra. We also note that if $D$ is a set of derivations of an algebra $A$ over $K$ then $A$ is $D$-simple if and only if $A$ is $D$-simple as a ring, again by the usual proof for the case of ordinary simplicity. However for a suitable $K$ there exist $K$-algebras which are differentiably simple as a ring but not as a $K$-algebra, as we shall see in §7 (we require that derivations of a $K$-algebra be $K$-linear). In a $D$-simple $K$-

algebra $A$ the set $\{x \in A \mid T(A)x = 0\}$ is a $D$-ideal and hence is 0. In particular a minimal ideal of $A$ is an irreducible $T(A)$-module. It follows that a minimal ideal of $A$ as a $K$-algebra is also a minimal ideal of $A$ as a ring. Conversely if $A$ is both a $D$-simple ring and a $K$-algebra then a minimal ideal of $A$ as a ring is also a (minimal) ideal of $A$ as a $K$-algebra.

If $d$ is a derivation of the algebra $A$ then $[d, r_x]$ $(= dr_x - r_x d) = r_{dx}$ and $[d, l_x] = l_{dx}$ and hence $[d, T] \subseteq T$. We call a *quasi-derivation* of $A$ any element $d$ of $\mathrm{Hom}_K(A, A)$ such that $[d, T] \subseteq T$. Thus the set qder $A$ of quasi-derivations of $A$ forms the Lie normalizer of $T$ in $\mathrm{Hom}_K(A, A)$. A quasi-derivation for $A$ as an algebra is also a quasi-derivation for $A$ regarded as a ring since $T$ is the same set for $A$ regarded as an algebra or as a ring. The following are examples of quasi-derivations which are not in general derivations.

(1) If $A$ is associative and $I$ is an ideal, then $(r_x \mid I) \in \mathrm{qder}\, I$ for all $x$ in $A$.

(2) If $c \in C(A)$ and $d \in \mathrm{der}\, A$, then $d + c \in \mathrm{qder}\, A$ and $dc \in \mathrm{qder}\, A$ (while $cd \in \mathrm{der}\, A$). The above definitions and facts (about the $D$-centroid etc.) go over for quasi-derivations as well.

LEMMA 2.1. *Let $H$ be an associative algebra over a ring $K$, let $M$ be an $H$-module with a minimal submodule $M_1$, and let $D$ be a subset of* $\mathrm{Hom}_K(M, M)$ *such that $[D, H_M] \subseteq H_M$. If $M_2, \cdots, M_q$ (for some $q \geqq 1$) are submodules of $M$ such that $M_1 \subset M_2 \subset \cdots \subset M_q$ and $M_{i+1}/M_i \cong M_1$ for $i = 1, \cdots, q-1$, and if $d \in D$ such that $dM_q \not\subseteq M_q$, then there is a submodule $M_{q+1}$, with $M_q \subset M_{q+1}$, and an index $j, 1 \leqq j \leqq q$, such that $dM_{j-1} \subseteq M_q$ $(M_0 = 0)$, $dM_j \subseteq M_{q+1}$, and the mapping $m + M_{j-1} \mapsto dm + M_q$ $(m \in M_j)$ is an isomorphism $\delta$ of $M_j/M_{j-1}$ onto $M_{q+1}/M_q$. In particular $M_{q+1}/M_q \cong M_1$.*

PROOF. If $N$ is a submodule of $M$ then the mapping $n \mapsto dn + N$ of $N$ into $M/N$ is a homomorphism since $dhn + N = hdn + [d, h_M]n + N (h \in H)$. Let $j$ be the largest index $(1 \leqq j \leqq q)$ such that $dM_{j-1} \subseteq M_q$, take $N = M_q$, and consider the restriction to $M_j$ of the above homomorphism. Let the image be $M_{q+1}/N$; this defines $M_{q+1}$. The kernel is $M_{j-1}$ since $M_1$ is minimal and $M_j/M_{j-1} \cong M_1$. This gives the required isomorphism of $M_j/M_{j-1}$ onto $M_{q+1}/M_q$, and the lemma's proof is complete.

Our first applications of this lemma will be with $M = A$ (an algebra over $K$), $D$ a set of quasi-derivations of $A$, and $H = T(A)$, so that submodules are the same as ideals. By a composition series of a ring or algebra, say of $A$, we shall mean (unless otherwise stated) a composition series for $A$ as a $T(A)$-module, so that the terms of the series are ideals of $A$.

LEMMA 2.2. *Suppose that $A$ is a quasi-differentiably simple algebra with a minimal ideal $M_1$. Then $A$ has a composition series and a unique maximal ideal $N$. Moreover $N$ is nilpotent, $A/N$ is simple, $A^2 = A$, and every composition factor is isomorphic to $M_1$ as a $T(A)$-module.*

PROOF. Suppose that $A$ does not have a composition series. Let $d_1, \cdots, d_n$ be a (possibly empty) sequence of not necessarily distinct quasi-derivations of $A$. Let $i_1$ be the first index (if any) such that $d_{i_1}M_1 \not\subseteq M_1$ and use $d_{i_1}$ to define an ideal $M_2$ as in Lemma 2.1. If $M_2, \cdots, M_r$ have already been constructed by Lemma 2.1 using $d_{i_1}, \cdots, d_{i_{r-1}}$ where $i_1 \leqq \cdots \leqq i_{r-1}$ and $d_{i_{r-1}} \cdots d_2 d_1 M_1 \subseteq M_r$, let $s = i_r$ be the lowest index (if any) after $i_{r-1}$ such that $d_s M_r \not\subseteq M_r$. Then Lemma 2.1 gives $M_{r+1}$. If $d_s M_r \not\subseteq M_{r+1}$ continue using $d_s$ until $M_{r+1}, \cdots, M_{r+u}$ have been obtained such that $d_s M_r \subseteq M_{r+u}$. Then $i_{r+u-1} = s$ and $d_s \cdots d_2 d_1 M_1 \subseteq M_{r+u}$. Proceeding until the indices have been exhausted, we obtain $M_1, \cdots, M_q$ with $d_n \cdots d_1 M_1 \subseteq M_q$. Then $M_q \neq A$ since we are supposing that there is no composition series, and there is a quasi-derivation $d$ such that $dM_q \not\subseteq M_q$. Applying Lemma 2.1 once more we get an $M_{q+1}$. If $m \in M_1$ and $x = d_n \cdots d_1 m$ then $x \in M_q$ and hence $xM_1 = M_1 x = 0$ since $M_{q+1}/M_q$ and $M_1$ are $T$-isomorphic. But the subspace of $A$ spanned by all $d_n \cdots d_1 m (d_n \in \text{qder } A, m \in M_1, n \geqq 0)$ is closed under $T$ and hence is $A$ itself. Therefore $AM_1 = M_1 A = 0$. But $\{a \in A \mid aA = Aa = 0\}$ is a quasi-differential ideal and hence $A^2 = 0$, a contradiction. Therefore $A$ has a composition series, in fact has one $0 \subset M_1 \subset \cdots \subset M_l = A$ such that $M_{i+1}/M_i \cong M_1$ as $T$-modules for $i = 1, \cdots, l-1$.

Let $N = M_{l-1}$. Then $N$ is maximal. Since $A^2$ is a quasi-differential ideal (because we do not use $1_A$ in generating $T$), $A^2 = A$ and $A/N$ is simple. Also $NM_{i+1} \subseteq M_i$ and $M_{i+1}N \subseteq M_i$ for all $i$ since $NA \subseteq N$ and $AN \subseteq N$. Therefore every product of at least $2^{l-1}$ elements of $N$, associated in any manner, is zero. If $N_1 \neq N$ is a maximal ideal then $N + N_1 = A$ and $A/N_1 \cong N/N \cap N_1$ is simple and nilpotent, a contradiction. Hence $N$ is unique. This completes the proof of the lemma.

## 3. The centroid and a tensor factorization

If $A$ is an algebra, $d \in \text{qder } A$ and $c \in C(A)$ then $[d, c] \in C(A)$ since if $t \in T(A)$ then $[[d, c], t] = [[d, t], c] + [d, [c, t]] = 0$ by the Jacobi identity for commutators. It follows that *if $d \in \text{qder } A$ then the mapping $c \mapsto [d, c] (c \in C(A))$ is a derivation of $C(A)$*. We shall denote this derivation by $d^*$.

LEMMA 3.1. *Let $A$ be a quasi-differentiably simple algebra over $K$. If $A$ has a minimal ideal $M_1$ and if $0 = M_0 \subset M_1 \subset \cdots \subset M_{l-1} = N \subset M_l = A$*

*is a composition series of $A$ constructed as in Lemma 2.1 then there are monomorphisms $\sigma_1, \cdots, \sigma_l$ of $C(A/N)$ into $C(A)$, as $K$-modules, such that the following holds for $i = 1, \cdots, l$. If $0 \neq \gamma \in C(A/N)$ then $\sigma_i(\gamma)A + M_{i-1} = M_i$, $\sigma_i(\gamma)N \subseteq M_{i-1}$, and if $\theta$ is any $T(A)$-isomorphism of $A/N$ onto $M_i/M_{i-1}$ then there exists a $\beta$ in $C(A/N)$ such that the mapping of $A/N$ into $M_i/M_{i-1}$ induced by $\sigma_i(\beta)$ is $\theta$.*

PROOF. By Lemma 2.1 there is a $T$-module isomorphism $\rho$ of $A/N$ onto $M_1$. Write $\Gamma = C(A/N)$ and define $\sigma_1$ by $\sigma_1(\gamma) = \mu_1\rho\gamma\pi_{l-1}$ ($\gamma \in \Gamma$) where $\pi_i$ denotes the natural projection of $A$ onto $A/M_i$ and $\mu_i$ is the injection of $M_i$ into $A$. The factors of $\sigma_1(\gamma)$ are $T$-homomorphisms and $\sigma_1(\gamma): A \to A$, so that $\sigma_1$ maps $\Gamma$ into $C(A)$. If $0 \neq \gamma \in \Gamma$ then $\gamma$ is onto and $\sigma_1(\gamma)A = M_1$, and hence $\sigma_1$ is one-one. If $\theta$ is a $T$-isomorphism of $A/N$ onto $M_1$ then $\rho^{-1}\theta \in \Gamma$, $\sigma_1(\rho^{-1}\theta) = \mu_1\theta\pi_{l-1}$, and $\rho^{-1}\theta$ is the required $\beta$.

In the construction of $M_2, \cdots, M_l$ by Lemma 2.1, let $d_i$ denote the quasi-derivation used to go from $M_i$ to $M_{i+1}$, with $j_i$ the corresponding index and $\delta_i$ the corresponding $T$-isomorphism of $M_{j_i}/M_{j_i-1}$ onto $M_{i+1}/M_i$. We define $\sigma_2, \cdots, \sigma_l$ recursively by setting $\sigma_{i+1}(\gamma) = [d_i, \sigma_{j_i}(\gamma)]$. Thus $\sigma_{i+1}$ maps $\Gamma$ into $C(A)$. Suppose the conclusions hold for $r < i$ ($i < l$). If $\gamma \neq 0$, then $d_i\sigma_{j_i}(\gamma)A + M_i = M_{i+1}$ and $\sigma_{j_i}(\gamma)d_iA \subseteq M_i$. Hence $\sigma_{i+1}(\gamma)A + M_i = M_{i+1}$, and $\sigma_{i+1}$ is one-one (and clearly $K$-linear). Similarly $\sigma_{i+1}(\gamma)N \subseteq M_i$. If $\theta$ is a $T$-isomorphism of $A/N$ onto $M_{i+1}/M_i$, then $\delta_i^{-1}\theta$ is a $T$-isomorphism of $A/N$ onto $M_{j_i}/M_{j_i-1}$. Hence there is a $\beta$ in $\Gamma$ such that $\sigma_{j_i}(\beta)$ induces $\delta_i^{-1}\theta$, i.e., $\nu_{j_i-1}\sigma_{j_i}(\beta) = \delta_i^{-1}\theta\nu_{l-1}$ (where we regard $\sigma_j$ as a mapping of $A$ into $M_j$ and $\nu_{j-1}$ is the projection of $M_j$ onto $M_j/M_{j-1}$). Then $\sigma_{i+1}(\beta) = [d_i, \sigma_{j_i}(\beta)]$ induces $\theta$ since $\nu_i\sigma_{j_i}(\beta)d_i = 0$ and $\delta_i\nu_{j_i-1} = \nu_id_i$ on $M_{j_i}$. This completes the proof.

LEMMA 3.2. *Let $A$ be a $D$-simple algebra over $K$ with a minimal ideal $M_1$, where $D \subseteq \operatorname{qder} A$. Then $C(A)$ is $D^*$-simple, where $D^*$ denotes $\{d^* \mid d \in D\}$ (and $d^*(c) = [d, c]$ $(c \in C(A))$). Moreover $C(A)$ has a composition series, with the same length $l$ as that of $A$.*

PROOF. (i) *If $c \in C = C(A)$ and $cA \subseteq M_i$ ($i > 0$)* (we use the notation of Lemma 3.1) *then $cN \subseteq M_{i-1}$*: Assuming that $cA \not\subseteq M_{i-1}$, $\pi_{i-1}c$ is a $T$-homomorphism of $A$ into $A/M_{i-1}$ with image $M_i/M_{i-1}$; the kernel is a maximal ideal of $A$, so by Lemma 2.2 is $N$.

(ii) $C = \sum_{i=1}^{l} \sigma_i(\Gamma)$ (where $\Gamma = C(A/N)$): It suffices to show that if $cA \subseteq M_i$, $cA \not\subseteq M_{i-1}$ then there exists a $\beta$ in $\Gamma$ such that $(c - \sigma_i(\beta))A \subseteq M_{i-1}$. Since $cN \subseteq M_{i-1}$, $c$ induces a $T$-isomorphism $\theta$ of $A/N$ onto $M_i/M_{i-1}$. By Lemma 3.1 there is a $\beta$ in $\Gamma$ such that $\sigma_i(\beta)$ also induces $\theta$, and this $\beta$ has the required property.

(iii) *$I = \{c \in C \mid cA \subseteq M_1\}$ is a minimal ideal of $C$*: It is obviously an ideal. To show that it is minimal we show that if $c, c' \in I$, $c \neq 0 \neq c'$, then there exists $c'' \in C$ such that $c' = cc''$. Here $c$ and $c'$ induce $T$-isomorphisms $\theta$ and $\theta'$ of $A/N$ onto $M_1$, and the required $c''$ is an element (which exists by Lemma 3.1) which induces the $T$-automorphism $\theta^{-1}\theta'$ of $A/N$.

(iv) *$C$ is $D^*$-simple*: Suppose that $H$ is a non-zero $D^*$-ideal of $C$. Then $HA = \{\sum h_j a_j\}$ is $D$-closed since $d(ha) = h(da) + (d^*h)a \in HA$ for all $d$ in $D$. Hence $HA = A$, and so there is an $h$ in $H$ such that $hA + N = A$. Then if $0 \neq \gamma \in \Gamma$ we have $0 \neq \sigma_1(\gamma)h \in H \cap I$. Since $H$ is $D^*$-closed, (ii) and the construction of the $\sigma_i$ in Lemma 3.1 show that $C = \sum \sigma_i(\Gamma) \subseteq H$, and $H = C$.

(v) *The ideals $\sum_{i=1}^{j} \sigma_i(\Gamma) = \{c \in C \mid cA \subseteq M_j\}$, $j = 0, \cdots, l$, form a composition series of $C$*: The equality follows from the proof of (ii). The expression on the right side shows that they are ideals, $C$ being commutative. The expression on the left side and the construction of the $\sigma_i$ in the proof of Lemma 3.1 show that the ideals are obtained by the method of Lemma 2.1 starting from the minimal ideal $I$, and thus form a composition series of $C$. This completes the proof of the lemma.

LEMMA 3.3. *Let $A, D$ and $M_1$ be as in Lemma 3.2, and let $N$ be the unique maximal ideal of $A$. Suppose that $E$ is a subfield of $C(A)$ such that $A/N$ as an $E$-algebra is central. If $\tau$ is any mapping of $A/N$ into $A$ which splits the exact sequence $0 \to N \to A \to A/N \to 0$ regarded as a sequence of $E$-module homomorphisms, then the mapping $s \otimes c \mapsto c(\tau s)$ $(s \in S = A/N$, $c \in C(A))$ gives an isomorphism $\tau'$, as $C$-modules, of $S \otimes_E C$ onto $A$, and $C$ has dimension $l$ over $E$. If $\tau$ can be chosen preserving products (that is, if the above sequence splits when regarded as consisting of algebra homomorphisms) then $\tau'$ is a ($C$, $E$ and $K$)-algebra isomorphism.*

PROOF. Since $C/(\text{radical } C)$ is a field, $E$ acts unitally on $A$ and $A$ is an $E$-algebra. Since $CN \subseteq N$, $S = A/N$ is also an $E$-algebra. Let $c_i = \sigma_i(1_S)$, $i = 1, \cdots, l$ (we continue using the notation of Lemma 3.1). Then $c_1, \cdots c_l$ are linearly independent over $E$, since if $c = c_j + \sum_{i<j} c_i e_i$ then $cA + M_{j-1} = M_j$ (because $c_iA + M_{i-1} = M_i$) and $c \neq 0$. If $cA \subseteq M_i$ and $cA \not\subseteq M_{i-1}$ then $c$ and $c_i$ both induce $T$-isomorphisms, $\bar{c}$ and $\bar{c}_i$, of $A/N$ onto $M_i/M_{i-1}$. Then $(\bar{c}_i)^{-1}\bar{c}$ is a $T$-automorphism of $A/N$, hence is in the centroid of $S$ as a $K$-algebra. Therefore there is an $e$ in $E$ such that $\pi_{i-1}(c - ec_i) = 0$. It follows that $c_1, \cdots, c_l$ are a basis of $C$ over $E$.

For a given splitting $E$-homomorphism $\tau$, $(s, c) \mapsto c(\tau s)$ is $E$-bilinear, hence $\tau'$ is well-defined. Every element of $S \otimes_E C$ is uniquely represented as $\sum_{i=1}^{l} s_i \otimes c_i$, $s_i \in S$. If $0 \neq \sum_i s_i \otimes c_i \in \ker \tau'$, let $j$ be the largest index such that $\tau s_j \neq 0$. Since $\tau s_j \notin N$ and $c_j$ induces a $T$-isomorphism of $A/N$ onto $M_j/M_{j-1}$, $c_j \tau s_j \notin M_{j-1}$. But $\sum_{i<j} c_i \tau s_i \in M_{j-1}$, a contradiction, and $\ker \tau' = 0$. Obviously $\tau'$ is a homomorphism of $C$-modules, where $c'(s \otimes c) = s \otimes c'c$. If $\tau$ preserves products then $cc'\tau(s_1 s_2) = (c\tau s_1)(c'\tau s_2)$, so that $\tau'$ is an isomorphism of algebras (over $C$, hence also over $E$ and $K$). This completes the proof of the lemma.

LEMMA 3.4. *Suppose that $A$ is a d-simple algebra, where $d$ is a derivation, with a minimal ideal $M_1$. Then $0 \to N \to A \to S(= A/N) \to 0$ splits (as a sequence of algebra homomorphisms), and in fact $S' = \{a \in A \mid da \in M_1\}$ is a splitting subalgebra $\tau S$.*

PROOF. Since $d$ is a derivation $S'$ is a subalgebra. The chain of ideals $M_1, \cdots, M_{l-1} = N, M_l = A$ may be constructed with $d$ always used to go from $M_i$ to $M_{i+1}$ (so that $j_i = i$). If $0 \neq a \in S' \cap N$, let $i$ be the index such that $a \in M_i$, $a \notin M_{i-1}$. Then $da \notin M_i$ by Lemma 2.1, which contradicts $dS' \subseteq M_1$. Therefore $S' \cap N = 0$. Moreover $dN + M_1 = A$ since it contains with $M_i$ also $dM_i + M_i = M_{i+1}$. Hence if $a \in A$ then $da = dn + a_1$ where $n \in N$ and $a_1 \in M_1$, $d(a - n) = a_1$, $a = (a - n) + n \in S' + N$. This completes the proof of the lemma.

## 4. The commutative associative case

Suppose that $A$ is a differentiably simple commutative associative ring. At characteristic 0, results of Posner [11] show that $A$ is an integral domain. In particular if $A$ has a minimal ideal then $A$ is a field. For the application to the proof of the Main Theorem it would suffice to prove this assuming that the radical $N$ of $A$ is nilpotent, $A/N$ is a field, and $A$ has a unit element; the proof in this case is trivial: If $y \in N$, $y^i \neq 0$, $y^{i+1} = 0$ and $dy \notin N$ for some derivation $d$, then $dy$ is a unit but $y^i(dy) = d(y^{i+1})/(i+1) = 0$, a contradiction. Now suppose that $A$ has prime characteristic. Harper [6] proved that if $A$ is a finite-dimensional algebra over a field $E$ and if $A$ has the form $A = E1 + N$ ($N$ the radical), then $A \cong B_n(E)$ for some $n \geqq 0$. The following result generalizes Harper's theorem in several ways. A portion of the proof is partly based on Harper's proof, but yields a shorter proof even of his special case. For the rings considered, the differential constants (i.e. elements annihilated by all derivations) form a subfield which may be identified with the differential centroid under a restriction of the mapping $x \mapsto l_x$ which identifies the ring with its centroid.

THEOREM 4.1. *Let $A$ be a differentiably simple commutative associative ring of prime characteristic $p$, and let $R = \{x \in A \mid x^p = 0\}$. If $Rx = 0$ for* *some* $x \neq 0$ *in* $A$ (*this will hold,* e.g., *if* $A$ *has a minimal ideal*), *then there is a subfield* $E$ *of* $A$ *and an* $n \geqq 0$ *such that* $A \cong B_n(E)$ ($\cong E_{[n]}$), *in fact isomorphic as algebras over* $E$. *Here* $E$ *may be taken to be any maximal subfield of* $A$ *containing the subfield* $F$ *of differential constants.*[1]

PROOF. By two theorems of Posner [11], $A$ has a unit element and the ideal $R$ is nilpotent (for the application to the proof of the Main Theorem it would have been enough just to assume these properties). By Zorn's lemma there exists a maximal subfield of $A$ containing $F$; let $E$ be any such maximal subfield. We now give the proof of the theorem in five parts.

(i) $E + R = A$: If $a \in A$ then $a^p \in F$, say $a^p = \alpha$, and the minimal polynomial of $a$ over $E$ divides $\lambda^p - \alpha$. If $E$ contains no $p^{\text{th}}$ root of $\alpha$, then $\lambda^p - \alpha$ is irreducible over $E$ and $E(a)$ is a field, which contradicts the maximality of $E$. Therefore $E$ contains a $p^{\text{th}}$ root $\beta$ of $\alpha$, $a - \beta \in R$, and $a \in E + R$.

Now regard $A$ as an algebra over $E$, choose a subset $\{y_j \mid j \in J\}$ of $R$ such that $\{y_j + R^2 \mid j \in J\}$ is a basis of $R/R^2$, let $X = \{X_j \mid j \in J\}$ be a corresponding set of commuting indeterminates over $E$, and let $\tau$ be the (unique) homomorphism of $E[X]$ to A such that $\tau X_j = y_j (j \in J)$ and $\tau 1 = 1$. Then

(ii) $\tau$ *is onto*: It suffices (since $R$ is nilpotent) to show for all $k > 0$ that

$$\{y_{j_1}^{i_1} \cdots y_{j_m}^{i_m} + R^{k+1} \mid j_l \in J,\ i_l \geqq 0,\ i_1 + \cdots + i_m = k\}$$

spans $R^k/R^{k+1}$. This is true for $k = 1$ by the choice of $\{y_j\}$, and its truth for $k + 1$ follows from that for $k$ because

$$R^k R = \sum (Ey_{j_1}^{i_1} \cdots y_{j_m}^{i_m} + R^{k+1})(Ey_l + R^2) \subseteq \sum (Ey_{j_1}^{i_1} \cdots y_{j_m}^{i_m} y_l + R^{k+2}) .$$

Now regard $A$ again as a ring.

(iii) *Given* $d$ *in* $\operatorname{der} A$, *there exists* an $F$-*linear derivation* $d'$ *of* $E[X]$ *such that* $\tau d' = d\tau$: Let $\{w_i\}$ be a basis of $A$ over $E$ composed of monomials in the $y_j$'s. If we write $de = \sum (d_i e) w_i (e \in E,\ d_i e \in E)$ then each $d_i$ is a derivation of $E$ and for each $e$ in $E$, $d_i e = 0$ except for a finite set of indices $i$. For each $w_i$ let $z_i$ be the element of $E[X]$ obtained by replacing the $y_j$'s by $X_j$'s. Also for each $j$ in $J$ pick an $X'_j$ in $E[X]$ such that $\tau X'_j = dy_j$. Then there is a (unique) $F$-linear derivation $d'$ of $E[X]$ such that $d'X_j = X'_j (j \in J)$ and $d'(e1) = \sum (d_i e) z_i (e \in E)$, as a straightforward verification shows, and this is the required $d'$.

[1] *Added April* 25, 1969. The writer has just learned of the paper by Shuen Yuan, *Differentiably simple rings of prime characteristic,* Duke Math. J. **31** (1964), 623-630, in which essentially the result of Theorem 4.1 is proved (under the hypothesis that the radical is nilpotent). The proof given here is different and simpler than Yuan's, and also makes the proof of the Main Theorem self-contained.

(iv) *Let* $D' = \{d' \in \operatorname{der}_F E[X] \mid \exists d \in \operatorname{der} A \ni \tau d' = d\tau\}$; *then* $\ker \tau$ *is a maximal* $D'$*-ideal and a* $\operatorname{der}_F E[X]$*-ideal of* $E[X]$: $\ker \tau$ is obviously a $D'$-ideal and is maximal by (iii) since $A$ is differentiably simple. Let $I$ be the additive subgroup of $E[X]$ generated by $\ker \tau + \Delta(\ker \tau)$ where $\Delta = \operatorname{der}_F E[X]$. Then $I$ is an ideal because $b(\delta k) = \delta(bk) - (\delta b)k$ ($b \in E[X]$, $\delta \in \Delta$, $k \in \ker \tau$), and $I$ is $D'$-closed because $d'(\delta k) = \delta(d'k) + [d', \delta]k$ and $[d', \delta] \in \Delta$. By maximality, either $I = \ker \tau$ and hence $\Delta(\ker \tau) \subseteq \ker \tau$, or else $I = E[X]$, in which case $\ker \tau$ would contain an element with a non-zero (monomial) term of degree $\leqq 1$. But this latter contradicts the fact that $\{1, y_j \mid j \in J\}$ is linearly independent modulo $R^2$ and $\tau$ maps monomials of degree $> 1$ into $R^2$.

(v) $\ker \tau = (X^p)$, *where* $(X^p)$ *denotes the ideal generated by* $\{X_j^p \mid j \in J\}$, *and the index set* $J$ *is finite*: $(X^p) \subseteq \ker \tau$. But $(X^p)$ is a maximal $\Delta$-ideal of $E[X]$ (just apply enough derivations $\partial/\partial x_j$ to an element not in $(X^p)$ to get a unit modulo $(X^p)$). Hence $\ker \tau = (X^p)$, and the nilpotency of $R$ implies that $J$ is finite. This completes the proof of the theorem.

COROLLARY 4.2. *If a differentiably simple commutative associative ring* $A$ *of prime characteristic has* ACC *on nilpotent ideals, then* $A \cong B_n(E)$ *for some field* $E$ *and some (finite)* $n \geqq 0$.

PROOF. With $\{y_j \mid j \in J\}$ as in the proof of the theorem, if $J' \subseteq J$ is finite then the ideal generated by $\{y_j \mid j \in J'\}$ is nilpotent. Hence $J$ is finite, say $|J| = n$. Then, as in (ii), $R^{p^n} = R^{p^n+1}$, and $R^{p^n} = (R^{p^n})^2$ is a differential ideal. Hence $R$ is nilpotent, and the result follows from the theorem.

## 5. Proof of $d$-simplicity

If $A$ is any algebra over a ring $K$, the quasi-derivations form a Lie algebra over $K$ under commutation (the Lie normalizer of $T(A)$), as do the derivations. If $c \in C(A)$ and $d \in \operatorname{qder} A$ then $cd \in \operatorname{qder} A$, since $[cd, t] = [c, t]d + c[d, t]$ and $cT(A) \subseteq T(A)$ ($cl_x = l_{cx}$, $cr_x = r_{cx}$). If $d \in \operatorname{der} A$ then it is easy to see that $cd \in \operatorname{der} A$ (and $dc$ is a quasi-derivation but not necessarily a derivation). Thus $\operatorname{qder} A$ is a left $C(A)$-module and $\operatorname{der} A$ is a submodule.

LEMMA 5.1. *Let* $A$, $D$, *and* $D^*$ *be as in Lemma* 3.2. *If* $C(A)$ *is* $d^*$*-simple for a given* $d$ *in* $D$ *then* $A$ *is* $d$*-simple. If* $D$ *is closed under commutation and left multiplication by elements of* $C(A)$ *then* $D^*$ *is also.*

PROOF. Suppose that $C = C(A)$ is $d^*$-simple and that $M \neq 0$ is a $d$-ideal of $A$. Since $A$ has a $T(A)$-composition series, $M$ contains a minimal ideal $M_1$ of $A$. Starting with $M_1$ construct the chain of ideals $M_i$ by always using the given $d$ in Lemma 2.1 until an ideal $M_q$ is obtained with $dM_q \subseteq M_q$. If $M_q \neq A$ then $H = \{c \in C \mid cA \subseteq M_q\}$ is a proper ideal of $C$, but if $h \in H$ and $a \in A$ then

$(d^*h)a = dha - hda \in M_q$, so that $H$ is $d^*$-closed, a contradiction. Therefore $M_q = A$, $M = A$ and $A$ is $d$-simple. The last statement holds because $[ad\, d_1, ad\, d_2] = ad[d_1, d_2]$ in Hom $(A, A)$, and $c(d^*c_1) = cdc_1 - cc_1d = (cd)^*c_1$.

If $A$ is a ring or algebra and if $D$ is a Lie subring or subalgebra of qder $A$, we say that $D$ is *regular* if it is also a left $C(A)$-submodule of qder $A$. This conforms with the terminology used by Ree [12] in his investigation of the regular Lie subalgebras of der $B_n(F)$. If $A$ is an algebra and if $A^2 = A$ then the centroid of $A$ is the same set whether $A$ is regarded as an algebra or as a ring. Hence a regular Lie subring of qder$_K A$ is also a regular Lie subring of qder $A$ when $A$ is regarded as a ring.

THEOREM 5.2. *If $A$ is a $D$-simple algebra over $K$ with a minimal ideal where $D$ is a regular Lie subring of* qder $A$ *then $A$ is $d$-simple for some $d$ in $D$.*

PROOF. Since $A$ is $D$-simple ($d$-simple) as an algebra if and only if it is $D$-simple ($d$-simple) as a ring ($d \in D \subseteq$ qder$_K A$), we may ignore $K$ and regard $A$ as a ring (the minimal ideal remains minimal). Also we may assume that $A$ is not simple. By Lemmas 5.1 and 3.2 we may assume that $A$ is commutative associative and that $D \subseteq$ der $A$. Then by Lemma 2.2 and Theorem 4.1, $A$ has prime characteristic $p$ and $A \cong B_n(E)$ for some field $E$ and some $n > 0$. We claim that

( i ) *there is a regular Lie subring $D_0$ of $D$ and a derivation $d_1$ in $D$ such that $A$ is not $D_0$-simple, $A$ is $(D_0 \cup \{d_1\})$-simple, and $[d_1, D_0] \subseteq D_0$*: Since the radical $R$ of $A$ is not a $D$-ideal, there is an $r$ in $R$ and a $d_1$ in $D$ such that $d_1r \notin R$ and hence $d_1r$ is a unit of $A$. Replacing $d_1$ by $(d_1r)^{-1}d_1$ we may assume that $d_1r = 1$. Let $D_0 = \{d - (dr)d_1 \mid d \in D\}$. Then $D_0 = \{d \in D \mid dr = 0\}$ and hence $D_0$ is a regular Lie subring of $D$, and $[d_1, D_0] \subseteq D_0$ since if $d_0r = 0$ then $(d_1d_0 - d_0d_1)r = -d_01 = 0$. Also $A$ is not $D_0$-simple since $rA$ is a proper $D_0$-ideal. Any $(D_0 \cup \{d_1\})$-ideal of $A$ is invariant under $d-(dr)d_1$ and $(dr)d_1$ for all $d$ in $D$, and hence $A$ is $(D_0 \cup \{d_1\})$-simple.

Now let $H$ be the (associative) subring of Hom $(A, A)$ generated by $T(A)$ and $D_0$. Then $[d_1\, H] \subseteq H$ and $A$ has no proper $H$-submodule invariant under $d_1$. Since $H$-submodules are in particular ideals of $A$, $A$ has an $H$-composition series. Starting with a minimal $H$-submodule $M_1$ of $A$ and applying Lemma 2.1 using $d_1$ at each step, we get an $H$-composition series $0 = M_0 \subset \cdots \subset M_l = A$ and $H$-isomorphisms $\delta_i : \bar{M}_i \longrightarrow \bar{M}_{i+1}$, where we write $\bar{M}_j = M_j/M_{j-1}$ (with $\bar{M}_l = \bar{A}$). Since $M_{l-1}$ is a $D_0$-ideal of $A$, any $d$ in $D_0$ induces a derivation on $\bar{A}$ (regarded as a ring) which we denote by $\bar{d}$. We also write $\bar{D}_0 = \{\bar{d} \mid d \in D_0\}$. Then $\bar{D}_0$ is a regular Lie ring of derivations of $\bar{A}$, and $\bar{A}$ is $\bar{D}_0$-simple. By induction on the $(T(A))$ composition length ($M_{l-1} \neq 0$ since $A$ is not $D_0$-simple) there is a $d_0$ in $D_0$ such that $\bar{A}$ is $\bar{d}_0$-simple. We have

(ii) *if $A$ is not $d_1$-simple then $\bar{A} \cong B_q(E)$ for some positive $q$*: By Theorem 4.1, $\bar{A} \cong B_q(E)$ for some $q \geqq 0$, with the same field $E$ as above (this latter fact is not actually needed) since $A/N \cong \bar{A}/\bar{N}$. Since $d_1$ gives all the mappings $\delta_j$, if $0 \neq a \in A$ then for some $i$, $d_1^i a \notin M_{l-1}$. But if $q = 0$ then $d_1^i a$ is a unit since $\bar{A}$ is a field and $M_{l-1}$ is nil, and hence any non-zero $d_1$-ideal would contain a unit.

Now suppose $q > 0$, let $x_1, \cdots, x_q$ be a set of nilpotent generators of $\bar{A}$ (i.e., $\bar{A} = \bar{E}[x_1, \cdots, x_q]$, $x_i^p = 0$, $i = 1, \cdots, q$; $\bar{E}$ a copy of $E$), and for $i = 1, \cdots, l$ let $M_i'$, $M_i''$ denote the ideals of $A$ such that $M_i \supset M_i' \supseteqq M_i'' \supset M_{i-1}$, $M_i'/M_{i-1} = (\delta_{l-1} \cdots \delta_i)^{-1}(x_1, \cdots, x_q)$, and $M_i''/M_{i-1} = (\delta_{l-1} \cdots \delta_i)^{-1}E(x_1 \cdots x_q)^{p-1}$; i.e., $M_i'/M_{i-1}$ and $M_i''/M_{i-1}$ correspond under the $H$-isomorphism to the unique maximal and minimal ideals of $\bar{A}$. Also pick $y_i$ in $A$ such that $y_i + M_{l-1} = x_i$ $(i = 1, \cdots, q)$ and set $w = (y_1 \cdots y_q)^{p-1}$. Then

(iii) *$wM_i' \subseteqq M_{i-1}''$ (where $M_0'' = 0$) and $wM_i + M_{i-1} = M_i''(i = 1, \cdots, l)$*: We have

$$d_1 w + M_{l-1} = \sum_i (p-1)(d_1 y_i + M_{l-1}) x_1^{p-1} \cdots x_i^{p-2} \cdots x_q^{p-1} ,$$

so that each term in $d_1 w + M_{l-1}$ is of total degree at least $(p-1)^q - 1$. Hence $(d_1 w + M_{l-1})(M_l' + M_{l-1}) \subseteqq M_l'' + M_{l-1}$, $(d_1 w)M_l' \subseteqq M_l''$, and, by the $H$-isomorphisms, $(d_1 w)M_i' \subseteqq M_i''(i = 1, \cdots, l)$. Also $wM_i + M_{i-1} = M_i''$ for all $i$ since this holds for $i = l$. By the definition of $M_i'$ and $M_i''$, $d_1 M_i' + M_i = M_{i+1}'$ and $d_1 M_i'' + M_i = M_{i+1}''$ $(i = 1, \cdots, l-1)$. Also $wM_1' = 0$ since $wM_l' \subseteqq M_{l-1}$. Suppose $wM_i' \subseteqq M_{i-1}''$ for some $i$ ($1 \leqq i < l$; this is true for $i = 1$). Then (since $[d_1, l_w] = l_{d_1 w}$)

$$wM_{i+1}' \subseteqq wd_1 M_i' + wM_i \subseteqq d_1(wM_i') + (d_1 w)M_i' + M_i'' \subseteqq d_1 M_{i-1}'' + M_i'' \subseteqq M_i'' .$$

(iv) *Let $d = d_0 + wd_1$; then $A$ is $d$-simple*: In proving this, for any ideal $I$ of $A$ we write $\Delta I$ and $\Delta_0 I$ for the ideal $dI + I$ and $d_0 I + I$, respectively, and similarly for $\bar{\Delta}_0$ on ideals of $\bar{A}$. Since $\bar{A}$ is $\bar{d}_0$-simple and has the same composition length as its dimension over $\bar{E}$, it follows that

$$(\bar{\Delta}_0)^{p^q-2}\left(\bar{E}(x_1 \cdots x_q)^{p-1}\right) = (x_1, \cdots, x_q)$$

and hence

$$(\Delta_0)^{p^q-2} M_i'' = M_i' \qquad (i = 1, \cdots, l).$$

Therefore, since $d_1 M_i' \subseteqq M_{i+1}'$, (iii) gives $\Delta^j M_i'' = \Delta_0^j M_i''$, $\Delta^{p^q-1} M_i'' = \Delta M_i' = M_i$ $(j = 1, \cdots, p^q - 1;\ i = 1, \cdots, l)$. But for $i < l$, $\Delta M_i = wd_1 M_i + M_i = wM_{i+1} + M_i = M_{i+1}''$. Therefore the ideals $\Delta^j M_1''$, $j = 1, \cdots, (p^q - 1)l$, together with the 0 ideal, form a composition series of $A$. Hence $A$ is $d$-simple since $M_1''$ is the unique minimal ideal of $A$ (or by the argument of (ii)). This completes the proof of the theorem.

## 6. Completion of proof of the main theorem

Let $A$ be a differentiably simple algebra over $K$ with a minimal ideal $M_1 \neq A$. Since der $A$ is a regular Lie ring, by Theorem 5.2 there is a derivation $d$ such that $A$ is $d$-simple. By Lemma 3.2, $C = C(A)$ is $d^*$-simple and $I = \{c \in C \mid cA \subseteq M_1\}$ is a minimal ideal of $C$. By Lemma 2.2, the radical $R$ of $C$ is nilpotent, and by Lemma 3.4, $E = \{c \in C \mid d^*c \in I\}$ is a subfield of $C$ with $E + R = C$. The differential constants of $C$ are in $E$ and in particular $K_A \subseteq E$. By §4, $C$ (and hence also $A$) has prime characteristic and $C \cong B_n(E)$, as an algebra over $E$, for some $n > 0$ ($R \neq 0$ since otherwise $C = E = I$ and $A = M_1$). Hence $I$ is 1-dimensional over $E$.

The ring $A$ is also an algebra over $E$. In the notation of Lemma 3.1, if $0 \neq \gamma \in \Gamma = C(A/N)$ then $\sigma_1(\gamma)A = M_1$, hence $CM_1 \subseteq M_1$ and $M_1$ is an $E$-ideal. Since $[d, E]A = (d^*E) \subseteq M_1$, in the construction of the chain of ideals $M_i$ using $d$ in Lemma 2.1, all the isomorphisms $\delta$ are $E$-linear; in particular $A/N$ and $\Gamma$ may be considered as algebras over $E$. Therefore the mapping $\rho$ used in defining $\sigma_1$ in Lemma 3.1 $(\sigma_1(\gamma) = \mu_1\rho\gamma\pi_{l-1})$ is $E$-linear, and $\sigma_1$ is an isomorphism of $\Gamma$ onto $I$ as $E$-modules. Therefore $A/N$ as an $E$-algebra is central. The subalgebra $S' = \{a \in A \mid da \in M_1\}$ of Lemma 3.4 is closed under $E$, so we have the situation of Lemma 3.3, and $A \cong S' \otimes_E B_n(E) \cong S'_{[n]}$ as an algebra over $E$, hence also over $K$, where $S' \cong A/N$ is a simple algebra over $E$ and hence also over $K$. This completes the proof of the Main Theorem.[2]

One of the main tools used in the proof of the Main Theorem was the passage from quasi-derivations of $A$ to derivations of $C(A)$. The proof of Lemma 3.4 was the only place where we required, for the $D$-simple algebra $A$ itself, that $D$ consist of derivations rather than merely quasi-derivations. The following gives several cases where this hypothesis may be weakened.

COROLLARY 6.1. *Let $A$ be a $D$-simple algebra with a minimal ideal, where $D \subseteq$ qder $A$. Then the conclusion of the Main Theorem holds in each of the following cases*

( i ) *$A$ has characteristic* 0;

(ii) *$A$ is commutative associative with a unit element*;

(iii) *$A$ is finite-dimensional over a field and is either alternative (including associative), or standard* [1], [14] *(including Jordan) of character-*

[2] *Added April* 25, 1969. The proof of the Main Theorem remains valid for Lie triple systems, and more generally for $\Omega$-algebras $A$ where $A$ is a $K$-module and each $\omega \in \Omega$ is $n$-ary multilinear for some $n \geqq 2$ (with the appropriate definitions of derivation, etc.).

*istic* $\neq 2$;

(iv) $D = \{d\}$ *and for each* $x, y$ *in* $A$ *there is a* $t = t(x, y)$ *in* $T(A)$ *such that* $d(xy) = (dx)y + t(dy)$.

PROOF. Case (i) follows from Lemma 3.2 and the (easy) characteristic 0 case of § 4. Case (ii) follows from Lemma 3.2 and the Main Theorem since here $A \cong C(A)$. Case (iii) follows from the Wedderburn principal theorem for alternative algebras [13] and for standard algebras [14] of characteristic $\neq 2$, since this provides the splitting subalgebra needed in Theorem 3.3, thus bypassing Lemma 3.4 (and § 5). In Case (iv) the set $S'$ of the proof of Lemma 3.4 is a subalgebra, and so as noted above the conclusion holds in this case also. This concludes the proof.

The Main Theorem probably remains true for any quasi-differentiably simple algebra with a minimal ideal. At any rate, Lemma 3.3 and Theorem 4.1, together with Theorem 5.2 and the argument of §6, provide a great deal of information about such an algebra. It can also be seen that in the use we have made so far of the concept, the definition of quasi-derivation could be further weakened.

Given one of the non-simple algebras $A$ of the Main Theorem, the algebra $S$ is uniquely determined up to isomorphism, since it is the unique simple difference algebra of $A$, and $n$ is uniquely determined since $p^n$ is the composition length of $A$($p$ the characteristic of $S$ and of $A$). One of the principal difficulties in proving the Main Theorem was finding a subalgebra of $A$ corresponding to $S$. It is easy to see that for any two such subalgebras there will be an automorphism of $A$ sending one to the other. However the subalgebra is not in general unique. To show this we need only give an automorphism of $A = S \otimes_{Z_p} B_n(Z_p)$ which moves $S \otimes 1$. Thus suppose that $S$ has a derivation $d' \neq 0$ and that $x \in B_n(Z_p)$ with $x \neq x^2 = 0$, and let $d$ be the linear mapping of $A$ determined by $d(s \otimes b) = d'(s) \otimes xb$ $(s \in S, b \in B_n(Z_p))$. Then $d$ is a derivation of $A, d \neq d^2 = 0, \exp d = 1_A + d$ is an automorphism of $A$, and $(\exp d)(S \otimes 1) \neq S \otimes 1$.

We now discuss the conjecture of Zassenhaus mentioned in § 1. For any Lie algebra $S$ over a field $F$ of characteristic $p$ and any integer $m > 0$ he constructed [17, pp. 64, 67] a Lie algebra $S^{(m)}$, which he called a power ring of $S$. This consists of the vector space over $F$ of all $m$-tuples $a = (a_0, \cdots, a_{m-1})$ of elements of $S$, with products given by $[a, b] = c$ where

$$c_i = \sum_{j=0}^{i} \binom{i}{j} [a_j, b_{i-j}] \qquad (i = 0, 1, \cdots, m-1).$$

Based on his characterization of the $d$-simple Lie algebras over $F$ with a chief $(= T(A)\text{-composition})$ series [17, pp. 61–79], Zassenhaus conjectured [17, p. 80] that if $L$ is a differentiably simple Lie algebra over $F$ (presumably with a chief series) then $L \cong S^{(p^n)}$ for some simple Lie algebra $S$ over $F$ and some $n \geqq 0$. It turns out that we can show rather easily (we omit the details) that $S^{(p^n)}$ and $S_{[n]} = S \otimes_F B_n(F)$ are isomorphic, under the following mapping

$$(s_0, \cdots, s_{p^n-1}) \longmapsto \sum_{i=0}^{p^n-1} \bar{i}!^{-1} s_i \otimes x_1^{i_1} \cdots x_n^{i_n} ,$$

where $i = i_1 + i_2 p + \cdots + i_n p^{n-1}$, $0 \leqq i_j < p\ (i = 0, \cdots, p^n - 1)$, $\bar{l}$ denotes the residue class modulo $p$ of $l/p^{\mathrm{ord}_p l}$, and $B_n(F) = F[x_1, \cdots, x_n]$, $x_j^p = 0$ $(j = 1, \cdots, n)$. Zassenhaus' conjecture then follows immediately from the Main Theorem. It seems clear that the tensor product form of $S_{[n]}$ used in the present paper is a much more convenient construction than that of the power rings.

## 7. The derivations of $S_{[n]}$ and a condition for $D$-simplicity

In view of the Main Theorem, it is desirable to determine the derivations of the algebra $S_{[n]}$ of that theorem. This we shall now do, of course in terms of the derivations of $S$. We begin by determining the derivations of a large class of tensor products.

THEOREM 7.1. *Let $A = S \otimes_F B$, regarded as an algebra over $F$, where $F$ is a field, $S$ and $B$ are algebras over $F$, and $B$ is commutative associative with a unit element. If $S$ or $B$ is finite-dimensional and if $S^2 = S$ or $\{s \in S \mid sS = Ss = 0\} = 0$ then*

$$\operatorname{der} A = (\operatorname{der} S) \otimes_F B + \Gamma \otimes_F (\operatorname{der} B)$$

*(the sum being a direct sum as vector spaces) where $\Gamma$ denotes the centroid of $S$ and*

$$(d' \otimes b_1)(s \otimes b) = (d's) \otimes (b_1 b) , \qquad (\gamma \otimes d'')(s \otimes b) = (\gamma s) \otimes (d''b)$$
$$(d' \in \operatorname{der} S,\ d'' \in \operatorname{der} B) .$$

PROOF. A straightforward verification shows that each $d' \otimes b$ and $\gamma \otimes d''$ is a derivation of $A$. Now let $d$ be a given derivation of $A$. We give the proof in three parts.

( i ) *Proof of the theorem when $S$ is associative with a unit element.* We identify the center of $S$ with $\Gamma$. Choose a basis $\{b_i \mid i \in I\}$ of $B$ and a basis $\{s_j\ j \in J\}$ of $\Gamma$, and extend the latter to a basis $\{s_j \mid j \in J'\}$ of $S$ where the index set $J' = J \cup J''$ with $J \cap J'' = \varnothing$. Define linear transformations $d_i'$ on $S$ $(i \in I)$ and $d_j''$ on $B$ $(j \in J')$ by writing

$$d(s \otimes 1) = \sum_{i \in I} (d_i' s) \otimes b_i , \qquad d(1 \otimes b) = \sum_{j \in J'} s_j \otimes (d_j'' b)$$
$$(s \in S, b \in B) .$$

Then each $d'_i$ is a derivation of $S$ since

$$\begin{aligned}\textstyle\sum_I d'_i(s_1s_2)\otimes b_i &= \big(d(s_1\otimes 1)\big)(s_2\otimes 1)+(s_1\otimes 1)d(s_2\otimes 1)\\ &= \textstyle\sum_I\{(d'_is_1)s_2+s_1(d'_is_2)\}\otimes b_i\ ,\end{aligned}$$

and similarly each $d''_j$ is a derivation of $S$. Applying $d$ to both sides of $(s\otimes 1)(1\otimes b)=(1\otimes b)(s\otimes 1)$ gives $(s\otimes 1)d(1\otimes b)=d(1\otimes b)(s\otimes 1)$ since $1\otimes b$ commutes with $d(s\otimes 1)$, and hence $0=\sum_{j\in J'}[s,s_j]\otimes(d''_jb)=\sum_{j\in J''}[s,s_j]\otimes(d''_jb)$ for all $s$ in $S$ and $b$ in $B$. For a given $b$ in $B$ and each $j$ in $J''$ write $d''_jb=\sum_{i\in I}\alpha_{ij}b_i$ $(\alpha_{ij}\in F)$. Then

$$0=\textstyle\sum_{j\in J''}[s,s_j]\otimes(d''_jb)=\sum_{i\in I}[s,\sum_{j\in J''}\alpha_{ij}s_j]\otimes b_i$$

for all $s$. Hence $\sum_{j\in J''}\alpha_{ij}s_j\in\Gamma$ for all $i$, $\alpha_{ij}=0$ for all $i$ and all $j$ in $J''$, and $d''_j=0$ for all $j$ in $J''$. Then

$$\begin{aligned}d(s\otimes b)&=d\big((s\otimes 1)(1\otimes b)\big)=\textstyle\sum_i(d'_is)\otimes b_ib+\sum_{j\in J'}ss_j\otimes d''_jb\\ &=\textstyle\sum_i(d'_is)\otimes b_ib+\sum_{j\in J}s_js\otimes d''_jb\qquad(s\in S,\ b\in B)\ ,\end{aligned}$$

and $d$ has the form $\sum_i d'_i\otimes b_i+\sum_{j\in J}s_j\otimes d''_j$. By the definition of the $d'_i$, for each $s$ in $S$, $d'_is=0$ except for finitely many of the indices $i$. Therefore if $S$ is finite-dimensional, then $d'_i=0$ except for finitely many $i$, so that $\sum_i d'_i\otimes b_i\in(\operatorname{der}S)\otimes B$, while of course the same is true if $I$ is finite. Similarly $\sum_{i\in J}s_j\otimes d''_j\in\Gamma\otimes(\operatorname{der}B)$. Finally, the sum is direct since if $\sum_i d'_i\otimes b_i\in\Gamma\otimes\operatorname{der}B$ then $\sum_i(d'_i\otimes b_i)(s\otimes 1)=0$ for all $s$, and $d'_i=0$ for all $i$. This completes the proof when $S$ is associative with 1.

(ii) *If $U=\Gamma+T(S)$ then there is an algebra isomorphism $\tau$ of $U\otimes B$ onto $C(A)+T(A)$ with $\tau(u\otimes b)=u\otimes l_b$ (regarded as a mapping of $A$, where $l_b$ is the multiplication by $b$ on $B$), and $\Gamma$ and $C(A)$ are commutative.* $U$ is an (associative) algebra of linear transformations on $S$ since $\gamma l_s=l_{\gamma s}$ and $\gamma r_s=r_{\gamma s}$. There is a unique linear mapping $\tau$ of $U\otimes B$ onto a space of linear transformations of $A$ with $\tau(u\otimes b)=u\otimes l_b$ $(u\in U,\ b\in B)$. Then $\tau$ is one-one since if $\big(\sum_i u_i\otimes b_i\big)(s\otimes 1)=0$ for all $s$ then $u_i=0$ for all $i$. Clearly $\tau$ preserves multiplication. Therefore $\tau\big(T(S)\otimes B\big)=T(A)$ since $\tau(l_s\otimes b)=l_{s\otimes b}$ and $\tau(r_s\otimes b)=r_{s\otimes b}$. If $\gamma,\gamma'\in\Gamma$ then $[\gamma,\gamma']S^2=\big([\gamma,\gamma']S\big)S=S\big([\gamma,\gamma']S\big)=0$ and hence the hypothesis on $S$ implies that $\Gamma$ is commutative. Also either $A^2=A$ or $\{a\in A\mid aA=Aa=0\}=0$, so that $C(A)$ is commutative. We claim that $\tau(\Gamma\otimes B)=C(A)$. Indeed if $c\in C(A)$ and we write $c(s\otimes 1)=\sum_i\gamma_i(s)\otimes b_i$ $(i\in S)$, we see that each $\gamma_i\in\Gamma$. But if $b\in B$ then $1_S\otimes l_b\in C(A)$ and so $c(s\otimes b)=(1_S\otimes l_b)c(s\otimes 1)=\sum_i\gamma_i(s)\otimes b_ib$, and $c=\sum_i\gamma_i\otimes b_i$. Here $\gamma_i=0$ except for finitely many $i$, as in (i). Therefore $\tau(\Gamma\otimes B)=C(A)$ and $\tau(U\otimes B)=C(A)+T(A)$.

(iii) *Proof of the theorem when $S$ is not associative or does not have a unit element.* Since $[d, T(A)] \subseteq T(A)$ and $[d, C(A)] \subseteq C(A)$, commutation by $d$ gives a derivation of $C(A) + T(A)$, and hence by (ii) also a derivation $\hat{d}$ of $U \otimes B$. The center of $U$ is $\Gamma$ since $\Gamma$ is commutative. Since $U$ is associative with a unit element, if $\{\gamma_j \mid j \in J\}$ is a basis of $\Gamma$ and $\{b_i \mid i \in I\}$ of $B$ then by (i) there are derivations $\hat{d}'_i$ of $U$ and $d''_j$ of $B$ such that

$$\begin{aligned} l_{d(s \otimes b)} &= [d, l_{s \otimes b}] = \tau\hat{d}(l_s \otimes b) \\ &= \tau \textstyle\sum_{i \in I} \hat{d}'_i(l_s) \otimes b_i b + \tau \sum_{j \in J} \gamma_j l_s \otimes d''_j b \qquad (s \in S,\ b \in B)\ . \end{aligned}$$

Then with $b = 1$ and with $d'_i (i \in I)$ defined by setting $d(s \otimes 1) = \sum_{i \in I} d'_i(s) \otimes b_i$ (so that as in (i) each $d'_i$ is a derivation of $S$) we have

$$\textstyle\sum_{i \in I} l_{d'_i(s)} \otimes l_{b_i} = \tau \sum_{i \in I} \hat{d}'_i(l_s) \otimes b_i \qquad (s \in S)$$

Hence $l_{d'_i(s)} = \hat{d}'_i(l_s)$ for all $i$, and (since $\gamma_j l_s = l_{\gamma_j s}$)

$$l_{\{d(s\otimes b) - \sum_{i \in I} d'_i(s) \otimes b_i b - \sum_{j \in J} \gamma_j s \otimes d''_j b\}} = 0 \qquad (s \in S,\ b \in B)$$

and the same equality holds with $l$ replaced by $r$. Then $d_0 = d - \sum_{i \in I} d'_i \otimes b_i - \sum_{j \in J} \gamma_j \otimes d''_j$ is a derivation of $A$, $0 = (d_0 S)S = S(d_0 S) = d_0 S^2$, and $d_0 = 0$. The desired conclusion follows as in (i). This completes the proof of the theorem.

In the course of the proof we have also established the following result for the infinite-dimensional case.

COROLLARY 7.2. *Let the hypotheses of the first sentence of Theorem* 7.1 *hold. If $S$ has a unit element, then every derivation $d$ of $A$ has the form $\sum_i d'_i \otimes b_i + \sum_j \gamma_j \otimes d''_j$ where $d'_i \in \operatorname{der} S$, $d''_j \in \operatorname{der} B$, and for each $s$ in $S$ (resp. $b$ in $B$), $d'_i(s) = 0$ $\big($resp. $d'_j(b) = 0\big)$ except for finitely many $i$ (resp. $j$) (and every mapping of this form is a derivation).*

In order to drop the hypothesis that $S^2 = S$ or $\{s \in S \mid sS = Ss = 0\} = 0$ we would have to take into account summands $d'''$ where $d'''S^2 = 0$ and $d'''S \subseteq \{s \in S \mid sS = Ss = 0\}$.

We now apply Theorem 7.1 to the determination of $\operatorname{der} S_{[n]}$ when $S$ is a simple algebra over a ring $K$ and $n > 0$. Let $E$ be the centroid of $S$, so that $E$ is a field containing $K_S$, and identify $A = S_{[n]}$ with $S \otimes_E B_n(E)$, with $S$ identified with $S \otimes 1$. If $b \in B_n(E)$ then the $E$-linear mapping $\tau_b$ of $S \otimes_E B_n(E)$ determined by $\tau_b(s \otimes b') = s \otimes bb'$ $\big(s \in S,\ b' \in B_n(E)\big)$ is in $C(A)$. It is easy to show (see [4]) that every element of $C(A)$ has this form. If $[d, \tau_b] = 0$ for all derivations of the form $d = 1_S \otimes d''$ $\big(d'' \in \operatorname{der}_E B_n(E)\big)$ then $d''b = 0$ for all $d''$, and $b \in E1$. Hence the differential centroid $F$ of $A$ is a subfield of $E$, the latter being regarded here as acting on $A$ (and of course $K_A \subseteq F$). In particular $S$ is also an $F$-algebra, and we may now identify $A$ with $S \otimes_F B_n(F)$ and der $A$ with $\operatorname{der}_F(S \otimes_F B_n(F))$. If $d' \in \operatorname{der} S$ then $d' \otimes 1 \in \operatorname{der}(S \otimes_{Z_p} B_n(Z_p))$ and hence $d'$ is $F$-linear. Thus $\operatorname{der} S = \operatorname{der}_F S$. Also $\operatorname{der}_F B_n(F)$ is the well known $np^n$-dimensional Jacobson-Witt algebra $W_n$ over $F$. We have now proved the following result.

COROLLARY 7.3. *If $S$ is a simple algebra (of prime characteristic) over a ring $K$ and if $n > 0$ then* $\operatorname{der} S_{[n]} = (\operatorname{der} S) \otimes_F B_n(F) + \Gamma \otimes_F W_n$ *(regarded as acting on $S \otimes_F B_n(F)$), where $F$ is the differential centroid of $S_{[n]}$, $\Gamma$ is the centroid of $S$, and $W_n$ is the Jacobson-Witt algebra over $F$.*

We now give a condition on a set $D$ of derivations of $S_{[n]}$ for $S_{[n]}$ to be $D$-simple. If $A = S \otimes_E B$, where $S$ is simple with centroid $E$ and $B = B_n(E)$ and if $d = \sum_i d_i' \otimes b_i + 1_S \otimes d'' \in \operatorname{der} A$, we shall say that $d''$ is the component of $d$ in der $B$, and denote it by $d_B$. A straightforward computation shows that $\tau_{d_B b} = [d, \tau_b]$ for all $b$ in $B$.

PROPOSITION 7.4. *Let $A = S_{[n]}$, identified with $S \otimes {}_E B_n(E)$, where $S$ is a simple algebra over a ring $K$ and $E = C(S)$, and let $D$ be a set of $E$-linear derivations of $A$. Then $A$ is $D$-simple if and only if $B = B_n(E)$ is $D_B$-simple, where $D_B = \{d_B \mid d \in D\}$. In particular, $S_{[n]}$ is differentiably simple, and in fact $d$-simple for some $E$-linear derivation $d$.*

PROOF. In proving the first conclusion we may ignore $K$ and regard $S$ and $A$ as algebras over $E$. We first show that every ideal of $A$ has the form $S \otimes H$ where $H$ is an ideal of $B$. Thus let $M$ be an ideal of $A$. If $\sum_j s_j \otimes b_j \in M$ where the $s_j$ are linearly independent over $E$, then, by the density theorem applied to $T(S)$, for each $j$ there is an $s_j'$ in $S$ such that $s_j' \otimes b_j \in M$. If $s \otimes b \in M$ then $S \otimes b \subseteq M$. It follows that $\{b \in B \mid \exists s \in S$ with $s \otimes b \in M\}$ is an ideal $H$ of $B$, and $M = S \otimes H$. If $H$ is any $D_B$-ideal of $B$ then $S \otimes H$ is a $D$-ideal of $A$. Conversely if $S \otimes H$ is a $D$-ideal we see that $d_B H \subseteq H$ for all $d$ in $D$. It is easy to see that an ideal $H$ of $B$ is a $D_B$-ideal if and only if $S \otimes H$ is a $D$-ideal of $A$. This gives the first conclusion. Now let $d = 1_S \otimes d''$ where $d''$ is the derivation of $B$ given by

$$d'' = (\partial/\partial x_1) + x_1^{p-1}(\partial/\partial x_2) + \cdots + (x_1 \cdots x_{n-1})^{p-1}(\partial/\partial x_n)$$

(where $B = E[x_1, \cdots, x_n]$, $x_i^p = 0$, $(y(\partial/\partial x_i)x_j = \delta_{ij} y (i, j = 1, \cdots, n))$. Then $B$ is $d''$-simple [3], $d$ is $K$-and $E$-linear, and $A$ is $d$-simple (just to show that $A$ is differentiably simple, it suffices to use $\{1_S \otimes \partial/\partial x_i \mid i = 1, \cdots, n\}$). This completes the proof.

In discussing the converse of the Main Theorem it remains to show that $S_{[n]}$ ($S$ simple) has a minimal ideal. Identify $S_{[n]}$ with $S \otimes {}_{Z_p} B_n(Z_p)$, where

$B_n(Z_p) = Z_p[x_1, \cdots, x_n]$, $x_i^p = 0$ $(i = 1, \cdots, n)$. Then it is easy to see that $S \otimes (x_1 \cdots x_n)^{p-1}$ is a minimal ideal of $S_{[n]}$ and in fact is contained in every non-zero ideal of $S_{[n]}$.

The following is an example of an algebra $A$ over a ring $K$ such that $A$ is differentiably simple as a ring but not as an algebra over $K$. Let $S$ be a central simple algebra over $Z_p$, $A = S \otimes_{Z_p} B_n(Z_p)$ for some $n > 0$, $K = B_n(Z_p)$, and regard $A$ as a $K$-algebra in the obvious way. Then a derivation of $A$, as a ring, is $K$-linear if and only if it has the form $\sum_i d_i' \otimes b_i$ and $A$, as a $K$-algebra, has $S \otimes (x_1, \cdots, x_n)$ as a proper differential ideal.

## 8. $D$-semisimple rings

In this section we obtain a $D$-structure theorem which gives an analogue of the part of the Wedderburn-Artin theorem which says that a semisimple artinian ring is a direct sum of simple rings. We state the results for rings; they can be extended to the case of algebras without difficulty.

Let $A$ be a ring and $D$ a set of quasi-derivations of $A$. If $I$ is an ideal of $A$ then the sum of all $D$-ideals of $A$ contained in $I$ is a $D$-ideal of $A$ which we denote by $I_D$. If $I$ is any $D$-ideal of $A$ then $D$ induces a set $D_{A/I}$ of quasi-derivations of $A/I$, and by a slight imprecision in language we shall speak of $D$-ideals of $A/I$ rather than $D_{A/I}$-ideals. Similarly if $D$ consists of derivations of $A$ then $D$ induces a set of derivations on $I$, and if $D$ consists of quasi-derivations and $I$ is a direct summand of $A$ then $D$ induces a set of quasi-derivations on $I$; in either case, if $I$ is $(D \mid I)$-simple we shall also say that $I$ is $D$-simple.

If the ideal $I$ is an intersection $\bigcap M_k$ of ideals of $A$ then it is easy to see that $I_D = \bigcap (M_k)_D$. If $A$ is associative and $R$ is the (Jacobson) radical of $A$ then we call $R_D$ the *$D$-radical* of $A$. For alternative rings (which of course include all associative rings) the radical $R$ is again taken to be the intersection of the regular maximal left ideals, and $R_D$ is taken to be the $D$-radical. Then again $R$ equals the intersection of the primitive ideals [7] and also is the largest ideal $I$ which is radical in the sense that for every $x$ in $I$ the left ideal generated by $\{yx - y \mid y \in A\}$ contains $x$ (and so in the associative case every $x$ has a quasi-inverse). Thus for alternative rings as well as for associative rings we have two characterizations of the $D$-radical: *$R_D$ is the (unique) largest radical $D$-ideal, and $R_D = \bigcap P_D$ where the intersection is over all primitive ideals $P$ of $A$.* If $A$ is a finite-dimensional Lie algebra then the radical $R$ is taken to be the (unique) largest solvable ideal, and in a context in which finite-dimensional power-associative algebras are being discussed the radical $R$ is taken to be the (unique) largest nil ideal (this agrees with the previous definition in the alternative case). In all these cases we call $R_D$ the $D$-radical of $A$ and we say that $A$ is $D$-semisimple if $R_D = 0$. It is easy to see that $A/R_D$ is $D$-semisimple.

We shall use the following dual to Lemma 2.1.

LEMMA 8.1. *Let $H$ be an associative ring, let $M$ be an $H$-module with a maximal submodule $M_1$, and let $D$ be a subset of* $\mathrm{Hom}(M, M)$ *such that* $[D, H_M] \subseteq H_M$. *If $M_2, \cdots, M_q$ (for some $q \geqq 1$) are submodules of $M$ such that $M_1 \supset M_2 \supset \cdots \supset M_q$ and $M_i/M_{i+1} \cong M/M_1$ for $i = 1, \cdots, q-1$, and if $d \in D$ such that $dM_q \not\subseteq M_q$, then there is a submodule $M_{q+1}$, with $M_q \supset M_{q+1}$, and an index $j$, $1 \leqq j \leqq q$, such that $dM_q \subseteq M_{j-1}$ ($M_0 = M$), $dM_{q+1} \subseteq M_j$, and the mapping $m + M_{q+1} \mapsto dm + M_j$ ($m \in M_q$) is an isomorphism of $M_q/M_{q+1}$ onto $M_{j-1}M_j$. In particular $M_q/M_{q+1} \cong M/M_1$.*

PROOF. Let $j$ be the largest index ($1 \leqq j \leqq q$) such that $dM_q \subseteq M_{j-1}$, and let $M_{q+1} = \{m \in M_q \,|\, dm \in M_j\}$. As in the proof of Lemma 2.1, the restriction to $M_q$ of the mapping $m \mapsto dm + M_j$ is a homomorphism with image $M_{j-1}/M_j$ and kernel $M_{q+1}$, and thus gives the required isomorphism.

THEOREM 8.2. *Let $I$ be an ideal of a ring $A$, let $D$ be a set of quasi-derivations of $A$, and suppose that $A/I_D$ has* DCC *on ideals. If $A/I$ is a direct sum of simple rings then $A/I_D$ is a direct sum of $D$-simple rings. In fact if $A/I = S_1 \oplus \cdots \oplus S_k$ ($S_i$ simple) then $A/I_D \cong S_1G_1 \oplus \cdots \oplus S_kG_k$ where, for each $i$, $G_i = 1$ or $S_i$ has prime characteristic $p_i$ and $G_i$ is a finite elementary abelian $p_i$-group.*

PROOF. Without loss of generality we may assume that $I_D = 0$. We first suppose that $A/I$ is simple, and apply Lemma 8.1 with $H = T(A)$, $M = A$ and $M_1 = I$. By DCC the chain of ideals constructed by Lemma 8.1 cannot be extended past some ideal $M_l$. Then $M_l$ is a $D$-ideal and hence $M_l = 0$. Since $(A/I)^2 = A/I$, $T(A)(M_i/M_{i+1}) = M_i/M_{i+1}$ for $i = 0, 1, \cdots, l-1$, $T(A)A = A$, and $A^2 = A$. Also $I$ is nilpotent, as in Lemma 2.2. Since $A$ has a $T(A)$-composition series, any $D$-ideal $L \neq A$ is contained in a maximal ideal $I'$. If $I' \neq I$ then $I + I' = A$ and $A/I' \cong I/I \cap I'$ is nilpotent, contradicting $A^2 = A$. Therefore $I' = I \supseteq L$, $L = 0$, and $A$ is $D$-simple.

Next suppose that $A/I = (L_1/I) \oplus \cdots \oplus (L_k/I)$ where the $L_j$ are ideals of $A$ containing $I$ such that $L_j/I = S_j$ is simple ($k$ is necessarily finite by DCC). For $j = 1, \cdots, k$, let $P_j = \sum_{i \neq j} L_i$. Then $A/P_j \cong (A/I)/(P_j/I) \cong S_j$ is simple, and $A/P_{jD}$ is $D$-simple with unique maximal ideal $P_j$. Moreover $P_{1D} \cap \cdots \cap P_{kD} = (P_1 \cap \cdots \cap P_k)_D = I_D$. We may choose an index $l \leqq k$ and a reordering of the $P_j$ such that $P_{1D} \cap \cdots \cap P_{lD} = I_D$ and such that if $1 \leqq j \leqq l$ then $M_j = \bigcap_{i=1,\cdots,l;\, i \neq j} P_{iD} \neq I_D$. Consider the homomorphism $\tau$ of

$A$ into $(A/P_{1D}) \oplus \cdots \oplus (A/P_{lD})$ given by $\tau x = (x + P_{1D}, \cdots, x + P_{lD})(x \in A)$. This has kernel $I_D$. Since $M_j \not\subseteq P_{jD}$, $P_{jD} + M_j = A$. Hence for any $x + P_{jD}$, there is a $y$ such that $\tau y = (0, \cdots, x + P_{jD}, \cdots, 0)$. Then $\tau$ is onto and $A/I_D \cong (A/P_{1D}) \oplus \cdots \oplus (A/P_{lD})$. Counting the number of maximal ideals on both sides we get $l \geqq k$, and so $l = k$. This and the Main Theorem complete the proof.

We remark that the theorem would be false without the assumption of DCC on ideals, as is shown by the following example. $A = F[x]$ ($F$ a field of characteristic 0), $I = (1 + x)$, $D = \{x(\partial/\partial x)\}$, where $I_D = 0$ but $(x)$ is a $D$-ideal.

COROLLARY 8.3. *Let $A$ be an (associative or) alternative ring with* DCC *on ideals and with radical $R$, and let $D$ be a set of quasi-derivations on $A$. If $A$ is $D$-semisimple and $A/R$ has* DCC *on left ideals then $A$ is a direct sum of $D$-simple rings.*

PROOF. $A/R$ is a subdirect sum of primitive rings which are either associative or Cayley rings [7]. Since $A/R$ is artinian it is a finite direct sum of simple rings by the same argument as in the associative case. Hence Theorem 8.2 gives the result.

We now discuss a similar result for an important class of power-associative rings, the flexible rings. A ring $A$ is called *flexible* if $(xy)x = x(yx)$ for all $x$, $y$ in $A$. Oehmke [10] proved that a finite-dimensional semisimple flexible strictly power-associative algebra over a field of characteristic $\neq 2, 3$ is a direct sum of simple algebras with a unit element. Using Theorem 8.2 we now give a new proof of this result, extending it to include the characteristic 3 case as well as generalizing it to a result on $D$-semisimple algebras. In giving this result we make use of the following definitions and facts. Let $A$ be an algebra over a field of characteristic $\neq 2$. Then $A^+$ denotes the algebra with the same underlying vector space as $A$ and with new multiplication $x \cdot y = (1/2)(xy + yx)$. For each $x$ in $A$ let $d_x$ be the mapping of $A$ into $A$ defined by $d_x y = [x, y]$ $(y \in A)$. A direct verification shows that each $d_x$ is a derivation of $A^+$ if (and only if) $A$ is flexible. Obviously a subspace of $A$ is an ideal of $A$ if and only if it is a $\{d_x \mid x \in A\}$-ideal of $A^+$.

COROLLARY 8.4. *Let $A$ be a finite-dimensional power-associative algebra over a field of characteristic $\neq 2$, with nilradical $R$ and with a given (possibly empty) set $D$ of quasi-derivations, and suppose that $A$ is $D$-semisimple. If $A/R$ is flexible and strictly power-associative then $A$ is direct sum of $D$-simple algebras (and is flexible, strictly power-associative and has a unit element). If $A$ has a trace form then again $A$ is a direct sum of $D$-simple algebras (and at characteristic $\neq 5$ is a non-commutative Jordan algebra).*

PROOF. The trace form case follows immediatly from Theorem 8.2 and Albert's theorem on trace forms [13, p. 136]. Also when $A/R$ is commutative the result holds by Theorem 8.2 and the fact [2, 8] that semisimple commutative strictly power-associative algebras are direct sums of simple algebras with a unit element (if $S$ has unit element then so does $SG$) (the strictness of the power-associativity is relevant only at characteristics 3 and 5). Now suppose that $A/R$ is flexible and strictly power-associative. Then $(A/R)^+$ is commutative and strictly power-associative. Also $(A/R)^+$ has no non-zero nil $\{d_x \mid x \in A/R\}$-ideal. By the just proved commutative case, $(A/R)^+$ is a direct sum of $\{d_x \mid x \in A/R\}$-simple ideals which have a unit element. These ideals of $(A/R)^+$ are also simple ideals of $A/R$, and the unit element of $(A/R)^+$ is also the unit element of $A/R$; this latter fact follows quickly from the flexible law, as in [4], or, using power-associativity, from an idempotent decomposition. We may now apply Theorem 8.2 to get the desired result. This completes the proof.

The decomposition of a $D$-semisimple ring into $D$-simple ideals can also be proved easily in the finite-dimensional associative case by using the minimal $D$-ideals. Before discovering the present version of Theorem 8.2 the author had used the minimal rather than maximal ideals to give a proof of Theorem 8.2 in the case when $A$ is a finite-dimensional power-associative algebra and the $S_i$ have a unit element. This also gave Corollaries 8.3 and 8.4. This was announced briefly in [5]. After [5] was submitted, the author received from T.S. Ravisankar, of Madras, India, a copy of a recent manuscript which gives a proof, different from the author's, that if a finite-dimensional flexible strictly power-associative algebra of characteristic $\neq 2, 3$ is $D$-semisimple ($D$ a set of derivations) then it satisfies the conclusion of the first part of Corollary 8.4. He also establishes in another proof the trace form case (again excluding characteristic 3).

While discussing semisimple flexible algebras we also mention the deeper question of determining the structure of $A^+$ for a simple flexible algebra $A$ (of characteristic $\neq 2$). This was answered by the author [4] in the finite-dimensional case as an application of the Main Theorem of the present paper. Aside from giving a uniform proof of the various special cases proved by a number of authors (see [4]), this solved the previously unsettled degree 2 characteristic $p$ case, included as well consideration of nil simple algebras, and showed that the result does not depend on power-associativity. Since the Main Theorem has now been proved in a more general form than when [4] was written, we now have the following form of the result on simple flexible rings.

THEOREM 8.5. *Let $A$ be a simple flexible ring of characteristic $\neq 2$. If $A$ is not anti-commutative and if $A^+$ has a minimal ideal, then either $A^+$ is simple or the characteristic is prime and $A^+ \cong B_n(E)$ for some $n > 0$ and some field $E$ containing the centroid of $A$.*

The proof is essentially the same as for the finite-dimensional case in [4]. Since $A^+$ is differentiably simple, the Main Theorem implies that if $A^+$ is not simple then the characteristic is prime and there is a commutative simple ring $S$ such that $A^+ \cong S_{[n]}$ for some $n > 0$. The problem then is to show that $S$ must be associative, and this may be done by showing that $S = E1$ where $E = C(S)$; for the details of the proof of this, see [4].

## 9. Semisimple Lie algebras

In this final section we apply the Main Theorem to the study of the structure of finite dimensional semisimple Lie algebras of characteristic $p$. The reason that this can be done is that in a Lie algebra $L$ a non-abelian ideal $M$ is minimal if and only if $M$ is $(\mathrm{ad}_M L)$-simple. We begin with a preliminary result on the relation between $L$ and its minimal ideals. All the Lie algebras considered are assumed to be finite-dimensional over a field. For any Lie algebra $L$ we write inder $L$ for the Lie algebra of inner derivations of $L$, i.e., inder $L = \{\mathrm{ad}\, x \mid x \in L\}$.

LEMMA 9.1. *Let $D$ be a set of derivations of a finite-dimensional Lie algebra $L$ and suppose that $L$ is $D$-semisimple. Then $L$ has only finitely many minimal $D$-ideals, say $L_1, \cdots, L_r$, their sum $M$ is direct, each $L_i$ is $(D \cup \mathrm{inder}\, L)$-simple, the mapping $x \mapsto \mathrm{ad}_M x (x \in L)$ is an isomorphism of $L$ onto a subalgebra of* der $M$ *containing* inder $M$, *and the mapping $d \mapsto d \mid M$ $(d \in D)$ of $D$ into* der $M$ *is one-one.*

PROOF. Without loss of generality we may assume that $D$ is a subalgebra of der $L$ containing inder $L$. Since $L$ is centerless we may identify $L$ with inder $L$ and thus since $[d, \mathrm{ad}_L x] = \mathrm{ad}_L(dx)$ we may assume that $L$ is an ideal of $D$ with 0 centralizer in $D$. Then it follows that the $D$-ideals of $L$ are exactly the ideals of $D$ contained in $L$, and $D$ is semisimple. Therefore by replacing $L$ by $D$ it will suffice to prove the result when $L$ is semi-simple and $D = \mathrm{inder}\, L$. With these assumptions, let $M = L_1 + \cdots + L_r$ be a maximal direct sum of minimal ideals of $L$. Then $M$ contains every minimal ideal of $L$, the annihilator in $L$ of $M$ contains no minimal ideal of $L$ (since any such would be abelian) and so is 0, and hence $x \mapsto \mathrm{ad}_M x$ is an isomorphism of $L$ into der $M$. The remaining conclusions follow easily. This completes the proof.

In the case in which $D = \operatorname{der} L$, the results of Lemma 9.1, except for the final statement, are due to Seligman [16], but the proof given here is shorter.

COROLLARY 9.2. *Let $L$ be a finite-dimensional semisimple Lie algebra with a set $D$ of derivations. Then any minimal $D$-ideal of $L$ is a minimal ideal of $L$.*

PROOF. A minimal $D$-ideal is differentiably simple and so any ideal of $L$ properly contained in it is nilpotent and hence 0.

We call the sum of the minimal ideals of a Lie algebra $L$ the *socle* of $L$, and if $D$ is a set of derivations of $L$ we call the sum of the minimal $D$-ideals of $L$ the $D$-socle of $L$. Thus if $L$ is semisimple the $D$-socle equals the socle.

The determination of the differentiably simple algebras and their derivation algebras leads quickly *via* Lemm 9.1 to the following description of all the semisimple Lie algebras (and their derivations) in terms of the socle.

Let $S_1, \cdots, S_r$ be simple Lie algebras over a field $F$ of characteristic $p$, and let $n_1, \cdots, n_r$ be non-negative integers (not necessarily distinct). Write $S = \bigoplus_{i=1}^r S_i \otimes B_i$ where $B_i$ denotes $B_{n_i}(F)$ and $B_i = F$ if $n_i = 0$ (all algebras and tensor products considered here are over $F$), and identify $S$ with inder $S$, so that

$$\begin{aligned} S = \operatorname{inder} S &= \textstyle\bigoplus_{i=1}^r (\operatorname{inder} S_i) \otimes B_i \\ &\subseteq \operatorname{der} S = \textstyle\bigoplus_{i=1}^r \big((\operatorname{der} S_i) \otimes B_i + \Gamma_i \otimes \operatorname{der} B_i\big) \end{aligned}$$

where $\Gamma_i$ denotes the centroid of $S_i$. Now let $L$ be any subalgebra of $\operatorname{der} S$ containing $S$ (hence $L$ is uniquely determined by a subalgebra of $\bigoplus_{i=1}^r \big((\operatorname{outder} S_i) \otimes B_i + \Gamma_i \otimes \operatorname{der} B_i)\big)$. For $i = 1, \cdots, r$ let $L_i$ denote the set of components in $\operatorname{der}(S_i \otimes B_i)$ of elements of $L$, and if $S$ is central, so that $\operatorname{der}(S_i \otimes B_i) = (\operatorname{der} S_i) \otimes B_i + 1_{S_i} \otimes \operatorname{der} B_i$, let $L_{B_i}$ denote the set of components in $\operatorname{der} B_i$ of elements of $L_i$ (in the terminology of §7).

THEOREM 9.3. *Every finite-dimensional semisimple Lie algebra of prime characteristic is isomorphic to one of the algebras $L$ just constructed, and the semisimple algebra uniquely determines $r$ and the pairs $(S_i, n_i)$, $i = 1, \cdots, r$, up to isomorphism and reordering. The algebra $L$ constructed is semisimple if and only if $S_i \otimes B_i$ is $L_i$-simple (which when $S_i$ is central is equivalent to $B_i$ being $L_{B_i}$-simple) for $i = 1, \cdots, r$. The mapping $x \mapsto \operatorname{ad}_L x$ ($x \in N_{\operatorname{der} S} L$) is an isomorphism of the normalizer of $L$ in* der $S$ *onto* der $L$. *The same results hold with differentiably semisimple in place of semisimple provided the condition on $L_i$ (or $L_{B_i}$) is replaced by the same condition on $(N_{\operatorname{der} S} L)_i \big(or (N_{\operatorname{der} S} L)_{B_i}\big)$.*

PROOF. By Lemma 9.1 any semisimple algebra with socle $M$ is isomorphic to a subalgebra of $\operatorname{der} M$ containing $\operatorname{inder} M$, and by the Main Theorem $M$ is isomorphic to some $S$ of the above form for suitable pairs $(S_i, n_i)$, these being essentially uniquely determined by $M$. This gives the first sentence. The ideal $S_i \otimes B_i$ of $L$ is minimal if and only if it is $L$-simple, or equivalently $L_i$-simple, and when $S_i$ is central this is equivalent to $B_i$ being $L_{B_i}$-simple. Since the centralizer of $S$ in $L$ is 0, every minimal ideal of $L$ is contained in $S$. Hence if each $S_i \otimes B_i$ is minimal then $L$ is semisimple. Conversely if $L$ is semisimple then each $S_i \otimes B_i$ is minimal because any ideal of $L$ properly contained in $S_i \otimes B_i$ would also be a proper ideal of $S_i \otimes B_i$ and hence nilpotent. This proves the second sentence. The mapping $\tau$ defined by $\tau x = \operatorname{ad}_L x (x \in N_{\operatorname{der} S} L)$ is a homomorphism into $\operatorname{der} L$. If $\operatorname{ad}_L x = 0$ then $\operatorname{ad}_S x = 0$ and $x = 0$. Hence $\tau$ is one-one. Suppose $d \in \operatorname{der} L$ and let $x$ be the unique element of $\operatorname{der} S$ such that $x(s) = [x, s] = d(s)$ $(s \in S)$. If $y \in L$ and $s \in S$ then

$$(dy)(s) = [dy, s] = -[y, ds] + d[y, s] = -[y, [x, s]] + [x, [y, s]] = [x, y](s) .$$

Hence $d = \operatorname{ad}_L x$, $x \in N_{\operatorname{der} S} L$ and $\tau$ is onto. The final statement may be proved the same as the first two by replacing semisimple, socle, ideal by differentiably semisimple, etc., and $L$-simple by $(\operatorname{der} L)$-simple, using the characterization of $\operatorname{der} L$ just obtained. This completes the proof.

COROLLARY 9.4. *Let $F$ be a field of characteristic $p$. If every simple Lie algebra over $F$ of dimension $\leqq m$ has all its derivations inner then every semisimple Lie algebra over $F$ of dimension $\leqq \min\{m+1, 3p\}$ is a direct sum of simple algebras.*

This is an immediate consequence of Theorem 9.3, and gives a generalization of Kostrikin's result [9] that a semisimple Lie algebra of dimension $< p$ over an algebraically closed field of characteristic $p > 5$ is a direct sum of simple algebras (of classical type). On the other hand, Theorem 9.3 shows that starting from a 3-dimensional central simple Lie algebra over $F$, we can construct a semisimple Lie algebra of dimension $3p+1$ and a perfect semisimple Lie algebra of dimension $4p$, neither of which is a direct sum of simple algebras.

UNIVERSITY OF CALIFORNIA, RIVERSIDE

REFERENCES

[1] A. A. ALBERT, *Power-associative rings*, Trans. Amer. Math. Soc. **64** (1948), 552-593.

[2] ———, *A theory of power-associative commutative algebras*, Trans. Amer. Math. Soc. **69** (1950), 503-527.

[3] ———, *On commutative power-associative algebras of degree two*, Trans. Amer. Math. Soc. **74** (1953), 323-343.

[4] R. E. BLOCK, *Determination of $A^+$ for the simple flexible algebras*, Proc. Nat. Acad. Sci. U.S.A. **61** (1968), 394-397.

[5] ———, *Differentiably simple algebras*, Bull. Amer. Math. Soc. **74** (1968), 1086-1090.

[6] L. R. HARPER, JR., *On differentiably simple algebras*, Trans. Amer. Math. Soc. **100** (1961), 63-72.

[7] E. KLEINFELD, *Primitive alternative rings and semisimplicity*, Amer. J. Math. **77** (1955), 725-730.

[8] L. A. KOKORIS, *New results on power-associative algebras*, Trans. Amer. Math. Soc. **77** (1954), 363-373.

[9] A. I. KOSTRIKIN, *Squares of adjoint endomorphisms in simple Lie p-algebras*, Izv. Ak. Nauk SSSR Ser. Mat. **31** (1967), 445-487 (in Russian).

[10] R. H. OEHMKE, *On flexible algebras*, Ann. of Math. (2) **68** (1958), 221-230.

[11] E. C. POSNER, *Differentiably simple rings*, Proc. Amer. Math. Soc. **11** (1960), 337-343.

[12] R. REE, *On generalized Witt algebras*, Trans. Amer. Math. Soc. **83** (1956), 510-546.

[13] R. D. SCHAFER, An Introduction to Nonassociative Algebras, New York, Academic Press, 1966.

[14] ———, *Standard Algebras*, Pac. J. Math. **29** (1969), 203-223.

[15] A. SAGLE and D. J. WINTER, *On homogeneous spaces and reductive subalgebras of simple Lie algebras*, Trans. Amer. Math. Soc. **128** (1967), 142-147.

[16] G. B. SELIGMAN, *Characteristic ideals and the structure of Lie algebras*, Proc. Amer. Math. Soc. **8** (1957), 159-164.

[17] H. ZASSENHAUS, *Über Lie'sche Ringe mit Primzahlcharakteristik*, Abh. Math. Sem. Hamburg **13** (1939), 1-100.

(Received September 17, 1968.)