ON A FAMILY OF LIE ALGEBRAS OF CHARACTERISTIC p

BY

S. A. JENNINGS AND RIMHAK REE(1)

Introduction. We study a family of Lie algebras of characteristic p which are defined as subalgebras of the derivation algebra of the group algebra of an elementary p-group. In particular we show that simple Lie algebras of dimensions $m(p^n-1)$, mp^n, p^n-2, where m and n are arbitrary integers such that $1 \leqq m < n$, and where $p > 2$ only for the dimensions p^n and p^n-2, are associated with this family. The algebras studied by M. S. Frank [2] are included in our family, but those of dimension $m(p^n-1)$ in general appear to be new.

Since this paper was written, the paper of A. A. Albert and M. S. Frank [1] has been published. The relation between the algebras studied in [1] and those in this paper will be mentioned in §9, although it is not thoroughly clarified yet.

1. **Definition of the family $\mathfrak{F}$.** Let Φ be an algebraically closed field of characteristic $p > 0$, and $\mathfrak{A}$ the group algebra over Φ of an abelian group $\mathfrak{G}$ of type $(p, p, \cdots, p)$ and order p^n. Let $D_0, \cdots, D_m$ be derivations(2) of $\mathfrak{A}$ such that $D_i \circ D_j = 0$ for all i, j, and let $a_0, \cdots, a_m \in \mathfrak{A}$ be such that

$$D_i a_j = D_j a_i \qquad (i, j = 0, 1, \cdots, m). \tag{1.0.1}$$

Consider the set $\mathfrak{L} = \mathfrak{L}(D_i, a_i)$ of all derivations of the form $D = f_0 D_0 + \cdots + f_m D_m$, where $f_i \in \mathfrak{A}$ satisfy $\sum D_i f_i = \sum a_i f_i$. By an elementary computation, we see easily that $\mathfrak{L}$ is a subalgebra of the derivation algebra(2) of $\mathfrak{A}$. (The case when $m+1=n$, $a_0 = \cdots = a_m = 0$, $D_i = \partial/\partial g_i$, where $g_0, \cdots, g_m$ is a set of independent generators of the group $\mathfrak{G}$, was considered by M. S. Frank [2], and the case $m+1=n$, $a_i=1$, $D_i=\partial/\partial g_i$, by A. A. Albert and M. S. Frank [1].)

In this paper, we study the family $\mathfrak{F}$ of algebras $\mathfrak{L}(D_i, a_i)$, where $D_0, \cdots, D_m$ satisfy the following conditions:

Received by the editors February 27, 1956.

(1) This paper was written during the summer of 1955 while the first author was a member of the Summer Research Institute of the Canadian Mathematical Congress and the second under grant G489 from the National Research Council of Canada. The authors wish to express their gratitude to both of these organizations.

(2) By a *derivation* D of an algebra $\mathfrak{A}$ over a field Φ we mean a linear mapping of $\mathfrak{A}$, regarded as a vector space over Φ, into itself such that $D(fg) = (Df)g + f(Dg)$ for all f, g in $\mathfrak{A}$. If D_1, D_2 are derivations of $\mathfrak{A}$, then $D_1 \circ D_2 = D_1D_2 - D_2D_1$ is easily seen to be a derivation of $\mathfrak{A}$. The totality of derivations of $\mathfrak{A}$ forms a Lie algebra over Φ with the ordinary addition and the multiplication $\circ$. It is called the *derivation algebra* of $\mathfrak{A}$.

(1.0.2) $D_i \circ D_j = 0$ for all i, j;

(1.0.3) $\sum f_i D_i = 0$, where $f_i \in \mathfrak{A}$, implies $f_i = 0$ for all i;

(1.0.4) $D_i f = 0$ for all i implies $f \in \Phi$;

(1.0.5) If $f \in \mathfrak{A}$ is such that $D_i f = \lambda_i f$, where $\lambda_i \in \Phi$, for all i, then $f = 0$ or f is a unit in $\mathfrak{A}$.

The elements $a_0, \cdots, a_m$ of $\mathfrak{A}$ will be always assumed to be chosen such that (1.0.1) is satisfied. An ordered set $(D_0, \cdots, D_m)$ of derivations of $\mathfrak{A}$ will be called a *semi-system* if (1.0.2)–(1.0.4) are satisfied, and a *system* if (1.0.2)–(1.0.5) are satisfied[3]. Since we fix $m > 0$ throughout this paper, a semi-system or a system $(D_0, \cdots, D_m)$ will usually be denoted by the notation (D_i). It is shown in [4] that $m < n$ must hold for a system. The following lemma is also shown in [4]:

LEMMA 1.1. *For a system (D_i), if f and $a_i \in \mathfrak{A}$ are such that $D_i f = a_i f$ for all i, then $f = 0$ or f is a unit in $\mathfrak{A}$.*

2. **Equivalent systems.** Two semi-systems (D_i) and (D_i') are said to be *equivalent* if there exist $c_{ij} \in \mathfrak{A}$ such that

$$D_i' = \sum_{s=0}^{m} c_{is} D_s \tag{2.0.1}$$

for $i = 0, \cdots, m$, and such that $\det(c_{ij})$ is a unit in $\mathfrak{A}$. From the properties (1.0.2)–(1.0.3) for (D_i') it follows easily that

$$D_i' c_{jk} = D_j' c_{ik} \tag{2.0.2}$$

for all i, j, and k.

LEMMA 2.1. *A semi-system equivalent to a system is a system.*

Proof. Let (D_i) be a semi-system equivalent to a system (D_i'), and let the relation (2.0.1) hold. Suppose $f \in \mathfrak{A}$ and $\lambda_i \in \Phi$ are such that $D_i f = \lambda_i f$ for all i. Then (2.0.1) yields $D_i' f = (\sum_s c_{is} \lambda_s) f$ for all i. Then from Lemma 1.1 it follows that $f = 0$ or f is a unit in $\mathfrak{A}$. Therefore (D_i') is a system.

Let (D_i) and (D_i') be equivalent systems related by (2.0.1). Let $(c_{ij})^{-1} = (c'_{ij})$. Then $D_i = \sum c'_{is} D'_s$, and $\sum f_i D_i = \sum f_i' D_i'$, where $f_i' = \sum_s f_s c'_{st}$. It may be readily verified that $\sum D_i f_i = \sum a_i f_i$ if and only if $\sum D_i' f_i' = \sum a_i' f_i'$, where

$$a_i' = \sum_s (a_s c_{is} - D_s c_{is}), \qquad i = 0, 1, \cdots, n. \tag{2.2.1}$$

Thus we may state

[3] *Semi-system* and *system* in this paper may be called in the language of [4] "orthogonal system satisfying (1.0.4)" and "orthogonal system satisfying (1.0.4)–(1.0.5)," respectively.

THEOREM 2.2. *If the system* (D_i') *is given by* (2.0.1), *then* $\mathfrak{L}(D_i, a_i) = \mathfrak{L}(D_i', a_i')$, *where* a_i' *are given by* (2.2.1).

The following lemma is useful in changing the formula (2.2.1).

LEMMA 2.3. *Let* (D_i) *be a system, and let* $a_{ij} \in \mathfrak{A}$ *be such that* $D_i a_{jk} = D_j a_{ik}$ *for all* $i, j, k = 0, 1, \cdots, m$. *Let* $\bar{a}_{ij}$ *be the cofactor of* a_{ji} *in the determinant of the* $(m+1) \times (m+1)$ *matrix* (a_{ij}). *Then* $\sum_{s=0}^{m} D_s \bar{a}_{is} = 0$ *for all* i.

Proof. For simplicity we assume that $i=0$. The other cases may be proved similarly. Since

$$\det (a_{ij}) = \sum \epsilon(s_0 s_1 \cdots s_m) a_{s_0 0} a_{s_1 1} \cdots a_{s_m m},$$

where $\epsilon(s_0 s_1 \cdots s_m)$ denotes $+1$ if the permutation

$$\pi = \begin{pmatrix} 0 & 1 \cdots m \\ s_0 & s_1 \cdots s_m \end{pmatrix}$$

is even, -1 if π is odd, therefore

$$\bar{a}_{0s} = \sum{}' \epsilon(s s_1 \cdots s_m) a_{s_1 1} \cdots a_{s_m m},$$

where the summation $\sum'$ runs over all permutations π such that $s_0 = s$. Since D_s is a derivation, we have

$$\sum D_s \bar{a}_{0s}$$
$$= \sum \epsilon(s s_1 \cdots s_m)\left[(D_s a_{s_1 1}) a_{s_2 2} \cdots a_{s_m m} + a_{s_1 1}(D_s a_{s_2 2}) \cdots a_{s_m m} + \cdots \right],$$

where the summation on the right runs over all permutations

$$\pi = \begin{pmatrix} 0 & 1 \cdots m \\ s & s_1 \cdots s_m \end{pmatrix}.$$

By hypothesis $D_s a_{s_1 1} = D_{s_1} a_{s1}$. Since $\epsilon(s s_1 \cdots s_m) = -\epsilon(s_1 s \cdots s_m)$, the two terms $\epsilon(s s_1 \cdots s_m)(D_s a_{s_1 1}) a_{s_2 2} \cdots a_{s_m m}$ and $\epsilon(s_1 s \cdots s_m)(D_{s_1} a_{s1}) a_{s_2 2} \cdots a_{s_m m}$ cancel each other. Similarly all the other terms are divided into such pairs. Thus we see that $\sum D_s \bar{a}_{0s} = 0$. Similarly $\sum D_s \bar{a}_{is} = 0$ for all i. Thus Lemma 2.3 is proved.

Using Lemma 2.3, we can change (2.2.1) into a more convenient form. We set $a_{ij} = c'_{ij}$. Then the formula corresponding to (2.0.2) shows that a_{ij} satisfy the condition of Lemma 2.3. Let $f = \det (c'_{ij})$. Then $\bar{a}_{ij} = f c_{ij}$. Hence by Theorem 2.2 we have $\sum_s D_s(f c_{is}) = 0$ for all i. Therefore $f \sum D_s c_{is} + \sum c_{is} D_s f = 0$, and we obtain

$$\sum D_s c_{is} + \sum c_{is}(f^{-1} D_s f) = 0. \tag{2.3.1}$$

From (2.3.1) and (2.2.1) we see that

$$a_i' = \sum_s c_{is}(a_s + f^{-1} D_s f),\ f = \det (c_{ij})^{-1}, \text{ for all } i. \tag{2.3.2}$$

3. **Principal systems.** A system (D_i) is called *principal* if $D_if\in\Phi$ for all i implies $f\in\Phi$. Elements $g_1, \cdots, g_n\in\mathfrak{A}$ are said to form a set of *principal generators* of $\mathfrak{A}$ if $g_i^p=1$ for all i and if the p^n elements $g_1^{u_1}\cdots g_n^{u_n}$, where $0\leqq u_i<p$, $g_i^0=1$, form a basis of $\mathfrak{A}$ over Φ. The following Lemmas 3.1 and 3.2 are proved in [4].

LEMMA 3.1. *Any system is equivalent to a principal system.*

LEMMA 3.2. *For any principal system (D_i), there exists a set of principal generators $g_1, \cdots, g_n$ of $\mathfrak{A}$ such that*

$$(3.2.1)\qquad D_i = \sum_{s=1}^{n} \alpha_{is}G_s$$

for all i, where $\alpha_{ij}\in\Phi$ and where $G_i=g_i\partial/\partial g_i$ are derivations of $\mathfrak{A}$ such that $G_ig_j=\delta_{ij}g_i$ for all i, j and δ_{ij} is the Kronecker delta. The principal generators (g_i) will be said to belong to the principal system (D_i).

From (1.0.3)–(1.0.4) we see easily that the α_{ij} in (3.2.1) must satisfy (3.2.2)–(3.2.3) below:

(3.2.2) If $u_1, \cdots, u_n$ are integers such that $\sum_s \alpha_{is}u_s = 0$ for all i, then $u_i \equiv 0 \pmod p$ for all i;

(3.2.3) If $\xi_0, \cdots, \xi_m \in \Phi$ are such that $\sum_{s=0}^{m} \xi_s\alpha_{si} = 0$ for all i, then $\xi_i = 0$ for all i.

Conversely if elements $\alpha_{ij}\in\Phi$ satisfy (3.2.2)–(3.2.3) and if D_i are defined by (3.2.1) with an arbitrary set of principal generators $g_1, \cdots, g_n$ of $\mathfrak{A}$, then (D_i) is a system, as is proved in §9 of [4]. We shall now show that the system (D_i) is principal. Let $D_if\in\Phi$ for all i, where $f=\sum\gamma_ug^u$, $\gamma_u\in\Phi$. Then $\gamma_u(e_i\cdot u)=0$ for all $u\neq 0$ and i, and hence by (3.2.4) we have $\gamma_u=0$ for all $u\neq 0$. Therefore $f\in\Phi$, and hence (D_i) is shown to be principal.

For any integers m and n such that $0\leqq m<n$, there exist $\alpha_{ij}\in\Phi$ such that (3.2.2)–(3.2.3) hold, since Φ is assumed to be algebraically closed and hence infinite.

Suppose that the system (D_i) is given by (3.2.1). Consider the $(m+1)$-dimensional vector space $\mathfrak{R}$ over Φ consisting of all $(m+1)$-tuples $x=(\xi_0, \cdots, \xi_m)$, $\xi_i\in\Phi$, and also the n-dimensional vector space $\overline{\mathfrak{V}}$ over Φ consisting of all n-tuples $u=(u_1, \cdots, u_n)$, $u_i\in\Phi$. Let $\mathfrak{V}$ be the subset of $\overline{\mathfrak{V}}$ consisting of all u such that $u_i\in GF(p)\subset\Phi$ for $i=1, 2, \cdots, n$. Define a bilinear function $x\cdot u$, where $x\in\mathfrak{R}$, $u\in\overline{\mathfrak{V}}$, with values in Φ by setting $x\cdot u=\sum_{i,j}\xi_i\alpha_{ij}u_j$. Then (3.2.2) and (3.2.3) are equivalent to (3.2.4) and (3.2.5), below, respectively:

(3.2.4) If $x\cdot u = 0$ for all $x \in \mathfrak{R}$ and if $u \in \mathfrak{V}$ then $u = 0$;

(3.2.5) $x\cdot u = 0$ for all $u \in \mathfrak{V}$ implies $x = 0$.

Suppose now that $g_1, \cdots, g_n$ are principal generators belonging to the principal system (D_i). For $u=(u_1, \cdots, u_n)\in\mathfrak{V}$ we shall write $g^u = g_1^{u_1}\cdots g_n^{u_n}$. Let $e_i\in\mathfrak{R}$ be a vector whose $(i+1)$th component is 1 and whose other components are all 0. Then $D_i g^u = (e_i\cdot u)g^u$, and, more generally,

(3.2.6) $(\xi_0 D_0 + \cdots + \xi_m D_m)g^u = (x\cdot u)g^u$, where $x = (\xi_0, \cdots, \xi_m) \in \mathfrak{R}$.

The notations introduced in this section will be preserved in what follows.

4. Type and dimension of $\mathfrak{L}$. For a derivation D and an element $a\in\mathfrak{A}$ we define a linear mapping $D-a$ of $\mathfrak{A}$, regarded as a vector space over Φ, into itself by $(D-a)f=Df-af$. Then the condition $D_ia_j=D_ja_i$ is equivalent to saying that the linear mappings D_i-a_i and D_j-a_j are commutative. Therefore, if $\mathfrak{L}=\mathfrak{L}(D_i; a_i)\in\mathfrak{F}$, then there exist a nonzero element $b\in\mathfrak{A}$ and $\alpha_i\in\Phi$ such that

(4.0.1) $$(D_i - a_i)b = \alpha_i b$$

for all i: b will be called a *proper element* of $(D_i; a_i)$ and $(\alpha_0, \cdots, \alpha_m)$ *proper root* belonging to b.

LEMMA 4.1. *If (D_i) is a principal system and if b is a proper element of $(D_i; a_i)$, then b is a unit in $\mathfrak{A}$ and all the other proper elements of $(D_i; a_i)$ are, up to a constant factor, of the form bg^u, where $g_1, \cdots, g_n$ is any fixed set of principal generators of $\mathfrak{A}$ belonging to (D_i) and where u runs over $\mathfrak{V}$. If $(\alpha_0, \cdots, \alpha_m)$ is the proper root belonging to b, then $(\alpha_0-(e_0\cdot u), \cdots, \alpha_m-(e_m\cdot u))$ is the proper root belonging to bg^u.*

Proof. The fact that b is a unit follows immediately from Lemma 1.1, since $D_ib=(a_i-\alpha_i)b$ for all i.

Let $D_ib'=(a_i-\alpha_i')b'$ for all i. Then $D_i(b^{-1}b')=(\alpha_i-\alpha_i')b^{-1}b'$. We may suppose that $b^{-1}b'=\sum_{u\in\mathfrak{V}}\gamma_u g^u$, where $\gamma_u\in\Phi$. Then $(e_i\cdot u)\gamma_u=(\alpha_i-\alpha_i')\gamma_u$ for all i. Therefore if $\gamma_u\neq 0$ then $e_i\cdot u=\alpha_i-\alpha_i'$ for all i. Furthermore, if $\gamma_{u'}\neq 0$ then $e_i\cdot u=\alpha_i-\alpha_i'=e_i\cdot u'$, and hence $(e_i\cdot u-u')=0$ for all i. Hence we have $u=u'$. Therefore, any proper element of $(D_i; a_i)$ is, up to a constant factor, of the form bg^u, and the proper root belonging to bg^u is $(\alpha_0-(e_0\cdot u), \cdots, \alpha_m-(e_m\cdot u))$.

It is easily seen that bg^u is a proper element of $(D_i; a_i)$ for any $u\in\mathfrak{V}$. Thus Lemma 4.1 is proved.

By Theorem 2.2 and Lemma 3.1, every $\mathfrak{L}\in\mathfrak{F}$ can be expressed as $\mathfrak{L}=\mathfrak{L}(D_i; a_i)$ with some principal system (D_i). If there exists a proper element b of $(D_i; a_i)$ such that the proper root belonging to b is zero, i.e. $\alpha_i=0$ for all i, then we shall say that $\mathfrak{L}$ is of *type* I. Otherwise, $\mathfrak{L}$ is said to be of *type* II. We will show that the above definition of the type of $\mathfrak{L}=\mathfrak{L}(D_i; a_i)$ is independent of the principal system (D_i) used to form $\mathfrak{L}$. This will be done by computing the dimension of $\mathfrak{L}$ over Φ as follows.

Let b be a proper element of $\mathfrak{L}=\mathfrak{L}(D_i; a_i)$ and let $(\alpha_0, \cdots, \alpha_m)$ be the proper root belonging to b. Since b is a unit in $\mathfrak{A}$, every element $D\in\mathfrak{L}$ can be written in the form $D=b\sum f_iD_i$, with $f_i\in\mathfrak{A}$. An elementary computation shows that the condition $\sum D_i(bf_i)=\sum a_ibf_i$ is equivalent to $\sum D_if_i=\sum\alpha_if_i$. Hence we have $\mathfrak{L}(D_i; a_i)=b\mathfrak{L}(D_i; \alpha_i)$ where $b\mathfrak{L}=\{bD \mid D\in\mathfrak{L}\}$. In particular, $\dim \mathfrak{L}(D_i; a_i)=\dim \mathfrak{L}(D_i; \alpha_i)$. Suppose now that (D_i) is a principal system and the $g_1, \cdots, g_n$ form a set of principal generators belonging to (D_i). Consider $D=\sum f_iD_i\in\mathfrak{L}(D_i; \alpha_i)$. We may write $f_i=\sum_{u\in\mathfrak{B}}\phi_{i,u}g^u$, where $\phi_{i,u}\in\Phi$. Then the condition $\sum D_if_i=\sum\alpha_if_i$ is easily seen to be equivalent to

$$\sum_i (e_i\cdot u)\phi_{i,u} = \sum_i \alpha_i\phi_{i,u} \qquad \text{(for all } u).$$

We set $D_u=g^u\sum_i\phi_{i,u}D_i$. Then $D=\sum D_u$, $D_u\in\mathfrak{L}(D_i; \alpha_i)$. Thus the vector space $\mathfrak{L}(D_i; \alpha_i)$ over Φ is a direct sum of the vector spaces $\mathfrak{L}_u$, $u\in\mathfrak{B}$, where $\mathfrak{L}_u$ consists of elements of the form $g^u\sum_i\xi_iD_i$, $\xi_i\in\Phi$. Now $g^u\sum\xi_iD_i\in\mathfrak{L}_u$ if and only if

$$\sum_i (e_i\cdot u)\xi_i = \sum_i \alpha_i\xi_i. \tag{4.2.1}$$

Suppose that $\mathfrak{L}=\mathfrak{L}(D_i; a_i)$ is of type I. Then we may assume $\alpha_i=0$ for all i. From (3.2.4) and (4.2.1) it follows easily that $\dim \mathfrak{L}_u=m$ for $u\neq 0$ and that $\dim \mathfrak{L}_0=m+1$. Hence $\dim \mathfrak{L}=mp^n+1$.

Suppose that $\mathfrak{L}=\mathfrak{L}(D_i; a_i)$ is of type II. By (3.2.5), we may set $\alpha_i=e_i\cdot k$, where $k\in\overline{\mathfrak{B}}$. Then by Lemma 4.1 we see that

$$((e_0\cdot k - u), \cdots, (e_m\cdot k - u)) \neq 0 \tag{4.2.2}$$

for all $u\in\mathfrak{B}$. Now (4.2.1) can be expressed in the form $(x\cdot k-u)=0$, where $x=(\xi_0, \cdots, \xi_m)$. Therefore, because of (4.2.2), we have $\dim \mathfrak{L}_u=m$ for all $u\in\mathfrak{B}$. Hence $\dim \mathfrak{L}=mp^n$. Thus we have proved

THEOREM 4.2. *If* $\mathfrak{L}$ *is of type* I, *then* $\dim \mathfrak{L}=mp^n+1$. *If* $\mathfrak{L}$ *is of type* II, *then* $\dim \mathfrak{L}=mp^n$.

5. **Another characterization of $\mathfrak{F}$.** Let $\mathfrak{L}=\mathfrak{L}(D_i; a_i)\in\mathfrak{F}$ be defined by a principal system (D_i). Let b be a proper element, and $(\alpha_0, \cdots, \alpha_m)$ the proper root belonging to b. We set $\alpha_i=e_i\cdot k$, $k\in\overline{\mathfrak{B}}$, as before. (If L is of type I, then, by Lemma 4.1, we may take k in $\mathfrak{B}$[4].) It was shown in the course of the proof of Theorem 4.2 that $\mathfrak{L}$ is spanned by the elements of the form $bg^u(\sum\xi_iD_i)$, where $(x\cdot u-k)=0$, $x=(\xi_0, \cdots, \xi_m)$.

Introduce the symbol $(x, u)=bg^u(\sum\xi_iD_i)$. Then:

---

(4) The idea of considering the case $k\neq 0$ for algebras of type I will become clear when the reader reaches §7.

(5.0.1) $\mathfrak{L}$ consists of elements of the form $\sum_{u\in\mathfrak{B}} (x_u, u)$, where $(x_u\cdot u - k) = 0$ for all $u \in \mathfrak{B}$;

(5.0.2) $\sum (x_u, u) = \sum (y_u, u)$ if and only if $x_u = y_u$ for all $u \in \mathfrak{B}$;

(5.0.3) $\lambda \sum (x_u, u) = \sum (\lambda x_u, u)$ if $\lambda \in \Phi$;

(5.0.4) $\sum (x_u, u) + \sum (y_u, u) = \sum (x_u + y_u, u)$;

(5.0.5) $(x, u) \circ (y, v) = \sum_{w\in\mathfrak{B}} \beta_w((x\cdot v + w)y - (y\cdot u + w)x, u + v + w)$.

The coefficients β_w in (5.0.5) are those in the representation $b = \sum_{w\in\mathfrak{B}} \beta_w g^w$. Note that $\sum \beta_w \neq 0$ since b is a unit in $\mathfrak{A}$. Note also that $(x\cdot u - k) = (y\cdot v - k) = 0$ implies $(((x\cdot v + w)y - (y\cdot u + w)x)\cdot(u + v + w - k)) = 0$. Conversely if we start with a bilinear function $x\cdot u$, $x\in\mathfrak{R}$, $u\in\overline{\mathfrak{B}}$, satisfying (3.2.4)–(3.2.5), an element $k\in\overline{\mathfrak{B}}$, and arbitrary elements $\beta_u\in\Phi$, then by (5.0.1)–(5.0.5) we can define an algebra $\mathfrak{L}$ over Φ. It can be easily verified that the multiplication $\circ$ is skew-symmetric and satisfies the Jacobi-identity. Therefore $\mathfrak{L}$ is a Lie algebra. If $\sum_{w\in\mathfrak{B}} \beta_w \neq 0$ then $\mathfrak{L}$ is isomorphic to an algebra in $\mathfrak{F}$. This can be seen as follows: Let $g_1, \cdots, g_n$ be a set of principal generators of $\mathfrak{A}$. We define linear mappings D_i, $0 \leq i \leq m$, by $D_i g^u = (e_i\cdot u)g^u$. It is easily verified that D_i are derivations of $\mathfrak{A}$ and that $(D_0, \cdots, D_m)$ is a system. If $b = \sum_{w\in\mathfrak{B}} \beta_w g^w$, then $\sum \beta_w \neq 0$ implies that b is a unit in $\mathfrak{A}$. Set $a_i = b^{-1}D_i b + e_i\cdot k$ for all i. Then $D_i a_j = D_j a_i$, and we have $\mathfrak{L} \simeq \mathfrak{L}(D_i; a_i)$, where (x, u) corresponds to $bg^u \sum \xi_i D_i$, $x = (\xi_0, \cdots, \xi_m)$.

In the above formulation (5.0.1)–(5.0.5), $\mathfrak{L}$ is of type I if and only if there exists $k'\in\mathfrak{B}$ such that $x\cdot k = x\cdot k'$ for all $x\in\mathfrak{R}$.

Suppose that $\mathfrak{L}$ is of type I. Then we may assume $k\in\mathfrak{B}$. Consider the first derived algebra $\mathfrak{L}'$ of $\mathfrak{L}$. In the right hand side of (5.0.5), if $u+v+w=k$, then for $x\in\mathfrak{L}_u$ and $y\in\mathfrak{L}_v$, $(x\cdot v + w) = -(x\cdot u - k) = 0$, $(y\cdot u + w) = -(y\cdot v - k) = 0$. Therefore, if $\sum (x_u, u)\in\mathfrak{L}'$ then $x_k = 0$. Thus we have proved

THEOREM 5.1. *If the algebra $\mathfrak{L}\in\mathfrak{F}$ is of type* I, *then $\mathfrak{L}'$ is contained, as an ideal, in the subalgebra of $\mathfrak{L}$ consisting of all $\sum (x_u, u)\in\mathfrak{L}$ such that $x_k = 0$. In particular*, $\dim \mathfrak{L}' \leq m(p^n - 1)$.

Consider now the special case where $m = 1$, $0 \neq k\in\mathfrak{B}$, $\beta_0 = 1$, $\beta_w = 0$ for all $w \neq 0$. If $\mathfrak{L}$ is of type I, and if $\sum (x_u, u)\in\mathfrak{L}'$ then $x_k = 0$, so that (5.0.5) becomes

(5.2.1) $$(x, u) \circ (y, v) = ((x\cdot v)y - (y\cdot u)x, u + v).$$

Suppose $u + v = 2k$. Then $(x\cdot u - k) = (y\cdot u - k) = 0$. Therefore, if $u \neq k$, $x \neq 0$, then $y = \lambda x$ with $\lambda\in\Phi$ since $m = 1$. Hence

$$(x\cdot v)y - (y\cdot u)x = \lambda(x\cdot v)x - \lambda(x\cdot u)x = 0.$$

Thus we see that if $\sum (x_u, u)\in\mathfrak{L}''$, the second derived algebra of $\mathfrak{L}$, then $x_k = x_{2k} = 0$. In other words, $\mathfrak{L}''$ is contained, as an ideal, in the subalgebra consisting of all $\sum(x_u, u)\in\mathfrak{L}$ such that $x_k=x_{2k}=0$. In particular, dim $\mathfrak{L}''\leqq p^n-2$. Later we shall see that $\mathfrak{L}''$ is simple and of dimension p^n-2, provided $p\neq 2$.

6. **Reduction theorems.** We define a subfamily $\mathfrak{F}_c$ of $\mathfrak{F}$ as follows: $\mathfrak{L}\in\mathfrak{F}_c$ if and only if there exists a principal system (D_i) and elements $\lambda_i\in\Phi$ such that $\mathfrak{L}=\mathfrak{L}(D_i;\lambda_i)$. As we shall see later, algebras in $\mathfrak{F}_c$ can be discussed fairly easily. It is an open question whether $\mathfrak{F}=\mathfrak{F}_c$ or not.

THEOREM 6.1. *Let $\mathfrak{L}=\mathfrak{L}(D_i;a_i)$ be defined by a principal system (D_i). Then $\mathfrak{L}\in\mathfrak{F}_c$ if and only if there exists $c_0,\cdots,c_m\in\mathfrak{A}$ and $\lambda_0,\cdots,\lambda_m\in\Phi$ such that $f=\det(\delta_{ij}+D_ic_j)$ is a unit in $\mathfrak{A}$ and such that*

$$(6.1.1)\qquad a_i = -f^{-1}D_if + D_i\left(\sum\lambda_sc_s\right) + \lambda_i \text{ for all } i=0,\cdots,m.$$

For the proof of Theorem 6.1 we need the following

LEMMA 6.2. *Suppose (D_i) is a principal system. If $h_0,\cdots,h_m\in\mathfrak{A}$ are such that $D_ih_j=D_jh_i$ for all i, j, then there exist $h\in\mathfrak{A}$ and $\gamma_0,\cdots,\gamma_m\in\Phi$ such that $h_i=D_ih+\gamma_i$ for all i.*

Proof of Lemma 6.2. Let $g_1,\cdots,g_n$ be a set of principal generators of $\mathfrak{A}$ belonging to (D_i), and let $h_i=\sum_{u\in\mathfrak{B}}\eta_{iu}g^u$, $\eta_{iu}\in\Phi$. Then $D_ih_j=D_jh_i$ implies $(e_i\cdot u)\eta_{ju}=(e_j\cdot u)\eta_{iu}$ for all $u\in\mathfrak{B}$. From (3.2.4) we have $((e_0\cdot u),\cdots,(e_m\cdot u))\neq 0$ if $u\neq 0$. Hence there exists $\rho_u\in\Phi$, for all $u\neq 0$, such that $\eta_{iu}=(e_i\cdot u)\rho_u$ for all i. Put $h=\sum_{u\in\mathfrak{B}}\rho_ug^u$, $\gamma_i=\eta_{i0}$. Then $h_i=D_ih+\gamma_i$ for all i, as required.

Proof of Theorem 6.1. Suppose $\mathfrak{L}\in\mathfrak{F}_c$. Then there exist a principal system (D_i') equivalent to (D_i) and a $\lambda_i\in\Phi$ such that $\mathfrak{L}=\mathfrak{L}(D_i';\lambda_i)$. Let (D_i) and (D_i') be related as in (2.0.1). Then (2.3.2) yields

$$(6.1.2)\qquad \lambda_i = \sum_s c_{is}(a_s + f^{-1}D_sf),\qquad f = \det(c'_{ij}).$$

By a formula corresponding to (2.0.2) and Lemma 6.2, we see that there exist $c_i\in\mathfrak{A}$ and $\gamma_{ij}\in\Phi$ such that

$$(6.1.3)\qquad c'_{ij} = D_ic_j + \gamma_{ij},\qquad i, j = 0,\cdots,m,$$

where γ_{ij} are uniquely determined by c'_{ij}, since (D_i) is principal. We shall show that $\det(\gamma_{ij})\neq 0$. Suppose $\xi_i\in\Phi$ are such that $\sum_{s=0}^m\gamma_{is}\xi_s=0$ for all i. Then (6.1.3) yields $\sum_s c'_{is}\xi_s=D_ic$, where $c=\sum_s c_s\xi_s$, and hence $D_i'c=\xi_i\in\Phi$ for all i. Since (D_i') is principal, we have $c\in\Phi$, and hence $\xi_i=0$ for all i. Thus $\det(\gamma_{ij})\neq 0$ is proved. Let (γ'_{ij}) be the inverse matrix of (γ_{ij}), and let $\bar\lambda_i=\sum_s\gamma_{is}\lambda_s$, $\bar c_i=\sum_s c_s\gamma'_{si}$, $\bar f=\det(D_i\bar c_j+\delta_{ij})$, $\gamma=\det(\gamma_{ij})$. Then $\bar f=f\gamma$, and from (6.1.2) and (6.1.3) we have easily $a_i=-\bar f^{-1}D_i\bar f+D_i(\sum\bar\lambda_s\bar c_s)+\bar\lambda_i$ for all i.

Suppose conversely, that there exist $c_i\in\mathfrak{A}$ and $\lambda_i\in\Phi$ such that $f=\det(D_ic_j+\delta_{ij})$ is a unit in $\mathfrak{A}$ and such that (6.1.1) holds. We set $c'_{ij}=D_ic_j+\delta_{ij}$, $(c_{ij})=(c'_{ij})^{-1}$, $D_i'=\sum_s c_{is}D_s$. First, we shall show that (D_i') is a system. Since (D_i) is already a system, by Lemma 2.1 it is sufficient to show that $D_i'\circ D_j'=0$ for all i, j. Since $D_i=\sum_s c'_{is}D_s'$ for all i, we have

$$0 = D_i \circ D_j = \sum_{s,t} (c'_{is}D'_s c'_{jt})D'_t - \sum_{s,t} (c'_{jt}D'_t c'_{is})D'_s + \sum_{s,t} c'_{is}c'_{jt}(D'_s \circ D'_t)$$
$$= \sum_t [(D_i c'_{jt})D'_t - (D_j c'_{it})D'_t] + \sum_{s,t} c'_{is}c_{jt}(D'_s \circ D'_t).$$

Now $D_i c'_{jt} = D_j c'_{it}$ for all i, j, t, so that $\sum_{s,t} c'_{is}c'_{jt}(D'_s \circ D'_t) = 0$ for all i, j. Finally since det (c'_{ij}) is a unit in $\mathfrak{A}$, we have $D'_s \circ D'_t = 0$ for all s and t. Thus (D'_i) is proved to be a system. We shall show that (D'_i) is principal. Suppose $D'_i f = \xi_i \in \Phi$ for all i. Then $D_i = \sum_s c'_{is}D'_s$ implies $D_i(f - \sum \xi_s c_s) = \xi_i \in \Phi$ for all i. Since (D_i) is principal we have $f - \sum \xi_s c_s \in \Phi$, $\xi_i = 0$ for all i, and hence $f \in \Phi$. Thus (D'_i) is a principal system. The fact that $\mathfrak{L} = \mathfrak{L}(D'_i; \lambda_i)$ follows easily from (6.1.1) and (2.3.2), and Theorem 6.1 is proved.

Define a subfamily $\mathfrak{F}_0$ of $\mathfrak{F}_c$ as follows: $\mathfrak{L} \in \mathfrak{F}_0$ if and only if there exists a principal system (D_i) such that $\mathfrak{L} = \mathfrak{L}(D_i; 0)$. Clearly every algebra in $\mathfrak{F}_0$ is of type I. Later we shall show that the first derived algebras $\mathfrak{L}'$ of $\mathfrak{L}$ in $\mathfrak{F}_0$ are simple for any prime $p > 0$. The following theorem may be proved just like Theorem 6.1.

THEOREM 6.3. *Let $\mathfrak{L} = \mathfrak{L}(D_i; a_i)$ be defined by a principal system (D_i). Then $\mathfrak{L} \in \mathfrak{F}_0$ if and only if there exist $c_0, \cdots, c_m \in \mathfrak{A}$ such that $f = \det(D_i c_j + \delta_{ij})$ is a unit in $\mathfrak{A}$ and such that $a_i = -f^{-1}D_i f$ for all i.*

Let (D_i) be a principal system, and $(g_1, \cdots, g_n)$ a set of principal generators belonging to (D_i). For convenience an element $h \in \mathfrak{A}$ will be called "*unitary*" with respect to (D_i) if η_0 in the expression $h = \sum_{u \in \mathfrak{B}} \eta_u g^u$, $\eta_u \in \Phi$, is not zero. This property does not depend on the choice of principal generators belonging to (D_i).

COROLLARY 6.4. *Let (D_i) be a principal system, and let f be a unit in $\mathfrak{A}$ which is unitary with respect to (D_i). Then $\mathfrak{L}(D_i; -f^{-1}D_i f) \in \mathfrak{F}_0$.*

Proof. In view of Theorem 6.3 it is sufficient to show that there exist $c_0, \cdots, c_m \in \mathfrak{A}$ such that $f = \gamma \det(D_i c_j + \delta_{ij})$ with a nonzero element γ in Φ.

It was proved in §9 of [4] that for any principal system (D_i), there exist elements $\alpha_i \in \Phi$ such that the derivation $D = \sum \alpha_i D_i$ satisfy the condition:

$$\text{(6.4.1)} \qquad Dh = 0 \text{ implies } h \in \Phi.$$

Let $(g_1, \cdots, g_n)$ be a set of principal generators belonging to (D_i), and $Dg^u = \delta_u g^u$, $\delta_u \in \Phi$. Then (6.4.1) yields $\delta_u \neq 0$ for all $u \neq 0$. Now let $f = \sum_{u \in \mathfrak{B}} \gamma_u g^u$, $\gamma_u \in \Phi$, where $\gamma_0 \neq 0$ by hypothesis. Put $c = \gamma_0^{-1} \sum_{u \neq 0} \gamma_u \delta_u^{-1} g^u$, $c_i = \alpha_i c$. Then $f = \gamma_0(1 + Dc)$, and we have $\det(D_i c_j + \delta_{ij}) = 1 + \sum D_i c_i = 1 + Dc$, and hence $f = \gamma_0 \det(D_i c_j + \delta_{ij})$. Thus Corollary 6.4 is proved.

7. **Some lemmas.** Algebras in $\mathfrak{F}_c$ are those obtained by setting $b = \sum \beta_w g^w = 1$ in the characterization (5.0.1)–(5.0.5), and will be considered in this section and the one following. For our purposes, however, it is more convenient to consider the algebra $\overline{\mathfrak{L}}$ which is defined as follows: Assuming always that

$\beta_0=1$, $\beta_w=0$ for $w\neq 0$ in (5.0.1)–(5.0.5), then

(i) if $\mathfrak{L}\in\mathfrak{F}_c$ is of type II, then we set $\bar{\mathfrak{L}}=\mathfrak{L}$;

(ii) if $\mathfrak{L}\in\mathfrak{F}_c$ is of type I and if either $m>1$ or $k=0$, then we set $\bar{\mathfrak{L}}$ to be the algebra consisting of all $\sum(x_u, u)\in\mathfrak{L}$ such that $x_k=0$;

(iii) if $\mathfrak{L}\in\mathfrak{F}_c$ is of type I, if $m=1$, and if $k\neq 0$, then we set $\bar{\mathfrak{L}}$ to be the algebra consisting of all $\sum(x_u, u)\in\mathfrak{L}$ such that $x_k=x_{2k}=0$.

We shall assume $p\neq 2$ in case (iii) and also in case (i) if $m=1$. With this assumption we shall prove that $\bar{\mathfrak{L}}$ is simple. Then we see from the result in §5 that $\mathfrak{L}$ in case (i), $\mathfrak{L}'$ in case (ii), and $\mathfrak{L}''$ in case (iii) are simple and of dimensions mp^n, $m(p^n-1)$, and p^n-2, respectively. In this section we shall prepare for the proof of the simplicity of $\bar{\mathfrak{L}}$.

LEMMA 7.1. *If nonzero elements u, v in $\mathfrak{B}$ are such that $x\cdot u=0$, where $x\in\mathfrak{R}$, implies $x\cdot v=0$, and vice versa, then there exists a nonzero $\lambda\neq 0$ in Φ such that $x\cdot u=\lambda x\cdot v$ for all $x\in\mathfrak{R}$.*

Proof. There exist $\alpha_{ij}\in\Phi$ such that $x\cdot u=\sum_{i=0}^{m}\sum_{j=1}^{n}\xi_i\alpha_{ij}u_j$, where $x=(\xi_0, \cdots, \xi_m)$, $u=(u_1, \cdots, u_n)$. Set $\beta_i=\sum_j \alpha_{ij}u_j$, $\gamma_i=\sum_j\alpha_{ij}v_j$. Then our hypothesis implies that $\xi_0\beta_0+\cdots+\xi_m\beta_m=0$ if and only if $\xi_0\gamma_0+\cdots+\xi_m\gamma_m=0$. Therefore, there exists a nonzero $\lambda\in\Phi$ such that $\beta_i=\lambda\gamma_i$ for all i, so that $x\cdot u=\lambda x\cdot v$ for all $x\in\mathfrak{R}$.

An element $(x, u)\in\bar{\mathfrak{L}}$ will be called a *u-term* or simply a term. Let $\mathfrak{J}$ be a nonzero ideal of $\bar{\mathfrak{L}}$, and let $A=\sum_{i=1}^{r}(x_i, u_i)$, where $x_i\neq 0$, $i=1, \cdots, r$, and where $u_1, \cdots, u_r$ are distinct, be a nonzero element in $\mathfrak{J}$ such that the number r of nonzero terms is as small as possible. Such an element A will be called a *minimal* element in $\mathfrak{J}$.

LEMMA 7.2. *Suppose $k\neq 0$. If $A=\sum(x_i, u_i)$ is a minimal element in an ideal $\mathfrak{J}\neq 0$, then, for any distinct i and $j\leqq r$ there exists a nonzero $\lambda\in\Phi$ such that $x\cdot(u_j-u_i)=\lambda x\cdot k$ for all $x\in\mathfrak{R}$.*

Proof. By Lemma 7.1, it is sufficient to show that $y\cdot k=0$ implies $y\cdot(u_i-u_j)=0$. Consider $A'=A\circ(y, 0)=\sum_{i=1}^{r}((y\cdot u_i)x_i, u_i)$. Since $A'\in\mathfrak{J}$, $A'-(y\cdot u_j)A$ is also in $\mathfrak{J}$ and has less than r nonzero terms. Hence $A'=(y\cdot u_j)A$, from which it follows that $(y\cdot u_i)x_i-(y\cdot u_j)x_i=0$. Therefore $y\cdot(u_i-u_j)=0$.

LEMMA 7.3. *Suppose $k=0$. If $A=\sum(x_i, u_i)$ is a minimal element in $\mathfrak{J}$, then, for any i and j, there exists a nonzero $\lambda\in\Phi$ such that $x\cdot u_i=\lambda x\cdot u_j$ for all $x\in R$.*

Proof. By Lemma 7.1, it is sufficient to show that $y\cdot u_1=0$ if and only if $y\cdot u_i=0$. Let $y\cdot u_1=0$. Then $A'=A\circ(y, -u_1)\in\mathfrak{J}$, and A' contains less than r terms, so that $A'=0$. Therefore

$$(x_i\cdot u_1)y+(y\cdot u_i)x_i=0 \tag{7.3.1}$$

for all i. Since $x_i\cdot u_i=0$, (7.3.1) yields $(x_i\cdot u_1)(y\cdot u_i)=0$. Suppose $y\cdot u_i\neq 0$.

Then $x_i \cdot u_1 = 0$, and hence (7.3.1) yields $y \cdot u_i = 0$, a contradiction. Thus $y \cdot u_i = 0$, and Lemma 7.3 is proved.

LEMMA 7.4. *If $A = \sum(x_i, u_i)$ is a minimal element in $\mathfrak{J}$, then $x_i \cdot u_j = 0$ for any $i \neq j$.*

Proof. Since $A \circ (x_i, u_i)$ contains less than r terms, we have $(x_j, u_j) \circ (x_i, u_i) = 0$ for any i and j. Hence

$$(x_i \cdot u_j)x_j - (x_j \cdot u_i)x_i = 0. \tag{7.4.1}$$

Therefore $(x_i \cdot u_j)(x_j \cdot u_j) - (x_j \cdot u_i)(x_i \cdot u_j) = 0$. Suppose $x_i \cdot u_j \neq 0$. Then (7.4.1) yields

$$x_j \cdot (u_j - u_i) = 0. \tag{7.4.2}$$

If $k = 0$ then Lemma 7.4 follows immediately from Lemma 7.3. Hence we assume $k \neq 0$. Then by Lemma 7.2 there exists $\lambda \neq 0$ such that $x_j \cdot (u_j - u_i) = \lambda x_j \cdot k$. Therefore (7.4.2) gives $x_j \cdot k = 0$, and hence $x_j \cdot u_j = 0$. Then by (7.4.2) we have $x_j \cdot u_i = 0$. But then (7.4.1) yields $x_i \cdot u_j = 0$, since $x_j \neq 0$. This is a contradiction, and Lemma 7.4 is proved.

LEMMA 7.5. *If $r > 1$ for a minimal element in $\mathfrak{J}$, then $\mathfrak{J}$ contains a minimal element $\sum(x_i, u_i)$ such that $u_1 \neq 0$, $u_2 \neq 0$.*

Proof. If $k = 0$, then every $u_i \neq 0$, and hence the lemma is clear. Suppose that $k \neq 0$, $u_1 \neq 0$, $u_2 = 0$. Since $x_2 \neq 0$, there exists $v \in \mathfrak{B}$ such that $x_2 \cdot v \neq 0$. If $u_1 + v = 0$ then $x_2 \cdot v = -x_2 \cdot u_1 = 0$ by Lemma 7.4, which is a contradiction. Hence

$$u_1 + v \neq 0, \qquad v \neq 0. \tag{7.5.1}$$

There exists a nonzero element $y \in \mathfrak{R}$ such that $y \cdot (v - k) = 0$. Consider $A' = A \circ (y, v) \in \mathfrak{J}$. Then $A' = \sum(x_i', u_i')$ contains a term $((x_2 \cdot v)y, v) \neq 0$. Therefore A' is a minimal element, and $u_1' = u_1 + v \neq 0$, $u_2' = v \neq 0$ by (7.5.1).

LEMMA 7.6. *Suppose $m > 1$. If $A = \sum(x_i, u_i)$ is a minimal element in $\mathfrak{J}$, and if $u_i \neq 0$ for some i, then $x_j \cdot k = 0$ for all $j \neq i$.*

Proof. The subspace $\mathfrak{R}'$ of $\mathfrak{R}$ consisting of all x' such that $x' \cdot u_i = 0$ is of dimension $m > 1$. Hence there exists $y \in R'$ such that y and x_j are linearly independent. The element $A' = A \circ (y, k - u_i)$ is in $\mathfrak{J}$ and contains less than r terms. Hence $A' = 0$, and we have $(x_j, u_i) \circ (y, k - u_i) = (x_j \cdot (k - u_i))y - (y \cdot u_j)x_j = 0$ for $j \neq i$. Since y and x_j are linearly independent, we have $x_j \cdot (k - u_i) = 0$. Then, by Lemma 7.4, we have $x_j \cdot k = 0$, as required.

LEMMA 7.7. *Suppose $m = 1$, $p > 2$, $k \neq 0$. If $\sum_{i=1}^{r} (x_i, u_i)$ is a minimal element in $\mathfrak{J} \neq 0$, and if $r > 1$, then $x_i \cdot k = 0$ for all i.*

Proof. We may assume $i = 1$. We have $x_1 \cdot (u_1 - k) = 0$, and $x_1 \cdot u_2 = 0$ by

Lemma 7.4. Hence $x_1\cdot(u_1-u_2-k)=0$. On the other hand, there exists a nonzero $\lambda\in\Phi$ such that

$$x\cdot(u_1-u_2)=\lambda x\cdot k \tag{7.7.1}$$

for all $x\in\mathfrak{R}$. By setting $x=x_1$ in (7.7.1), we have $(\lambda-1)x_1\cdot k=0$. If $\lambda\neq 1$ then $x_1\cdot k=0$, as required. Suppose $\lambda=1$. Then by (7.7.1) we have $x\cdot(u_1-u_2)=x\cdot k$ for all $x\in\mathfrak{R}$. Therefore $\mathfrak{L}$ is of type I, and we may assume $u_1-u_2=k$. Hence $u_2\neq 0$, and we have $x_2\cdot(u_2+k)=0$, $x_2\cdot(u_2-k)=0$. Since $p\neq 2$, we have $x_2\cdot u_2=x_2\cdot k=0$. By Lemma 7.4, $x_1\cdot u_2=0$. Now the subspace $\mathfrak{R}'$ consisting of all x' such that $x'\cdot u_2=0$ is of dimension $m=1$, since $0\neq u_2\in\mathfrak{B}$. Hence $x_1=\mu x_2$ with some $\mu\in\Phi$. Then $x_1\cdot k=\mu x_2\cdot k=0$, as required.

LEMMA 7.8. *If $A=\sum_{i=1}^{r}(x_i, u_i)$, $x_i\neq 0$, is a minimal element in a nonzero ideal $\mathfrak{J}$ in $\bar{\mathfrak{L}}$, where p is assumed $\neq 2$ if both of $k\neq 0$ and $m=1$ hold, then $r=1$.*

Proof. Suppose $r>1$. We shall derive a contradiction.

First consider the case $k\neq 0$. By Lemma 7.5, we may assume that $u_1\neq 0$, $u_2\neq 0$. Then, by Lemmas 7.6 and 7.7, we have $x_i\cdot u_i=x_i\cdot k=0$ for all $i=1,\cdots,r$. Since $x_1\neq 0$, there exists an element $v\in\mathfrak{B}$ with $x_1\cdot v\neq 0$. Then $x_1\cdot(v-k)\neq 0$, since $x_1\cdot k=0$. The subspaces $\mathfrak{R}'=\{x'\mid x'\cdot(v-k)=0\}$ and $\mathfrak{R}''=\{x''\mid x''\cdot k=0\}$ are both of dimension m. Since $x_1\notin\mathfrak{R}'$, $x_1\in\mathfrak{R}''$ we have $\mathfrak{R}'\neq\mathfrak{R}''$. Let $y\in\mathfrak{R}'$, $y\notin\mathfrak{R}''$. Then $y\cdot(v-k)=0$, $y\cdot k\neq 0$, and also $u_i+v\neq 0$ for all i. Since

$$A'=A\circ(y, v)=\sum((x_i\cdot v)y-(y\cdot u_i)x_i,\ u_i+v) \tag{7.8.1}$$

is a minimal element, by Lemmas 7.6 and 7.7, we have $(x_i\cdot v)(y\cdot k)-(y\cdot u_i)(x_i\cdot k)=0$ for all i. Since $x_i\cdot k=0$, $y\cdot k\neq 0$, we have $x_i\cdot v=0$ for all $i=1,\cdots,r$, a contradiction. Therefore $r=1$, as required.

Next consider the case $k=0$. Choose $v\in\mathfrak{B}$, as before, such that $x_1\cdot v\neq 0$, and $y\in\mathfrak{R}$ such that $y\cdot v=0$, $y\cdot u_1\neq 0$. Consider A' given by (7.8.1). By Lemma 7.4, we have $(x_1\cdot v)y-(y\cdot u_1)x_1)\cdot(u_i+v)=0$ for all i, and hence $(x_1\cdot v)(y\cdot u_i)=(y\cdot u_1)(x_1\cdot v)$, which yields $y\cdot(u_i-u_1)=0$, since $x_1\cdot v\neq 0$. By Lemma 7.3, there exists a nonzero $\lambda\in\Phi$ such that $y\cdot u_i=\lambda y\cdot u_1$. Then $(\lambda-1)(y\cdot u_1)=0$. Since $y\cdot u_1\neq 0$, $\lambda=1$. Then $x\cdot u_i=x\cdot u_1$ for all $x\in\mathfrak{R}$, and hence $u_i=u_1$, $r=1$. Thus Lemma 7.8 is proved.

In the following, we shall denote by $\mathfrak{R}(u)$, where $u\in\bar{\mathfrak{B}}$, the subspace $\mathfrak{R}'=\{x'\mid x'\cdot u=0\}$ of R, provided there exists at least one element $x\in\mathfrak{R}$ such that $x\cdot u\neq 0$. Note that $\mathfrak{R}(u)$, if it exists, is always of dimension m. If $\mathfrak{L}$ is of type II and if $u\in\mathfrak{B}$ then by (4.2.2) there exists $x\in\mathfrak{R}$ such that $x\cdot(u-k)\neq 0$, and hence we can always define $\mathfrak{R}(u-k)$.

LEMMA 7.9. *If $0\neq(x, u)\in\mathfrak{J}$, an ideal of $\bar{\mathfrak{L}}$, and if $x\notin\mathfrak{R}(v-k)$, $x\notin\mathfrak{R}(v-2k)$, then all v-terms are contained in $\mathfrak{J}$.*

Proof. Since $x\notin\mathfrak{R}(v-2k)$, we have $v-u\neq k$. Let $y_1,\cdots,y_m$ be a basis of $\mathfrak{R}(v-u-k)$. Then $(z_i, v)=(x, u)\circ(y_i, v-u)\in\mathfrak{J}$, where $z_i=(x\cdot v-u)y_i-(y_i\cdot u)x$. It is sufficient to show that $z_1, \cdots, z_m$ are linearly independent. Suppose $\sum\lambda_i z_i=0$ with $\lambda_i\in\Phi$. Then

$$(7.9.1) \qquad (x\cdot v-u)\sum\lambda_i y_i-(\sum\lambda_i y_i\cdot u)x=0.$$

Since $y_i\in\mathfrak{R}(v-u-k)$, (7.9.1) yields $(\sum\lambda_i y_i\cdot u)(x\cdot v-u-k)=0$. However, $(x\cdot v-u-k)=(x\cdot v-2k)\neq 0$. Hence $\sum\lambda_i y_i\cdot u=0$. Then (7.9.1) gives $\sum\lambda_i y_i=0$, because $(x\cdot v-u)=(x\cdot v-k)\neq 0$, and since $y_1, \cdots, y_m$ are linearly independent, $\lambda_i=0$, $i=1, \cdots, m$.

Lemma 7.10. *If all u-terms are contained in* $\mathfrak{J}$ *and if* $\mathfrak{R}(u-k)\neq\mathfrak{R}(v-k)$, $\mathfrak{R}(u-k)\neq\mathfrak{R}(v-2k)$, *then all v-terms are contained in* $\mathfrak{J}$.

Proof. By Lemma 7.9, it is sufficient to show that there exists $x\in\mathfrak{R}(u-k)$ such that $x\notin\mathfrak{R}(v-k)$, $x\notin\mathfrak{R}(v-2k)$. Suppose that every $x\in\mathfrak{R}(u-k)$ is either in $\mathfrak{R}(v-k)$ or in $\mathfrak{R}(v-2k)$. Let $x_i\in\mathfrak{R}(u-k)$ be such that $x_i\notin\mathfrak{R}(v-ik)$, $i=1, 2$. Then $x_1\in\mathfrak{R}(v-2k)$ and $x_2\in\mathfrak{R}(v-k)$. Then $x=x_1+x_2\notin\mathfrak{R}(v-ik)$, $i=1, 2$, and $x\in\mathfrak{R}(u-k)$.

Lemma 7.11. *Suppose* $k\neq 0$. *If* $0\neq(x, 0)\in\mathfrak{J}$ *and if* $x\cdot v\neq 0$, *then all v-terms are contained in* $\mathfrak{J}$. *If all* 0*-terms are contained in* $\mathfrak{J}$ *and if* $\mathfrak{R}(k)\neq\mathfrak{R}(v)$ *then all v-terms are contained in* $\mathfrak{J}$.

Proof. Lemma 7.11 follows immediately from Lemmas 7.9 and 7.10, since $x\cdot k=0$.

Lemma 7.12. *Suppose* $p\neq 2$. *If* $0\neq x\in\mathfrak{R}$ *then there exists* $u\in\mathfrak{B}$ *such that* $x\notin\mathfrak{R}(u-k)$, $x\notin\mathfrak{R}(u-2k)$.

Proof. If $x\cdot(u'-k)=0$ for all $u'\in\mathfrak{B}$, then $x\cdot u'=0$ for all $u'\in\mathfrak{B}$, and hence $x=0$. Therefore there exists $u'\in\mathfrak{B}$ such that $x\cdot(u'-k)\neq 0$. If $x\cdot(u'-2k)\neq 0$, then $u=u'$ is the required element. Suppose $x\cdot(u'-2k)=0$. Then $x\cdot(u'-k)=x\cdot k\neq 0$. Hence $k\neq 0$ and $u=0$ is the required element of $\mathfrak{B}$, since $x\cdot 2k\neq 0$ follows from $p\neq 2$.

Lemma 7.13. *Suppose that* $k\neq 0$ *and that* $p>2$ *if* $m=1$. *Then all* 0*-terms are contained in any ideal* $\mathfrak{J}\neq 0$ *of* $\bar{\mathfrak{L}}$.

Proof. First consider the case $p\neq 2$. By Lemma 7.8 there exists a nonzero element (x', u') in $\mathfrak{J}$. Since $x'\neq 0$, by Lemma 7.12 there exists $u\in\mathfrak{B}$ such that $x'\notin\mathfrak{R}(u-k)$, $x'\notin\mathfrak{R}(u-2k)$. Then, by Lemma 7.9, all u-terms are contained in $\mathfrak{J}$. Let $0\neq x\in\mathfrak{R}(u-k)$. Then, again by Lemma 7.12, there exists $v\in\mathfrak{B}$ such that $x\notin\mathfrak{R}(v-ik)$, $i=1, 2$. Thus by Lemma 7.9 all v-terms are in $\mathfrak{J}$, and clearly $\mathfrak{R}(u-k)\neq\mathfrak{R}(v-k)$. Now $\mathfrak{R}(-k)=\mathfrak{R}(-2k)$, since $p\neq 2$. Since $\mathfrak{R}(u-k)\neq\mathfrak{R}(v-k)$, we see that either $\mathfrak{R}(u-k)$ or $\mathfrak{R}(v-k)$ is different from $\mathfrak{R}(-k)=\mathfrak{R}(-2k)$. Then by Lemma 7.10 all 0-terms are contained in $\mathfrak{J}$.

Next consider the case $p=2$, $m>1$. Let $0\neq(x, u)\in\mathfrak{J}$. If $x\cdot k=0$ then take

$v\in\mathfrak{B}$ such that $x\cdot v\neq 0$. Hence $x\cdot(v-k)\neq 0$. Since $\mathfrak{N}(k)$ and $\mathfrak{N}(v-k)$ are different and both of dimension m, there exists $y\in\mathfrak{N}(v-k)$ such that $y\notin\mathfrak{N}(k)$. Consider $(x', u+v)=(x, u)\circ(y, v)=((x\cdot v)y-(y\cdot u)x, u+v)$. Then $(x', u+v)\in\mathfrak{J}$, and $x'\cdot k=((x\cdot v)y-(y\cdot u)x)\cdot k=(x\cdot v)(y\cdot k)\neq 0$. Therefore we may assume that there exists a nonzero element (x, u) in $\mathfrak{J}$ such that $x\cdot k\neq 0$. Let $x_1=x, x_2, \cdots, x_m$ be a basis of $\mathfrak{N}(u-k)$. Put $(y_i, 0)=(x_1, u)\circ(x_i, u)$. Then $(y_i, 0)\in\mathfrak{J}$ and $y_i=(x_1\cdot k)x_i-(x_i\cdot k)x_1$. Since $x_1\cdot k\neq 0$, the elements $y_2, \cdots, y_m$ form a basis of $\mathfrak{N}(u-k)\cap\mathfrak{N}(k)$. Set $y_2=y$. Then there exists $v\in\mathfrak{B}$ such that $y\cdot v\neq 0$. Since $y\cdot k=0$, we have $y\cdot(v-k)\neq 0$. Since $\mathfrak{N}(k)\neq\mathfrak{N}(v-k)$, there exists $z\in\mathfrak{N}(v-k)$ such that $z\notin\mathfrak{N}(k)$. Now $(y, 0)\circ(z, v)=((y\cdot v)z, v)\in\mathfrak{J}$. Since $y\cdot v\neq 0$, we have $(z, v)\in\mathfrak{J}$. Now $z\cdot k\neq 0$ implies, as before, that $(z', 0)\in\mathfrak{J}$ for any $z'\in\mathfrak{N}(v-k)\cap\mathfrak{N}(k)$. We have $(y, 0)\in\mathfrak{J}$ with $y\notin\mathfrak{N}(v-k)\cap\mathfrak{N}(k)$. Since $\mathfrak{N}(v-k)\cap\mathfrak{N}(k)$ is of dimension $m-1$, we see that all 0-terms are contained in $\mathfrak{J}$.

8. **Simplicity of $\bar{\mathfrak{L}}$.** We are now ready to prove the following

THEOREM 8.1. *If $\mathfrak{L}\in\mathfrak{F}_0$, then the first derived algebra $\mathfrak{L}'$ is simple for any prime $p>0$. $\mathfrak{L}'$ is of dimension $m(p^n-1)$, where $1\leqq m<n$.*

Proof. If $\mathfrak{L}\in\mathfrak{F}_0$ then $\mathfrak{L}$ belongs to the case(ii) of §7 with $k=0$. Therefore, by Theorem 5.1, it is sufficient to show that $\bar{\mathfrak{L}}$ is simple for this case.

Let $\mathfrak{J}$ be a nonzero ideal of $\bar{\mathfrak{L}}$. By Lemma 7.8, $\mathfrak{J}$ contains an element of the form $(x, u)\neq 0$. Since $x\neq 0$ there exists $v\in\mathfrak{B}$ such that $x\cdot v\neq 0$. Then by Lemma 7.9 all v-terms are contained in $\mathfrak{J}$. Now, let nonzero $w\in\mathfrak{B}$ be such that $x\cdot w=0$. Since $x\cdot v\neq 0$, we have $\mathfrak{N}(w)\neq\mathfrak{N}(v)$. Hence there exists $y\in\mathfrak{N}(v)$ such that $y\notin\mathfrak{N}(w)$. Since (y, v) is a v-term, we have $(y, v)\in\mathfrak{J}$. Then, by Lemma 7.9, $y\notin\mathfrak{N}(w)$ implies that all w-terms are contained in $\mathfrak{J}$. Therefore $\mathfrak{J}=\bar{\mathfrak{L}}$, and hence $\bar{\mathfrak{L}}=\mathfrak{L}'$ is simple.

In the following, we shall denote by $\mathfrak{F}_{\mathrm{I}}$, and $\mathfrak{F}_{\mathrm{II}}$, the subfamilies of $\mathfrak{F}$ consisting of all algebras of types I and II respectively. Then $\mathfrak{F}_0\subset\mathfrak{F}_{\mathrm{I}}$. Let $\mathfrak{F}_{\mathrm{I}}-\mathfrak{F}_0$ be the set-theoretical difference of $\mathfrak{F}_{\mathrm{I}}$ and $\mathfrak{F}_0$.

THEOREM 8.2. *If $m>1$ then the first derived algebra $\mathfrak{L}'$ of any algebra $\mathfrak{L}$ in $\mathfrak{F}_c\cap(\mathfrak{F}_{\mathrm{I}}-\mathfrak{F}_0)$ is simple and of dimension $m(p^n-1)$, where $1<m<n$, for any prime $p>0$.*

Proof. As in the proof of Theorem 8.1, it is sufficient to show that $\bar{\mathfrak{L}}$ is simple for the case (ii) of §7 when $k\neq 0$.

Let $\mathfrak{J}$ be a nonzero ideal of $\bar{\mathfrak{L}}$. By Lemma 7.13, all 0-terms are contained in $\mathfrak{J}$. Hence by Lemma 7.11, if $\mathfrak{N}(u)\neq\mathfrak{N}(k)$ then all u-terms are contained in $\mathfrak{J}$.

Suppose that $\mathfrak{N}(u)=\mathfrak{N}(k)$, with $u\neq k$, $2k$. Then $\mathfrak{N}(u-k)=\mathfrak{N}(u-2k)=\mathfrak{N}(k)$. Let $0\neq x\in\mathfrak{N}(k)$, $x\cdot v\neq 0$, $v\in\mathfrak{B}$. Then $\mathfrak{N}(k)\neq\mathfrak{N}(v)$ and hence by Lemma 7.11 all v-terms are contained in $\mathfrak{J}$. We have $x\cdot(v-k)=x\cdot(v-2k)=x\cdot v\neq 0$. Hence $\mathfrak{N}(v-k)\neq\mathfrak{N}(u-k)=\mathfrak{N}(u-2k)$. Then by Lemma 7.10 all u-terms are contained in $\mathfrak{J}$.

Suppose now $u=2k\neq 0$. Then $p\neq 2$. Choose $v\in\mathfrak{B}$ such that $\mathfrak{N}(v)\neq\mathfrak{N}(k)$. Then $\mathfrak{N}(2k-v)\neq\mathfrak{N}(k)$. Therefore by Lemma 7.11 all v-terms and all $2k-v$ terms are contained in $\mathfrak{J}$. Let $x_1, \cdots, x_m$ be a basis of $\mathfrak{N}(v-k)$, and let $x_1\cdot k\neq 0$. We set $(y_i, 2k)=(x_1, v)\circ(x_i, 2k-v)$. Then $(y_i, 2k)\in\mathfrak{J}$ and $y_2, \cdots, y_m$ are linearly independent. Hence $(y, 2k)\in\mathfrak{J}$ for any $y\in\mathfrak{N}(v-k)\cap\mathfrak{N}(k)$. Let $0\neq y\in\mathfrak{N}(v-k)\cap\mathfrak{N}(k)$, which is possible since $m>1$, and let $y\cdot v'\neq 0$. Then $\mathfrak{N}(v')\neq\mathfrak{N}(k)$, and as before $(y', 2k)\in\mathfrak{J}$ for any $y'\in\mathfrak{N}(v'-k)\cap\mathfrak{N}(k)$. Since $y\notin\mathfrak{N}(v'-k)\cap\mathfrak{N}(k)$, all $2k$-terms are contained in $\mathfrak{J}$. Thus $\mathfrak{J}=\bar{\mathfrak{L}}$, which proves the simplicity of $\bar{\mathfrak{L}}=\mathfrak{L}'$.

The following two theorems may be proved similarly.

THEOREM 8.3. *Suppose $m=1$, $p>2$. Then the second derived algebra $\mathfrak{L}''$ of any algebra $\mathfrak{L}$ in $\mathfrak{F}_c\cap(\mathfrak{F}_{\mathrm{I}}-\mathfrak{F}_0)$ is simple and of dimension p^n-2, where $n>1$.*

THEOREM 8.4. *Suppose $p>2$ if $m=1$. Then any algebra $\mathfrak{L}$ in $\mathfrak{F}_c\cap\mathfrak{F}_{\mathrm{II}}$ is simple and of dimension mp^n, where $1\leqq m<n$.*

9. **Remarks.** Let $g_1, \cdots, g_n$ be a set of principal generators of $\mathfrak{A}$. The algebra considered by M. S. Frank [2] is obtained as $\mathfrak{L}=\mathfrak{L}(D_1, \cdots, D_n; a_1, \cdots, a_n)$ by setting $D_i=\partial/\partial g_i$, $a_1=\cdots=a_n=0$. Put $D_i'=g_i\partial/\partial g_i$. Then (D_i') is a principal system equivalent to (D_i), and $\mathfrak{L}(D_i;\ 0)=\mathfrak{L}(D_i';\ a_i')$, where $a_1'=\cdots=a_n'=-1$, as is easily seen from (2.2.3). Put $k=(-1, \cdots, -1)\in\mathfrak{B}$. Then $a_i'=e_i\cdot k$ for all i. Hence $\mathfrak{L}$ falls into the family considered in Theorem 8.2. $\mathfrak{L}'$ is simple and of dimension $(n-1)(p^n-1)$ if $n>2$.

The algebra denoted by the notation $\mathfrak{T}_n$ in [1] is obtained as $\mathfrak{L}(D_i, a_i)$ by setting $D_i=\partial/\partial g_i$, $a_i=1$ for $i=1, 2, \cdots, n$. Set $D_i'=g_i\,\partial/\partial g_i$ as before. Then (2.2.3) yields $a_i'=g_i-1$. Suppose that $\mathfrak{L}=\mathfrak{L}(D_i', a_i')$ is of type I. Then there exists a nonzero $b\in\mathfrak{A}$ such that $(D_i'-a_i)b=0$ for all i, from which it follows easily that $\partial(bg_i)/\partial g_i=bg_i$ for all i. Hence we have $bg_i=0$, $b=0$, a contradiction. Thus $\mathfrak{T}_n$ is of type II, and hence of dimension $(n-1)p^n$. The authors have been unable to decide whether or not $\mathfrak{L}\in\mathfrak{F}_c$. If $\mathfrak{L}\in\mathfrak{F}_c$ then $\mathfrak{L}$ will fall into the family considered in Theorem 8.4.

Consider now any simple algebra $\mathfrak{L}$ of dimension p^n-1 obtained by setting $m=1$ in our Theorem 8.1. It is spanned by elements of the form $g^u(\xi_0D_0+\xi_1D_1)$, where $g_1, \cdots, g_n$ is a set of principal generators belonging to the principal system (D_0, D_1) and where $\xi_0, \xi_1\in\Phi$ are such that $\xi_0D_0g^u+\xi_1D_1g^u=0$. Therefore we may take as a basis of $\mathfrak{L}$ elements of the form $e_u=(D_1g^u)D_0-(D_0g^u)D_1$, u running over all elements $\neq 0$ in $\mathfrak{B}$. Set

$$D_1g^u = \phi_i(u)g^u,\ i = 0, 1; \qquad \phi(u, v) = \phi_1(u)\phi_0(v) - \phi_0(u)\phi_1(v).$$

Then it is easily seen that $e_u\circ e_v=\phi(u, v)e_{u+v}$ for all u and v. The function $\phi(u, v)$ is a skew-symmetric bilinear form with respect to u and v. Therefore the algebra $\mathfrak{L}$ becomes a special case of the algebras considered in Theorem 11 of [1] if $\phi(u, v)$ satisfies the condition:

(9.0.1) $\phi(u, v) = 0$ if and only if u and v are linearly dependent over $GF(p)$.

However, an arbitrary principal system (D_0, D_1), which can be used to define a simple algebra of dimension $p^n - 1$ as in Theorem 8.1, does not always satisfy the condition (9.0.1).

Similar remarks may be made about the connection between simple algebras of dimension $p^n - 2$ given in our Theorem 8.3 and those in Theorem 12 of [1].

References

1. A. A. Albert and M. S. Frank, *Simple Lie algebras of characteristic p*, Rendiconti del Seminario Matematico della Università e Politecnico di Torino vol. 14 (1954–55) pp. 117–139.

2. Marguerite Straus Frank, *A new class of simple Lie algebras*, Proc. Nat. Acad. Sci. U.S.A. vol. 40 (1954) pp. 713–719.

3. I. Kaplansky, *Seminar on simple Lie-algebras*, Bull. Amer. Math. Soc. vol. 60 (1954) pp. 470–471.

4. Rimhak Ree, *On generalized Witt algebras*, Trans. Amer. Math. Soc. vol. 83 (1956) pp. 510–546.

The University of British Columbia,
Vancouver, B. C.