NEW SIMPLE LIE ALGEBRAS OF PRIME CHARACTERISTIC(1)

BY

RICHARD BLOCK

1. **Introduction.** For a number of years, the only known simple Lie algebras of characteristic $p>0$ not analogues of the classical algebras of characteristic zero were those of dimension p^n of H. Zassenhaus [9], and of dimension np^n of N. Jacobson [5], both generalizations of the p-dimensional algebras of E. Witt. During the last few years, a number of new classes of simple Lie algebras have been determined. These are due to Kaplansky, who in [6] noted the existence of a class of algebras of dimension rp^n, $1 \leqq r \leqq n$, generalizing those of Zassenhaus and Jacobson; to M. S. Frank, who in [2] obtained algebras $\mathfrak{S}_n$ of dimension $(n-1)(p^n-1)$; and to A. A. Albert and M. S. Frank, who in [1] determined new classes of simple algebras $\mathfrak{T}_n$, $\mathfrak{V}_m$, $\mathfrak{L}_0$, and $\mathfrak{L}_\delta$, of dimensions $(n-1)p^n$, $p^{2m}-2$, p^n-1 and p^n-2 respectively, and a generalization of the Zassenhaus algebras, of dimension p^n.

In this paper we obtain a new class of simple Lie algebras, which we shall designate by the symbol $\mathfrak{L}(\mathfrak{G}, \delta, f)$. Here $\mathfrak{G}$ is an additive group, of order $p^n>1$, which is a direct sum of a finite number of finite elementary p-groups $\mathfrak{G}_0, \cdots, \mathfrak{G}_m$. These groups are then finite dimensional vector spaces over the prime field $\mathfrak{F}_p$. We let $m(\mathfrak{G})$ denote the index m, allow $\mathfrak{G}_0$ to be zero, and assume that either $p>2$ or $\mathfrak{G} \neq \mathfrak{G}_1$. For $i=1, \cdots, m$, we take δ_i to be a nonzero element of $\mathfrak{G}_i$, and write $\delta=\delta_1+\cdots+\delta_m$. We index a basis of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ over a field $\mathfrak{F}$ of characteristic p by the elements of $\mathfrak{G}$ other than 0 and $-\delta$, denoting by $v(\alpha)$ the basis element corresponding to α. Furthermore we assume given, for each i, a nondegenerate skew-symmetric biadditive function f_i on $(\mathfrak{G}_i, \mathfrak{G}_i)$ to $\mathfrak{F}$, such that, for $i=1, \cdots, m$, there are additive functions g_i, h_i, on $\mathfrak{G}_i$ to $\mathfrak{F}$, with $g_i(\delta_i)=0$ and $f_i(\alpha, \beta)=g_i(\alpha)h_i(\beta)-g_i(\beta)h_i(\alpha)$ for every α and β in $\mathfrak{G}_i$. The definition of the algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ may then be completed by defining multiplication in the algebra by $v(\alpha)v(\beta)=\sum_{i=0}^{m} f_i(\alpha_i, \beta_i) \cdot v(\alpha+\beta-\delta_i)$, where α_i and β_i are the components of α and β in $\mathfrak{G}_i$, and where δ_0 and $v(0)$ denote zero. Then we shall prove that $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is a central simple Lie algebra. Its dimension is p^n-2 except when $\mathfrak{G}=\mathfrak{G}_0$, in which case the

Presented to the Society on September 1, 1955 and April 14, 1956 under the titles *Some properties of new simple Lie algebras* and *New simple Lie algebras of order* p^n-2; received by the editors March 8, 1957.

(1) This paper is essentially the author's doctoral thesis, the University of Chicago, August, 1956. The author wishes to express his gratitude to Professor A. A. Albert, under whom the thesis was written.

This work was sponsored in part by the Office of Ordnance Research, U. S. Army, under Contract DA-11-022-ORD-1571.

dimension is p^n-1. The algebras for which $\mathfrak{G}=\mathfrak{G}_0$ and $\mathfrak{G}=\mathfrak{G}_1$ are direct generalizations of the algebras $\mathfrak{L}_0$ and $\mathfrak{L}_\delta$, respectively.

G. B. Seligman in [7; 8] considered algebras over an algebraically closed field of characteristic $p>7$, and proved that if a restricted simple Lie algebra has a restricted representation with the associated trace form nondegenerate, then the algebra must be classical. It has been an open question whether there exist nonclassical restricted simple Lie algebras with any nondegenerate trace form. We shall find a nondegenerate trace form for every one of the algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$, and shall determine which of them are restricted. These restricted algebras generalize the algebras $\mathfrak{B}_m$. We shall show them to be the same, up to isomorphism, as a certain class of algebras which we shall denote by $\mathfrak{B}_{m,\mu}$, these being subalgebras of the Witt-Jacobson algebras. We shall also examine the closely related simple algebras $\mathfrak{S}_n$ and $\mathfrak{T}_n$ $(n>2)$ for the property of being restricted and having a trace form, proving that $\mathfrak{S}_n$ is restricted, but has a nondegenerate trace form if and only if $n=3$, and that $\mathfrak{T}_n$ is not restricted. Thus the algebras $\mathfrak{B}_{m,\mu}$ and $\mathfrak{S}_3$ constitute the only known nonclassical restricted simple Lie algebras with a nondegenerate trace form(2).

We shall show that if $p>3$, $\mathfrak{G}\neq\mathfrak{G}_0$, $\mathfrak{G}\neq\mathfrak{G}_1$ and $n>2m$, then $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is not isomorphic to any previously known simple Lie algebra, even though its dimension is not new(3). The question as to when algebras of the same dimension are nonisomorphic is a very deep one, especially when the strong properties of matrix algebras are not available. In general, it is not enough to show that the algebras have Cartan subalgebras of different dimensions. For it has not been known whether the Cartan decompositions relative to two Cartan subalgebras of a simple algebra need be essentially the same. In fact we shall give an example here, for any positive integer q and any prime characteristic, of one of our simple algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ with Cartan subalgebras of q distinct dimensions.

Here we shall make the first use of the algebras of derivations for distinguishing among algebras of the same dimension. For $p>3$, we shall determine the algebra of derivations of $\mathfrak{L}(\mathfrak{G}, \delta, f)$, and show that two algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ and $\mathfrak{L}(\mathfrak{G}', \delta', f')$ are isomorphic only if either $\mathfrak{G}_0=0$, $\mathfrak{G}_0'=0$ and $m(\mathfrak{G})=m(\mathfrak{G}')$, or $\mathfrak{G}_0\neq 0$, $\mathfrak{G}_0'\neq 0$ and $\min [2, m(\mathfrak{G})]=\min [2, m(\mathfrak{G}')]$. Moreover the determination of derivations yields a proof that except for a 7-dimensional algebra of characteristic 3 and possibly certain algebras of characteristic 2, the algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ are nonclassical.

2. **New Lie algebras.** Let $\mathfrak{F}$ be a field of characteristic p and let the nonzero group

(2) Certain of our results on restrictedness have also been obtained by Seligman.

(3) *Added in proof.* Since this was written, the paper of S. A. Jennings and R. Ree, *On a family of Lie algebras of characteristic p*, Trans. Amer. Math. Soc. vol. 84 (1957) pp. 192–207, has appeared. They determine simple Lie algebras of dimensions $m(p^n-1)$, mp^n, and p^n-2, where $1\leqq m<n$. Their algebras of dimension p^n-1 are included among ours, and the class of their algebras of dimension p^n-2 may be seen to be the same as the class of our algebras for which $\mathfrak{G}=\mathfrak{G}_1$.

$$\mathfrak{G} = \mathfrak{G}_0 + \cdots + \mathfrak{G}_m \tag{1}$$

be the direct sum of a finite number of finite abelian groups $\mathfrak{G}_0, \cdots, \mathfrak{G}_m$. Then every α in $\mathfrak{G}$ has a unique expression as the sum

$$\alpha = \alpha_0 + \cdots + \alpha_m \tag{2}$$

with components α_i in $\mathfrak{G}_i$. Select some δ in $\mathfrak{G}$. Then

$$\delta = \delta_0 + \cdots + \delta_m \qquad (\delta_i \in \mathfrak{G}_i). \tag{3}$$

Also let $f=f(\alpha, \beta)$ be a skew-symmetric biadditive form on $\mathfrak{G}$ taking values in $\mathfrak{F}$. Now suppose that

$$u: \alpha \to u(\alpha) = u_\alpha$$

is a one-to-one mapping of $\mathfrak{G}$ onto a basis of a vector space $\mathfrak{L}$ over $\mathfrak{F}$. Then the multiplication table

$$u_\alpha u_\beta = \sum_{i=0}^{m} f(\alpha_i, \beta_i) u(\alpha + \beta - \delta_i) \tag{4}$$

defines an anticommutative algebra $\mathfrak{L}$ over $\mathfrak{F}$.

If $\delta_i = 0$ for more than one index i then, by taking the sum of the $\mathfrak{G}_i$ over those indices for which $\delta_i = 0$ and considering this as a single subgroup $\mathfrak{G}_k$ of $\mathfrak{G}$ with $\delta_k = 0$, we get an algebra of the type defined by Formulas (1) through (4), with smaller m and with $\delta_i \neq 0$ except for one index, say $i=0$. Hence we may assume, without loss of generality, that

$$\delta_0 = 0, \qquad \delta_i \neq 0 \qquad (i = 1, \cdots, m), \tag{5}$$

where we allow $\mathfrak{G}_0$ *to be zero.*

The definition of the algebra $\mathfrak{L}$ does not involve any expression of the form $f(\alpha_i, \beta_j)$ with $\alpha_i \in \mathfrak{G}_i$, $\beta_j \in \mathfrak{G}_j$, $i \neq j$. Hence we may also assume, without loss of generality, that all such expressions are zero, so that, denoting by f_i the restriction of f to $\mathfrak{G}_i$, we have

$$f(\alpha, \beta) = f_0(\alpha_0, \beta_0) + \cdots + f_m(\alpha_m, \beta_m).$$

We now determine when $\mathfrak{L}$ satisfies the Jacobi identity. We have

$$\begin{aligned}(u_\alpha u_\beta) u_\gamma &= \left\{ \sum_{i=0}^{m} f(\alpha_i, \beta_i) u(\alpha + \beta - \delta_i) \right\} u_\gamma \\ &= \sum_{i,j=0}^{m} f(\alpha_i, \beta_i) f(\alpha_j + \beta_j - \delta_i, \gamma_j) u(\alpha + \beta + \gamma - \delta_i - \delta_j).\end{aligned}$$

For any particular k and l, we take the term for which $i=k$, $j=l$ and, when $k \neq l$, the term for which $i=l$, $j=k$, and add these to the similar terms in $(u_\beta u_\gamma) u_\alpha + (u_\gamma u_\alpha) u_\beta$. We get a term in $u(\alpha+\beta+\gamma-\delta_k-\delta_l)$ whose coefficient is the following:

$$f(\alpha_k, \beta_k)f(\alpha_l, \gamma_l) + f(\gamma_k, \alpha_k)f(\alpha_l, \beta_l) + f(\alpha_k, \beta_k)f(\beta_l, \gamma_l) + f(\beta_k, \gamma_k)f(\beta_l, \alpha_l) + f(\beta_k, \gamma_k)f(\gamma_l, \alpha_l) + f(\gamma_k, \alpha_k)f(\gamma_l, \beta_l), \tag{6}$$

plus a term, in case $k \neq l$, obtained from (6) by interchanging k and l. This term is the negative of (6) since f is skew-symmetric and so the sum is zero. In case $k = l$, the coefficient is given by (6) plus the expression $f(\alpha_k, \beta_k)f(\gamma_k, \delta_k) + f(\beta_k,\gamma_k)f(\alpha_k,\delta_k) + f(\gamma_k,\alpha_k)f(\beta_k,\delta_k)$. Thus, since (6) is zero when $k = l$ and since $u(\alpha+\beta+\gamma-2\delta_i) = u(\alpha+\beta+\gamma-2\delta_j)$ only if $i=j$, we see that the Jacobi identity is satisfied if and only if

$$f(\alpha_i, \beta_i)f(\gamma_i, \delta_i) + f(\beta_i, \gamma_i)f(\alpha_i, \delta_i) + f(\gamma_i, \alpha_i)f(\beta_i, \delta_i) = 0 \tag{7}$$

for $i = 1, \cdots, m$ and for all α, β and γ in $\mathfrak{G}$.

If $f(\gamma_i, \delta_i) \neq 0$ for some γ_i in $\mathfrak{G}_i$, then we take $g_i(\alpha_i) = f(\alpha_i, \delta_i)$ and $h_i(\alpha_i) = f(\gamma_i, \alpha_i)[f(\gamma_i, \delta_i)]^{-1}$, so that g_i and h_i are additive functions on $\mathfrak{G}_i$, taking values in $\mathfrak{F}$, with

$$g_i(\delta_i) = 0. \tag{8}$$

Moreover, (7) implies that

$$f(\alpha_i, \beta_i) = g_i(\alpha_i)h_i(\beta_i) - g_i(\beta_i)h_i(\alpha_i) \tag{9}$$

for every α_i, β_i in $\mathfrak{G}_i$.

Conversely if $g = g_i$, $h = h_i$ are given additive functions on $\mathfrak{G}_i$, with values in $\mathfrak{F}$, satisfying (8), then taking f such that (9) holds, we have $f(\alpha_i, \delta_i) = g(\alpha_i)h(\delta_i)$. Hence for $\alpha = \alpha_i$, $\beta = \beta_i$ and $\gamma = \gamma_i$ in $\mathfrak{G}_i$ we have

$$\begin{aligned} f(\alpha, \beta)f(\gamma, \delta_i) + f(\beta, \gamma)f(\alpha, \delta_i) + f(\gamma, \alpha)f(\beta, \delta_i) \\ = [g(\alpha)h(\beta)g(\gamma) + g(\beta)h(\gamma)g(\alpha) + g(\gamma)h(\alpha)g(\beta) - g(\beta)h(\alpha)g(\gamma) \\ - g(\gamma)h(\beta)g(\alpha) - g(\alpha)h(\gamma)g(\beta)]h(\delta_i) = 0, \end{aligned}$$

and (7) holds. Thus we have proved the following theorem.

THEOREM 1. *The algebra defined by Formulas* (1) *through* (5) *is a Lie algebra if and only if it is true that for* $i = 1, \cdots, m$, *either* $f(\alpha_i, \delta_i) = 0$ *for all* α_i *in* $\mathfrak{G}_i$ *or there exist additive functions* g_i, h_i *on* $\mathfrak{G}_i$ *with values in* $\mathfrak{F}$, *such that* (8) *and* (9) *hold.*

We note that the condition of Theorem 1 holds for any i such that $\mathfrak{G}_i$ is a vector space over $\mathfrak{F}_p$ of dimension $\leqq 3$, since (7) holds automatically for such a $\mathfrak{G}_i$.

3. **Simple algebras.** The algebra $\mathfrak{L}$ contains the one-dimensional ideal $u_0\mathfrak{F}$, since for any α in $\mathfrak{G}$, $u_0u_\alpha = 0$. Henceforth we consider the algebra $\mathfrak{L}' = \mathfrak{L} - u_0\mathfrak{F}$. It has basis elements

$$v_\alpha = v(\alpha) = u_\alpha + u_0F \qquad (\alpha \in \mathfrak{G}, \alpha \neq 0),$$

and its multiplication is determined by

$$v_\alpha v_\beta = \sum_{i=0}^{m} f(\alpha_i, \beta_i) v(\alpha + \beta - \delta_i), \qquad v(0) = 0. \tag{10}$$

The subspace of $\mathfrak{L}'$ spanned by the basis elements v_α for $\alpha \neq -\delta$ forms an ideal. For by (10), $v_\alpha v_\beta$ contains a term in $v_{-\delta}$ only if $\alpha+\beta-\delta_i = -\delta$ for some i, in which case $\alpha_i = -\beta_i$ and $f(\alpha_i, \beta_i) = 0$. We call this ideal $\mathfrak{L}(\mathfrak{G}, \delta, f)$. The condition of Theorem 1 for an algebra to be a Lie algebra holds for the algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ also, as follows from the proof of Theorem 1.

THEOREM 2. *If the algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is simple then each f_i is nondegenerate and $\mathfrak{G}$ is an elementary p-group.*

For suppose that $f(\alpha_i, \beta_i) = 0$ for some nonzero α_i in $\mathfrak{G}_i$ and every β_i in $\mathfrak{G}_i$. Then $v(\alpha_i)v_\beta = 0$ for every β in $\mathfrak{G}$, so that $v(\alpha_i)\mathfrak{F}$ forms a one-dimensional ideal of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ unless $\alpha_i = -\delta$. If $\alpha_i = -\delta$ then $v_{-2\delta}\mathfrak{F}$ forms a one-dimensional ideal of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ unless $2\delta = 0$, so that we may assume that $m = 1$, that is, $\delta = \delta_1$, that $2\delta = 0$, and that $f(\delta, \beta) = 0$ for every β in $\mathfrak{G}$. But then all elements of the form $v_\alpha + v_{\alpha+\delta}$, $\alpha \in \mathfrak{G}$, $\alpha \neq 0, \delta$, span a proper ideal, since in this case $(v_\alpha + v_{\alpha+\delta})v_\beta = [f(\alpha_0, \beta_0) + f(\alpha_1, \beta_1)](v_{\alpha+\beta} + v_{\alpha+\beta+\delta})$. Now if some $\mathfrak{G}_i$ is not an elementary p-group, then there is a nonzero element $\alpha_i = p\gamma_i$ in $\mathfrak{G}_i$, so that $f(\alpha_i, \beta_i) = pf(\gamma_i, \beta_i) = 0$ and f_i is degenerate. Thus if each f_i is nondegenerate, then each $\mathfrak{G}_i$ is an elementary p-group, so that $\mathfrak{G}$ is also an elementary p-group and the theorem is proved.

We shall henceforth assume that $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is a Lie algebra, so that, if $i \neq 0$ and f_i is nondegenerate, there are additive functions g_i, h_i on $\mathfrak{G}_i$ such that (8) and (9) hold.

We shall proceed to the proof of the converse of Theorem 2, making use of the following two notions. For α in $\mathfrak{G}$, $\alpha \neq 0$, $-\delta$, and $x = \sum_{\beta \neq 0, -\delta} \xi_\beta v_\beta$ in $\mathfrak{L}(\mathfrak{G}, \delta, f)$, we say that α is *x-admissible* if $\xi_\alpha \neq 0$, and we define the *length* $\lambda(x)$ of x to be the number of nonzero coordinates ξ_β of x.

Albert and Frank [1] introduced the special cases of the algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ for which $\mathfrak{G} = \mathfrak{G}_0$ and $\mathfrak{G} = \mathfrak{G}_1$, calling the algebras $\mathfrak{L}_0$ and $\mathfrak{L}_\delta$, respectively. They considered $\mathfrak{G}$ as being an n-dimensional vector space over the prime field $\mathfrak{F}_p$. The algebra $\mathfrak{L}_0$ was proved to be simple for any p and $n > 1$ under the assumption that $f(\alpha, \beta) = 0$ only if α and β are linearly dependent over $\mathfrak{F}_p$. For the algebra $\mathfrak{L}_\delta$, the notation w_α in [1] corresponds to our $v_{\alpha+\delta}$. Albert and Frank proved, for every $p > 2$ and $n > 1$, that $\mathfrak{L}_\delta$ is simple if there is a fixed basis of $\mathfrak{G}$ with δ as a basis element, such that $f(\alpha, \beta) = 0$ implies that α, β either are linearly dependent over $\mathfrak{F}_p$ or both have zero coefficient in δ. In the following two lemmas, we shall prove $\mathfrak{L}_0$ and $\mathfrak{L}_\delta$ to be simple under the weaker hypothesis that f is nondegenerate.

LEMMA 1. *If $\mathfrak{G} = \mathfrak{G}_0$, that is, $m = 0$, and if f is nondegenerate, then $\mathfrak{L}(\mathfrak{G}, \delta, f) = \mathfrak{L}_0$ is simple.*

For suppose that $\mathfrak{M}$ is a nonzero ideal of $\mathfrak{L}_0$ and that $x=\sum_\beta \xi_\beta v_\beta$ is a nonzero element of $\mathfrak{M}$ of minimal length. If $\lambda(x)>1$, let α and α' be distinct x-admissible elements of $\mathfrak{G}$. Then there is no γ such that $f(\alpha,\gamma)=0$ and $f(\alpha',\gamma)\neq 0$, for otherwise $xv_\gamma=\sum_\beta \xi_\beta f(\beta,\gamma)v_{\beta+\gamma}$ would be nonzero and have smaller length than x. Hence for any γ in $\mathfrak{G}$, $f(\alpha,\gamma)=0$ if and only if $f(\alpha',\gamma)=0$. Now suppose that γ is such that $f(\alpha,\gamma)\neq 0$; then also $f(\alpha',\gamma)\neq 0$. If we take $y=xv_\gamma=\sum_\beta \xi_\beta f(\beta,\gamma)v_{\beta+\gamma}$, then $\alpha+\gamma$ and $\alpha'+\gamma$ are y-admissible, y is a nonzero element of $\mathfrak{M}$ and $\lambda(y)\leqq\lambda(x)$, so that y also has minimal length. Therefore $f(\alpha+\gamma,\alpha'+\gamma)=0$ since $f(\alpha'+\gamma,\alpha'+\gamma)=0$. But also $f(\alpha,\alpha')=0$ since $f(\alpha',\alpha')=0$, and so $0=f(\alpha+\gamma,\alpha'+\gamma)=f(\alpha,\gamma)-f(\alpha',\gamma)$. Hence for any γ we have $f(\alpha,\gamma)=f(\alpha',\gamma)$, $f(\alpha-\alpha',\gamma)=0$, so that by the nondegeneracy of f, $\alpha-\alpha'=0$ and $\alpha=\alpha'$, a contradiction.

Thus $\lambda(x)=1$ and $\mathfrak{M}$ contains some v_α with $\alpha\neq 0$. Let $\mathfrak{A}$ be the set of all β for which v_β is in $\mathfrak{M}$. If $\beta\in\mathfrak{A}$ and $f(\beta,\gamma)\neq 0$ then $\gamma\in\mathfrak{A}$, since $v_\beta v_{\gamma-\beta}=f(\beta,\gamma)v_\gamma\neq 0$. The nonzero element α is in $\mathfrak{A}$ and by the nondegeneracy of f there is an α' with $f(\alpha,\alpha')\neq 0$. Thus α' is also in $\mathfrak{A}$. Suppose that $\gamma\notin\mathfrak{A}$. Then $f(\alpha',\gamma)=0$, so that $f(\alpha',\alpha+\gamma)=f(\alpha',\alpha)\neq 0$ and $\alpha+\gamma$ is in $\mathfrak{A}$. We may choose γ' such that $f(\gamma,\gamma')\neq 0$; thus $\gamma'\notin\mathfrak{A}$. But then $f(\alpha,\gamma')=0$, $f(\alpha+\gamma,\gamma')=f(\gamma,\gamma')\neq 0$, and since $\alpha+\gamma$ is in $\mathfrak{A}$, so is γ', a contradiction. Hence $\mathfrak{A}=\mathfrak{G}$, $\mathfrak{M}$ contains every basis element, $\mathfrak{M}=\mathfrak{L}_0$ and $\mathfrak{L}_0$ is simple.

LEMMA 2: *If $p>2$, $\mathfrak{G}=\mathfrak{G}_1$ and f is nondegenerate, then the Lie algebra $\mathfrak{L}(\mathfrak{G},\delta,f)=\mathfrak{L}_\delta$ is simple.*

In this proof we shall use our assumption that there are additive functions $g=g_1$ and $h=h_1$ such that (8), (9) hold. We note that by the nondegeneracy of f, there is no nonzero α in $\mathfrak{G}$ such that $g(\alpha)=h(\alpha)=0$. Let $\mathfrak{M}$ be a nonzero ideal of $\mathfrak{L}_\delta$, $x=\sum_\beta \xi_\beta v_\beta$ be a nonzero element of $\mathfrak{M}$ of minimal length, and suppose that $\lambda(x)>1$. If $g(\alpha)=0$ for some x-admissible α, then with γ such that $g(\gamma)\neq 0$, we have $f(\alpha,\gamma)=-g(\gamma)h(\alpha)\neq 0$, $\lambda(xv_\gamma)\leqq\lambda(x)$, $\alpha+\gamma-\delta$ is (xv_γ)-admissible and $g(\alpha+\gamma-\delta)=g(\gamma)\neq 0$. Hence we may assume that $g(\beta)\neq 0$ for some x-admissible β. Now if $g(\alpha)=0$ for some x-admissible α, then $f(\beta,\alpha)=g(\beta)h(\alpha)\neq 0$, $xv_\alpha\neq 0$ since $\beta+\alpha-\delta\neq 0$, and $\lambda(xv_\alpha)<\lambda(x)$, a contradiction. Hence for every x-admissible β, $g(\beta)\neq 0$. Take an x-admissible α and let $y=xv_{-\alpha+2\delta}$. Then $f(\alpha,-\alpha+2\delta)=2g(\alpha)h(\delta)\neq 0$, $\delta=\alpha+(-\alpha+2\delta)-\delta$ is y-admissible, $y\neq 0$ and $\lambda(y)\leqq\lambda(x)$, so that $\lambda(y)=\lambda(x)$. Thus $\beta-\alpha+\delta=\beta+(-\alpha+2\delta)-\delta$ is y-admissible for every x-admissible β, and since δ is y-admissible and $g(\delta)=0$, we have $g(\beta-\alpha+\delta)=g(\beta)-g(\alpha)=0$ for every x-admissible β. Now let α and β be distinct x-admissible elements of $\mathfrak{G}$. If $\alpha+\beta-\delta\neq 0$, then since $\lambda(xv_\beta)<\lambda(x)$, we have $xv_\beta=0$, $f(\alpha,\beta)=g(\alpha)h(\beta)-g(\alpha)h(\alpha)=0$, $h(\alpha)=h(\beta)$, $\alpha=\beta$, a contradiction, while if $\alpha+\beta-\delta=0$, we obtain the same contradiction by using $xv_{-\beta}$.

Hence $\lambda(x)=1$ and $\mathfrak{M}$ contains some basis element v_α. If $g(\alpha)=0$, so that $h(\alpha)\neq 0$, then with β such that $g(\beta)\neq 0$, we have $f(\alpha,\beta)=-g(\beta)h(\alpha)\neq 0$. Thus

$\mathfrak{M}$ contains $v_{\alpha+\beta-\delta}$ where $g(\alpha+\beta-\delta)=g(\beta)\neq 0$, so that $\mathfrak{M}$ always contains a v_γ with $g(\gamma)\neq 0$. Now let β be such that $g(\beta)=0$ and $\beta\neq-\delta$. It follows that $h(\beta+\delta)\neq 0$. Then $\mathfrak{M}$ contains $v_\gamma v_{-\gamma+\beta+\delta}=f(\gamma, \beta+\delta)v_\beta$, and thus $\mathfrak{M}$ contains v_β since $f(\gamma, \beta+\delta)=g(\gamma)h(\beta+\delta)\neq 0$. In particular $\mathfrak{M}$ contains v_δ and so $\mathfrak{M}$ also contains $v_\alpha v_\delta=f(\alpha, \delta)v_\alpha$ and v_α for any α such that $g(\alpha)\neq 0$, since $f(\alpha, \delta)=g(\alpha)h(\delta)\neq 0$. Hence $\mathfrak{M}$ contains every basis element and $\mathfrak{M}=\mathfrak{L}_\delta$.

THEOREM 3. *Suppose that either $p>2$ or $\mathfrak{G}\neq\mathfrak{G}_1$, and that each f_i is non-degenerate. Then $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is a central simple algebra. When $\mathfrak{G}\neq\mathfrak{G}_0$, the dimension of the simple algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is p^n-2, while when $\mathfrak{G}=\mathfrak{G}_0$, the dimension is p^n-1, where $\mathfrak{G}$ is an elementary p-group of order p^n, $n>1$, in either case.*

The simplicity of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ when $\mathfrak{G}\neq\mathfrak{G}_0, \mathfrak{G}_1$ remains to be proved. We note that if α_i is a nonzero element of $\mathfrak{G}_i$, then there is a β_i in $\mathfrak{G}_i$ such that $f(\alpha_i, \beta_i)\neq 0$ and $\alpha_i+\beta_i-\delta_i\neq 0$, for by the nondegeneracy of f_i there is a γ_i in $\mathfrak{G}_i$ such that $f(\alpha_i, \gamma_i)\neq 0$, and if $\alpha_i+\gamma_i-\delta_i=0$ then $f(\alpha_i, \delta_i)=f(\alpha_i, \alpha_i+\gamma_i)\neq 0$ and we could take δ_i for β_i.

Now let $\mathfrak{M}$ be a nonzero ideal of $\mathfrak{L}(\mathfrak{G}, \delta, f)$, and $x=\sum_\beta \xi_\beta v_\beta$ an element of $\mathfrak{M}$ of minimal length, and suppose that $\lambda(x)>1$. Then for some i, and we take $i=0$ if possible, there are distinct elements α_i and α_i' in $\mathfrak{G}_i$ such that α_i and α_i' are the components in $\mathfrak{G}_i$ of x-admissible elements α and α'. We may assume that some x-admissible element is not in $\mathfrak{G}_i$. For otherwise we may take an x-admissible β_i, a γ_i in $\mathfrak{G}_i$ such that $f(\beta_i, \gamma_i)\neq 0$, and for some $j\neq i$, an element $\gamma_j\neq 0$, $-\delta_j$ in $\mathfrak{G}_j$, and then, with $\gamma=\gamma_i+\gamma_j$, we may use xv_γ in place of x, since $\lambda(xv_\gamma)\leqq\lambda(x)$ and $\beta_i+\gamma_i-\delta_i+\gamma_j$ is (xv_γ)-admissible. Thus we may suppose that the component α_j of α is nonzero for some $j\neq i$, and also, by multiplying x if necessary by $v(\gamma_i)$ with $f(\delta_i, \gamma_i)\neq 0$, that $\alpha_i\neq\delta_i$. Choose ϵ_j in $\mathfrak{G}_j$ such that $f(\alpha_j, \epsilon_j)\neq 0$ and $\alpha_j+\epsilon_j-\delta_j\neq 0$. We note that if $i\neq 0$ then $\alpha_i+\delta_i$ is not x-admissible, for otherwise $xv(\epsilon_j)$ would be a nonzero element of $\mathfrak{M}$ of smaller length than x. Since $xv(-\alpha_i)=\sum_\beta \xi_\beta f(\beta_i, -\alpha_i)v(\beta-\alpha_i-\delta_i)$ has smaller length than x and so is zero, we have $f(\beta_i, -\alpha_i)=0$ for every x-admissible β. Now consider $y=xv(-\alpha_i+\epsilon_j)=\sum_\beta \xi_\beta f(\beta_j, \epsilon_j)v(\beta-\alpha_i+\epsilon_j-\delta_j)$. Then $\alpha-\alpha_i+\epsilon_j-\delta_j$ is y-admissible and $\lambda(y)\leqq\lambda(x)$, so that $\lambda(y)=\lambda(x)$ and $\alpha'-\alpha_i+\epsilon_j-\delta_j$ is also y-admissible. Choose ϵ_i such that $f(\alpha_i'-\alpha_i, \epsilon_i)\neq 0$ and $\alpha_i'-\alpha_i+\epsilon_i-\delta_i\neq 0$, and take $z=yv(\epsilon_i)$ unless $\epsilon_i=-\delta$. If $\epsilon_i=-\delta$ then $m=i=1$ and $j=0$, so that by our assumption on i, we have $\beta_0=\beta_0'$ for any y-admissible elements β and β', and we take $z=yv(\alpha_0+\epsilon_0+\epsilon_1)$ in this case. Thus $\mathfrak{M}$ contains z, $z\neq 0$ and $\lambda(z)<\lambda(y)$, a contradiction.

Hence $\lambda(x)=1$ and $\mathfrak{M}$ contains some v_α with $\alpha\neq 0$. Let β be any element of $\mathfrak{G}$ other than $-\delta$; we shall show that v_β is in $\mathfrak{M}$. For some i, $\beta_i\neq-\delta_i$, and by multiplying if necessary v_α by $v(\gamma_i+\gamma_j)$ with $f(\alpha_i, \gamma_i)\neq 0$, we may assume that $\alpha_j\neq 0$ for some $j\neq i$. Choosing a γ_j in $\mathfrak{G}_j$ such that $f(\alpha_j, \gamma_j)\neq 0$ and $\alpha_j+\gamma_j-\delta_j\neq 0$ and considering $v_\alpha v(-\alpha+\alpha_j+\gamma_j)=f(\alpha_j, \gamma_j)v(\alpha_j+\gamma_j-\delta_j)$, where we first multiply v_α by an appropriate v_γ in case $-\alpha+\alpha_j+\gamma_j=-\delta$, we may

assume that $\alpha=\alpha_j$ is in $\mathfrak{G}_j$. Now for any $\beta_i' \neq -\delta_i$ in $\mathfrak{G}_i$, we may choose β_i'' in $\mathfrak{G}_i$ such that $f(\beta_i'', \beta_i'+\delta_i)\neq 0$ and $-\beta_i''+\beta_i'+\delta_i\neq -\delta_i$. Also choose ϵ_j such that $f(\alpha_j, \epsilon_j)\neq 0$ and $-\alpha_j+\epsilon_j\neq -\delta_j$. Then $\mathfrak{M}$ contains

$$v(\alpha_j)v(\beta_i'' - \alpha_j + \epsilon_j) = f(\alpha_j, \epsilon_j)v(\beta_i'' + \epsilon_j - \delta_j)$$

and

$$v(\beta_i'' + \epsilon_j - \delta_j)v(-\beta_i'' + \beta_i' + \delta_i - \epsilon_j + \delta_j) = f(\beta_i'', \beta_i' + \delta_i)v(\beta_i').$$

Thus $\mathfrak{M}$ contains v_β, for since $\beta_i\neq -\delta_i$, we may take β_i' such that $f(\beta_i', \beta_i+\delta_i)\neq 0$ and then use $v(\beta_i')v(-\beta_i'+\beta+\delta_i)=f(\beta_i', \beta_i+\delta_i)v_\beta$, unless $-\beta_i'+\beta+\delta_i=-\delta$, in which case with appropriate β_i', ζ_i and ζ_j we may use

$$v(\beta_i')v(-\beta_i' + \zeta_i + \delta_i + \zeta_j) = f(\beta_i', \zeta_i + \delta_i)v(\zeta_i + \zeta_j),$$

$$v(\zeta_i + \zeta_j)v(-\zeta_i - \zeta_j + \beta + \delta_i) = f(\zeta_i, \beta_i + \delta_i)v_\beta.$$

Hence $\mathfrak{M}$ contains a basis of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ and $\mathfrak{M}=\mathfrak{L}(\mathfrak{G}, \delta, f)$ is simple.

Our proofs of simplicity are independent of $\mathfrak{F}$, so that the simple algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ are central.

We shall now determine which nondegenerate functions f satisfy the condition of Theorem 1, which, as we have noted, is necessary and sufficient for the algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ to be a Lie algebra.

THEOREM 4. *Suppose that $\delta=\delta_i$ is a nonzero element of the group $\mathfrak{G}=\mathfrak{G}_i$, and that $g=g_i$ and $h=h_i$ are additive functions on $\mathfrak{G}$ with values in $\mathfrak{F}$, such that $g(\delta_i)=0$. Then a necessary and sufficient condition for the function f defined by* (9) *to be nondegenerate is that $\mathfrak{G}$ be an elementary p-group, that is, a vector space over the prime field $\mathfrak{F}_p$, and that there exists a basis $(\delta, \beta_1, \cdots, \beta_r)$ of $\mathfrak{G}$ over $\mathfrak{F}_p$ such that for some k with $0\leqq k<r$, $g(\delta)=g(\beta_1)=\cdots=g(\beta_k)=0$ and the sets $\{g(\beta_{k+1}), \cdots, g(\beta_r)\}$, $\{h(\delta), \cdots, h(\beta_k)\}$ each are linearly independent over $\mathfrak{F}_p$.*

For we already know that it is necessary that $\mathfrak{G}$ be an elementary p-group. It is also clear that g cannot be identically zero and that if $g(\beta)=h(\beta)=0$, then $\beta=0$. Then taking $\{\delta, \beta_1, \cdots, \beta_k\}$ to be a basis of the kernel of g, and extending this to a basis of $\mathfrak{G}$,the condition follows. Conversely if the condition holds and $f(\alpha, \beta)=0$ for all β in $\mathfrak{G}$, then $f(\alpha, \delta)=g(\alpha)h(\delta)=0$ so that $g(\alpha)=0$, and $f(\alpha, \beta_r)=-g(\beta_r)h(\alpha)=0$ so that also $h(\alpha)=0$, and therefore $\alpha=0$ and f is nondegenerate.

Henceforth we shall assume that whenever we refer to $\mathfrak{L}(\mathfrak{G}, \delta, f)$, the algebra is a simple Lie algebra. Thus in particular the dimension over $\mathfrak{F}_p$ of each nonzero $\mathfrak{G}_i$ will be greater than one.

4. **Cartan subalgebras.** In this section we assume that the base field $\mathfrak{F}$ is algebraically closed. Let $\mathfrak{H}$ be a nilpotent subalgebra of a Lie algebra $\mathfrak{L}$. A function ρ on $\mathfrak{H}$ to $\mathfrak{F}$ is called a *root* of $\mathfrak{L}$ with respect to $\mathfrak{H}$ if there is a nonzero x in $\mathfrak{L}$ such that for every right multiplication R_h with h in $\mathfrak{H}$, x is annihilated by some power of $R_h-\rho(h)I$. The set of all such x is called the *root space* $\mathfrak{L}_\rho$ for ρ. Then $\rho=0$ is a root, $\mathfrak{L}_0$ is a subalgebra of $\mathfrak{L}$, the *zero-subalgebra* for $\mathfrak{H}$,

which contains $\mathfrak{H}$, and $\mathfrak{L}$ has a decomposition as the (vector space) direct sum of all root spaces $\mathfrak{L}_\rho$. If $\mathfrak{H}=\mathfrak{L}_0$, then $\mathfrak{H}$ is called a *Cartan subalgebra* of $\mathfrak{L}$, and the decomposition of $\mathfrak{L}$ into root spaces is called a *Cartan decomposition* of $\mathfrak{L}$. The condition $\mathfrak{H}=\mathfrak{L}_0$ is equivalent to the condition that the nilpotent subalgebra $\mathfrak{H}$ is its own normalizer, that is, that yh in $\mathfrak{H}$ for every h in $\mathfrak{H}$ implies that y is in $\mathfrak{H}$. If x is a *regular* element of $\mathfrak{L}$, that is, if the zero-subalgebra $\mathfrak{H}$ corresponding to x (or $x\mathfrak{F}$) has minimal dimension, then this subalgebra $\mathfrak{H}$ is a Cartan subalgebra of $\mathfrak{L}$. Thus Cartan subalgebras exist for any $\mathfrak{L}$.

The property of being the zero-subalgebra for a regular element is not used as the definition of a Cartan subalgebra, since such use would not be of advantage in the existing structure theory, and since the property is very difficult to prove for a given subalgebra. For zero characteristic, all Cartan subalgebras of $\mathfrak{L}$ are conjugate and thus all are zero-subalgebras for regular elements. However for prime characteristic, Theorem 6 below shows that a Cartan subalgebra of a simple algebra $\mathfrak{L}$ need not contain a regular element, and that the Cartan decompositions relative to two Cartan subalgebras of $\mathfrak{L}$ need not be essentially the same.

We shall first determine Cartan decompositions for the algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$. Let $\mathfrak{N}_0$ be a maximal subset of $\mathfrak{G}_0$ for which restriction of f is identically zero, that is, a subset of $\mathfrak{G}_0$ such that for any β in $\mathfrak{G}_0$, $f(\alpha, \beta)=0$ for all α in $\mathfrak{N}_0$ if and only if β is in $\mathfrak{N}_0$. Then $\mathfrak{N}_0$ is a subgroup of $\mathfrak{G}_0$, and $\mathfrak{N}_0=0$ only if $\mathfrak{G}_0=0$. Let $\mathfrak{N}_i$ be the kernel of g_i, $i=1, \cdots, m$, and let $\mathfrak{N}=\mathfrak{N}_0+\cdots+\mathfrak{N}_m$.

THEOREM 5. *The subspace $\mathfrak{H}_\mathfrak{N}$ of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ spanned by all v_α with α in $\mathfrak{N}$ $(\alpha \neq -\delta)$ is a Cartan subalgebra of $\mathfrak{L}(\mathfrak{G}, \delta, f)$.*

For $\mathfrak{H}_\mathfrak{N}$ is clearly abelian. Suppose that $x=\sum_\gamma \xi_\gamma v_\gamma$ is in the zero-subalgebra of $\mathfrak{H}_\mathfrak{N}$. Then for the right multiplication $R[v(\delta_i)]$, $i\neq 0$, we have $xR[v(\delta_i)]^t=\sum_\gamma \xi_\gamma f(\gamma_i, \delta_i)^t v_\gamma=0$ for some t, so that $g_i(\gamma_i)=0$ for any x-admissible γ. Also for any α in $\mathfrak{N}_0$ we have $xR(v_\alpha)^t=\sum_\gamma \xi_\gamma f(\gamma_0, \alpha)^t v_{\gamma+t\alpha}=0$, so that $f(\gamma_0, \alpha)=0$ for any x-admissible γ and any α in $\mathfrak{N}_0$, that is, γ_0 is in $\mathfrak{N}_0$ and γ is in $\mathfrak{N}$ for any x-admissible γ, x is in $\mathfrak{H}_\mathfrak{N}$ and $\mathfrak{H}_\mathfrak{N}$ is a Cartan subalgebra.

Since $\mathfrak{H}_\mathfrak{N}$ is abelian, any root ρ is linear on $\mathfrak{H}_\mathfrak{N}$. Moreover $v_\beta R(v_\alpha)^p=f(\beta, \alpha)^p v_\beta$, so that $v_\beta[R(v_\alpha)-f(\beta, \alpha)I]^p=0$, and if $f(\beta, \alpha)=f(\gamma, \alpha)$ for all α in $\mathfrak{N}$ then $\beta-\gamma$ is in $\mathfrak{N}$. It follows that any root ρ corresponds to a coset $\beta+\mathfrak{N}$ such that $\rho(v_\alpha)=f(\beta, \alpha)$ for any α in $\mathfrak{N}$, and such that the corresponding root space $\mathfrak{L}_\rho$ is spanned by all v_γ with γ in $\beta+\mathfrak{N}$. Thus if $\mathfrak{G}$ has order p^n and $\mathfrak{N}$ has order p^r, then $\mathfrak{H}_\mathfrak{N}$ has dimension p^r-2 (or p^r-1 in case $\mathfrak{G}=\mathfrak{G}_0$), each root space $\mathfrak{L}_\rho$ for $\rho\neq 0$ has dimension p^r, and the roots form an elementary p-group of order p^{n-r}.

THEOREM 6. *For any prime p and positive integer q, there exists a simple Lie algebra of characteristic p with Cartan subalgebras of q distinct dimensions.*

We shall use for the required examples algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ with $\mathfrak{G}=\mathfrak{G}_0$. Let $\mathfrak{G}$ be a vector space over $\mathfrak{F}_p$ of dimension $r=q(q+1)/2+1$, with basis $\mathfrak{B}=\{\beta_1, \cdots, \beta_r\}=\mathfrak{B}_1\cup\cdots\cup\mathfrak{B}_q\cup\{\beta_r\}$, where $\mathfrak{B}_1=\{\beta_1\}$, $\mathfrak{B}_2=\{\beta_2, \beta_3\}$, $\cdots$, $\mathfrak{B}_q=\{\beta_{r-q}, \cdots, \beta_{r-1}\}$. Also let $\{\xi_{ij}: i, j=1, \cdots, r; i<j\}$ be a set of $r(r-1)/2$ elements of $\mathfrak{F}$ which are linearly independent over $\mathfrak{F}_p$. We define the skew-symmetric biadditive function f on $\mathfrak{G}$ in terms of its values for the elements of the basis $\mathfrak{B}$ by setting $f(\beta_i, \beta_j)=\xi_{ij}$ for $i<j$ if β_i, β_j are in different sets $\mathfrak{B}_k$ or if $j=r$, and $f(\beta_i, \beta_j)=0$ if β_i, β_j are in the same $\mathfrak{B}_k$. Then f is non-degenerate, since if $f(\alpha, \beta_r)=0$ for $\alpha\neq 0$, then $\alpha=t\beta_r$, in which case $f(\alpha, \beta_1)\neq 0$. Thus $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is a simple Lie algebra. Let $\mathfrak{N}(k)$ be the subspace of $\mathfrak{G}$ spanned by $\mathfrak{B}_k$, $k=1, \cdots, q$. Then clearly f is identically zero on $\mathfrak{N}(k)$ and if $f(\alpha, \gamma)=0$ for every α in $\mathfrak{N}(k)$ then γ is in $\mathfrak{N}(k)$. Therefore the subspace $\mathfrak{H}_{\mathfrak{N}(k)}$ of $\mathfrak{L}(\mathfrak{G}, \delta, f)$, spanned (over $\mathfrak{F}$) by all v_α with α in $\mathfrak{N}(k)$, is a Cartan subalgebra of dimension p^k-1, $k=1, \cdots, q$, and the theorem is proved.

5. **Trace forms and restrictedness.** A symmetric bilinear form t on a Lie algebra $\mathfrak{L}$ is called a *trace form* (or an *invariant* or *associative form*) if

$$t(ab, c) = t(a, bc) \tag{11}$$

for every a, b and c in $\mathfrak{L}$.

We define a bilinear form on $\mathfrak{L}(\mathfrak{G}, \delta, f)$ in terms of the form for the elements of a basis by setting

$$t(v_\alpha, v_\beta) = 1 \text{ if } \alpha+\beta=-\delta, \qquad t(v_\alpha, v_\beta) = 0 \text{ if } \alpha+\beta\neq-\delta. \tag{12}$$

THEOREM 7. *The form defined by* (12) *is a nondegenerate trace form on the simple Lie algebra* $\mathfrak{L}(\mathfrak{G}, \delta, f)$.

The form is obviously symmetric. To prove (11), it is enough to show for basis elements v_α, v_β, v_γ that $t(v_\alpha v_\beta, v_\gamma)=t(v_\alpha, v_\beta v_\gamma)$. But $t(v_\alpha v_\beta, v_\gamma)=\sum_{i=0}^{m} f(\alpha_i, \beta_i)t\{v(\alpha+\beta-\delta_i), v_\gamma\}=\sum_{i=0}^{m} f(\alpha_i, \beta_i)\lambda_i$, where $\lambda_i=1$ or 0 according to whether $\alpha+\beta+\gamma-\delta_i=-\delta$ or not. Also $t(v_\alpha, v_\beta v_\gamma)=\sum_{i=0}^{m} f(\beta_i, \gamma_i)\cdot t\{v_\alpha, v(\beta+\gamma-\delta_i)\}=\sum_{i=0}^{m} f(\beta_i, \gamma_i)\lambda_i$. When $\lambda_i=1$, we have $\alpha_i+\beta_i+\gamma_i=0$ and $f(\alpha_i, \beta_i)=f(-\beta_i-\gamma_i, \beta_i)=f(-\gamma_i, \beta_i)=f(\beta_i, \gamma_i)$, so that t is a trace form. Since the Lie algebra is simple and t is not identically zero, t is nondegenerate.

A centerless Lie algebra $\mathfrak{L}$ over a field $\mathfrak{F}$ of characteristic p is called *restricted* if the pth power of every inner derivation is inner, that is, if for every x in $\mathfrak{L}$ there is an element z (necessarily unique) in $\mathfrak{L}$ such that for every y in $\mathfrak{L}$,

$$y(R_x)^p = yR_z \tag{13}$$

holds for the right multiplications R_x and R_z. The element z is denoted by x^p. It then follows [3] that for any x, y in $\mathfrak{L}$ and ξ in $\mathfrak{F}$,

$$(x+y)^p = x^p + y^p + s(x, y), \qquad (\xi x)^p = \xi^p x^p, \tag{14}$$

where $s(x, y)$ is a linear combination of $(p-1)$-fold products of x and y. If $\mathfrak{L}$ is a subspace of an associative algebra $\mathfrak{A}$ closed under commutation and

(associative) pth powers, then for x in $\mathfrak{L}$, $z=x^p$ satisfies (13) and $\mathfrak{L}$ (assumed to be centerless) is restricted; by (14) and the restrictedness of $\mathfrak{A}$, it is enough that $\mathfrak{L}$ contain the pth power of every element in some basis of it.

We shall prove the restrictedness of certain of the algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ by using particular representations of them. Let $\mathfrak{B}_n=\mathfrak{F}[z_1, \cdots, z_n]$ be the commutative associative algebra of all polynomials in $z_1, \cdots, z_n$ with coefficients in $\mathfrak{F}$, subject only to the restrictions that $z_1^p=\cdots=z_n^p=1$, so that $\mathfrak{B}_n$ has dimension p^n over $\mathfrak{F}$. A derivation of $\mathfrak{B}_n$ is determined by the values, which may be arbitrary elements of $\mathfrak{B}_n$, onto which it sends $z_1, \cdots, z_n$. We shall use the vector $(a_1, \cdots, a_n)$ to denote the derivation A which, for $i=1, \cdots, n$, sends z_i onto a_i. Then if $\mathfrak{B}=(b_1, \cdots, b_n)$ is another derivation, the commutator product of A and B is the derivation $C=A\cdot B=(c_1, \cdots, c_n)$, where

$$c_i=\sum_{j=1}^{n}\left(\frac{\partial a_i}{\partial z_j}b_j-\frac{\partial b_i}{\partial z_j}a_j\right) \qquad (i=1, \cdots, n). \tag{15}$$

Let $x_i=z_i-1$, $i=1, \cdots, n$. Then $\mathfrak{B}_n$ also equals the commutative associative algebra $\mathfrak{F}[x_1, \cdots, x_n]$ of all polynomials in $x_1, \cdots, x_n$, subject only to the restriction that $x_1^p=\cdots=x_n^p=0$, and the derivation $(a_1, \cdots, a_n)$ is also the unique derivation sending x_i onto a_i, $i=1, \cdots, n$. Since $\partial a/\partial x_j=\partial a/\partial z_j$ for any a in $\mathfrak{B}_n$, (15) becomes

$$c_i=\sum_{j=1}^{n}\left(\frac{\partial a_i}{\partial x_j}b_j-\frac{\partial b_i}{\partial x_j}a_j\right) \qquad (i=1, \cdots, n). \tag{16}$$

Now suppose that $n=2m$ and let $\mu_1, \cdots, \mu_m$ be arbitrary fixed nonzero elements of $\mathfrak{F}$. Define $\mathfrak{B}_{m,\mu}$ to be the set of all derivations of $\mathfrak{B}_{2m}$ of the form

$$A(\phi)=\left(\mu_1\frac{\partial\phi}{\partial z_{m+1}}, \cdots, \mu_m\frac{\partial\phi}{\partial z_{2m}}, -\mu_1\frac{\partial\phi}{\partial z_1}, \cdots, -\mu_m\frac{\partial\phi}{dz_m}\right), \tag{17}$$

where the term of ϕ in $(z_1\cdots z_{2m})^{p-1}$ has coefficient zero. Then $\mathfrak{B}_{m,\mu}$ is also the set of all derivations

$$A(\phi)=\left(\mu_1\frac{\partial\phi}{\partial x_{m+1}}, \cdots, \mu_m\frac{\partial\phi}{\partial x_{2m}}, -\mu_1\frac{\partial\phi}{\partial x_1}, \cdots, -\mu_m\frac{\partial\phi}{\partial x_m}\right), \tag{18}$$

where the term of ϕ in $(x_1\cdots x_{2m})^{p-1}$ has coefficient zero. By (15) we have

$$A(\phi)\cdot A(\psi)=A(\theta), \qquad \theta=\sum_{j=1}^{m}\mu_j\left(\frac{\partial\phi}{\partial z_j}\frac{\partial\psi}{\partial z_{m+j}}-\frac{\partial\phi}{\partial z_{m+j}}\frac{\partial\psi}{\partial z_j}\right), \tag{19}$$

and also the similar formula with x in place of z. Write

$$D(k_1, \cdots, k_{2m})=A(z_1^{k_1}\cdots z_{2m}^{k_{2m}}). \tag{20}$$

Then the $D(k_1, \cdots, k_{2m})$ with $0 \leqq k_j < p$ and $(k_1, \cdots, k_{2m}) \neq (0, \cdots, 0)$, $(p-1, \cdots, p-1)$ form a basis of $\mathfrak{V}_{m,\mu}$ over $\mathfrak{F}$, and by (19) we have

$$D(k_1, \cdots, k_{2m}) \cdot D(s_1, \cdots, s_{2m})$$

$$= \sum_{i=1}^{m} \mu_i (k_i s_{m+i} - k_{m+i} s_i) D(k_1 + s_1, \cdots, k_i + s_i - 1, k_{i+1} \tag{21}$$

$$+ s_{i+1}, \cdots, k_{m+i} + s_{m+i} - 1, k_{m+i+1} + s_{m+i+1}, \cdots, k_{2m} + s_{2m}),$$

where the indices are to be added modulo p. Since $(k_i s_{m+i} - k_{m+i} s_i) = 0$ if $k_i + s_i - 1 = k_{m+i} + s_{m+i} - 1 = p-1$, it follows that $\mathfrak{V}_{m,\mu}$ is closed under commutator products, that is, $\mathfrak{V}_{m,\mu}$ is a Lie algebra.

When $\mu_1 = \cdots = \mu_m = 1$ and $p > 2$, the algebra $\mathfrak{V}_{m,\mu}$, with the representation used in (18), was studied in [1] by Albert and Frank, who called it $\mathfrak{V}_m$.

LEMMA 3. *If $\mathfrak{G}_0 = 0$ and $\mathfrak{G}_1, \cdots, \mathfrak{G}_m$ are 2-dimensional over $\mathfrak{F}_p$ then $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is isomorphic to an algebra $\mathfrak{V}_{m,\mu}$, and conversely each $\mathfrak{V}_{m,\mu}$ is isomorphic to an algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ with $\mathfrak{G}$ of this type.*

Indeed for $i = 1, \cdots, m$ take a basis ζ_i, $\delta_i - \zeta_i$ of $\mathfrak{G}_i$ over $\mathfrak{F}_p$ and let $\mu_i = f(\zeta_i, \delta_i)$, so that $\mu_i \neq 0$. Then consider the mapping

$$w: v\left\{\sum_{i=1}^{m} [k_i \zeta_i + k_{m+i}(\delta_i - \zeta_i)]\right\} \to D(k_1, \cdots, k_{2m})$$

for $k_1, \cdots, k_{2m}$ in $\mathfrak{F}_p$. Here $v_{-\delta}$ corresponds to $D(p-1, \cdots, p-1)$, so that the linear mapping w^* determined by w sends $\mathfrak{L}(\mathfrak{G}, \delta, f)$ onto $\mathfrak{V}_{m,\mu}$. It follows from (10) and (21) that w^* preserves multiplication of basis elements and thus w^* is the required isomorphism. The converse also follows, since μ_i determines f_i.

Now write

$$E(k_1, \cdots, k_{2m}) = A(x_1^{k_1} \cdots x_{2m}^{k_{2m}}). \tag{22}$$

Then the $E(k_1, \cdots, k_{2m})$ with $0 \leqq k_j < p-1$ and $(k_1, \cdots, k_{2m}) \neq (0, \cdots, 0)$, $(p-1, \cdots, p-1)$ also form a basis of $\mathfrak{V}_{m,\mu}$, and their multiplication table is the same as that of the D, given by (21), but now of course $E(q_1, \cdots, q_{2m}) = 0$ if $q_j \geqq p$ for some j, $1 \leqq j \leqq 2m$.

LEMMA 4. *The algebra $\mathfrak{V}_{m,\mu}$ is restricted.*

Since $\mathfrak{V}_{m,\mu}$ is contained in the algebra of all linear transformations of $\mathfrak{B}_{2m}$, it is enough to prove that $\mathfrak{V}_{m,\mu}$ contains the (associative) pth power of each of the basis elements $E(k_1, \cdots, k_{2m})$. This pth power is of course always a derivation of $\mathfrak{B}_{2m}$, so that it is determined by the values it takes on $x_1, \cdots, x_{2m}$. If C is a linear transformation of $\mathfrak{B}_{2m}$ sending x_j onto c_j, then for the (associative) product of C and $E = E(k_1, \cdots, k_{2m})$ we have, by (18) and (22),

$$x_jCE = c_jE = \sum_{i=1}^{m} \mu_i \left(k_{m+i} x_1^{k_1} \cdots x_{m+i}^{k_{m+i}-1} \cdots x_{2m}^{k_{2m}} \frac{\partial c_j}{\partial x_i} - k_i x_1^{k_1} \cdots x_i^{k_i-1} \cdots x_{2m}^{k_{2m}} \frac{\partial c_j}{\partial x_{m+i}} \right) \qquad (j = 1, \cdots, 2m). \tag{23}$$

Now first suppose that $k_t > 1$ for some t, $1 \leqq t \leqq 2m$. Then x_t is a factor of each x_jE, and by (23), if x_t^s is a factor of each x_jE^s then x_t^{s+1} is a factor of each x_jE^{s+1}. Thus x_t^p is a factor of each x_jE^p and $E^p = 0$.

Next suppose that each k_t is 0 or 1. If $1 \leqq j \leqq m$ and

$$c_{j,s} = x_jE^s = k_j k_{m+j} \mu_j^s x_1^{sk_1} \cdots x_j^{k_j} \cdots x_{m+j}^{0} \cdots x_{2m}^{sk_{2m}}, \tag{24}$$

and we substitute in (23) with $C = E^s$ and $c_j = c_{j,s}$, then in the right hand side of (23) the two terms of the ith summand cancel for $i \neq j$ and we have

$$\begin{aligned} c_{j,s+1} &= c_{j,s}E = x_jE^{s+1} \\ &= k_j^2 k_{m+j}^2 \mu_j^{s+1} x_1^{(s+1)k_1} \cdots x_j^{2kj-1} \cdots x_{m+j}^{0} \cdots x_{2m}^{(s+1)k_{2m}}. \end{aligned} \tag{25}$$

Since k_j, k_{m+j} are 0 or 1, (25) is (24) with $s+1$ in place of s. But when $1 \leqq j \leqq m$, by the definition of E we have (24) if $k_j = s = 1$, so (24) holds for $s = p$, and $x_jE^p = 0$ except when $k_j = k_{m+j} = 1$ and $k_i = 0$ for $i \neq j$, $m+j$, in which case $x_jE^p = \mu_j^p x_j$. When $m < j \leqq 2m$, we have to interchange the exponents of x_j and x_{m+j} in the right hand sides of (24), (25) and multiply by $(-1)^s$, $(-1)^{s+1}$ respectively. Again $x_jE^p = 0$ except when $k_{j-m} = k_j = 1$ and $k_i = 0$ for $i \neq m-j, j$, in which case $x_jE^p = (-\mu_j)^p x_j$. Thus $E^p = 0$ unless $E = A(x_jx_{m+j})$ for some j, $1 \leqq j \leqq m$, in which case $E^p = \mu_j^{p-1}E$, so that $\mathfrak{V}_{m,\mu}$ is restricted.

THEOREM 8. *The simple Lie algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is restricted if and only if $\mathfrak{G}_0 = 0$ and $\mathfrak{G}_1, \cdots, \mathfrak{G}_m$ have order p^2. These restricted algebras are the same, up to isomorphism, as the algebras $\mathfrak{V}_{m,\mu}$, which are simple for $p > 2$ or $m > 1$.*

The necessity of the condition for restrictedness is what remains to be proved. Suppose that $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is restricted and that α is a nonzero element of $\mathfrak{G}_i$. Then for any v_β,

$$v_\beta(v_\alpha)^p = f(\beta_i, \alpha) f(\beta_i - \delta_i, \alpha) \cdots f(\beta_i - (p-1)\delta_i, \alpha) v_\beta. \tag{26}$$

Denoted by $q(\beta, \alpha)$ the coefficient of v_β on the right hand side of (26). Suppose that $(v_\alpha)^p = \sum_\gamma \xi(\gamma) v_\gamma$. If $i = 0$ and β is some element of $\mathfrak{G}_0$ such that $f(\beta, \alpha) \neq 0$, then $q(\beta, \alpha) = f(\beta, \alpha)^p \neq 0$. But $v(\beta)\{\sum_\gamma \xi(\gamma) v_\gamma\}$ has no term in $v(\beta)$. Hence $\mathfrak{G}_0 = 0$ and $i \neq 0$. Choose α such that $f(\alpha, \delta_i) \neq 0$. For any nonzero β in $\mathfrak{G}_i$, $v(\beta)\{\sum_\gamma \xi(\gamma) v_\gamma\}$ gives a term in $v(\beta)$ only when $\gamma = \delta_i$. But then $\xi(\delta_i) f(\beta, \delta_i) = q(\beta, \alpha)$. When $\beta = \alpha$ we have $q(\beta, \alpha) = 0$ and $f(\beta, \delta_i) \neq 0$, so that $\xi(\delta_i) = 0$ and therefore $q(\beta, \alpha) = 0$ for any β in $\mathfrak{G}_i$.

Now let $\gamma_1, \cdots, \gamma_r, \delta_i$ be a basis of $\mathfrak{G}_i$ over $\mathfrak{F}_p$. Since f_i is nondegenerate,

$f(\gamma_s, \delta_i) \neq 0$ for some s, say for $s=1$. Then $q(\gamma_r, \gamma_1)=0$ so that $f(\gamma_r - j\delta_i, \gamma_1)=0$ for some j in $\mathfrak{F}_p$. By changing the basis element γ_r to $\gamma_r - j\delta_i$ if necessary, we may assume that $f(\gamma_r, \gamma_1)=0$. Since $f(\gamma_1+\delta_i, \delta_i)\neq 0$, we also have $q(\gamma_r, \gamma_1+\delta_i)=0$. Thus for some k in $\mathfrak{F}_p$, $f(\gamma_r - k\delta_i, \gamma_1+\delta_i)=0$, $f(\gamma_r, \delta_i)+kf(\gamma_1, \delta_i)=g_i(\gamma_r)\cdot h_i(\delta_i)+kg_i(\gamma_1)h_i(\delta_i)=0$, $g_i(\gamma_r+k\gamma_1)=0$. But $0=f(\gamma_1, \gamma_r+k\gamma_1)=g_i(\gamma_1)h_i\cdot(\gamma_r+k\gamma_1)$, so that $h(\gamma_r+k\gamma_1)=0$ also. Thus $\gamma_r+k\gamma_1=0$, $r=1$, $\mathfrak{G}_i$ is 2-dimensional over $\mathfrak{F}_p$, and the theorem is proved.

6. **The algebras $\mathfrak{S}_n$ and $\mathfrak{T}_n$.** The simple algebras $\mathfrak{B}_{m,\mu}$ are closely related to the simple algebras $\mathfrak{S}_n$ of Frank [2], and $\mathfrak{T}_n$ of Albert and Frank [1]. We shall use here the same notation as in the preceding section for $\mathfrak{B}_n = \mathfrak{F}[x_1, \cdots, x_n]$ and its derivations. Then $\mathfrak{S}_n$ is defined to be the set of all derivations $A=(a_1, \cdots, a_n)$ of $\mathfrak{B}_n$ such that the divergence

$$\frac{\partial a_1}{\partial x_1} + \cdots + \frac{\partial a_n}{\partial x_n}$$

of A is zero and such that for each $i=1, \cdots, n$ and $j=0, \cdots, p-1$, the element a_i has no term in $x_i^j(x_1 \cdots x_{i-1}x_{i+1} \cdots x_n)^{p-1}$. It was proved in [2] that for any $n>2$ and any prime p, $\mathfrak{S}_n$ is a simple Lie algebra of dimension $(n-1)(p^n-1)$, and that $\mathfrak{S}_n$ is spanned by the derivations

$$D_{ij}(d) = (g_1, \cdots, g_n), \quad g_i = \frac{\partial d}{\partial x_j}, \quad g_j = -\frac{\partial d}{\partial x_i}, \quad g_k = 0 \quad (k \neq i, j), \tag{27}$$

where d is any element of $\mathfrak{B}_n$ and $i \neq j$, $i, j = 1, \cdots, n$. Then of course

$$D_{ij}(d) = -D_{ji}(d), \tag{28}$$

and we also have, for i, j, k distinct,

$$D_{jk}\left(\frac{\partial d}{\partial x_i}\right) = -D_{ij}\left(\frac{\partial d}{\partial x_k}\right) + D_{ik}\left(\frac{\partial d}{\partial x_j}\right). \tag{29}$$

In particular

$$D_{jk}(x_jx_k) = -D_{ij}(x_ix_j) + D_{ik}(x_ix_k). \tag{30}$$

We shall write

$$E_{ij}(s_1, \cdots, s_n) = D_{ij}(x_1^{s_1} \cdots x_n^{s_n}).$$

Then $\mathfrak{S}_n$ is spanned by the elements $E_{ij}(s_1, \cdots, s_n)$ with $i<j$ and $0 \leqq s_k < p$ for each s_k. From (16) and (27) we may compute that

$$\begin{aligned} &E_{ij}(s_1, \cdots, s_n)\cdot E_{ij}(t_1, \cdots, t_n) \\ &= (s_it_j - s_jt_i)E_{ij}(s_1+t_1, \cdots, s_i+t_i-1, \cdots, s_j+t_j-1, \cdots, s_n+t_n) \end{aligned} \tag{31}$$

and, for i, j, k distinct,

$$
\begin{aligned}
&E_{ij}(s_1, \cdots, s_n) \cdot E_{ik}(t_1, \cdots, t_n) \\
&\quad = s_i t_k E_{ij}(s_1 + t_1, \cdots, s_i + t_i - 1, \cdots, s_k + t_k - 1, \cdots, s_n + t_n) \\
&\quad - s_j t_i E_{ik}(s_1 + t_1, \cdots, s_i + t_i - 1, \cdots, s_j + t_j - 1, \cdots, s_n + t_n) \\
&\quad + s_i t_i E_{jk}(s_1 + t_1, \cdots, s_i + t_i - 2, \cdots, s_n + t_n).
\end{aligned} \tag{32}
$$

Using (30) we see that, for i, j, k distinct,

$$
\begin{aligned}
E_{ij}(s_1, \cdots, s_n) \cdot D_{ij}(x_i x_j) &= (s_i - s_j) E_{ij}(s_1, \cdots, s_n), \\
E_{ij}(s_1, \cdots, s_n) \cdot D_{ik}(x_i x_k) &= (s_i - s_k - 1) E_{ij}(s_1, \cdots, s_n)
\end{aligned} \tag{33}
$$

THEOREM 9. *The algebra $\mathfrak{S}_n$ is restricted.*

As we noted in the preceding section, in order to prove $\mathfrak{S}_n$ restricted it will suffice to show that it contains the (associative) pth power of each of the derivations $E_{ij}(s_1, \cdots, s_n)$. If A is a linear transformation of $\mathfrak{B}_n$ sending x_t onto a_t, then for the (associative) product of A and $E = E_{ij}(s_1, \cdots, s_n)$ we have

$$
x_t AE = a_t E = s_j x_1^{s_1} \cdots x_j^{s_j - 1} \cdots x_n^{s_n} \frac{\partial a_t}{\partial x_i} - s_i x_1^{s_1} \cdots x_i^{s_i - 1} \cdots x_n^{s_n} \frac{\partial a_t}{\partial x_j},
$$

the analogue of (23). Thus if $0 < s_k < p$ for some $k \neq i, j$, then $x_t E^p$ has x_k^p as a factor, so that $E^p = 0$ in this case. But if $E = D_{ij}(x_i^{s_i} x_j^{s_j})$, then, exactly as for the element $E(s_i, 0, s_j, 0)$ of the algebra $\mathfrak{B}_2$, we have $E^p = 0$ unless $s_i = s_j = 1$, in which case $E^p = E$. Thus $\mathfrak{S}_n$ is restricted.

In our examination of trace forms on the algebras $\mathfrak{S}_n$, we shall use the following lemma, which is itself of interest.

LEMMA 5. *Assume $\mathfrak{F}$ algebraically closed and let $\mathfrak{H}$ be the subspace of $\mathfrak{S}_n$ spanned by all elements $E_{ij}(s_1, \cdots, s_n)$ with $s_i = s_j$ and $s_k = s_i - 1$ for $k \neq i, j$, where $i, j = 1, \cdots, n$. Then $\mathfrak{H}$ is a Cartan subalgebra of $\mathfrak{S}_n$.*

For it follows from (31), (32), (28) and (29) that $\mathfrak{H}$ is abelian. Now let $\rho_2, \cdots, \rho_n$ be elements of $\mathfrak{F}$ which are linearly independent over $\mathfrak{F}_p$, and write

$$
b = \sum_{i=2}^{n} \rho_i D_{1i}(x_1 x_i).
$$

Then b is in $\mathfrak{H}$, and by (33), (28) and (30), we have

$$
E_{1j}(s_1, \cdots, s_n) \cdot b = \left\{ \rho_j(s_1 - s_j) + \sum_{k \neq 1, j} \rho_k(s_1 - s_k - 1) \right\} E_{1j}(s_1, \cdots, s_n)
$$

and, when $1 \neq i, j$,

$$
\begin{aligned}
E_{ij}(s_1, \cdots, s_n) \cdot b = \Big\{ &-\rho_i(s_i - s_1 - 1) - \rho_j(s_j - s_1 - 1) \\
&+ \sum_{k \neq 1, i, j} \rho_k(-s_i + s_1 + 1 + s_i - s_k - 1) \Big\} E_{ij}(s_1, \cdots, s_n).
\end{aligned}
$$

Now choosing a basis of $\mathfrak{S}_n$ from among the $E_{ij}(s_1, \cdots, s_n)$, we see that, for any c in $\mathfrak{S}_n$, if $(\cdots(c\cdot b)\cdots b)=0$ then $c\cdot b=0$ and c is in $\mathfrak{H}$. Hence $\mathfrak{H}$ is a Cartan subalgebra of $\mathfrak{S}_n$.

THEOREM 10. *When $n>3$ any trace form on $\mathfrak{S}_n$ is identically zero.*

We may assume that $\mathfrak{F}$ is algebraically closed. Suppose that t is a nonzero trace form on $\mathfrak{S}_n$, $n>3$. Since $\mathfrak{S}_n$ is simple, t is nondegenerate. But the restriction to a Cartan subalgebra of a nondegenerate trace form on a Lie algebra is always nondegenerate on the subalgebra. Thus for $D=D_{12}(x_1x_2)$, there must be some $E=E_{ij}(s_1, \cdots, s_n)$, with $s_i=s_j$ and $s_k=s_i-1$ for $k\neq i, j$, such that $t(D, E)\neq 0$. By (30) and (28), we may assume that $i=1$. Now since $n>3$, we may take an element $c=(0, \cdots, 1, \cdots, 0)$ with 1 in the kth place, $k\neq 1, 2, j$. Then for the right multiplication R_c we have $D_{12}(x_1x_2x_k^{p-1})(R_c)^{p-1}=-D$, while $E(-R_c)^{p-1}=0$ since $s_k=s_1-1<p-1$. But by $p-1$ applications of (11), we have $t(D, E)=t\{-D_{12}(x_1x_2x_k^{p-1}), E(R_c)^{p-1}\}=0$, a contradiction, and the theorem is proved.

We now consider the remaining case, $n=3$. Here we shall write, for i, j, k distinct,

$$e_{ij}(\alpha) = e_{ij}(\alpha_i, \alpha_j, \alpha_k) = E_{ij}(s_1, s_2, s_3),$$

where

$$\alpha_l = s_l \qquad (\alpha_l = 0, \cdots, p-1; l = 1, 2, 3).$$

We define a symmetric bilinear form t on $\mathfrak{S}_3$ in terms of the values of the form for the elements $e_{ij}(\alpha)$ by setting

$$(34)\quad t\{e_{ij}(\alpha), e_{ik}(p-\alpha_i, p-\alpha_k-1, p-\alpha_j-1)\} = \alpha_i, \qquad (i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2),$$

and letting t vanish on other pairs of elements $e_{ij}(\alpha)$, except of course those for which t is defined through (34) by the use of (28) and symmetry of the form.

We note that a basis of $\mathfrak{S}_3$ is given by all $e_{12}(\alpha)$, $e_{13}(\beta)$, $e_{23}(\gamma)$ such that α_1 or α_2 is nonzero, $\beta_1\neq 0$ or $\beta_2=p-1$, and $\gamma_1=p-1$ and γ_2 or γ_3 is nonzero. Then in order to show that the effect of t for an $e_{ij}(\alpha)$ is the same as its effect for the linear combination of elements in our basis which equals $e_{ij}(\alpha)$, it suffices to show that the expressions

$$\sum_{(q,r)=(1,2),(2,3),(3,1)} \alpha_s t\{e_{qr}(\alpha_q, \alpha_r, \alpha_s-1), e_{ij}(\beta)\}$$

always vanish, and this follows from (34), each term vanishing unless $\alpha_i+\beta_i=\alpha_j+\beta_j=\alpha_k+\beta_k+1=p$. Hence t is well-defined.

THEOREM 11. *The form t is a nondegenerate trace form on $\mathfrak{S}_3$.*

We need to verify (11) for the elements $e_{ij}(\alpha)$. By (28) and the symmetry

of the form, it is enough to consider the following three types of substitutions for a, b, c. First, when

$$a = e_{ij}(\alpha), \qquad b = e_{ij}(\beta), \qquad c = e_{ij}(\gamma),$$

we use (31), and obtain $t(a\cdot b, c)=0=t(a, b\cdot c)$. Next, when

$$a = e_{ij}(\alpha), \qquad b = e_{ij}(\beta), \qquad c = e_{ik}(\gamma),$$

we have

$$t(a\cdot b, c) = (\alpha_i\beta_j - \alpha_j\beta_i)t\{e_{ij}(\alpha_i + \beta_i - 1, \alpha_j + \beta_j - 1, \alpha_k + \beta_k), e_{ik}(\gamma)\}$$

and, by (32),

$$t(a, b\cdot c) = t\{e_{ij}(\alpha), -\beta_j\gamma_i e_{ik}(\beta_i + \gamma_i - 1, \beta_k + \gamma_k, \beta_j + \gamma_j - 1) + \beta_i\gamma_i e_{jk}(\beta_j + \gamma_j, \beta_k + \gamma_k, \beta_i + \gamma_i - 2)\},$$

so that $t(a\cdot b, c)=0=t(a, b\cdot c)$ unless $\alpha_i+\beta_i+\gamma_i-1=\alpha_j+\beta_j+\gamma_j=\alpha_k+\beta_k+\gamma_k+1=p$, in which case $t(a\cdot b, c)=(\alpha_i\beta_j-\alpha_j\beta_i)(-\gamma_i)=(-\beta_j\gamma_i)\alpha_i+(\beta_i\gamma_i)\alpha_j=t(a, b\cdot c)$. Finally, when

$$a = e_{ij}(\alpha), \qquad b = e_{ik}(\beta), \qquad c = e_{jk}(\gamma),$$

we have

$$t(a\cdot b, c) = t\{\alpha_i\beta_k e_{ij}(\alpha_i + \beta_i - 1, \alpha_j + \beta_j, \alpha_k + \beta_k - 1) - \alpha_j\beta_i e_{ik}(\alpha_i + \beta_i - 1, \alpha_k + \beta_k, \alpha_j + \beta_j - 1), e_{jk}(\gamma)\}$$

and

$$t(a, b\cdot c) = t\{e_{ij}(\alpha), -\beta_k\gamma_j e_{ik}(\beta_i + \gamma_i, \beta_k + \gamma_k - 1, \beta_j + \gamma_j - 1) + \beta_i\gamma_k e_{jk}(\beta_j + \gamma_j, \beta_k + \gamma_k - 1, \beta_i + \gamma_i - 1)\}$$

so that $t(a\cdot b, c)=0=t(a, b\cdot c)$ unless $\alpha_i+\beta_i+\gamma_i=\alpha_j+\beta_j+\gamma_j=\alpha_k+\beta_k+\gamma_k=p$, in which case $t(a\cdot b, c)=(\alpha_i\beta_k)(-\gamma_j)+(-\alpha_j\beta_i)(-\gamma_k)=(-\beta_k\gamma_j)\alpha_i+(\beta_i\gamma_k)\alpha_j=t(a, b\cdot c)$. Hence t is a trace form and, since $\mathfrak{S}_3$ is simple and t is not identically zero, t is nondegenerate.

We turn now to the algebra $\mathfrak{T}_n$. This is defined to be the set of all derivations $(a_1, \cdots, a_n)$ of $\mathfrak{B}_n$ for which the divergence equals the coordinate sum, that is, for which

$$\frac{\partial a_1}{\partial x_1} + \cdots + \frac{\partial a_n}{\partial x_n} = a_1 + \cdots + a_n.$$

It was proved in [1] that for every $n>2$ and $p>2$, $\mathfrak{T}_n$ is a simple Lie algebra of dimension $(n-1)p^n$ over $\mathfrak{F}$.

THEOREM 12. *The algebra $\mathfrak{T}_n$ is not restricted.*

For suppose that $\mathfrak{T}_n$ were restricted, with $A=(a_1, \cdots, a_n)$ the (restricted)

pth power in $\mathfrak{T}_n$ of the derivation $(x_1, 1-x_1, 0, \cdots, 0)$. A simple computation shows that the ordinary (associative) pth power of $(x_1, 1-x_1, 0, \cdots, 0)$ is the derivation $(x_1, -x_1, 0, \cdots, 0)$ of $\mathfrak{B}_n$. Hence for every element $B = (b_1, \cdots, b_n)$ of $\mathfrak{T}_n$, we must have $B \cdot A = B \cdot (x_1, -x_1, 0, \cdots, 0)$, that is,

$$\sum_{i=1}^{n} \left(\frac{\partial b_j}{\partial x_i} a_i - \frac{\partial a_j}{\partial x_i} b_i \right) = \frac{\partial b_j}{\partial x_1} x_1 - \frac{\partial b_j}{\partial x_2} x_1 + \xi_j b_1 \qquad (j = 1, \cdots, n), \tag{35}$$

where $\xi_1 = -1$, $\xi_2 = 1$ and $\xi_3 = \cdots = \xi_n = 0$. First taking $B = (1, -1, 0, \cdots, 0)$, we have

$$-\frac{\partial a_j}{\partial x_1} + \frac{\partial a_j}{\partial x_2} = \xi_j \qquad (j = 1, \cdots, n). \tag{36}$$

Then with $B = (x_1, 1-x_1, 0, \cdots, 0)$, so that $B \cdot A = 0$, we have

$$-\xi_j a_1 - \frac{\partial a_j}{\partial x_1} x_1 - \frac{\partial a_j}{\partial x_2} + \frac{\partial a_j}{\partial x_2} x_1 = -\xi_j (a_1 - x_1) - \frac{\partial a_j}{\partial x_2} = 0, \tag{37}$$

$$(j = 1, \cdots, n).$$

Taking $j = 1$ in (37) we see that

$$a_1 = x_1. \tag{38}$$

Now with $B = (1-x_2, x_2, 0, \cdots, 0)$ we use (38) and (35) for $j = 1$ to obtain $-a_2 - (1-x_2) = x_1 - (1-x_2)$, that is, $a_2 = -x_1$.

We next take $k > 2$. It follows from (37) and (36) that $\partial a_k/\partial x_1 = \partial a_k/\partial x_2 = 0$. Hence using $B = (1-x_k, 0, \cdots, x_k, \cdots, 0)$, where $b_k = x_k$, we obtain, from the case $j = k$ of (35),

$$a_k - \frac{\partial a_k}{\partial x_k} x_k = 0. \tag{39}$$

Finally, taking $B = (0, 1, 0, \cdots, -1, \cdots, 0)$, where $b_k = -1$, we get $\partial a_k/\partial x_k = 0$, which in combination with (39) shows that $a_k = 0$. Hence $A = (x_1, -x_1, 0, \cdots, 0)$, which is not in $\mathfrak{T}_n$, a contradiction.

7. **The derivation algebra of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ and criteria for nonisomorphism.** Let D be a derivation of the simple Lie algebra $\mathfrak{L}(\mathfrak{G}, \delta, f)$ and let $c(\alpha, \gamma)$ be the coefficient of $v_{\alpha+\gamma}$ in $v_\alpha D$, so that

$$D: v_\alpha \to \sum_{\gamma \in \mathfrak{G}} c(\alpha, \gamma) v_{\alpha+\gamma} = \sum_{\gamma \in \mathfrak{G}} c(\alpha, -\alpha + \gamma) v_\gamma, \tag{40}$$

where we may set

$$c(\alpha, -\alpha) = c(\alpha, -\alpha - \delta) = 0 \tag{41}$$

for every α in $\mathfrak{G}$. Since D is a derivation, we have $(v_\alpha v_\beta)D = (v_\alpha D)v_\beta + v_\alpha(v_\beta D)$ for every α, β in $\mathfrak{G}$ with $\alpha, \beta \neq -\delta$. Thus

$$(42)\quad \sum_{\gamma\in G}\sum_{i=0}^{m}\{f(\alpha_i,\beta_i)c[\alpha+\beta-\delta_i,\ -(\alpha+\beta-\delta_i)+\gamma] - f(\gamma_i+\delta_i,\beta_i)c(\alpha,\ -\alpha+\gamma-\beta+\delta_i)-f(\alpha_i,\gamma_i+\delta_i)c(\beta,\ -\beta+\gamma-\alpha+\delta_i)\}v_\gamma=0.$$

Take ϵ such that $\gamma=\alpha+\beta+\epsilon\neq 0$. Then (42) gives

$$(43)\quad \sum_{i=0}^{m}\{f(\alpha_i,\beta_i)c(\alpha+\beta-\delta_i,\epsilon+\delta_i)-f(\alpha_i+\epsilon_i+\delta_i,\beta_i)c(\alpha,\epsilon+\delta_i) - f(\alpha_i,\beta_i+\epsilon_i+\delta_i)c(\beta,\epsilon+\delta_i)\}=0.$$

Conversely, if the linear transformation D of $\mathfrak{L}(\mathfrak{G},\delta,f)$ satisfies (43) for every $\alpha,\beta\neq-\delta$ and every ϵ such that $\alpha+\beta+\epsilon\neq 0$, then it satisfies (42) and is a derivation.

We shall use $R_\alpha=R(\alpha)$ to denote right multiplication on $\mathfrak{L}(\mathfrak{G},\delta,f)$ by the element v_α with α in $\mathfrak{G}$. Since right multiplication by $v_{-\delta}$ is a derivation on the algebra $\mathfrak{L}'=\mathfrak{L}-\mathfrak{F}u_0$, where $\mathfrak{L}$ is defined by (1) through (5), and since $(\mathfrak{L}')^2\subseteq\mathfrak{L}(\mathfrak{G},\delta,f)$, it follows that $R_{-\delta}$ is a derivation of $\mathfrak{L}(\mathfrak{G},\delta,f)$. We shall call any linear combination of the R_α an *extended inner derivation* of $\mathfrak{L}(\mathfrak{G},\delta,f)$.

For any k and any γ_k in $\mathfrak{G}_k$, define a linear transformation $D(\gamma_k,-\delta_k)$ of $\mathfrak{L}(\mathfrak{G},\delta,f)$ by setting

$$(44)\qquad v_\alpha D(\gamma_k,-\delta_k)=f(\alpha_k,\gamma_k)v(\alpha-\delta_k).$$

LEMMA 6. *The mappings $D(\gamma_k,-\delta_k)$ are derivations of $\mathfrak{L}(\mathfrak{G},\delta,f)$.*

We have $c(\alpha,\epsilon+\delta_i)=0$ for $D(\gamma_k,-\delta_k)$ unless $\epsilon=-\delta_i-\delta_k$ for some i. When $\epsilon=-\delta_i-\delta_k$, the left hand side of (43) equals

$$\begin{aligned}f(\alpha_i,\beta_i)f(\alpha_k+\beta_k-\delta_i,\gamma_k)-f(\alpha_i-\delta_k,\beta_i)f(\alpha_k,\gamma_k)-f(\alpha_i,\beta_i-\delta_k)f(\beta_k,\gamma_k)\\ =f(\alpha_i,\beta_i)[f(\alpha_k+\beta_k,\gamma_k)-f(\alpha_k,\gamma_k)-f(\beta_k,\gamma_k)]\\ +[f(\alpha_i,\beta_i)f(\gamma_k,\delta_i)+f(\gamma_k,\alpha_k)f(\beta_i,\delta_k)+f(\beta_k,\gamma_k)f(\alpha_i,\delta_k)],\end{aligned}$$

which clearly equals zero when $i\neq k$, and (7) gives the desired result when $i=k$.

Now let $\sigma_{01},\cdots,\sigma_{0r_0}$ be a basis of $\mathfrak{G}_0$ over $\mathfrak{F}_p$ and $\sigma_{i1},\cdots,\sigma_{ir_i}$, δ_i a basis of $\mathfrak{G}_i$ over $\mathfrak{F}_p$ such that $f(\sigma_{i1},\delta_i)\neq 0$, $i=1,\cdots,m$. Denote by $s_{ij}(\alpha)$ the coefficient of σ_{ij} in α, for $i=0,\cdots,m$, and by $s_i(\alpha)$ the coefficient of δ_i in α, for $i=1,\cdots,m$. Define linear transformations $D(\delta,0)$ and $D(\sigma_{ij},0)$ of $\mathfrak{L}(\mathfrak{G},\delta,f)$ by setting

$$(45)\qquad v_\alpha D(\delta,0)=\left[-1+\sum_{i=1}^{m}s_i(\alpha)\right]v_\alpha$$

if $\mathfrak{G}_0=\mathbf{0}$, $D(\delta,0)=0$ if $\mathfrak{G}_0\neq 0$, and

$$(46)\qquad v_\alpha D(\sigma_{ij},0)=s_{ij}(\alpha)v_\alpha,$$

where these definitions of course depend on the particular bases chosen for the $\mathfrak{G}_k$.

LEMMA 7. *The mappings* $D(\delta, 0)$ *and* $D(\sigma_{ij}, 0)$ *are derivations of* $\mathfrak{L}(\mathfrak{G}, \delta, f)$.

For each of these mappings we have $c(\alpha, \epsilon+\delta_k)=0$ unless $\epsilon=-\delta_k$. When considering $D(\delta, 0)$ we may suppose that $\mathfrak{G}_0=0$. Then with $\epsilon=-\delta_k$, (43) reduces to

$$f(\alpha_k, \beta_k)\left\{\left[-2+\sum_{i=1}^{m} s_i(\alpha+\beta)\right]-\left[-1+\sum_{i=1}^{m} s_i(\alpha)\right]-\left[-1+\sum_{i=1}^{m} s_i(\beta)\right]\right\}=0,$$

which clearly holds. Next consider $D(\sigma_{ij}, 0)$. Then with $\epsilon=-\delta_k$, (43) reduces to $f(\alpha_k, \beta_k)\{s_{ij}(\alpha+\beta)-s_{ij}(\alpha)-s_{ij}(\beta)\}=0$, which also holds.

We now begin showing that when $p>3$ the derivations discussed in Lemmas 6 and 7, together with the extended inner derivations, span the algebra of derivations of $\mathfrak{L}(\mathfrak{G}, \delta, f)$. We shall henceforth assume that $p>3$ except when explicitly otherwise stated.

We shall also henceforth assume that, for any element γ in $\mathfrak{G}$, if we use some coefficient $c(\gamma, \zeta)$ (not multiplied by a factor which equals zero) then $\gamma\neq-\delta$. Then in every case in which we shall apply (43) for which it could happen that α or β was equal to $-\delta$, it will be possible, by a trivial modification of the proof, to take α and β such that neither equals $-\delta$. We shall make no further mention of this in applying (43) in the following proofs.

LEMMA 8. *Suppose that* $\alpha_j\in\mathfrak{G}_j$ *and* $\beta_k\in\mathfrak{G}_k$, $j\neq k$. *Then for any element* θ *of* $\mathfrak{G}$ *we have*

$$f(\beta_k, \theta_k)c(\alpha_j, \theta-\delta_j)=f(\alpha_j, \theta_j)c(\beta_k, \theta-\delta_k). \tag{47}$$

For if $\alpha_j+\beta_k+\theta-\delta_j-\delta_k\neq0$ then (43) with $\epsilon=\theta-\delta_j-\delta_k$ gives (47). Now consider the case $\alpha_j+\beta_k+\theta-\delta_j-\delta_k=0$. If $0\neq\theta_j, \theta_k$ then using (47) for the previous case we have $f(\beta_k, \theta_k)c(\alpha_j, \theta-\delta_j)=f(\alpha_j, \theta_j)c(\beta_k+\theta_k, \theta-\delta_k)$ $=f(\beta_k, \theta_k)c(\alpha_j+\theta_j, \theta-\delta_j)=f(\alpha_j, \theta_j)c(\beta_k, \theta-\delta_k)$, while if say $f(\alpha_j, \theta_j)=0$ and $f(\beta_k, \theta_k)\neq0$ then both sides of (47) vanish since $c(\alpha_j, \theta-\delta_j)=f(\alpha_j, \theta_j)[f(\beta_k, \theta_k)]^{-1}\cdot c(\beta_k+\theta_k, \theta-\delta_k)=0$, and the lemma is proved.

LEMMA 9. *If* α_j, β_j *are in* $\mathfrak{G}_j$ *and if the component* θ_i *of* θ *is nonzero for some* $i\neq j$ *then*

$$f(\beta_j, \theta_j)c(\alpha_j, \theta-\delta_j)=f(\alpha_j, \theta_j)c(\beta_j, \theta-\delta_j). \tag{48}$$

For with γ_i such that $f(\gamma_i, \theta_i)\neq0$, Lemma 8 implies that

$$\begin{aligned} f(\beta_j, \theta_j)c(\alpha_j, \theta-\delta_j) &= f(\beta_j, \theta_j)f(\alpha_j, \theta_j)[f(\gamma_i, \theta_i)]^{-1}c(\gamma_i, \theta-\delta_i) \\ &= f(\alpha_j, \theta_j)c(\beta_j, \theta-\delta_j). \end{aligned}$$

All elements of $\mathfrak{G}$ occurring in the proofs of the next three lemmas are in $\mathfrak{G}_j$. We shall drop the subscript j, write c_α for $c(\alpha, \theta-\delta_j)$ and take $\epsilon=\theta-2\delta_j$ in these three proofs.

LEMMA 10. *If α_j, β_j and θ are in $\mathfrak{G}_j$ and $f(\theta_j, \delta_j)\neq 0$ then* (48) *holds, provided that $\alpha_j+\theta-\delta_j$ and $\beta_j+\theta-\delta_j$ are nonzero.*

For (43) implies that $f(\alpha, \delta)c_\alpha - f(\alpha+\theta, \delta)c_\alpha - f(\alpha, \theta)c_\delta = 0$, that is, $f(\delta, \theta)c_\alpha = f(\alpha, \theta)c_\delta$, and similarly $f(\delta, \theta)c_\beta = f(\beta, \theta)c_\delta$. Thus $f(\beta, \theta)c_\alpha = f(\beta, \theta)[f(\delta, \theta)]^{-1} \cdot f(\alpha, \theta)c_\delta = f(\alpha, \theta)c_\beta$, and the lemma is proved.

LEMMA 11. *Suppose that α_j, β_j and θ are in $\mathfrak{G}_j$, $j\neq 0$, and that $f(\theta, \delta_j)=0$ and $\theta\neq\delta_j$, that is, $g_j(\theta)=0$ and $h_j(\theta)\neq h_j(\delta_j)$. Then* (48) *holds.*

We may suppose that $\theta\neq 0$ since otherwise both sides of (48) vanish. We shall first show that

$$c_\gamma = c_{\gamma+\delta} \tag{49}$$

for every γ. Suppose that $g(\gamma)\neq 0$. If t is an integer such that $t\not\equiv -1 \pmod p$ then $\gamma+t\gamma+(\theta-2\delta)\neq 0$ and (43) gives $f(t\gamma, \theta-\delta)c_\gamma = f(\gamma, \theta-\delta)c_{t\gamma}$. Since $f(\gamma, \theta-\delta) = g(\gamma)h(\theta-\delta)\neq 0$, we have $c_{t\gamma}=tc_\gamma$. Now with s such that $2s \equiv 1 \pmod p$, we have $c_{-\gamma}=2c_{-s\gamma}=-2sc_\gamma=-c_\gamma$. Since $\gamma+(-\gamma+\delta)+\epsilon=\theta-\delta \neq 0$ and $c_{\gamma-\gamma+\delta-\delta}=c_0=0$, we have, by (43), $f(-\gamma+\delta, \gamma+\theta-\delta)c_\gamma = f(\gamma, -\gamma+\theta)c_{-\gamma+\delta}$, that is, $c_\gamma=-c_{-\gamma+\delta}$, and hence $c_{\gamma+\delta}=-c_{-\gamma}=c_\gamma$. Thus (49) holds for any γ such that $g(\gamma)\neq 0$.

Now suppose that $\gamma\neq 0$ and $g(\gamma)=0$, so that $h(\gamma)\neq 0$, and choose η such that $g(\eta)\neq 0$. Since $\eta+\gamma+\epsilon\neq 0$, we have $f(\eta,\gamma)c_{\eta+\gamma-\delta} = f(\eta+\theta-\delta,\gamma)c_\eta + f(\eta, \gamma+\theta-\delta)c_\gamma$, which reduces to

$$c_{\eta+\gamma} = c_\eta + [h(\gamma)]^{-1}h(\gamma+\theta-\delta)c_\gamma. \tag{50}$$

Iterating this we obtain $c_{\eta+t\gamma}=c_\eta+t[h(\gamma)]^{-1}h(\gamma+\theta-\delta)c_\gamma$, while substituting $t\gamma$ for γ in (50) we obtain $c_{\eta+t\gamma} = c_\eta + [h(t\gamma)]^{-1}h(t\gamma+\theta-\delta)c_{t\gamma}$. Hence $h(t\gamma+\theta-\delta)c_{t\gamma}=t^2h(\gamma+\theta-\delta)c_\gamma$, and it follows, using (41), that, for $t \not\equiv 0 \pmod p$, $c_{t\gamma}=0$ if and only if $c_\gamma=0$. If $c_\gamma\neq 0$ then $-\eta+(\eta+\gamma+\delta)+\epsilon = \gamma+\theta-\delta\neq 0$ and, by (43), $f(-\eta, \eta+\gamma+\delta)c_\gamma = f(-\eta+\theta-\delta, \eta+\gamma+\delta)c_{-\eta} + f(-\eta, \eta+\gamma+\theta)c_{\eta+\gamma+\delta}$, that is, $f(-\eta, \gamma+\delta)c_\gamma = f(-\eta, \gamma+\theta)c_{-\eta} + f(-\eta, \gamma+\theta) \cdot \{c_\eta + [h(\gamma)]^{-1}h(\gamma+\theta-\delta)c_\gamma\}$, whence $h(\gamma)h(\gamma+\delta) = h(\gamma+\theta)h(\gamma+\theta-\delta)$ and, by expanding,

$$2h(\gamma)[h(\delta) - h(\theta)] = h(\theta)[h(\theta) - h(\delta)]. \tag{51}$$

But when $c_\gamma\neq 0$ then $c_{2\gamma}\neq 0$ also and we may substitute 2γ for γ in (51) and obtain $4h(\gamma)[h(\delta)-h(\theta)] = 2h(\gamma)[h(\delta)-h(\theta)]$, $h(\delta)=h(\theta)$, $\theta=\delta$, a contradiction. Hence $c_\gamma=0=c_{\gamma+\delta}$ and (49) holds for any γ.

If $\alpha+\beta+\epsilon=0$ then $\beta=-\alpha-\theta-2\delta$ and either $g(\alpha)=g(\beta)=0$ and $c_\alpha=c_\beta=0$ or $g(\alpha)\neq 0$ and, by (50), $c_\beta=-c_\alpha$, $f(\beta, \theta)=-f(\alpha, \theta)$ and (48) holds. Similarly

(48) holds when $(\alpha+\delta)+\beta+\epsilon=0$. Now we may use (43) to obtain both $f(\alpha, \beta)c_{\alpha+\beta-\delta} = f(\alpha + \theta - \delta, \beta)c_\alpha + f(\alpha, \beta + \theta - \delta)c_\beta$ and $f(\alpha + \delta, \beta)c_{\alpha+\beta} = f(\alpha+\theta, \beta)c_{\alpha+\delta}+f(\alpha+\delta, \beta+\theta-\delta)c_\beta$, whence, by applying (49) and subtracting,

$$f(\beta, \delta)c_{\alpha+\beta} = f(\beta, \delta)c_\alpha + f(\beta, \delta)c_\beta. \tag{52}$$

If $f(\beta, \delta)=0$ then $g(\beta)=0$, $f(\beta, \theta)=0$, $c_\beta=0$ and (48) holds, while if $f(\beta, \delta)\neq 0$, then (52) gives $c_{\alpha+\beta}=c_\alpha+c_\beta$, which with (43) and (49) gives

$$f(\beta, \theta - \delta)c_\alpha = f(\alpha, \theta - \delta)c_\beta. \tag{53}$$

Multiplying both sides of (53) by $h(\theta)[h(\theta-\delta)]^{-1}$, we obtain (48), and the lemma is proved.

LEMMA 12. *Formula* (48) *holds when* $j=0$ *and* α_0, β_0 *and* θ *are in* $\mathfrak{G}_0$.

In this proof we again drop the subscripts $j=0$ and denote $c(\alpha, \theta)$ by c_α. We may assume $\theta\neq 0$. We shall first show that

$$c_{t\gamma} = tc_\gamma \tag{54}$$

for any γ and any integer t. If $f(\gamma, \theta)\neq 0$ then $\gamma+t\gamma+\theta\neq 0$ and, by (43), $f(\gamma+\theta, t\gamma)c_\gamma+f(\gamma, t\gamma+\theta)c_{t\gamma}=0$, so that (54) holds for such γ. For any η such that $f(\eta, \theta)\neq 0$, we have $\eta-\theta+\theta\neq 0$, so that (43) gives $f(\eta, -\theta)c_{\eta-\theta}=f(\eta, -\theta)c_\eta$, $c_{\eta-\theta}=c_\eta$ and, by iteration, $c_{\eta+t\theta}=c_\eta$ for any integer t. On the other hand, $\eta+t\theta+\theta\neq 0$, and (43) gives $f(\eta, t\theta)c_{\eta+t\theta}=f(\eta, t\theta)c_\eta+f(\eta, t\theta+\theta)c_{t\theta}$, so that $c_{t\theta}=0$ for $t\not\equiv -1 \pmod p$, while $c_{-\theta}=0$ by (41). Thus (54) holds for γ a multiple of θ.

Now suppose that $f(\gamma, \theta)=0$ and γ is not a multiple of θ. By the non-degeneracy of f, we may choose η such that

$$0 \neq f(\eta, \theta), f(\eta, 2\gamma + \theta). \tag{55}$$

Suppose that $c_\gamma\neq 0$. Since $\eta+\gamma+\theta\neq 0$, (43) gives $f(\eta, \gamma)c_{\eta+\gamma}=f(\eta+\theta, \gamma)c_\eta+f(\eta, \gamma+\theta)c_\gamma$. But then $f(\eta, \gamma)\neq 0$, since otherwise we would have $f(\eta, \gamma+\theta)=f(\eta, \theta)\neq 0$ and $c_\gamma=0$. Thus we have

$$c_{\eta+\gamma} = c_\eta + [f(\eta, \gamma)]^{-1}f(\eta, \gamma + \theta)c_\gamma. \tag{56}$$

Then since $-\eta + (\eta + \gamma) + \theta \neq 0$, (43) and (56) give $f(-\eta, \eta+\gamma)c_\gamma=f(-\eta+\theta, \eta+\gamma)c_{-\eta}+f(-\eta, \eta+\gamma+\theta)c_{\eta+\gamma}=f(-\eta, \gamma+\theta)c_{-\eta}+f(-\eta, \gamma+\theta)c_\eta+f(-\eta, \gamma+\theta)[f(\eta, \gamma)]^{-1}f(\eta, \gamma+\theta)c_\gamma$, whence $f(\eta, \gamma)f(-\eta, \gamma)=f(-\eta, \gamma+\theta)\cdot f(\eta, \gamma+\theta)$, and $0=f(\eta, \theta)[2f(\eta, \gamma)+f(\eta, \theta)]=f(\eta, \theta)f(\eta, 2\gamma+\theta)$, which contradicts (55). Hence $c_\gamma=0=c_{t\gamma}$, so that (54) is true.

Now if $\alpha+\beta+\theta=0$ then $\beta=-\alpha-\theta$, $c_\beta=c_{-\alpha-\theta}=c_{-\alpha}=-c_\alpha$, $f(\beta, \theta)=-f(\alpha, \theta)$ and (48) holds. Similarly (48) holds if $2\alpha+2\beta+\theta=0$, so we may assume that $0\neq\alpha+\beta+\theta$, $2\alpha+2\beta+\theta$. Then (43) gives $f(\alpha, \beta)c_{\alpha+\beta}=f(\alpha+\theta, \beta)c_\alpha+f(\alpha, \beta+\theta)c_\beta$ and $f(2\alpha, 2\beta)c_{2\alpha+2\beta}=f(2\alpha+\theta, 2\beta)c_{2\alpha}+f(2\alpha, 2\beta+\theta)c_{2\beta}$, whence, by applying (55) and subtracting, we get $f(\theta, 2\beta)c_{2\alpha}+f(2\alpha, \theta)c_{2\beta}=0$, which gives (48), and the lemma is proved.

LEMMA 13. *The derivation D differs by an extended inner derivation from a derivation for which $c(\beta_k, \zeta)=0$ for every k and β_k in $\mathfrak{G}_k$ and every $\zeta \neq 0, -\delta_k$.*

Indeed if $\theta \neq 0, \delta_1, \cdots, \delta_m$, choose j and α_j in $\mathfrak{G}_j$ such that $f(\alpha_j, \theta_j) \neq 0$ and $\alpha_j+\theta-\delta_j \neq 0$, and define

$$k_\theta = [f(\alpha_j, \theta_j)]^{-1} c(\alpha_j, \theta - \delta_j). \tag{57}$$

Then k_θ is well defined by (57) since Lemmas 8 through 12 proved that (47) holds unless $j=k>0$ and either $\theta=\delta_j$ or $\alpha_j+\theta-\delta_j=0$ or $\beta_j+\theta-\delta_j=0$. We also set $k_\theta=0$ for $\theta=0, \delta_1, \cdots, \delta_m$. Now consider the extended inner derivation R of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ induced by right multiplication by $\sum_\theta k_\theta v_\theta$. For β_k in $\mathfrak{G}_k$, R maps $v(\beta_k)$ onto $\sum_\theta f(\beta_k, \theta_k) k_\theta v(\beta_k+\theta-\delta_k) = \sum_{\theta \neq \delta_0, \ldots, \delta_m} c(\beta_k, \theta-\delta_k) \cdot v(\beta_k+\theta-\delta_k)$. Hence the derivation $D-R$ has $c(\beta_k, \theta-\delta_k)=0$ for $\theta \neq 0, \delta_1, \cdots, \delta_m$, that is, $c(\beta_k, \zeta)=0$ for $\zeta \neq -\delta_k, \delta_1-\delta_k, \cdots, \delta_m-\delta_k$. But if $\zeta=\delta_j-\delta_k$ for $j \neq 0, k$, then with α_j in $\mathfrak{G}_j$ such that $f(\alpha_j, \delta_j) \neq 0$ we have $\alpha_j+\beta_k+(-\delta_k) \neq 0$ and, by (43), $f(\alpha_j, \delta_j) c(\beta_k, \zeta)=0$, and the lemma is proved.

Recall that in selecting a basis of $\mathfrak{G}_k$ over $\mathfrak{F}_p$ we chose σ_{k1} such that $f(\sigma_{k1}, \delta_k) \neq 0$, $k=1, \cdots, m$. We shall write $\sigma_{k1}=\sigma_k$ and $f(\sigma_k, \delta_k)=a_k$.

LEMMA 14. *The derivation D differs by*

$$\sum_{k=1}^{m} (a_k)^{-1} \{ c(\sigma_k, -\delta_k) D(\delta_k, -\delta_k) - c(2\delta_k, -\delta_k) D(\sigma_k, -\delta_k)/2 \}$$

from a derivation for which $c(\alpha_k, -\delta_k)=0$ for every $k \neq 0$ and α_k in $\mathfrak{G}_k$.

By the definition of $D(\gamma_k, -\delta_k)$ in (44), the conclusion of the lemma is equivalent to the statement that, for the coefficients $c(\alpha, \beta)$ determined by D,

$$c(\alpha_k, -\delta_k) = (a_k)^{-1} \{ c(\sigma_k, -\delta_k) f(\alpha_k, \delta_k) - c(2\delta_k, -\delta_k) f(\gamma_k, \sigma_k)/2 \} \tag{58}$$

for every $k \neq 0$ and $\alpha_k \neq \delta_k$ in $\mathfrak{G}_k$. All elements of $\mathfrak{G}$ occurring henceforth in the proof of this lemma are in $\mathfrak{G}_k$, and we shall drop the subscripts k and denote $c(\alpha, -\delta_k)$ by c_α. By (43) we have

$$f(\beta, \gamma) c_{\beta+\gamma-\delta} = f(\beta-\delta, \gamma) c_\beta + f(\beta, \gamma-\delta) c_\gamma, \tag{59}$$

provided $\beta+\gamma+(-2\delta) \neq 0$. If $f(\gamma, \delta) \neq 0$ then for any integer t we have $\gamma+t\gamma+(-2\delta) \neq 0$ and $f(-\delta, t\gamma) c_\gamma + f(\gamma, -\delta) c_{t\gamma}=0$, that is,

$$c_{t\gamma} = t c_\gamma. \tag{60}$$

Also when $f(\gamma, \delta) \neq 0$ we have $\gamma+2\delta+(-2\delta) \neq 0$, $f(\gamma, 2\delta) c_{\gamma+\delta} = f(\gamma, 2\delta) c_\gamma + f(\gamma, \delta) c_{2\delta}$, $c_{\gamma+\delta} = c_\gamma + c_{2\delta}/2$ and, by iteration,

$$c_{\gamma+t\delta} = c_\gamma + t c_{2\delta}/2. \tag{61}$$

If $\alpha=-\sigma+\delta$ or $-\sigma+2\delta$, then (61) and (60) give (58), so we may assume that $\alpha \neq -\sigma+\delta, -\sigma+2\delta, \delta$. Then $\alpha+(\sigma+\delta)+(-2\delta) \neq 0$, and, by (59) and (61), we have

(62) $f(\alpha, \sigma+\delta)c_{\alpha+\sigma} = f(\alpha-\delta, \sigma+\delta)c_\alpha + f(\alpha, \sigma)c_\sigma + f(\alpha, \sigma)c_{2\delta}/2.$

Now if $f(\alpha,\delta)=0$, we have $(\alpha+\sigma)+(-\sigma+\delta)+(-2\delta)=\alpha-\delta\neq 0$ and $f(\alpha+\sigma, -\sigma+\delta)c_\alpha = f(\alpha, -\sigma)c_{\alpha+\sigma}+f(\alpha, -\sigma)c_{-\sigma+\delta}$, that is, by (62), (61) and (60), $-f(\alpha+\delta,\sigma)c_\alpha = -f(\alpha-\delta,\sigma)c_\alpha - f(\alpha,\sigma)c_\sigma - f(\alpha,\sigma)c_{2\delta}/2 + f(\alpha,\sigma)c_\sigma - f(\alpha, \sigma)c_{2\delta}/2$, whence $2f(\delta, \sigma)c_\alpha = f(\alpha, \sigma)c_{2\delta}$, which gives (58) for the case $f(\alpha, \delta)=0$. In particular it follows that (61) holds even when $f(\gamma, \delta)=0$.

Now $\alpha+\sigma+(-2\delta)\neq 0$ and, by (61) and (59), $f(\alpha, \sigma)c_{\alpha+\sigma} - f(\alpha, \sigma)c_{2\delta}/2 = f(\alpha, \sigma)c_{\alpha+\sigma-\delta} = f(\alpha-\delta, \sigma)c_\alpha + f(\alpha, \sigma-\delta)c_\sigma$, that is, $f(\alpha, \sigma)c_{\alpha+\sigma} = f(\alpha-\delta, \sigma)c_\alpha + f(\alpha, \sigma-\delta)c_\sigma + f(\alpha, \sigma)c_{2\delta}/2$, which, subtracted from (62), gives $f(\alpha, \delta)c_{\alpha+\sigma} = f(\alpha, \delta)c_\alpha + f(\alpha, \delta)c_\sigma$. Thus if $f(\alpha, \delta)\neq 0$, then $c_{\alpha+\sigma} = c_\alpha + c_\sigma$, which, substituted in (62), gives (58), and the lemma is proved.

LEMMA 15. *Suppose that $c(\alpha_k, \zeta)=0$ for every k, α_k in $\mathfrak{G}_k$ and nonzero ζ. Then $c(\alpha, \zeta)=0$ for every α and nonzero ζ.*

For suppose that $c(\alpha, \zeta)\neq 0$ for some α and nonzero ζ. Thus also $\alpha+\zeta\neq 0$. If $\alpha+\alpha_i+(\zeta-\delta_i)\neq 0$, then, by (43), $0=f(\zeta_i, \alpha_i)c(\alpha, \zeta)$, since $c(\alpha_i, \zeta-\delta_i+\delta_j)\neq 0$ only if $\zeta=\delta_i-\delta_j$, $i\neq j$, in which case $f(\alpha_j, \zeta_j+\delta_j)=0$. Similarly, if $\alpha+(-\alpha_i)+(\zeta-\delta_i)\neq 0$, then $f(\zeta_i, \alpha_i)c(\alpha, \zeta)=0$. Hence $f(\alpha_i, \zeta_i)=0$ for all i. Moreover $\alpha+\delta_i+(\zeta-\delta_i)=\alpha+\zeta\neq 0$, so that $f(\alpha_i, \delta_i)c(\alpha, \zeta) = f(\alpha_i+\zeta, \delta_i)c(\alpha, \zeta)$, that is, $f(\zeta_i, \delta_i)=0$ for all i.

Now suppose that $0\neq\alpha_i+\zeta_i, \zeta_i$ for some i. By the nondegeneracy of f_i, we may choose β_i such that $0\neq f(\alpha_i+\zeta_i, \beta_i), f(\zeta_i, \beta_i)$. Either $\alpha+\beta_i+(\zeta-\delta_i)\neq 0$ or $\alpha-\beta_i+(\zeta-\delta_i)\neq 0$. But $c(\alpha\pm\beta_i-\delta_i, \zeta)=0$ since $f(\alpha_i\pm\beta_i-\delta_i, \zeta_i) = \pm f(\beta_i, \zeta_i)\neq 0$. Thus (43) gives either $0=f(\alpha_i+\zeta_i, \beta_i)c(\alpha, \zeta)$ or $0=f(\alpha_i+\zeta_i, -\beta_i)c(\alpha, \zeta)$, so that $c(\alpha, \zeta)=0$, a contradiction.

Hence for any i either $\alpha_i+\zeta_i=0$ or $\zeta_i=0$. Then, since $0\neq\zeta, \alpha+\zeta$, we have $\zeta_j=0$ and $\alpha_j\neq 0$ for some j and $\alpha_k=-\zeta_k\neq 0$ for some $k\neq j$. Then $f(\alpha_k, \delta_k) = f(-\zeta_k, \delta_k)=0$. Now choose γ_j such that $f(\alpha_j, \gamma_j)\neq 0$. Then $\alpha+(\gamma_j-\alpha_k)+(\zeta-\delta_j)$ has a nonzero component in $\mathfrak{G}_k$, so that (43) gives

$$
\begin{aligned}
&f(\alpha_j, \gamma_j)c(\alpha+\gamma_j-\alpha_k-\delta_j, \zeta)\\
&= f(\alpha_j+\zeta_j, \gamma_j)c(\alpha, \zeta) + f(\alpha_k+\zeta_k+\delta_k, -\alpha_k)c(\alpha, \zeta-\delta_j+\delta_k) + f(\alpha_j, \gamma_j+\zeta_j)c(\gamma_j-\alpha_k, \zeta)\\
&\quad + f(\alpha_k, -\alpha_k+\zeta_k+\delta_k)c(\gamma_j-\alpha_k, \zeta-\delta_j+\delta_k) + \sum_{i\neq j,k} f(\alpha_i, \zeta_i+\delta_i)c(\gamma_j-\alpha_k, \zeta-\delta_k+\delta_i).
\end{aligned}
$$

But $c(\alpha+\gamma_j-\alpha_k-\delta_j, \zeta)=0$ since $\alpha_k-\alpha_k+\zeta_k\neq 0$, $c(\gamma_j-\alpha_k, \zeta)=0$ since $-\alpha_k+\zeta_k\neq 0$, and, when $i\neq j, k$, $f(\alpha_i, \zeta_i+\delta_i)c(\gamma_j-\alpha_k, \zeta-\delta_j-\delta_i)=0$ since either $\zeta_i+\delta_i\neq 0$ or $f(\alpha_i, \zeta_i+\delta_i)=0$. Hence we get $f(\alpha_j, \gamma_j)c(\alpha, \zeta)=0$, $c(\alpha, \zeta)=0$, a contradiction, and the lemma is proved.

LEMMA 16. *Suppose that $c(\alpha, \zeta)=0$ whenever $\zeta\neq 0$. Then the derivation D differs by a scalar multiple of $D(\delta, 0)$ from a derivation for which*

$$c(t_1\delta_1 + \cdots + t_m\delta_m, 0) = 0$$

for any integers $t_1, \cdots, t_m$.

In this proof we shall write $c(\alpha, 0) = c(\alpha) = c_\alpha$. By the hypothesis, there are nonzero terms in (43) only when $\epsilon = -\delta_j$ for some j, in which case we have

$$f(\alpha_j, \beta_j)\{c(\alpha + \beta - \delta_j) - c_\alpha - c_\beta\} = 0, \tag{63}$$

provided $\alpha+\beta-\delta_j \neq 0$. Choose α such that $f(\alpha_i, \delta_i) \neq 0$ for $i = 1, \cdots, m$. Suppose that $t_j \not\equiv 0 \pmod{p}$. Then with $\beta = t_1\delta_1 + \cdots + t_m\delta_m$ we have $f(\alpha_j, \beta_j) = t_j f(\alpha_j, \delta_j) \neq 0$, so that (63) gives

$$c(\alpha + t_1\delta_1 + \cdots + t_m\delta_m - \delta_j) = c_\alpha + c(t_1\delta_1 + \cdots + t_m\delta_m). \tag{64}$$

But then for $i = 1, \cdots, m$ we have $c(\alpha+\delta_i) = c_\alpha + c(2\delta_i)$, so that, by iteration, $c(\alpha + t_1\delta_1 + \cdots + t_m\delta_m - \delta_j) = c_\alpha + t_1 c(2\delta_1) + \cdots + (t_j - 1)c(2\delta_j) + \cdots + t_m c(2\delta_m)$, which, combined with (64), gives

$$c(t_1\delta_1 + \cdots + t_m\delta_m) = t_1 c(2\delta_1) + \cdots + (t_j - 1)c(2\delta_j) + \cdots + t_m c(2\delta_m). \tag{65}$$

Now when $\mathfrak{G}_0 \neq 0$, choose β_0 and β_0' in $\mathfrak{G}_0$ such that $f(\beta_0, \beta_0') \neq 0$, and β_i in $\mathfrak{G}_i$ such that $f(\beta_i, \delta_i) \neq 0$. Then with $j = 0$, (63) gives $f(\beta_0, \beta_0')\{c(\beta_0+\beta_i) - c(\beta_0-\beta_0'+\beta_i-\delta_i) - c(\beta_0'+\delta_i)\} = 0$, while with $j = i$, (63) gives $f(\beta_i, \delta_i) \cdot \{c(\beta_0+\beta_i-\delta_i) - c(\beta_0-\beta_0'+\beta_i-\delta_i) - c(\beta_0'+\delta_i)\} = 0$. Thus $c(\beta_0+\beta_i-\delta_i) = c(\beta_0+\beta_i)$. Now with γ such that $f(\gamma_i, \delta_i) \neq 0$ and $c(\gamma-\delta_i) = c_\gamma$, (63) gives $f(\gamma_i, 2\delta_i)\{c_\gamma - c(\gamma-\delta_i) - c(2\delta_i)\} = 0$, so that $c(2\delta_i) = 0$ for $i = 1, \cdots, m$, and by (65) the lemma holds when $\mathfrak{G}_0 \neq 0$.

Now suppose that $\mathfrak{G}_0 = 0$. By (64), we have $c_\alpha + c(2\delta_i) = c(\alpha+\delta_i) = c_\alpha + c(\delta_i+\delta_k) = c(\alpha+\delta_k) = c_\alpha + c(2\delta_k)$, so that $c(2\delta_i) = c(2\delta_k)$ for $i, k = 1, \cdots, m$. Thus, by (65) and (45), $v(t_1\delta_1 + \cdots + t_m\delta_m)D = c(2\delta_1)(-1 + t_1 + \cdots + t_m) \cdot v(t_1\delta_1 + \cdots + t_m\delta_m) = c(2\delta_1)v(t_1\delta_1 + \cdots + t_m\delta_m)D(\delta, 0)$, and the lemma is proved.

LEMMA 17. *Suppose that $c(\alpha, \zeta) = 0$ whenever either $\zeta \neq 0$ or α is of the form $t_1\delta_1 + \cdots + t_m\delta_m$. Then D is a linear combination of the derivations $D(\sigma_{ij}, 0)$.*

By the definition of the derivations $D(\sigma_{ij}, 0)$ in (46), it is enough to show that

$$c_{\alpha+\beta} = c_\alpha + c_\beta \tag{66}$$

for every α and β, where in this proof we continue to write $c(\alpha, 0) = c(\alpha) = c_\alpha$. We may again use (63) whenever $\alpha+\beta-\delta_j \neq 0$, and (64) whenever $t_j f(\alpha_j, \delta_j) \neq 0$. We shall first show that

$$c(\alpha - \delta_i) = c_\alpha \tag{67}$$

for any α and any i. It follows from (64) that if $f(\alpha_i, \delta_i) \neq 0$ then $c(\alpha-\delta_i) = c_\alpha + (p-1)c(2\delta_i) = c_\alpha$, so that we may assume here that $i \neq 0$, $f(\alpha_i, \delta_i) = 0$, and $\alpha \neq 0, \delta_i$. Now we may choose γ such that, for some j, the expressions $f(\alpha_j-\delta_i, \gamma_j)$, $\alpha-\delta_i+\gamma-\delta_j$, $f(\alpha_i+\gamma_i, \delta_i)$, $f(\alpha_j, \gamma_j)$ and $\alpha+\gamma-\delta_j$ are all nonzero. Then, by (63) and the case of (67) already proved,

$$c(\alpha - \delta_i) + c_\gamma = c(\alpha + \gamma - \delta_i - \delta_j) = c(\alpha + \gamma - \delta_j) = c_\alpha + c_\gamma,$$

so that (67) holds. Hence (63) reduces to

$$f(\alpha_i, \beta_i)\{c_{\alpha+\beta} - c_\alpha - c_\beta\} = 0, \tag{68}$$

again under the condition that $\alpha+\beta-\delta_i \neq 0$.

If α has nonzero components α_i, α_j, $i \neq j$, then we may take γ such that the expressions $f(\alpha_j, \gamma_j)$, $\gamma+\alpha-\delta_j$, $f(\alpha_i, \gamma_i)$ and $\gamma+\alpha-\alpha_j-\delta_i$ are all nonzero. Then $c_\gamma+c_\alpha = c_{\gamma+\alpha} = c(\gamma+\alpha-\alpha_j)+c(\alpha_j) = c_\gamma+c(\alpha-\alpha_j)+c(\alpha_j)$. Thus $c_\alpha = c(\alpha-\alpha_j)+c(\alpha_j)$, so that it is enough to prove (66) when α, β are nonzero elements of $\mathfrak{G}_i$ such that either $f(\alpha, \beta)=0$ or $\alpha+\beta-\delta_i=0$. Suppose that $\alpha \neq -\beta$, $-\beta+\delta_i$. Since f_i is a nondegenerate form and $p \neq 2$, we may choose γ in $\mathfrak{G}_i$ such that $0 \neq f(\alpha, \gamma)$, $f(\beta, \gamma)$, $f(\alpha+\beta, \gamma)$. Then (68) implies that $c_{\alpha+\beta}+c_\gamma = c_{\alpha+\beta+\gamma} = c_\alpha+c_{\beta+\gamma} = c_\alpha+c_\beta+c_\gamma$, and (66) holds when $\alpha \neq -\beta$, $-\beta+\delta_i$. But $c(-\alpha+\delta_i) = c_{-\alpha} = c_{(p-1)\alpha} = (p-1)c_\alpha$, and the lemma is proved.

THEOREM 13. *When $p>3$ the derivations $D(\sigma_k, -\delta_k)$, $D(\delta_k, -\delta_k)$, $D(\sigma_{ij}, 0)$ and $D(\delta, 0)$, defined in* (44), (46) *and* (45), *together with the extended inner derivations, span the algebra $\bar{\mathfrak{L}}(\mathfrak{G}, \delta, f)$ of all derivations of $\mathfrak{L}(\mathfrak{G}, \delta, f)$.*

This is an immediate consequence of Lemmas 13 through 17.

We shall now determine the structure of the algebra $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$ of outer derivations of $\mathfrak{L}(\mathfrak{G}, \delta, f)$. We shall write $n, n_0, \cdots, n_m$ for the dimensions of $\mathfrak{G}, \mathfrak{G}_0, \cdots, \mathfrak{G}_m$ over $\mathfrak{F}_p$.

When $\mathfrak{G}=\mathfrak{G}_0$, the set consisting of the inner derivations R_α, for all nonzero α in $\mathfrak{G}$, and the derivations $D(\sigma_{01}, 0), \cdots, D(\sigma_{0n}, 0)$, is clearly linearly independent over $\mathfrak{F}$ and hus tis a basis of $\bar{\mathfrak{L}}(\mathfrak{G}, \delta, f)$. Since any two derivations $D(\sigma_{ij}, 0)$, $D(\sigma_{kl}, 0)$ commute, $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$ is an n-dimensional abelian algebra in this case.

Now suppose that $\mathfrak{G} \neq \mathfrak{G}_0$. The set of derivations

$$\mathfrak{R} = \{R_\alpha : \alpha \in \mathfrak{G}, \alpha \neq 0\}$$

is linearly independent, since $v(\sigma_1)R_{-\delta} = -f(\sigma_1, \delta_1)v(\sigma_1-\delta-\delta_1) \neq 0$ while $v(\sigma_1)R_\gamma = f(\sigma_1, \gamma_1)v(\sigma_1+\gamma-\delta_1)$ has no term in $v(\sigma_1-\delta-\delta_1)$ when $\gamma \neq -\delta$. The set of derivations

$$\mathfrak{S} = \{D(\sigma_k, -\delta_k), D(\delta_k, -\delta_k) : k = 1, \cdots, m\}$$

is also linearly independent, since $\sum_{k=1}^{m} [b_k D(\sigma_k, -\delta_k) + b_k' D(\delta_k, -\delta_k)]$ maps $v(\delta_k)$ onto zero only if $b_k=0$ and maps $v(\sigma_k)$ onto zero only if $b_k'=0$. We define a set of derivations $\mathfrak{T}$ by setting

$$\mathfrak{T} = \{D(\delta, 0), D(\sigma_{ij}, 0) : i = 1, \cdots, m; j = 2, \cdots, n_i - 1\}$$

when $\mathfrak{G}_0=0$, and

$$\mathfrak{T} = \{D(\sigma_{0k}, 0), D(\sigma_{ij}, 0) : k = 1, \cdots, n_0; i = 1, \cdots, m; j = 2, \cdots, n_i - 1\}$$

when $\mathfrak{G}_0 \neq 0$.

Since $v_\alpha v(\delta_i) = f(\alpha_i, \delta_i)v_\alpha = \sum_{j=1}^{n_i-1} s_{ij}(\alpha)f(\sigma_{ij}, \delta_i)v_\alpha$, we have $R(\delta_i) = \sum_{j=1}^{n_i-1} f(\sigma_{ij}, \delta_i)D(\sigma_{ij}, 0)$. Then when $i \neq 0$, $D(\sigma_{i1}, 0)$ is contained in the space spanned by $R(\delta_i)$ and $\mathfrak{T}$ since $f(\sigma_{i1}, \delta_i) \neq 0$. But the set $\mathfrak{T} \cup \{D(\sigma_{11}, 0), \cdots, D(\sigma_{m1}, 0)\}$ is clearly linearly independent and thus $\mathfrak{T} \cup \{R(\delta_1), \cdots, R(\delta_m)\}$ is linearly independent. Since $v_\alpha R_\beta$ has no term in $v(\alpha - \delta_k)$ for any k, and has a term in v_α only if $\beta = \delta_i$ for some $i \neq 0$, it follows that $\mathfrak{R} \cup \mathfrak{S} \cup \mathfrak{T}$ is linearly independent. Then by Theorem 13 we have the following result.

LEMMA 18. *The set* $\mathfrak{R} \cup \mathfrak{S} \cup \mathfrak{T}$ *is a basis of* $\bar{\mathfrak{L}}(\mathfrak{G}, \delta, f)$ *when* $\mathfrak{G} \neq \mathfrak{G}_0$.

We continue to assume that $\mathfrak{G} \neq \mathfrak{G}_0$. We shall write $R^*_{-\delta}$ for the outer derivation determined by $R_{-\delta}$, and $D^*(\alpha, \beta)$ for the outer derivation determined by $D(\alpha, \beta)$, where $(\alpha, \beta) = (\sigma_{ij}, 0)$, $(\delta, 0)$, $(\sigma_i, -\delta_i)$ or $(\delta_i, -\delta_i)$. Now when $\mathfrak{G}_0 = 0$, the set

$$\mathfrak{B} = \{R^*_{-\delta}, D^*(\sigma_i, -\delta_i), D^*(\delta_i, -\delta_i), D^*(\sigma_{ij}, 0), D^*(\delta, 0): i = 1, \cdots, m; j = 2, \cdots, n_i - 1\} \tag{69}$$

is a basis of $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$, and when $\mathfrak{G}_0 \neq 0$, the set

$$\mathfrak{C} = \{R^*_{-\delta}, D^*(\sigma_k, -\delta_k), D^*(\delta_k, -\delta_k), D^*(\sigma_{0l}, 0), D^*(\sigma_{ij}, 0): i, k = 1, \cdots, m; j = 2, \cdots, n_i - 1; l = 1, \cdots, n_0\} \tag{70}$$

is a basis of $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$.

For any i, j, k and l, $D(\sigma_{ij}, 0)$ commutes with $D(\sigma_{kl}, 0)$, $D(\delta, 0)$, $D(\sigma_k, -\delta_k)$, $D(\delta_k, -\delta_k)$ and $R_{-\delta}$. When $j \neq k$, $D(\beta_j, -\delta_j)$ and $D(\gamma_k, -\delta_k)$ commute for any β_j in $\mathfrak{G}_j$ and γ_k in $\mathfrak{G}_k$, while

$$\begin{aligned} v_\alpha[D(\sigma_i, -\delta_i) \cdot D(\delta_i, -\delta_i)] &= [f(\alpha_i, \sigma_i)f(\alpha_i, \delta_i) - f(\alpha_i, \delta_i)f(\alpha_i - \delta_i, \sigma_i)]v(\alpha - 2\delta_i) \\ &= f(\sigma_i, \delta_i)f(\alpha_i, -\delta_i)v(\alpha - 2\delta_i) = a_i v_\alpha R(-\delta_i). \end{aligned}$$

Moreover $v_\alpha[D(\gamma_i, -\delta_i) \cdot R_{-\delta}]$ has no nonzero terms except those in the elements $v(\alpha - \delta - \delta_i - \delta_j)$ with $i, j \neq 0$. Hence all products of elements of $\mathfrak{C}$ are zero except when $m = 1$, in which case

$$D^*(\sigma_1, -\delta_1) \cdot D^*(\delta_1, -\delta_1) = a_1 R^*_{-\delta} \neq 0. \tag{71}$$

If $\mathfrak{G}_0 = 0$ then $D(\delta, 0) \neq 0$ and

$$\begin{aligned} v_\alpha[D(\delta, 0) \cdot D(\gamma_i, -\delta_i)] &= \left\{\left[-1 + \sum_{j=1}^{m} s_j(\alpha)\right]f(\alpha_i, \gamma_i) \right. \\ &\quad \left. - f(\alpha_i, \gamma_i)\left[-2 + \sum_{j=1}^{m} s_j(\alpha)\right]\right\} v(\alpha - \delta_i) \\ &= f(\alpha_i, \gamma_i)v(\alpha - \delta_i) = v_\alpha D(\gamma_i, -\delta_i). \end{aligned}$$

Hence

$$D^*(\delta, 0)\cdot D^*(\sigma_i, -\delta_i) = D^*(\sigma_i, -\delta_i), \tag{72}$$
$$D^*(\delta, 0)\cdot D^*(\delta_i, -\delta_i) = D^*(\delta_i, -\delta_i), i = 1, \cdots, m.$$

Furthermore

$$v_\alpha[D(\delta, 0)\cdot R_{-\delta}] = \left[-1 + \sum_{j=1}^{m} s_j(\alpha)\right]\left[\sum_{i=1}^{m} f(\alpha_i, -\delta_i)v(\alpha - \delta - \delta_i)\right]$$
$$- \sum_{i=1}^{m}\left\{f(\alpha_i, -\delta_i)\left[-(m+2) + \sum_{j=1}^{m} s_j(\alpha)\right]v(\alpha - \delta - \delta_i)\right\}$$
$$= \sum_{i=1}^{m} (m+1)f(\alpha_i, -\delta_i)v(\alpha - \delta - \delta_i) = (m+1)v_\alpha R_{-\delta}.$$

Hence

$$D^*(\delta, 0)\cdot R^*_{-\delta} = (m+1)R^*_{-\delta}, \tag{73}$$

and we have determined all products of elements of $\mathfrak{B}$. We collect these results in the following theorem.

THEOREM 14. *Suppose that $p>3$. If $\mathfrak{G}=\mathfrak{G}_0$ then the algebra $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$ of outer derivations of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is an n-dimensional abelian algebra. If $\mathfrak{G}_0=0$, then $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$ has dimension $n+2$, with a basis $\mathfrak{B}$ given by* (69), *and all nonzero products of elements of $\mathfrak{B}$ are given by* (72), (73) *and, in case $m=1$,* (71). *If $\mathfrak{G}_0\neq 0$ and $\mathfrak{G}\neq\mathfrak{G}_0$, then $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$ has dimension $n+1$, with a basis $\mathfrak{C}$ given by* (70), *and is abelian unless $m=1$, in which case the only nonzero product of elements of $\mathfrak{C}$ is given by* (71).

We deduce as immediate consequences of this theorem the solvability of $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$ and our criterion for nonisomorphism of algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ of the same dimension. We let $m(\mathfrak{G})$ denote the index m occurring in the direct sum decomposition (1) of $\mathfrak{G}$.

COROLLARY 1. *Two algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ and $\mathfrak{L}(\mathfrak{G}', \delta', f')$ of the same dimension are isomorphic only if either $\mathfrak{G}_0=0$, $\mathfrak{G}_0'=0$ and $m(\mathfrak{G})=m(\mathfrak{G}')$, or $\mathfrak{G}_0\neq 0$, $\mathfrak{G}_0'\neq 0$ and* $\min[2, m(\mathfrak{G})]=\min[2, m(\mathfrak{G}')]$.

This follows upon our noting the dimensions of the algebras of outer derivations and their squares, since if $\mathfrak{G}_0=0$ then $[\mathfrak{L}^*(\mathfrak{G}, \delta, f)]^{(2)}$ has dimension $2m+1$ when $m+1\not\equiv 0 \pmod p$ and dimension $2m$ otherwise, while if $\mathfrak{G}_0\neq 0$ then $[\mathfrak{L}^*(\mathfrak{G}, \delta, f)]^{(2)}$ is one-dimensional if and only if $m=1$.

COROLLARY 2. *The algebra $\mathfrak{L}^*(\mathfrak{G}, \delta, f)$ is always solvable.*

Indeed the second derived algebra $[\mathfrak{L}^*(\mathfrak{G}, \delta, f)]^{(2)}$ is always zero unless $\mathfrak{G}=\mathfrak{G}_1$, in which case $[\mathfrak{L}^*(\mathfrak{G}, \delta, f)]^{(3)}=0$.

By examining the dimensions of the known algebras and applying Corollary 2, we find that when $p>3$ one of our algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ may be isomorphic to a previously known nonclassical simple Lie algebra only if $\mathfrak{G}=\mathfrak{G}_0$, $\mathfrak{G}=\mathfrak{G}_1$ or $n=2m$, Moreover by Theorem 8 (on restrictedness) it follows that if $p>2$ and $n>2m$ then $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is not isomorphic to any classical algebra.

The algebras $\mathfrak{L}(\mathfrak{G}, \delta, f)$ for which $n=2m$ are the same as the algebras $\mathfrak{B}_{m,\mu}$ considered in §5. Let $\mathfrak{P}_r$ be the simple Lie algebra of all r-rowed square matrices of trace zero modulo scalar matrices. Then $\mathfrak{B}_{m,\mu}$ and $\mathfrak{P}_r$ have the same dimension when $r=p^m$. It is proved in [1] that $\mathfrak{B}_m$ is isomorphic to $\mathfrak{P}_r$ if and only if $m=1$ and $r=p=3$, and the proof for $\mathfrak{B}_m$ may easily be extended to a proof for $\mathfrak{B}_{m,\mu}$. However, this theorem is an immediate consequence of results on the derivations of the algebras, and we include it in our final corollary.

COROLLARY 3. *When $p>2$, $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is isomorphic to a classical algebra only if $p=3$ and $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is 7-dimensional. When $p=2$, $\mathfrak{L}(\mathfrak{G}, \delta, f)$ is not isomorphic to any algebra $\mathfrak{P}_r$.*

For it is proved in [9] that the algebra of outer derivations of $\mathfrak{P}_r$ has dimension 0 or 1 for any p, and it is proved in [4] that when $p>2$ all derivations of the classical algebras of types B, C, and D are inner. But for any p, the outer derivations $D^*(\sigma_1, -\delta_1)$, $D^*(\delta_1, -\delta_1)$ (or $D^*(\sigma_{01}, 0)$, $D^*(\sigma_{02}, 0)$ when $\mathfrak{G}=\mathfrak{G}_0$) of $\mathfrak{L}(\mathfrak{G}, \delta, f)$ are linearly independent. There is no isomorphism between $\mathfrak{L}(\mathfrak{G}, \delta, f)$ and an exceptional simple algebra of dimension q unless $p=2$ and $q=14$, since otherwise their dimensions are distinct.

BIBLIOGRAPHY

1. A. A. Albert and M. S. Frank, *Simple Lie algebras of characteristic p*, Univ. e Politec. Torino Rend. Sem. Mat. vol. 14 (1954–1955) pp. 117–139.

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

3. N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. vol. 42 (1937) pp. 206–224.

4. ———, *Classes of restricted Lie algebras of characteristic p.* I, Amer. J. Math. vol. 63 (1941) pp. 481–515.

5. ———, *Classes of restricted Lie algebras of characteristic p.* II, Duke Math. J. vol. 10 (1943) pp. 107–121.

6. I. Kaplansky, *Seminar on simple Lie algebras.* The First Summer Mathematical Institute, Bull. Amer. Math. Soc. vol. 60 (1954) pp. 470–471.

7. G. B. Seligman, *On a class of semisimple restricted Lie algebras*, Proc. Nat. Acad. Sci. U.S.A. vol. 40 (1954) pp. 726–728.

8. ———, *On Lie algebras of prime characteristic*, Memoirs Amer. Math. Soc., no. 19, 1956.

9. H. Zassenhaus, *Über Lie'sche ringe mit primzahlcharakteristik*, Abh. Math. Sem. Univ. Hamburg vol. 13 (1939) pp. 1–100.

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILL.