TWO NEW CLASSES OF SIMPLE LIE ALGEBRAS(1)

BY
MARGUERITE FRANK

0. **Introduction.** In this paper we define a Lie algebra R of dimension p^{2n+1} over a field F of characteristic $p > 2$, which we show to be central simple if $n + 2$ is not divisible by p. From the fact that all derivations of R are inner we conclude that R is not isomorphic to known algebras of identical dimension (except, possibly, if $n = \frac{1}{2}(p^{2r} + 2r - 1)$, $r \geqq 1$). If $n + 2 \equiv 0 \pmod{p}$, it is shown that the algebra R^2, of dimension $p^{2n+1} - 1$ over F, is central simple and also new. We finally perform a Cartan decomposition of both algebras.

As R is a subalgebra of the Jacobson-Witt algebra(2), we start with a brief description of the latter: If F is an arbitrary field of characteristic $p > 0$, let B_n be the algebra of all polynomials in $x_1, \cdots, x_n$ subject to the condition that $x_1^p = \cdots = x_n^p = 0$. Then the space W_n of all derivations over F of B_n is the set of all transformations

$$a: f = f(x_1, \cdots, x_n) \to fa = \frac{\partial f}{\partial x_1} a_1 + \cdots + \frac{\partial f}{\partial x_n} a_n,$$

for $a_1, \cdots, a_n$ in B_n. Thus every derivation of B_n may be represented by an n-tuple $a = (a_1, \cdots, a_n)$ with coordinates in B_n. The space W_n becomes a Lie algebra over F with respect to the product $f(ab) = (fa)b - (fb)a$. It may be verified by elementary computation that $(a_1, \cdots, a_n)(b_1, \cdots, b_n) = (c_1, \cdots, c_n)$ with

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

We shall in particular denote the partial differential operators

$$(0, \cdots, 0, \underset{i}{1}, 0, \cdots, 0)$$

by Δ_i.

Let F_n denote the Lie algebra over F of all n-rowed square matrices with elements in F, with respect to the product $[A_1 A_2] = A_1 A_2 - A_2 A_1$, where $A_1 A_2$ stands for the associative product of the two matrices. If M is a subalgebra of F_n, the direct product $M \times B_n$ will denote the Lie algebra over F of sums of n-rowed square matrices $A\phi = (a_{ij}\phi)$, where $A = (a_{ij}) \in M$, $\phi \in B_n$, and the product of two

Received by the editors February 23, 1962.
(1) This paper was sponsored by the National Science Foundation (G-7317).
(2) Cf. [7].

matrices is given by $[A_1\phi_1, A_2\phi_2] = [A_1A_2]\phi_1\phi_2$. The construction leading to the definition of the new algebras is based on the following easily proved result([3]).

THEOREM 0.1. *Let M be a Lie subalgebra of F_n. Then the subspace L of all derivations $a = (a_1, \cdots, a_n)$ in W_n whose "associated matrix"*

$$\left(\frac{\partial a_i}{\partial x_j}\right)_{i,j=1,\ldots,n} \tag{2}$$

belongs to $M \times B_n$, is a Lie algebra.

Proof. If $a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n)$ are in L with associated matrices

$$\left(\frac{\partial a_i}{\partial x_j}\right) = A, \quad \left(\frac{\partial b_i}{\partial x_j}\right) = B$$

in $M \times B_n$, let $ab = c = (c_1, \cdots, c_n)$ where c_i is given by (1), and define the matrix

$$\left(\frac{\partial c_i}{\partial x_j}\right) = C$$

in $F_n \times B_n$. Compute

$$\frac{\partial c_i}{\partial x_j} = \sum_{k=1}^{n} \left[\frac{\partial a_i}{\partial x_k}\frac{\partial b_k}{\partial x_j} - \frac{\partial b_i}{\partial x_k}\frac{\partial a_k}{\partial x_j}\right] + \sum_{k=1}^{n} \frac{\partial}{\partial x_k}\left(\frac{\partial a_i}{\partial x_j}\right) b_k$$

$$- \sum_{k=1}^{n} \frac{\partial}{\partial x_k}\left(\frac{\partial b_i}{\partial x_j}\right) a_k.$$

Writing this relation in matrix notation, we have

$$C = [AB] + (A)b - (B)a, \tag{3}$$

where $(A)b$ denotes the matrix in $F_n \times B_n$ whose elements are those of A operated on by the derivation b, and hence belongs to $M \times B_n$ since A does; similarly $(B)a$ is in $M \times B_n$. Finally, since $[AB]$ belongs to the Lie algebra $M \times B_n$, so does the matrix C; c is in L and L is a Lie algebra. This completes the proof of the theorem.

In the following, we shall specify the algebra M to be the normalizer of the algebra of matrices which represent B_n in the regular representation with respect to a natural basis. We characterize this algebra—as a linear subspace of F_{p^n}—by linear equations over F. Owing to Theorem 0.1, these in turn yield a set of linear first order differential equations which cut out a subalgebra of W_{p^n}—the new algebra R alluded to in the first paragraph.

([3]) A generalized version of this result is at the center of another paper in preparation. It provides a common framework for all known simple Lie algebras of characteristic $p > 0$ not analogous to algebras of characteristic zero (namely, all those of [1], [2], [3], [4], [7], [8], [9], [12]). A first incomplete draft of both papers is to be found in [5].

1. **Characterization of M.** We assume from now on that $p > 2$. We proceed to construct first of all a regular representation in F_{p^n} of the associative commutative p^n-dimensional algebra $B_n = F[x_1, \cdots, x_n]$. We call the integer i, satisfying the constraints $1 \leqq i \leqq p^n$, an *index*. Using p-adic notation we can denote the index

$$i = (i_0 + i_1 p + \cdots + i_{n-1} p^{n-1}) + 1 \qquad (0 \leqq i_k < p),$$

in a unique way by its n digits—which we consider as ordinary integers, *not* as elements of the prime field, unless they belong explicitly to relations over F—and we write

$$i = [i_0, i_1, \cdots, i_{n-1}].$$

Similarly, we shall write

$$x_1^{i_0} x_2^{i_1} \cdots x_n^{i_{n-1}} = x[i_0, i_1, \cdots, i_{n-1}] = x[i]$$
$$(0 \leqq i_k \leqq p-1,\ k = 0, 1, \cdots, n-1),$$

for all basis monomials in B_n, and order those in a natural way by the relation

$$x[i] < x[j] \Leftrightarrow i < j.$$

In these first sections, we will work with pairs of indices i and $i + m'$. The following convention is used throughout: If $m' \geqq 0$, let $m = m' + 1$; if $m' < 0$, let $\bar{m} = -m'$. In either case, m or $\bar{m}$ is an index.

The next two lemmas, which clarify certain properties of p-adic notation, will be stated without proof, as they are easily established by elementary computation.

LEMMA 1.1. *Let i and $j = i + m'$ be two indices with $m' \geqq 0$. Then*
(a) $i_\mu + m_\mu \leqq p-1\ (\mu \leqq k) \Leftrightarrow j_\mu = i_\mu + m_\mu\ (\mu \leqq k) \Leftrightarrow i_\mu \leqq j_\mu\ (\mu \leqq k)$.
(b) $i_\mu \leqq j_\mu (\mu < k) \Rightarrow : i_k = j_k + 1 \Leftrightarrow m_k = p-1, i_k \neq 0$.

LEMMA 1.2. *Let i and $j = i + m'$ be two indices with $m' < 0$. Then* $i_\mu \leqq j_\mu\ (\mu \neq k)$, $i_k - 1 \leqq j_k \Rightarrow j_k = i_k - 1$, $\bar{m}_\mu = 0\ (\mu \geqq k)$.

In order to simplify the notation, we introduce for a pair of arbitrary indices i and j the constraint symbols $i \curlyvee j$ and $i \curlyvee^k j$, for $k = 0, 1, \cdots, n-1$, as follows:

$$(4) \qquad \begin{cases} i \curlyvee j \Leftrightarrow i_\mu \leqq j_\mu & (\text{all } \mu). \\ i \curlyvee^k j \Leftrightarrow \begin{cases} i_\mu \leqq j_\mu & (\mu \neq k), \\ i_k = j_k + 1. \end{cases} \end{cases}$$

It follows from part (a) of Lemma 1.1 that if i and m are indices, the product $x[i]x[m]$ is given by $x[j]$ for $j = i + m'$, $m' = m - 1$, if and only if j is an index

and $i \curlyvee j$; otherwise the product vanishes. Thus a regular representation of B_n with respect to its ordered basis is given by the mapping:

$$x[m] \to A^n_{m'} \in F_{p^n} \qquad (m = 1, \cdots, p^n),$$

where $m' = m - 1$, and

$$A^n_{m'} = (a_{ij;m'})$$

with

$$(5) \qquad \begin{cases} a_{ij;m'} = 1 & \text{if } j = i + m' \text{ and } i \curlyvee j, \\ a_{ij;m'} = 0 & \text{otherwise.} \end{cases}$$

Denote by $\tilde{B}_n$ the associative algebra of matrices $A^n_{m'}$ over F, and let M be the normalizer of $\tilde{B}_n$ in F_{p^n}. That is, M is the Lie algebra over F generated by all matrices A in F_{p^n} such that

$$[AX] \in \tilde{B}_n \qquad (\text{all } X \in \tilde{B}_n).$$

Then M contains at least the subspace $\tilde{B}_n$. Moreover if Δ is a derivation of B_n,

$$(b_1 b_2)\Delta - (b_1\Delta)b_2 = b_1(b_2\Delta) \qquad (\text{all } b_i \in B_n),$$

and it follows that the matrix in F_{p^n} determined by the mapping $\Delta : b \in B_n \to b\Delta$ belongs to M also.

Denote by $v_k[r]$ the derivation vector $(a_1, \cdots, a_n)$ in W_n with $a_t = 0$, $i \neq k$, and $a_k = x[r]$. Let i and $m' + p^{k-1} + 1$ be a pair of indices. It then follows easily from Lemmas 1.1 and 1.2 that, for $1 \leqq k \leqq n$,

$$(6) \qquad x[i]\, v_k[m' + p^{k-1} + 1] = i_{k-1}\, x[i + m']$$

if $i + m'$ is an index, and if either $i \curlyvee i + m'$, or $i \curlyvee^{k-1} i + m'$. If these conditions are not fulfilled, the left side of (6) vanishes. The matrices in M corresponding to the derivations $v_k[m' + p^{k-1} + 1]$ in W_n, for $k = 1, \cdots, n$, are thus given by

$$A^{k-1}_{m'} = (a^{k-1}_{ij;m'}) \qquad (m' = -p^{k-1}, -p^{k-1} + 1, \cdots, p^n - p^{k-1} - 1),$$

with components in F

$$(7) \qquad \begin{cases} a^{k-1}_{ij;m'} = i_{k-1} & \text{if } j = i + m' \text{ and } \begin{cases} i_\mu \leqq j_\mu & (\mu \neq k-1) \\ i_{k-1} \leqq j_{k-1} + 1, \end{cases} \\ a^{k-1}_{ij;m'} = 0 & \text{otherwise.} \end{cases}$$

Now if $A \in M$, the mapping $X \in \tilde{B}_n \to [AX]$ is a derivation of $\tilde{B}_n$ which vanishes if and only if $[AX] = 0$ for all X in $\tilde{B}_n$, that is, if and only if $A \in \tilde{B}_n$(4). Considering now $\tilde{B}_n$ as an abelian ideal of M, we can thus write

$$M - \tilde{B}_n \cong W_n.$$

(4) Since B_n is commutative, $\tilde{B}_n$ is its own F_{p^n}-commutator.

Hence M is spanned exactly by all matrices corresponding to the multiplications and derivations of B_n, and we have proved

THEOREM 1.1. *The algebra M has as basis the $(n+1)p^n$ matrices given by* (5) *and* (7).

2. **Defining equations of M.** In this section we shall consistently use the following notation:

$$N_j = p^n - p^j = [p-1, \cdots, p-1, \underset{j}{p-2}, p-1, \cdots, p-1] \qquad (j = 0, 1, \cdots, n-1), \tag{8}$$

$$N_n = p^n = [p-1, \cdots, p-1].$$

We note that if j and k are distinct from n, $N_j < N_k$ if $j > k$. Denote by $\{i, t\}$ the (i, t)-component of matrices in F_{p^n}. For every fixed m', $-(p^n-1) \leqq m' \leqq p^n - 1$, we single out in particular—whenever these are defined—the components

$$\theta_j(m') = \{N_j - m', N_j\} \qquad (j = 0, 1, \cdots, n). \tag{9}$$

We observe that $\theta_n(m')$ is defined if and only if $0 \leqq m' \leqq p^n - 1$, and that $\theta_k(m')$ is defined for indices $k < n$ such that

$$-p^k \leqq m' \leqq N_k - 1. \tag{10}$$

We characterize these conditions further by

LEMMA 2.1. *If $\theta_k(m')$ is not defined for some $k < n$, and if for a pair of indices i, $i + m'$, $i_\mu \leqq (i+m')_\mu$ for all $\mu \neq k$, then $(i+m')_k = p-1$ if $m' \geqq 0$; $(i+m')_k < i_k - 1$ if $m' < 0$.*

Proof. Let $m' \geqq 0$. If $\theta_k(m')$ is not defined, by (10), $m' > N_k - 1$, $m > N_k$, so that $m_\mu = p-1$ for $\mu \geqq k$. Since $i + m' \leqq p^n$, i_k necessarily has value zero, and by Lemma 1.1, $(i+m')_\mu = i_\mu + m_\mu$ for $\mu < k$, $(i+m')_k = i_k + m_k = p-1$.

Let $m' < 0$. If $\theta_k(m')$ is not defined, by (10), $p^n - p^k - m' > p^n$, $m' < -p^k$, $\bar{m} = -m' > p^k$ so that $\bar{m}_j \geqq 1$ for some $j \geqq k$. But then by Lemma 1.2, we must have $(i+m')_k < i_k - 1$.

Define further

$$\theta_j^k(m') \tag{11}$$

as the component $\theta_j(m')$ of the matrix $A^k_{m'}$ for $k = 0, 1, \cdots, n$. Then the value of these components is exhibited in the following two lemmas, the first of which is derived from (5) and (7) by elementary computation.

LEMMA 2.2. *If $0 \leqq m' \leqq p^n - 1$, $\theta_n^n(m') = 1$, $\theta_n^k(m') = -(m_k + 1)$ for $k \neq n$. While if $0 \leqq m' \leqq N_r - 1$ for $r < n$ maximal, then for $0 \leqq j \leqq r$,*

$$m_j \neq p-1 \Rightarrow \begin{cases} \theta_j^k(m') = -(m_k + 1) & (k \neq j,\ k \neq n), \\ \theta_j^j(m') = -(m_j + 2), \\ \theta_j^n(m') = 1. \end{cases}$$

$$m_j = p-1 \Rightarrow \begin{cases} \theta_j^k(m') = 0 & (k \neq j), \\ \theta_j^j(m') = -1. \end{cases}$$

Similarly, if $-p^r \leqq m' < 0$ for some minimal $r \geqq 0$, we let $\bar{m} = -m'$, with $\bar{m}_j = 0$ for $j \geqq r$, $\bar{m}_{r-1} \neq 0$ if $r \geqq 1$. Then $N_r - m' = N_r + \bar{m} = [\bar{m}_0, \cdots, \bar{m}_{r-1}, p-1, \cdots, p-1]$; while for $r < j < n$,

$$N_j - m' = N_j + \bar{m} = [\bar{m}_0, \cdots, \bar{m}_{r-1}, 0, \cdots, 0, \underset{j}{p-1}, \cdots, p-1].$$

From (7), we can thus conclude

LEMMA 2.3. *If* $-p^r \leqq m' < 0$, *for* $r \geqq 0$ *minimal, then* $\theta_j^k(m')$ *is defined for* $r \leqq j$, $k < n$; $\theta_j^j(m') = -1$; *and* $\theta_j^k(m') = 0$ *for* $j \neq k$.

For each value of m', let $E = E(m')$ denote the square matrix of variable order, with elements in F:

$$(\theta_j^k(m')), \tag{12}$$

which by (10) can be defined for j, $k = n, 0, 1, \cdots, r$ if $0 \leqq m' \leqq N_r - 1$ for $r < n$ maximal; and for j, $k = r, r+1, \cdots, n-1$ if $-p^r \leqq m' < 0$ for $r \leqq n-1$ minimal. If $m' = N_n - 1$, let $E(m') = (\theta_n^n(N_n - 1))$, an identity matrix of order one.

LEMMA 2.4. *The matrix* $E(m')$ *given by* (12) *is regular for each value of* m'.

Proof. We know that $E(N_n - 1)$ is regular. If $0 \leqq m' \leqq N_r - 1$, for $r < n$ maximal, suppose there are g subscripts $j \leqq r$ with $m_j = p-1$. Then $0 \leqq g \leqq r+1$ and if $g > 0$, we renumber these subscripts $j_1, \cdots, j_g$. If $g < r+1$, renumber the remaining $j \leqq r$ as $j_{g+1}, \cdots, j_{r+1}$, denote $-(m_j + 2)$ by t_ρ for $\rho = g+1, \cdots, r+1$, and let $n = j_{r+2}$. Reordering the rows and columns of E according to the new indicial sequence we obtain, by substituting the values of $\theta_j^k(m')$ given by Lemma 2.2, a similar matrix

$$E' = \begin{pmatrix} -I_g & 0 \\ 0 & A \end{pmatrix},$$

where I_g is an identity matrix of rank g and $A = (a_{\mu\nu})$ a square matrix of order $r+2-g$ with

$$\begin{aligned} a_{\mu\mu} &= t_\mu && (\mu \neq r+2-g), \\ a_{\mu\nu} &= t_\nu + 1 && (\mu \neq \nu,\ \nu \neq r+2-g), \\ a_{\mu,r+2-g} &= 1 && (\text{all } \mu). \end{aligned} \tag{13}$$

Subtracting the first row from the remaining rows of A, we obtain a matrix which is clearly regular for all values of t_μ. If $m' < 0$, the lemma follows directly from Lemma 2.3.

We are now ready to prove the main theorem of this section.

THEOREM 2.1. *If i and $i + m'$ are indices, and $|m'| \leqq p^n - 1$, the components $\{i, i + m'\}$ of every matrix in M satisfy the following sets $\mathscr{L}(m')$ of linear equations over F.*

$$\{i, i + m'\} = -\sum_{k=0}^{n-1} \lambda_k \theta_k(m') + \left[\sum_{k=0}^{n-1} \lambda_k + 1\right] \theta_n(m') \quad \text{if } i \curlyvee i + m', \tag{14}$$

$$= -\lambda_k \theta_k(m') \quad \text{if } i \curlyvee^k i + m', \tag{15}$$

$$= 0 \quad \text{otherwise}, \tag{16}$$

where the components $\theta_k(m')$ are given by (9), *the constraints by* (4) *and where the coefficients in F*

$$\lambda_k = \lambda_k(i, m') = (i + m')_k + 1. \tag{17}$$

Proof. If $m' \geqq 0, \theta_n(m')$ is always defined, and from Lemma 2.1 we know that if $\theta_k(m')$ is not defined for $k < n$, then by (17), $\lambda_k(i, m') = 0$ for all pairs $i \curlyvee i + m'$ or $i \curlyvee^k i + m'$. In case $m' < 0$, $i \curlyvee i + m'$ is never feasible and if $\theta_k(m')$ is not defined, then again by Lemma 2.1, $i \curlyvee^k i + m'$ is impossible. Hence, no ambiguity arises out of the possible lack of definition of the $\theta_k(m')$.

We next verify that these equations reduce to identities for $\{i, i + m'\} = \theta_k(m')$. Indeed in that case, $i + m' = N_k$,

$$(i + m')_\mu = p - 1, \quad \lambda_\mu(i, m') = 0 \qquad (\mu \neq k),$$

$$(i + m')_k = p - 2, \quad \lambda_k(i, m') = -1 \quad (\text{if } k < n),$$

either $i \curlyvee i + m'$ or $i \curlyvee^k i + m'$ and (14) or (15) reduce to identities.

We know that all A_m^k, satisfy (16); we now show that equations (14), (15) are also satisfied by these matrices. Clearly for $\sigma \neq m'$, A_σ^k satisfies $\mathscr{L}(m')$ trivially since all components $\{i, i + m'\}$ are zero. While if $m' < -p^{n-1}$,

$$\bar{m} = -m' \geqq p^{n-1} + 1, \quad \bar{m}_{n-1} > 0,$$

we see from Lemma 1.2 that neither $i \curlyvee i + m'$, nor $i \curlyvee^k i + m'$ is feasible for any index i, subscript k, and so equations $\mathscr{L}(m')$ imply that $\{i, i + m'\} = 0$ for all i, in agreement with (5) and (7).

Case I. Assume $i \curlyvee i + m'$. Then $m' \geqq 0$, and we let $m = m' + 1$. By Lemma 1.1, if for some subscript j, $m_j = p - 1$, then $i_j = 0$ and $(i + m')_j + 1 = p$. Hence, equation (14) determines the $\{i, i + m'\}$ component of A_m^k, as

$$(18) \qquad \sum_{j \ni m_j \neq p-1} [\, i_j + m_j + 1 \,][\, \theta_n^k(m') - \theta_j^k(m') \,] + \theta_n^k(m').$$

In particular for $k = n$, we know from Lemma 2.2 that $\theta_n^n(m') = \theta_j^n(m') = 1$; so that expression (18) reduces to $\theta_n^n(m') = 1$, which is in agreement with the value given by (5).

If $k \neq n$, again by Lemma 2.2, $\theta_j^k(m') = \theta_n^k(m')$ if $j \neq k$ and if $m_j \neq p - 1$, so that expression (18) becomes

$$(19) \qquad [i_k + m_k + 1][\theta_n^k(m') - \theta_k^k(m')] + \theta_n^k(m')$$

if $m_k \neq p - 1$. While if $m_k = p - 1$, expression (18) reduces to the function $\theta_n^k(m')$, which by Lemma 2.2 is zero; this coincides with the value given by (7), since by Lemma 1.1, we must then have $i_k = 0$.

Let $m_k \neq p - 1$; by Lemma 2.2, $\theta_n^k(m') = -(m_k + 1) = \theta_k^k(m') + 1$. Hence (19) becomes $i_k + m_k + 1 - (m_k + 1) = i_k$ in agreement with the value given by (7).

Case II. Assume $i \curlyvee {}^k i + m'$. By assumption then $(i + m')_k + 1 = i_k$, and so equation (15) states that

$$(20) \qquad \{i, i + m'\} = -i_k \theta_k(m').$$

If $m' \geqq 0$, by Lemma 1.1 we must have $m_k = p - 1$; hence by Lemma 2.2, it follows that this function has value zero on matrices $A_{m'}^j$ for $j \neq k$, in agreement with (5), (7). While on $A_{m'}^k$, since $\theta_k^k(m') = -1$, this component takes on the value i_k in agreement with (7). If $m' < 0$, it follows again from Lemma 2.3 and the above relation that $\{i, i + m'\} = 0$ on $A_{m'}^j$ for $j \neq k$ in agreement with (5), (7). Finally by Lemma 2.3, $\theta_k^k(m') = -1$ so that, as before, $\{i, i + m'\}$ on $A_{m'}^k$ is given by i_k in agreement with (7). This completes the proof of the theorem.

THEOREM 2.2. *The sets* $\mathscr{L}(m')$ *of equations* (14), (15), (16), *define the algebra* M *as subspace of* F_{p^n}.

Proof. Let A be a matrix in F_{p^n} satisfying all equations $\mathscr{L}(m')$. Write A as the um of matrices $A_{m'}$ for $-(p^n - 1) \leqq m' \leqq (p^n - 1)$, where $A_{m'}$ has $\{i, j\} = 0$ unless $j = i + m'$. Then for each m, $A_{m'}$ satisfies equations $\mathscr{L}(m')$. From Lemma 2.4 we can conclude that there exist coefficients ρ_μ in F such that the components $\theta_j(m')$ of the matrix

$$(21) \qquad \hat{A}_{m'} = A_{m'} - \sum_{\mu=0}^{n} \rho_\mu A_{m'}^\mu$$

vanish for all j for which $\theta_j(m')$ is defined. Clearly $\hat{A}_{m'}$ satisfies $\mathscr{L}(m')$ if $A_{m'}$ does, and it follows from (14), (15), (16) that all components $\{i, i + m'\}$ of $\hat{A}_{m'}$ vanish, $\hat{A}_{m'} = 0$, and by (21), $A_{m'} \in M$. Since m' was arbitrary it follows that A is in M.

3. **The algebra** R. Denote by $\mathscr{L}^*(m')$ the set of differential equations obtained from the set $\mathscr{L}(m')$ of Theorem 2.1, by letting for all indices i, j, $\{i, j\}$ denote the differential function $\partial a_i/\partial x_j$ of the vector $(a_1, \cdots, a_{p^n})$ in W_{p^n}. In particular then, we let

$$\theta_j(m') = \{N_j - m', N_j\} = \frac{\partial a_{N_j - m'}}{\partial x_{N_j}} \qquad (j = 0, \cdots, n-1, n).$$

By Theorem 0.1, the subspace of W_{p^n} spanned by those derivations $(a_1, \cdots, a_{p^n})$ of W_{p^n} which satisfy equations $\mathscr{L}^*(m')$ for all m', $|\, m' \,| \leqq p^n - 1$, is a Lie algebra, which we shall denote by R.

Let i be an arbitrary index > 1. Then there exists a minimal r for which $i_r > 0$, and it is then easily verified that $i \curlyvee^r i - 1$, so that by (7), $\{i, i-1\}$ on A^r_{-1} has value $i_r \neq 0$. We define the n derivation vectors

$$E_\rho = (0, t^2_\rho x_1, \cdots, t^i_\rho x_{i-1}, \cdots, t^{p^n}_\rho x_{p^n-1}) \quad (\rho = 0, \cdots, n-1), \tag{22}$$

where the coefficients t^μ_ρ in F are such that the associated matrix (2) of E_ρ is A^ρ_{-1}. Thus E_ρ belongs to R and in particular, for $\rho = r$, we have $t^i_r = i_r \neq 0$.

To simplify the notation, let the generator

$$x_{N_j} = Z_j \qquad (j = 0, 1, \cdots, n), \tag{23}$$

and let the subalgebra $F[Z_0, \cdots, Z_n]$ of B_{p^n} be denoted by C_n.

LEMMA 3.1. *Let ϕ be an arbitrary monomial of degree ρ in C_n. Then for every index i, R contains a derivation $a^i(\phi) = (a^i_1, \cdots, a^i_{p^n})$ with $a^i_i = \phi$, where $a^i_j = 0$ for $j > i$, and a^i_j, for $j < i$, is a homogeneous ρth degree polynomial in B_{p^n}.*

Proof. We prove this by induction on i. Let $i = 1$; we show $a^1(\phi) = (\phi, 0, \cdots, 0)$ satisfies equations $\mathscr{L}^*(m')$. If $m' \neq N_j - 1$ for $j = 0, 1, \cdots, n$, these equations are trivially satisfied. Let first $m' = N_k - 1$ for $k < n$. Then the function

$$\theta_j(m') = \{N_j - N_k + 1, N_j\}$$

is nonzero on $a^1(\phi)$ only if $j = k$, and then $\theta_k(m') = \partial\phi/\partial Z_k$. Now for $t = 1$, $\{t, t + m'\} = \{1, N_k\} = \partial\phi/\partial Z_k$ on $a^1(\phi)$; since $t = 1$, $1 \curlyvee N_k$, and by (14), (17) the coefficient of $\theta_k(m')$ is given by $-((1 + m')_k + 1) = -((N_k)_k + 1) = 1$. Hence for $t = 1$, equations $\mathscr{L}^*(N_k - 1)$ are satisfied for all $k < n$. For $t > 1$, $\{t, t + m'\} = 0$, while the coefficient of $\theta_k(m')$, given by either (14) or (15), vanishes, since $t + m' = t + N_k - 1 > N_k$ implies that $(t + m')_k = p - 1$. Hence equations $\mathscr{L}^*(N_k - 1)$ are satisfied for all $k < n$. Finally let $m' = N_n - 1$. Then $\theta_j(N_n - 1)$ is undefined for $j < n$, $\theta_n(N_n - 1) = \partial\phi/\partial Z_n$ on $a^1(\phi)$. If $t + m' \leqq p^n$, t can only equal 1, $1 \curlyvee p^n$, and the coefficients

$$\lambda_k(1, N_n - 1) = -[(N_n)_k + 1] = 0$$

for $k = 0, 1, \cdots, n^- - 1$. Thus both sides of (14) equal $\partial\phi/\partial Z_n$, and we have proved the lemma for $i = 1$.

Assume the lemma valid for $i \geqq 1$, and let r be minimal with $(i+1)_r \neq 0$. Then by (22) the derivation b obtained from the product

$$E_r(a_1, \cdots, a_{i-1}, \phi, 0, \cdots, 0)$$

has components $b_{i+1} = (i+1)_r \phi$, $b_j = 0$ for $j > (i+1)$. Moreover, if all a_j are homogeneous ρth degree polynomials, it is obvious from (1) and (22) that all b_j, for $j < (i+1)$ also have that property.

LEMMA 3.2. *Let $0 \neq a = (a_1, \cdots, a_{p^n})$ belong to R. If i is the maximal index for which $a_i \neq 0$, then $a_i \in C_n$.*

Proof. We prove this by induction on $-i$. Let first $i = p^n$, $a_{p^n} \neq 0$. Then we have $p^n \curlyvee j$ or $p^n \curlyvee^k j$ only if $j = N_n$ or N_k, $k < n$; that is, by (16), $\{p^n, j\} = 0$ unless $j = N_\rho$, $\rho = 0, 1, \cdots, n$, and $a_{p^n} \in C_n$.

Assume the statement for an arbitrary index $i > 1$. Then if $i_r > 0$, and r is minimal with that property, and $(a_1, \cdots, a_{i-1}, 0, \cdots, 0)$ belongs to R, the product

$$b = E_r(a_1, \cdots, a_{i-1}, 0, \cdots, 0)$$

has components $b_i = i_r a_{i-1}$, $b_j = 0$, $j > i$, by (22). Hence if $a_{i-1} \neq 0$, $a_{i-1} \in C_n$, the induction is valid and the lemma holds for all $1 \leqq i \leqq p^n$.

If b is in B_{p^n}, let the C_n-projection of b denote the partial sum of polynomials in $Z_0, Z_1, \cdots, Z_n$ in the polynomial expansion of b. Denote by U_n the ideal of B_{p^n} spanned by polynomials whose C_n-projection is zero. Then if b is in U_n, so is $\partial b/\partial Z_\mu$ for $\mu = 0, 1, \cdots, n$.

If ϕ is an arbitrary monomial in C_n of degree ρ, let

$$D_i(\phi) = (a_1, \cdots, a_{i-1}, \phi, 0, \cdots, 0) \qquad (i = 1, \cdots, p^n), \tag{24}$$

where the ρth degree homogeneous polynomials

$$a_\mu \in U_n \qquad (\mu = 1, \cdots, i-1). \tag{25}$$

That such a derivation exists in R follows directly from Lemma 3.1; while its uniqueness is a consequence of Lemma 3.2. Since for each i, there are p^{n+1} linearly independent $D_i(\phi)$, we have proved

THEOREM 3.1. *The algebra R is p^{2n+1}-dimensional over F, and is spanned by derivations $D_i(\phi)$, given by* (24), (25), *for all monomials ϕ in C_n, and all indices i.*

By extension, if

$$\phi = \phi_1 + \cdots + \phi_k,$$

for monomials ϕ_j in C_n, we let

$$D_i(\phi) = D_i(\phi_1) + \cdots + D_i(\phi_k).$$

LEMMA 3.3. *Let i, j, k be arbitrary indices with $i + j - k = N_r$, $r < n$. Then either $i_r = j_r = p - 1$, or:*

$$k \curlyvee i \text{ or } k \curlyvee^r i \Leftrightarrow k \curlyvee j \text{ or } k \curlyvee^r j \Leftrightarrow \begin{cases} i_\mu + j_\mu \geqq p - 1 & (\mu \neq r), \\ i_r + j_r \geqq p - 2. \end{cases}$$

Proof. We write $k = i + j - N_r$ as the sum

$$1 + \sum_{\mu \neq r} [\, i_\mu + j_\mu - (p-1) \,] p^\mu + [\, i_r + j_r - (p-2) \,] p^r.$$

Then clearly we have

$$\begin{aligned} (26) \qquad k_\mu \leqq i_\mu \text{ (all } \mu < r) &\Leftrightarrow k_\mu = i_\mu + j_\mu - (p-1) && \text{(all } \mu < r) \\ &\Leftrightarrow i_\mu + j_\mu \geqq p - 1 && \text{(all } \mu < r). \end{aligned}$$

Suppose i_r and j_r are not both $p - 1$; then $i_r + j_r - (p-2) < p$, and if constraints (26) hold, we have additionally

$$k_r \leqq i_r + 1 \Leftrightarrow k_r = i_r + j_r - (p-2) \Leftrightarrow i_r + j_r \geqq p - 2.$$

Moreover, if $k_r \leqq i_r + 1$, then clearly the three sets of constraints given in (26) are also equivalent for all $\mu > r$. The lemma then follows by interchanging i and j in these relations. By similar elementary considerations we obtain

LEMMA 3.4. *Let i, j, k be arbitrary indices with $i + j - k = N_n$. Then*

$$k \curlyvee i \Leftrightarrow k \curlyvee j \Leftrightarrow i_\mu + j_\mu \geqq p - 1 \qquad (\textit{all } \mu).$$

We are now ready to determine the multiplication table of R in the following

THEOREM 3.2. *If $D_i(\phi)$, $D_j(\chi)$ are elements of R, then their product is given by*

$$\begin{aligned} D_i(\phi) D_j(\chi) &= D_{i+j-N_r}(\psi_r) \quad \textit{if} \begin{cases} i_\mu + j_\mu \geqq p - 1 & (\mu \neq r), \\ i_r + j_r = p - 2, \end{cases} \\ &= \sum_{\rho=0}^{n} D_{i+j-N_\rho}(\psi_\rho) \quad \textit{if } i_\mu + j_\mu \geqq p - 1 \qquad (\textit{all } \mu), \\ &= 0 \quad \textit{otherwise}, \end{aligned}$$

where

$$(27) \qquad \begin{cases} \psi_\rho = -(j_\rho + 1) \dfrac{\partial \phi}{\partial Z_\rho} \chi + (i_\rho + 1) \dfrac{\partial \chi}{\partial Z_\rho} \phi & (\rho < n), \\ \psi_n = \left[\sum_{\mu=0}^{n-1} (j_\mu + 1) + 1 \right] \dfrac{\partial \phi}{\partial Z_n} \chi - \left[\sum_{\mu=0}^{n-1} (i_\mu + 1) + 1 \right] \dfrac{\partial \chi}{\partial Z_n} \phi. \end{cases}$$

Proof. We note first that if $i_\mu + j_\mu \geqq p - 1$ for all μ, it follows that $i + j \geqq N_n + 1$, so that $D_{i+j-N_\rho}(\psi_\rho)$ is defined for all ρ. Similarly, if $i_\mu + j_\mu \geqq p - 1$ for $\mu \neq r$, $i_r + j_r = p - 2$, then $i + j > N_r$ and $D_{i+j-N_r}(\psi_r)$ is defined.

To prove the theorem, let $D_i(\phi) = (a_1, \cdots, a_i, 0, \cdots, 0) = a$, $D_j(\chi) = (b_1, \cdots, b_j, 0, \cdots, 0) = b$, with $a_i = \phi$, $b_j = \chi$. Then by (1), the product $D_i(\phi)D_j(\chi)$ is a vector with components

$$c_k = \sum_{\mu=1}^{p^n} \left[\frac{\partial a_k}{\partial x_\mu} b_\mu - \frac{\partial b_k}{\partial x_\mu} a_\mu \right] \qquad (k = 1, \cdots, p^n).$$

And if we denote this product in R by

$$\sum_{k=1}^{p^n} D_k(\eta_k),$$

for polynomials η_k in C_n, we see by (24) and (25) that η_k is equal to the C_n-projection of c_k. Since by (25), b_μ, for $\mu \neq j$, a_μ, for $\mu \neq i$, are in U_n, the C_n-projections of c_k and of

$$\frac{\partial a_k}{\partial x_j}\chi - \frac{\partial b_k}{\partial x_i}\phi \tag{28}$$

coincide. It follows from equations $\mathscr{L}^*(j-k)$ that for every element in R, the function $\{k,j\}$ is either zero or equal to a linear combination of functions

$$\theta_\rho(j-k) = \{N_\rho - (j-k), N_\rho\} \qquad (\rho = 0, 1, \cdots, n). \tag{29}$$

If $N_\rho - (j-k) \neq i$, the function $\theta_\rho(j-k)$ assumes at the element $D_i(\phi)$ a value in U_n. Thus, if $k \neq i + j - N_\rho$ for any ρ, the function $\{k,j\}$ of a is in U_n. By interchanging i and j, a and b, it follows symmetrically, in that case, that $\partial b_k/\partial x_i$ must also be in U_n. But then the C_n-projection of (28) is zero, and $\eta_k = 0$ for $k \neq i + j - N_\rho$.

Consider next an index

$$k = i + j - N_r, \qquad 0 \leqq r < n.$$

Then $N_r - (j-k) = i$, and the C_n-projection of $\partial a_k/\partial x_j$ is equal to the value of the function

$$-\lambda_r(k, j-k)\{i, N_r\} \tag{30}$$

at $D_i(\phi)$ so long as $k \curlyvee j$ or $k \curlyvee^r j$, and is zero otherwise. In the first case by (17), $\lambda_r(k, j-k) = j_r + 1$, and (30) becomes

$$-(j_r + 1)\frac{\partial \phi}{\partial Z_r}. \tag{31}$$

By symmetry, the C_n-projection of $\partial b_k/\partial x_i$ is equal to

$$-(i_r + 1)\frac{\partial \chi}{\partial Z_r} \tag{32}$$

so long as $k \curlyvee i$ or $k \curlyvee^r i$, and is zero otherwise. In case both $i_r = j_r = p-1$, the C_n-projection of (28) is therefore zero under all conditions so that $\eta_k = \eta_{i+j-N_r}$

and the polynomial ψ_r given by (27) both vanish. If i_r and j_r are not both $p-1$, owing to Lemma 3.3 we conclude from (28), (31), (32) that η_{i+j-N_r} is equal to ψ_r in (27), so long as $i_\mu + j_\mu \geqq p-1$ for $\mu \neq r$, $i_r + j_r \geqq p-2$, and is zero otherwise.

Finally, let $k = i + j - N_n$. Then the C_n-projection of $\partial a_k / \partial x_j$ is given by the value of the function

$$\left[1 + \sum_{\mu=0}^{n-1} \lambda_\mu(k, j-k)\right] \{i, N_n\} \tag{33}$$

at $D_i(\phi)$ so long as $k \vee j$, and is zero otherwise. In the first instance, since $\lambda_\mu(k, j-k) = j_\mu + 1$, this value becomes

$$\left[\sum_{\mu=0}^{n-1} (j_\mu + 1) + 1\right] \frac{\partial \phi}{\partial Z_n}. \tag{34}$$

By symmetry, the C_n-projection of $\partial b_k / \partial x_i$ is obtained from (34) by interchanging i and j and replacing ϕ by χ, so long as $k \vee i$, and vanishes otherwise. Owing to Lemma 3.4, we conclude that η_{i+j-N_n} is given by the polynomial ψ_n in (27) so long as $i_\mu + j_\mu \geqq p-1$ for all μ, and is zero otherwise.

Now the pair of indices i and j satisfies one and only one of the following three alternatives: Either $i_\mu + j_\mu \geqq p-1$ for all μ; or $i_k + j_k = p-2$ for some $0 \leqq k \leqq n-1$, while $i_\mu + j_\mu \geqq p-1$ for $\mu \neq k$; or constraints $i_\mu + j_\mu \geqq p-1$, $\mu \neq k$, $i_k + j_k \geqq p-2$ are not feasible for any $0 \leqq k \leqq n-1$. Recapitulating all previous results in this light, we obtain the statement of the theorem.

4. **Simplicity.** To prove the simplicity of R we start with a tool lemma; we denote by Z the maximum degree monomial $(Z_0 Z_1 \cdots Z_n)^{p-1}$ in C_n, and we let

$$L_k$$

denote the subspace of R spanned by all $D_j(\phi_j)$ with $j \leqq k$. Also we denote by

$$I = (x_1, \cdots, x_{p^n})$$

the derivation in R whose associated matrix (2) is the identity matrix.

LEMMA 4.1. *If $D_i(\phi)$ is a basis element of R, let $r \leqq n-1$ be minimal with the property that $(i+1)_r > 0$, and let ϕ be a monomial in C_n of degree ρ. Then*

$$D_i(\phi)\Delta_{N_\mu} = D_i(\partial\phi / \partial Z_\mu) \qquad (\mu = 0, 1, \cdots, n), \tag{35}$$

$$D_i(\phi)I = (\rho - 1)D_i(\phi), \tag{36}$$

$$D_i(\phi)E_r + (i+1)_r D_{i+1}(\phi) \in L_i, \tag{37}$$

and in particular

$$D_i(Z)E_r = -(i+1)_r D_{i+1}(Z) + \sum_{\mu \leqq i} \gamma_\mu D_\mu(Z) \quad (\text{some } \gamma_\mu \text{ in } F), \tag{38}$$

where E_r is the element in R given by (22) (5).

(5) It is easy to show that $E_r = -D_{N_r+1}(Z_r)$.

Proof. Relation (35) is an immediate consequence of Theorem 3.1. As for relation (36), it follows directly from (1) and the fact that all components of $D_i(\phi)$ are homogeneous polynomials in B_{p^n} of degree ρ. While relations (37) and (38) are based on (1) and (22), and the fact that Z is the only monomial of maximum degree in C_n.

LEMMA 4.2. *If p divides $n+2$, the algebra R^2 does not contain $D_1(Z)$, but contains every other element $D_i(\phi)$, with ϕ a monomial in C_n.*

Proof. Let $a=(a_1,\cdots,a_{p^n})$, $b=(b_1,\cdots,b_{p^n})$ be two arbitrary derivations in R. Then $ab=c=(c_1,\cdots,c_{p^n})$ with

$$c_1=\sum_{m'=0}^{p^n-1}\left[\frac{\partial a_1}{\partial x_{1+m'}}\,b_{1+m'}-\frac{\partial b_1}{\partial x_{1+m'}}\,a_{1+m'}\right]. \tag{39}$$

Let $m=m'+1$. Now $1\curlyvee 1+m'$ for all $0\leqq m'\leqq p^n-1$, and by (14) the function $\{1,1+m'\}$ is equal to the linear combination of functions

$$\left[\sum_{k=0}^{n-1}(m_k+1)+1\right]\{N_n-m',N_n\}-\sum_{k=0}^{n-1}(m_k+1)\,\{N_k-m',N_k\}$$

on all derivations in R. Substituting this back in (39) for the particular derivations a and b we have

$$\begin{aligned}c_1=&\sum_{m'=0}^{p^n-1}\left[\sum_{k=0}^{n-1}(m_k+1)+1\right]\left[\frac{\partial a_{N_n-m'}}{\partial Z_n}\,b_{m'+1}-\frac{\partial b_{N_n-m'}}{\partial Z_n}\,a_{m'+1}\right]\\&-\sum_{m'=0}^{p^n-1}\sum_{k=0}^{n-1}(m_k+1)\left[\frac{\partial a_{N_k-m'}}{\partial Z_k}\,b_{m'+1}-\frac{\partial b_{N_k-m'}}{\partial Z_k}\,a_{m'+1}\right].\end{aligned} \tag{40}$$

Let $\mu_i=p-1-m_i$, and define the index $\mu=[\mu_0,\cdots,\mu_{n-1}]$; then $\mu+m=p^n+1$ and we let $\mu'=\mu-1=(p^n-1)-m'$. We note that since $n+2\equiv 0 \pmod p$, the following identity holds in F:

$$\sum_{k=0}^{n-1}(m_k+1)+1=-\left[\sum_{k=0}^{n-1}(\mu_k+1)+1\right].$$

The first summation term of c_1 can thus be written as

$$\begin{aligned}&\sum_{m'=0}^{p^n-1}\left[\sum_{k=0}^{n-1}(m_k+1)+1\right]\frac{\partial a_{N-m'}}{\partial Z_n}\,b_{m'+1}\\&+\sum_{\mu'=0}^{p^n-1}\left[\sum_{k=0}^{n-1}(\mu_k+1)+1\right]\frac{\partial b_{\mu'+1}}{\partial Z_n}\,a_{N-\mu'},\end{aligned}$$

which is equal to

$$\sum_{m'=0}^{p^n-1}\left[\sum_{k=0}^{n-1}(m_k+1)+1\right]\frac{\partial}{\partial Z_n}(a_{N_n-m'}b_{m'+1}). \tag{41}$$

If $m' + 1 > N_k$ for $k < n$, then $m_k = p - 1$. Hence the second summation term of c_1 can be expressed as

$$\Sigma_0 + \Sigma_1 + \cdots + \Sigma_{n-1}, \tag{42}$$

where

$$\Sigma_k = \sum_{m'=0}^{N_k - 1} (m_k + 1) \left[\frac{\partial a_{N_k - m'}}{\partial Z_k} b_{m'+1} - \frac{\partial b_{N_k - m'}}{\partial Z_k} a_{m'+1} \right].$$

Define the index $v = [v_0, \cdots, v_k, \cdots, v_{n-1}] = N_k + 1 - m$, and let $v' = v - 1$. Since over $F, m_k + 1 = -(v_k + 1)$, we can write

$$\begin{aligned} \sum_k &= \sum_{m'=0}^{N_k - 1} (m_k + 1) \frac{\partial a_{N_k - m'}}{\partial Z_k} b_{m'+1} \\ &\quad + \sum_{v'=0}^{N_k - 1} (v_k + 1) \frac{\partial b_{v'+1}}{\partial Z_k} a_{N_k - v'} \\ &= \sum_{m'=0}^{N_k - 1} (m_k + 1) \frac{\partial (a_{N_k - m'} b_{m'+1})}{\partial Z_k} \\ &\qquad (k = 0, 1, \cdots, n-1). \end{aligned} \tag{43}$$

We conclude from (40), (41), (43), that the coefficient of Z in the polynomial expansion of c_1 is necessarily zero.

Owing to relation (35) it is clear that R^2 contains all $D_i(\phi)$ for all monomials ϕ in C_n distinct from Z; while since $\gamma_1 \equiv 0$ in (38), it follows that $D_j(Z)$ is in R^2 for $j > 1$. This completes the proof of the lemma, and we can establish

THEOREM 4.1. *If p does not divide $n + 2$, R is a central simple p^{2n+1}-dimensional algebra. If p divides $n + 2$, then R^2 is central simple and has dimension $p^{2n+1} - 1$ over F.*

Proof. Let $\mathfrak{A}$ be a nonzero ideal of R. Then by (1), through successive multiplications by suitable Δ_i, we obtain a nonzero element d in $\mathfrak{A}$ whose components are all in F. If for some $0 \leqq j \leqq n$, the N_j-component of d is $\lambda \neq 0$ in F, then $\lambda^{-1} D_1(Z_j) d = \Delta_1$ is in $\mathfrak{A}$ by (1). If all N_j-components of d are zero, then its i-component is nonzero for some maximal $i < N_0$, and repeated multiplications by suitable derivations E_r given by (22), yield, by (1), a vector d' in $\mathfrak{A}$ whose components are all in F and whose N_0-component is nonzero. Thus $\mathfrak{A}$ contains $\Delta_1 = D_1(1)$; but then multiplication by $E_0, E_1, \cdots, E_{n-1}$ generate in turn all derivations $\Delta_j = D_j(1)$ for $j = 2, \cdots, p^n$. Thus $\mathfrak{A}$ contains all Δ_j and hence by (35) all $D_j(\phi)$ for monomials ϕ in C_n distinct from Z.

Now the degree of Z is $(n + 1)(p - 1)$ which is congruent to one only if p divides $n + 2$. Hence if $p \nmid n + 2$, by (36), since $I \in \mathfrak{A}$, the product

$D_j(Z)\, I = -(n+2)\, D_j(Z)$ is in $\mathfrak{A}$, $D_j(Z)$ is in $\mathfrak{A}$ for all indices j, $R = R^2$, and R is simple and clearly central simple.

Assume $p \mid n+2$ and let $\mathfrak{A}$ be a nonzero ideal in R^2. It follows as before that $\mathfrak{A}$ contains all Δ_j, and hence also $D_j(\phi)$ for monomials ϕ in C_n distinct from Z if $j > 1$, and $D_1(\phi)$ for monomials ϕ distinct from Z or $\partial Z/\partial Z_\mu$ for any μ. Since $p > 2$, and $n \geqq 1$, $\mathfrak{A}$ contains in particular the elements I and E_ρ for $\rho = 0,1,\cdots,n-1$. The degree of $\partial Z/\partial Z_\mu$ being $\equiv 0 \pmod p$, we can then conclude from (36) that all $D_1(\partial Z/\partial Z_\mu)$ belong to $\mathfrak{A}$. We must now show that $D_j(Z) \in \mathfrak{A}$ for $j \geqq 2$.

By Theorem 3.2, we write

$$D_1(\partial Z/\partial Z_0)\, D_{N_n}(Z_0^2) = D_1(\psi_n) + D_2(\psi_0) + \sum_{0<\rho<n} D_{N_n - N_\rho + 1}(\psi_\rho) \tag{44}$$

where, by Lemma 4.2, ψ_n being of maximum degree in C_n, must vanish identically. Moreover, since $(\partial^2 Z/\partial Z_0 \partial Z_\rho) Z_0^2 = \partial Z_0^2/\partial Z_\rho = 0$ for $\rho \neq 0$, we have

$$\psi_\rho = \psi_n = 0 \qquad (0 < \rho < n). \tag{45}$$

Finally, since $(N_n)_0 + 1 = p$, and $(1)_0 + 1 = 1$, by (27),

$$\psi_0 = [\partial Z_0^2/\partial Z_0]\,[\partial Z/\partial Z_0] = -2Z. \tag{46}$$

As the left expression of (44) is in $\mathfrak{A}$, it follows that $D_2(Z)$ is also in $\mathfrak{A}$, and from (38) with $\gamma_1 = 0$ by Lemma 4.2, we can conclude that $\mathfrak{A}$ contains all $D_j(Z)$, $j \geqq 2$. Thus $R^2 = \mathfrak{A}$, and R^2 is simple and clearly also central simple.

5. **Derivation algebras.** In this section we shall follow the technique of Block([6]) and distinguish R and R^2 from certain known algebras by exhibiting differences in their respective derivation algebras. In order to show that every derivation of R is inner, we need a few preliminary definitions and lemmas. To simplify the notation we shall at first obtain general results by considering subalgebras of W_n for $n \geqq 1$ arbitrary.

If Q is a subalgebra of W_n and x in W_n is such that $Qx \subseteq Q$, we denote by $ad\,(x)$, the derivation of Q over F: $d \in Q \to dx$. We shall say that two derivations Δ, $\bar{\Delta}$ of Q are equivalent, and write $\Delta \equiv \bar{\Delta}$, if $\Delta - \bar{\Delta} = ad(x)$ for some x in Q.

Denote by Q_ρ for $\rho = 0,1,\cdots,m$ the subspaces of Q generated by all vectors $(a_1,\cdots,a_n)$ with the property that $a_1,\cdots,a_n$ are all homogeneous polynomials in B_n of identical degree ρ. If $Q_m \neq 0$, $Q_{m+1} = 0$, we say that m is the maximum degree of Q.

Similarly, denote by Q_ρ^* for $\rho = 0,1,\cdots,p-1$, the subspace

$$Q_\rho + Q_{p+\rho} + \cdots + Q_{kp+\rho}, \tag{47}$$

where $kp + \rho \leqq m$, $(k+1)\,p + \rho > m$. Then by (1), we have

([6]) Cf. [2].

$$Q_i^* Q_j^* \subseteq \begin{cases} Q_{i+j-1}^* & \text{if } i+j-1 < p, \\ Q_{i+j-(p+1)}^* & \text{otherwise.} \end{cases} \tag{48}$$

The algebra Q will be called *admissible* if it can be expressed as a vector direct sum

$$Q = Q_0 + Q_1 + \cdots + Q_m, \tag{49}$$

and if moreover Q_0 is n-dimensional over F.

We shall say that a polynomial in B_n is *truncated in* x_j, if the x_j-exponent of all its monomials with nonzero coefficients is inferior to $p-1$. By extension, a vector in W_n will be *truncated in* x_j if all its components are.

LEMMA 5.1. *Let Q be an admissible subalgebra of W_n containing the "identity" vector $I = (x_1, \cdots, x_n)$. Then every derivation of Q over F is equivalent to a derivation Δ with $(I)\Delta = 0$, $(Q_\rho^*)\Delta \subseteq Q_\rho^*$ for $\rho = 0, 1, \cdots, p-1$, and $(\Delta_i)\Delta$ truncated in x_i for $i = 1, \cdots, n$.*

Proof. It follows directly from (1) that

$$b^\rho I = (\rho - 1) b^\rho \Leftrightarrow b^\rho \in Q_\rho^* \qquad (\rho = 0, 1, \cdots, p-1). \tag{50}$$

If Δ is a derivation of Q, by (47), (49) we can write $(I)\Delta = \sum_{\rho=0}^{p-1} a^\rho$ for elements a^ρ in Q_ρ^*; then letting

$$a = -\sum_{\rho \neq 1} (\rho - 1)^{-1} a^\rho,$$

we have

$$(I)(\Delta - ad(a)) \in Q_1^*. \tag{51}$$

Let $\bar{\Delta} = \Delta - ad(a)$; then $\Delta \equiv \bar{\Delta}$, and if b^0 is an arbitrary element of Q_0^*, we have $I\, b^0 = b^0$,

$$(I)\bar{\Delta} b^0 = (b^0)\bar{\Delta} - I((b^0)\bar{\Delta}). \tag{52}$$

By (51) the left side expression is in Q_0^*, but by (50) the projection of the right side expression on Q_0^* is zero. Hence, $(I)\,\bar{\Delta}\, b^0 = 0$ for all b^0 in Q_0^*, and in particular $((I)\bar{\Delta})\Delta_j = 0$ for $j = 1, \cdots, n$ so that $(I)\bar{\Delta} \in Q_0$. By (51), this is impossible unless $(I)\bar{\Delta} = 0$. For ρ arbitrary, b^ρ in Q_ρ^*, applying $\bar{\Delta}$ to both sides of the equation of (50), we have

$$(b^\rho)\bar{\Delta}\, I = (\rho - 1)\,(b^\rho)\bar{\Delta}$$

and again it follows from (50) that $(b^\rho)\bar{\Delta} \in Q_\rho^*$, $(Q_\rho^*)\bar{\Delta} \subseteq Q_\rho^*$.

We finally show that $(\Delta_j)\bar{\Delta}$ is truncated in x_j. Since $\Delta_i \Delta_j = 0$ for all i, j, we have at once

$$(\Delta_i)\bar{\Delta}\Delta_j = (\Delta_j)\bar{\Delta}\Delta \qquad (\text{all } i, j). \tag{53}$$

Suppose $(\Delta_j)\bar{\Delta} = (b_1, \cdots, b_n) = b$. Then by (53)

$$\frac{\partial b_\mu}{\partial x_i} = \frac{\partial c_{\mu i}}{\partial x_j} \qquad (i, \mu = 1, \cdots, n), \tag{54}$$

for elements $c_{\mu i}$ in B_n. If for some $1 \leqq \mu \leqq n$, b_μ is not truncated in x_j, let ϕ be a monomial of the form $x_j^{p-1}\psi$, ψ in $F[x_1, \cdots, x_{j-1}, x_{j+1}, \cdots, x_n]$, whose coefficient in the expansion of b_μ is nonzero. Then by (54), $\partial\psi/\partial x_i = 0$ for $i \neq j$, that is, $\psi \in F$, but then ϕ is of degree $p-1$, $b \in Q_{p-1}^*$ in contradiction with the fact that $b \in Q_0^*$. Hence $(\Delta_j)\bar{\Delta}$ is truncated in x_j for every j.

LEMMA 5.2. *Let Q be an admissible subalgebra of W_n, and let Δ be a derivation of Q such that $(Q_\rho^*)\Delta \subseteq Q_\rho^*$, $\rho = 0, 1, \cdots, p-1$. Then there exists an element e in $(W_n)_1$ such that $Q_1\, e \subseteq Q_1$, and such that the projection of $e\Delta_i - (\Delta_i)\Delta$ on Q_0 is zero for $i = 1, \cdots, n$.*

Proof. By assumption, we have

$$(\Delta_i)\Delta = \sum_{j=1}^{n} e_{ij}\Delta_j + \alpha_i \quad (i = 1, \cdots, n), \tag{55}$$

where α_i in Q_0^* has zero projection on Q_0, and the matrix $E = (e_{ij})$ is in F_n.

Let $D = (d_{ij})$ be a matrix in F_n such that the vector

$$d = \left(\sum_{j=1}^{n} d_{1j}x_j, \cdots, \sum_{j=1}^{n} d_{nj}x_j \right)$$

is in Q_1; then again by assumption, $(d)\Delta \in Q_1^*$,

$$(d)\Delta = \left(\sum_{j=1}^{n} g_{1j}x_j, \cdots, \sum_{j=1}^{n} g_{nj}x_j \right) + \beta, \tag{56}$$

where the first vector is in Q_1, and β in Q_1^* has zero projection on Q_1. Then we can write $(d\Delta_k)\Delta = \sum_{j=1}^{n} d_{jk}(\Delta_j)\Delta$ also as the sum, $(d)\Delta\Delta_k + d((\Delta_k)\Delta)$. Substituting (55) and (56) in these expressions, we obtain the equation

$$\sum_{j\mu} d_{jk}e_{j\mu}\Delta_\mu + \eta = \sum_i g_{ik}\Delta_i + \sum_{j\mu} e_{kj}\, d_{\mu j}\Delta_\mu + \gamma,$$

where γ, η in Q_0^* have zero projection on Q_0. Since the Δ_μ are linearly independent over F, we conclude that for $1 \leqq k \leqq n$,

$$\sum_{j=1}^{n} (d_{jk}\, e_{j\mu} - e_{kj}\, d_{\mu j}) = g_{\mu k} \qquad (\mu = 1, \cdots, n). \tag{57}$$

That is, letting

$$e = \left(\sum_{j=1}^{n} e_{j1}x_j, \cdots, \sum_{j=1}^{n} e_{jn}x_j \right),$$

relation (57), by (1), expresses the fact that $ed \in Q_1$. Since d was arbitrary, we have $eQ_1 \subseteq Q_1$, and moreover by (55), $e\Delta_i - (\Delta_i)\Delta$ has zero projection on Q_0. This completes the proof of the lemma.

As the algebras R and R^2 are, by Theorem 3.1, clearly both admissible, we may apply to them the above two lemmas. But before doing so, we now establish certain specific properties of these algebras which will be needed for the main result of this section.

LEMMA 5.3. *If $e \in (W_{p^n})_1$ is such that $R_1 e \subseteq R_1$, then $e \in R$.*

Proof. We can assume that, modulo R,

$$e = (a_1, \cdots, a_{p^n}),$$

where the components a_i are all homogeneous polynomials of degree one in U_n. Suppose $e \neq 0$, and let the index i be maximal with the property that $a_i \neq 0$. If $i \neq p^n$, let r be minimal with the property that $(i+1)_r \neq 0$. Then by assumption, the product $E_r e$ is in R, where E_r is given by (22). But for $j > i+1$ the j-components of $E_r e$ are zero, while its $(i+1)$-component is equal to $(i+1)_r a_i$ in U_n, in contradiction with Lemma 3.2.

Suppose next that $a_{p^n} \neq 0$, and let the function $\{N_n, k\} = t \neq 0$ on e for some fixed index $k \neq N_0, \cdots, N_n$. Then there exists an r for which $k_r \neq p-1$. Now the "diagonal" vector v in R_1 whose associated matrix is A_0^r, has by (7), $\{i,i\} = i_r$, $\{i,j\} = 0$ for $i \neq j$. Thus by (1), the function $\{N_n, k\}$ on the product ev is given by $t(k_r - (N_n)_r) = t(k_r + 1) \neq 0$. Again by Lemma 3.2, ev cannot be in R, and this contradiction implies that $e = 0$, as required.

LEMMA 5.4. *In the algebra R, the set of indices $J = \{N_n, N_0, N_1, \cdots, N_{n-1}\}$ fulfills the following three conditions:*

(i) $d \neq 0 \in R$, $d\Delta_{N_j} = 0$ $(j = 0, \cdots, n) \Rightarrow d \in R_0$.

(ii) $d \neq 0 \in R_r$, for $r < m \Rightarrow d = \sum d^j$ *with d^j in R_r truncated in Z_j.*

(iii) *If $d \neq 0$ in R_r is truncated in Z_j, and if $d\Delta_{N_i} = 0$ for all N_i in a subset H of J, $N_j \notin H$, then there exists an element c in R_{r+1} with $d = c\Delta_{N_j}$, $c\Delta_{N_i} = 0$ for for all N_i in H.*

Proof. Property (i) follows from Lemma 3.2. Now clearly, the maximum degree m of R is equal to the maximum degree $(n+1)(p-1)$ of polynomials in C_n. If d in R is homogeneous of degree $r < m$, then by Theorem 3.2, d is a linear combination over F of derivations $D_i(\phi_j)$, where each monomial ϕ_j of degree $r < m$ in C_n is necessarily truncated in Z_μ for some $0 \leqq \mu \leqq n$, $\phi_j = \partial\psi_j/\partial Z_\mu$, ψ_j in C_n. Hence by (35), $D_i(\phi_j) = D_i(\psi_j)\Delta_{N_\mu}$, and $D_i(\phi_j)$ is truncated in Z_μ. Thus R has property (ii).

To prove that (iii) holds in R, let d be truncated in Z_j. Again by Theorem 3.2, express d as the sum of basis derivations $D_i(\phi_i)$, where all polynomials ϕ_i in C_n

are necessarily truncated in Z_j. Moreover if $d\Delta_{N\mu} = 0$ for a subset H of J, by (35), $\partial\phi_i/\partial Z_\mu = 0$ for $i = 1, \cdots, p^n$, all μ with N_μ in H. Expand ϕ_i as

$$\phi_{i0} + \phi_{i1}Z_j + \cdots + \phi_{ip-2}Z_j^{p-2},$$

for $\phi_{i\rho}$ in C_n, $\partial\phi_{i\rho}/\partial Z_\mu = \partial\phi_{i\rho}/\partial Z_j = 0$, all μ with N_μ in H, $i = 1, \cdots, p^n$. Then if

$$\psi_i = \phi_{i0}Z_j + \frac{1}{2}\phi_{i1}Z_j^2 + \cdots + \frac{1}{p-1}\phi_{ip-2}Z_j^{p-1},$$

$D_i(\psi_i)\Delta_{N_j} = D_i(\phi_i)$ for $i = 1, \cdots, p^n$, and $D_i(\psi_i)\Delta_{N_\mu} = 0$ for all N_μ in H, by (35), so that $e = \sum_{i=1}^{p^n} D_i(\psi_i)$ is the required element in R.

If $n + 2 \equiv 0\ (p)$, it is clear that properties (i) and (ii) hold for the set of indices J in the algebra R^2. On the other hand, (iii) is valid only in a weakened form. The above argument, associating to an element d truncated in Z_j, and with $d\Delta_{N_\mu} = 0, N_\mu$ in H, an element e in R^2 with $d = e\Delta_{N_j}$ and $e\Delta_{N\mu} = 0$, holds if and only if the polynomial ϕ_1 is not of degree $m - 1$. Indeed if $d = D_1(\partial Z/\partial Z_j)$, no element e in R^2 can be found with the required properties. We can therefore state

LEMMA 5.5. *In the algebra $R^2 \neq R$, the set of indices $J = \{N_n, N_0, \cdots, N_{n-1}\}$ fulfills conditions* (i) *and* (ii) *of Lemma* 5.4 *as well as a third condition*

(iii)′ *If $d = D_1(\phi_1) + \sum_{\mu>1} D_\mu(\phi_\mu)$ is in R^2, and d is truncated in Z_j with $d\Delta_{N_i} = 0$ for all N_i in a subset H of J, and if degree $\phi_1 < m - 1$, then there exists an e in R^2 with $e\Delta_{N_i} = 0$ for all N_i in H, and such that $d = e\Delta_{N_j}$.*

LEMMA 5.6. *In the algebras R or R^2, if d is an element such that*

$$(58)\quad d\ ad(\beta) = d\left[\prod_{i=1}^{r} ad(\alpha_i)\right] ad(\beta) = 0 \quad (\text{all } \alpha_i \text{ in } R_1,\ \text{all } \beta \text{ in } R_2,\ \text{all } r \geqq 1),$$

then $d \in R_m$, where m is the maximum degree of R.

Proof. Let (58) hold for an element

$$d = \sum_i D_i(\phi_i) \neq 0$$

in R. Without loss of generality we can assume d in R_s for some $s \leqq m$. We suppose $s < m$ and arrive at a contradiction.

If $\phi_{p^n} = 0$, by (37) through successive multiplications by elements in R_1 we obtain a derivation whose p^n-component is nonzero. Let us therefore assume $\phi = \phi_{p^n} \neq 0$.

Case I. Suppose $0 \neq \phi \in F[Z_n]$. If f_v is an arbitrary polynomial in $F[Z_v]$, $0 \leqq v \leqq n - 1$, consider the product $dD_{N_n}(f_v)$. By Theorem 3.2, it is easily verified that

$$(59)\qquad dD_{N_n}(f_v) + D_{N_n}\left(\frac{\partial\phi}{\partial Z_n}f_v - \phi_{N_v}\frac{\partial f_v}{\partial Z_v}\right) \in L_{p^n-1}.$$

Since $dx = 0$ for all x in R_2, putting $f_\nu = Z_\nu^2$, it follows from (59) that $2\phi_{N\nu} = (\partial\phi/\partial Z_n)\, Z_\nu$ for $0 \leqq \nu \leqq n-1$. But then, letting $f_\nu = Z_\nu$, we obtain from (59),

$$dD_{N_n}(Z_\nu) + \frac{1}{2} D_{N_n}\left(\frac{\partial\phi}{\partial Z_n} Z_\nu\right) \in L_{p^n-1}.$$

Since clearly $s \neq 0$, $(\partial\phi/\partial Z_n)\, Z_\nu$ is nonzero and not in $F[Z_n]$, and we are reduced to

Case II. Suppose $\phi \notin F[Z_n]$. Let $\mu \leqq n-1$ be such that $\partial\phi/\partial Z_\mu = \bar{\phi} \neq 0$. Since $\bar{\phi}$ is of degree $s-1 \leqq m-2$, $\bar{\phi} Z_\sigma Z_\tau \neq 0$ for some $0 \leqq \sigma, \tau \leqq n$. We will now show the product $dD_{N_\mu}(Z_\sigma Z_\tau)$ to be nonzero. Indeed, by Theorem 3.2, we see that $D_{N_n}(\phi) D_{N_\mu}(Z_\sigma Z_\tau)$ has its p^n-component equal to $\bar{\phi} Z_\sigma Z_\tau \neq 0$. For $j < N_n$, consider the remaining products

$$D_j(\phi_j) D_{N_\mu}(Z_\sigma Z_\tau). \tag{60}$$

If there is no ν for which $j + N_\mu - N_\nu = N_n$, the above expression clearly belongs to L_{p^n-1}. While if $j = N_n - N_\mu + N_\nu = p^n + p^\mu - p^\nu$, write

$$j = [\, p-1, \cdots, p-1, \underset{\mu}{0}, \cdots, 0, \underset{\nu}{p-1}, \cdots, p-1\,] \qquad (\mu < \nu < n), \tag{61}$$

then $j_\mu + (N_\mu)_\mu = p-2$, and it follows by Theorem 3.2 that expression (60) is equal to a derivation $D_j(\psi_\mu)$ also in L_{p^n-1}, since $j < N_n$. Thus the p^n-component of the product $dD_{N_\mu}(Z_\sigma Z_\tau)$ is nonzero, in contradiction with our hypothesis, and d must belong to R_m as required. This completes the proof of the lemma.

The main result of this section is now relatively easy to establish.

THEOREM 5.1. *Every derivation of R over F is inner.*

Proof. Let Δ be a derivation of R. Owing to Lemma 5.1, we can assume that $(R_\rho^*)\Delta \subseteq R_\rho^*$ for $\rho = 0, \cdots, p-1$, and that $(\Delta_i)\Delta$ is truncated in x_i for all indices i.

We show by induction that for $j = 0, 1, \cdots, n$, there exist elements a^j in R_1^* such that the derivation of R

$$\delta^j = \Delta + ad(a^j)$$

satisfies

$$(\Delta_{N_\mu})\delta^j = 0 \qquad (\mu = 0, \cdots, j). \tag{62}$$

For $j = 0$, since $(\Delta_{N_0})\Delta$ is truncated in Z_0, by condition (iii) of Lemma 5.4, there exists an element a^0 in R_1^* with $(\Delta_{N_0})\Delta = a^0 \Delta_{N_0}$ in R_0^*. Assume the existence of such a^j for $j \leqq k$, $k \geqq 0$. Since $a^k \in R_1^*$, $(R_\rho^*)\delta^k \subseteq R_\rho^*$ for $\rho = 0, \cdots, p-1$. By (62), $(\Delta_{N_\mu})\delta^k = 0$ for $\mu = 0, \cdots, k$, so that

$$0 = (\Delta_{N_\mu} \Delta_{N_{k+1}})\delta^k = ((\Delta_{N_{k+1}})\delta^k)\Delta_{N_\mu} \qquad (\mu = 0, \cdots, k).$$

Since $(\Delta_{N_{k+1}})\delta^k$ is truncated in Z_{k+1}, condition (ii) of Lemma 5.4 ensures the existence of an element $\hat{a}^{k+1}$ in R_1^* with

$$\hat{a}^{k+1} \Delta_{N_{k+1}} = (\Delta_{N_{k+1}})\delta^k, \qquad \hat{a}^{k+1} \Delta_{N_\mu} = 0 \qquad (\mu = 0, \cdots, k).$$

Let $a^{k+1} = a^k + \hat{a}^{k+1}$. Then $\delta^{k+1} = \Delta + ad\,(a^{k+1})$ satisfies condition (62) for $\mu = 0, \cdots, k+1$ and the induction is valid. Let $\delta^n = \bar{\Delta}$. Then $\Delta \equiv \bar{\Delta}$, and

$$(\Delta_{N_j})\bar{\Delta} = 0 \qquad (j = 0, \cdots, n).$$

Since for k arbitrary, we have

$$0 = (\Delta_{N_j}\Delta_k)\bar{\Delta} = [(\Delta_k)\bar{\Delta}]\Delta_{N_j} \qquad (j = 0, \cdots, n),$$

it follows by condition (i) of Lemma 5.4 that $(\Delta_k)\bar{\Delta} \in R_0$ for $k = 1, \cdots, p^n$. Since $a^n \in R_1^*$, $(R_\rho^*)\bar{\Delta} \subseteq R_\rho^*$ for $\rho = 0, 1, \cdots, p-1$, and applying Lemma 5.2 to the derivation $\bar{\Delta}$, we know there exists an element e in $(W_{p^n})_1$ with $R_1 e \subseteq R_1$ and

$$e\Delta_k = (\Delta_k)\bar{\Delta} \qquad (k = 1, \cdots, p^n).$$

By Lemma 5.3 e must be in R_1 and if we let

$$\Delta^* = \bar{\Delta} + ad(e),$$

$\Delta^* \equiv \Delta$, $(\Delta_k)\Delta^* = 0$ for $k = 1, \cdots, p^n$ and $(R_\rho^*)\Delta^* \subseteq R_\rho^*$ for $\rho = 0, 1, \cdots, p-1$. We show by induction that $(R_\rho)\Delta^* = 0$ for all $\rho < p$. We know this to be true for $\rho = 0$ and we assume it for all $\rho \leqq r < p-1$, $r \geqq 0$. Then

$$(R_{r+1}\Delta_i)\Delta^* = ((R_{r+1})\Delta^*)\Delta_i = 0 \qquad (i = 1, \cdots, p^n),$$

so that $(R_{r+1})\Delta^* \subseteq R_0$. If $r+1 < p$, $r+1 \not\equiv 0 \pmod{p}$, and this is impossible unless $(R_{r+1})\Delta^* = 0$. The induction is thus valid for all $\rho < p$.

Let d be arbitrary in R_m, where m is the maximum degree of R. Then certainly (58) holds for d. Since $(R_1)\Delta^* = (R_2)\Delta^* = 0$, applying Δ^* to both sides of relation (58), we obtain, letting $\hat{d} = (d)\Delta^*$,

$$\hat{d}\, ad(\beta) = \hat{d}\left[\prod_{i=1}^{r} ad(\alpha_i)\right] ad(\beta) = 0$$

(all α_i in R_1, β in R_2, $r \geqq 1$).

Owing to Lemma 5.6, we can conclude that $\hat{d}$ is in R_m. If $\hat{d} \neq 0$, there exists a suitable sequence of m partial differential operators Δ_{μ_i} such that

$$\hat{d} \prod_{i=1}^{m} \Delta_{\mu_i} \neq 0.$$

But then

$$d \prod_{i=1}^{m} \Delta_{\mu_i}$$

is in R_0 and is not mapped into zero by Δ^*. This contradiction implies that $(d)\Delta^* = 0$ for all d in R_m. Assume $(d)\Delta^* = 0$ for all d in R_k, for $k \leqq m$, and let c be in R_{k-1}. Then by properties (ii), (iii) of Lemma 5.4 we can write

$$c = \sum_{j=0}^{n} \bar{c}_j \Delta_{N_j},$$

with $\bar{c}_j$ necessarily in R_k, so that $(c)\Delta^* = 0$. The induction is therefore valid on $-k$, and Δ^* maps R on zero. Thus $\Delta^* = 0$ and $\Delta \equiv 0$. This completes the proof of the theorem([7]).

THEOREM 5.2. *If $n + 2 \equiv 0 \pmod{p}$, the algebra of outer derivations of R^2 over F is at most $(n+1)$-dimensional.*

Proof. If $n + 2 \equiv 0 \pmod{p}$, Z is of degree $(n+1)(p-1) \equiv 1 \pmod{p}$ and it follows from Lemma 4.2 that

$$R^2 = R_0^* + \bar{R}_1^* + R_2^* + \cdots + R_{p-1}^*,$$

where $\bar{R}_1^*$ is spanned by all $D_j(\phi)$, with ϕ a monomial in C_n of degree $\equiv 1 \pmod{p}$, $j = 1, \cdots, p^n$, except $D_1(Z)$. Since R^2 is admissible it follows as before by Lemma 5.1 that any derivation of R^2 is congruent to a derivation Δ with $(R_\rho^*)\Delta \subseteq R_\rho^*$ for $\rho = 0, 2, \cdots, p-1$, $(\bar{R}_1^*)\Delta \subseteq \bar{R}_1^*$, and with $(\Delta_i)\Delta$ truncated in x_i for $i = 1, \cdots, p^n$. Let V denote the subspace of derivations Δ of R^2 with these properties. In particular then, if $\Delta \in V$, we can write, for $\mu = 0, \cdots, n$,

$$(\Delta_{N_\mu})\Delta = \lambda_\mu D_1\left(\frac{\partial Z}{\partial Z_\mu}\right) + D_1\left(\frac{\partial \phi_\mu}{\partial Z_\mu}\right) + \sum_{j \geq 2} D_j(\theta_j), \tag{63}$$

for suitable unique λ_μ in F, and polynomials θ_j, ϕ_μ in C_n, the latter all of degree $\leqq m - 1$. Let V_0 denote the subspace of V spanned by all Δ for which the coefficients λ_μ in (63) vanish for $\mu = 0, \cdots, n$. Then clearly,

$$\dim V - \dim V_0 \leqq n + 1,$$

and the lemma follows once we show that every derivation in V_0 is inner. By substituting $\bar{R}_1^*$ for R_1^*, Lemma 5.5 for Lemma 5.4, and an arbitrary Δ in V_0 to the derivation Δ in the proof argument of Theorem 5.1, it follows as before that $\Delta \equiv 0$, and we have the required result.

COROLLARY. *If $p \nmid n + 2$, the p^{2n+1}-dimensional algebras R are new for all $n \neq \frac{1}{2}(p^{2r} + 2r - 1)$, $r \geqq 1$. If $p \mid n + 2$, the $(p^{2n+1} - 1)$-dimensional algebras R^2 are new for all n.*

Proof. The simple p^{2n+1}-dimensional Albert-Zassenhaus algebras([8]) generalized by Block in [3] are shown there to possess an outer derivation algebra of dimension $2n$ over F. This class, which includes—for the value $m = 1$—the

([7]) The known fact (cf. [7]) that every derivation of W_n over F is inner follows in a similar way from Lemmas 5.1., 5.2, 5.3, 5.4, 5.6, the last three of which remain valid if we substitute W_n for both W_{p^n} and R, and replace Z_j by x_j for j in the set J now given by $\{1, \cdots, n\}$.

([8]) Cf. [12], [1].

simple mp^{2n+1}-dimensional algebras of Jennings and Ree defined in [8], is thus distinct from the class of algebras R.

Now the mp^k-dimensional algebras of [8] are defined for $1 \leqq m < k$, and may share the dimensionality of R for $m = p^r < k$ with $2n + 1 = r + k > p^r + r$, $r \geqq 0$. The same situation arises with the Kaplansky algebras(9), which are also mp^k-dimensional and defined for $1 \leqq m \leqq k$. When these are restricted, they become the Jacobson-Witt algebras W_k(10). Whether for $k = m = p^r$ and $2n + 1 = p^r + r$ (with r necessarily even, since $p > 2$) R is isomorphic to W_{p^r} remains an open question. But if $m < k$, we now show that the outer derivation algebras of members of the above two classes are at least $(k - m)$-dimensional.

For $1 \leqq m < k$ the simple mp^k-dimensional algebras of [8] and those of [9] share the following schematized definition and will be alluded to jointly as $S_{m,k}$. Let E_{m+1} be an $(m+1)$-dimensional vector space over F, and G_k be an elementary p-group of order p^k. Then $S_{m,k}$ is spanned over F by elements (x_α, α) with $\alpha \in G_k$ and $x_\alpha \in E_\alpha$, where for every α in G_k, E_α is a specific m-dimensional subspace of E_{m+1}. If $x_\alpha, y_\alpha \in E_\alpha, \mu(x_\alpha, \alpha) + \nu(y_\alpha, \alpha) = (\mu x_\alpha + \nu y_\alpha, \alpha)$ for all μ, ν in F. Multiplication within $S_{m,k}$ is given by

$$(64) \qquad (x_\alpha, \alpha) \circ (y_\beta, \beta) = (z, \alpha + \beta), \qquad z = g(x_\alpha, \beta) y_\beta - g(y_\beta, \alpha) x_\alpha,$$

where $g(x, \beta)$ is a bi-additive function on $E_{m+1} \times G_k$ to F (with, in particular, $g(x, 0) = 0$, all x in E_{m+1}) and specific additional properties for each of the two classes which insure, in particular, that $z \in E_{\alpha+\beta}$(11).

Now if d is any additive function on G_k to F, the mapping

$$(65) \qquad (x_\alpha, \alpha) \to d(\alpha)\,(x_\alpha, \alpha) \qquad (x_\alpha \in E_\alpha, \alpha \in G_k),$$

is a derivation of $S_{m,k}$, and by (64) is inner if and only if

$$d(\alpha) = -\,g(y_0, \alpha)$$

for some fixed y_0 in E_0. Since there are k linearly independent additive functions on G_k to F, the space of outer derivations of $S_{m,k}$ with property (65) is $(k - m)$-dimensional, and it follows that R is not isomorphic to members of either class for $m < k$.

---

(9) Cf. [9], [10].

(10) Cf. [11].

(11) Although relation (5.0.5) of [8] is more general than (64), the simple algebras considered in that paper all belong to a class $\mathfrak{F}_c$ for which (5.0.5) reduces directly to (64) (cf. §7 of [8]).

As for the algebras of [9], their basis over F can be given by elements $(i.\ \alpha)$ for $i = 1, \cdots, m$, $\alpha \in G_k$, with $(i, \alpha) \circ (j, \beta) = h_i(\beta)\,(j, \alpha + \beta) - h_j(\alpha)\,(i, \alpha + \beta)$, where the h_i are m linearly independent additive functions on G_k to F (with additional properties). If for coefficients λ_i in F we let $\sum_{i=1}^m \lambda_i (i, \alpha) = (\lambda, \alpha)$, with $\lambda = (\lambda_1, \cdots, \lambda_m)$ in E_m, and $\sum_{i=1}^m \lambda_i h_i(\alpha) = g(\lambda, \alpha)$, all α in G_k, we obtain relation (64) in the special instance where $E_\alpha = E_m$ for all α in G_k.

Let $p \mid n+2$. Block has shown in [2] that his class of $(p^{2n+1}-1)$-dimensional simple algebras, which includes those of Albert in [1] and Jennings and Ree in [8] sharing the same dimensionality([12]), has an outer derivation algebra which is exactly $(2n+1)$-dimensional over F, and we can thus conclude by Theorem 5.2 that this class does not contain R^2.

6. **Cartan decomposition.** We select the following monomials of C_n, defined for every index i:

$$\eta_i = Z_0^{p-(i_0+1)} Z_1^{p-(i_1+1)} \cdots Z_{n-1}^{p-(i_{n-1}+1)} Z_n^{\tau(i)} \tag{66}$$

where $\tau(i)$, the exponent of Z_n, is defined uniquely by the relations

$$\begin{aligned} &0 \leqq \tau(i) \leqq p-1, \\ &\tau(i) \equiv \sum_{\mu=0}^{n-1} (i_\mu + 1) + 1 \pmod{p}. \end{aligned} \tag{67}$$

Then the degree of η_i is $\geqq 1$ for all i. In particular for $i \neq N_k$, the degree of η_i is $\geqq 2$; while for $i = N_k$, $\eta_{N_k} = Z_k$ for $k = 0, 1, \cdots, n$. To simplify the notation, we let

$$I_k = D_{N_k}(\eta_{N_k}) = D_{N_k}(Z_k) \qquad (k = 0, 1, \cdots, n). \tag{68}$$

We prove

THEOREM 6.1. *Let H be the subspace of R spanned by the vectors $D_i(\eta_i)$ for $i = 1, \cdots, p^n$, where η_i are monomials in C_n given by* (66), (67). *Then H is an abelian Cartan subalgebra of R.*

Proof. We start by showing that H is abelian. Indeed consider the product $D_i(\eta_i)D_j(\eta_j)$. Applying Theorem 3.2, we see at once that for all $k = i + j - N_\rho$, $0 \leqq \rho \leqq n$, the polynomial ψ_ρ given by (27) vanishes, as required. Suppose that for polynomials ϕ_i in C_n,

$$d = \sum_i D_i(\phi_i) \tag{69}$$

is an element in R with the property that

$$dH \subseteq H. \tag{70}$$

It is easy to establish by elementary computation from Theorem 3.2 that for all ϕ in C_n,

$$D_i(\phi) I_k = D_i(\psi_k) \qquad (k = 0, 1, \cdots, n), \tag{71}$$

with

([12]) The $m(p^k - 1)$-dimensional algebras of [8], defined for $1 \leqq m < k$, share the dimensionality of R^2 only for $m = 1$, $k = 2n+1$. For suppose $p^{2n+1} - 1 = m(p^k - 1)$, then $2n + 1 = sk$ for an integer $s \geqq 3$ if $m \neq 1$. But then the requirement $p^{2n+1} - 1 < k(p^k - 1)$ $\Rightarrow p^{3k} < kp^k$ which is impossible.

$$(72)\qquad \begin{cases} \psi_k = \dfrac{\partial \phi}{\partial Z_k} Z_k + (i_k + 1)\phi \qquad (k < n), \\ \psi_n = \dfrac{\partial \phi}{\partial Z_n} Z_n - \left[\sum_{\rho=0}^{n-1} (i_\rho + 1) + 1\right]\phi . \end{cases}$$

It follows from (69), (70), (71), (72), that $\phi_i = \lambda_i \eta_i$ for λ_i in F, d is in H, and H is a Cartan subalgebra of R. As an obvious corollary we have

COROLLARY. *If $n+2 \equiv 0 \pmod p$ the subspace $\bar{H}$ of R^2, spanned by all $D_i(\eta_i)$ except $D_1(Z)$, is a Cartan subalgebra of R^2.*

Denoting by G_{n+1} the p-group of order p^{n+1} whose elements can be represented by vectors $= (\alpha_0, \cdots, \alpha_n)$ with components α_i in the prime field F_p, we prove

THEOREM 6.2. *The Cartan decomposition of R with respect to H is given by $R = \sum_\alpha L_\alpha$, where the roots α in G_{n+1} are additive functions on H to F with*

$$(73)\qquad \alpha(I_k) = \alpha_k \quad (k = 0, 1, \cdots, n); \quad \alpha(D_i(\eta_i)) = 0 \quad (i \neq N_0, \cdots, N_n).$$

The subspace L_α is p^n-dimensional over F and is generated by basis derivations $D_i(\xi_{\alpha i})$ of R, where

$$(74)\qquad \xi_{\alpha i} = \prod_{\mu=0}^{n} Z_\mu^{\rho_\mu(i)} \qquad (i = 1, \cdots, p^n),$$

with the exponents $\rho_\mu = \rho_\mu(i)$ satisfying the constraints $0 \leqq \rho_\mu \leqq p-1$, together with the congruences, mod p,

$$(75)\qquad \rho_r \equiv \alpha_r - (i_r + 1) \quad (r < n); \quad \rho_n \equiv \alpha_n + \left[\sum_{\mu=0}^{n-1} (i_\mu + 1) + 1\right].$$

Proof. We first show that if h is arbitrary in H, say

$$h = \sum_{j=0}^{n} e_j I_j + \tilde{h},$$

where $e_j \in F$, and $\tilde{h} \in R_2 + \cdots + R_m$ is strictly nilpotent, we have

$$(76)\qquad D_i(\xi_{\alpha i})\,[ad(h) - \alpha(h)]^k = D_i(\xi_{\alpha i})\, ad(\tilde{h})^k \qquad (k \geqq 1).$$

For $k = 1$, we compute by Theorem 3.2 the product

$$(77)\qquad D_i(\xi_{\alpha i}) \sum_{j=0}^{n} e_j I_j = D_i(\xi_{\alpha i})\, ad\,(h - \tilde{h}).$$

Owing to (74), (75), this is seen to be

$$(78)\qquad \left(\sum_{j=0}^{n} e_j \alpha_j\right) D_i(\xi_{\alpha i}) = \alpha(h) D_i(\xi_{\alpha i}).$$

Hence (76) certainly holds for $k = 1$. Assume it holds for some fixed $k \geqq 1$. Then

$$D_i(\xi_{\alpha i})\,[ad(h)-\alpha(h)\,]^{k+1} = D_i(\xi_{\alpha i})\,ad(\tilde{h})^{k+1} + D_i(\xi_{\alpha i})\,ad(\tilde{h})^k[ad(h-\tilde{h})-\alpha(h)].$$

Now since H is abelian, the second expression on the right is equal to

$$D_i(\xi_{\alpha i})\,[ad(h-\tilde{h})-\alpha(h)]\;ad(\tilde{h})^k\,,$$

which by (77), (78) vanishes. Hence the induction is valid and (76) holds for all $k \geqq 1$. In particular, since the maximum degree of R is $m=(n+1)(p-1)$, $ad(\tilde{h})^{m+1}=0$, so that for $k \geqq m+1$,

$$L_\alpha[ad(h)-\alpha(h)\,]^k = 0 \quad (\text{all } \alpha \text{ in } G_{n+1}, \text{ all } h \text{ in } H).$$

This completes the proof of the theorem.

COROLLARY. *If* $n+2 \equiv 0 \pmod{p}$, *the decomposition of* R^2 *with respect to* $\bar{H}$ *is given by* $R^2 = \sum_{\alpha \neq 0} L_\alpha + \bar{H}$.

BIBLIOGRAPHY

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

2. Richard Block, *New simple Lie algebras of prime characteristic*, Trans. Amer. Math. Soc. **89** (1958), 421–449.

3. ———, *On torsion-free abelian groups and Lie algebras*, Proc. Amer. Math. Soc. **9** (1958), 613–620.

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

5. ———, *On a theory relating matric Lie algebras of characteristic p and subalgebras of the Jacobson-Witt algebra, with applications leading to the definition of new simple Lie algebras*, Progress Report I.T. Math. Dept., pp. 1–102, Univ. of Minnesota, 1960.

6. N. Jacobson, *Classes of restricted Lie algebras of characteristic p.* I, Amer. J. Math. **53** (1941), 481–515.

7. ———, *Classes of restricted Lie algebra of characteristic p.* II, Duke Math. J. **10** (1943), 107–121.

8. S. A. Jennings and Rimhak Ree, *On a family of Lie algebras of characteristic p*, Trans. Amer. Math. Soc. **84** (1957), 192–207.

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

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

11. George Seligman, *A survey of Lie algebras of characteristic p*, Linear algebras, National Res. Council Pub. #502, 1957, pp. 24–32.

12. Hans Zassenhaus, *Über Lie'sche ringe mit primzahlcharakteristik*, Abh. Math. Sem. Univ. Hamburg **13** (1939), 1–100.

MATHEMATICA,
PRINCETON, NEW JERSEY