TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 153, January 1971

CLASSIFICATION OF GENERALIZED WITT ALGEBRAS OVER ALGEBRAICALLY CLOSED FIELDS(1)

BY
ROBERT LEE WILSON

Abstract. Let Φ be a field of characteristic $p>0$ and $m, n_1, \ldots, n_m$ be integers $\geqq 1$. A Lie algebra $W(m : n_1, \ldots, n_m)$ over Φ is defined. It is shown that if Φ is algebraically closed then $W(m : n_1, \ldots, n_m)$ is isomorphic to a generalized Witt algebra, that every finite-dimensional generalized Witt algebra over Φ is isomorphic to some $W(m : n_1, \ldots, n_m)$, and that $W(m : n_1, \ldots, n_m)$ is isomorphic to $W(s : r_1, \ldots, r_s)$ if and only if $m=s$ and $r_i=n_{\sigma(i)}$ for $1 \leqq i \leqq m$ where σ is a permutation of $\{1, \ldots, m\}$. This gives a complete classification of the finite-dimensional generalized Witt algebras over algebraically closed fields. The automorphism group of $W(m : n_1, \ldots, n_m)$ is determined for $p>3$.

Introduction. Let Φ be a field of characteristic $p>0$. Kaplansky [5] (generalizing earlier definitions by Witt [1], Zassenhaus [11] and Jacobson [2]) has defined a family of Lie algebras over Φ in the following manner: Let $I=\{i, j, \ldots\}$ be a set of indices, $\mathscr{G}$ be a total additive group of functionals on I with values in Φ, and $\mathscr{L}$ be a vector space with basis $I \times \mathscr{G}$. Define a bilinear multiplication in $\mathscr{L}$ by

$$[(i, \sigma), (j, \tau)] = \tau(i)(j, \sigma+\tau)-\sigma(j)(i, \sigma+\tau).$$

It is easily seen that $\mathscr{L}$ is a Lie algebra. Following Ree [7] we will call such algebras *generalized Witt algebras*.

The problem we consider in this paper is the classification of the finite-dimensional generalized Witt algebras over algebraically closed fields. The study of this problem was begun by Ree [7] who showed that generalized Witt algebras over algebraically closed fields are isomorphic to certain algebras of derivations. (We state this result in detail in §2.) We give a complete solution to this problem by constructing for any field Φ of characteristic $p>0$ and any integers $m, n_1, \ldots, n_m \geqq 1$ a Lie algebra $W(m : n_1, \ldots, n_m)$ over Φ and proving the following theorem (which was announced in [10]):

Received by the editors April 13, 1970.
AMS 1969 *subject classifications*. Primary 1730.
Key words and phrases. Generalized Witt algebras.
(1) Most of the results of this paper are contained in the author's doctoral dissertation written under the guidance of Professor G. B. Seligman at Yale University. The author wishes to express his thanks to Professor Seligman for his guidance and encouragement. The author was a National Science Foundation graduate fellow at Yale and has received partial support from a Sloan Foundation grant at the Courant Institute of Mathematical Sciences.

THEOREM 1. *Let Φ be an algebraically closed field of characteristic $p>0$. Then*

(a) *$W(m : n_1, \ldots, n_m)$ is isomorphic to a generalized Witt algebra.*

(b) *Every finite-dimensional generalized Witt algebra over Φ is isomorphic to some $W(m : n_1, \ldots, n_m)$.*

(c) *The algebras $W(m : n_1, \ldots, n_m)$ and $W(s : r_1, \ldots, r_s)$ are isomorphic if and only if $m=s$ and $r_i=n_{\sigma(i)}$ for $1 \leqq i \leqq m$ where σ is a permutation of $\{1, \ldots, m\}$.*

The algebras $W(m : n_1, \ldots, n_m)$ have been studied by Kostrikin and Šafarevič [6] who have proved a statement equivalent to (a). The conclusion in (c) that $m=s$ is due to Ree [7, Theorem 12.14].

The definition of $W(m : n_1, \ldots, n_m)$ is given in §1. The proof of Theorem 1 is contained in §§2 and 3. In §4 the automorphism group of $W(m : n_1, \ldots, n_m)$ is determined for $p>3$.

Since several families of nonclassical simple Lie algebras may be defined as subalgebras of generalized Witt algebras (e.g., [4]), the results of this paper are of considerable use in the study of nonclassical simple Lie algebras. In particular, they can be used to prove that all the finite-dimensional nonclassical simple Lie algebras listed in [9, pp. 105–110] are of Cartan type (in the sense of [6] or [10]) thus effecting a considerable simplification in the description of the known finite-dimensional nonclassical simple Lie algebras. This topic will be treated in a later paper.

1. **Definitions.** We begin by defining a family of associative algebras over an arbitrary field Φ. Let $\boldsymbol{C}$ denote the complex numbers, $\boldsymbol{Z}$ the integers and $\boldsymbol{N}$ the nonnegative integers. Let $A(m)$ be the set of $\boldsymbol{N}$ valued functions on $\{1, \ldots, m\}$. Define $\varepsilon_i \in A(m)$ by $\varepsilon_i(j)=\delta_{ij}$. For $\alpha, \beta \in A(m)$ define $\alpha!=\prod \alpha(i)!$, $|\alpha|=\sum \alpha(i)$ and $C(\alpha, \beta)=\prod C(\alpha(i), \beta(i))$ (where $C(r, s)$ is the binomial coefficient $r!/s!(r-s)!$). Let $\mathscr{A}(m)=\boldsymbol{C}[[x_1, \ldots, x_m]]$. For $\alpha \in A(m)$ define $x^\alpha=(\prod x_i^{\alpha(i)})/\alpha! \in \mathscr{A}(m)$. Then

$$x^\alpha x^\beta = C(\alpha+\beta, \beta)x^{\alpha+\beta}. \tag{1.1}$$

Set $\bar{\mathscr{A}}(m)=\{\sum a_\alpha x^\alpha \mid a_\alpha \in \boldsymbol{Z}\} \subseteq \mathscr{A}(m)$ where the summation extends over all $\alpha \in A(m)$ and infinite sums are allowed. Then $\bar{\mathscr{A}}(m)$ is a $\boldsymbol{Z}$-subalgebra of $\mathscr{A}(m)$. For any field Φ define $\mathfrak{A}(m)=\bar{\mathscr{A}}(m) \otimes_{\boldsymbol{Z}} \Phi$. Then $\mathfrak{A}(m)$ is an associative algebra over Φ. Denoting $x^\alpha \otimes 1$ by x^α we see that multiplication in $\mathfrak{A}(m)$ satisfies (1.1). For $1 \leqq i \leqq m$ denote x^{ε_i} by x_i.

For $0 \neq \sum a_\alpha x^\alpha \in \mathfrak{A}(m)$ define $|\sum a_\alpha x^\alpha|=\min\{|\alpha| \mid a_\alpha \neq 0\}$. Define $|0|=\infty$ and set $\mathfrak{A}(m)_i=\{x \in \mathfrak{A}(m) \mid |x| \geqq i+1\}$. Then $\mathfrak{A}(m)$ is a topological algebra with $\{\mathfrak{A}(m)_i \mid i \geqq -1\}$ as a base of neighborhoods of 0. Define $\bar{\mathfrak{A}}(m)$ to be the subalgebra of $\mathfrak{A}(m)$ consisting of all finite linear combinations of $\{x^\alpha \mid \alpha \in A(m)\}$. Then $\bar{\mathfrak{A}}(m)$ is dense in $\mathfrak{A}(m)$. For any subalgebra $\mathfrak{A}$ of $\mathfrak{A}(m)$ define $\mathfrak{A}_i=\mathfrak{A} \cap \mathfrak{A}(m)_i$ for all $i \in \boldsymbol{N}$.

We now define a sequence of divided power operators on $\mathfrak{A}(m)$. These are the analogues of the mappings $x \to x^r/r!$ in $\mathscr{A}(m)$.

LEMMA 1. *There is a unique sequence of continuous mappings* $y \to y^{(r)}$ ($r \in N$) *of* $\mathfrak{A}(m)_0$ *into* $\mathfrak{A}(m)$ *satisfying*:

(1.2) $x^{(0)} = 1$ *for all* $x \in \mathfrak{A}(m)_0$.

(1.3) $(x^{\alpha})^{(r)} = ((r\alpha)!/(\alpha!)^r r!)x^{r\alpha}$ *for all* $\alpha \in A(m)$ *such that* $\alpha \neq 0$ *and all* $r \in N$.

(1.4) $(ax)^{(r)} = a^r x^{(r)}$ *for all* $a \in \Phi$, $x \in \mathfrak{A}(m)_0$ *and* $r \in N$.

(1.5) $(x+y)^{(r)} = \sum_{i=0}^{r} x^{(i)} y^{(r-i)}$ *for all* $x, y \in \mathfrak{A}(m)_0$ *and all* $r \in N$.

Proof. For the coefficient in (1.3) to be interpreted as an element of Φ it must be an integer. Hence we first show that if $0 \neq \alpha \in A(m)$ and $r \in N$ then $(r\alpha)!/(\alpha!)^r r! \in Z$. Since $0 \neq \alpha$ we may suppose without loss of generality that $\alpha(1) \neq 0$. Then $(r\alpha)!/(\alpha!)^r r!$ is the product of $(r\alpha(1))!/(\alpha(1)!)^r r!$ and $\prod_{i=2}^{m} \{(r\alpha(i))!/(\alpha(i)!)^r\}$. Now it suffices to show that each factor is an integer, i.e., if $r, b \in N$ then $(rb)!/(b!)^r \in Z$ and if $b \geqq 1$ then $(rb)!/(b!)^r r! \in Z$. But this is immediate from the fact that $(rb)!/(b!)^r = \prod_{j=1}^{r} C(jb, b)$ together with the observation that if $b \neq 0$ then $C(jb, b) = jC(jb-1, b-1)$.

Now (1.2)–(1.5) define a unique sequence of maps $y \to y^{(r)}$ of $\bar{\mathfrak{A}}(m)_0$ into $\bar{\mathfrak{A}}(m)$. Since $\bar{\mathfrak{A}}(m)$ is dense in $\mathfrak{A}(m)$ these can be uniquely extended to continuous maps of $\mathfrak{A}(m)_0$ into $\mathfrak{A}(m)$.

Following Kostrikin and Šafarevič [6, p. 256] we call a derivation D of $\mathfrak{A}(m)$ *special* if

$$y^{(r)}D = (yD)y^{(r-1)} \quad \text{for all } y \in \mathfrak{A}(m)_0 \text{ and all } r \in Z,\ r \geqq 1. \tag{1.6}$$

It is easily seen that the special derivations of $\mathfrak{A}(m)$ span a Lie subalgebra of the derivation algebra. We denote this subalgebra by $W(m)$.

Now let Φ be a field of characteristic $p > 0$. Let $\boldsymbol{n} = (n_1, \ldots, n_m)$ be an m-tuple of integers $\geqq 1$. Define $A(m:\boldsymbol{n}) = \{\alpha \in A(m) \mid \alpha(i) < p^{n_i} \text{ for } 1 \leqq i \leqq m\}$. Now if $\alpha, \beta \in A(m:\boldsymbol{n})$ and $\alpha+\beta \notin A(m:\boldsymbol{n})$ then $p \mid C(\alpha+\beta, \alpha)$. Thus $\mathfrak{A}(m:\boldsymbol{n}) = \langle x^{\alpha} \mid \alpha \in A(m:\boldsymbol{n})\rangle$ is a subalgebra of $\mathfrak{A}(m)$. Define $W(m:\boldsymbol{n})$ to be the stabilizer of $\mathfrak{A}(m:\boldsymbol{n})$ in $W(m)$.

From (1.1) and (1.3) we see that $\{x_i \mid 1 \leqq i \leqq m\}$ generates $\mathfrak{A}(m)_0$ under algebra operations and divided power operations. Thus (1.6) shows that if D is a special derivation satisfying $x_i D = 0$ for $1 \leqq i \leqq m$ then $D = 0$. Define derivations $D_1, \ldots, D_m$ of $\mathfrak{A}(m)$ by

$$x^{\alpha} D_i = x^{\alpha - \varepsilon_i} \tag{1.7}$$

(where we set $x^{\beta} = 0$ for $\beta \notin A(m)$). It is easily seen that if $a_1, \ldots, a_m \in \mathfrak{A}(m)$ (respectively $\mathfrak{A}(m:\boldsymbol{n})$) then $\sum D_j a_j \in W(m)$ (respectively $W(m:\boldsymbol{n})$). For any $D \in W(m)$ we have $x_i(D - \sum_{j=1}^{m} D_j(x_j D)) = 0$ for $1 \leqq i \leqq m$. Hence $D = \sum D_j(x_j D)$. This proves the following lemma (due to Kostrikin and Šafarevič [6]).

LEMMA 2. $W(m)$ *is a free* $\mathfrak{A}(m)$ *module with basis* $\{D_1, \ldots, D_m\}$ *and* $W(m:\boldsymbol{n})$ *is a free* $\mathfrak{A}(m:\boldsymbol{n})$ *module with basis* $\{D_1, \ldots, D_m\}$.

It is easily seen that the restriction map $D \to D \mid \mathfrak{A}(m:\boldsymbol{n})$ is an isomorphism of $W(m:\boldsymbol{n})$ into Der $(\mathfrak{A}(m:\boldsymbol{n}))$. Thus we may, when necessary, regard $W(m:\boldsymbol{n})$ as a subalgebra of Der $(\mathfrak{A}(m:\boldsymbol{n}))$.

We see from (1.3)–(1.5) that $y^{(r)}=y^r/r!$ for $r<p$. Hence every derivation of $A(m{:}\mathbf{1})$ is special so that $W(1{:}1)$ is the Witt algebra [1] and the algebras $W(m{:}\mathbf{1})$ are the Jacobson-Witt algebras [2]. If E is an m-dimensional vector space and $\mathscr{F}$ is the flag $E=E_0\supseteq E_1\supseteq\cdots$ then the algebra $W(\mathscr{F})$ of Kostrikin and Šafarevič [6, p. 261] is isomorphic to $W(m{:}\boldsymbol{n})$ where dim E_{j-1} is equal to the number of i for which $n_i\geqq j$.

Using (1.1) and (1.7) we see that multiplication in $W(m{:}\boldsymbol{n})$ is defined by bilinearity and

$$(1.8)\qquad [D_ix^\alpha, D_jx^\beta] = D_ix^{\alpha+\beta-\varepsilon_j}C(\alpha+\beta-\varepsilon_j, \beta)-D_jx^{\alpha+\beta-\varepsilon_i}C(\alpha+\beta-\varepsilon_i, \alpha).$$

The binomial coefficients may be evaluated using the following remark:

$$(1.9)\qquad \begin{array}{l}\text{If } u = \sum_{i=0}^n u_ip^i \text{ and } v = \sum_{i=0}^n v_ip^i \text{ then}\\ C(u+v, u) \equiv \prod_{i=0}^n C(u_i+v_i, u_i) \pmod p.\end{array}$$

(For if we set $\tilde{u}=\sum_{j=0}^n u_j((p^j-1)/(p-1))$ it is easily seen that $u!/p^{\tilde{u}}\equiv(-1)^{\tilde{u}}u_0!\cdots u_n!$ (mod p). Defining $\tilde{v}$ similarly in terms of the v_i and $(u+v)^\sim$ similarly in terms of the u_i+v_i we see that $\tilde{u}+\tilde{v}=(u+v)^\sim$ from which (1.9) follows.)

We will have occasion to use the following special cases of (1.8) and (1.9):

$$(1.10)\qquad [D_ix^\alpha, D_j] = D_ix^{\alpha-\varepsilon_j}.$$

$$(1.11)\qquad [D_ix^\alpha, D_jx_j] = D_ix^\alpha(\alpha(j)-\delta_{ij}).$$

We will also use the following properties of binomial coefficients:

$$(1.12)\qquad \begin{array}{l}\text{If } C(r+s-1, r) \equiv 0 \pmod p \text{ for all } r,\ 0 < r < s,\\ \text{then } s = p^w \text{ for some } w\in \boldsymbol{Z}.\end{array}$$

$$(1.13)\qquad \begin{array}{l}\text{If } C(s+r-1, r)-C(s+r-1, r-1) \equiv -1 \pmod p\\ \text{for all } r,\ 0 < r < s, \text{ then } s = p^w \text{ for some } w\in \boldsymbol{Z}.\end{array}$$

To prove (1.12) write $s=\sum s_ip^i$ where $0\leqq s_i<p$ for all i. If $s=1$ the result holds. If $s>1$ then $C(s, 1)\equiv 0$ (mod p) so by (1.9) $s_0=0$. Similarly we see that if $s_0=s_1=\cdots=s_{i-1}=0$ then either $s=p^i$ or $s_i=0$. This proves (1.12). The proof of (1.13) is similar.

2. **Proof of Theorem 1.** Throughout this section we assume that Φ is an algebraically closed field of characteristic $p>0$.

Let $\mathfrak{A}$ be a commutative associative algebra with unit over Φ. A set $\boldsymbol{D}=\{D_1, \ldots, D_m\}$ of derivations of $\mathfrak{A}$ is called a system if it is linearly independent over $\mathfrak{A}$ and if its $\mathfrak{A}$-span, denoted by $\mathscr{L}(\mathfrak{A}{:}\boldsymbol{D})$, is a Lie subalgebra of the derivation algebra of $\mathfrak{A}$. A system $\{D_1, \ldots, D_m\}$ is said to be orthogonal if $[D_i, D_j]=0$ for all $1\leqq i, j\leqq m$. Two systems $\boldsymbol{D}=\{D_1, \ldots, D_m\}$ and $\boldsymbol{E}=\{E_1, \ldots, E_n\}$ are said to be equivalent if $\mathscr{L}(\mathfrak{A}{:}\boldsymbol{D})=\mathscr{L}(\mathfrak{A}{:}\boldsymbol{E})$. Clearly this occurs if and only if $m=n$ and $D_i=\sum E_jc_{ij}$ for $1\leqq i\leqq m$ where $c_{ij}\in\mathfrak{A}$ for $1\leqq i, j\leqq m$ and det (c_{ij}) is a unit in $\mathfrak{A}$.

If $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$ containing c_{ij} for $1 \leqq i, j \leqq m$ and $\det (c_{ij})^{-1}$ we say that the systems are equivalent over $\mathfrak{B}$. A derivation D of $\mathfrak{A}$ is said to be normal if $a \in \mathfrak{A}$ and $aD=0$ imply that $a \in \Phi$.

Denote by $\mathbf{1}$ the n-tuple $(1, \ldots, 1)$. Let $\boldsymbol{y}=(y_1, \ldots, y_n)$ be an n-tuple of elements of $\mathfrak{A}(m:\mathbf{1})$. For $\alpha \in A(n:\mathbf{1})$ define $\boldsymbol{y}^\alpha = \prod_{i=1}^n (y_i^{\alpha(i)}/\alpha(i)!)$. We will call $\boldsymbol{y}$ a system of *standard generators* for $\mathfrak{A}(n:\mathbf{1})$ if $y_i^p=0$ for $1 \leqq i \leqq m$ and $\{\boldsymbol{y}^\alpha \mid \alpha \in A(n:\mathbf{1})\}$ is a basis for $\mathfrak{A}(n:\mathbf{1})$. If $\boldsymbol{y}$ is a system of standard generators for $\mathfrak{A}(n:\mathbf{1})$ define derivations $C_i(\boldsymbol{y})$ for $1 \leqq i \leqq n$ by

$$(2.1)\qquad \begin{aligned} y_j C_i(\boldsymbol{y}) &= 0 && \text{if } j < i, \\ &= 1 && \text{if } j = i, \\ &= (y_i \cdots y_{j-i})^{p-1} && \text{if } j > i. \end{aligned}$$

We now state some of Ree's results on generalized Witt algebras.

Proposition 1. (a) [7, §2] *Any finite-dimensional generalized Witt algebra over* Φ *is isomorphic to some* $\mathscr{L}(\mathfrak{A}:\boldsymbol{D})$.

(b) [7, *Theorem* 6.10] $\mathscr{L}(\mathfrak{A}:\boldsymbol{D})$ *is isomorphic to a finite-dimensional generalized Witt algebra if and only if* $\mathfrak{A}$ *is finite dimensional and there exists an orthogonal system* $\{E_1, \ldots, E_m\}$ *equivalent to* $\boldsymbol{D}$ *and satisfying the following conditions*:

(2.2) *If* $a \in \mathfrak{A}$ *and* $aE_i = \lambda_i a$ *where* $\lambda_i \in \Phi$ *for all* i, $1 \leqq i \leqq m$, *then either* $a=0$ *or* a *is a unit in* $\mathfrak{A}$.

(2.3) *If* $a \in \mathfrak{A}$ *and* $aE_i=0$ *for all* i, $1 \leqq i \leqq m$, *then* $a \in \Phi$.

(c) [7, *Theorems* 8.3, 9.2] *If* $\boldsymbol{D}$ *is an orthogonal system of derivations of* $\mathfrak{A}$ *satisfying* (2.2) *and* (2.3) *and if* $\mathfrak{A}$ *is finite dimensional then* $\mathfrak{A} \cong \mathfrak{A}(n:\mathbf{1})$ *for some n. Furthermore there exists an orthogonal system* $\boldsymbol{E}$ *equivalent to* $\boldsymbol{D}$ *such that* E_1 *is normal and nilpotent.*

(d) [7, *Theorems* 8.3, 9.3] *If* D *is a normal and nilpotent derivation of* $\mathfrak{A}(n:\mathbf{1})$ *then there exists a system of standard generators* $\boldsymbol{y}$ *of* $\mathfrak{A}(n:\mathbf{1})$ *such that* $D=C_1(\boldsymbol{y})$. *If* E *is any derivation of* $\mathfrak{A}(n:\mathbf{1})$ *such that* $[D, E]=0$ *then* $E=\sum_{i=1}^n C_i(\boldsymbol{y})\gamma_i$ *where the* $\gamma_i \in \Phi$.

(e) [7, *Theorem* 12.14] *If* $\mathscr{L}(\mathfrak{A}:\boldsymbol{D})$ *and* $\mathscr{L}(\mathfrak{A}':\boldsymbol{E})$ *are isomorphic and finite dimensional where* $\boldsymbol{D}=\{D_1, \ldots, D_m\}$ *and* $\boldsymbol{E}=\{E_1, \ldots, E_s\}$ *are systems satisfying* (2.2) *and* (2.3) *then* $m=s$.

(f) [8, *Corollary* 1.2] *If* $\boldsymbol{D}=\{D_1, \ldots, D_m\}$ *is a system of derivations of* $\mathfrak{A}(n:\mathbf{1})$ *satisfying* (2.2) *and* (2.3) *and if* $p>2$ *then* $\dim \operatorname{Der} \mathscr{L}(\mathfrak{A}(n:\mathbf{1}):\boldsymbol{D}) = mp^n+n-m$.

We will now apply these results to the proof of Theorem 1. By Lemma 2 we have $W(m:\boldsymbol{n}) \cong \mathscr{L}(\mathfrak{A}(m:\boldsymbol{n}):\boldsymbol{D})$ where $\boldsymbol{D}=\{D_1|\mathfrak{A}(m:\boldsymbol{n}), \ldots, D_m|\mathfrak{A}(m:\boldsymbol{n})\}$ and the D_i are defined by (1.7). Since $\boldsymbol{D}$ is clearly an orthogonal system satisfying (2.2) and (2.3), Proposition 1(b) shows that $W(m:\boldsymbol{n})$ is isomorphic to a generalized Witt algebra. This proves Theorem 1(a).

For the proof of Theorem 1(b) we wish to find a system $\boldsymbol{E}$ of derivations of $\mathfrak{A}(n:\mathbf{1})$ such that $W(m:\boldsymbol{n}) \cong L(\mathfrak{A}(n:\mathbf{1}):\boldsymbol{E})$. To do this set $l_1=0$, $l_i=\sum_{j=1}^{i-1} n_j$ for

$2 \leqq i \leqq m$, and $n = \sum_{j=1}^{m} n_j$. Then if $\boldsymbol{y}$ is a system of standard generators for $\mathfrak{A}(n:\mathbf{1})$ we see (using (1.1) and the fact that $\{x^\alpha \mid \alpha \in \mathfrak{A}(m:\boldsymbol{n})\}$ is a basis for $\mathfrak{A}(m:\boldsymbol{n})$) that the map $\tau: x^{p^k \varepsilon_i} \to (-1)^k y_{l_i+k+1}$ for $1 \leqq i \leqq m$ and $0 \leqq k < n_i$ extends to an isomorphism of $\mathfrak{A}(m:\boldsymbol{n})$ onto $\mathfrak{A}(n:\mathbf{1})$. It is easily seen that the derivation $\tau^{-1} D_i \tau$ of $\mathfrak{A}(n:\mathbf{1})$ is equal to $C_{l_i+1}(\boldsymbol{y}) - C_{l_{i+1}+1}(\boldsymbol{y})(y_{l_i+1} \cdots y_{l_{i+1}})$ for $1 \leqq i < m$ and that $\tau^{-1} D_m \tau = C_{l_m+1}(\boldsymbol{y})$. Thus $\{\tau^{-1} D_1 \tau, \ldots, \tau^{-1} D_m \tau\}$ is equivalent to $\{C_{l_i+1}(\boldsymbol{y}) \mid 1 \leqq i \leqq m\}$ and hence $W(m:\boldsymbol{n})$ is isomorphic to $\mathscr{L}(\mathfrak{A}(n:\mathbf{1}) : C_{l_1+1}(\boldsymbol{y}), \ldots, C_{l_m+1}(\boldsymbol{y}))$.

Now by Proposition 1(a–c) any generalized Witt algebra is isomorphic to some $\mathscr{L}(\mathfrak{A}(n:\mathbf{1}):\boldsymbol{D})$ where $\boldsymbol{D}$ is an orthogonal system of derivations satisfying (2.2) and (2.3). Thus Theorem 1(b) follows from

LEMMA 3. *If $\boldsymbol{D}$ is an orthogonal system of derivations of $\mathfrak{A}(n:\mathbf{1})$ satisfying* (2.2) *and* (2.3) *then there exists a sequence of integers $0 = l_1 < l_2 < \cdots < l_m < n$ and a system of standard generators $\boldsymbol{y}$ of $\mathfrak{A}(n:\mathbf{1})$ such that $\boldsymbol{D}$ is equivalent to $\{C_{l_i+1}(\boldsymbol{y}) \mid 1 \leqq i \leqq m\}$.*

We will prove Lemma 3 in the next section.

We now determine the derivation algebra of $W(m:\boldsymbol{n})$. This result will be used in the proof of Theorem 1(c).

LEMMA 4. Der $W(m:\boldsymbol{n})$ *has basis* $B_1(m:\boldsymbol{n}) \cup B_2(m:\boldsymbol{n})$ *where* $B_1(m:\boldsymbol{n}) = \{\text{ad } D_i x^\alpha \mid 1 \leqq i \leqq m, \alpha \in A(m:\boldsymbol{n})\}$, *and* $B_2(m:\boldsymbol{n}) = \{(\text{ad } D_i)^{p^k} \mid 1 \leqq i \leqq m, 1 \leqq k < n_i\}$.

Proof. It is easily seen that $B_1(m:\boldsymbol{n}) \cup B_2(m:\boldsymbol{n})$ consists of $mp^n + n - m$ linearly independent derivations of $W(m:\boldsymbol{n})$. If $p > 2$ Proposition 1(f) shows that $B_1(m:\boldsymbol{n}) \cup B_2(m:\boldsymbol{n})$ must be a basis for Der $W(m:\boldsymbol{n})$. Thus it is necessary only to show that $B_1(m:\boldsymbol{n}) \cup B_2(m:\boldsymbol{n})$ spans Der $W(m:\boldsymbol{n})$ when $p = 2$. (The proof we give for this does not, in fact, depend on p.) The proof has several steps.

(1) For $1 \leqq i \leqq m$ define U_i to be the subspace of $W(m:\boldsymbol{n})$ spanned by $\{D_j x^\alpha \mid 1 \leqq j \leqq m, \alpha(i) = p^{n_i} - 1\}$. Then if $\mathscr{D}$ is a derivation of $W(m:\boldsymbol{n})$ such that $D_j \mathscr{D} = 0$ for all $j < i$ there exists $D \in W(m:\boldsymbol{n})$ such that $D_j(\mathscr{D} + \text{ad } D) = 0$ for all $j < i$ and $D_i(\mathscr{D} + \text{ad } D) \in U_i$.

Proof. Let $D_i \mathscr{D} = \sum D_k x^\alpha a(k, \alpha)$ where the summation extends over all $\alpha \in A(m:\boldsymbol{n})$ and all $k \in \boldsymbol{Z}$, $1 \leqq k \leqq m$. If $j < i$ then $0 = [D_i, D_j]\mathscr{D} = [D_i \mathscr{D}, D_j] = \sum D_k x^{\alpha - \varepsilon_j} a(k, \alpha)$ (by (1.10)). Hence if $j < i$ and $\alpha(j) \neq 0$ then $a(k, \alpha) = 0$ for all k. Hence setting $D = \sum D_k x^{\alpha + \varepsilon_i} a(k, \alpha)$ where the summation extends over all k, $1 \leqq k \leqq m$, and over all $\alpha \in A(m:\boldsymbol{n})$ such that $\alpha(i) \neq p^{n_i} - 1$ gives the result.

(2) If $\mathscr{D}$ is a derivation of $W(m:\boldsymbol{n})$ such that $D_i \mathscr{D} \in U_i$ then $D_i \mathscr{D} = 0$.

Proof. Let $D_i \mathscr{D} = \sum D_k x^\alpha a(k, \alpha)$ as in (1). Note that $U_i \cap (W(m:\boldsymbol{n}) \text{ ad } D_i) = (0)$. Now by (1.11) we see that $[(D_i x_i)\mathscr{D}, D_i] = D_i \mathscr{D} - [D_i x_i, D_i \mathscr{D}] \in U_i \cap (W(m:\boldsymbol{n}) \text{ ad } D_i)$ so $D_i \mathscr{D} = [D_i x_i, D_i \mathscr{D}]$. Thus by (1.11) we see that

$$\sum D_k x^\alpha a(k, \alpha) = \sum D_k x^\alpha (\delta_{ik} - \alpha(i)) a(k, \alpha).$$

Thus $\alpha(i) a(i, \alpha) = 0$ for all α. Since $a(i, \alpha) \neq 0$ implies that $\alpha(i) \equiv -1 \pmod{p}$ this shows that $a(i, \alpha) = 0$ for all α. If $m = 1$ this shows that $D_i \mathscr{D} = 0$ as required. If $m > 1$ and $j \neq i$

then $[D_i, D_j\mathscr{D}] = -[D_i\mathscr{D}, D_j] \in U_i \cap (W(m:\boldsymbol{n}) \text{ ad } D_i)$ so $[D_i\mathscr{D}, D_j]=0$. Similarly $[D_i\mathscr{D}, D_jx_j]=0$. Then (1.10) and (1.11) show that $D_i\mathscr{D}=0$.

(3) Define a partial order on $\boldsymbol{Z}^m$ by $\boldsymbol{r} \leqq \boldsymbol{n}$ if and only if $r_i \leqq n_i$ for $1 \leqq i \leqq m$. Then if $\mathscr{D}$ is a derivation of $W(m:\boldsymbol{n})$ there exists $\boldsymbol{E}$ in the linear span of $B_1(m:\boldsymbol{n})$ such that $W(m:\boldsymbol{r})(\mathscr{D}-\mathscr{E}) \subseteq W(m:\boldsymbol{r})$ for all $\boldsymbol{r} \leqq \boldsymbol{n}$ and $W(m:\mathbf{1})(\mathscr{D}-\mathscr{E})=(0)$.

Proof. It is easily seen that if $\boldsymbol{r} \leqq \boldsymbol{n}$ then

$$W(m:\boldsymbol{r}) = \{D \in W(m:\boldsymbol{n}) \mid D(\text{ad } D_i)^{p^{n_i}}=0 \text{ for all } i,\ 1 \leqq i \leqq m\}.$$

Now by (1) and (2) we can find an inner derivation $\mathscr{E}_1$ such that $D_i(\mathscr{D}-\mathscr{E}_1)=0$ for $1 \leqq i \leqq m$. Then by the above characterization of $W(m:\boldsymbol{r})$, $W(m:\boldsymbol{r})(\mathscr{D}-\mathscr{E}_1) \subseteq W(m:\boldsymbol{r})$. Since every derivation of $W(m:\mathbf{1})$ is inner (by [2, Theorem 12]) we can find an inner derivation $\mathscr{E}_2$ of $W(m:\boldsymbol{n})$ such that $W(m:\mathbf{1})(\mathscr{D}-\mathscr{E}_1-\mathscr{E}_2)=(0)$. Since the linear span of $B_1(m:\boldsymbol{n})$ is equal to the ideal of inner derivations of $W(m:\boldsymbol{n})$, this proves (3).

(4) If $\mathscr{D}$ is a derivation of $W(m:\boldsymbol{n})$ such that $W(m:\mathbf{1})\mathscr{D}=(0)$ and if $\beta \in A(m:\boldsymbol{n})$ is such that $D_jx^\alpha\mathscr{D}=0$ for all j, $1 \leqq j \leqq m$, and all $\alpha < \beta$ but $D_ix^\beta\mathscr{D} \neq 0$ for some i, then $\beta = p^w\varepsilon_k$ for some $w, k \in \boldsymbol{Z}$, $1 \leqq k \leqq m$ and $D_ix^\beta\mathscr{D} = D_ia$ where $a \in \Phi$.

Proof. If there exist l, k, $1 \leqq l \neq k \leqq m$, such that $\beta(k) \neq 0$ and $\beta(l) \neq 0$ then (taking $k \neq i$)

$$(D_ix^\beta)\mathscr{D} = [D_ix^{\beta-(\beta(k)-1)\varepsilon_k}, D_kx^{\beta(k)\varepsilon_k}]\mathscr{D} = 0,$$

a contradiction. Hence $\beta = s\varepsilon_k$ for some $s, k \in \boldsymbol{Z}$. Now as $[D_ix^\beta, D_j]\mathscr{D}=0$ for $1 \leqq j \leqq m$ we have $(D_ix^\beta)\mathscr{D} = \sum D_la_l$ where the $a_l \in \Phi$. Then by (1.11) for $1 \leqq j \leqq m$ we have $-D_ja_j = [\sum D_la_l, D_jx_j] = [D_ix^\beta, D_jx_j]\mathscr{D} = \sum D_la_l(\beta(j)-\delta_{ij})$. Setting $j=i$ we see that $a_l=0$ for all $l \neq i$ whenever $\beta(i)=0$. But if $\beta(i) \neq 0$ then $\beta(l)=0$ and setting $j=l$ we again see that $a_l=0$. Hence $(D_ix^\beta)\mathscr{D} = D_ia$ where $a \in \Phi$.

Now for $0 < r < s$ we have

$$\begin{aligned}[D_ix^\beta, D_kx^{r\varepsilon_k}]\mathscr{D}(\text{ad } D_k)^{r-1} &= [D_ix^\beta, D_kx^{r\varepsilon_k}](\text{ad } D_k)^{r-1}\mathscr{D} \\ &= D_ia(C(s+r-1, r) - \delta_{ik}C(s+r-1, r-1)).\end{aligned}$$

Also

$$[D_ix^\beta, D_kx^{r\varepsilon_k}]\mathscr{D}(\text{ad } D_k)^{r-1} = [(D_ix^\beta)\mathscr{D}, D_kx^{r\varepsilon_k}](\text{ad } D_k)^{r-1} = -D_ia\delta_{ik}.$$

Thus $C(s+r-1, r) - \delta_{ik}C(s+r-1, r-1) = -\delta_{ik}$ for $0 < r < s$. Hence by (1.12) and (1.13) we see that $s = p^w$ as required.

(5) If $\mathscr{D}$ is a derivation of $W(m:\boldsymbol{n})$ and if $W(m:\boldsymbol{r})\mathscr{D}=(0)$ where $\mathbf{1} \leqq \boldsymbol{r} < \boldsymbol{n}$ and $r_i < n_i$ for some i, $1 \leqq i \leqq m$, then there exists $\mathscr{E}$ in the linear span of $B_2(m:\boldsymbol{n})$ such that $W(m : r_1, \ldots, r_i+1, \ldots, r_m)(\mathscr{D}-\mathscr{E})=(0)$.

Proof. If $W(m : r_1, \ldots, r_i+1, \ldots, r_m)\mathscr{D}=(0)$ we take $\mathscr{E}=0$. If not there exists some $\beta \in A(m : r_1, \ldots, r_i+1, \ldots, r_m)$ satisfying the hypotheses of (4). Then by (4) (and the fact that $W(m:\boldsymbol{r})\mathscr{D}=(0)$) we see that $\beta = p^{r_i}\varepsilon_i$. Setting $\mathscr{E} = (\text{ad } D_i)^{p^{r_i}}a$ where a is as in (4) we have $(D_ix^{p^{r_i}\varepsilon_i})(\mathscr{D}-\mathscr{E})=0$. Now if $j \neq i$ then $(D_jx^{p^{r_i}\varepsilon_i})(\mathscr{D}-\mathscr{E}) = [D_jx_i, D_ix^{p^{r_i}\varepsilon_i}](\mathscr{D}-\mathscr{E})=0$. Hence $W(m : r_1, \ldots, r_i+1, \ldots, r_m)(\mathscr{D}-\mathscr{E})=(0)$ as required.

Lemma 4 now follows from (3) and (5) by induction on $\boldsymbol{n}$.

We now prove Theorem 1(c). If $r_i=n_{\sigma(i)}$ for $1\leqq i\leqq m$ where σ is a permutation of $\{1,\dots,m\}$ then it is clear from the definitions that $W(m:\boldsymbol{n})$ and $W(m:\boldsymbol{r})$ are isomorphic. Conversely suppose that $W(m:\boldsymbol{n})$ and $W(s:\boldsymbol{r})$ are isomorphic. Then by Proposition 1(e) $m=s$. Since (by the preceding remark) we may rearrange the n_i and the r_i, we may assume that $n_1\geqq n_2\geqq\cdots\geqq n_m$ and $r_1\geqq r_2\geqq\cdots\geqq r_m$. Now define

$$W(m:\boldsymbol{n})_{(0)} = \{D\in W(m:\boldsymbol{n}) \mid (\text{ad } D)^p \text{ is an inner derivation}\}$$

and for $i\in \boldsymbol{N}$, $i>0$, define

$$W(m:\boldsymbol{n})_{(i)} = \{D\in W(m:\boldsymbol{n})_{(i-1)} \mid W(m:\boldsymbol{n})(\text{ad } D) \subseteq W(m:\boldsymbol{n})_{(i-1)}\}.$$

Then clearly $W(m:\boldsymbol{n})_{(i)}\cong W(m:\boldsymbol{r})_{(i)}$ for all $i\in\boldsymbol{N}$. We will show that this implies that $r_i=n_i$ for $1\leqq i\leqq m$ thus proving Theorem 1(c). The proof has several steps.

(1) If $\sum D_i a_i\in W(m:\boldsymbol{n})$ define $|\sum D_i a_i|=\min |a_i|$. Then a derivation $\mathscr{E}$ of $W(m:\boldsymbol{n})$ is inner if and only if $|D\mathscr{E}|\geqq |D|-1$ for every $D\in W(m:\boldsymbol{n})$.

Proof. From (1.8) we see that if $\mathscr{E}$ is inner then $|D\mathscr{E}|\geqq|D|-1$ for all $D\in W(m:\boldsymbol{n})$. If $\mathscr{E}$ is an outer derivation then by Lemma 4 $\mathscr{E}=\sum_{i=1}^{m}\sum_{j=1}^{n_i-1}(\text{ad } D_i)^{p^j}\alpha_{ij}+$ ad E' where the $\alpha_{ij}\in\Phi$, $E'\in W(m:\boldsymbol{n})$ and some $\alpha_{kl}\neq 0$. Then setting $D=D_1x^{p^l\varepsilon_k}$ we have $|D\mathscr{E}|=0<p^l-1=|D|-1$.

(2) $W(m:\boldsymbol{n})_{(0)}=\langle D_i x^{\alpha}\mid 1\leqq i\leqq m,\ |\alpha|\geqq 1-\delta_{1,n_i}\rangle$.

Proof. By formula (ii), p. 188 of [3], if $\mathscr{L}$ is a Lie algebra over Φ and $a,b\in\mathscr{L}$ then $(\text{ad}(a+b))^p=(\text{ad } a)^p+(\text{ad } b)^p+\text{ad } c$ for some $c\in\mathscr{L}$. Hence $W(m:\boldsymbol{n})_{(0)}$ is a subspace of $W(m:\boldsymbol{n})$. Now if $|\alpha|>0$ and $D\in W(m:\boldsymbol{n})$ then (1.8) shows that $|D(\text{ad } D_i x^{\alpha})|\geqq|D|$ for all i, $1\leqq i\leqq m$. Hence $|D(\text{ad } D_i x^{\alpha})^p|\geqq|D|$ for all $D\in W(m:\boldsymbol{n})$ so that by (1) $(\text{ad } D_i x^{\alpha})^p$ is an inner derivation for all i, $1\leqq i\leqq m$. If $n_i=1$ then $(\text{ad } D_i)^p=0$ and hence is an inner derivation. Hence $W(m:n)_{(0)}\supseteq \langle D_i x^{\alpha}\mid 1\leqq i\leqq m,\ |\alpha|\geqq 1-\delta_{1,n_i}\rangle$. If the inclusion is proper then, since $W(m:\boldsymbol{n})_{(0)}$ is a subspace, there is some $0\neq D=\sum_{n_i\neq 1} D_i a_i\in W(m:\boldsymbol{n})_{(0)}$ where the $a_i\in\Phi$. Then $(\text{ad } D)^p=\sum_{n_i\neq 1}(\text{ad } D_i)^p a_i^p$ is an inner derivation, contradicting the linear independence of $B_1(m:\boldsymbol{n})\cup B_2(m:\boldsymbol{n})$.

(3) For $k\in\boldsymbol{N}$ define a subset $T_k\subseteq W(m:\boldsymbol{n})$ by $T_k=\langle D_i x^{\alpha}\mid 1\leqq i\leqq m,\ |\alpha|\geqq k+1-\delta_{1,n_i}\rangle$. If $n_1>1$ then $T_{k+1}=\{D\in T_k\mid W(m:\boldsymbol{n})(\text{ad } D)\subseteq T_k\}$ for all $k\in\boldsymbol{N}$.

Proof. It is immediate from (1.8) that

$$T_{k+1}\subseteq\{D\in T_k \mid W(m:\boldsymbol{n})(\text{ad } D)\subseteq T_k\}\quad\text{for all } k\in\boldsymbol{N}.$$

Conversely assume that $D=\sum D_i x^{\alpha} a_{i,\alpha}\in T_k$ and that $W(m:\boldsymbol{n})(\text{ad } D)\subseteq T_k$. Then in particular $D_j(\text{ad } D)\in T_k$ for all j, $1\leqq j\leqq m$. Thus if $\alpha(j)\neq 0$ and $a_{i,\alpha}\neq 0$ we have $|\alpha-\varepsilon_j|\geqq k+1-\delta_{1,n_i}$ so that $|\alpha|\geqq k+2-\delta_{1,n_i}$ and hence $D_i x^{\alpha}\in T_{k+1}$. Thus $D\in T_{k+1}$ unless $a_{i,0}\neq 0$ for some i, $1\leqq i\leqq m$. But then $(D_1x_i)(\text{ad } D)=\sum D_l x^{\alpha} b_{l,\alpha}\in T_k$ where $b_{1,0}\neq 0$. But this implies that $0\geqq k+1-\delta_{1,n_1}\geqq 1$, a contradiction. Thus $D\in T_{k+1}$ proving (3).

(4) For $k \in N$ define $A(k:m:\boldsymbol{n})=\{\alpha \in A(m:\boldsymbol{n}) \mid |\alpha|=k\}$. Define $P(k:m:\boldsymbol{n})$ to be the cardinality of $A(k:m:\boldsymbol{n})$. Let $m=m'+m''$ where m' is the number of i such that $n_i>1$. Then if $m'>0$,

(2.4) $\dim W(m:\boldsymbol{n})/W(m:\boldsymbol{n})_{(0)}=m'$.

(2.5) $\dim W(m:\boldsymbol{n})_{(i)}/W(m:\boldsymbol{n})_{(i+1)}=m'P(i+1:m:\boldsymbol{n})+m''P(i:m:\boldsymbol{n})$ for all $i \in N$.

Proof. Since $m'>0$ it follows from (2) and (3) that $W(m:\boldsymbol{n})_{(i)}=T_i$ for all $i \in N$. Since T_i/T_{i+1} has basis

$$\begin{aligned}\{D_j x^\alpha+T_{i+1} \mid 1 \leqq j \leqq m, |\alpha| = i+1-\delta_{1,n_j}\} \\ = \{D_j x^\alpha+T_{i+1} \mid 1 \leqq j \leqq m', \alpha \in A(i+1:m:\boldsymbol{n})\} \\ \cup \{D_j x^\alpha+T_{i+1} \mid m' < j \leqq m, \alpha \in A(i:m:\boldsymbol{n})\},\end{aligned}$$

the result is immediate.

(5) If $n_i>r_i$ and $n_j=r_j$ for $i<j\leqq m$ then $P(p^{r_i}-1:m:\boldsymbol{n})=P(p^{r_i}-1:m:\boldsymbol{r})$ and $P(p^{r_i}:m:\boldsymbol{n})>P(p^{r_i}:m:\boldsymbol{r})$.

Proof. Clearly $A(p^{r_i}-1:m:\boldsymbol{n})\supseteq A(p^{r_i}-1:m:\boldsymbol{r})$. Let $\alpha \in A(p^{r_i}-1:m:\boldsymbol{n})$. Then if $j\geqq i+1$ we have $\alpha(j)<p^{n_j}=p^{r_j}$ and if $j\leqq i$ we have $\alpha(j)\leqq|\alpha|=p^{r_i}-1<p^{r_i}\leqq p^{r_j}$. Hence $\alpha \in A(p^{r_i}-1:m:\boldsymbol{r})$. Thus $P(p^{r_i}-1:m:\boldsymbol{n})=P(p^{r_i}-1:m:\boldsymbol{r})$. Also $A(p^{r_i}:m:\boldsymbol{n})\supseteq A(p^{r_i}:m:\boldsymbol{r})$ but $p^{r_i}\varepsilon_i \in A(p^{r_i}:m:\boldsymbol{n})$ and $p^{r_i}\varepsilon_i \notin A(p^{r_i}:m:\boldsymbol{r})$ so $P(p^{r_i}:m:\boldsymbol{n})>P(p^{n_i}:m:\boldsymbol{r})$.

(6) $n_i=r_i$ for $1\leqq i\leqq m$.

Proof. If not we may assume (interchanging the n's and the r's if necessary) that for some i we have $n_i>r_i$ and $n_j=r_j$ for $i<j\leqq m$. Then $n_1>1$ so by (2) $W(m:\boldsymbol{n})$ is not restricted. Then $W(m:\boldsymbol{r})$ is not restricted since it is isomorphic to $W(m:\boldsymbol{n})$. Hence, again by (2), $r_1>1$. Now we must have $\dim W(m:\boldsymbol{n})_{(i)}=\dim W(m:\boldsymbol{r})_{(i)}$ for all $i \in N$. Thus by (2.4) $m'=$(number of i such that $n_i>1$)$=$(number of i such that $r_i>1$). Then by (2.5)

$$m'P(p^{r_i}:m:\boldsymbol{n})+m''P(p^{r_i}-1:m:\boldsymbol{n}) = m'P(p^{r_i}:m:\boldsymbol{r})+m''P(p^{r_i}-1:m:\boldsymbol{r}).$$

But this contradicts (5).

This completes the proof of Theorem 1(c).

3. **Proof of Lemma 3.** In this section we prove Lemma 3 and thus complete the proof of Theorem 1. We continue to assume that Φ is an algebraically closed field of characteristic $p>0$. We begin by showing that Lemma 3 is a consequence of the following weaker result:

Lemma 3′. *If $\boldsymbol{D}=\{D_1, \ldots, D_m\}$ is an orthogonal system of deviations of $\mathfrak{A}(n:\mathbf{1})$ satisfying* (2.2) *and* (2.3) *and if $m\geqq 2$ then there exists an integer l_2, $0<l_2<n$, a system of derivations $\boldsymbol{E}$ equivalent to $\boldsymbol{D}$, and a system of standard generators $\boldsymbol{y}$ of $\mathfrak{A}(n:\mathbf{1})$ such that*

$$\begin{aligned} E_1 &= C_1(\boldsymbol{y}), \\ E_2 &= C_{l_2+1}(\boldsymbol{y}), \\ E_i &= \sum_{j=l_2+2}^{n} C_j(\boldsymbol{y})\alpha_{ij} \quad \textit{for } i > 2 \textit{ where the } \alpha_{ij} \in \Phi. \end{aligned} \tag{3.1}$$

Note that for $m=1$ Lemma 3 is a restatement of Proposition 1(c), (d) and for $m=2$ Lemmas 3 and 3′ are identical. Assume that $m>2$, that Lemma 3′ holds and that Lemma 3 holds for $m-1$. Let l_2, $\boldsymbol{E}$, and $\boldsymbol{y}$ be as in the conclusion of Lemma 3′. Let $\mathfrak{B}$ be the subalgebra of $\mathfrak{A}(n{:}\mathbf{1})$ generated by $\{y_i \mid i>l_2\}$. Then for $i\geqq 2$ E_i stabilizes $\mathfrak{B}$ and $\{E_2|\mathfrak{B},\dots,E_m|\mathfrak{B}\}$ is a system of derivations of $\mathfrak{B}$ satisfying (2.2) and (2.3). Hence by the induction assumption there exists a system of standard generators $\{z_i \mid l_2<i\leqq n\}$ of $\mathfrak{B}$, a system of derivations $\{F_2,\dots,F_m\}$ of $\mathfrak{B}$ equivalent over $\mathfrak{B}$ to $\{E_2|\mathfrak{B},\dots,E_m|\mathfrak{B}\}$, and a sequence of integers $l_2<l_3<\cdots<l_m$ such that $F_i=C_{l_i+1}(\boldsymbol{z})$ for $2\leqq i\leqq m$. Thus $F_i=\sum (E_j|\mathfrak{B})c_{ij}$ for $2\leqq i\leqq m$ where the $c_{ij}\in\mathfrak{B}$. Setting $G_i=\sum E_jc_{ij}$ for $2\leqq i\leqq m$, $z_i=y_i$ for $1\leqq i\leqq l_2$, and

$$G_1 = E_1+(G_2-E_2)(z_1\cdots z_{l_2})^{p-1}$$

we see that $\boldsymbol{G}$ and $\boldsymbol{z}$ satisfy the conclusions of Lemma 3. Thus Lemma 3 is a consequence of Lemma 3′.

Now let $\boldsymbol{D}$ be as in Lemma 3′. Let S be the set of all pairs $(\boldsymbol{y},\boldsymbol{E})$ where $\boldsymbol{y}$ is a system of standard generators for $\mathfrak{A}(n{:}\mathbf{1})$ and $\boldsymbol{E}$ is a system of derivations of $\mathfrak{A}(n{:}\mathbf{1})$ equivalent to $\boldsymbol{D}$ and such that there is a sequence of integers $0<l_2<\cdots<l_m<n$ such that

$$\begin{aligned} E_1 &= C_1(\boldsymbol{y}), \\ E_i &= C_{l_i+1}(\boldsymbol{y})+\sum_{j=l_i+2}^{n} C_j(\boldsymbol{y})\alpha_{ij} \quad \text{for } i \geqq 2 \text{ where the } \alpha_{ij}\in\Phi. \end{aligned} \tag{3.2}$$

By applying Proposition 1(c), (d) and the usual procedure for reducing a matrix to triangular form it is easily seen that S is nonempty.

For $(\boldsymbol{y},\boldsymbol{E})\in S$ define $t(\boldsymbol{y},\boldsymbol{E})$ to be the m-tuple $(l_m,\dots,l_2,l)$ where the l_i are as in (3.2) and $l=\max\{i \mid l_2+1\leqq i\leqq n,\ \alpha_{2,j}=0 \text{ whenever } l_2+2\leqq j\leqq i\}$. Since $l=n$ is equivalent to $E_2=C_{l_2+1}(\boldsymbol{y})$ we see that Lemma 3′ is equivalent to the statement that there exists some $(\boldsymbol{y},\boldsymbol{E})\in S$ such that $t(\boldsymbol{y},\boldsymbol{E})=(l_m,\dots,l_2,n)$. The proof of this statement has several steps.

(1) (Ree [7, p. 535]) Let $(\boldsymbol{y},\boldsymbol{E})\in S$ and $t(\boldsymbol{y},\boldsymbol{E})=(l_m,\dots,l_2,l)$. Then if $l\neq n$ there exists $(\boldsymbol{y}',\boldsymbol{E}')\in S$ with $t(\boldsymbol{y},\boldsymbol{E})=t(\boldsymbol{y}',\boldsymbol{E}')$ and $\alpha'_{2,l+1}=1$.

Proof. Set $y_i'=\lambda^{p^{i-1}}y_i$ and $E_i'=E_i\lambda^{-p^{l_i}}$ where λ is a $(p^l-p^{l_2})$ root of $\alpha_{2,l+1}^{-1}$.

(2) For $\alpha\in A(n{:}\mathbf{1})$ define $\|\alpha\|=\sum_{i=1}^{n}\alpha(i)p^{i-1}$. If $0\neq a=\sum a_\alpha \boldsymbol{y}^\alpha$ where $\boldsymbol{y}$ is a system of standard generators for $\mathfrak{A}(n{:}\mathbf{1})$ and the $a_\alpha\in\Phi$ define $\|a\|=\max\{\|\alpha\| \mid a_\alpha\neq 0\}$. Define $\|0\|=-1$. Let E be a derivation of $\mathfrak{A}(n{:}\mathbf{1})$ such that $\|y_iE\|=p^{i-1}-1$ for all i, $1\leqq i\leqq n$. Then $\|fE\|=\|f\|-1$ for all $f\in\mathfrak{A}(n{:}\mathbf{1})$, $f\neq 0$. Consequently E is a normal nilpotent derivation.

Proof. Clearly $\|\ \|$ satisfies:

(3.3) $\|fg\|\leqq\|f\|+\|g\|$.

(3.4) If $\|f\|>\|g\|$ then $\|f+g\|=\|f\|$.

Now $\boldsymbol{y}^\alpha E=\sum_{i=1}^{n}(y_iE)\boldsymbol{y}^{\alpha-\varepsilon_i}$. By (3.3)

$$\|(y_iE)\boldsymbol{y}^{\alpha-\varepsilon_i}\| \leqq \|\alpha\|-p^{i-1}+(p^{i-1}-1) = \|\alpha\|-1.$$

Furthermore equality holds if and only if $(y_1\cdots y_{i-1})^{p-1}y^{\alpha-\varepsilon_i}\neq 0$, i.e., if and only if $\alpha(i)\neq 0$ and $\alpha(j)=0$ for $j<i$. Hence equality holds for exactly one i and so by (3.4) $\|y^\alpha E\|=\|y^\alpha\|-1$. From this it is easily seen that $\|fE\|=\|f\|-1$ for all $f\in \mathfrak{A}(n:\mathbf{1}), f\neq 0$.

(3) If E is a normal derivation of $\mathfrak{A}(n:\mathbf{1})$ and $x_1,\ldots,x_r$; $y_1,\ldots,y_r$ are two sequences of elements of $\mathfrak{A}(n:\mathbf{1})$ such that $x_1E=y_1E$, $x_iE=(x_1\cdots x_{i-1})^{p-1}$ and $y_iE=(y_1\cdots y_{i-1})^{p-1}$ for $2\leqq i\leqq r$, and $x_i^p=y_i^p$ for $1\leqq i\leqq r$ then $x_i=y_i$ for $1\leqq i\leqq r$.

Proof. Since $(x_1-y_1)E=0$ we have $x_1-y_1\in\Phi$. Then $0=(x_1^p-y_1^p)=(x_1-y_1)^p$ so $x_1=y_1$. If $x_1=y_1,\ldots,x_{i-1}=y_{i-1}$ then $(x_i-y_i)E=0$ so as above $x_i=y_i$.

(4) Let $\boldsymbol{y}$ and E be as in (2). Denote by $\mathfrak{A}_{(i)}$ the subalgebra of $\mathfrak{A}(n:\mathbf{1})$ generated by $y_1,\ldots,y_i$. Then there exists a system of standard generators $\boldsymbol{z}$ of $\mathfrak{A}(n:\mathbf{1})$ such that $E=C_1(\boldsymbol{z})$ and $z_i\in\mathfrak{A}_{(i)}$ for all i, $1\leqq i\leqq n$.

Proof. By (2) E is a normal derivation of $\mathfrak{A}(n:\mathbf{1})$. Moreover since $\|y_iE\|=p^{i-1}-1$ we have $y_iE\in\mathfrak{A}_{(i)}$ for all i, $1\leqq i\leqq n$. Thus E restricts to a normal derivation of $\mathfrak{A}_{(i)}$. Now by Proposition 1(d) there exists a system of standard generators $\boldsymbol{z}$ of $\mathfrak{A}(n:\mathbf{1})$ such that $E=C_1(\boldsymbol{z})$. Also there exists a system of standard generators $\{t_1,\ldots,t_i\}$ of $\mathfrak{A}_{(i)}$ such that $E|\mathfrak{A}_{(i)}=C_1(\boldsymbol{t})$. Then by (3) $z_i=t_i\in\mathfrak{A}_{(i)}$.

(5) (Jennings and Ree [4, p. 193]) Let $\{D_1,\ldots,D_m\}$ be an orthogonal system of derivations of $\mathfrak{A}$. Let $E_i=\sum_{j=1}^m D_jc_{ij}$ for $1\leqq i\leqq m$ where the $c_{ij}\in\mathfrak{A}$. Then $[E_i,E_j]=0$ if and only if $c_{jl}E_i=c_{il}E_j$ for all l, $1\leqq l\leqq m$.

Proof.

$$\begin{aligned}[E_i,E_j] &= \sum_{k=1}^m\sum_{l=1}^m [D_kc_{ik},D_lc_{jl}]\\ &= \sum_{k=1}^m\sum_{l=1}^m D_k(c_{ik}D_l)c_{jl}-D_l(c_{jl}D_k)c_{ik}\\ &= \sum_{k=1}^m D_k(c_{ik}E_j-c_{jk}E_i).\end{aligned}$$

(6) Let $(\boldsymbol{y},\boldsymbol{E})\in S$, $t(\boldsymbol{y},\boldsymbol{E})=(l_m,\ldots,l_2,l)$, $l\neq n$, $\alpha_{2,l+1}=1$, and $l_m<l-l_2$. Then there exists a system of derivations $\boldsymbol{F}$ equivalent to $\boldsymbol{E}$ over $\mathfrak{A}_{(l)}$ and a system of standard generators $\boldsymbol{z}$ of $\mathfrak{A}(n:\mathbf{1})$ such that $(\boldsymbol{z},\boldsymbol{F})\in S$ and $t(\boldsymbol{z},\boldsymbol{F})>t(\boldsymbol{y},\boldsymbol{E})$ in the lexicographic ordering.

Proof. For $1\leqq i\leqq m$ define $G_i=\sum_{j=1}^m E_jc_{ij}$ where $c_{11}=(y_{l_2+1}\cdots y_l)^{p-1}$, $c_{12}=(1-(y_1\cdots y_l)^{p-1})$, $c_{21}=1$, $c_{22}=-(y_1\cdots y_{l_2})^{p-1}$, $c_{i1}=y_{l+1}E_i$ for $2<i\leqq m$, $c_{i2}=-(y_1\cdots y_{l_2})^{p-1}c_{i1}$ for $2<i\leqq m$, and $c_{ij}=\delta_{ij}$ for $1\leqq i\leqq m$ and $2<j\leqq m$.

det (c_{ij}) is a unit so $\boldsymbol{G}$ is a system of derivations equivalent to $\boldsymbol{E}$ over $\mathfrak{A}_{(l)}$ (for all the $c_{ij}\in\mathfrak{A}_{(l)}$). Moreover it is easily checked that $c_{ij}G_1=c_{1j}G_i$ for all i,j, $1\leqq i,j\leqq m$. Hence by (5) $[G_1,G_i]=0$ for $1\leqq i\leqq m$.

We now show that G_1 is normal and nilpotent. Set $w_i=y_{l_2+i}$ for $1\leqq i\leqq l-l_2$, $w_i=y_{i-l+l_2}$ for $l-l_2+1\leqq i\leqq l$, and $w_i=y_i$ for $i>l$. Now it is easily checked that $w_1G_1=1$, $w_iG_1=(w_1\cdots w_{i-1})^{p-1}$ for $2\leqq i\leqq l$, and $w_iG_1=-(w_1\cdots w_{i-1})^{p-1}+$terms in $w_1, \ldots, w_{i-1}$ of degree less than $(p-1)(i-1)$ for $i>l$. Thus $\|w_iG_1\|=p^{i-1}-1$ for all i, $1\leqq i\leqq n$ (where $\|\ \|$ is defined with respect to the system of standard generators $\boldsymbol{w}$). Hence by (2) G_1 is a normal nilpotent derivation. Now by Proposition 1(d) there exists a system of standard generators $\boldsymbol{z}$ of $\mathfrak{A}(n:\mathbf{1})$ such that $C_1(\boldsymbol{z})=G_1$. Also since $[G_1, G_i]=0$ we have $G_i=\sum_{j=1}^{n} C_j(\boldsymbol{z})\beta_{ij}$ for $2\leqq i\leqq m$ where the $\beta_{ij}\in\Phi$. Moreover by (3) for $1\leqq i\leqq l-l_2$ we have $z_i=w_i=y_{l_2+i}$. Hence $z_iG_2=y_{l_2+i}G_2=0$ for $1\leqq i\leqq l-l_2$. Thus $\beta_{2j}=0$ for $1\leqq j\leqq l-l_2$. Now by applying the usual procedure for reduction to triangular form we obtain a system of derivations $\boldsymbol{F}$ such that $(\boldsymbol{z}, \boldsymbol{F})\in S$. If $t(\boldsymbol{z}, \boldsymbol{F})=(k_m, \ldots, k_2, k)$ then $k_m\geqq l-l_2>l_m$. Hence $t(\boldsymbol{z}, \boldsymbol{F})>t(\boldsymbol{y}, \boldsymbol{E})$ as required.

(7) Let $\boldsymbol{y}$ be a system of standard generators for $\mathfrak{A}(n:\mathbf{1})$. If $k>n$ set $C_k(\boldsymbol{y})=0$. Then for $1\leqq i\leqq n$ and $j\in N$, we have $(C_i(\boldsymbol{y}))^{p^j}=(-1)^jC_{i+j}(\boldsymbol{y})$.

Proof. It is easily seen that $(C_i(\boldsymbol{y}))^p$ and $-C_{i+1}(\boldsymbol{y})$ agree on $\boldsymbol{y}$ and hence are equal. The general result follows by induction on j.

(8) The conclusion of (6) still holds if $l_m=l-l_2$.

Proof. Set $F_1=E_1+E_m$ and $F_i=E_i$ for $2\leqq i\leqq m$. Then E_1 satisfies the hypotheses of (2) and hence is normal and nilpotent. Hence there exists a system of standard generators $\boldsymbol{z}$ of $\mathfrak{A}(n:\mathbf{1})$ such that $C_1(\boldsymbol{z})=F_1$. Now since

$$E_1 = C_1(\boldsymbol{y}),$$
$$E_2 = C_{l_2+1}(\boldsymbol{y})+C_{l+1}(\boldsymbol{y})+\sum_{j=l+2}^{n} C_j(\boldsymbol{y})\alpha_{2j},$$

and

$$E_i = C_{l_i+1}(\boldsymbol{y})+\sum_{j=l_i+2}^{n} C_j(\boldsymbol{y})\alpha_{ij} \quad \text{where the } \alpha_{ij}\in\Phi,$$

we have (by (7))

$$(3.5)\qquad F_1^{p^k} = \left\{C_{k+1}(\boldsymbol{y})+C_{l_m+k+1}(\boldsymbol{y})+\sum_{j=l_m+2}^{n} C_{j+k}(\boldsymbol{y})(\alpha_{mj})^{p^k}\right\}(-1)^k.$$

Hence

$$E_2 = F_1^{p^{l_2}}(-1)^{l_2}+\sum_{j=l+2}^{n} C_j(\boldsymbol{y})(\alpha_{2j}-(\alpha_{m,j-l_2})^{p^{l_2}}).$$

Now by (3.5) $C_j(\boldsymbol{y})$ is equal to a Φ linear combination of the $F_1^{p^k}$ for $k\geqq j-1$. Thus there are $\beta_{2j}\in\Phi$ such that

$$F_2 = E_2 = F_1^{p^{l_2}}(-1)^{l_2}+\sum_{j=l+1}^{n-1} F_1^{p^j}\beta_{2,j+1}(-1)^j.$$

Thus by (7)

$$F_2 = C_{l_2+1}(\boldsymbol{z})+\sum_{j=l+2}^{n} C_j(\boldsymbol{z})\beta_{2j}.$$

Similarly we see that

$$F_i = C_{l_i+1}(\boldsymbol{z})+\sum_{j=l_i+2}^{n} C_j(\boldsymbol{z})\beta_{ij} \quad \text{where the } \beta_{ij}\in\Phi$$

for $2<i\leqq m$. Thus $(z, F)\in S$ and $t(z, F)=(l_m, \ldots, l_2, k)$ where $k>l$ so $t(z, F)>t(y, E)$.

(9) If $1\leqq u\leqq v<l_i+1$ and the $\alpha_{ij}\in\Phi$ then

$$\left(C_u(y)+\sum_{j=l_i+1}^{n} C_j(y)\alpha_{ij}(y_u\cdots y_v)^{p-1}\right)^p = -\left(C_{u+1}(y)+\sum_{j=l_i+1}^{n} C_j(y)\alpha_{ij}(y_{u+1}\cdots y_v)^{p-1}\right).$$

Proof. This follows immediately from (7) and formula (ii), p. 188 of [3].

(10) If $1\leqq u<l_i+1$ and $u\leqq v$ then

$$\left(C_1(y)+\sum_{j=l_i+1}^{n} C_j(y)\alpha_{ij}(y_1\cdots y_u)^{p-1}\right)^{p^v} = \left(C_{v+1}(y)+\sum_{j=l_i+1}^{n} C_{j+v-u}(y)(\alpha_{ij})^{p^{v-u}}\right)(-1)^v.$$

Proof. This follows from (7) and (9).

(11) The conclusion of (6) still holds if $l_m>l-l_2$ and $l\geqq l_m$.

Proof. Set $F_1=E_1+E_m(y_1\cdots y_{l_2+l_m-l})^{p-1}$ and $F_i=E_i$ for $i>1$. Then the result follows from (10) exactly as (8) follows from (7).

(12) Let $(y, E)\in S$ and $t(y, E)=(l_m, \ldots, l_2, l)$ where $l\neq n$. Then there exists $(z, F)\in S$ such that F is equivalent to E over $\mathfrak{A}_{(l)}$ and $t(z, F)>t(y, E)$.

Proof. Suppose that (y, E) is a counterexample. Then by (1), (6), (8), and (11) we have $l_m>l-l_2$ and $l<l_m$. Thus since $l>l_2$ we cannot have $m=2$. Thus (12) is proved if $m=2$.

We now proceed by induction on m. Assuming that (12) holds for systems of $m-1$ derivations we see that there is a system of derivations $\{F_1, \ldots, F_{m-1}\}$ equivalent to $\{E_1, \ldots, E_{m-1}\}$ over $\mathfrak{A}_{(l)}$ and a system of standard generators z of $\mathfrak{A}(n{:}\mathbf{1})$ such that $(z, \{F_1, \ldots, F_{m-1}\})$ satisfies (3.2) for appropriate choices of the constants and that $t(y, \{E_1, \ldots, E_{m-1}\})<t(z, \{F_1, \ldots, F_{m-1}\})$. Now E_m vanishes on $\mathfrak{A}_{(l)}$ (since $l<l_m$) so $[E_m, F_1]=0$. Also $\mathfrak{A}_{(l_m)}F_1\subseteq\mathfrak{A}_{(l_m)}$ since each of the E_i stabilizes all the $\mathfrak{A}_{(j)}$, F_1 is an $\mathfrak{A}_{(l)}$ linear combination of the E_i, and $\mathfrak{A}_{(l)}\subseteq\mathfrak{A}_{(l_m)}$. Thus as in (4) we see that $z_i\in\mathfrak{A}_{(l_m)}$ for $1\leqq i\leqq l_m$. Hence $z_iE_m=0$ for $1\leqq i\leqq l_m$. If we set $F_m=E_m$ and apply to F the usual process for reduction to triangular form we obtain a system G equivalent to E over $\mathfrak{A}_{(l)}$ and such that $(z, G)\in S$ and $t(z, G)>t(y, E)$.

(13) There exists some $(y, E)\in S$ with $t(y, E)=(l_m, \ldots, l_2, n)$.

Proof. If $t(y, E)$ is maximal in the lexicographic ordering of $t(S)$ then by (12) $t(y, E)=(l_m, \ldots, l_2, n)$.

As was noted above (13) is equivalent to the conclusion of Lemma 3′. Hence this completes the proof of Lemma 3 and of Theorem 1.

4. **Automorphisms.** In this section we will determine the automorphism group of $W(m{:}\mathbf{n})$. Throughout this section we assume that Φ is an algebraically closed

field of characteristic $p \geqq 5$. We begin by stating some results of Ree which relate automorphisms of $W(m:\boldsymbol{n})$ to automorphisms of $\mathfrak{A}(m:\boldsymbol{n})$.

If $\mathfrak{A}$ is any algebra, $\sigma \in \operatorname{Aut} \mathfrak{A}$, and $D \in \operatorname{Der} \mathfrak{A}$ then $\sigma^{-1} D\sigma$ is again a derivation of $\mathfrak{A}$ which we will denote by D^{σ}. The map $\tilde{\sigma}: D \to D^{\sigma}$ is clearly an endomorphism of Der $\mathfrak{A}$. If W is a subalgebra of Der $\mathfrak{A}$ an automorphism σ of $\mathfrak{A}$ is said to be *admissible to* W if $W\tilde{\sigma} \subseteq W$. The automorphisms of $\mathfrak{A}$ which are admissible to W form a subsemigroup of Aut $\mathfrak{A}$ which we denote by Aut $(\mathfrak{A}: W)$. Clearly the map $\sigma \to \tilde{\sigma}$ is a homomorphism of Aut $(\mathfrak{A}: W)$ into End W. For the pairs $(\mathfrak{A}(m): W(m))$ and $(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ more can be said. Ree [7, p. 544] has proved

PROPOSITION 2. *The map $\sigma \to \tilde{\sigma}$ is an isomorphism of* Aut $(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ *onto* Aut $(W(m:\boldsymbol{n}))$.

We will prove (corollary to Lemma 5) a corresponding (though weaker) result for $\mathfrak{A}(m)$.

Proposition 2 shows that to determine Aut $(W(m:\boldsymbol{n}))$ it is sufficient to determine Aut $(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$. We will do this by determining

$$\operatorname{Aut}_c (\mathfrak{A}(m): W(m)) = \{\sigma \in \operatorname{Aut} (\mathfrak{A}(m): W(m)) \mid \sigma \text{ is continuous}\}$$

and showing that Aut $(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ is isomorphic to the stabilizer of $\mathfrak{A}(m:\boldsymbol{n})$ in $\operatorname{Aut}_c (\mathfrak{A}(m): W(m))$.

We now obtain (for certain subalgebras of $\mathfrak{A}(m)$) a relation between the divided power operations and the admissible automorphisms. Note that if $\mathfrak{A}$ is any subalgebra of $\mathfrak{A}(m)$ containing 1 then $\mathfrak{A} = \Phi \oplus \mathfrak{A}_0$. Since (by (1.1)) $x^p = 0$ for all $x \in \mathfrak{A}_0$ we see that if $\sigma \in \operatorname{Aut} \mathfrak{A}$ then $1\sigma = 1$ and $\mathfrak{A}_0\sigma = \mathfrak{A}_0$.

LEMMA 5. *Let $\mathfrak{A}$ be a subalgebra of $\mathfrak{A}(m)$ containing* 1. *Assume that*

(4.1) *If $y \in \mathfrak{A}_0$, $r \in \boldsymbol{N}$, $y^{(r)} \in \mathfrak{A}$, and $1 \leqq s \leqq r$ then $y^{(s)} \in \mathfrak{A}$.*

(4.2) *If $D \in \operatorname{Der} \mathfrak{A}$ and if $y^{(r)}D = y^{(r-1)}(yD)$ for all $y \in \mathfrak{A}_0$ and $r \in \boldsymbol{N}$ such that $y^{(r)} \in \mathfrak{A}$ then D has a unique extension to an element of $W(m)$.*

Let W be the stabilizer of $\mathfrak{A}$ in $W(m)$. (By (4.2) *we may identify W with a subalgebra of* Der $\mathfrak{A}$.) *Assume that*

(4.3) *If $a \in \mathfrak{A}$ and $aD = 0$ for all $D \in W$ then $a \in \Phi$.*

Then for any $\sigma \in \operatorname{Aut} \mathfrak{A}$ the following conditions are equivalent:

(4.4) *If $y \in \mathfrak{A}_0$, $r \in \boldsymbol{N}$, and either $y^{(r)} \in \mathfrak{A}$ or $(y\sigma)^{(r)} \in \mathfrak{A}$ then $y^{(r)}\sigma = (y\sigma)^{(r)}$.*

(4.5) *If $y \in \mathfrak{A}_0$, $r \in \boldsymbol{N}$, and either $y^{(r)} \in \mathfrak{A}$ or $(y\sigma^{-1})^{(r)} \in \mathfrak{A}$ then $y^{(r)}\sigma^{-1} = (y\sigma^{-1})^{(r)}$.*

(4.6) $\sigma \in \operatorname{Aut} (\mathfrak{A}: W)$.

(4.7) $\sigma^{-1} \in \operatorname{Aut} (\mathfrak{A}: W)$.

Proof. Assume that (4.4) holds, $y \in \mathfrak{A}_0$, $r \in \boldsymbol{N}$, and either $y^{(r)} \in \mathfrak{A}$ or $(y\sigma^{-1})^{(r)} \in \mathfrak{A}$. Then $y^{(r)}\sigma^{-1} = (y\sigma^{-1}\sigma)^{(r)}\sigma^{-1} = (y\sigma^{-1})^{(r)}$. Hence (4.5) holds. Replacing σ by σ^{-1} we see that (4.4) and (4.5) are equivalent.

Now assume that (4.5) holds and that $D \in W$. Then if $y \in \mathfrak{A}_0$, $r \in \boldsymbol{N}$, and $y^{(r)} \in \mathfrak{A}$ by (4.1) we have $y^{(r-1)} \in \mathfrak{A}$ and so

$$y^{(r)}D^{\sigma} = y^{(r)}\sigma^{-1}D\sigma = (y\sigma^{-1})^{(r)}D\sigma = ((y\sigma^{-1})^{(r-1)}(y\sigma^{-1}D))\sigma = y^{(r-1)}(yD^{\sigma}).$$

Hence by (4.2) D^σ has a unique extension to $W(m)$ and so $D^\sigma \in W$. Hence $\sigma \in \mathrm{Aut}\ (\mathfrak{A}: W)$.

Conversely assume that (4.6) holds. We will verify (4.5) by induction on r. Clearly $y^{(0)}\sigma^{-1} = 1 = (y\sigma^{-1})^{(0)}$ so it holds for $r=0$. Suppose that (4.5) holds for all $r \in N$ such that $r < s$. Let $y \in \mathfrak{A}_0$, and either $y^{(s)} \in \mathfrak{A}$ or $(y\sigma^{-1})^{(s)} \in \mathfrak{A}$. Then (by (4.1)) either $y^{(s-1)} \in \mathfrak{A}$ or $(y\sigma^{-1})^{(s-1)} \in \mathfrak{A}$ so by the induction assumption $(y\sigma^{-1})^{(s-1)} = y^{(s-1)}\sigma^{-1}$. Then for any $D \in W$,

$$\begin{aligned} y^{(s)}\sigma^{-1}D &= y^{(s)}D^\sigma\sigma^{-1} = (y^{(s-1)}yD^\sigma)\sigma^{-1} = (y^{(s-1)}\sigma^{-1})(yD^\sigma\sigma^{-1}) \\ &= (y\sigma^{-1})^{(s-1)}(y\sigma^{-1}D) = (y\sigma^{-1})^{(s)}D. \end{aligned}$$

Hence $(y^{(s)}\sigma^{-1} - (y\sigma^{-1})^{(s)})D = 0$ for all $D \in W$ so by (4.3) $y^{(s)}\sigma^{-1} - (y\sigma^{-1})^{(s)} \in \Phi$. But σ and the divided power operations stabilize $\mathfrak{A}_0$ so $y^{(s)}\sigma^{-1} - (y\sigma^{-1})^{(s)} \in \Phi \cap \mathfrak{A}_0 = (0)$. Hence (4.5) holds for all $r \in N$. Thus (4.5) and (4.6) are equivalent. Replacing σ by σ^{-1} we see that (4.4) and (4.7) are equivalent, proving the lemma.

Note that the algebras $\mathfrak{A}(m)$ and $\mathfrak{A}(m:\boldsymbol{n})$ satisfy the hypotheses of the lemma. If $\mathfrak{A} = \mathfrak{A}(m)$ then $W = W(m)$ and if $\mathfrak{A} = \mathfrak{A}(m:\boldsymbol{n})$ then $W = W(m:\boldsymbol{n})$.

Corollary. Aut $(\mathfrak{A}(m): W(m))$ *is a group. The map* $\sigma \to \tilde{\sigma}$ *is an isomorphism of* Aut $(\mathfrak{A}(m): W(m))$ *into* Aut $W(m)$.

Proof. By the lemma Aut $(\mathfrak{A}(m): W(m))$ is inverse closed and hence is a group. If $\sigma \in \mathrm{Aut}\ (\mathfrak{A}(m): W(m))$ then $\tilde{\sigma}^{-1} = (\sigma^{-1})^\sim$ and hence $\tilde{\sigma} \in \mathrm{Aut}\ W(m)$. If $\tilde{\sigma}$ is the identity then for $1 \leqq i, j \leqq m$ we have $x_iD_j = \delta_{ij} = \delta_{ij}\sigma^{-1} = (x_iD_j)\sigma^{-1} = (x_iD_j^\sigma)\sigma^{-1} = (x_i\sigma^{-1})D_j$. Thus $x_i\sigma = x_i$ for $1 \leqq i \leqq m$ and hence $x^{p^j\varepsilon_i} = (x_i)^{(p^j)} = (x_i\sigma)^{(p^j)} = (x_i)^{(p^j)}\sigma = x^{p^j\varepsilon_i}\sigma$ for all $j \in N$. Since the $x^{p^j\varepsilon_i}$ generate $\mathfrak{A}(m)$, σ is the identity. Hence $\sigma \to \tilde{\sigma}$ is an isomorphism.

Before we can determine $\mathrm{Aut}_c\ (\mathfrak{A}(m): W(m))$ we need more information about the topology of $\mathfrak{A}(m)$ and the divided power operations. This is contained in the next two lemmas.

Lemma 6. (a) $\mathfrak{A}(m)_i\mathfrak{A}(m)_j \subseteq \mathfrak{A}(m)_{i+j+1}$,
(b) $(\mathfrak{A}(m)_i)^{(j)} \subseteq \mathfrak{A}(m)_{j(i+1)-1}$.

Proof. Recalling that $\mathfrak{A}(m)_i$ consists of linear combinations of $\{x^\alpha \mid |\alpha| \geqq i+1\}$ we see that (a) follows from (1.1). Now if $|\alpha| \geqq i+1$ then by (1.3) $(x^\alpha)^{(j)} \in \mathfrak{A}(m)_{j(i+1)-1}$. Assuming that (b) holds for all j such that $1 \leqq j < k$ and that $x, y \in \mathfrak{A}(m)_i$ are such that $x^{(k)}$, $y^{(k)} \in \mathfrak{A}(m)_{k(i+1)-1}$, we see by (1.4), (1.5) and (a) that $(x+by)^{(j)} \in \mathfrak{A}(m)_{k(i+1)-1}$ for all $b \in \Phi$. Thus $(\bar{\mathfrak{A}}(m)_i)^{(k)} \subseteq \mathfrak{A}(m)_{k(i+1)-1}$. Since $\bar{\mathfrak{A}}(m)_i$ is dense in $\mathfrak{A}(m)_i$ and the divided power operations are continuous, (b) is proved.

Lemma 7. *Let* $x, y \in \mathfrak{A}(m)_0$, $r, s \in N$, $r \geqq 1$. *Then*
(4.8) $x^{(r)}x^{(s)} = C(r+s, r)x^{(r+s)}$.
(4.9) $(xy)^{(r)} = r!\, x^{(r)}y^{(r)}$.
(4.10) $(x^{(r)})^{(s)} = ((rs)!/(r!)^s s!)x^{(rs)}$.

Proof. For $r, s \in N$ define

$$\mathfrak{B}_{r,s} = \{x \in \mathfrak{A}(m)_0 \mid x^{(r)}x^{(s)} - C(r+s, r)x^{(r+s)} = 0\}.$$

Set $\mathfrak{B} = \bigcap \mathfrak{B}_{r,s}$. Then (4.8) is equivalent to the statement that $\mathfrak{B} = \mathfrak{A}(m)_0$. Since each $\mathfrak{B}_{r,s}$ is the kernel of a continuous map, $\mathfrak{B}$ is closed, and hence to prove that $\mathfrak{B} = \mathfrak{A}(m)_0$, it is sufficient to prove that $\mathfrak{B} \supseteq \bar{\mathfrak{A}}(m)_0$, i.e., that $x^\alpha \in \mathfrak{B}$ for all $0 \neq \alpha \in A(m)$ and that $\mathfrak{B}$ is closed under addition and scalar multiplication. Now it is easily seen from (1.3) that $x^\alpha \in \mathfrak{B}$ for all $0 \neq \alpha \in A(m)$ and from (1.4) that $\mathfrak{B}$ is closed under scalar multiplication. If $x, y \in \mathfrak{B}$ then by (1.5)

$$\begin{aligned}(x+y)^{(r)}(x+y)^{(s)} &= \left(\sum_{i=0}^{r} x^{(i)}y^{(r-i)}\right)\left(\sum_{j=0}^{s} x^{(j)}y^{(s-j)}\right) \\ &= \sum_{i=0}^{r}\sum_{j=0}^{s} C(i+j, i)C(r+s-i-j, r-i)x^{(i+j)}y^{(r+s-i-j)} \\ &= \sum_{k=0}^{r+s} A_k x^{(k)}y^{(r+s-k)}\end{aligned}$$

where

$$A_k = \sum_{l=\max(0,k-s)}^{l=\min(r,k)} C(k, l)C(r+s-k, r-l).$$

Now by comparing coefficients of $(u^k/k!)(v^{r+s-k}/(r+s-k)!)$ in the identity $((u+v)^r/r!)((u+v)^s/s!) = C(r+s, r)(u+v)^{r+s}/(r+s)!$ in $Z[u, v]$ we see that $A_k = C(r+s, r)$ for $0 \leqq k \leqq r+s$. Hence $(x+y)^{(r)}(x+y)^{(s)} = C(r+s, r)\sum_{k=0}^{r+s} x^{(k)}y^{(r+s-k)} = C(r+s, r)(x+y)^{(r+s)}$ so that $x+y \in \mathfrak{B}$. This proves (4.8).

To prove (4.9) define (for $x \in \mathfrak{A}(m)_0$)

$$\mathfrak{B}(x) = \{y \in \mathfrak{A}(m)_0 \mid (xy)^{(r)} - r!\, x^{(r)}y^{(r)} = 0 \text{ for all } r \in N\}$$

and define $\mathfrak{B} = \{x \in \mathfrak{A}(m)_0 \mid \mathfrak{B}(x) = \mathfrak{A}(m)_0\}$. Then $\mathfrak{B} = \bigcap \mathfrak{B}(x)$ where the intersection is taken over all $x \in \mathfrak{A}(m)_0$. Then proving (4.9) is equivalent to showing that $\mathfrak{B} = \mathfrak{A}(m)_0$. As above $\mathfrak{B}(x)$ is closed. Furthermore it is obviously closed under scalar multiplication. It is easily seen from (1.3) that for any $0 \neq \alpha$, $\beta \in A(m)$, $x^\alpha \in \mathfrak{B}(x^\beta)$. If $y, z \in \mathfrak{B}(x)$ then (1.5) and (4.8) show that $y+z \in \mathfrak{B}(x)$. Hence $\mathfrak{B}(x^\alpha) \supseteq \bar{\mathfrak{A}}(m)_0$ and so $\mathfrak{B}(x^\alpha) = \mathfrak{A}(m)_0$ for all $0 \neq \alpha \in A(m)$. Hence $\mathfrak{B} \supseteq \bar{\mathfrak{A}}(m)_0$ and so $\mathfrak{B} = \mathfrak{A}(m)_0$ as required.

Finally to prove (4.10) we set

$$\mathfrak{B} = \{x \in \mathfrak{A}(m)_0 \mid (x^{(r)})^{(s)} - ((rs)!/(r!)^s s!)x^{(rs)} = 0 \text{ for all } r, s \in N, r \geqq 1\}.$$

As above it is sufficient to prove that $\mathfrak{B} = \mathfrak{A}(m)_0$ and since $\mathfrak{B}$ is closed it is sufficient to show that $x^\alpha \in \mathfrak{B}$ for all $0 \neq \alpha \in A(m)$ and that $\mathfrak{B}$ is closed under addition and scalar multiplication. It follows immediately from (1.3) and (1.4) that $x^\alpha \in \mathfrak{B}$ for all $0 \neq \alpha \in A(m)$ and that $\mathfrak{B}$ is closed under scalar multiplication. If $x, y \in \mathfrak{B}$ then

$$((x+y)^{(r)})^{(s)} = \left(\sum_{i=0}^{r} x^{(i)}y^{(r-i)}\right)^{(s)} = \sum \prod_{i=0}^{r} (x^{(i)}y^{(r-i)})^{(j_i)}$$

(where the summation extends over all sequences $j_0, \ldots, j_r$ of elements of $\boldsymbol{N}$ such that $\sum_{i=0}^r j_i = s$). Then by (4.9) and the assumption that $x, y \in \mathfrak{B}$ we have

$$(x^{(i)}y^{(r-i)})^{(j_i)} = ((ij_i)!\,((r-i)j_i)!/((i!)(r-i)!)^{j_i}j_i!)x^{(ij_i)}y^{((r-i)j_i)}.$$

Then by (4.8)

$$\prod_{i=0}^{r} (x^{(i)}y^{(r-i)})^{(j_i)} = \left(t!\,(rs-t)!\Big/\prod_{i=0}^{r} (((i!)(r-i)!)^{j_i}j_i!)\right)x^{(t)}y^{(rs-t)}$$

where $t = \sum_{i=0}^r ij_i$. Thus $((x+y)^{(r)})^{(s)} = \sum_{t=0}^{rs} A_t x^{(t)}y^{(rs-t)}$ where

$$A_t = t!\,(rs-t)! \sum \prod_{i=0}^{r} (1/(((i!)(r-i)!)^{j_i}j_i!))$$

where the summation is over all sequences $j_0, \ldots, j_r$ of elements of $\boldsymbol{N}$ such that $\sum_{i=0}^r j_i = s$ and $\sum_{i=0}^r ij_i = t$. Now by comparing the coefficients of $(u^t/t!)(v^{rs-t}/(rs-t)!)$ in the identity $((u+v)^r/r!)^s/s! = ((rs)!/r!^s\,s!)\,((u+v)^{rs}/(rs)!)$ in $\boldsymbol{Z}[u, v]$ we see that $A_t = (rs)!/r!^s\,s!$ for $0 \leqq t \leqq rs$. Hence by (1.5) $((x+y)^{(r)})^{(s)} = ((rs)!/r!^s\,s!)(x+y)^{(rs)}$ so $x+y \in \mathfrak{B}$. Hence $\mathfrak{B} = \mathfrak{A}(m)_0$.

LEMMA 8. *Let* $\sigma \in \operatorname{Aut} \mathfrak{A}(m)$ *be continuous. Then the following conditions are equivalent*:

(4.11) $y^{(r)}\sigma = (y\sigma)^{(r)}$ *for all* $y \in \mathfrak{A}(m)_0$ *and all* $r \in \boldsymbol{N}$.

(4.12) $x_i^{(p^j)}\sigma = (x_i\sigma)^{(p^j)}$ *for* $1 \leqq i \leqq m$ *and all* $j \in \boldsymbol{N}$.

Proof. Clearly (4.12) is a special case of (4.11). Assume that (4.12) holds and set $\mathfrak{B} = \{y \in \mathfrak{A}(m)_0 \mid y^{(r)}\sigma - (y\sigma)^{(r)} = 0$ for all $r \in \boldsymbol{N}\}$. Now $\mathfrak{B}$ is closed under addition (by (1.5)), scalar multiplication (by (1.4)), multiplication (by (4.9)), and the divided power operations (by (4.10)). By (4.12) $x_i \in \mathfrak{B}$ for $1 \leqq i \leqq m$. Hence $\mathfrak{B} \supseteq \bar{\mathfrak{A}}(m)_0$. But $\mathfrak{B}$ is closed since σ and the divided power operations are continuous. Hence $\mathfrak{B} = \mathfrak{A}(m)_0$ proving the lemma.

LEMMA 9. *Let σ be a continuous endomorphism of* $\mathfrak{A}(m)$. *Then* $\sigma \in \operatorname{Aut}(\mathfrak{A}(m) : W(m))$ *if and only if σ satisfies* (4.12) *and*

(4.13) $\det(x_i\sigma D_j)$ *is a unit in* $\mathfrak{A}(m)$.

Proof. Suppose that σ is an endomorphism of $\mathfrak{A}(m)$ satisfying (4.11). Then for any $\alpha \in A(m)$ by (1.1), (1.3) and Lemma 6 we have $x^\alpha\sigma = \prod x_i^{(\alpha(i))}\sigma = \prod (x_i\sigma)^{(\alpha(i))} \in A(m)_{|\alpha|-1}$. Hence $\mathfrak{A}(m)_i\sigma \subseteq \mathfrak{A}(m)_i$ for all $i \in \boldsymbol{N}$ and so σ induces linear maps $\sigma_i : \mathfrak{A}(m)_{i-1}/\mathfrak{A}(m)_i \to \mathfrak{A}(m)_{i-1}/\mathfrak{A}(m)_i$ for all $i \in \boldsymbol{N}$.

Now suppose that $\sigma \in \operatorname{Aut}(\mathfrak{A}(m) : W(m))$. Then by Lemmas 5 and 8 σ satisfies (4.11) and (4.12). Now since σ is an automorphism σ_1 is surjective. Since $\mathfrak{A}(m)_0/\mathfrak{A}(m)_1$ is finite dimensional σ_1 is bijective. Relative to the basis $\{x_i + \mathfrak{A}(m)_1 \mid 1 \leqq i \leqq m\}$ of $\mathfrak{A}(m)_0/\mathfrak{A}(m)_1$, σ_1 has matrix $(x_i\sigma D_j\psi)$ where ψ is the projection of $\mathfrak{A}(m) = \mathfrak{A}(m)_0 \oplus \Phi$ onto Φ. Since σ_1 is a bijection $0 \neq \det(x_i\sigma D_j\psi) = (\det(x_i\sigma D_j))\psi$ so (4.13) holds.

Conversely if (4.12) and (4.13) hold and σ is an automorphism then by Lemmas 5 and 8 $\sigma \in \mathrm{Aut}\,(\mathfrak{A}(m): W(m))$. Hence it is sufficient to show that σ is an automorphism, i.e., that σ is bijective. We begin by showing that σ_i is bijective for all $i \in \boldsymbol{N}$.

Since $\det(x_i\sigma D_j\psi) \neq 0$, σ_1 is bijective. Assume that σ_i is bijective for all $i<j$. Now $\mathfrak{A}(m)_{j-1}/\mathfrak{A}(m)_j$ is finite dimensional so to show that σ_j is bijective it is sufficient to show that it is surjective. Thus it is sufficient to show that if $\alpha \in A(m)$ and $|\alpha|=j$ then there exists $y \in \mathfrak{A}(m)_{j-1}$ and $z \in \mathfrak{A}(m)_j$ such that

(4.14) $y\sigma = x^\alpha + z$.

Now if $\alpha = j\varepsilon_k$ for some k then by (1.3) $x^\alpha = x_k^{(j)}$. By the result for σ_1 there exist $y_1 \in \mathfrak{A}(m)_0$ and $z_1 \in \mathfrak{A}(m)_1$ such that $y_1\sigma = x_k + z_1$. Since (4.12) and hence (by Lemma 8) (4.11) hold we have $y_1^{(j)}\sigma = (y_1\sigma)^{(j)} = (x_k+z_1)^{(j)}$. Now by (1.5) and Lemma 6 we have $(x_k+z_1)^{(j)} = x_k^{(j)} + z$ where $z = \sum_{l=0}^{j-1} x_k^{(l)} z_1^{(j-l)} \in \mathfrak{A}(m)_j$. Thus setting $y = y_1^{(j)}$ we see that (4.14) is satisfied. If α is not of the form $j\varepsilon_k$ then we may write $\alpha = \beta + \gamma$ where $\beta \neq 0$, $\gamma \neq 0$ and $C(\alpha, \beta) = 1$. (For if $\alpha(k) \neq 0$ set $\beta = \alpha(k)\varepsilon_k$, and $\gamma = \alpha - \beta$.) If $|\beta| = i$ then $|\gamma| = j - i$. Since $i, j-i < j$ by the induction assumption we may find $y_1 \in \mathfrak{A}(m)_{i-1}$, $z_1 \in \mathfrak{A}(m)_i$, $y_2 \in \mathfrak{A}(m)_{j-i-1}$, and $z_2 \in \mathfrak{A}(m)_{j-i}$ such that $y_1\sigma = x^\beta + z_1$ and $y_2\sigma = x^\gamma + z_2$. Then setting $y = y_1 y_2$ we see that $y\sigma = x^\alpha + z$ where $z = x^\beta z_2 + x^\gamma z_1 + z_1 z_2$. By Lemma 4 $y \in \mathfrak{A}(m)_{j-1}$ and $z \in \mathfrak{A}(m)_j$. Hence σ_j is bijective and so by induction σ_i is bijective for all i.

Now suppose $x \in \ker \sigma$. Then if $x \in \mathfrak{A}(m)_{i-1}$, $x + \mathfrak{A}(m)_i \in \ker \sigma_i$ so that $x \in \mathfrak{A}(m)_i$. Hence $\ker \sigma \subseteq \bigcap \mathfrak{A}(m)_i = (0)$ so σ is injective. Finally if $x \in \mathfrak{A}(m)$ then $x = a + x_0$ where $a \in \Phi$ and $x_0 \in \mathfrak{A}(m)_0$. Since σ_1 is bijective there exists $y_1 \in \mathfrak{A}(m)_0$ such that $x_0 - y_1\sigma = x_1 \in \mathfrak{A}(m)_1$. Suppose that $x_i \in \mathfrak{A}(m)_i$ and $y_i \in \mathfrak{A}(m)_{i-1}$ have been defined for $r > i \geqq 1$ so that $x_{i-1} - y_i\sigma = x_i$. Then since σ_r is bijective there exists $y_r \in \mathfrak{A}(m)_{r-1}$ such that $x_{r-1} - y_r\sigma = x_r \in \mathfrak{A}(m)_r$. Thus we may inductively define x_i and y_i for all $i \in \boldsymbol{N}$. Then

$$x = a + x_0 = a + \sum_{i=1}^{\infty} (x_{i-1} - x_i) = a + \sum_{i=1}^{\infty} y_i\sigma.$$

Then, by the continuity of σ, $x = y\sigma$ where $y = a + \sum_{i=1}^{\infty} y_i$. Hence σ is bijective. This completes the proof of Lemma 9.

Corollary 1. *If $y_1, \ldots, y_m \in \mathfrak{A}(m)_0$ and $\det(y_i D_j)$ is a unit then there is a unique $\sigma \in \mathrm{Aut}_c\,(\mathfrak{A}(m): W(m))$ satisfying $y_i = x_i\sigma$ for $1 \leqq i \leqq m$.*

Proof. Obviously there is a unique continuous endomorphism σ of $\mathfrak{A}(m)$ with $y_i = x_i\sigma$ for $1 \leqq i \leqq m$ and satisfying (4.12). By the lemma $\sigma \in \mathrm{Aut}_c\,(\mathfrak{A}(m): W(m))$.

Corollary 2. *Each $\sigma \in \mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ can be uniquely extended to $\bar{\sigma} \in \mathrm{Aut}_c\,(\mathfrak{A}(m): W(m))$.*

Proof. Let $\sigma \in \mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$. In the same manner as in the lemma we see that $\det(x_i\sigma D_j)$ is a unit in $\mathfrak{A}(m:\boldsymbol{n})$ and hence in $\mathfrak{A}(m)$. Then by Corollary 1 there is a unique $\bar{\sigma} \in \mathrm{Aut}_c\,(\mathfrak{A}(m): W(m))$ such that $x_i\bar{\sigma} = x_i\sigma$ for $1 \leqq i \leqq m$. By Lemma 5 this implies that σ and $\bar{\sigma}$ agree on $\mathfrak{A}(m:\boldsymbol{n})$ proving the lemma.

Thus $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ may be identified with the stabilizer of $\mathfrak{A}(m:\boldsymbol{n})$ in $\mathrm{Aut}_c\,(\mathfrak{A}(m): W(m))$. Clearly $\sigma \in \mathrm{Aut}\,(\mathfrak{A}(m): W(m))$ stabilizes $\mathfrak{A}(m:\boldsymbol{n})$ if and only if $(x^{p^j\varepsilon_i})\sigma \in \mathfrak{A}(m:\boldsymbol{n})$ for all $1 \leqq i \leqq m$ and all $0 \leqq j < n_i$. Setting $x_i\sigma = y_i$ and using (4.11) we see that this is equivalent to $y_i^{(p^j)} \in \mathfrak{A}(m:\boldsymbol{n})$ for all $1 \leqq i \leqq m$ and all $0 \leqq j < n_i$.

Lemma 10. *If $x = \sum a(\alpha)x^\alpha$ where the summation is over all $\alpha \in A(m:\boldsymbol{n})$ and the $a(\alpha) \in \Phi$ then $x^{(p^j)} \in \mathfrak{A}(m:\boldsymbol{n})$ for all j, $1 \leqq j \leqq k$ if and only if $a(p^l\varepsilon_i) = 0$ whenever $l \geqq n_i - k$.*

Proof. By (1.5) we see that $x^{(p^j)} \in \mathfrak{A}(m:\boldsymbol{n})$ for all j, $1 \leqq j \leqq k$ if and only if $(x^\alpha)^{(p^j)} \in \mathfrak{A}(m:\boldsymbol{n})$ for all j, $1 \leqq j \leqq k$ and all $\alpha \in A(m:\boldsymbol{n})$ such that $a(\alpha) \neq 0$. By (1.3) we see that if $j \geqq 1$, $(x^\alpha)^{(p^j)} = 0$ unless $\alpha = p^l\varepsilon_i$ for some $1 \leqq i \leqq m$ and $l \in N$, and that $(x^{p^l\varepsilon_i})^{(p^j)} = x^{p^{l+j}\varepsilon_i}$. Thus $(x^\alpha)^{(p^j)} \in \mathfrak{A}(m:\boldsymbol{n})$ unless $\alpha = p^l\varepsilon_i$ where $l + j \geqq n_i$.

Define $S(m:\boldsymbol{n})$ to be the set of all m-tuples $(y_1, \ldots, y_m)$ such that, for $1 \leqq i \leqq m$, $y_i = \sum a(i, \alpha)x^\alpha$ where the summation extends over all $0 \neq \alpha \in A(m:\boldsymbol{n})$, the $a(i, \alpha) \in \Phi$, $a(i, p^l\varepsilon_j) = 0$ whenever $n_i + l - 1 \geqq n_j$, and $\det\,(y_iD_j)$ is a unit.

Let $V(m)$ be an m-dimensional vector space over Φ with basis $\{v_1, \ldots, v_m\}$ for $1 \leqq i \leqq m$. Define subspaces $V(m:\boldsymbol{n})_i$ of $V(m)$ for $1 \leqq i \leqq m$ by

$$V(m:\boldsymbol{n})_1 = \langle v_j \mid n_j = \max\{n_k \mid 1 \leqq k \leqq m\}\rangle,$$

and

$$V(m:\boldsymbol{n})_i = \langle v_j \mid n_j \geqq \max\{n_k \mid 1 \leqq k \leqq m, v_k \notin V(m:\boldsymbol{n})_{i-1}\}\rangle \quad \text{for } i \geqq 2.$$

Let $\mathscr{V}(m:\boldsymbol{n})$ be the flag

$$V(m) = V(m:\boldsymbol{n})_m \supseteq V(m:\boldsymbol{n})_{m-1} \supseteq \cdots \supseteq V(m:\boldsymbol{n})_1 \supseteq (0).$$

Then we have the following description of $\mathrm{Aut}\,(W(m:\boldsymbol{n}))$ (which has been proven in the special cases $\boldsymbol{n} = \mathbf{1}$ by Jacobson [2, §8] (where we must note that since Φ is algebraically closed $r = 0$) and $m = 1$ by Ree [7, Theorem 12.13]):

Theorem 2. *Let Φ be an algebraically closed field of characteristic $p \geqq 5$. Then* $\mathrm{Aut}\,(W(m:\boldsymbol{n}))$ *is isomorphic to* $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$. *The map $\sigma \to (x_1\sigma, \cdots, x_m\sigma)$ is a bijection of* $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ *onto $S(m:\boldsymbol{n})$ and* $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ *has a solvable normal subgroup $\mathscr{B}_1$ such that* $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))/\mathscr{B}_1$ *is isomorphic to the stabilizer of $\mathscr{V}(m:\boldsymbol{n})$ in* $\mathrm{GL}\,(V(m))$.

Proof. As mentioned above Ree has proved the isomorphism of $\mathrm{Aut}\,(W(m:\boldsymbol{n}))$ and $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$. Lemma 10 and the corollaries to Lemma 9 show that the map $\sigma \to (x_1\sigma, \ldots, x_m\sigma)$ is a bijection of $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ onto $S(m:\boldsymbol{n})$. To prove the last statement we let $\mathscr{B}_i$ be the subgroup of $\mathrm{Aut}\,(\mathfrak{A}(m:\boldsymbol{n}): W(m:\boldsymbol{n}))$ consisting of all automorphisms which induce the identity on $\mathfrak{A}(m:\boldsymbol{n})_0/\mathfrak{A}(m:\boldsymbol{n})_i$. Now the map $\sigma \to (a(i, \varepsilon_j))_{1 \leqq i,j \leqq m}$ is easily seen to be a homomorphism of

Aut $(\mathfrak{A}(m:\boldsymbol{n}):W(m:\boldsymbol{n}))$ onto the subgroup of GL $(m:\Phi)$ consisting of all matrices (a_{ij}) such that $a_{ij}=0$ whenever $n_i-n_j\geqq 1$, i.e., onto the stabilizer of $\mathscr{V}(m:\boldsymbol{n})$ in GL $(V(m))$. Clearly the kernel of this homomorphism is $\mathscr{B}_1$. Thus we need only show that $\mathscr{B}_1$ is solvable.

Let $\sigma_i\in\mathscr{B}_1$. Then if $x\in\mathfrak{A}(m:\boldsymbol{n})_0$ we have $x\equiv x\sigma_i \bmod \mathfrak{A}(m:\boldsymbol{n})_i$. We claim that if $x\in\mathfrak{A}(m:\boldsymbol{n})_k$ then $x\equiv x\sigma_i \bmod \mathfrak{A}(m:\boldsymbol{n})_{i+k}$. To see this note that $\mathfrak{A}(m:\boldsymbol{n})_k$ is spanned by the x^α where $|\alpha|\geqq k+1$. Since $x^\alpha=\prod x_j^{(\alpha(j))}$ Lemma 6 shows that $x^\alpha\equiv x^\alpha\sigma_i \bmod \mathfrak{A}(m:\boldsymbol{n})_{i+|\alpha|-1}$ giving the result. Now (following [2, p. 117]) we let $x\in\mathfrak{A}(m:\boldsymbol{n})_0$, $\sigma_i\in\mathscr{B}_i$ and $\tau_j\in\mathscr{B}_j$. Then $x\sigma_i^{-1}=x+x'$ where $x'\in\mathfrak{A}(m:\boldsymbol{n})_i$, $x\tau_j^{-1}=x+x''$ where $x''\in\mathfrak{A}(m:\boldsymbol{n})_j$, $x'\tau_j^{-1}=x'+x'''$ where $x'''\in\mathfrak{A}(m:\boldsymbol{n})_{i+j}$, and $x''\sigma_i=x''+x''''$ where $x''''\in\mathfrak{A}(m:\boldsymbol{n})_{i+j}$. Then we have the following chain of equalities and congruences mod $\mathfrak{A}(m:\boldsymbol{n})_{i+j}$:

$$\begin{aligned} x\sigma_i^{-1}\tau_j^{-1}\sigma_i\tau_j &= (x+x')\tau_j^{-1}\sigma_i\tau_j = (x+x'+x''+x''')\sigma_i\tau_j \\ &\equiv (x+x'+x'')\sigma_i\tau_j = (x+x''+x'''')\tau_j \\ &\equiv (x+x'')\tau_j = x. \end{aligned}$$

Thus $(\sigma_i,\tau_j)\in\mathscr{B}_{i+j}$. Now for $i>\sum_{j=1}^m p^{n_j}$, $\mathfrak{A}(m:\boldsymbol{n})_i=(0)$ so $\mathscr{B}_i=\{1\}$. Hence $\mathscr{B}_1$ is solvable.

References

1. H.-J. Chang, *Über Wittsche Lie-Ringe*, Abh. Math. Sem. Hansischen **14** (1941), 151–184. MR **3**, 101.

2. N. Jacobson, *Classes of restricted Lie algebras of characteristic p*. II, Duke Math. J. **10** (1943), 107–121. MR **4**, 187.

3. ———, *Lie algebras*, Interscience Tracts in Pure and Appl. Math., vol. 10, Interscience, New York, 1962. MR **26** #1345.

4. S. A. Jennings and R. Ree, *On a family of Lie algebras of characteristic p*, Trans. Amer. Math. Soc. **84** (1957), 192–207. MR **18**, 583.

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

6. A. I. Kostrikin and I. R. Šafarevič, *Graded Lie algebras of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **30** (1969), 251–322.

7. R. Ree, *On generalized Witt algebras*, Trans. Amer. Math. Soc. **83** (1956), 510–546. MR **18**, 491.

8. ———, *Note on generalized Witt algebras*, Canad. J. Math. **11** (1959), 345–352. MR **21** #3468.

9. G. B. Seligman, *Modular Lie algebras*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Heft 40, Springer-Verlag, Berlin, 1967.

10. R. L. Wilson, *Nonclassical simple Lie algebras*, Bull. Amer. Math. Soc. **75** (1969), 987–991.

11. H. Zassenhaus, *Über Liesche Ringe mit Primzahlcharacteristik*, Abh. Math. Sem. Univ. Hamburg **13** (1940), 1–100.

Courant Institute of Mathematical Sciences, New York University,
New York, New York 10012