ON GENERALIZED WITT ALGEBRAS(1)

BY
RIMHAK REE

Introduction. Let Φ be a field of characteristic $p>0$. The Witt algebra over Φ is a Lie algebra with basis $e_0, e_1, \cdots, e_{p-1}$ and relations $e_i \circ e_j = (j-i)e_{i+j}$, where $i+j$ is to be calculated modulo p. H. Zassenhaus [5, p. 47] generalized the Witt algebra to algebras with basis $\{e_\alpha\}$, where α runs over a subgroup of the additive group of the ground field Φ, and with the relations $e_\alpha \circ e_\beta = (\beta-\alpha)e_{\alpha+\beta}$. Another generalization was obtained by N. Jacobson [3]. In his investigations Witt [1] used implicitly the fact that the Witt algebra is the derivation algebra of the group algebra of a cyclic group of order p. In the paper cited above, Jacobson proved that the derivation algebra of the group algebra of an elementary p-group, by which we shall mean throughout this paper an abelian group of the type $(p, p, \cdots, p)$, is simple if the order of the group is greater than 2.

Recently, I. Kaplansky [4, p. 471] gave an ingenious generalization of the Witt algebra, which includes the generalizations obtained by Zassenhaus and Jacobson. Let $I=\{i, j, \cdots\}$ be a set of indices, and $\mathfrak{G}$ a total(2) additive group of functionals on I with values in the ground field Φ. Kaplansky considers the Lie algebra $\mathfrak{L}$ over Φ with basis $\{(i, \sigma)\}$, where $i\in I$, $\sigma\in\mathfrak{G}$, and the multiplication

$$(0.0.1) \qquad (i, \sigma) \circ (j, \tau) = \tau(i)(j, \sigma + \tau) - \sigma(j)(i, \sigma + \tau).$$

It appears that $\mathfrak{L}$ is simple except when I consists of a single element and Φ is of characteristic 2. Zassenhaus' algebra is the case when I consists of a single element, while Jacobson's is the case where $\mathfrak{G}$ consists of all functionals with values in the prime field of Φ. We shall call the above algebra $\mathfrak{L}$ a *generalized Witt algebra*. In order that $\mathfrak{L}$ be finite dimensional it is necessary and

Received by the editors February 4, 1956.

(1) The results in this paper are contained in a dissertation presented to the Faculty of Graduate Studies of the University of British Columbia in partial fulfillment of the requirements for the degree of Doctor of Philosophy, May, 1955. The author wishes to express his gratitude to Professor S. A. Jennings for his guidance, and to Professor H. Zassenhaus of McGill University for his careful examination of the manuscript. The author's original proofs of Lemmas 6.7–6.9 were greatly simplified by Professor Zassenhaus' suggestions. The author also wishes to express his gratitude for a grant from the Canadian Mathematical Congress which permitted him to attend the Summer Research Institute of the Congress during the summer of 1954.

(2) A set $\mathfrak{G}$ of functionals defined on a set I with values in a field Φ is called *total* if the following condition is satisfied: For any mapping $i\rightarrow\alpha_i$ of I into Φ such that $\alpha_i=0$ for all but possibly a finite number of $i\in I$, the relation $\sum_{i\in I}\alpha_i\sigma(i)=0$ for all $\sigma\in\mathfrak{G}$ implies $\alpha_i=0$ for all $i\in I$.

sufficient that both I and $\mathfrak{G}$ be finite. If $\mathfrak{G}$ is finite, then Φ must be of characteristic $p>0$, and $\mathfrak{G}$ is an elementary p-group.

Let now $\mathfrak{A}$ be a commutative associative algebra over Φ. A subalgebra $\mathfrak{L}$ of the derivation algebra of $\mathfrak{A}$ will be called regular if $fD\in\mathfrak{L}$ for every $f\in\mathfrak{A}$ and $D\in\mathfrak{L}$. For a regular subalgebra $\mathfrak{L}$, if there exist $D_1, \cdots, D_m\in\mathfrak{L}$ such that every $D\in\mathfrak{L}$ is expressed uniquely as $D=f_1D_1+\cdots+f_mD_m$, where $f_i\in\mathfrak{A}$, then $\mathfrak{L}$ will be said to be defined by the system $(D_1, \cdots, D_m)$ and denoted by the notation $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. It is shown in §2 that any generalized Witt algebra can be written in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, where $\mathfrak{A}$ is the group algebra of an elementary p-group. The object of this paper is to study the family $\mathfrak{F}$ of Lie algebras of characteristic p which can be written in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, with main emphasis on simple algebras. Our principal results are as follows: If $\mathfrak{A}$ is a field then all algebras in $\mathfrak{F}$ are simple except when $p=2$, $m=1$ (Theorem 5.1). If Φ is algebraically closed then any simple algebra in $\mathfrak{F}$ is a generalized Witt algebra (Theorem 6.10). A simpler form of the generalized Witt algebra is given in Theorem 9.3. By using this form, the problem of whether or not every generalized Witt algebra can be defined over $GF(p)$ is partly solved, and it is shown that some new finite simple Lie rings are contained in $\mathfrak{F}$. A subfamily $\mathfrak{F}'$ of $\mathfrak{F}$, consisting for the most part of nonsimple algebras, has an interesting property: every algebra in $\mathfrak{F}'$ has the same ideal theory as that of a commutative associative algebra (see §11). In the last section, we extend Jacobson's results on automorphisms of his algebras to the case of generalized Witt algebras, and show that m is an invariant of the algebra $\mathfrak{L}=\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ if $\mathfrak{L}$ is normal simple.

All algebras considered in this paper are finite-dimensional, unless the contrary is specified.

1. **The algebra** $\mathfrak{L}(\mathfrak{A}; D_1 \cdots, D_m)$. Throughout this paper, Φ will denote a field of characteristic $p>0$, $\mathfrak{A}$ a commutative associative algebra over Φ, with a unit element, and $\mathfrak{D}(\mathfrak{A})$ the derivation algebra (over Φ) of $\mathfrak{A}$. The multiplication in $\mathfrak{D}(\mathfrak{A})$ will be denoted by $\circ$, i.e., $D_1\circ D_2=D_1D_2-D_2D_1$.

Suppose there exist derivations $D_1, \cdots, D_m$ of $\mathfrak{A}$ such that

$$D_i\circ D_j = \sum_{k=1}^{m} a_{ijk}D_k \tag{1.0.1}$$

for $i, j=1, \cdots, m$, where $a_{ijk}\in\mathfrak{A}$. Then the set $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ of all derivations of $\mathfrak{A}$ of the form $f_1D_1+\cdots+f_mD_m$, where $f_i\in\mathfrak{A}$, forms a subalgebra of $\mathfrak{D}(\mathfrak{A})$. More generally, the set of all derivations of $\mathfrak{A}$ of the form $f_1D_1+\cdots+f_mD_m$, where f_i runs over an ideal $\mathfrak{O}$ of $\mathfrak{A}$, forms a subalgebra of $\mathfrak{D}(\mathfrak{A})$. For,

$$f_iD_i\circ g_jD_j = f_i(D_ig_j)D_j - g_j(D_jf_i)D_i + \sum_{k=1}^{m} f_ig_ja_{ijk}D_k,$$

where all the coefficients of the right-hand side belong to $\mathfrak{O}$. In the following we shall restrict the algebras $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ by imposing the condition:

$$(1.0.2) \qquad f_1D_1 + \cdots + f_mD_m = 0 \text{ implies } f_1 = \cdots = f_m = 0.$$

The number m will be called the *D-dimension* of $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$.

Because of the condition (1.0.2) there exists a one-one correspondence

$$f_1D_1 + \cdots + f_mD_m \leftrightarrow (f_1, \cdots, f_m)$$

between the elements of $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ and the set of all vectors $(f_1, \cdots, f_m)$, where f_i runs over $\mathfrak{A}$. If we identify $f_1D_1 + \cdots + f_mD_m$ with $(f_1, \cdots, f_m)$ then

$$\alpha(f_1, \cdots, f_m) = (\alpha f_1, \cdots, \alpha f_m) \qquad \text{for } \alpha \in \Phi.$$

$$(1.0.3) \qquad (f_1, \cdots, f_m) + (g_1, \cdots, g_m) = (f_1 + g_1, \cdots, f_m + g_m),$$

$$(f_1, \cdots, f_m) \circ (g_1, \cdots, g_m) = (h_1, \cdots, h_m),$$

where

$$h_i = \sum_s (f_s(D_s g_i) - g_s(D_s f_i)) + \sum_{s,t} f_s g_t a_{sti}.$$

Suppose that the derivations $D_1, \cdots, D_m$ are commutative, i.e., $D_i \circ D_j = 0$ for all i, j, not necessarily satisfying (1.0.2). Then, conversely, we may define a Lie algebra $\mathfrak{L}^*$ over Φ by starting with the set $\mathfrak{L}^*$ of all vectors $(f_1, \cdots, f_m)$ and defining scalar multiplication, addition, and multiplication according to (1.0.3) where we put $a_{ijk} = 0$ for all i, j, k. $\mathfrak{L}^*$ is in general different from $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. But it is easily seen that the set $\mathfrak{J}$ of all vectors $(f_1, \cdots, f_m)$ satisfying $\sum f_i D_i = 0$ forms an ideal of $\mathfrak{L}^*$ and that $\mathfrak{L}^*/\mathfrak{J} = \mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. Since we are mainly interested in simple algebras, we prefer to work with $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ rather than $\mathfrak{L}^*$. In what follows we study the properties of the algebras $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, always assuming (1.0.2).

2. **Generalized Witt algebras.** We show that any generalized Witt algebra $\mathfrak{L}$ can be written in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. Let $\mathfrak{L}$ be defined with respect to a finite set $I = \{1, \cdots, m\}$ of indices and a finite total(2) additive group $\mathfrak{G}$ of functionals on I with values in Φ. Let $\overline{\mathfrak{G}} = \{u_\sigma, u_\tau, \cdots\}$ be a multiplicative group isomorphic to $\mathfrak{G}$ via the correspondence $u_\sigma \leftrightarrow \sigma$. For each $i \in \mathfrak{J}$ we define the mapping $\theta_i: \overline{\mathfrak{G}} \to \Phi$ by $\theta_i(u_\sigma) = \sigma(i)$. Then $\theta_1, \cdots, \theta_m$ are homomorphisms of $\overline{\mathfrak{G}}$ into the additive group of Φ such that

$$(2.0.1) \qquad \theta_1(u_\sigma) = \cdots = \theta_m(u_\sigma) = 0 \text{ implies } u_\sigma = 1.$$

The fact that $\mathfrak{G}$ is total can be expressed as follows:

(2.0.2) $\alpha_1\theta_1 + \cdots + \alpha_m\theta_m = 0$, with $\alpha_i \in \Phi$, implies $\alpha_1 = \cdots = \alpha_m = 0$.

Now let $\mathfrak{A}$ be the group algebra of $\mathfrak{G}$ over Φ, and define the linear mapping D_i of $\mathfrak{A}$ into itself by $D_i u_\sigma = \theta_i(u_\sigma)u_\sigma$. Then D_i is a derivation of $\mathfrak{A}$, since

$$\begin{aligned} D_i(u_\sigma u_\tau) &= D_i(u_{\sigma+\tau}) = \theta_i(u_{\sigma+\tau})u_{\sigma+\tau} \\ &= \theta_i(u_\sigma)u_\sigma u_\tau + \theta_i(u_\tau)u_\sigma u_\tau \\ &= (D_i u_\sigma)u_\tau + u_\sigma(D_i u_\tau). \end{aligned}$$

It is clear that (1.0.1) is satisfied for $D_1, \cdots, D_m$, since $D_i \circ D_j = 0$ for all i and j. We will show that (1.0.2) is also satisfied. Let $f_1D_1 + \cdots + f_mD_m = 0$, with $f_i \in \mathfrak{A}$. Then we have $\sum_i f_i\theta_i(u_\sigma) = 0$ for all u_σ. Let $f_i = \sum_\tau \alpha_i(\tau)u_\tau$. Then we have $\sum_i \alpha_i(\tau)\theta_i(u_\sigma) = 0$ for all τ and σ. From (2.0.2) it follows that $\alpha_i(\tau) = 0$ for all i and τ. Thus $f_1 = \cdots = f_m = 0$. Therefore we can define the algebra $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. The set $\{u_\sigma D_i\}$, where $i \in \mathrm{I}$, $\sigma \in \mathfrak{G}$, is a basis of this algebra, and we have

$$\begin{aligned} u_\sigma D_i \circ u_\tau D_j &= u_\sigma(D_i u_\tau)D_j - u_\tau(D_j u_\sigma)D_i \\ &= \tau(i)u_{\sigma+\tau}D_j - \sigma(j)u_{\sigma+\tau}D_i. \end{aligned}$$

Comparing the above with (0.0.1), we see easily that the given generalized Witt algebra is isomorphic with $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. We note that (2.0.1) is equivalent to the following property of $D_1, \cdots, D_m$:

(2.0.3) $$D_1f = \cdots = D_mf = 0 \text{ implies } f \in \Phi.$$

Conversely, for any elementary p-group $\mathfrak{G}$, if there exist homomorphisms $\theta_1, \cdots, \theta_m$ of $\mathfrak{G}$ into the additive group of Φ such that (2.0.1) and (2.0.2) hold, then we can construct a generalized Witt algebra by the above method.

Suppose now that homomorphisms $\theta_1, \cdots, \theta_m$ satisfy (2.0.1) and (2.0.2). Let the order of $\mathfrak{G}$ be p^n, and let $x_1, \cdots, x_n$ be a set of independent generators of $\mathfrak{G}$. We set $\theta_i(x_j) = \alpha_{ij} \in \Phi$. Then (2.0.1) and (2.0.2) are respectively equivalent to the following conditions:

If $k_1, \cdots, k_n$ are integers such that

(2.0.4) $$\sum_{j=1}^{n} \alpha_{ij}k_j = 0, \quad i = 1, \cdots, m,$$

then $k_1 \equiv \cdots \equiv k_n \equiv 0 \pmod{p}$, and

(2.0.5) The rank of the matrix (α_{ij}), $i = 1, \cdots, m$, $j = 1, \cdots, n$, is m.

Thus a generalized Witt algebra whose dimension is mp^n is completely characterized by mn elements $\alpha_{ij} \in \Phi$ satisfying (2.0.4) and (2.0.5). From (2.0.5) it follows immediately that $m \leqq n$. If $m = 1$ then (2.0.4) implies that Φ is of rank $\geqq n$ over $GF(p)$. Therefore if $m = 1$, and $\Phi = GF(p)$ then $n = 1$, so that the only generalized Witt algebra of D-dimension 1 over $GF(p)$ is the Witt algebra.

3. **Reduction of the algebras $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ to orthogonal form.** In this section, we show that any simple algebra of the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ can be written as $\mathfrak{L}(\mathfrak{A}; D_1', \cdots, D_m')$, where $D_i' \circ D_j' = 0$ for all i, j.

An ordered set $(D_1, \cdots, D_m)$ of derivations of a commutative associative algebra $\mathfrak{A}$ will be called a *system of derivations* of $\mathfrak{A}$ or simply a system if it satisfies (1.0.1) and (1.0.2). We shall say that the algebra $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is *defined* by the system $(D_1, \cdots, D_m)$. A system $(D_1, \cdots, D_m)$ will be called *orthogonal* if $D_i \circ D_j = 0$ for all i, j, that is, if in (1.0.1) $a_{ijk} = 0$ for all i, j, k, *orthonormal* if there exist m elements $f_i \in \mathfrak{A}$ such that $D_i f_j = \delta_{ij}$ (Kronecker delta). An orthonormal system is always orthogonal. Two systems $(D_1, \cdots, D_m)$ and $(D_1', \cdots, D_m')$ of $\mathfrak{A}$ will be called *equivalent* if there exist $c_{ij} \in \mathfrak{A}$ such that

$$D_i' = \sum_j c_{ij} D_j \qquad (i = 1, \cdots, m)$$

and such that $\det (c_{ij})$ is a unit of $\mathfrak{A}$. $(D_1, \cdots, D_m)$ and $(D_1', \cdots, D_m')$ are equivalent if and only if $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m) = \mathfrak{L}(\mathfrak{A}; D_1', \cdots, D_m')$ as sets.

LEMMA 3.1. *A system $(D_1, \cdots, D_m)$ of derivations of $\mathfrak{A}$ is equivalent to an orthonormal system if and only if there exist $f_1, \cdots, f_m \in \mathfrak{A}$ such that* $\det (D_i f_j)$ *is a unit in $\mathfrak{A}$.*

Proof. Suppose that $(D_1, \cdots, D_m)$ is equivalent to an orthonormal system $(D_1', \cdots, D_m')$ and let $D_i = \sum_j c_{ij} D_j'$, $D_i' f_j = \delta_{ij}$, where $\det (c_{ij})$ is a unit in $\mathfrak{A}$. Then we have $D_i f_j = c_{ij}$. Thus $\det (D_i f_j)$ is a unit in $\mathfrak{A}$.

Conversely, suppose that $\det (D_i f_j)$ is a unit in $\mathfrak{A}$ for some $f_1, \cdots, f_m \in \mathfrak{A}$. Let (c_{ij}') be the inverse matrix of the matrix $(D_i f_j)$. We set $D_i' = \sum_j c_{ij}' D_j$. Then $(D_1', \cdots, D_m')$ is equivalent to $(D_1, \cdots, D_m)$ and we have $D_i' f_j = \delta_{ij}$, so that $(D_1', \cdots, D_m')$ is orthonormal, which proves the lemma.

For a given algebra $\mathfrak{L} = \mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ we denote by $\mathfrak{K}$ the set of all elements $c \in \mathfrak{A}$ such that $Dc = 0$ for all $D \in \mathfrak{L}$. $\mathfrak{K}$ is a subalgebra of $\mathfrak{A}$. $\mathfrak{K}$ will be called the *algebra of constants* of $\mathfrak{L}$. Since $\mathfrak{A}$ is always assumed to have a unit element, we have $c \in \mathfrak{K}$ if and only if $D_1 c = \cdots = D_m c = 0$ for some defining system $(D_1, \cdots, D_m)$ of $\mathfrak{L}$.

The following lemma is useful.

LEMMA 3.2. *If the algebra $\mathfrak{K}$ of constants has a divisor of zero, then $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is not simple.*

Proof. Let $c \in \mathfrak{K}$ be a divisor of zero. The set $\mathfrak{J}$ of all cD, where $D \in \mathfrak{L}$, forms an ideal of $\mathfrak{L}$. For, $(cD) \circ D' = c(D \circ D') \in \mathfrak{J}$. If $\mathfrak{J} = 0$ then from (1.0.2) it follows that $c = 0$, a contradiction. If $\mathfrak{J} = \mathfrak{A}$ then $D_1 = c(f_1 D_1 + \cdots + f_m D_m)$ for some $f_1, \cdots, f_m \in \mathfrak{A}$. Then again from (1.0.2) it follows that $1 = cf_1$, which is impossible if c divides 0, and therefore $\mathfrak{L}$ is not simple.

A commutative associative algebra $\mathfrak{A}$ with unit element is *completely primary* if the set of all nonunits coincides with the radical of $\mathfrak{A}$.

LEMMA 3.3. *If $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple then $\mathfrak{A}$ is completely primary.*

Proof. Since $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple, from (3.2) it follows that the algebra $\mathfrak{K}$ of constants has no divisor of zero. Since $\mathfrak{A}$ is commutative and $\mathfrak{K}$ is finite-dimensional over the ground field, $\mathfrak{K}$ is a field. Let $f \in \mathfrak{A}$ be a nonunit. Since $D_i f^p = pf^{p-1} D_i f = 0$ for all i, we have $f^p \in \mathfrak{K}$. If $f^p \neq 0$ then f^p is a unit in $\mathfrak{A}$, and hence f is also a unit. This is a contradiction. Therefore $f^p = 0$ for all nonunits f. Thus $\mathfrak{A}$ is completely primary.

LEMMA 3.4. *Let $\mathfrak{A}$ be completely primary. If $f_1, \cdots, f_n$ are such that $ff_1 = \cdots = ff_n = 0$ with $f \in \mathfrak{A}$ implies $f = 0$, then at least one f_i is a unit in $\mathfrak{A}$.*

Proof. Assume that all f_i are nonunits. Then there exists a positive integer k such that $f_1^k = \cdots = f_n^k = 0$, and hence

$$f_1^{r_1} \cdots f_n^{r_n} = 0 \tag{3.4.1}$$

if $r_1 + \cdots + r_n \geqq nk$, where $r_1, \cdots, r_n$ are non-negative integers. Suppose, therefore, that (3.4.1) holds whenever $r_1 + \cdots + r_n > r$, a positive integer. Let $r_1 + \cdots + r_n = r$, $f = f_1^{r_1} \cdots f_n^{r_n}$. Then $ff_1 = \cdots = ff_n = 0$, and hence $f = 0$. Using complete induction with respect to r, we can conclude that (3.4.1) holds, whenever $r_1 + \cdots + r_n > 0$. In particular, $f_1 = \cdots = f_n = 0$. Take a nonzero $f \in \mathfrak{A}$. Then we have $ff_1 = \cdots = ff_n = 0$, a contradiction. Therefore at least one f_i must be a unit.

We can now prove the following

THEOREM 3.5. *If $\mathfrak{A}$ is completely primary, then any system $(D_1, \cdots, D_m)$ of derivations of $\mathfrak{A}$ is equivalent to an orthonormal system. In particular, any simple algebra of the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is defined by an orthonormal system.*

Proof. Let $u_1, \cdots, u_n$ be a basis of $\mathfrak{A}$ over the ground field Φ. We set

$$f_{i_1 \cdots i_r} = \begin{vmatrix} D_1 u_{i_1} & \cdots & D_1 u_{i_r} \\ & \cdots & \\ D_r u_{i_1} & \cdots & D_r u_{i_r} \end{vmatrix} \tag{3.5.1}$$

where $1 \leqq r \leqq m$. We shall prove by using (3.4) that $f_{i_1 \cdots i_m}$ is a unit for some choice of $i_1, \cdots, i_m$. Suppose, therefore, that $f \in \mathfrak{A}$ is such that $ff_{i_1 \cdots i_m} = 0$ for all $i_1, \cdots, i_m$. If

$$ff_{i_1 \cdots i_r} = 0 \tag{3.5.2}$$

is true for some r, and all $i_1, i_2, \cdots, i_r$, then by expanding the determinant $f_{i_1 \cdots i_r}$ along the rth column, we have

$$(3.5.3) \qquad ff_{i_1\cdots i_r} = (fc_1D_1 + \cdots + fc_rD_r)u_{i_r} = 0,$$

where $c_r = f_{i_1\cdots i_{r-1}}$. Since (3.5.3) is true for all i_r, we have $fc_iD_i + \cdots + fc_rD_r = 0$. Then from (1.0.2) we have $fc_1 = \cdots = fc_r = 0$, and in particular $ff_{i_1\cdots i_{r-1}} = 0$ for all $i_1, \cdots, i_{r-1}$. Proceeding by induction with respect to r, we can conclude that (3.5.2) holds for all r. Taking the case $r=1$, we have $fD_1u_{i_1}=0$ for all i_1. Therefore $fD_1=0$. Hence from (1.0.2) we have $f=0$. Therefore by Lemma 3.4 $f_{i_1\cdots i_m}$ is a unit for some $i_1, \cdots, i_m$. Then from Lemma 3.1 it follows that $(D_1, \cdots, D_m)$ is equivalent to an orthonormal system.

The second part of the theorem follows immediately from the above result and Lemma 3.3.

4. **Some lemmas.** We establish here a number of results we will need later. We assume throughout this section that $(D_1, \cdots, D_m)$ is orthonormal, that $x_1, \cdots, x_m \in \mathfrak{A}$ are such that $D_ix_j = \delta_{ij}$, and that $\mathfrak{J}$ is an ideal of $\mathfrak{L} = \mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$.

LEMMA 4.1. *If $D = f_1D_1 + \cdots + f_mD_m \in \mathfrak{J}$, then $f_kD \in \mathfrak{J}$ for any k.*

Proof. Since $Dx_k = f_k$, we have $D \circ (x_kD) = f_kD \in \mathfrak{J}$.

LEMMA 4.2. *If $D = f_1D_1 + \cdots + f_mD_m \in \mathfrak{J}$ and if f_k is a unit in $\mathfrak{A}$, then there exists $g_1D_1 + \cdots + g_mD_m \in \mathfrak{J}$, where $g_k = 1$ and where $g_i = 0$ for any i such that $f_i = 0$.*

Proof. Consider the element $U \in \mathfrak{J}$, where

$$U = \left(\frac{x_k}{f_k} D_k\right) \circ D = \frac{x_k}{f_k}(D_k \circ D) - D\left(\frac{x_k}{f_k}\right)D_k$$
$$= \frac{x_k}{f_k}(D_k \circ D) - D_k + \frac{x_k(Df_k)}{f_k^2} D_k.$$

Since $f_kD \in \mathfrak{J}$ by Lemma 4.1, we have also $V \in \mathfrak{J}$, where

$$V = \left(\frac{x_k}{f_k^2} D_k\right) \circ (f_kD) = \frac{x_k}{f_k}(D_k \circ D) + \frac{x_k(D_kf_k)}{f_k^2} D - f_kD\left(\frac{x_k}{f_k^2}\right)D_k$$
$$= \frac{x_k}{f_k}(D_k \circ D) + \frac{x_k(D_kf_k)}{f_k^2} D - D_k + \frac{2x_k(Df_k)}{f_k^2} D_k.$$

Then we have $V - 2U \in \mathfrak{J}$, where

$$V - 2U = -\frac{x_k}{f_k}(D_k \circ D) + \frac{x_k(D_kf_k)}{f_k^2} D + D_k.$$

Setting $V - 2U = g_1D_1 + \cdots + g_mD_m$, we have

$$g_k = -\frac{x_k(D_kf_k)}{f_k} + \frac{x_k(D_kf_k)}{f_k} + 1 = 1,$$

and for $i \neq k$,

$$g_i = -\frac{x_k(D_k f_i)}{f_k} + \frac{x_k(D_k f_k) f_i}{f_k^2}.$$

Therefore, if $f_i = 0$ then $g_i = 0$, completing the proof.

LEMMA 4.3. *If $f_1, \cdots, f_m$ belong to the algebra $\mathfrak{K}$ of constants of $\mathfrak{L}$ and are such that $f_1D_1 + \cdots + f_mD_m \in \mathfrak{J}$, and if some f_k is a unit, then $D_i \in \mathfrak{J}$ for all $i = 1, \cdots, m$.*

Proof. Suppose that f_k is a unit. Then $(f_1D_1 + \cdots + f_mD_m) \circ ((x_k/f_k)D_i) = D_i \in \mathfrak{J}$ for all $i = 1, \cdots, m$.

LEMMA 4.4. *$D_1 \in \mathfrak{J}$ implies $\mathfrak{J} = \mathfrak{L}$ except when $p = 2$, $m = 1$.*

Proof. If $D_1 \in \mathfrak{J}$ then from Lemma 4.3 it follows that $D_i \in \mathfrak{J}$ for $i = 1, \cdots, m$. Take an arbitrary element $f \in A$. Then from $D_j \circ (fD_i) = (D_j f)D_i$ we have

(4.4.1) $$(D_j f)D_i \in I \quad \text{for all } i, j.$$

First we consider the case $p \neq 2$. Since $D_i(x_i^2) = 2x_i$, from (4.4.1) we have $2x_iD_i \in \mathfrak{J}$. Since $p \neq 2$, we have $x_iD_i \in \mathfrak{J}$. Hence

(4.4.2) $$(fD_i) \circ (x_iD_i) = fD_i - x_i(D_i f)D_i \in \mathfrak{J}.$$

On the other hand, since $D_i(x_i f) = f + x_i(D_i f)$, from (4.4.1) we have

(4.4.3) $$fD_i + x_i(D_i f)D_i \in \mathfrak{J}.$$

From (4.4.2) and (4.4.3) we have $2fD_i \in \mathfrak{J}$. Since $p \neq 2$ we have $fD_i \in \mathfrak{J}$. Since f and i are arbitrary, we have $\mathfrak{J} = \mathfrak{L}$.

Now we consider the case $p = 2$, $m > 1$. For given i we may take j such that $j \neq i$. Since $D_i(x_ix_j) = x_j$, from (4.4.1) we have $x_jD_i \in \mathfrak{J}$. Then $(fD_j) \circ (x_jD_i) = fD_i - x_j(D_i f)D_j \in \mathfrak{J}$. However, we have $x_j(D_i f)D_j = D_i(x_j f)D_j \in \mathfrak{J}$ from (4.4.1). Therefore $fD_i \in \mathfrak{J}$. Since f and i are arbitrary we have $\mathfrak{J} = \mathfrak{L}$, completing the proof.

5. **Derivations of a field.** A subalgebra $\mathfrak{L}$ of the derivation algebra $\mathfrak{D}(\mathfrak{A})$ of $\mathfrak{A}$ will be called *regular* if $fD \in \mathfrak{L}$ for every $f \in \mathfrak{A}$ and $D \in \mathfrak{L}$. $\mathfrak{D}(\mathfrak{A})$ itself is a regular subalgebra of $\mathfrak{D}(\mathfrak{A})$. If $\mathfrak{A}$ is itself a field, any regular subalgebra $\mathfrak{L}$ of $\mathfrak{D}(\mathfrak{A})$ may be considered as a vector space over the field $\mathfrak{A}$, since if $D, D' \in \mathfrak{L}$, then $fD + f'D' \in \mathfrak{L}$, where $f, f' \in \mathfrak{A}$. Take a basis $D_1, \cdots, D_m$ of $\mathfrak{L}$ over $\mathfrak{A}$. Then it is easily seen that $D_1, \cdots, D_m$ satisfy (1.0.1) and (1.0.2). Therefore, if $\mathfrak{A}$ is a field, any regular subalgebra of $\mathfrak{D}(\mathfrak{A})$ is of the type $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, and we call m the *D-dimension* of the regular subalgebra $\mathfrak{L}$.

THEOREM 5.1. *Let $\mathfrak{A}$ be a field over Φ. Then any regular subalgebra $\mathfrak{L}$ of the derivation algebra of $\mathfrak{A}$ over Φ is simple except when $p = 2$, $m = 1$, where m is the D-dimension of $\mathfrak{L}$.*

Proof. $\mathfrak{L}$ can be written in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. By Theorem 3.5 we may assume that $(D_1, \cdots, D_m)$ is orthonormal.

Let $\mathfrak{J}$ be a nonzero ideal of $\mathfrak{L}$ and $f_1D_1 + \cdots + f_mD_m$ be a nonzero element in $\mathfrak{J}$ such that the number of nonzero f_i is as small as possible. If $f_k \neq 0$ then by Lemma 4.2 $\mathfrak{J}$ contains an element $g_1D_1 + \cdots + g_mD_m$ such that $g_k = 1$ and such that $g_i = 0$ whenever $f_i = 0$, so we may assume at the outset that $f_k = 1$ for some k. Since $\mathfrak{J}$ is an ideal, we have $D_i \circ (f_1D_1 + \cdots + f_mD_m) = (D_if_1)D_1 + \cdots + (D_if_m)D_m \in \mathfrak{J}$ for $i = 1, \cdots, m$. Since $f_k = 1$, the number of nonzero coefficients in $(D_if_1)D_1 + \cdots + (D_if_m)D_m$ is less than that of $f_1D_1 + \cdots + f_mD_m$. Therefore $D_if_j = 0$ for all i, j, and hence we have $f_1, \cdots, f_m \in \mathfrak{K}$, the algebra of constants of $\mathfrak{L}$. Since $\mathfrak{K}$ is a subfield of $\mathfrak{A}$, from Lemma 4.3 we have $D_i \in \mathfrak{J}$ for $i = 1, \cdots, m$, and $\mathfrak{J} = \mathfrak{L}$ from Lemma 4.4. Therefore $\mathfrak{L}$ is simple.

The method used in the proof of Theorem 5.1 can also be applied to the case of a field of characteristic 0, if we start with an orthonormal system. For example, consider the field $\Phi(x_1, \cdots, x_m)$ of rational functions in m variables $x_1, \cdots, x_m$ over a field Φ of characteristic 0, and let $\mathfrak{A}$ be a finite-dimensional extension field of $\Phi(x_1, \cdots, x_m)$. Then $\mathfrak{A}$ is an infinite-dimensional algebra over Φ. It is well known that there exist derivations $\partial/\partial x_1, \cdots, \partial/\partial x_m$ of $\mathfrak{A}$ over Φ such that $(\partial/\partial x_i)x_j = \delta_{ij}$, and that every derivation D of $\mathfrak{A}$ written is uniquely in the form

$$D = f_1 \frac{\partial}{\partial x_1} + \cdots + f_m \frac{\partial}{\partial x_m}, \quad \text{where} \quad f_1, \cdots, f_m \in \mathfrak{A}.$$

In other words, the derivation algebra $\mathfrak{D}(\mathfrak{A})$ of $\mathfrak{A}$ over Φ can be written as $\mathfrak{D}(\mathfrak{A}) = \mathfrak{L}(\mathfrak{A}; \partial/\partial x_1, \cdots, \partial/\partial x_m)$. The above method enables us to prove that $\mathfrak{D}(\mathfrak{A})$ is an infinite-dimensional simple Lie algebra of characteristic zero.

If we consider the polynomial domain $\mathfrak{A} = \Phi[x_1, \cdots, x_m]$, instead of $\Phi(x_1, \cdots, x_m)$, as an algebra over Φ, then again we may prove that $\mathfrak{D}(\mathfrak{A})$ is simple.

The above two classes of infinite-dimensional simple Lie algebras, together with the infinite-dimensional algebras constructed by Kaplansky's method, may be regarded as analogues of the Witt algebra in the case of characteristic 0.

6. **Simple algebras when Φ is algebraically closed.** The main result of this section is that if the ground field Φ is algebraically closed then any simple algebra of the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is a generalized Witt algebra.

LEMMA 6.1. *Suppose that $\mathfrak{L} = \mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple. If $f \in \mathfrak{A}$ is such that $D_if = \lambda_if$, $\lambda_i \in \Phi$, for all i, then $f = 0$ or f is a unit in $\mathfrak{A}$.*

Proof. If f is as above, the set $\mathfrak{J}$ of all elements of the form fD, where $D \in \mathfrak{L}$, is an ideal of $\mathfrak{L}$. For, if $\sum g_iD_i \in \mathfrak{L}$ then $(fD) \circ (\sum g_iD_i) = f\sum((Dg_i)D_i - g_i\lambda_iD) \in \mathfrak{J}$. Since $\mathfrak{L}$ is assumed to be simple, $\mathfrak{J} = 0$ for $\mathfrak{J} = \mathfrak{A}$. If $\mathfrak{J} = 0$ then $f = 0$ by (1.0.2). If $\mathfrak{J} = \mathfrak{A}$ then again by (1.0.2) f is a unit in $\mathfrak{A}$, as required.

By Theorem 3.5, any simple algebra of the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is defined by an orthonormal system. Moreover, by Lemma 3.2, the algebra $\mathfrak{K}$ of constants for the simple algebra $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is a field over Φ, and if Φ is algebraically closed, we have $\mathfrak{K}=\Phi$. Since we are mainly interested in this section in simple algebras, we shall assume that the conditions (6.1.1)–(6.1.3) below hold. The last two of these are necessary if $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple, as is seen from Lemma 6.1 and the above remark. The ground field Φ is assumed algebraically closed.

(6.1.1) The system $(D_1, \cdots, D_m)$ is orthogonal.

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

(6.1.3) $D_1 f = \cdots = D_m f = 0$ implies $f \in \Phi$.

These conditions and the fact that Φ is algebraically closed will enable us to prove that $\mathfrak{A}$ is the group algebra of an elementary p-group.

LEMMA 6.2. *Suppose that Φ is algebraically closed. Then any nonzero ideal of an algebra $\mathfrak{L}=\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ defined by a system satisfying the conditions* (6.1.1)–(6.1.3) *above contains an element of the form $\sum a_i D_i$, where at least one a_i is a unit in $\mathfrak{A}$.*

Proof. Let $\mathfrak{J}$ be the nonzero ideal of $\mathfrak{L}$. For any i, the mapping: $X \rightarrow D_i \circ X$ defines a linear transformation of $\mathfrak{J}$ into itself. Since $D_i \circ (D_j \circ X) = D_j \circ (D_i \circ X)$ for all i and j, and since Φ is algebraically closed, there exists a nonzero element $A = \sum a_i D_i$ in $\mathfrak{J}$ such that $D_i \circ A = \lambda_i A$, where $\lambda_i \in \Phi$, for all i. Then we have $D_i a_j = \lambda_i a_j$ for all i and j. Hence by (6.1.2), every a_j is either 0 or a unit in $\mathfrak{A}$. Since not all a_j are zero, at least one a_j must be a unit.

LEMMA 6.3. *Suppose that Φ is algebraically closed. Then for any system $(D_1, \cdots, D_m)$ the conditions* (6.1.1)–(6.1.3) *imply the following: If $f, a_1, \cdots, a_m$ in $\mathfrak{A}$ are such that $D_i f = a_i f$ for all i, then $f=0$ or f is a unit in $\mathfrak{A}$.*

Proof. The set of all elements of the form $\sum f f_i D_i$ is easily seen to be an ideal of the algebra $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$. If $f \neq 0$ then $\mathfrak{J} \neq 0$ and hence by Lemma 6.2 there exists an element $\sum a_i D_i$ in $\mathfrak{J}$ for which at least one a_i is a unit. Suppose $\sum f f_i D_i = \sum a_i D_i$. Then $f f_i = a_i$ and hence f is a unit.

LEMMA 6.4. *Suppose that Φ is algebraically closed. Then any orthogonal system equivalent to an orthogonal system $(D_1, \cdots, D_m)$ satisfying* (6.1.2) *and* (6.1.3) *also satisfies* (6.1.2) *and* (6.1.3).

Proof. Let $(D_1', \cdots, D_m')$ be the orthogonal system equivalent to $(D_1, \cdots, D_m)$, and let $D_i = \sum_j c_{ij} D_j'$. If $D_j' f = \lambda_j f$ for all j then $D_i f = a_i f$, where $a_i = \sum_j c_{ij} \lambda_j$. Then from Lemma 6.3 it follows that $f=0$ or f is a unit. Thus (6.1.2) is verified for $(D_1', \cdots, D_m')$. Suppose now $D_j' f = 0$ for all j.

Since det (c_{ij}) is a unit in A, we have $D_if=0$ for all i. Therefore $f\in\Phi$. Thus (6.1.3) is also verified.

We consider $\mathfrak{A}$ as an Ω-module, where the operator domain Ω consists of multiplications by elements in Φ and the linear mappings $D_1, \cdots, D_m$ (of $\mathfrak{A}$ into itself). Since every two operators in Ω are commutative, and since Φ is algebraically closed, all the factor modules in any composition series of the Ω-module $\mathfrak{A}$ are one-dimensional vector spaces over Φ.

We decompose $\mathfrak{A}$ into a direct sum $\mathfrak{A}=\sum\mathfrak{A}_\nu$ of directly indecomposable Ω-submodules. Then, since $D_1, \cdots, D_m$ are commutative, each D_i has exactly one characteristic root $\lambda_{i\nu}$ in $\mathfrak{A}_\nu$, when we consider D_i as a linear mapping of $\mathfrak{A}_\nu$ into itself, and there exists a nonzero $u_\nu\in\mathfrak{A}_\nu$ such that $D_iu_\nu=\lambda_{i\nu}u_\nu$ for all i and ν. By the condition (6.1.2), u_ν is a unit. Since $u_\nu^p\in\Phi$ by (6.1.3), and since Φ is algebraically closed, we may assume

$$u_\nu^p = 1 \text{ for all } \nu. \tag{6.4.1}$$

We shall prove that all the u_ν forms an elementary p-group with respect to the multiplication in $\mathfrak{A}$.

LEMMA 6.5. *If $D_if=\lambda_if$, $\lambda_i\in\Phi$, for all i, and if $f\neq 0$, then there exists an $\mathfrak{A}_\rho$ such that $f\in\mathfrak{A}_\rho$, $\lambda_i=\lambda_{i\rho}$.*

Proof. Let $f=\sum f_\nu$, where $f_\nu\in\mathfrak{A}_\nu$. Then from $D_if=\lambda_if$ it follows that $\sum D_if_\nu=\sum\lambda_if_\nu$. Since $D_if_\nu\in\mathfrak{A}_\nu$, we have $D_if_\nu=\lambda_if_\nu$ for all i and ν. Suppose that $f_\nu\neq 0\neq f_\mu$ for two different indices ν and μ. Then, by condition (6.1.2), f_ν and f_μ are units. By an easy calculation we obtain $D_i(f_\nu f_\mu^{-1})=0$ for all i. Then by (6.1.3) we have $f_\nu f_\mu^{-1}\in\Phi$. However, this is impossible since $\mathfrak{A}_\nu\cap\mathfrak{A}_\mu=0$, and therefore all but one of the f_ν are zero. Thus there exists an $\mathfrak{A}_\rho$ such that $f\in\mathfrak{A}_\rho$. Since $f\neq 0$ is assumed, and since D_i has only one characteristic root $\lambda_{i\rho}$ in $\mathfrak{A}_\rho$, we have $\lambda_i=\lambda_{i\rho}$.

Now, for any two indices ν and μ, we have $D_i(u_\nu u_\mu)=(\lambda_{i\nu}+\lambda_{i\mu})u_\nu u_\mu$ for all i. Therefore, since $u_\nu u_\mu\neq 0$ by (6.4.1), it follows from Lemma 6.5 that there exists an $\mathfrak{A}_\rho$ such that $u_\nu u_\mu\in\mathfrak{A}_\rho$ and such that

$$\lambda_{i\nu} + \lambda_{i\mu} = \lambda_{i\rho} \text{ for all } i. \tag{6.5.1}$$

From (6.5.1) it follows that $D_i(u_\nu u_\mu u_\rho^{-1})=0$ for all i. Then (6.1.3) yields $u_\nu u_\mu=\alpha u_\rho$ with some $\alpha\in\Phi$, and therefore by (6.4.1) $\alpha^p=1$. Hence $(\alpha-1)^p=0$, $\alpha=1$. Thus we have $u_\nu u_\mu=u_\rho$. Therefore all the u_ν form a group $\mathfrak{G}$ with respect to the multiplication in $\mathfrak{A}$. $\mathfrak{G}$ is an elementary p-group because of (6.4.1).

We shall show that there exists only one index ν such that $\lambda_{i\nu}=0$ for all i. If $f=1$ is the unity element of $\mathfrak{A}$ then $D_if=0$ for all i. Therefore by Lemma 6.5 there exists an index 0 such that $1\in\mathfrak{A}_0$. Suppose that $\lambda_{i\nu}=0$ for all i. Then $D_i(u_\nu)=0$ for all i. By (6.1.3) we have $u_\nu\in\Phi$, and hence $u_\nu=1$, $\nu=0$. Generalizing the previous statement we can show easily that $\lambda_{i\nu}=\lambda_{i\mu}$ for all i implies $\nu=\mu$.

LEMMA 6.6. *An element* $f \in \mathfrak{A}$ *belongs to* $\mathfrak{A}_\nu$ *if and only if there exist integers* $t_i > 0$, $i = 1, \cdots, m$, *such that*

$$(D_i - \lambda_{i\nu})^{t_i} f = 0, \qquad (i = 1, \cdots, m). \tag{6.6.1}$$

Proof. The "only if" part is obvious. In order to prove the "if" part, let $f = \sum f_\mu$, $f_\mu \in \mathfrak{A}_\mu$. Since $\mathfrak{A}_\mu$ are Ω-submodules, (6.6.1) yields $(D_i - \lambda_{i\nu})^{t_i} f_\mu = 0$ for all i and μ. Then $f_\mu = 0$ for $\mu \neq \nu$ follows from the fact that D_i has only one characteristic root $\lambda_{i\mu}$ in $\mathfrak{A}_\mu$. Hence $f = f_\nu \in \mathfrak{A}_\nu$.

COROLLARY 6.7. *If* $D_i f \in \mathfrak{A}_0$ *for all* i *then* $f \in \mathfrak{A}_0$.

LEMMA 6.8. $\mathfrak{A}_\nu = u_\nu \mathfrak{A}_0$ *for all* ν.

Proof. Let $f \in \mathfrak{A}_\nu$, $g \in \mathfrak{A}_\mu$. Then there exist integers $s_i > 0$ such that

$$(D_i - \lambda_{i\mu})^{s_i} g = 0, \qquad (i = 1, \cdots, m). \tag{6.8.1}$$

By applying the Cartan-Weyl identity to (6.3.1) and (6.5.1) we obtain

$$(D_i - (\lambda_{i\nu} + \lambda_{i\mu}))^{t_i + s_i - 1}(fg) = 0 \tag{6.8.2}$$

for all i. Then by Lemma 6.3 and (6.2.1), we have $fg \in \mathfrak{A}_\rho$, where $u_\nu u_\mu = u_\rho$. Thus we may write

$$\mathfrak{A}_\nu \mathfrak{A}_\mu \subseteq \mathfrak{A}_\rho, \qquad (u_\nu u_\mu = u_\rho). \tag{6.8.3}$$

Since u_ν is a unit of $\mathfrak{A}$ it follows that the linear multiplication induced by left multiplication with u_ν is invertible, hence there is the decomposition of $\mathfrak{A}$ into the direct sum

$$\mathfrak{A} = \sum_\mu u_\nu \mathfrak{A}_\mu. \tag{6.8.4}$$

Moreover, the module $u_\nu \mathfrak{A}_\mu$ is Ω-invariant, because for $g \in \mathfrak{A}_\mu$ we have $D_i(u_\nu g) = (D_i u_\nu) g + u_\nu D_i(g) = u_\nu(\lambda_{i\nu} g + D_i g) \in u_\nu \mathfrak{A}_\mu$. Hence by using the group property of $\mathfrak{G}$ it follows that (6.8.4) is a direct decomposition of $\mathfrak{A}$ into Ω-submodules each of which is contained in a different summand of the given Remak decomposition of $\mathfrak{A}$. In other words we have $u_\nu \mathfrak{A}_\mu = \mathfrak{A}_\rho$, where $u_\rho = u_\nu u_\mu$, and in particular $\mathfrak{A}_\nu = u_\nu \mathfrak{A}_0$.

From (6.8.3) we have

COROLLARY 6.9. $\mathfrak{A}_0$ *is a subalgebra of* $\mathfrak{A}$.

Since $\mathfrak{A}_0$ depends on the system $(D_1, \cdots, D_m)$ we may write $\mathfrak{A}_0 = \mathfrak{A}_0(D_1, \cdots, D_m)$. We shall show that there exists an orthogonal system $(E_1, \cdots, E_m)$ equivalent to the given system $(D_1, \cdots, D_m)$ such that $\mathfrak{A}_0(E_1, \cdots, E_m) = \Phi$. To do this, it will be sufficient to show that we can always find an orthogonal system $(D_1', \cdots, D_m')$ equivalent to $(D_1, \cdots, D_m)$

such that the dimension of $\mathfrak{A}_0(D_1', \cdots, D_m')$ is less than that of $\mathfrak{A}_0(D_1, \cdots, D_m)$ whenever the latter is greater than one. Since $D_i 1 = 0$ for all i, it follows that there is a Ω-composition series

$$(6.10.1)\quad 0 < \Phi < \Phi + \Phi w_2 < \cdots < \Phi + \Phi w_2 + \cdots + \Phi w_n = \mathfrak{A}_0$$

for the Ω-module $\mathfrak{A}_0$. If w_2 is not a unit then by (6.1.3) we have $w_2^p = 0$. Then $1 + w_2$ is a unit. By replacing w_2 by $1 + w_2$ if w_2 is not a unit, we can always assume that w_2 is a unit. From (6.10.1) we have $D_i w_2 = \beta_i \in \Phi$ for all i. By (6.1.3) we see that not all β_i are zero. We may assume without loss of generality that $\beta_1 \neq 0$. We set $x = \beta_1^{-1} w_2$, $D_1'' = D_1$, $D_i'' = \beta_1 D_i - \beta_i D_1$ for $i \neq 1$. Then $(D_1'', \cdots, D_m'')$ is an orthogonal system equivalent to $(D_1, \cdots, D_m)$ such that $D_1'' x = 1$, $D_i'' x = 0$ for all $i \neq 1$. Set $D_1' = x D_1''$, $D_i' = D_i''$ for $i \neq 1$. Then $(D_1', \cdots, D_m')$ is an orthogonal system equivalent to $(D_1'', \cdots, D_m'')$ and hence to $D_1, \cdots, D_m)$ such that

$$(6.10.3)\qquad D_1' x = x \neq 0, \quad \text{where} \quad x \in \mathfrak{A}_0(D_1, \cdots, D_m);$$

$$(6.10.4)\qquad D_i = \sum_j c_{ij} D_j', \text{ where } c_{ij} \in \mathfrak{A}_0(D_1, \cdots, D_m).$$

The new orthogonal system $(D_1', \cdots, D_m')$, being equivalent to $(D_1, \cdots, D_m)$, satisfies (6.1.2) and (6.1.3) by Lemma 6.4.

We shall show that $\mathfrak{A}_0(D_1', \cdots, D_m')$ is properly contained in $\mathfrak{A}_0(D_1, \cdots, D_m)$. Take a basis $v_1, \cdots, v_r$ of $\mathfrak{A}_0(D_1', \cdots, D_m')$ such that

$$(6.10.5)\qquad D_i' v_1 = 0, \qquad D_i' v_k = \sum_{s<k} \alpha_{iks} v_s \qquad (k > 1),$$

for all i, where $\alpha_{iks} \in \Phi$. From (6.10.5) and (6.1.3) we have $v_1 \in \Phi$, and hence $v_1 \in \mathfrak{A}_0(D_1, \cdots, D_m)$. Suppose that $v_1, \cdots, v_{k-1} \in \mathfrak{A}_0(D_1, \cdots, D_m)$. Then from (6.10.4) and (6.10.5) we have

$$(6.10.6)\qquad D_i v_k = \sum_{s<k} \sum_{j=1}^{m} c_{ij} \alpha_{jks} v_s.$$

Since c_{ij}, α_{jks}, and v_s belong to $\mathfrak{A}_0(D_1, \cdots, D_m)$, by Corollary 6.9 we see that the right-hand side of (6.10.6) belongs to $\mathfrak{A}_0(D_1, \cdots, D_m)$ for all i. Therefore from Corollary 6.7 it follows that $v_k \in \mathfrak{A}_0(D_1, \cdots, D_m)$. Proceeding by induction with respect to k, we have $v_k \in \mathfrak{A}_0(D_1, \cdots, D_m)$ for all k. Therefore $\mathfrak{A}_0(D_1', \cdots, D_m') \leqq \mathfrak{A}_0(D_1, \cdots, D_m)$. Suppose $\mathfrak{A}_0(D_1', \cdots, D_m') = \mathfrak{A}_0(D_1, \cdots, D_m) = \mathfrak{A}_0$. Since $f \in \mathfrak{A}_0$ implies $D_1' f \in \mathfrak{A}_0$, we can regard D_1' as a linear mapping of $\mathfrak{A}_0$ into itself. By the definition of $\mathfrak{A}_0$, 0 is the only characteristic root of D_1' in $\mathfrak{A}_0$. However, this contradicts (6.10.3). Thus $\mathfrak{A}_0(D_1, \cdots, D_m)$ is properly contained in $\mathfrak{A}_0(D_1, \cdots, D_m)$, and hence the dimension of the former is less than that of the latter. Repeating the above process, we obtain an orthogonal system $(E_1, \cdots, E_m)$ equivalent to the given system $(D_1, \cdots, D_m)$ such that $\mathfrak{A}_0(E_1, \cdots, E_m)$ is one-dimensional.

Since the algebras $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ defined by the equivalent systems are the same, we may suppose $\mathfrak{A}_0 = \Phi$. Then from Lemma 6.8 we have

$$\mathfrak{A} = \sum \Phi u_\nu, \qquad D_i u_\nu = \lambda_{i\nu} u_\nu, \tag{6.10.7}$$

for all i and ν. From (6.7.9) we see that $\mathfrak{A}$ is the group algebra of the elementary p-group $\mathfrak{G}$ formed by all u_ν. We shall show that if (6.10.7) holds, then $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is isomorphic to a generalized Witt algebra. We define the mapping θ_i of $\mathfrak{G}$ into Φ by $\theta_i(u_\nu) = \lambda_{i\nu}$. Then from (6.2.1) it follows that $\theta_1, \cdots, \theta_m$ are homomorphisms of $\mathfrak{G}$ into the additive group of Φ. We shall show that (2.0.1) and (2.0.2) are satisfied by $\theta_1, \cdots, \theta_m$. Suppose $\theta_1(u_\sigma) = \cdots = \theta_m(u_\sigma) = 0$. Then $\lambda_{i\sigma} = 0$ for all i, and hence $\sigma = 0$, $u_\sigma = 1$. Thus (2.0.1) is satisfied. Suppose now that $\alpha_1\theta_1 + \cdots + \alpha_m\theta_m = 0$. Then $\sum_i \alpha_i \lambda_{i\nu} = 0$ for all ν, and hence from (6.10.7) we have $\alpha_1 D_1 + \cdots + \alpha_m D_m = 0$. Then (1.0.2) yields $\alpha_1 = \cdots = \alpha_m = 0$. Thus (2.0.2) is also satisfied. Therefore by the result in §2 $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is isomorphic to a generalized Witt algebra.

Thus we have proved the following

THEOREM 6.10. *Suppose that Φ is algebraically closed and that the system $(D_1, \cdots, D_m)$ is orthogonal. Then the algebra $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is isomorphic to a generalized Witt algebra if and only if the following conditions* (6.1.2) *and* (6.1.3) *hold*:

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

(6.1.3) *$D_1 f = \cdots D_m f = 0$ implies $f \in \Phi$.*

In particular, if an algebra $\mathfrak{L}$ of the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, where $(D_1, \cdots, D_m)$ is not necessarily orthogonal, over an algebraically closed field Φ is simple, then $\mathfrak{L}$ is isomorphic to a generalized Witt algebra and $\mathfrak{A}$ to the group algebra of an elementary p-group.

Let $\mathfrak{A}$, $\mathfrak{B}$ be commutative associative algebras over the same ground field Φ, and $(D_1, \cdots, D_m)$, $(E_1, \cdots, E_m)$ orthogonal systems of derivations of $\mathfrak{A}$, $\mathfrak{B}$, respectively, such that

$$\mathfrak{A}_0(D_1, \cdots, D_m) = \mathfrak{A}, \qquad \mathfrak{B}_0(E_1, \cdots, E_m) = \Phi. \tag{6.11.1}$$

Let $\mathfrak{C}$ be the Kronecker product algebra of $\mathfrak{A}$, $\mathfrak{B}$, and define derivations F_i of $\mathfrak{C}$ by setting $F_i = D_i$ on $\mathfrak{A}$ and $F_i = E_i$ on $\mathfrak{B}$. Then $(F_1, \cdots, F_m)$ is an orthogonal system over $\mathfrak{C}$. It is easily seen that the conditions (6.1.2) and (6.1.3) are satisfied for $(F_1, \cdots, F_m)$. Hence by Theorem 6.10 we obtain $\mathfrak{L}(\mathfrak{C}; F_1, \cdots, F_m)$ isomorphic to a generalized Witt algebra. $\mathfrak{L}(\mathfrak{C}; F_1, \cdots, F_m)$ may be regarded as a *composite* of $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ and $\mathfrak{L}(\mathfrak{B}; E_1, \cdots, E_m)$.

Note that $(F_1, \cdots, F_m)$ does not always satisfy the conditions (6.1.2)–(6.1.3) unless (6.11.1) holds.

7. **Nilpotent systems** (1). A system $(D_1, \cdots, D_m)$ will be called *nilpotent* if there exists a positive integer k such that $D_1^k = \cdots = D_m^k = 0$. If the ground field Φ is algebraically closed then an orthogonal system $(D_1, \cdots, D_m)$ is nilpotent if and only if $\mathfrak{A}_0(D_1, \cdots, D_m) = \mathfrak{A}$. In the preceding section we have proved that if Φ is algebraically closed then any simple algebra of the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ can be defined by an orthogonal system for which $\mathfrak{A}_0 = \Phi$. The case $\mathfrak{A}_0 = \mathfrak{A}$ and the case $\mathfrak{A}_0 = \Phi$ are two extreme cases. Now we shall prove the following

THEOREM 7.1. *Suppose that Φ is algebraically closed. Then any orthogonal system $(D_1, \cdots, D_m)$ satisfying* (6.1.2) *and* (6.1.3) *is equivalent to a nilpotent orthogonal system. In particular, any generalized Witt algebra over Φ can be written in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, where $\mathfrak{A}$ is the group algebra of an elementary p-group and where $(D_1, \cdots, D_m)$ is a nilpotent orthogonal system.*

Proof. We shall use the notations employed in the preceding section. Because of the remark in the first paragraph of this section, it is sufficient to prove the following: If $(D_1, \cdots, D_m)$ is an orthogonal system satisfying (6.1.2) and (6.1.3) and if $\mathfrak{A}_0 = \mathfrak{A}_0(D_1, \cdots, D_m) \neq \mathfrak{A}$ then there exists an orthogonal system $(D_1', \cdots, D_m')$ which satisfies the conditions (6.1.2) and (6.1.3) and is equivalent to $(D_1, \cdots, D_m)$ such that $\mathfrak{A}_0$ is properly contained in $\mathfrak{A}_0' = \mathfrak{A}_0(D_1', \cdots, D_m')$. By Lemma 6.8 we have $\mathfrak{A} = \sum u_\nu \mathfrak{A}_0$, $D_i u_\nu = \lambda_{i\nu} u_\nu$, where $\lambda_{i\nu} \in \Phi$. Therefore, if $\mathfrak{A}_0 \neq \mathfrak{A}$, then there exists a $u_\sigma \neq 1$, which we shall fix hereafter. Since not all $\lambda_{i\sigma}$ are 0, we may assume without loss of generality that $\lambda_{1\sigma} \neq 0$. We set $D_1'' = D_1$, $D_i'' = \lambda_{1\sigma} D_i - \lambda_{i\sigma} D_1$ for $i \neq 0$, and $x = \lambda_{1\sigma}^{-1} u_\sigma$. Then x is a unit and $(D_1'', \cdots, D_m'')$ is an orthogonal system equivalent to $(D_1, \cdots, D_m)$ such that $D_1'' x = x$, $D_i'' x = 0$ for $i \neq 1$. We set $D_1' = x^{-1} D_1''$, and $D_i' = D_i''$ for $i \neq 1$. Then $(D_1', \cdots, D_m')$ is an orthogonal system equivalent to $(D_1'', \cdots, D_m'')$, and hence to $(D_1, \cdots, D_m)$, such that $D_1' x = 1$, $D_i' x = 0$ for $i \neq 1$. Therefore $x \in A_0'$ by Corollary 6.8. Thus $\mathfrak{A}_0 \neq \mathfrak{A}_0'$. Since $u_0 \in \mathfrak{A}_0'$, from the above construction we have

$$D_i' = \sum_j c_{ij} D_j, \qquad c_{ij} \in \mathfrak{A}_0'. \tag{7.1.1}$$

Using (7.1.1) and proceeding the same way as in the preceding section we see that $\mathfrak{A}_0$ is properly contained in $\mathfrak{A}_0'$.

REMARK. A derivation E of $\mathfrak{A}$ over Φ will be called *normal* if $Ef = 0$ implies $f \in \Phi$. It is clear that if D_1 in the above proof is normal then $\lambda_{1\nu} \neq 0$ for every $\nu \neq 0$ and hence we may use D_1 instead of D. Then $D_1' = (\lambda_{1\sigma} u_\sigma)^{-1} D_1$ is also normal. Therefore if $(D_1, \cdots, D_m)$ is an orthogonal system satisfying (6.1.2) and (6.1.3) and if D_1 is normal then there exists a nilpotent system $(D_1', \cdots,$

D'_m) equivalent to $(D_1, \cdots, D_m)$ such that D'_1 is normal. This fact will be used later in §9.

The above result may be refined if it is combined with the following

THEOREM 7.2. *If a nilpotent orthogonal system* $(D_1, \cdots, D_m)$ *satisfies* (6.1.3) *then there exist* $x_1, \cdots, x_n \in \mathfrak{A}$ *such that the elements* $x_1^{\nu_1} \cdots x_n^{\nu_n}$, *where* $0 \leqq \nu_i < p$, $x_i^0 = 1$, $x_i^p \in \Phi$, *form a basis of* $\mathfrak{A}$ *over* Φ *and such that* $D_i x_1 \in \Phi$, $D_i x_k \in \Phi(x_1, \cdots, x_{k-1})$, *the subalgebra of* $\mathfrak{A}$ *generated by* $x_1, \cdots, x_{k-1}$ *over* Φ, *for all* i *and* $k > 1$. *If, in particular,* Φ *is perfect in the sense that every element in* Φ *is a pth power of an element in* Φ, *then* $x_1, \cdots, x_n$ *may be taken such that either* $x_1^p = \cdots = x_n^p = 1$ *or* $x_1^p = \cdots = x_n^p = 0$.

The proof follows easily from the following two lemmas.

LEMMA 7.3. *Suppose that* $(D_1, \cdots, D_m)$ *is a nilpotent orthogonal system. If* $v_1, \cdots, v_r \in \mathfrak{A}$ *are linearly independent over* Φ, *if* $D_i v_1 = 0$, *and if* $D_i v_k$ *is a linear combination of* $v_1, \cdots, v_{k-1}$ *for all* i *and* $k > 1$, *then there exists an element* $v \in \mathfrak{A}$ *which is not a linear combination of* $v_1, \cdots, v_r$ *such that* $D_i v$ *is a linear combination of* $v_1, \cdots, v_r$ *for all* i, *provided that* $\mathfrak{A}$ *is not spanned by* $v_1, \cdots, v_r$.

Proof. Denote by $\mathfrak{R}_k$ the Ω-subspace of $\mathfrak{A}$ spanned by $v_1, \cdots, v_k$. Then $\mathfrak{R}_1 < \mathfrak{R}_2 < \cdots < \mathfrak{R}_r$ and each factor space $\mathfrak{R}_k/\mathfrak{R}_{k-1}$ is one-dimensional. Since any increasing sequence of Ω-subspaces of an Ω-space $\mathfrak{A}$ can be refined into a composition series of $\mathfrak{A}$, there exists a composition series $\mathfrak{R}_1 < \cdots < \mathfrak{R}_r < \mathfrak{R}_{r+1} < \cdots$ of $\mathfrak{A}$. Since $(D_1, \cdots, D_m)$ is nilpotent and orthogonal, we have $D_i \mathfrak{R}_{r+1} \leqq \mathfrak{R}_r$ for all i. Take an element v in $\mathfrak{R}_{r+1}$ but not in $\mathfrak{R}_r$. Then $D_i v \in \mathfrak{R}_r$ for all i, as required.

In the following if $x_1, \cdots, x_k \in \mathfrak{A}$, we shall denote by $\Phi(x_1, \cdots, x_k)$ the subalgebra of $\mathfrak{A}$ generated by $x_1, \cdots, x_k$ over Φ. The ground field Φ is not necessarily algebraically closed.

LEMMA 7.4. *Suppose that* $(D_1, \cdots, D_m)$ *is a nilpotent orthogonal system satisfying* (6.1.3), *and that* $x_1, \cdots, x_r \in \mathfrak{A}$ *are such that the elements* $x_1^{\nu_1} \cdots x_r^{\nu_r}$, *where* $0 \leqq \nu_i < p$, $x_i^0 = 1$, *are linearly independent over* Φ *and such that* $D_i x_k \in \Phi(x_1, \cdots, x_{k-1})$ *for all* i *and* k. *If* $x_{r+1} \notin \Phi(x_1, \cdots, x_r)$ *is such that* $D_i x_{r+1} \in \Phi(x_1, \cdots, x_r)$ *for all* i, *then the elements* $x_1^{\nu_1} \cdots x_{r+1}^{\nu_{r+1}}$, *where* $0 \leqq \nu_i < p$, $x_i^0 = 1$, *are linearly independent over* Φ.

Proof. An element of the form $y = x_1^{\nu_1} \cdots x_r^{\nu_r}$, where $0 \leqq \nu_i < p$, will be called a *monomial*, and the number $w = w(y) = \nu_1 + \nu_2 p + \cdots + \nu_r p^{r-1}$ the *weight* of the monomial y. A monomial is uniquely determined by its weight. A monomial of weight w will be denoted by y_w. If $f = \alpha_0 y_0 + \alpha_1 y_1 + \cdots + \alpha_w y_w$, where $\alpha_i \in \Phi$, $\alpha_w \neq 0$, then the weight $w(f)$ of f is defined by $w(f) = w$. It follows easily from our assumption that $w(D_i f) < w(f)$ for all i if $0 \neq f \in \Phi(x_1, \cdots, x_r)$.

Any linear combination of the elements $x_1^{\nu_1} \cdots x_{r+1}^{\nu_{r+1}}$ can be written in the form $f_0 + f_1 x_{r+1} + \cdots + f_{p-1} x_{r+1}^{p-1}$ with $f_0, \cdots, f_{p-1} \in \Phi(x_1, \cdots, x_r)$. We shall prove by induction with respect to k that if $f_0, \cdots, f_k \in \Phi(x_1, \cdots, x_r)$, $0 \leqq k < p$, then

$$(7.4.1) \qquad f_0 + f_1 x_{r+1} + \cdots + f_k x_{r+1}^k = 0 \text{ implies } f_0 = \cdots = f_k = 0.$$

If $k=0$ then (7.4.1) is clear. Suppose that (7.4.1) holds for all $k<\nu$ but not for $k=\nu$. Let $k=\nu, f_0+f_1x_{r+1}+ \cdots +f_kx_{r+1}^k=0, f_k \neq 0$, and let f_k be of minimal weight with respect to this property. For any i, we have

$$(7.4.2) \qquad (D_if_k)x_{r+1}^k + ((kD_ix_{r+1})f_k + D_if_{k-1})x_{r+1}^{k-1} + \cdots = 0.$$

Since $w(D_if_k) < w(f_k)$, we have $D_if_k=0$ for all i. Then (6.1.3) yields $f_k \in \Phi$. Since $f_k \neq 0$, we may assume $f_k=1$. Then (7.4.2) yields $D_i(kx_{r+1}+f_{k-1})=0$ for all i, and hence by (6.1.3) $kx_{r+1}+f_{k-1} \in \Phi$. Since $0<k<p$, this contradicts the assumption that $x_{r+1} \notin \Phi(x_1, \cdots, x_r)$. Thus (7.4.1) is proved for all k, completing the proof of the lemma.

An algebra $\mathfrak{L}$ over Φ is called *normal simple* if $\mathfrak{L}_{\mathrm{K}}$ is simple for any extension K of Φ. L is normal simple if $\mathfrak{L}_{\mathrm{K}}$ is simple for any algebraically closed extension K of Φ. It is known [4] that the generalized Witt algebras are normal simple if $p>2$ or if $p=2$, $m>1$.

THEOREM 7.5. *Suppose that $p>2$ or that $p=2$, $m>1$. If $(D_1, \cdots, D_m)$ is a nilpotent orthogonal system then $\mathfrak{L}=\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple if and only if the algebra $\mathfrak{K}$ of constants of $\mathfrak{L}$ is a field, while $\mathfrak{L}$ is normal simple if and only if $\mathfrak{K}=\Phi$.*

We need a general remark. Let $\mathfrak{L}$ be an algebra over Φ, and Φ' a subfield of Φ. Since $\mathfrak{L}$ is a vector space over Φ, $\mathfrak{L}$ can be regarded as a vector space $\mathfrak{L}'$ over Φ'. The multiplication xy in $\mathfrak{L}$ is bilinear as a multiplication in $\mathfrak{L}'$. Therefore $\mathfrak{L}'$ is an algebra over Φ', although not necessarily finite dimensional. If $\{u_i\}$ is a basis of $\mathfrak{L}$ over Φ, and if $\{a_j\}$ is a basis of Φ over Φ', then the set $\{a_ju_i\}$ is a basis of $\mathfrak{L}'$ over Φ'. We refer the algebra $\mathfrak{L}'$ as "$\mathfrak{L}$ regarded as an algebra over Φ'." Lemma 7.6 below is probably well known, and in any event the proof may be supplied readily by the reader.

LEMMA 7.6. *$\mathfrak{L}'$ is simple if and only if $\mathfrak{L}$ is simple.*

LEMMA 7.7. *If Φ has a finite degree >1 over Φ', then $\mathfrak{L}'$ is not normal simple.*

Proof. Since Φ is algebraic over Φ', there exists an extension K of Φ' such that Φ_{K} has a zero divisor a. The set $\mathfrak{J}$ of all elements of the form af, where $f \in \mathfrak{K}'_{\mathrm{K}}$ is an ideal of $\mathfrak{L}'_{\mathrm{K}}$ since $(af)g=a(fg)$ for all $f, g \in \mathfrak{L}'_{\mathrm{K}}$. $\mathfrak{J}$ is different from zero, since $a \neq 0$. We shall show that $\mathfrak{J} \neq \mathfrak{L}'_{\mathrm{K}}$. The set of all $x \in \Phi_{\mathrm{K}}$ such that $ax=0$ is a subalgebra of Φ_{K} of dimension $\geqq 1$, so let $a_1, \cdots, a_r$ be a basis of this subalgebra over K. Take $a_{r+1}, \cdots, a_s \in \Phi_{\mathrm{K}}$ such that $a_1, \cdots, a_s$ is a basis of Φ_{K} over K. Since $a \neq 0$, we have $r<s$. Let $u_1, \cdots, u_n$ be a basis of $\mathfrak{L}$ over Φ. Then a_ju_i, $j=1, \cdots, s$, $i=1, \cdots, n$, form a basis of $\mathfrak{L}'_{\mathrm{K}}$ over K. Then

$\{aa_ju_i\}$ is a system of generators of $\mathfrak{J}$ over K, and $aa_1 = \cdots = aa_r = 0$, so that $\mathfrak{J} \neq \mathfrak{L}'_K$. Therefore $\mathfrak{L}'_K$ is not simple, and hence $\mathfrak{L}'$ is not normal simple.

Consider the algebra $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ whose algebra $\mathfrak{K}$ of constants is a field. Since $\mathfrak{K}$ is a subfield of the algebra $\mathfrak{A}$, we may consider $\mathfrak{A}$ as an algebra $\overline{\mathfrak{A}}$ over $\mathfrak{K}$. Since $D_ic = 0$ for all $c \in \mathfrak{K}$, D_i defines a derivation $\overline{D}_i$ of $\overline{\mathfrak{A}}$. It is easily seen that $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is the algebra $\mathfrak{L}(\overline{\mathfrak{A}}; \overline{D}_1, \cdots, \overline{D}_m)$ regarded as an algebra over Φ. Therefore by Lemma 7.6 $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple if and only if $\mathfrak{L}(\overline{\mathfrak{A}}; \overline{D}_1, \cdots, \overline{D}_m)$ is simple, provided that $\mathfrak{K}$ is a field. Note that (1.0.1) and (1.0.2) remain valid for the derivations $\overline{D}_1, \cdots, \overline{D}_m$.

LEMMA 7.8. *Let $\mathfrak{K}$ be the algebra of constants of $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, and* K *an extension of Φ. Then the algebra of constants of $\mathfrak{L}(\mathfrak{A}_K; D_1, \cdots, D_m)$ is $\mathfrak{K}_K$.*

Proof. Let $u_1, \cdots, u_r$ be a basis of $\mathfrak{K}$, and $u_1, \cdots, u_r, \cdots, u_n$ a basis of $\mathfrak{A}$. Suppose $f = \sum \alpha_i u_i$, where $\alpha_i \in$ K, belongs to the algebra of constants of $\mathfrak{L}(\mathfrak{A}_K; D_1, \cdots, D_m)$. We shall show that $\alpha_{r+1} = \cdots = \alpha_n = 0$. For any i, we have $\alpha_{r+1}D_iu_{r+1} + \cdots + \alpha_nD_iu_n = 0$. If $\alpha_{r+1}, \cdots, \alpha_n$ were not all zero, then there would exist $\beta_{r+1}, \cdots, \beta_n \in \Phi$, not all zero, such that $\beta_{r+1}D_iu_{r+1} + \cdots + \beta_nD_iu_n = 0$ for all i, since $D_iu_j \in \mathfrak{A}$. Then we have $\beta_{r+1}u_{r+1} + \cdots + \beta_nu_n \in \mathfrak{K}$, a contradiction. Thus $\alpha_{r+1} = \cdots = \alpha_n = 0$. Therefore the algebra of constants for $\mathfrak{L}(\mathfrak{A}_K; D_1, \cdots, D_m)$ is $\mathfrak{K}_K$.

Proof of 7.5. Suppose that $\mathfrak{L}$ is simple. Then, by Lemma 3.2, $\mathfrak{K}$ is a field. Suppose that $\mathfrak{L}$ is normal simple. Let K be an algebraically closed extension of Φ. By Lemma 7.8 the algebra of constants of $\mathfrak{L}_K$ is $\mathfrak{K}_K$. Since $\mathfrak{K}_K$ is a field, $\mathfrak{K} = \Phi$.

Conversely suppose that $\mathfrak{K}$ is a field. First consider the case $\mathfrak{K} = \Phi$, and let K be an algebraically closed extension of Φ. Then by Lemma 7.8 the algebra of constants of $\mathfrak{L}_K$ is K. Since K is algebraically closed, and since $(D_1, \cdots, D_m)$ is nilpotent and orthogonal, by Theorem 6.10, $\mathfrak{L}_K$ is a generalized Witt algebra. Hence $\mathfrak{L}_K$ is simple. Therefore $\mathfrak{L}$ is normal simple. Since the algebra of constants of $\mathfrak{L}(\overline{\mathfrak{A}}; \overline{D}_1, \cdots, \overline{D}_m)$ is always $\mathfrak{K}$, $\mathfrak{L}(\overline{\mathfrak{A}}; \overline{D}_1, \cdots, \overline{D}_m)$ is normal simple, and hence $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple.

COROLLARY 7.9. *The derivation algebra of the group algebra $\mathfrak{A}$ over Φ of an abelian group $\mathfrak{G}$ whose order is divisible by p is simple if and only if $\mathfrak{G}$ is an elementary abelian group, provided that the order of $\mathfrak{G}$ is greater than* 2.

Proof. Suppose that $\mathfrak{G}$ is an elementary p-group with independent generators $x_1, \cdots, x_n$. Then $\mathfrak{A} = \Phi(x_1, \cdots, x_n)$ and it is easily seen [2, p. 217] that $\mathfrak{D}(\mathfrak{A}) = \mathfrak{L}(\mathfrak{A}; \partial/\partial x_1, \cdots, \partial/\partial x_n)$. Let $\mathfrak{K}$ be the algebra of constants for $\mathfrak{L}$, and let $f \in \mathfrak{K}$. Then $\partial f/\partial x_i = 0$ for all i clearly implies that $f \in \Phi$. Hence $\mathfrak{K} = \Phi$. Since $(\partial/\partial x_1, \cdots, \partial/\partial x_n)$ is a nilpotent orthogonal system, the simplicity of $\mathfrak{D}(\mathfrak{A})$ follows from Theorem 7.5.

Suppose now that $\mathfrak{G}$ is not an elementary p-group. Choose an element $x \in \mathfrak{G}$ as follows: if $\mathfrak{G}$ contains an element $y \neq 1$ of order relatively prime to p, then we set $x=y$; otherwise, choose an element y of order p^r, $r>1$, in $\mathfrak{G}$ and set $x=y^p$. In the latter case we see easily that $Dx=0$ for all $D\in\mathfrak{D}(\mathfrak{A})$. In the former case, $y^q=1$, $(p, q)=1$, and hence $qy^{q-1}Dy=0$. Therefore we have also $Dx=0$ for all $D\in\mathfrak{D}(\mathfrak{A})$. The element $x-1\neq 0$ is a zero divisor belonging to the algebra of constants for $\mathfrak{D}(\mathfrak{A})$, and the set $\mathfrak{J}=\{(x-1)D \mid D\in\mathfrak{D}(\mathfrak{A})\}$ forms an ideal of $\mathfrak{D}(\mathfrak{A})$. In order to show that $\mathfrak{J}$ is a nonzero proper ideal, we decompose $\mathfrak{G}$ into a direct product of a group $\mathfrak{G}_1$ and a cyclic p-group $\mathfrak{G}_2\neq 1$ generated by an element z. Define a linear transformation E of $\mathfrak{A}$ by the rule: $E(g_1z^t)=tg_1z^{t-1}$, where $g_1\in\mathfrak{G}_1$. Then it is easily seen that E is a derivation of $\mathfrak{A}$ such that $Ez=1$. We have $0\neq(x-1)E\in\mathfrak{J}$, since $(x-1)Ez=x-1\neq 0$. Thus $\mathfrak{J}\neq 0$ is proved. Suppose $E\in\mathfrak{J}$; $E=(x-1)D$ with $D\in\mathfrak{D}(\mathfrak{A})$. Then we have $1=(x-1)(Dz)$, a contradiction, since $x-1$ is a zero divisor. Thus $\mathfrak{J}\neq\mathfrak{D}(\mathfrak{A})$ is also proved. Therefore $\mathfrak{D}(\mathfrak{A})$ is not simple.

COROLLARY 7.10. *Let $\mathfrak{A}=\Phi(x_1, \cdots, x_n)$ be the group algebra of an elementary p-group with independent generators $x_1, \cdots, x_n$. Suppose that $(D_1, \cdots, D_m)$ is an orthogonal system such that*

$$D_i = a_{i1}\frac{\partial}{\partial x_1} + \cdots + a_{in}\frac{\partial}{\partial x_n},$$

where $a_{ik}\in\Phi(x_1, \cdots, x_{k-1})$ for all i and k. Unless $p=2$, $m=1$, $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is normal simple if and only if the following condition is satisfied:

(7.10.1) *For any k, there does not exist $f\in\Phi(x_1, \cdots, x_{k-1})$ such that $a_{ik}=D_if$ for all i.*

Proof. We may assume Φ is algebraically closed. It is easily seen that $(D_1, \cdots, D_m)$ is nilpotent. Therefore, by Theorem 7.5, $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is normal simple if and only if (6.1.3) is satisfied. Since $D_ix_k=a_{ik}$, (7.10.1) follows from (6.1.3). Suppose now that (7.10.1) is satisfied. Let $f\in\Phi(x_1, \cdots, x_r)$. If $r=1$ then (6.1.3) is clear, since $D_ix_1=a_{i1}\in\Phi$ and not all a_{i1} are zero by (7.10.1). We shall proceed by induction with respect to r. Suppose that $r>1$ and that (6.1.3) is true if $f\in\Phi(x_1, \cdots, x_{r-1})$. Suppose now $f=b_0+b_1x_r+\cdots+b_kx_r^k$, where $b_0, \cdots, b_k\in\Phi(x_1, \cdots, x_{r-1})$, $b_k\neq 0$. If $D_if=0$ for all i, then

$$D_if = (D_ib_0 + b_1a_{ir}) + \cdots + (D_ib_{k-1} + kb_ka_{ir})x_r^{k-1} + (D_ib_k)x_r^k = 0. \tag{7.10.2}$$

Therefore $D_ib_k=0$ for all i. Then the induction assumption gives $b_k\in\Phi$. From (7.10.2) we have $D_ib_{k-1}+kb_ka_{ik}=0$ for all i. If $0<k$ we set $h=(kb_k)^{-1}b_{k-1}$. Then we have $h\in\Phi(x_1, \cdots, x_{r-1})$ and $a_{ir}+D_ih=0$ for all i, a contradiction. Therefore $k=0$. Then $f\in\Phi(x_1, \cdots, x_{r-1})$ and the induction assumption gives $f\in\Phi$. Thus (6.1.3) holds for all $f\in\mathfrak{A}$.

Let $\mathfrak{L}=\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ be the algebra given in the above Corollary 7.10, and let $\mathfrak{L}'=\mathfrak{L}(\mathfrak{B}; E_1, \cdots, E_m)$ be an algebra defined by a group algebra

$\mathfrak{B}$ (over Φ) of an elementary p-group with independent generators $y_1, \cdots, y_r$ and by derivations of $\mathfrak{B}$ given by

$$E_i = \alpha_{i1}y_1 \frac{\partial}{\partial y_1} + \cdots + \alpha_{ir}y_r \frac{\partial}{\partial y_r},$$

where $\alpha_{ij} \in \Phi$. Unless $m=1$, $p=2$, the algebra $\mathfrak{L}'$ is normal simple if and only if the following condition is satisfied:

(7.10.2) If integers $k_1, \cdots, k_r$ are such that $\sum_{s=1}^{r} \alpha_{is}k_s = 0$ for all i, then $k_1 \equiv \cdots \equiv k_r \equiv 0 \pmod{p}$.

In case (7.10.2) holds, L' is a generalized Witt algebra. We have $\mathfrak{A}_0(D_1, \cdots, D_m) = \mathfrak{A}_0$ and $\mathfrak{B}_0(E_1, \cdots, E_m) = \Phi$, and hence by the remark following Theorem 6.10 we can construct a "composite" $\mathfrak{L}'' = \mathfrak{L}(\mathfrak{C}; F_1, \cdots, F_m)$ of $\mathfrak{L}$ and $\mathfrak{L}'$. Here $\mathfrak{C}$ becomes the group algebra (over Φ) of an elementary p-group with independent generators $x_1, \cdots, x_n, y_1, \cdots, y_r$, and

$$F_i = a_{i1} \frac{\partial}{\partial x_1} + \cdots + a_{in} \frac{\partial}{\partial x_n} + \alpha_{i1}y_1 \frac{\partial}{\partial y_1} + \cdots + \alpha_{ir}y_r \frac{\partial}{\partial y_r}.$$

Thus, unless $m=1$, $p=2$, the algebra $\mathfrak{L}''$ is normal simple if (7.10.1) and (7.10.2) are satisfied. We may also prove that the conditions (7.10.1) and (7.10.2) are necessary in order that $\mathfrak{L}''$ be simple.

8. **Nilpotent systems (2). The case $m=1$.** If the D-dimension $m=1$, then we can still further sharpen the results obtained in the preceding section. In particular, it will be proved that any generalized Witt algebra of the form $\mathfrak{L}(\mathfrak{A}; D)$ over an algebraically closed field is uniquely determined by its dimension. The results obtained here will be the basis of the argument in the next section.

Consider the group algebra $\mathfrak{A} = \Phi(x_1, \cdots, x_n)$ of an elementary p-group with independent generators $x_1, \cdots, x_n$ and the derivation D of $\mathfrak{A}$ defined by

$$D = \frac{\partial}{\partial x_1} + x_1^{p-1} \frac{\partial}{\partial x_2} + \cdots + x_1^{p-1} \cdots x_{n-1}^{p-1} \frac{\partial}{\partial x_n}. \tag{8.0.1}$$

Then D is nilpotent. Let $y_w = x_1^{\nu_1} \cdots x_n^{\nu_n}$ be a monomial of weight $w = \nu_1 + \nu_2 p + \cdots + \nu_n p^{n-1}$. Then Dy_w is easily seen to be a linear combination of monomials of weight $< w$. Since $x_1^{p-1} \cdots x_k^{p-1}$ is the monmial of maximal weight in $\Phi(x_1, \cdots, x_k)$, there does not exist $f \in \Phi(x_1, \cdots, x_k)$ such that $Df = x_1^{p-1} \cdots x_k^{p-1}$. Therefore from Corollary 7.10 it follows that

$$Df = 0 \text{ implies } f \in \Phi. \tag{8.0.2}$$

Hence if $2 < p$ then the algebra $\mathfrak{L}(\mathfrak{A}; D)$ is normal simple.

REMARK. Jacobson [3, Theorem 4] proved the existence of a derivation D

of $\mathfrak{A}$ satisfying (8.0.2) under the condition that Φ is *infinite*. However, the above arguments show that such a derivation exists for any field Φ.

LEMMA 8.1. *If $f\in\mathfrak{A}$ is of weight $w\geqq 1$ then Df is of weight $w-1$.*

Proof. We may assume that $f=y_w$ is a monomial of weight w. Suppose that Dy_w is of weight $<w-1$. Then $Dy_1, \cdots, Dy_w$ are linear combinations of $y_0, \cdots, y_{w-2}$, and hence there exist $\alpha_1, \cdots, \alpha_w\in\Phi$, which are not all zero, such that $\sum\alpha_i Dy_i=0$. Hence we have $D(\sum\alpha_i y_i)=0$, $\sum\alpha_i y_i\in\Phi$, and $\alpha_1=\cdots=\alpha_w=0$, a contradiction. Therefore Dy_w is of weight $w-1$.

As an immediate consequence of (8.1) we have

LEMMA 8.2. *If $0\leqq w<p^n-1$ then there exists an element $f\in\mathfrak{A}$ such that $Df=y_w$.*

Now we consider an arbitrary algebra $\mathfrak{L}(\mathfrak{A}; D)$ of D-dimension $m=1$, where D is a nilpotent derivation satisfying (8.0.2). We shall assume that Φ is perfect. If $\mathfrak{A}$ is of dimension greater than 1 then we can easily find an element $x\in\mathfrak{A}$ such that $Dx=1$, $x^p=1$. Then $1, x, \cdots, x^{p-1}$ are linearly independent. Suppose we have already found $x_1, \cdots, x_k\in\mathfrak{A}$ satisfying (8.3.1)–(8.3.3) below:

(8.3.1) $\quad x_i^p = 1 \quad$ for all $i = 1, \cdots, k$;

(8.3.2) $\quad$ The elements $x_1^{\nu_1}\cdots x_k^{\nu_k}$, where $0\leqq\nu_i<p$, $x_i^0=1$, are linearly independent over Φ;

(8.3.3) $\quad Dx_1 = 1,\quad Dx_2 = x_1^{p-1}, \cdots, Dx_k = x_1^{p-1}\cdots x_{k-1}^{p-1}.$

If $\mathfrak{A}$ is not spanned by the elements $x_1^{\nu_1}\cdots x_k^{\nu_k}$, then by Lemma 7.3 there exists $v\in\mathfrak{A}$ such that $Dv\in\Phi(x_1, \cdots, x_k)$, while $v\notin\Phi(x_1, \cdots, x_k)$. We set $Dv=\alpha x_1^{p-1}\cdots x_k^{p-1}+g$, where $\alpha\in\Phi$ and where g is a linear combination of monomials of weight $<p^k-1$. By Lemma 8.2 there exists $f\in\Phi(x_1, \cdots, x_k)$ such that $Df=g$. Then $D(v-f)=\alpha x_1^{p-1}\cdots x_k^{p-1}$. Hence $\alpha\neq 0$, otherwise $D(v-f)=0$, $v-f\in\Phi$, and $v\in\Phi(x_1, \cdots, x_k)$. Since Φ is perfect, there exists $\beta\in\Phi$ such that $x_{k+1}=\alpha^{-1}(v-f)+\beta$ satisfies $x_{k+1}^p=1$. Thus we have proved the existence of x_{k+1} satisfying

(8.3.4)
$$Dx_{k+1} = x_1^{p-1}\cdots x_k^{p-1},\qquad x_{k+1}^p = 1,$$
$$x_{k+1}\notin\Phi(x_1, \cdots, x_k).$$

Then by Lemma 7.4 the elements $x_1^{\nu_1}\cdots x_{k+1}^{\nu_{k+1}}$ are linearly independent over Φ. Repeating the above process we obtain $x_1, \cdots, x_n\in\mathfrak{A}$ such that the elements $x_1^{\nu_1}\cdots x_n^{\nu_n}$, where $0\leqq\nu_i<p$, form a basis of $\mathfrak{A}$ and such that (8.3.4) holds for all k. Let $\mathfrak{G}$ be the multiplicative group generated by the elements $x_1, \cdots, x_n$. Then $\mathfrak{A}=\Phi(x_1, \cdots, x_n)$ is the group algebra of $\mathfrak{G}$ over Φ, and D can be written in the form (8.0.1).

By a similar argument we may choose $x_1, \cdots, x_n$ satisfying $x_1^p = \cdots = x_p^n = 0$ instead of $x_1^p = \cdots = x_n^p = 1$. Thus we have proved

THEOREM 8.3. *Suppose that* Φ *is a perfect field. If* $\mathfrak{A}$ *has a nilpotent derivation* D *satisfying* (8.0.2) *then* $\mathfrak{A}$ *is the group algebra of an elementary* p*-group with independent generators* $x_1, \cdots, x_n$ (*or* $1+x_1, \cdots, 1+x_n$) *by which* D *can be written in the form* (8.0.1).

COROLLARY 8.4. *Suppose that* Φ *is algebraically closed. Then any generalized Witt algebra of D-dimension* 1 *is uniquely determined by its dimension and can be written in the form* $\mathfrak{L}(\mathfrak{A}; D)$, *where* $\mathfrak{A}$ *and* D *are the same as in Theorem* 8.3, *that is,* $\mathfrak{A} = \Phi(x_1, \cdots, x_n)$ *is the group algebra of an elementary* p*-group with independent generators* $x_1, \cdots, x_n$ (*or,* $1+x_1, \cdots, 1+x_n$), *and where* D *is given by* (8.0.1). *If* $\mathfrak{A} = \Phi(x_1, \cdots, x_n)$ *then any generalized Witt algebra* $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_n)$ *of D-dimension* n *is isomorphic to the algebra* $\mathfrak{L}(\mathfrak{A}; \partial/\partial x_1, \cdots, \partial/\partial x_n)$.

The proof of the second part of Corollary 8.4 is as follows: It was shown in §2 that any generalized Witt algebra $\mathfrak{L}$ can be defined by an orthogonal system $(D_1, \cdots, D_m)$ which can be written in the form $D_i = \sum_j \alpha_{ij} x_j (\partial/\partial x_j)$, $(i = 1, \cdots, m)$, where $\alpha_{ij} \in \Phi$ and where $x_1, \cdots, x_n$ form a system of independent generators of an elementary (multiplicative) p-group of which $\mathfrak{A}$ is the group algebra over Φ. It was also shown there that the $m \times n$ matrix (α_{ij}) is of rank m. In our present case where $m = n$, (α_{ij}) is a nonsingular square matrix. Therefore $(D_1, \cdots, D_n)$ is equivalent to $(x_1(\partial/\partial x_1), \cdots, x_n(\partial/\partial x_n))$ and hence to $(\partial/\partial x_1, \cdots, \partial/\partial x_n)$. Therefore, $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_n) = \mathfrak{L}(\mathfrak{A}; \partial/\partial x_1, \cdots, \partial/\partial x_n)$, which is uniquely determined by Φ and n up to isomorphisms. (Note that we have started with a generalized Witt algebra. If we had started with an orthogonal system $(D_1, \cdots, D_n)$ satisfying (6.1.2)–(6.1.3) then we could use the main result of §6 in order to identify it as a generalized Witt algebra.)

The proof of the second part can also be derived from the following general theorem of H. Zassenhaus (cf. his forthcoming book on representation theory): Any n linearly independent elements of a vector module $\mathfrak{B}$ of dimension n over a commutative ring $\mathfrak{A}$ with unit element, which is its own quotient ring, form a basis of $\mathfrak{B}$ over $\mathfrak{A}$.

Thus the problem of classification of the generalized Witt algebras is completely solved for the two extreme cases: $m = 1$ and $m = n$. The author has been unable to solve this problem in general.

9. **Principal and normal systems.** Let $\mathfrak{A}$ be the group algebra over the ground field Φ of an elementary p-group $\mathfrak{G}$ of order p^n. A set $\{x_1, \cdots, x_n\}$ of elements in $\mathfrak{A}$ will be called a set of *principal generators* of $\mathfrak{A}$ if $x_i^p = 1$ for all i and if the p^n elements $x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}$, where $0 \leq \nu_i < p$, $x_i^0 = 1$, form a basis of $\mathfrak{A}$ over Φ. (Note that the group $\mathfrak{G}$ does not always coincide with the multiplicative group generated by $x_1, \cdots, x_n$.) Consider now mn elements α_{ij},

($i=1, \cdots, m; j=1, \cdots, n$), in Φ satisfying the conditions (9.0.1)–(9.0.2) below (cf. (2.0.4)–(2.0.5)):

(9.0.1) If $k_1, \cdots, k_n$ are integers such that $\sum_j \alpha_{ij}k_j = 0$ for $i = 1, \cdots, m$, then $k_1 \equiv \cdots \equiv k_n \equiv 0 \pmod{p}$;

(9.0.2) The rank of the $m \times n$ matrix (α_{ij}) is m.

It is easily seen that, for given m and n such that $m \leqq n$, if Φ contains sufficiently many elements then we can always find mn elements $\alpha_{ij} \in \Phi$ satisfying (9.0.1)–(9.0.2) above. Take an arbitrary set $\{x_1, \cdots, x_n\}$ of principal generators of $\mathfrak{A}$ and an arbitrary set of mn elements $\alpha_{ij} \in \Phi$ satisfying (9.0.1)–(9.0.2), and define linear transformations $D_1, \cdots, D_m$ of $\mathfrak{A}$ by the rule:

$$D_i(x_1^{\nu_1} \cdots x_n^{\nu_n}) = (\alpha_{i1}\nu_1 + \cdots + \alpha_{in}\nu_n) x_1^{\nu_1} \cdots x_n^{\nu_n},$$

for $i=1, \cdots, m$. Then it is easily verified that $D_1, \cdots, D_m$ are derivations of $\mathfrak{A}$. We have $D_i \circ D_j = 0$ for all i and j. In order to prove this statement, set

$$(9.0.3) \qquad u_\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}, \qquad \lambda_{i\nu} = \alpha_{i1}\nu_1 + \cdots + \alpha_{in}\nu_n.$$

Then $D_i u_\nu = \lambda_{i\nu} u_\nu$, and we have

$$\begin{aligned}(D_i \circ D_j)u_\nu &= D_i(D_j u_\nu) - D_j(D_i u_\nu) \\ &= \lambda_{i\nu}\lambda_{j\nu}u_\nu - \lambda_{j\nu}\lambda_{i\nu}u_\nu = 0\end{aligned}$$

for all u_ν, and hence $D_i \circ D_j = 0$ is proved. Suppose $\sum f_i D_i = 0$ with $f_i \in \mathfrak{A}$. Then $(\sum f_i D_i)x_j = 0$, and hence $\sum_i f_i \alpha_{ij} = 0$ for all j. Then from (9.0.2) it follows easily that $f_i = 0$ for all i. Thus we have proved that $(D_1, \cdots, D_m)$ is an orthogonal system. Any system obtained in the above manner will be called *principal*. Principal systems were used in §2 to define generalized Witt algebras.

We shall show that any principal system $(D_1, \cdots, D_m)$ satisfies the conditions (6.1.2)–(6.1.3). Suppose $D_i f = 0$ for all i. Set $f = \sum \gamma_\nu u_\nu$ with $\gamma_\nu \in \Phi$. Then $\lambda_{i\nu}\gamma_\nu = 0$ for all i and ν. If $\gamma_\nu \neq 0$, then $\lambda_{i\nu} = 0$ for all i, and hence from (9.0.1) and (9.0.3) it follows that $\nu_1 \equiv \cdots \equiv \nu_n \equiv 0 \pmod{p}$, $u_\nu = 1$. Therefore $f = \gamma_0 u_0 \in \Phi$, proving (6.1.3). Suppose now $D_i f = \lambda_i f$ for all i with $f = \sum \gamma_\nu u_\nu$, λ_i and γ_ν all being in Φ. Then $\gamma_\nu \lambda_{i\nu} = \lambda_i \gamma_\nu$ for all i and ν. If $\gamma_\nu \neq 0$, $\gamma_\mu \neq 0$, then $\lambda_{i\nu} = \lambda_{i\mu} (= \lambda_i)$, and hence $D_i(u_\nu u_\mu^{-1}) = 0$ for all i. Since (6.1.3) holds for the system $(D_1, \cdots, D_m)$, we have $u_\nu u_\mu^{-1} \in \Phi$, which, however, is impossible unless $\nu = \mu$. Therefore $f = \gamma u_\nu$ for some $\gamma \in \Phi$ and u_ν. Since u_ν is a unit in $\mathfrak{A}$, (6.1.2) is also verified.

It is proved in §6, assuming Φ is algebraically closed, that any orthogonal system $(D_1, \cdots, D_m)$ satisfying (6.1.2)–(6.1.3) is equivalent to a principal system and that the system $(D_1, \cdots, D_m)$ is principal if and only if $D_i f \in \Phi$ for all i implies $f \in \Phi$, i.e., $\mathfrak{A}_0(D_1, \cdots, D_m) = \Phi$.

We recall that a derivation D of $\mathfrak{A}$ is called normal if and only if $Df = 0$ implies $f \in \Phi$. A system $(D_1, \cdots, D_m)$ will be called *normal* if some D_i is normal. Two systems $(D_1, \cdots, D_m)$ and $(D_1', \cdots, D_m')$ will be called *scalar-equivalent* if $D_i' = \sum_j \gamma_{ij} D_j$ for all i, where $\gamma_{ij} \in \Phi$ and where the matrix (γ_{ij}) is nonsingular. Any system scalar-equivalent to a principal system is also principal.

LEMMA 9.1. *If Φ is infinite, then for any principal system there exists a normal principal system scalar-equivalent to it.*

Proof. Let the principal system $(D_1, \cdots, D_m)$ be defined by means of $\alpha_{ij} \in \Phi$ satisfying (9.0.1)–(9.0.2), a set $\{x_1, \cdots, x_n\}$ of principal generators, and the relations $D_i x_j = \alpha_{ij} x_j$. Consider the p^n linear forms $\phi(\nu; \xi) = \sum_{ij} \xi_i \alpha_{ij} \nu_j$ in the indeterminates $\xi_1, \cdots, \xi_m$, where $0 \leq \nu_i < p$. By (9.0.1), we have $\phi(\nu; \xi) \neq 0$ if $\nu \neq 0$. Since Φ is infinite there exist $\beta_1, \cdots, \beta_m \in \Phi$ such that $\phi(\nu; \beta) \neq 0$ for all $\nu \neq 0$. We shall show that $D = \sum \beta_i D_i$ is normal. Suppose $Df = 0$, where $f = \sum \gamma_\nu u_\nu$ with $\gamma_\nu \in \Phi$. Since $Du_\nu = \phi(\nu; \beta) u_\nu$, we have $\gamma_\nu \phi(\nu; \beta) = 0$ for all $\nu \neq 0$. Then $\phi(\nu; \beta) \neq 0$ for $\nu \neq 0$ implies $\gamma_\nu = 0$ for all $\nu \neq 0$. Therefore $f \in \Phi$ and hence D is shown to be normal. Since not all β_i are zero, we may assume $\beta_1 \neq 0$ without loss of generality. Set $D_1' = D$, $D_i' = D_i$ for $i > 1$. Then $(D_1', \cdots, D_m')$ is a normal principal system scalar-equivalent to $(D_1, \cdots, D_m)$.

From Lemma 9.1 and the remark following the proof of Theorem 7.1, we obtain the following refinement of Theorem 7.1.

THEOREM 9.2. *If Φ is algebraically closed then any orthogonal system satisfying* (6.1.2) *and* (6.1.3) *is equivalent to a normal nilpotent orthogonal system.*

The characterization of the generalized Witt algebras given in the following theorem contains considerably fewer parameters than that given by Kaplansky.

THEOREM 9.3. *Suppose Φ is algebraically closed. Then any generalized Witt algebra over Φ can be written in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, where $\mathfrak{A} = \Phi(x_1, \cdots, x_n)$ is the group algebra of an elementary p-group with independent generators $x_1, \cdots, x_n$, and where*

$$(9.3.1)\quad D_1 = \frac{\partial}{\partial x_1} + x_1^{p-1} \frac{\partial}{\partial x_2} + \cdots + x_1^{p-1} \cdots x_{n-1}^{p-1} \frac{\partial}{\partial x_n},$$

$$(9.3.2)\quad \begin{aligned} D_i = {} & \alpha_{ii}\left(\frac{\partial}{\partial x_i} + x_i^{p-1} \frac{\partial}{\partial x_{i+1}} + \cdots + x_i^{p-1} \cdots x_{n-1}^{p-1} \frac{\partial}{\partial x_n}\right) \\ & + \alpha_{i,i+1}\left(\frac{\partial}{\partial x_{i+1}} + \cdots + x_{i+1}^{p-1} \cdots x_{n-1}^{p-1} \frac{\partial}{\partial x_n}\right) + \alpha_{in} \frac{\partial}{\partial x_n}, \quad (1 < i) \end{aligned}$$

with $\alpha_{ij} \in \Phi$.

Proof. By Theorem 9.2, a generalized Witt algebra $\mathfrak{L}$ can be written in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$, where $(D_1, \cdots, D_m)$ is a normal nilpotent orthogonal system. We shall assume that D_1 is normal. Then by Theorem 8.3 there exist $x_1, \cdots, x_n \in \mathfrak{A}$ such that $x_1^p = \cdots = x_n^p = 1$, such that the monomials $x_1^{\nu_1} \cdots x_n^{\nu_n}$, $0 \leq \nu < p$, form a basis of $\mathfrak{A}$ over Φ, and such that D_1 takes the form (9.3.1). Suppose that D is an arbitrary derivation of $\mathfrak{A}$ commutative with D_1. From $D_1(Dx_1) = D(D_1x_1) = 0$, we have $Dx_1 = \alpha_1 \in \Phi$. For any $k > 0$, we have

$$\begin{aligned} D_1(Dx_{k+1}) &= D(D_1x_{k+1}) = D\left((D_1x_k)x_k^{p-1}\right) \\ &= (DD_1x_k)x_k^{p-1} - (D_1x_k)(Dx_k)x_k^{p-2} \\ &= D_1((Dx_k)x_k^{p-1}). \end{aligned}$$

Therefore we have $D_1(Dx_{k+1} - (Dx_k)x_k^{p-1}) = 0$, and hence $Dx_{k+1} - (Dx_k)x_k^{p-1} = \alpha_{k+1} \in \Phi$, from which we see easily that

$$\text{(9.3.3)} \qquad D = \alpha_1\left(\frac{\partial}{\partial x_1} + \cdots + x_1^{p-1} \cdots x_{n-1}^{p-1} \frac{\partial}{\partial x_n}\right) + \cdots + \alpha_n \frac{\partial}{\partial x_n}.$$

Since every D_i commutes with D_1, it has the form (9.3.3). Then by taking a suitable scalar-equivalent system we obtain $(D_1, \cdots, D_m)$ of the form (9.3.2).

REMARK. If we take $1+x_1, \cdots, 1+x_n$ as independent generators of the group $\mathfrak{G}$ instead of $x_1, \cdots, x_n$, then the forms (9.3.1)–(9.3.2) can still be preserved, and we have $x_1^p = \cdots = x_n^p = 0$. In this case, it is easily seen that

$$\frac{\partial}{\partial x_i} + x_i^{p-1} \frac{\partial}{\partial x_{i+1}} + \cdots + x_i^{p-1} \cdots x_{n-1}^{p-1} \frac{\partial}{\partial x_n} = (-D_1)^{p^{i-1}}.$$

Therefore, if a generalized Witt algebra $\mathfrak{L}$ contains D^p for every $D \in \mathfrak{L}$ then $\mathfrak{L}$ must be the derivation algebra of the group algebra of an elementary p-group.

10. **The case $\Phi = GF(p)$.** Let $\mathfrak{L}$ be an algebra over a field Φ, and $u_1, \cdots, u_n$ a basis of $\mathfrak{L}$ over Φ. Then $u_iu_j = \sum \alpha_{ijk}u_k$, where $\alpha_{ijk} \in \Phi$. If we can choose a basis $\{u_i\}$ of $\mathfrak{L}$ over Φ such that all the α_{ijk} belong to a subfield Φ' of Φ, then we shall say that the algebra is *definable* over Φ'. In other words, an algebra $\mathfrak{L}$ over Φ is definable over Φ' if and only if there exists an algebra L' over Φ' such that $L'_\Phi = L$.

Corollary 8.4 shows that any generalized Witt algebra of D-dimension $m = 1$ over an algebraically closed field Φ is definable over $GF(p)$, which may naturally be regarded as a subfield of Φ. Whether or not this is true for an arbitrary D-dimension m is not known.

As an application of Theorem 9.3, we shall show that if $\mathfrak{A}$ is the group algebra of an elementary p-group of order p^3 then any generalized Witt algebra $\mathfrak{L}$ of D-dimension 2 over an algebraically closed field Φ is definable over $GF(p)$. Let $\{x^iy^jz^k\}$ be a basis of $\mathfrak{A}$, where $x^p = y^p = z^p = 0$. By Theorem 9.3, we may assume that

$$D_1 = \frac{\partial}{\partial x} + x^{p-1}\frac{\partial}{\partial y} + x^{p-1}y^{p-1}\frac{\partial}{\partial z}, \qquad D_2 = \alpha\left(\frac{\partial}{\partial y} + y^{p-1}\frac{\partial}{\partial z}\right) + \beta\frac{\partial}{\partial z}$$

where $\alpha, \beta \in \Phi$. Suppose first that $\alpha \neq 0$. Then we may assume $\alpha = 1$. If, furthermore, $\beta = 0$, then our assertion is proved. Suppose $\beta \neq 0$. Taking a nonzero element $\lambda \in \Phi$, we set $x' = \lambda x$, $y' = \lambda^p y$, $z' = \lambda^{p^2} z$. Then the set $\{x'^i y'^j z'^k\}$ forms a basis of $\mathfrak{A}$, and we have $D_1 = \lambda D_1'$, $D_2 = \lambda^p D_2'$, where

$$D_1' = \frac{\partial}{\partial x'} + x'^{p-1} \frac{\partial}{\partial y'} + x'^{p-1} y'^{p-1} \frac{\partial}{\partial z'},$$

$$D_2' = \frac{\partial}{\partial y'} + y'^{p-1} \frac{\partial}{\partial z'} + \lambda^{p^2 - p} \beta \frac{\partial}{\partial z'} \cdot$$

Therefore if we determine λ by the equation $\lambda^{p^2-p}\beta = 1$, then we see that $\mathfrak{L}$ is definable over $GF(p)$. If $\alpha = 0$ then we may take $\beta = 1$, and hence our assertion is also clear.

At the end of §2, we have remarked that the only algebra which can be constructed by Kaplansky's method for the case where D-dimension $m = 1$ and $\Phi = GF(p)$ is the original Witt algebra (of D-dimension p). Consider now the algebra $\mathfrak{L} = \mathfrak{L}(\mathfrak{A}; D)$, where $\mathfrak{A}$ is the group algebra over $GF(p)$, $p > 2$, of an elementary p-group with independent generators $x_1, \cdots, x_n$, $(n > 1)$, and where

$$D = \frac{\partial}{\partial x_1} + x_1^{p-1} \frac{\partial}{\partial x_2} + \cdots + x_1^{p-1} \cdots x_{n-1}^{p-1} \frac{\partial}{\partial x_n} \cdot$$

This algebra $\mathfrak{L}$ is defined over $GF(p)$ and normal simple. Although $\mathfrak{L}_{GF(p^n)}$ can be obtained by Kaplansky's method of construction, $\mathfrak{L} = \mathfrak{L}_{GF(p)}$ itself cannot be obtained by that method. For, if it were isomorphic to some other generalized Witt algebra $\mathfrak{L}'$ over $GF(p)$ then the coincidence of the D-dimensions of $\mathfrak{L}$ and $\mathfrak{L}'$ would imply that $\mathfrak{L}'$ would have D-dimension 1 (see the last theorem of this paper). Then from the above remark it follows that $\mathfrak{L}'$ is the original Witt algebra over $GF(p)$, which is a contradiction, since $\mathfrak{L}$ is of dimension $p^n > p$.

It may be shown similarly that any normal simple algebra over $GF(p)$ of the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ cannot be obtained directly by Kaplansky's construction if $m < n$. Thus we may say safely that some new *finite* simple Lie algebras can be obtained in the form $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$.

REMARK. If we construct a generalized Witt algebra $\mathfrak{L}$ over Φ and regard it as an algebra over $GF(p)$, as is done in §7, then we can obtain simple algebras over $GF(p)$. However, Lemma 7.7 shows that such algebras are not normal simple.

11. **Nonsimple algebras.** Let L be a Lie algebra over Φ with the multiplication $\circ$. For any two ideals $\mathfrak{J}_1$ and $\mathfrak{J}_2$ of $\mathfrak{L}$ we shall denote by $\mathfrak{J}_1 \circ \mathfrak{J}_2$ the ideal of $\mathfrak{L}$ generated by all $x_1 \circ x_2$, where $x_i \in \mathfrak{J}_i$. Let $\mathfrak{R}$ be a *commutative associative* algebra over Φ, and denote by $\Lambda(\mathfrak{R})$, and $\Lambda(\mathfrak{L})$ the lattices (defined by inclusion) of all ideals of $\mathfrak{R}$ and $\mathfrak{L}$ respectively. If there exists a lattice iso-

morphism σ: $\Lambda(\mathfrak{K})\rightarrow\Lambda(\mathfrak{L})$ such that $(\mathfrak{D}_1\mathfrak{D}_2)^\sigma=\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$ holds for any two ideals $\mathfrak{D}_1, \mathfrak{D}_2\in\Lambda(\mathfrak{K})$, then we shall say that $\mathfrak{K}$ and $\mathfrak{L}$ have *the same ideal theory*. In this case, if $\mathfrak{R}$ is the radical of $\mathfrak{K}$ then $\mathfrak{R}^\sigma$ is the radical of $\mathfrak{L}$. Note that any simple Lie algebra $\mathfrak{L}$ over Φ and the field $\mathfrak{K}=\Phi$ have the same ideal theory. In this section we shall construct Lie algebras $\{\mathfrak{L}\}$ for which there exist commutative associative algebras $\{\mathfrak{K}\}$ such that $\mathfrak{L}$ and $\mathfrak{K}$ have the same ideal theory.

Consider a finite dimensional extension Ψ of the ground field Φ and a polynomial $\phi(\lambda)$ of degree n with coefficients in Ψ. Let $\Psi(x)$ be the algebra over Ψ with the basis $1, x, x^2, \cdots, x^{np-1}$, where x^p satisfies the equation $\phi(x^p)=0$, and let $\mathfrak{A}$ be the algebra $\Psi(x)$ regarded as an algebra over Φ. Clearly there exists a derivation D of $\mathfrak{A}$ such that $Dx=1$ and such that $Da=0$ for all $a\in\Psi$. Then the algebra $\mathfrak{L}=\mathfrak{L}(\mathfrak{A}; D)$ is uniquely determined by the polynomial ϕ, provided that Φ and Ψ are fixed, so that $\mathfrak{L}(\mathfrak{A}; D)$ may be denoted by $\mathfrak{L}(\phi)$ without ambiguity. It is easily seen that the algebra $\mathfrak{K}$ of constants of $\mathfrak{L}(\mathfrak{A}; D)$ is generated by x^p over Ψ, and that $\mathfrak{K}\cong\Psi[\lambda]/(\phi(\lambda))$ as algebras over Φ. Hence $\mathfrak{K}$ is a principal ideal ring. Every ideal of $\mathfrak{K}$ can be written as $\mathfrak{D}=\mathfrak{K}a=(a)$, where $a\in\mathfrak{K}$, and it is always possible to choose a monic factor $a(\lambda)$, i.e., a factor whose leading coefficient is 1, of $\phi(\lambda)$ such that $\mathfrak{D}=(a(x^p))$, since $\phi(x^p)\in\mathfrak{D}$. Thus there exists a one-one correspondence between ideals of $\mathfrak{K}$ and monic factors of $\phi(\lambda)$.

THEOREM 11.1. *Suppose that $2<p$. Then the algebra $\mathfrak{L}(\mathfrak{A}; D)$ defined above has no annihilating ideals except the zero ideal. The algebra $\mathfrak{L}(\mathfrak{A}; D)$ and its algebra $\mathfrak{K}$ of constants have the same ideal theory.*

Here by an *annihilating ideal* of a Lie algebra $\mathfrak{L}$ we mean an ideal $\mathfrak{J}$ of $\mathfrak{L}$ such that $\mathfrak{J}_k=0$ for some k, where $\mathfrak{J}_1=\mathfrak{L}\circ\mathfrak{J}$, $\mathfrak{J}_k=\mathfrak{L}\circ\mathfrak{J}_{k-1}$ for $k=2, 3, \cdots$.

Proof of (11.1). We shall prove first that $\mathfrak{K}$ and $\mathfrak{L}$ have the same ideal theory. For any ideal $\mathfrak{D}$ of $\mathfrak{K}$ we define $\mathfrak{D}^\sigma$ to be the set of all elements of the form afD, where $a\in\mathfrak{D}$ and $f\in\mathfrak{A}$. Then $\mathfrak{D}^\sigma$ is an ideal of $\mathfrak{L}$, since $afD\circ gD=a(fDg-gDf)D\in\mathfrak{D}^\sigma$. We shall show that σ is the desired lattice isomorphism between $\Lambda(\mathfrak{K})$ and $\Lambda(\mathfrak{L})$. Let $\mathfrak{J}\neq 0$ be an ideal of $\mathfrak{L}$ and let $a(\lambda)$ have the minimal positive degree among polynomials such that $a(x)D\in\mathfrak{J}$. Then $D\circ a(x)D=(Da(x))D\in\mathfrak{J}$, and the minimality of the degree of $a(\lambda)$ yields $Da(x)=0$, and hence $a=a(x)\in\mathfrak{K}$. Express f as $f=c_0+c_1x+\cdots+c_{p-1}x^{p-1}$, where $c_i\in\mathfrak{K}$. If $0\leqq i<p-1$, then $aD\circ c_ix^{i+1}D=(i+1)ac_ix^iD\in\mathfrak{J}$, and hence $ac_ix^iD\in\mathfrak{J}$ for $i=0, \cdots, p-2$. Since $ac_{p-1}x^{p-2}D\in\mathfrak{J}$ and since

$$(ac_{p-1}x^{p-2}D)\circ(x^2D) = 4ac_{p-1}x^{p-1}D,$$

we have $4ac_{p-1}x^{p-1}D\in\mathfrak{J}$, and hence $ac_{p-1}x^{p-1}D\in\mathfrak{J}$. Thus $afD\in\mathfrak{J}$ for any $f\in\mathfrak{A}$. Now, for any $h(\lambda)\in\Psi[\lambda]$ such that $h(x)D\in\mathfrak{J}$, we set $h(\lambda)=a(\lambda)q(\lambda)+r(\lambda)$, where $q(\lambda)$, $r(\lambda)\in\Psi[\lambda]$ and where $\deg r(\lambda)<\deg a(\lambda)$. Since $h(x)D$, $a(x)q(x)D\in\mathfrak{J}$, we have $r(x)D\in\mathfrak{J}$. Then the minimality of the degree of $a(\lambda)$

yields $r(\lambda)=0$. Thus we have proved that every element in $\mathfrak{J}$ is of the form afD, where $f\in A$. Hence $\mathfrak{D}^\sigma=\mathfrak{J}$ if we denote by $\mathfrak{D}$ the ideal of $\mathfrak{R}$ generated by a. Let $\mathfrak{D}_1$, $\mathfrak{D}_2$ be ideals of $\mathfrak{R}$ such that $\mathfrak{D}_1^\sigma\leqq\mathfrak{D}_2^\sigma$. We shall show that $\mathfrak{D}_1\leqq\mathfrak{D}_2$. Suppose $a_1\in\mathfrak{D}_1$. Then, by the definition of the mapping σ, we have $a_1D\in\mathfrak{D}_1^\sigma$, and hence $a_1\mathfrak{D}\in\mathfrak{D}_2^\sigma$. Therefore there exist $a_2\in\mathfrak{D}_2$ and $f\in\mathfrak{A}$ such that $a_1D=a_2fD$. Hence $a_1=a_2f$. Express f in the form $f=\sum c_ix^i$, where $c_i\in\mathfrak{R}$. Then $a_1=\sum a_2c_ix^i$. Since a_1, a_2, and c_i are polynomials in x^p, we have $a_1=a_2c_0$. Hence $a_1\in\mathfrak{D}_2$ and $\mathfrak{D}_1\leqq\mathfrak{D}_2$ is proved. If $\mathfrak{D}_1^\sigma=\mathfrak{D}_2^\sigma$ then $\mathfrak{D}_1^\sigma\leqq\mathfrak{D}_2^\sigma$ and $\mathfrak{D}_2^\sigma\leqq\mathfrak{D}_1^\sigma$ imply $\mathfrak{D}_1\leqq\mathfrak{D}_2$ and $\mathfrak{D}_2\leqq\mathfrak{D}_1$ respectively. Hence $\mathfrak{D}_1=\mathfrak{D}_2$ and therefore $\sigma:\Lambda(\mathfrak{R})\rightarrow\Lambda(\mathfrak{L})$ is a lattice isomorphism. We shall prove $(\mathfrak{D}_1\mathfrak{D}_2)^\sigma=\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$ for any two ideals $\mathfrak{D}_1$, $\mathfrak{D}_2$ of $\mathfrak{R}$. Take $a_i\in\mathfrak{R}$ such that $\mathfrak{D}_i=(a_i)$, $i=1, 2$. Then $\mathfrak{D}_1^\sigma$ and $(\mathfrak{D}_1\mathfrak{D}_2)^\sigma$ are the sets of all elements of the form a_ifD and a_1a_2fD, where $f\in\mathfrak{A}$, respectively, since $\mathfrak{D}_1\mathfrak{D}_2=(a_1a_2)$. From $a_1f_1D\circ a_2f_2D=a_1a_2(f_1Df_2-f_2Df_1)D$ we have $\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma\leqq(\mathfrak{D}_1\mathfrak{D}_2)^\sigma$. In order to prove $(\mathfrak{D}_1\mathfrak{D}_2)^\sigma\leqq\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$, it is sufficient to prove that $a_1a_2cx^iD\in\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$ for any $c\in\mathfrak{R}$ and $0\leqq i<p$. If $0\leqq i<p-1$, then $a_1D\circ a_2cx^{i+1}D=(i+1)a_1a_2cx^iD\in\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$, and hence $a_1a_2cx^iD\in\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$. Since $a_1xD\circ a_2cx^{p-1}D=-2a_1a_2cx^{p-1}D$, we have $a_1a_2cx^{p-1}D\in\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$. Thus $(\mathfrak{D}_1\mathfrak{D}_2)^\sigma\leqq\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$ is proved. Hence $(\mathfrak{D}_1\mathfrak{D}_2)^\sigma=\mathfrak{D}_1^\sigma\circ\mathfrak{D}_2^\sigma$. Therefore $\mathfrak{R}$ and $\mathfrak{L}$ have the same ideal theory.

In order to prove the first half, let $\mathfrak{J}$ be an ideal of $\mathfrak{L}$. Then there exists an ideal $\mathfrak{D}$ of $\mathfrak{R}$ such that $\mathfrak{J}=\mathfrak{D}^\sigma$. Since $\mathfrak{L}=\mathfrak{R}^\sigma$, we have $\mathfrak{J}\circ\mathfrak{L}=\mathfrak{D}^\sigma\circ\mathfrak{R}^\sigma=(\mathfrak{D}\mathfrak{R})^\sigma=\mathfrak{D}^\sigma=\mathfrak{J}$. Therefore $\mathfrak{J}$ is not annihilating unless $\mathfrak{J}=0$. Thus Theorem 11.1 is completely proved.

LEMMA 11.2. *With the notations as in the proof of* (11.1), *if $\mathfrak{D}$ is an ideal of $\mathfrak{R}$ and if $a(\lambda)$ is a divisor of $\phi(\lambda)$ such that $\mathfrak{D}=(a(x^p))$, then $\mathfrak{L}/\mathfrak{D}^\sigma\cong\mathfrak{L}(a(\lambda))$ as algebras over Φ.*

Proof. We define a mapping π: $\mathfrak{L}(\phi(\lambda))\rightarrow\mathfrak{L}(a(\lambda))$ by $\pi(f(x)D)=f(x)D$. If $f(x)D=g(x)D$ in $\mathfrak{L}(\phi(\lambda))$ then $f(\lambda)\equiv g(\lambda)\pmod{\phi(\lambda)}$, and hence $f(\lambda)\equiv g(\lambda)\pmod{a(\lambda)}$. Therefore $f(x)D=g(x)D$ in $\mathfrak{L}(a(\lambda))$. Thus π is well defined. It is easily seen that π is a homomorphism of the algebra $\mathfrak{L}(\phi)$ onto the algebra $\mathfrak{L}(a)$. Now $\pi(f(x)D)=0$ if and only if $fD\in\mathfrak{D}^\sigma$. Therefore $\mathfrak{L}(\phi)/\mathfrak{D}^\sigma\cong\mathfrak{L}(a)$ as required.

THEOREM 11.3. *If $2<p$ then any semi-simple algebra of the type $\mathfrak{L}(\phi)$ can be decomposed into a direct sum of simple algebras of the same type.*

Proof. By Theorem 11.1, $\mathfrak{L}(\phi)$ is semi-simple if and only if $\mathfrak{R}$ is semi-simple, and therefore, if and only if ϕ can be expressed as a product $\phi=\phi_1\cdots\phi_r$ of distinct irreducible polynomials in $\Psi[\lambda]$. Suppose then that $\mathfrak{L}(\phi)$ is semi-simple and that $\phi=\phi_1\cdots\phi_r$. We set $\psi_i=\phi/\phi_i$, $\mathfrak{D}_i=(\psi_i(x^p))$. Then $\mathfrak{R}$ is decomposed into the direct sum: $\mathfrak{R}=\mathfrak{D}_1+\cdots+\mathfrak{D}_r$. Hence, by Theorem 11.1, we have

$$\mathfrak{L}(\phi)=\mathfrak{D}_1^\sigma+\cdots+\mathfrak{D}_r^\sigma. \tag{11.3.1}$$

From the definition of $\mathfrak{D}_i$ it follows easily that $\mathfrak{D}_2^\sigma + \cdots + \mathfrak{D}_r^\sigma = (\phi_1(x^p))$. Hence by Lemma 11.2 we have $\mathfrak{L}(\phi)/(\mathfrak{D}_2^\sigma + \cdots + \mathfrak{D}_r^\sigma) \cong \mathfrak{L}(\phi_1)$. Then from (11.3.1) we have $\mathfrak{D}_1^\sigma \cong \mathfrak{L}(\phi_1)$, and similarly $\mathfrak{D}_i \cong \mathfrak{L}(\phi_i)$ for all i. Since ϕ_i is irreducible, $\mathfrak{L}(\phi_i)$ is simple.

12. **Automorphisms of** $L(A; D_1, \cdots, D_m)$. By an automorphism of an algebra $\mathfrak{L}$ over Φ we mean a nonsingular linear transformation σ of L such that $(xy)^\sigma = x^\sigma y^\sigma$ for all $x, y \in \mathfrak{L}$. Because of the linearity, any automorphism is completely determined by its effect on a basis of $\mathfrak{L}$ over Φ. The automorphism group of the Witt algebra was determined by Ho-Jui Chang [1], and that of the derivation algebra of the group algebra of an elementary p-group by Jacobson [3]. In this section first we discuss certain relationships between automorphisms of $\mathfrak{A}$ and $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$.

Let σ be an automorphism of $\mathfrak{A}$ and D a derivation of $\mathfrak{A}$. The mapping D^σ which is defined by $D^\sigma f^\sigma = (Df)^\sigma$ is easily seen to be a derivation of $\mathfrak{A}$. For two derivations D_1, D_2 of $\mathfrak{A}$ we have $(D_1+D_2)^\sigma = D_1^\sigma + D_2^\sigma$, $(D_1 \circ D_2)^\sigma = D_1^\sigma \circ D_2^\sigma$, and $(fD)^\sigma = f^\sigma D^\sigma$ for any $f \in \mathfrak{A}$. Let $\mathfrak{L}$ be a subalgebra of the derivation algebra of $\mathfrak{A}$. An automorphism σ of $\mathfrak{A}$ will be called *admissible* to $\mathfrak{L}$ if $D^\sigma \in \mathfrak{L}$ for any $D \in \mathfrak{L}$. If σ is admissible to $\mathfrak{L}$ then the mapping $D \to D^\sigma$ is an automorphism of $\mathfrak{L}$, which will be said to be *induced* by σ.

If an automorphism σ of $\mathfrak{A}$ is admissible to $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ then from

$$(f_1D_1 + \cdots + f_mD_m)^\sigma = f_1^\sigma D_1^\sigma + \cdots + f_m^\sigma D_m^\sigma$$

it follows that $(D_1^\sigma, \cdots, D_m^\sigma)$ is a system equivalent to $(D_1, \cdots, D_m)$. Thus we have proved the "only if" part of the following

THEOREM 12.1. *Suppose that* $5 \leq p$ *and that* $(D_1, \cdots, D_m)$ *is an orthonormal system. Then every automorphism* σ *of* $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ *is induced by an automorphism of* $\mathfrak{A}$ *if and only if* $(D_1^\sigma, \cdots, D_m^\sigma)$ *is a system equivalent to* $(D_1, \cdots, D_m)$.

To complete the proof, suppose that σ is an automorphism of $\mathfrak{L}$ such that $(D_1^\sigma, \cdots, D_m^\sigma)$ is equivalent to $(D_1, \cdots, D_m)$. Then we may define linear mappings σ_{ij} of $\mathfrak{A}$ into itself such that

$$(fD_i)^\sigma = \sum_{j=1}^{m} f^{\sigma_{ij}} D_j^\sigma \tag{12.1.1}$$

for all $f \in \mathfrak{A}$ and $i = 1, \cdots, m$. Setting $f = 1$ in (12.1.1) yields

$$1^{\sigma_{ij}} = \delta_{ij} \text{ (Kronecker delta).} \tag{12.1.2}$$

From $(fD_i)^\sigma \circ (gD_j)^\sigma = (fD_i \circ gD_j)^\sigma = (f(D_ig)D_j)^\sigma - (g(D_jf)D_i)^\sigma$ and (12.1.1) we have

$$(fD_i)^\sigma \circ (gD_j)^\sigma = \sum_k [(fD_ig)^{\sigma_{jk}} - (gD_jf)^{\sigma_{ik}}] D_k^\sigma.$$

On the other hand, from $D_i^\sigma \circ D_j^\sigma = 0$ and (12.1.1) we have

$$(fD_i)^\sigma \circ (gD_j)^\sigma = \sum_{s,k} [f^{\sigma is} D_s^\sigma g^{\sigma jk} - g^{\sigma js} D_s^\sigma f^{\sigma ik}] D_k^\sigma.$$

Therefore we have

$$(fD_ig)^{\sigma jk} - (gD_jf)^{\sigma ik} = \sum_s [f^{\sigma is} D_s^\sigma g^{\sigma jk} - g^{\sigma js} D_s^\sigma f^{\sigma ik}]. \tag{12.1.3}$$

Setting $f=1$ in (12.1.3) yields $(D_ig)^{\sigma ik} = D_i^\sigma g^\sigma{}_{jk}$. Substituting this in (12.1.3) yields

$$(fD_ig)^{\sigma ik} - (gD_jf)^{\sigma ik} = \sum_s [f^{\sigma is}(D_sg)^{\sigma jk} - g^{\sigma js}(D_sf)^{\sigma ik}]. \tag{12.1.4}$$

We shall use the fact that $(D_1, \cdots, D_m)$ is orthonormal. Let $x_1, \cdots, x_m \in \mathfrak{A}$ be such that $D_ix_j = \delta_{ij}$. Setting $i=j=k$, $g=x_i$ in (12.1.4) yields

$$(x_iD_if)^{\sigma ii} = \sum_r x_i^{\sigma ir}(D_rf)^{\sigma ii}. \tag{12.1.5}$$

Setting $f=x_j$, where $j \neq i$, in (12.1.5) yields

$$0 = x_i^{\sigma ij} \qquad (i \neq j). \tag{12.1.6}$$

Substituting (12.1.6) in (12.1.5), we have

$$(x_iD_if)^{\sigma ii} = x_i^{\sigma ii}(D_if)^{\sigma ii}. \tag{12.1.7}$$

Setting $j=i\neq k$, $g=x_i$ in (12.1.4) and using (12.1.6), we have

$$f^{\sigma ik} - (x_iD_if)^{\sigma ik} = -x_i^{\sigma ii}(D_if)^{\sigma ik}.$$

Setting $f=x_j$, where $j\neq i$, in the above, we have $x_j^{\sigma ik}=0$ for $j\neq i\neq k$. Combining this result with (12.1.6), we conclude that if $i\neq j$ then

$$x_k^{\sigma ij} = 0 \tag{12.1.8}$$

for all k. Setting $k=i\neq j$, $g=x_i$ in (12.1.4) and using (12.1.8), we have

$$f^{\sigma ji} - (x_iD_jf)^{\sigma ii} = -x_i^{\sigma jj}(D_jf)^{\sigma ii} \qquad (j \neq i). \tag{12.1.9}$$

Setting $f=x_j$ in (12.1.9) and using (12.1.8), we have

$$x_i^{\sigma ii} = x_i^{\sigma jj}. \tag{12.1.10}$$

Setting $f=x_ix_j$, where $j\neq i$, in (12.1.7), we obtain

$$(x_ix_j)^{\sigma ii} = x_i^{\sigma ii} x_j^{\sigma ii}. \tag{12.1.11}$$

Setting $f=x_j^2$ in (12.1.9), we have $(x_j^2)^{\sigma_{ji}}-2(x_ix_j)^{\sigma_{ii}}=-2x_i^{\sigma_{ii}}x_j^{\sigma_{ii}}$. Therefore, using (12.1.10) and (12.1.11), we have

$$(12.1.12)\qquad (x_j^2)^{\sigma_{ji}} = 0 \qquad (i\neq j).$$

Setting $i=j=k$, $f=x_i^2$ in (12.1.4) and using (12.1.12), we have

$$(12.1.13)\qquad (x_i^2D_ig)^{\sigma_{ii}} - 2(gx_i)^{\sigma_{ii}} = (x_i^2)^{\sigma_{ii}}(D_ig)^{\sigma_{ii}} - 2g^{\sigma_{ii}}x_i^{\sigma_{ii}}.$$

Setting $f=gx_i$ in (12.1.7), we have

$$(x_i^2D_ig + x_ig)^{\sigma_{ii}} = x_i^{\sigma_{ii}}(x_iD_ig)^{\sigma_{ii}} + x_i^{\sigma_{ii}}g^{\sigma_{ii}}.$$

Therefore, by (12.1.7), we have

$$(12.1.14)\qquad (x_i^2D_ig)^{\sigma_{ii}} + (gx_i)^{\sigma_{ii}} = (x_i^{\sigma_{ii}})^2(D_ig)^{\sigma_{ii}} + g^{\sigma_{ii}}x_i^{\sigma_{ii}}.$$

Setting $f=x_i^2$ in (12.1.7) yields $2(x_i^2)^{\sigma_{ii}}=2(x_i^{\sigma_{ii}})^2$ and hence $(x_i^2)^{\sigma_{ii}}=(x_i^{\sigma_{ii}})^2$, since $p\neq 2$. Then (12.1.13) and (12.1.14) yield $3(gx_i)^{\sigma_{ii}}=3g^{\sigma_{ii}}x_i^{\sigma_{ii}}$ and hence

$$(12.1.15)\qquad (gx_i)^{\sigma_{ii}} = g^{\sigma_{ii}}x_i^{\sigma_{ii}}$$

for all g, since $p\neq 3$. By using (12.1.15) and (12.1.10) in (12.1.9), we have for $i\neq j$ and $f\in\mathfrak{A}$

$$(12.1.16)\qquad f^{\sigma_{ji}} = 0.$$

Setting $k=j\neq i$, $g=x_i$ in (12.1.4) and using (12.1.16) we have $f^{\sigma_{jj}}=f^{\sigma_{ii}}$ for any $f\in\mathfrak{A}$, i and j. Therefore we may set $\sigma_{11}=\cdots=\sigma_{mm}=\sigma$, using the same letter as the given automorphism of $\mathfrak{A}$ over Φ. Setting $i=j=k$ in (12.1.4) yields

$$(12.1.17)\qquad (fD_ig)^\sigma - (gD_if)^\sigma = f^\sigma(D_ig)^\sigma - g^\sigma(D_if)^\sigma.$$

Replacing g in (12.1.17) by x_ig, we have

$$(12.1.18)\quad (fg + x_ifD_ig - x_igD_if)^\sigma = f^\sigma(g + x_iD_ig)^\sigma - (x_ig)^\sigma(D_if)^\sigma.$$

Now, (12.1.15) yields $(x_ig)^\sigma=x_i^\sigma g^\sigma$ for any $g\in\mathfrak{A}$. Therefore, by (12.1.17) and (12.1.18), we have $(fg)^\sigma=f^\sigma g^\sigma$ for all $f, g\in\mathfrak{A}$. We shall show that every element $h\in\mathfrak{A}$ can be written in the form $h=f^\sigma$. From (12.1.1) we have $(fD_i)^\sigma=f^\sigma D_i^\sigma$. Therefore if $(fD_i)^\sigma=hD_i^\sigma$ then $f^\sigma=h$. If $f^\sigma=g^\sigma$ then $(fD_i)^\sigma=(gD_i)^\sigma$ and hence $fD_i=gD_i$, $f=g$. Therefore σ is an automorphism of $\mathfrak{A}$. Let $D\in\mathfrak{L}$, $f\in\mathfrak{A}$. Then $D=\sum f_iD_i$, and $(fD)^\sigma=\sum(ff_iD_i)^\sigma=\sum(ff_i)^\sigma D_i^\sigma=\sum f^\sigma f_i^\sigma D_i^\sigma=f^\sigma D^\sigma$. Therefore the given automorphism σ of $\mathfrak{L}$ is induced by the automorphism σ of $\mathfrak{A}$. Thus Theorem 12.1 is proved.

COROLLARY 12.2. *Suppose that $5\leqq p$ and that $\mathfrak{A}$ is a field over Φ. Then any automorphism of an algebra of the form $\mathfrak{L}(\mathfrak{A}; D)$ is induced by an automorphism of $\mathfrak{A}$. The automorphism group of $\mathfrak{L}(\mathfrak{A}; D)$ is isomorphic to a subgroup of the* *automorphism group of $\mathfrak{K}$ over Φ, where $\mathfrak{K}$ is the algebra of constants of $\mathfrak{L}(\mathfrak{A}; D)$. In particular, if $\mathfrak{K}=\Phi$ then $\mathfrak{L}(\mathfrak{A}; D)$ has no automorphism except the identity.*

Proof. Let σ be an automorphism of $\mathfrak{L}(\mathfrak{A}; D)$. Then $D^\sigma=aD$ with $a\neq 0$. Hence D^σ and D are equivalent. By Theorem 12.1, σ is induced by an automorphism of $\mathfrak{A}$. If $f\in\mathfrak{K}$ then $D^\sigma f^\sigma=(Df)^\sigma=0$. Hence $Df^\sigma=0, f^\sigma\in\mathfrak{K}$. Therefore σ induces an automorphism of $\mathfrak{K}$. If σ induces the identity automorphism on $\mathfrak{K}$, then we have $(f^\sigma)^p=f^p$ for any $f\in\mathfrak{A}$, since $f^p\in K$. Therefore, $(f^\sigma-f)^p=0$, $f^\sigma=f$, and hence $\sigma=1$. Hence the automorphism group of $\mathfrak{L}(\mathfrak{A}; D)$ over Φ is isomorphic to a subgroup of the automorphism group of $\mathfrak{K}$ over Φ, as required.

By the above result, we can construct easily simple Lie algebras which have no automorphism except the identity. For example, let $\Phi=\mathrm{P}(\xi_1, \cdots, \xi_m$, where P is a field of characteristic p and where $\xi_1, \cdots, \xi_m$ are m indeterminates over P, and let $\mathfrak{A}=\Phi(x_1, \cdots, x_m)$, where $x_i^p=\xi_i$. We set

$$D=\frac{\partial}{\partial x_1}+x_1^{p-1}\frac{\partial}{\partial x_2}+\cdots+x_1^{p-1}\cdots x_{m-1}^{p-1}\frac{\partial}{\partial x_m}\cdot$$

Then the algebra $\mathfrak{L}(\mathfrak{A}; D)$ over Φ has the desired property.

In the course of the proof of Theorem 12.1, only the fact that $p\neq 2, 3$ was used. Therefore Theorem 12.1 holds even when $p=0$. Thus any automorphism of the derivation algebra of the function field $\mathfrak{A}$ of one variable over a field of characteristic 0 is induced by an automorphism of $\mathfrak{A}$ over Φ.

Now we shall consider automorphisms of the generalized Witt algebras. In the following, $\mathfrak{A}=\Phi(x_1, \cdots, x_n)$ will denote the group algebra of an elementary p-group with independent generators $x_1, \cdots, x_n$. A polynomial $f(\lambda)\in\Phi[\lambda]$ is called a *p-polynomial* if $f(\lambda)$ is of the form $f(\lambda)=\alpha_0\lambda^{p^k}+\alpha_1\lambda^{p^{k-1}}+\cdots+\alpha_k\lambda$, where $\alpha_i\in\Phi$.

Lemmas 12.3 and 12.4 are proved in [3, p. 110].

LEMMA 12.3. *If $1, u_1, u_2, \cdots, u_{N-1}$, where $N=p^n$, is a basis of $\mathfrak{A}$ over Φ, then there exist n distinct indices, say, $1, 2, \cdots, n$, such that the elements $u_1^{k_1}\cdots u_n^{k_n}$, where $0\leq k_i<p$, $u_i^0=1$, form a basis of $\mathfrak{A}$ over Φ.*

LEMMA 12.4. *The characteristic polynomial of any derivation in $\mathfrak{A}$ is a p-polynomial.*

LEMMA 12.5. *If all the roots of the minimum polynomial of a derivation D in $\mathfrak{A}$ are in Φ and distinct, and if D does not satisfy any nonzero p-polynomial of degree less than p^n, then all the characteristic roots of D are in Φ and distinct.*

Proof. Since all the roots of the minimal polynomial of D are in Φ and distinct, D can be diagonalized, that is, there exists a basis $1, u_1, u_2, \cdots$ of $\mathfrak{A}$ such that $Du_i=\lambda_i u_i$, $\lambda_i\in\Phi$, for all i. By Lemma 12.3 we may assume that the elements $u_1^{k_1}\cdots u_n^{k_n}$ form a basis of $\mathfrak{A}$ over Φ. Since $D(u_1^{k_1}\cdots u_n^{k_n})=(\sum\lambda_i k_i)u_1^{k_1}\cdots u_n^{k_n}$, it is sufficient to show that $\sum\lambda_i k_i=0$ with $0\leq k_i<p$

implies $k_1 = \cdots = k_n = 0$. Suppose that there exists $(k_1, \cdots, k_n) \neq (0, \cdots, 0)$ $0 \leqq k_i < p$, such that $\sum \lambda_i k_i = 0$. Since $k^{p^j} \equiv k \pmod p$ we have $\sum \lambda_i^{p^j} k_i = 0$ for $j = 0, 1, 2, \cdots$. Then the matrix $(\lambda_i^{p^j})$, where $1 \leqq i \leqq n$, $0 \leqq j \leqq n-1$, is singular. Therefore there exists $\alpha_0, \alpha_1, \cdots, \alpha_{n-1} \in \Phi$, not all zero, such that $\sum_j \alpha_j \lambda_i^{p^j} = 0$ for all i. Since $D^{p^j} u_i = \lambda^{p^j} u_i$ we have $(\sum \alpha_j D^{p^j}) u_i = 0$ for all i. Then the derivation $\sum_j \alpha_j D^{p^j} = 0$, since $u_1, \cdots, u_n$ generate $\mathfrak{A}$ over Φ. This contradicts our assumption. Therefore $\sum \lambda_i k_i = 0$ must imply $k_1 \equiv \cdots \equiv k_n \equiv 0 \pmod p$.

The following two lemmas may be verified easily.

Lemma 12.6. *Suppose $5 \leqq p$. If $\alpha_0, \alpha_1, \cdots, \alpha_{p-1} \in \Phi$ are such that $\alpha_i \alpha_j = \alpha_{i+j}$, where $i+j$ is calculated* mod p, *for all $i \neq j$, and if $\alpha_0 \neq 0$, then $\alpha_i = 1$ for all i.*

Lemma 12.7. *Suppose $5 \leqq p$. If $\alpha_0 = 0, \alpha_1, \cdots, \alpha_{p-1} \in \Phi$ are such that $j\alpha_j - i\alpha_i = (j-i)\alpha_{i+j}$, where $i+j$ is calculated* mod p, *for all i and j, then $\alpha_i = i\alpha_1$ for all i.*

Let $\mathfrak{L} = \mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ be a generalized Witt algebra defined by a principal system $(D_1, \cdots, D_m)$. We shall assume that Φ is a perfect infinite field and that $5 \leqq p$. Let σ be an automorphism of $\mathfrak{L}$. By Lemma 9.1 there exist $\gamma_1, \cdots, \gamma_m \in \Phi$ such that $D = \gamma_1 D_1 + \cdots + \gamma_m D_m$ is normal. By Lemma 12.4 the characteristic polynomial $\chi(\lambda)$ of D is a p-polynomial of degree p^n. All the roots of $\chi(\lambda)$ are in Φ and distinct. We shall show that the characteristic polynomial of D^σ is also $\chi(\lambda)$. Since

$$(12.8.1) \qquad D \circ (D \circ \cdots (D \circ X) \cdots)(\text{taken } p^i \text{ times}) = D^{p^i} \circ X$$

for any i and $X \in \mathfrak{L}$, and since no nonzero derivation of $\mathfrak{A}$ commutes with all elements in $\mathfrak{L}$, we see that $\chi(D^\sigma) = 0$ and that D^σ does not satisfy any nonzero p-polynomial of degree less than p^n. $\chi(D^\sigma) = 0$ implies that the minimum polynomial of D^σ has distinct roots contained in Φ. Therefore by Lemma 12.5 all the characteristic roots of D^σ are distinct, and hence the minimal polynomial of D^σ coincides with the characteristic polynomial of D^σ. Therefore $\chi(\lambda)$ is the characteristic polynomial of D^σ. In particular, $D^\sigma f = 0$ implies $f \in \Phi$, that is, D^σ is normal. Since the characteristic roots of D^σ are in Φ and distinct, D^σ can be diagonalized, so that there exists a basis $1, u_1, u_2, \cdots$ of $\mathfrak{A}$ over Φ such that $D^\sigma u_i = \lambda_i u_i$, $\lambda_i \in \Phi$ for all i. By Lemma 12.3 we may assume that the elements $u_1^{k_1} \cdots u_n^{k_n}$ form a basis of $\mathfrak{A}$. Then the p^n elements $\sum \lambda_i k_i$, $0 \leqq k_i < p$, are precisely the (distinct) roots of $\chi(\lambda)$. On the other hand, since λ_i is also a characteristic root of D, there exists a nonzero element $x_i \in \mathfrak{A}$ such that $Dx_i = \lambda_i x_i$. Then $1, x_1, \cdots, x_{N-1}$, where $N = p^n$, form a basis of $\mathfrak{A}$. Since $D_1, \cdots, D_m$ are commutative with D, we have $D(D_j x_i) = \lambda_i D_j x_i$, and hence $D_j x_i = \alpha_{ji} x_i$ with $\alpha_{ji} \in \Phi$ for all i and j. Since $\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ is simple and since $x_i \neq 0$, by Lemma 3.2 we see that x_i is a unit in $\mathfrak{A}$. Therefore we may assume that $x_i^p = 1$ for all i. The elements $x_1^{k_1} \cdots x_n^{k_n}$, $0 \leqq k_i < p$, form a basis of $\mathfrak{A}$ over Φ. Note that the matrix (α_{ij}) is of rank m. Similarly, $D_i^\sigma u_j = \alpha'_{ij} u_j$, $\alpha'_{ij} \in \Phi$, for $i=1, \cdots, m$ and $j=1, \cdots, n$. The matrix (α'_{ij}) is also of rank m.

Consider the subspace $\mathfrak{M}(k_1, \cdots, k_n)$ of $\mathfrak{L}$, which will also be denoted by $\mathfrak{M}_k$, spanned by $X \in \mathfrak{L}$ for which $D \circ X = (\lambda_1 k_1 + \cdots + \lambda_n k_n)X$. It is easily seen that $\mathfrak{M}_k$ consists of elements of the form

$$x_1^{k_1} \cdots x_n^{k_n}(\beta_1 D_1 + \cdots + \beta_m D_m),$$

where $\beta_i \in \Phi$, so that $\mathfrak{M}_k$ is of dimension m. The image $\mathfrak{M}_k^\sigma$ of $\mathfrak{M}_k$ under the isomorphism σ is also of dimension m, and can be characterized as the set of all $Y \in \mathfrak{L}$ for which $D^\sigma \circ Y = (\lambda_1 k_1 + \cdots + \lambda_n k_n) Y$. Therefore $u_1^{k_1} \cdots u_n^{k_n} \cdot (\beta_1 D_1^\sigma + \cdots + \beta_m D_m^\sigma) \in M_k^\sigma$ for any $\beta_i \in \Phi$. If $0 \leqq k_i < p-1$ for all i, then the m elements $u_1^{k_1} \cdots u_n^{k_n} D_i^\sigma$, $i=1, \cdots, m$, are linearly independent. For, if $u_1^{k_1} \cdots u_n^{k_n}(\sum \beta_i D_i^\sigma) = 0$ then $(\sum_i \beta_i \alpha'_{ij}) u_j u_1^{k_1} \cdots u_n^{k_n} = 0$, and hence $\sum_i \beta_i \alpha'_{ij} = 0$ for all j. Since (α'_{ij}) is of rank m, we have $\beta_1 = \cdots = \beta_m = 0$. Therefore if $0 \leqq k_i < p-1$ for all i, then $\mathfrak{M}_k^\sigma$ consists of elements of the form $u_1^{k_1} \cdots u_n^{k_n} \cdot (\beta_1 D_1^\sigma + \cdots + \beta_m D_m^\sigma)$, where $\beta_i \in \Phi$.

We are now ready to prove $u_i^p \neq 0$ for all i. Suppose $u_1^p = 0$. We shall denote $\mathfrak{M}(p-2, 0, \cdots, 0)$, $\mathfrak{M}(p-3, 0, \cdots, 0)$ simply by $\mathfrak{M}(p-2)$, $\mathfrak{M}(p-3)$ respectively. Then $u_1^p = 0$ implies $Y \circ Y' = 0$ for any $Y \in \mathfrak{M}(p-2)^\sigma$ and $Y' \in \mathfrak{M}(p-3)^\sigma$. Hence $X \circ X' = 0$ for any $X \in \mathfrak{M}(p-2)$ and $X' \in \mathfrak{M}(p-3)$. This is a contradiction, since

$$x_1^{p-2} D_1 \circ x_1^{p-3} D_1 = -\lambda_1 x_1^{-5} D_1 \neq 0. \tag{12.8.2}$$

Therefore $u_1^p \neq 0$, and similarly $u_i^p \neq 0$ for all i. Hence we may assume $u_i^p = 1$ for all i.

Now that we have shown that $u_i^p = 1$ for all i, it is easily seen that $\mathfrak{M}_k^\sigma$ consists of all elements of the form $u_1^{k_1} \cdots u_n^{k_n}(\beta_1 D_1^\sigma + \cdots + \beta_m D_n^\sigma)$, where $\beta_i \in \Phi$, without any restriction on k_i. Since $\mathfrak{L}$ is the sum of all $\mathfrak{M}_k$, it is also the sum of all $\mathfrak{M}_k^\sigma$. Therefore every element in $\mathfrak{L}$ can be written in the form $g_1 D_1^\sigma + \cdots + g_m D_m^\sigma$, where $g_i \in \mathfrak{A}$. This shows that $(D_1^\sigma, \cdots, D_m^\sigma)$ is a system equivalent to $(D_1, \cdots, D_m)$. By taking a suitable scalar-equivalent system if necessary, we may assume without loss of generality that $D_i x_j = \delta_{ij} x_j$, where δ_{ij} is the Kronecker delta, for $i, j = 1, \cdots, m$. Note that $m \leqq n$. Similarly, there exists a system $(E_1, \cdots, E_m)$ scalar-equivalent to $(D_1^\sigma, \cdots, D_m^\sigma)$ such that $E_i u_j = \delta_{ij} u_j$ for $i, j = 1, \cdots, m$. We set

$$(x_1^i D_1)^\sigma = u_1^i(\rho_{i1} E_1 + \cdots + \rho_{im} E_m), \tag{12.8.3}$$

where $\rho_{ij} \in \Phi$. We also set $(x_k D_k)^\sigma = u_k F$ for any fixed $k > 1$. Since F commutes with every E_j, $D_1^\sigma \circ (x_k D_k)^\sigma = 0$ yields easily $\rho_{0k} u_k F = 0$, and hence we have

$$\rho_{01} \neq 0, \qquad \rho_{0k} = 0 \qquad (1 < k). \tag{12.8.4}$$

Now (12.8.3) yields easily $\rho_{i1}\rho_{j1} = \rho_{i+j,1}$ for $i \neq j$. Hence by (12.6) and (12.8.4) we have $\rho_{i1}=1$ for all i. Hence (12.8.4) yields $D_1^\sigma=E_1$. Similarly $D_i^\sigma=E_i$ for all i. Again (12.8.3) yields, for any $k>1$, $j\rho_{jk}-i\rho_{ik}=(j-i)\rho_{i+j,k}$. Hence by Lemma 12.7 we have $\rho_{ik}=i\rho_{1k}$ for all i. We shall write ρ_k for ρ_{1k}. Then (12.8.3) can be written as

$$(12.8.5)\qquad (x_1^i D_1)^\sigma = u_1^i(E_1 + i(\rho_2 E_2 + \cdots + \rho_m E_m)).$$

As before, we set $(x_kD_k)^\sigma=u_kF$, $Fu_1=\gamma_k u_1$ for $k>1$. Then $(x_1^iD_1)^\sigma \circ (x_kD_k)^\sigma=0$ and (12.8.5) imply, for $i\not\equiv 0 \pmod p$,

$$(12.8.6)\qquad \rho_k F = \gamma_k(E_1 + i(\rho_2E_2 + \cdots + \rho_mE_m)).$$

By changing i in (12.8.6), we obtain $\rho_kF=\gamma_kE_1$ and $\gamma_k(\rho_2E_2+\cdots+\rho_mE_m)=0$. Therefore if $\rho_k\neq 0$ then $\gamma_k\neq 0$, and hence we have $\rho_2E_2+\cdots+\rho_mE_m=0$, a contradiction. Hence $\rho_k=0$ for all $k>1$. Since $E_1=D_1^\sigma$, (12.8.5) yields $(x_1^iD_1)^\sigma=u_1^iD_1^\sigma$. Similarly we have $(x_j^iD_j)^\sigma=u_j^iD_j^\sigma$ for all i and j. We set $D_j'=x_j^{-1}D_j$. Then $(D_1',\cdots,D_m')$ is an orthonormal system equivalent to $(D_1,\cdots,D_m)$. Since $(D_j')^\sigma=u_j^{-1}D_j^\sigma$, $((D_1')^\sigma,\cdots,(D_m')^\sigma)$ is equivalent to $(D_1^\sigma,\cdots,D_m^\sigma)$ which is equivalent to $(D_1,\cdots,D_m)$. Hence $((D_1')^\sigma,\cdots,D(_m')^\sigma)$ is equivalent to $(D_1',\cdots,D_m')$. By Theorem 12.1, σ is induced by an automorphism σ of $\mathfrak{A}$.

Suppose that $D_i^\sigma=D_i$ for all i. Then $D^\sigma=D$. We set $y=x_1^{k_1}\cdots x_n^{k_n}$. Then we have

$$Dy^\sigma = D^\sigma y^\sigma = (Dy)^\sigma = (\lambda_1k_1+\cdots+\lambda_nk_n)y^\sigma.$$

Hence $y^\sigma=\alpha y$ with $\alpha\in\Phi$. Since $(y^\sigma)^p=(y^p)^\sigma=1$, we have $\alpha^p=1$, $\alpha=1$. Thus $y^\sigma=y$. Since $x_1^{k_1}\cdots x_n^{k_n}$ form a basis of $\mathfrak{A}$, the automorphism σ of $\mathfrak{A}$ is the identity. Thus we have proved the following

THEOREM 12.8. *Suppose that Φ is an infinite perfect field and that $5\leq p$. Then any automorphism σ of a generalized Witt algebra $\mathfrak{L}(\mathfrak{A}; D_1,\cdots,D_m)$ is induced by an automorphism of $\mathfrak{A}$. If $D_i^\sigma=D_i$ for all i, then σ is the identity.*

COROLLARY 12.9. *Let $\mathfrak{L}(\mathfrak{A}; D_1,\cdots,D_m)$ be a generalized Witt algebra, and assume that there exist nonzero elements $x_1,\cdots,x_m\in\mathfrak{A}$ such that $D_ix_j=\delta_{ij}x_j$ for $i, j=1,\cdots,m$. If an automorphism σ of $\mathfrak{A}$ admissible to $\mathfrak{L}$ leaves every x_j invariant, then σ is the identity.*

Proof. Since $(D_1^\sigma,\cdots,D_m^\sigma)$ is equivalent to $(D_1,\cdots,D_m)$, we may set $D_i^\sigma=\sum c_{ij}D_j$. Then $D_i^\sigma x_j^\sigma=\delta_{ij}x_j^\sigma=c_{ij}x_j$. Since x_j is a unit, we have $\delta_{ij}=c_{ij}$, and hence $D_i^\sigma=D_i$ for all i. Therefore by Theorem 12.8 σ is the identity.

What automorphisms of $\mathfrak{A}$ are admissible to $\mathfrak{L}(\mathfrak{A}; D_1,\cdots,D_m)$? In the following we shall consider only the case $m=1$. If Φ is algebraically closed, then any generalized Witt algebras of D-dimension 1 can be written in the form $\mathfrak{L}(\mathfrak{A}; D)$, where $\mathfrak{A}=\Phi(x_1,\cdots,x_n)$ is the group algebra of an elementary p-group with independent generators $1+x_1,\cdots,1+x_n$, and where

$$D = \frac{\partial}{\partial x_1} + x_1^{p-1}\frac{\partial}{\partial x_2} + \cdots + x_1^{p-1} \cdots x_{n-1}^{p-1}\frac{\partial}{\partial x_n}.$$

(Once $\mathfrak{L}$ is given in this form, we may prove, without any condition on Φ, that any automorphism of $\mathfrak{L}$ is induced by an automorphism of $\mathfrak{A}$.) Denote by y_w the monomial $x_1^{\nu_1} \cdots x_n^{\nu_n}$ of weight $w = \nu_1 + \nu_2 p + \cdots + \nu_n p^{n-1}$. If $f = \alpha_w y_w + \alpha_{w+1} y_{w+1} + \cdots$, where $\alpha_w, \alpha_{w+1}, \cdots, \in \Phi$, $\alpha_w \neq 0$, then we define the *weight* of f to be w. Lemmas 12.10 and 12.11, below, are easily verified.

LEMMA 12.10. *If $f \in \mathfrak{A}$ is of weight $w > 0$, then Df is of weight $w - 1$.*

LEMMA 12.11. *Let $\mathfrak{N}$ be the radical of $\mathfrak{A}$. If $f \in \mathfrak{N}^2$ then $w(f)$ is not a power of p.*

LEMMA 12.12. *Let $\mathfrak{N}$ be the radical of $\mathfrak{A}$, σ an automorphism of $\mathfrak{A}$ admissible to $\mathfrak{L}$, and let*

$$x_i^\sigma = \alpha_{i1}x_1 + \cdots + \alpha_{in}x_n \pmod{\mathfrak{N}^2} \tag{12.12.1}$$

for $i = 1, \cdots, n$, where $\alpha_{ij} \in \Phi$. Then $\alpha_{ij} = 0$ for $j < i$.

Proof of 12.12. Let $bD^\sigma = D$, where $b \in \mathfrak{A}$. If $1 < i$ then from (12.12.1) we have

$$(x_1^{p-1} \cdots x_{i-1}^{p-1})^\sigma b = \alpha_{i1} + \alpha_{i2}x_1^{p-1} + \cdots + \alpha_{in}x_1^{p-1} \cdots x_{n-1}^{p-1} \pmod{\mathfrak{N}}.$$

Therefore $\alpha_{i1} = 0$ for $1 < i$. We set

$$x_i^\sigma = \alpha_{i1}x_1 + \cdots + \alpha_{in}x_n + f_i, \qquad f_i \in \mathfrak{N}^2. \tag{12.12.2}$$

Take a fixed $i > 1$ and assume that

$$\alpha_{rs} = 0 \text{ for } s < r, \text{ and that } w(f_r) > p^{r-1} \tag{12.12.3}$$

whenever $r < i$. Suppose that $\alpha_{i1} = \cdots = \alpha_{i,k-1} = 0$, $\alpha_{ik} \neq 0$ for some k such that $1 < k < i$. From (12.12.2) we have

$$\begin{aligned}(x_1^\sigma \cdots x_{i-1}^\sigma)^{p-1} b \\ = \alpha_{ik}x_1^{p-1} \cdots x_{k-1}^{p-1} + \cdots + \alpha_{in}x_1^{p-1} \cdots x_{n-1}^{p-1} + Df_i.\end{aligned} \tag{12.12.4}$$

From (12.12.3) it follows easily that $w((x_1^\sigma \cdots x_{i-1}^\sigma)^{p-1} b) \geq p^{i-1} - 1 > p^{k-1} - 1$. Therefore (12.12.4) yields $w(Df_i) = p^{k-1} - 1$. Then from Lemma 12.10 we have $w(f_i) = p^{k-1}$ which is a contradiction by Lemma 12.11. Hence $\alpha_{ij} = 0$ for $j < i$. Then (12.12.4) yields $w(Df_i) \geq p^{i-1} - 1$. Hence $w(f_i) > p^{i-1}$. Thus (12.12.3) holds for all r, completing the proof.

Denote by $\mathfrak{U}$ the group of all admissible automorphisms of $\mathfrak{A}$. Then the mapping $\sigma \to (\alpha_{ij})$ defined by (12.12.1) is a homomorphism of $\mathfrak{U}$ onto a group of $n \times n$ matrices, which is solvable by Lemma 12.12. Let $\mathfrak{U}'$ be the kernel of the homomorphism. The automorphism group of $\mathfrak{A}$ over Φ is essentially the same as that of its radical $\mathfrak{N}$, since $\mathfrak{A}/\mathfrak{N}\cong\Phi$. Therefore $\mathfrak{U}'$ can be regarded as a subgroup of the group $\mathfrak{B}$ of all automorphisms of $\mathfrak{N}$ which induce the identity on $\mathfrak{N}/\mathfrak{N}^2$. Since $\mathfrak{N}$ is nilpotent, $\mathfrak{B}$ is solvable (see [3, p. 117]). Hence $\mathfrak{U}'$ is solvable. Therefore $\mathfrak{U}$ is also solvable. Thus we have proved the following

THEOREM 12.13. *Suppose* $5\leqq p$. *The automorphism group of the algebra* $\mathfrak{L}(\mathfrak{A}; D)$ *given in Corollary* 8.4 *is solvable.*

Finally we shall prove the following

THEOREM 12.14. *If two normal simple algebras* $\mathfrak{L}=\mathfrak{L}(\mathfrak{A}; D_1, \cdots, D_m)$ *and* $\mathfrak{L}'=\mathfrak{L}(\mathfrak{A}'; D_1', \cdots, D_{m'}')$ *over the same ground field* Φ *are isomorphic then their D-dimensions coincide*: $m=m'$.

Proof. Since $\mathfrak{L}$ and $\mathfrak{L}'$ are normal simple, we may assume without loss of generality that Φ is algebraically closed, and that $\mathfrak{L}$ and $\mathfrak{L}'$ are generalized Witt algebras. Let p^n, $p^{n'}$ be the dimensions of $\mathfrak{L}$, $\mathfrak{L}'$ respectively, so that $mp^n=m'p^{n'}$. Suppose $m<m'$, and hence $n'<n$. By Theorem 9.1 there exists $D\in\mathfrak{L}$ whose characteristic roots are distinct. Let D' be the element corresponding to D, $\chi'(\lambda)$ the characteristic polynomial of D'. $\chi'(\lambda)$ is a p-polynomial by Lemma 12.4, and of degree $p^{n'}$. From $\chi'(D')=0$ and (12.8.1) it follows easily that $\chi'(D)=0$, since no nonzero derivation of $\mathfrak{A}$ commutes with all elements in $\mathfrak{L}$. This is a contradiction, since D does not satisfy any nonzero polynomial of degree less than p^n. Therefore $m=m'$ must hold.

REFERENCES

1. Ho-Jui Chang, *Ueber Wittsche Lie-Ringe*, Abh. Math. Sem. Hansischen Univ. vol. 14 (1941) pp. 151–184.

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

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

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

5. H. Zassenhaus, *Ueber Lie'sche Ringe mit Primzahlcharacteristik*, Abh. Math. Sem. Hansischen Univ. vol. 13 (1940) pp. 1–100.

UNIVERSITY OF BRITISH COLUMBIA,
VANCOUVER, B. C.