MODULAR LIE ALGEBRAS. I

BY

CHARLES W. CURTIS(1)

1. **Introduction.** A Lie algebra $\mathfrak{l}$ over a field E of characteristic $p>0$ is called separable if its Killing form $B(X, Y) = \text{trace}(\text{ad } X \text{ ad } Y)$ is nondegenerate. Separable algebras over algebraically closed fields enjoy many of the properties of complex semi-simple algebras; in particular the Cartan subalgebras are commutative, and they possess root systems which determine the algebras up to isomorphism. These results, and a complete classification of the simple separable algebras over an algebraically closed field of characteristic $p>7$, have been obtained recently by Seligman [12](2).

In this paper we develop the basic properties of modular Lie algebras; these are separable algebras which are obtained from semi-simple algebras of characteristic zero in the following way. Let $\mathfrak{L}$ be a semi-simple algebra over an algebraically closed field C of characteristic zero. Then $\mathfrak{L}$ possesses a Cartan subalgebra $\mathfrak{H}$, and a Cartan basis (X_i) relative to $\mathfrak{H}$, such that the constants of structure determined by the basis (X_i) belong to an algebraic number field K. A finite set of exceptional prime ideals in K, which is independent of the choice of the Cartan subalgebra $\mathfrak{H}$ and the basis (X_i), is then defined; this set includes the prime ideals which divide the rational primes 2 and 3, and the primes which divide the determinant of the Killing matrix $(B(X_i, X_j))$. Now let $\mathfrak{p}$ be a fixed nonexceptional prime, and let $\mathfrak{o}$ be the ring of $\mathfrak{p}$-integers in K. Then $\Sigma = \sum \mathfrak{o} X_i$ forms a Lie subring of $\mathfrak{L}$, and $\mathfrak{l} = \Sigma/\mathfrak{p}\Sigma$ is a separable Lie algebra over the residue field $\overline{K} = \mathfrak{o}/\mathfrak{p}$, with the further properties that the natural homomorphism of $\Sigma \rightarrow \mathfrak{l}$ maps $\mathfrak{H}$ onto a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{l}$, and defines a (1-1) mapping of the set of roots of $\mathfrak{L}$ relative to $\mathfrak{H}$ onto the set of roots of $\mathfrak{l}$ relative to $\mathfrak{h}$. We call a Lie algebra $\mathfrak{l}$ defined in this way a *modular Lie algebra*.

As Seligman has observed, a p-power operation can be defined in every separable algebra $\mathfrak{l}$ of characteristic p in such a way that $\mathfrak{l}$ becomes a restricted Lie algebra in the sense of Jacobson [9]. The study of restricted representations of $\mathfrak{l}$, which preserve the p-power operation in addition to the usual properties of a representation, is equivalent to the study of right $\mathfrak{a}$-modules, where $\mathfrak{a}$ is a finite dimensional enveloping algebra of $\mathfrak{l}$ called the u-algebra. The

Presented to the Society, September 1, 1955, under the title *On the structure and representation theory of Lie algebras of characteristic* $p>0$; received by the editors August 31, 1955.

(1) National Research Fellow.

(2) Numbers in brackets refer to the references at the end of the paper.

main results of this paper deal with the theory of $\mathfrak{a}$-modules, where $\mathfrak{a}$ is the u-algebra of a separable modular algebra $\mathfrak{l}$. In §7, it is proved that every irreducible $\mathfrak{a}$-module is absolutely irreducible. The Cartan-Weyl theory of weights of irreducible $\mathfrak{a}$-modules is developed, and in particular it is proved that two irreducible $\mathfrak{a}$-modules $\mathfrak{m}$ and $\mathfrak{m}'$ which possess leading weights λ and λ', respectively, are $\mathfrak{a}$-isomorphic if and only if $\lambda=\lambda'$. Not every irreducible $\mathfrak{a}$-module need possess a priori a leading weight; it is proved in §8, however, that if an irreducible $\mathfrak{a}$-module possesses an extreme weight, then it has a leading weight, and in this case the Weyl group of $\mathfrak{l}$ acts transitively upon the set of extreme weights of $\mathfrak{m}$. In §9 it is proved that every irreducible $\mathfrak{a}$-module which possesses a leading weight is $\mathfrak{a}$-isomorphic to a composition factor of an $\mathfrak{a}$-module obtained by a reduction process from an irreducible representation space of $\mathfrak{L}$.

The author wishes to thank Dr. G. Seligman for his generosity in making available to the author his unpublished manuscript on the classification of separable algebras, and for his helpful comments on an earlier version of this paper.

2. **A preliminary remark on the rank of a Lie algebra.** We begin with some definitions. Let $\mathfrak{L}$ be a Lie algebra over an arbitrary field E, having a basis $X_1, \cdots, X_n$ over E, and let $X^*=\sum \tau_i X_i$ be the general element of $\mathfrak{L}$; then $X^* \in \mathfrak{L}^R$(3) where $R=E(\tau_1, \cdots, \tau_n)$ is the field of rational functions in n variables τ_i. Let

$$f(\lambda; \tau) = \lambda^n + \mu_1(\tau)\lambda^{n-1} + \cdots + \mu_n(\tau) \tag{1}$$

be the characteristic polynomial of the l.t. (linear transformation) ad X^*: $Y\rightarrow[YX^*]$ acting in $\mathfrak{L}^R$. Then the $\mu_i(\tau)$ are homogeneous polynomials in the τ's with coefficients in the ring generated over the subring of E consisting of the rational integral multiples of 1 by the constants of structure c_{ijk} of $\mathfrak{L}$, given by the equations

$$[X_i X_j] = \sum c_{ijk} X_k. \tag{2}$$

There exists a unique integer $l>0$, called the *rank* of $\mathfrak{L}$, such that $\mu_{n-l}(\tau)\neq 0$, and $\mu_{n-l+1}(\tau)= \cdots =\mu_n(\tau)=0$. It is known that the rank of $\mathfrak{L}$ is independent of the choice of the basis $X_1, \cdots, X_n$ of $\mathfrak{L}$. For reference we state the following result, which is an immediate consequence of our definitions.

LEMMA 1. *Let $\mathfrak{L}$ be a Lie algebra over a field E, and let Ω be an extension field of E. Then the rank of $\mathfrak{L}^\Omega$ is equal to the rank of $\mathfrak{L}$.*

A subalgebra $\mathfrak{H}$ of a Lie algebra $\mathfrak{L}$ is called a *Cartan subalgebra* if (1) $\mathfrak{H}$ is nilpotent, and (2) $[\mathfrak{H}, X]\subseteq\mathfrak{H}$ implies $X\in\mathfrak{H}$ for all X in $\mathfrak{L}$.

If the base field is infinite, then Cartan subalgebras are known to exist, and the dimension of a Cartan subalgebra is equal to the rank of $\mathfrak{L}$.

(3) By $\mathfrak{L}^R$ we mean the Lie algebra obtained by extension of the field E to R.

3. **Preliminary results on semi-simple algebras of characteristic zero**(4). Let $\mathfrak{L}$ be a semi-simple Lie algebra over an algebraically closed field C of characteristic zero. We write Q for the prime field in C, and Z for the subring of Q consisting of the multiples of 1; then Q and Z are isomorphic to the field of rational numbers and the ring of rational integers, respectively. Let $\mathfrak{H}$ be a Cartan subalgebra of $\mathfrak{L}$, and let $\alpha, \beta, \cdots$ be the roots(5) of $\mathfrak{L}$ relative to $\mathfrak{H}$. Let $B(X, Y) = \text{trace } (\text{ad } X \text{ ad } Y)$ be the Killing form on $\mathfrak{L}$; then B is nondegenerate on $\mathfrak{L}$, and its restriction to $\mathfrak{H}$ is nondegenerate. For each root α, there exists a unique element H'_α in $\mathfrak{H}$ such that $B(H'_\alpha, H) = \alpha(H)$ for all H in $\mathfrak{H}$. Then $\alpha(H'_\alpha)$ is a nonzero element of Q, and if we put $H_\alpha = 2\alpha(H'_\alpha)^{-1}H'_\alpha$, then $\alpha(H_\alpha) = 2$. Let $l = \dim \mathfrak{H} = \text{rank } \mathfrak{L}$. It is known that there exists a set of l linearly independent roots $\alpha_1, \cdots, \alpha_l$, called a *fundamental system* of roots, such that every root of $\mathfrak{L}$ relative to $\mathfrak{H}$ is an image of one of the α_i, $1 \leqq i \leqq l$, by an element of the group W generated by the Weyl reflections $\Lambda \to \Lambda - \Lambda(H_{\alpha_i})\alpha_i$, $1 \leqq i \leqq l$. Every root α can be expressed in the form $\alpha = \sum_{i=1}^{l} d_i\alpha_i$, where the d_i are elements of Z. If we write $H_{\alpha_i} = H_i$, $1 \leqq i \leqq l$, then $H_1, \cdots, H_l$ form a basis of $\mathfrak{H}$. The linear functions $\sum_1^l q_i\alpha_i$ with coefficients q_i in Q are called rational linear functions on $\mathfrak{H}$, and may be ordered lexicographically with respect to the ordered set $(\alpha_1, \cdots, \alpha_l)$. In particular the roots are linearly ordered in this way, and when we write $\alpha < \beta$, $\alpha < 0$, etc. it is to be understood that "$<$" is the lexicographic order relation. If α is a root and m an integer, then $m\alpha$ is a root if and only if $m = \pm 1$. For any pair of roots α and β, $\alpha(H_\beta) \in Z$.

If the dimension of $\mathfrak{L}$ is n, then there exist $n - l$ distinct roots, and root vectors $E_\alpha, E_\beta, \cdots$ in (1-1) correspondence with them which can be chosen in such a way that the following relations hold.

$$\mathfrak{L} = \mathfrak{H} + \sum_{\alpha>0} CE_\alpha + \sum_{\alpha>0} CE_{-\alpha} \text{ (direct sum)}; \tag{3}$$

$$[HH'] = 0, \qquad [E_\alpha H] = \alpha(H)E_\alpha, \qquad H, H' \in \mathfrak{H}; \tag{4}$$

$$[E_\alpha E_\beta] = \begin{cases} N_{\alpha\beta}E_{\alpha+\beta} & \text{if } \alpha + \beta \text{ is a root,} \\ 0 & \text{if } \alpha + \beta \text{ is not a root,} \\ H_\beta & \text{if } \alpha = -\beta, \end{cases} \tag{5}$$

where for each pair of roots (α, β), $N_{\alpha\beta}^2 \in Z$; and

$$\begin{aligned} B(E_\alpha, E_\beta) &= 0 \qquad \text{if } \alpha + \beta \neq 0, \\ B(E_{-\alpha}, E_\alpha) &= 2B(H'_\alpha, H'_\alpha)^{-1}, \\ B(E_\alpha, H) &= 0, \qquad H \in \mathfrak{H}. \end{aligned} \tag{6}$$

---

(4) For proofs of these results we refer to Weyl [14]; for the terminology we use and for a discussion of some of these questions see also Gantmacher [5] and Harish-Chandra [7].

(5) We do not call the zero linear function a root.

A basis $X_1, \cdots, X_n$ of $\mathfrak{L}$ is called an *admissible basis* relative to a Cartan subalgebra $\mathfrak{H}$ if $X_1, \cdots, X_m$ are the root vectors E_{α_i} belonging to the positive roots of $\mathfrak{L}$ relative to $\mathfrak{H}$, $X_{m+l+1}, \cdots, X_n$ are the root vectors corresponding to the negative roots, and $(X_{m+1}, \cdots, X_{m+l})=(H_1, \cdots, H_l)$ is the basis of $\mathfrak{H}$ determined by the fundamental system of roots $\alpha_1, \cdots, \alpha_l$, all normalized so that the relations (3), (4), (5), and (6) hold. It is known that if $\mathfrak{H}$ is any Cartan subalgebra of $\mathfrak{L}$, then there exists an admissible basis of $\mathfrak{L}$ relative to $\mathfrak{H}$. We shall write (X_i) for an admissible basis, and call the field K generated by the constants of structure $N_{\alpha\beta}$ in (5) the *coefficient field* determined by the basis. Then K is an algebraic number field, which contains all the constants of structure c_{ijk} determined by the basis (X_i).

4. **Arithmetical preparations.** Let (X_i) be an admissible basis of $\mathfrak{L}$ with coefficient field K. Let $a_{ij}=-\alpha_i(H_j)=-\alpha_i(X_{m+j})$, $1\leqq i, j\leqq l$; then the a_{ij} are rational integers with certain properties, and the matrix (a_{ij}) is called the Weyl matrix of $\mathfrak{L}$ (see [7, p. 29]).

We shall write $\mathfrak{o}_\mathfrak{p}$ for a discrete valuation ring in K, $\mathfrak{p}$ for the corresponding prine ideal, $\overline{K}$ for the residue class field $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}$, and ϕ for the homomorphism (or place) mapping $\mathfrak{o}_\mathfrak{p}$ upon $\overline{K}$.

We note that for any prime ideal $\mathfrak{p}$ in K such that $2\notin\mathfrak{p}$, the elements $B(E_{-\alpha}, E_\alpha)\in\mathfrak{o}_\mathfrak{p}$ for all roots α. This fact is a consequence of (6), and the formula

$$B(H_\alpha', H_\alpha') = \alpha(H_\alpha') = 4\left(\sum_\beta (p_{\beta\alpha} + q_{\beta\alpha})^2\right)^{-1},$$

where the sum is over all roots β, and where $p_{\beta\alpha}$ and $q_{\beta\alpha}$ are the uniquely determined rational integers, $p_{\beta\alpha}\leqq 0\leqq q_{\beta\alpha}$, such that $\beta+k\alpha$ is a root if and only if $p_{\beta\alpha}\leqq k\leqq q_{\beta\alpha}$.

DEFINITION. A non-archimedean prime ideal $\mathfrak{p}$ in K is called *non-exceptional* (relative to the basis (X_i)) if the following conditions are satisfied.

(i) $2\notin\mathfrak{p}$, $3\notin\mathfrak{p}$;

(ii) $\det(a_{ij})\notin\mathfrak{p}$; and

(iii) $B(E_{-\alpha}, E_\alpha)\notin\mathfrak{p}$ for all roots α;

otherwise $\mathfrak{p}$ is called exceptional. Evidently the number of exceptional prime ideals is finite.

Let $\mathfrak{p}$ be a non-archimedean prime ideal in K such that $2\notin\mathfrak{p}$. Let $\Sigma_\mathfrak{p}$ be the set of linear combinations with coefficients in $\mathfrak{o}_\mathfrak{p}$ of the elements H_α, E_α, where α ranges through the set of all roots of $\mathfrak{L}$. Inspection of the table (3)–(5) reveals that $\Sigma_\mathfrak{p}$ is closed under the bracket operation. (The $N_{\alpha\beta}\in\mathfrak{o}_\mathfrak{p}$ because their squares are in Z.)

Next suppose that $2\notin\mathfrak{p}$, and $B(E_{-\alpha}, E_\alpha)\notin\mathfrak{p}$ for all roots α. We prove that the admissible basis (X_i) is an $\mathfrak{o}_\mathfrak{p}$-basis for the ring $\Sigma_\mathfrak{p}$. It is sufficient to prove that for all roots α, H_α is an $\mathfrak{o}_\mathfrak{p}$-linear combination of the H_i, $1\leqq i\leqq l$. Let $\alpha=\sum d_i\alpha_i$, where the $d_i\in Z$, $1\leqq i\leqq l$. Then

$$\begin{aligned} H_\alpha &= 2B(H'_\alpha, H'_\alpha)^{-1}H'_\alpha = B(E_{-\alpha}, E_\alpha)H'_\alpha \\ &= B(E_{-\alpha}, E_\alpha)\left(\sum d_i H'_{\alpha_i}\right) = 2^{-1}B(E_{-\alpha}, E_\alpha)\left(\sum B(H'_{\alpha_i}, H'_{\alpha_i})H_i\right) \\ &= \sum_{i=1}^{l} B(E_{-\alpha}, E_\alpha)B(E_{-\alpha_i}, E_{\alpha_i})^{-1}d_i H_i \end{aligned}$$

where the $B(E_{-\alpha}, E_\alpha)B(E_{-\alpha_i}, E_{\alpha_i})^{-1}d_i \in \mathfrak{o}_\mathfrak{p}$, $1 \leqq i \leqq l$.

Finally, let $\mathfrak{p}$ be a nonexceptional prime ideal in K. We prove that if we set $B_{ij} = B(X_i, X_j)$, $1 \leqq i, j \leqq n$, then the $B_{ij} \in \mathfrak{o}_\mathfrak{p}$, and $\det (B_{ij}) \notin \mathfrak{p}$. Since $\Sigma_\mathfrak{p}$ is closed under the bracket operation, it follows that $\Sigma_\mathfrak{p}$ is mapped into itself by ad X_i, $1 \leqq i \leqq n$. But $B_{ij} = \text{trace}\ (\text{ad}\ X_i\ \text{ad}\ X_j)$, hence the $B_{ij} \in \mathfrak{o}_\mathfrak{p}$. From (6) we see that the matrix (B_{ij}) can be expressed in the form

$$(7) \qquad (B_{ij}) = (B(X_i, X_j)) = \begin{pmatrix} B_0 & & & \\ & B_\alpha & & \\ & & B_\beta & \\ & & & \ddots \end{pmatrix},$$

where $B_0 = (B(X_i, X_j))$, $m+1 \leqq i, j \leqq m+l$, where exactly one block

$$B_\alpha = \begin{pmatrix} 0 & B(E_{-\alpha}, E_\alpha) \\ B(E_{-\alpha}, E_\alpha) & 0 \end{pmatrix}$$

appears for each pair of roots $(\alpha, -\alpha)$, and where the matrix (B_{ij}) has zeros except for the blocks we have listed along the main diagonal. Then we have

$$(8) \qquad \det (B_{ij}) = (\det B_0)\left(\prod_{\alpha>0} \det B_\alpha\right).$$

By (iii) in the definition of an exceptional prime ideal, the second factor on the right does not belong to $\mathfrak{p}$. We have for all i and j, $B(H_i, H_j) = -2a_{ij}B(H'_{\alpha_i}, H'_{\alpha_i})^{-1} = -a_{ij}B(E_{-\alpha_i}, E_{\alpha_i})$ by (6). Therefore

$$\det B_0 = \det (B(H_i, H_j)) = (-1)^l(\det (a_{ij}))\left(\prod_{1\leqq i\leqq l} B(E_{-\alpha_i}, E_{\alpha_i})\right),$$

so that $\det B_0 \neq \mathfrak{p}$. Thus $\det (B_{ij}) \notin \mathfrak{p}$ if $\mathfrak{p}$ is nonexceptional.

We shall discuss the uniqueness of the coefficient fields and of the sets of exceptional prime ideals determined by two admissible bases (X_i) and (X'_i) relative to Cartan subalgebras $\mathfrak{H}$ and $\mathfrak{H}'$, respectively. By a result of Chevalley [4] there exists an automorphism $\sigma = \exp\ (\text{ad}\ Z)$ of the adjoint group of $\mathfrak{L}$ such that $\mathfrak{H}^\sigma = \mathfrak{H}'$. An examination of the table (3)–(6) shows that (X_i^σ) is an admissible basis of $\mathfrak{L}$ relative to $\mathfrak{H}'$. The coefficient field relative to the basis (X_i) is identical with the coefficient field of the basis (X_i^σ). By a result of Weyl [14, p. 372], we have the formula $N_{\alpha\beta}^2 = -(i+1)k$, where $\beta - i\alpha, \cdots, \beta-\alpha, \beta, \beta+\alpha, \cdots, \beta+k\alpha$ is the string of roots of the form $\beta+j\alpha$, $j \in Z$, and consequently the constants $N'_{\alpha\beta}$ and $N_{\alpha\beta}$ determined by the bases (X_i') and (X_i'') of $\mathfrak{L}$ relative to $\mathfrak{H}'$ differ at most by a permutation of the roots. Therefore the coefficient field K is independent of the choice of an admissible basis.

In order to compare the exceptional prime ideals relative to the admissible bases (X_i) and (X_i'), we may assume that the Cartan subalgebras which give rise to these bases are identical. If we let E_α and E_α' be the root vectors in the two bases, then since the elements H_α' are uniquely determined, (6) shows that the primes which divide some $B(E_\alpha, E_{-\alpha})$ are identical with the primes which divide some $B(E_\alpha', E_{-\alpha}')$. We use finally the known result that the determinants of the Weyl matrices relative to two fundamental systems of roots of $\mathfrak{L}$ relative to a Cartan subalgebra $\mathfrak{H}$ differ at most by a unit factor. Therefore the set of exceptional primes is an invariant of the algebra $\mathfrak{L}$.

5. **Modular Lie algebras.** A Lie algebra $\mathfrak{l}$ over a field E of characteristic $p>0$ is called *separal le* if the Killing form $B(x, y)$ of $\mathfrak{l}$ is nondegenerate. It is immediate that if $\mathfrak{l}$ is a separable algebra, then so is $\mathfrak{l}^F$, where F is an extension field of E. In any separable algebra $\mathfrak{l}$, a p-power operation can be defined so that $\mathfrak{l}$ becomes a restricted Lie algebra in the sense of Jacobson [9]. The definition of x^p is based on the fact that $(\text{ad } x)^p$ is a derivation of $\mathfrak{l}$; hence by [16, p. 53], $(\text{ad } x)^p$ is an inner derivation ad y. The element y is uniquely determined because of the separability (see [12]), and hence if we set $y=x^p$, so that $[zy]=[zx^p]=z(\text{ad } x)^p$, $z\in\mathfrak{l}$, $\mathfrak{l}$ becomes a restricted Lie algebra. In the sequel, "separable algebra" means "restricted separable algebra" under this definition of the p-power operation. This paper is devoted to a study of certain separable algebras which are constructed as follows.

Let $\mathfrak{L}$, (X_i), K, $\mathfrak{H}$ be as in §4, and let $\mathfrak{p}$ be a fixed nonexceptional prime, containing the rational prime p. We shall adhere to these notations for the rest of the paper, and we shall write $\mathfrak{o}$ for $\mathfrak{o}_\mathfrak{p}$, $\overline{K}$ for the residue field $\mathfrak{o}/\mathfrak{p}$, Σ for $\Sigma_\mathfrak{p}$, and $\phi:\phi(a)=\bar{a}$ for the homomorphism of $\mathfrak{o}$ onto $\overline{K}$. Then $\Sigma=\sum \mathfrak{o}X_i$ is closed under the bracket operation, and may be regarded as a Lie algebra over the *ring* $\mathfrak{o}$. $\mathfrak{p}\Sigma=\sum\mathfrak{p}X_i$ is an ideal in Σ, and $\Sigma/\mathfrak{p}\Sigma$ is a Lie algebra over $\mathfrak{o}$. Let T be the natural mapping of Σ onto $\Sigma/\mathfrak{p}\Sigma$; we shall write $x=XT$ for $X\in\Sigma$, and $\mathfrak{l}=\Sigma/\mathfrak{p}\Sigma$. If we define $\bar{a}x=\bar{a}(XT)=(aX)T$, for $a\in\mathfrak{o}$, then $\mathfrak{l}$ becomes a Lie algebra of dimension n over $\overline{K}$ which will be called a *modular Lie algebra.*

THEOREM 1. *The modular Lie algebra $\mathfrak{l}=\Sigma/\mathfrak{p}\Sigma$ defined at a nonexceptional prime ideal $\mathfrak{p}$ is a separable algebra over $\overline{K}$ whose rank is equal to the rank of $\mathfrak{L}$. The natural mapping T: $\Sigma\to\mathfrak{l}$ maps $\mathfrak{H}\cap\Sigma$ onto a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{l}$. The restriction of the Killing form of $\mathfrak{l}$ to $\mathfrak{h}$ is nondegenerate.*

Proof. The cosets $(X_iT)=(x_i)$ form a basis of $\mathfrak{l}$ over $\overline{K}$, and from (2) we have $[x_ix_j]=\sum\bar{c}_{ijk}x_k$. If $B^*(x, y)$ is the Killing form on $\mathfrak{l}$, then

$$B^*(x_i, x_j) = \text{trace}(\text{ad } x_i \text{ ad } x_j) = \sum_{\mu,\nu=1}^{n} \bar{c}_{\mu i\nu}\bar{c}_{\nu j\mu}$$

$$= \phi\left(\sum_{\mu,\nu=1}^{n} c_{\mu i\nu}c_{\nu j\mu}\right) = \phi(B(X_i, X_j)),$$

and by linearity we have, for all X, Y in Σ,

$$\phi(B(X, Y)) = B^*(XT, YT). \tag{9}$$

In particular, $\det B^*(x_i, x_j) = \det \phi(B(X_i, X_j)) = \phi(\det (B(X_i, X_j))) \neq 0$ by the remarks in §4, and hence $\mathfrak{l}$ is separable.

For each root α of $\mathfrak{L}$ relative to $\mathfrak{H}$, we have $\alpha(H_i) \in Z \subseteq \mathfrak{o}$ for $1 \leqq i \leqq l$. Therefore, if we set $\mathfrak{h} = (\mathfrak{H} \cap \Sigma)T$, we can define a unique linear function $\bar{\alpha}$ on $\mathfrak{h}$ whose value on H_iT is given by $\bar{\alpha}(H_iT) = \phi(\alpha(H_i))$, $1 \leqq i \leqq l$. It follows that for all $H \in \mathfrak{H} \cap \Sigma$ we have

$$\phi(\alpha(H)) = \bar{\alpha}(HT), \tag{10}$$

and in particular, since $H_\alpha \in \mathfrak{H} \cap \Sigma$, $\bar{\alpha}(H_\alpha T) = \phi(\alpha(H_\alpha)) = \phi(2) \neq 0$ in $\overline{K}$ so that the linear functions $\bar{\alpha}$ on $\mathfrak{h}$ are all different from zero. For any root vector $X_i = E_\alpha$, the relation $[X_iH] = \alpha(H)X_i$, $H \in \mathfrak{H} \cap \Sigma$, implies that

$$[x_ih] = \bar{\alpha}(h)x_i, \qquad h \in \mathfrak{h}. \tag{11}$$

From (11) and the fact that all $\bar{\alpha} \neq 0$ we see that $[\mathfrak{h}x] \subseteq \mathfrak{h}$ implies $x \in \mathfrak{h}$, and since $\mathfrak{h}$ is commutative, we conclude that $\mathfrak{h} = (\mathfrak{H} \cap \Sigma)T$ is a Cartan subalgebra of $\mathfrak{l}$.

Let $f(\lambda; \tau)$ be the characteristic polynomial of ad X^*, where $X^* = \sum \tau_i X_i$ is the general element of $\mathfrak{L}$. If we let $x^* = \sum \tau_i' x_i$ be the general element of $\mathfrak{l}$ with respect to the basis $(X_iT) = (x_i)$, then it can be verified that the coefficients $\mu_k^*(\tau')$ of the characteristic polynomial $f'(\lambda; \tau')$ of ad x^* are obtained from the $\mu_k(\tau)$ of (1) by replacing the τ_i by τ_i', $1 \leqq i \leqq n$, and the coefficients of the τ's, which are in $\mathfrak{o}$, by their images under ϕ. If l is the rank of $\mathfrak{L}$, then $\mu_{n-l+1}^*(\tau') = \cdots = \mu_n^*(\tau') = 0$, so that rank $\mathfrak{l} \geqq l$.

In order to prove that the rank of $\mathfrak{l}$ does not exceed l, we form $\mathfrak{l}^L$, where L is any infinite field containing $\overline{K}$. Then the linear functions $\bar{\alpha}$, extended by linearity to $\mathfrak{h}^L$, are all different from zero. Since L is an infinite field, there exists an element $h = \sum \xi_i x_i$, $\xi_i \in L$, in $\mathfrak{h}^L$ such that $\bar{\alpha}(h) \neq 0$ for all $\bar{\alpha}$. It follows from (11) that the characteristic polynomial of ad h has exactly l roots equal to zero. Now $x^* = \sum \tau_i' x_i$ also may be viewed as the general element[6] of $\mathfrak{l}^L$. Upon substituting ξ_i for τ_i' in $\mu_{n-1}^*(\tau')$ we obtain $\mu_{n-l}^*(\xi_1, \cdots, \xi_n) \neq 0$, otherwise the characteristic polynomial of ad h would have more than l roots equal to zero. Thus the rank of $\mathfrak{l}^L$ does not exceed l, and by Lemma 1 and what has already been proved, the rank of $\mathfrak{l}$ is equal to l.

---

[6] We may assume that the τ_i' are transcendental over L.

Finally, by (9) and (6) it follows that $B^*(h, x_i)=0$ for $1\leqq i\leqq m$ and $m+l+1\leqq i\leqq n$ and all h in $\mathfrak{h}$. Therefore the restriction of B^* to $\mathfrak{h}$ is nondegenerate, because $\mathfrak{l}$ is separable. This completes the proof of the theorem.

The linear functions $\bar{\alpha}$ on $\mathfrak{h}$ which were defined in the proof of Theorem 1 are roots of $\mathfrak{l}$ with respect to $\mathfrak{h}$ (see [12] or [16] for a discussion of roots of Lie algebras of characteristic $p>0$.) The following result describes the properties of the roots $\bar{\alpha}$ which we shall need.

THEOREM 2. *The mapping $\alpha\rightarrow\bar{\alpha}$ is a* (1-1) *mapping of the set R of roots of $\mathfrak{L}$ relative to $\mathfrak{H}$ onto the set $\overline{R}$ of roots of $\mathfrak{l}$ relative to $\mathfrak{h}$, such that the following statements are valid.*

(a) *$\alpha, \beta, \alpha+\beta\in R$ implies $\bar{\alpha}+\bar{\beta}\in\overline{R}$ and $\alpha+\beta\rightarrow\bar{\alpha}+\bar{\beta}$;*

(b) *$\alpha\in R$ implies $-\bar{\alpha}\in\overline{R}$ and $-\alpha\rightarrow-\bar{\alpha}$;*

(c) *$\bar{\alpha}_1, \cdots, \bar{\alpha}_l$ are linearly independent, and form a fundamental system*(7) *of roots of $\mathfrak{l}$ relative to $\mathfrak{h}$.*

(d) *if $m=0, 1, \cdots, p-1$, then $m\bar{\alpha}\in\overline{R}$ if and only if $m=1$ or $m=p-1$.*

Proof. In order to prove that that mapping $\alpha\rightarrow\bar{\alpha}$ is (1-1) and onto, it is convenient to extend the base field $\overline{K}$ to its algebraic closure Ω. The functions $\bar{\alpha}$, extended to $\mathfrak{h}^\Omega$ by linearity, are all different from zero, and this fact, together with the multiplication table of the basis (x_i) of $\mathfrak{l}$, implies that $\mathfrak{h}^\Omega$ is a Cartan subalgebra of $\mathfrak{l}^\Omega$, and that the functions $\bar{\alpha}$ are roots of $\mathfrak{l}^\Omega$ with respect to $\mathfrak{h}^\Omega$. Suppose that $\bar{\alpha}=\bar{\beta}$, where $\alpha\neq\beta$; then the dimension of the root space of $\bar{\alpha}$ is not less than two, and since the characteristic of $\overline{K}$ exceeds 3, this contradicts a result of Jacobson [12, Theorems 5.1 and 5.2]. The mapping $\alpha\rightarrow\bar{\alpha}$ is onto, since a root of $\mathfrak{l}$ relative to $\mathfrak{h}$ distinct from the $\bar{\alpha}$ would define a root of $\mathfrak{l}^\Omega$ distinct from the $\bar{\alpha}$, and this is impossible, since the root vectors belonging to the roots $\bar{\alpha}$, together with the elements of $\mathfrak{h}^\Omega$, span $\mathfrak{l}^\Omega$. Over the infinite field Ω, elements of $\mathfrak{l}^\Omega$ belonging to distinct roots are linearly independent.

Statements (a) and (b) are obvious. We have $\bar{\alpha}_i(H_jT)=-\phi(a_{ij})$ for $1\leqq i, j\leqq l$. Since $\det\phi(a_{ij})\neq 0$, the roots $\bar{\alpha}_1, \cdots, \bar{\alpha}_l$ are linearly independent. Now let Λ be any $\mathfrak{p}$-integral linear function on $\mathfrak{H}:\Lambda(H_i)\in\mathfrak{o}$, $1\leqq i\leqq l$. We write $\phi\Lambda=\overline{\Lambda}$ for the unique linear function on $\mathfrak{h}$ such that $\overline{\Lambda}(H_iT)=\phi(\Lambda(H_i))$, $1\leqq i\leqq l$, in agreement with our definition of the roots $\bar{\alpha}$. Let S_i be the reflection determined by α_i on the dual space of $\mathfrak{H}$, and let $\overline{S}_i$ be the reflection determined by $\bar{\alpha}_i$ on the dual space of $\mathfrak{h}$. Then for all $\mathfrak{p}$-integral linear functions Λ, ΛS_i is $\mathfrak{p}$-integral, and

$$\phi(\Lambda S_i) = \overline{\Lambda}\overline{S}_i, \qquad 1\leqq i\leqq l. \tag{12}$$

From (12) and the fact that $\alpha_1, \cdots, \alpha_l$ is a fundamental system, (c) follows

(7) By analogy with Cartan's definition in the characteristic zero theory, we call $\bar{\alpha}_1, \cdots, \bar{\alpha}_l$ a fundamental system if every root $\bar{\alpha}$ is an image of some $\bar{\alpha}_i$ by an element of the group of l.t. on the dual space of $\mathfrak{h}$ generated by the reflections $\lambda\rightarrow\lambda-\lambda(h_i)\bar{\alpha}_i$, $1\leqq i\leqq l$, where $h_i=H_iT$.

directly. Finally, since the characteristic $p>3$, statement (d) holds for $\mathfrak{l}^\Omega$, and hence for $\mathfrak{l}$, by [12, Theorem 5.3].

We show next that the p-power operation on the basis elements x_i of $\mathfrak{l}$ is given by the following formulas.

$$
\begin{aligned}
x_i^p &= 0, &\qquad 1 \leqq i \leqq m,\ m+l+1 \leqq i \leqq n;\\
x_i^p &= x_i, &\qquad m+1 \leqq i \leqq m+l.
\end{aligned}
\tag{13}
$$

That the $x^p=0$, $1\leqq i\leqq m$, $m+l+1\leqq i\leqq n$, follows from a result of Jacobson [12, Theorem 4.1]. For $i=1, \cdots, l$ we have $x_{m+i}=H_iT$, and by the definition of the p-power operation it is sufficient to prove that for all $X\in\Sigma$, $X(\mathrm{ad}\, H_i)^p\equiv[XH_i]$ (mod $\mathfrak{p}\Sigma$). We need check it only for a root vector $X=E_\alpha$, and in this case the statement is obvious, since $\alpha(H_i)\in Z$.

6. **Preliminary results on representation theory.** We show in this section that each irreducible representation of $\mathfrak{L}$ gives rise to a restricted representation of $\mathfrak{l}$. Let $\mathfrak{A}$ be the universal associative algebra of $\mathfrak{L}$ (see [2; 6; 15]). Let $P=(i_1, \cdots, i_m)$, $Q=(j_1, \cdots, j_l)$, $R=(k_1, \cdots, k_m)$ be row vectors whose coefficients are non-negative rational integers. We write $|P|=\sum_{\nu=1}^m i_\nu$, and similarly define $|Q|$, $|R|$; we write $0=(0, \cdots, 0)$ so that $|0|=0$. If (X_i) is an admissible basis of $\mathfrak{L}$ (see §3), then the elements(8)

$$Z(P, Q, R) = X_1^{i_1}\cdots X_m^{i_m}X_{m+1}^{j_1}\cdots X_{m+l}^{j_l}X_{m+l+1}^{k_1}\cdots X_n^{k_m},$$

where $|P|, |Q|, |R|\geqq 0$, form a basis of $\mathfrak{A}$ over C. The number $|P|+|Q|+|R|$ is called the *degree* of $Z(P, Q, R)$. The degree of $F=\sum a(P, Q, R)Z(P, Q, R)$, $a(P, Q, R)\in C$, is defined to be the largest $|P|+|Q|+|R|$ for which $a(P, Q, R)\neq 0$, and we write deg F for this number, with the convention that $\deg 0=-\infty$. Then it is known that

$$
\begin{aligned}
\deg (F+G) &\leqq \max (\deg F + \deg G),\\
\deg (FG) &= \deg F + \deg G,\\
\deg [FG] &= \deg (FG-GF) < \deg F + \deg G.
\end{aligned}
\tag{14}
$$

From (14) it follows in particular that $\deg (X_{i_1}\cdots X_{i_r})=r$, $1\leqq i_j\leqq n$, and

$$\deg\left(\sum_{0\leqq r, 1\leqq i_j\leqq n} a_{i_1\cdots i_r}X_{i_1}\cdots X_{i_r}\right) = \max_{a_{i_1}\cdots_{i_r}\neq 0}(r), \qquad a_{i_1\cdots i_r}\in C.$$

Let $\mathfrak{B}$ be the set of all linear combinations of the $Z(P, Q, R)$ with coefficients in $\mathfrak{o}$. Then $\mathfrak{B}$ is contained in the subring of $\mathfrak{A}$ generated by the elements of $\Sigma=\sum_i\mathfrak{o}X_i$ and $\mathfrak{o}$; in fact, $\mathfrak{B}$ is identical with this subring. All that has to be proved is that $Z(P, Q, R)Z(P', Q', R')$ is an $\mathfrak{o}$-linear combination of the

(8) We shall identify $\mathfrak{L}$ with the linear part of $\mathfrak{A}$.

$Z(P, Q, R)$, and this, in turn, follows if we can show that an arbitrary product $X_{i_1} \cdots X_{i_r}$ of the X_j is an $\mathfrak{o}$-linear combination of the $Z(P, Q, R)$. This fact is established by induction on the degree of $X_{i_1} \cdots X_{i_r}$, and on the minimum number of transpositions of the X_{i_j} required to put $X_{i_1} \cdots X_{i_r}$ in the form $Z(P, Q, R)$, i.e. in the form $X_{j_1} \cdots X_{j_r}$, where $j_1 \leqq j_2 \leqq \cdots \leqq j_r$. The reduction is achieved by the usual straightening process, using the fact that $[X_i X_j] = \sum c_{ijk} X_k$, where the $c_{ijk} \in \mathfrak{o}$.

Let $\mathfrak{a}$ be the u-algebra (see [9]) of the modular Lie algebra $\mathfrak{l} = \Sigma/\mathfrak{p}\Sigma$ over $\bar{K}$; we shall identify $\mathfrak{l}$ with its image in $\mathfrak{a}$ under the natural imbedding of $\mathfrak{l}$ into $\mathfrak{a}$. Then $\mathfrak{a}$ has a basis over $\bar{K}$ consisting of the standard monomials

$$z(P, Q, R) = x_1^{i_1} \cdots x_m^{i_m} x_{m+1}^{j_1} \cdots x_{m+l}^{j_l} x_{m+l+1}^{k_1} \cdots x_n^{k_m}, \tag{15}$$

where $0 \leqq i_t, j_t, k_t < p$.

Now $\mathfrak{a}$, as well as $\mathfrak{l}$, can be regarded as a Lie algebra over $\mathfrak{o}$, having the elements (15) as a set of generators, and scalar multiplication defined by $af = \bar{a}f$ for $a \in \mathfrak{o}$, $f \in \mathfrak{a}$. The mapping $T:\Sigma \to \mathfrak{l}$ may be regarded as an $\mathfrak{o}$-linear homomorphism of the Lie algebra Σ over $\mathfrak{o}$ into the associative algebra $\mathfrak{a}$ over $\mathfrak{o}$. Thus T is an $\mathfrak{o}$-linear mapping of $\Sigma \to \mathfrak{a}$ such that

$$[XT]T = [XT, YT] = (XT)(YT) - (YT)(XT)$$

for all $X, Y \in \Sigma$. From the properties of the algebra $\mathfrak{B}$ which we have derived, it follows that T can be extended uniquely to an $\mathfrak{o}$-linear associative homomorphism $\tilde{T}$ of $\mathfrak{B}$ onto $\mathfrak{a}$ such that $1\tilde{T} = 1$, $X\tilde{T} = XT$ for all $X \in \Sigma$, and such that $(aX)\tilde{T} = \bar{a}(XT)$ for $X \in \Sigma$, $a \in \mathfrak{o}$. We shall determine the kernel of the homomorphism $\tilde{T}$.

From the definition of the p-power operation in $\mathfrak{l}$, it follows that for each $X \in \Sigma$ there exists an element $X^{[p]}$, which is uniquely determined mod $\mathfrak{p}\Sigma$, such that $X^{[p]}T = (XT)^p$, and such that for all $Y \in \Sigma$,

$$Y(\text{ad } X)^p \equiv [YX^{[p]}] \pmod{\mathfrak{p}\Sigma}. \tag{16}$$

From this formula we obtain the following congruence in $\mathfrak{B}$:

$$[F, X^p - X^{[p]}] \equiv 0 \pmod{\mathfrak{p}\mathfrak{B}} \tag{17}$$

for all $X \in \Sigma$, $F \in \mathfrak{B}$. From (16), since $F \to [FX^{[p]}]$ and $(\text{ad } X)^p$ are derivations in $\mathfrak{B}$ modulo $\mathfrak{p}\mathfrak{B}$, we have

$$F(\text{ad } X)^p \equiv [FX^{[p]}] \pmod{\mathfrak{p}\mathfrak{B}}.$$

On the other hand we have by a well known identity [10, p. 102], $F(\text{ad } X)^p \equiv [FX^p] \pmod{\mathfrak{p}\mathfrak{B}}$. From these formulas we obtain (17).

LEMMA 2. *The $\mathfrak{o}$-linear homomorphism $T:\Sigma \to \mathfrak{l}$ can be extended to a unique homomorphism $\tilde{T}$ of $\mathfrak{B}$ onto the u-algebra $\mathfrak{a}$ of $\mathfrak{l}$, such that the kernel $\mathfrak{X}$ of $\tilde{T}$ is the ideal in $\mathfrak{B}$ generated by the elements $X_i^{[p]} - X_i^p$, $1 \leqq i \leqq n$, and the elements of $\mathfrak{p}$.*

Proof. Obviously the ideal $\mathfrak{X}'$ generated by the $X_i^{[p]}-X_i^p$ and $\mathfrak{p}$ is contained in $\mathfrak{X}$. Now let F be an element of $\mathfrak{B}$ such that $F\notin\mathfrak{X}'$; we prove that $F\tilde{T}\neq 0$. Let $F=\sum a(P, Q, R)Z(P, Q, R)$, $a(P, Q, R)\in\mathfrak{o}$. Since all the $X_i^{[p]}$ have degree not greater than one, it follows that F is congruent mod $\mathfrak{X}'$ to an expression $F'=\sum a(P, Q, R)Z(P, Q, R)$ with coefficients in $\mathfrak{o}$ in which all the components of P, Q, R in a term whose coefficient is not zero are less than p, and such that no nonzero coefficient is in $\mathfrak{p}$. Since $F\notin\mathfrak{X}'$, $F'\notin\mathfrak{X}'$, and hence $F'\neq 0$. Moreover $F\tilde{T}=F'\tilde{T}$ since $\mathfrak{X}'\subseteq\mathfrak{X}$, and $F'\tilde{T}\neq 0$ because the elements $z(P, Q, R)$ in which the components of P, Q, and R are less than p are linearly independent in $\mathfrak{a}$. Thus $\mathfrak{X}'=\mathfrak{X}$, and the lemma is proved.

Let ρ be a representation of $\mathfrak{A}$ by l.t. in a finite dimensional space $\mathfrak{M}$ over C. Then $\mathfrak{M}$ becomes a right $\mathfrak{A}$-module if we define $UF=U\rho(F)$ for $U\in\mathfrak{M}$, $F\in\mathfrak{A}$. Conversely every right $\mathfrak{A}$-module defines a representation of $\mathfrak{A}$. When we speak of $\mathfrak{A}$-modules, it is assumed that the vector spaces involved are finite dimensional. Similar remarks apply to the u-algebra $\mathfrak{a}$ of $\mathfrak{l}$. If $\mathfrak{M}$ (resp. $\mathfrak{m}$) is an $\mathfrak{A}$-module (resp. $\mathfrak{a}$-module), then a linear function Λ (resp. λ) on $\mathfrak{H}$ (resp. $\mathfrak{h}$) is called a *weight* of $\mathfrak{M}$ (resp. $\mathfrak{m}$) if $\mathfrak{M}_\Lambda=\{U \mid UH=\Lambda(H)U$ for all $H\in\mathfrak{H}\}\neq 0$ (resp. $\mathfrak{m}_\lambda=\{u \mid uh=\lambda(h)u$ for all $h\in\mathfrak{h}\}\neq 0$). A linear function Λ on $\mathfrak{H}$ is called an *integral linear function* if $\Lambda(H_i)\in Z$ for $1\leqq i\leqq l$; Λ is a *dominant integral function* if $\Lambda(H_i)\geqq 0$ for $1\leqq i\leqq l$. It is known that every weight of an $\mathfrak{A}$-module $\mathfrak{M}$ is an integral function, and that every $\mathfrak{A}$-module has a highest weight Λ, with respect to the lexicographic order in the set of rational functions on $\mathfrak{H}$, such that Λ is a dominant integral function. The weights of an $\mathfrak{A}$-module $\mathfrak{M}$ have the property that $\Lambda(H_\alpha)$ is an integer for every root α, and that if Λ is the highest weight, and α any positive root, then $\Lambda(H_\alpha)\geqq 0$. If $\mathfrak{M}$ is an irreducible $\mathfrak{A}$-module, then the dimension of the space $\mathfrak{M}_\Lambda$ belonging to the highest weight Λ is equal to one. Two irreducible $\mathfrak{A}$-modules having the same highest weight are $\mathfrak{A}$-isomorphic. If Λ is any dominant integral function on $\mathfrak{H}$, then there exists a (finite dimensional) irreducible $\mathfrak{A}$-module whose highest weight is Λ. For proofs of these results, see [7; 14].

LEMMA 3. *Let $\mathfrak{M}$ be an irreducible $\mathfrak{A}$-module. Then there exists a finitely generated $\mathfrak{o}$-submodule $\mathfrak{M}_0$ of $\mathfrak{M}$ such that $\mathfrak{M}_0$ spans $\mathfrak{M}$, and such that $\mathfrak{M}_0\mathfrak{B}\subseteq\mathfrak{M}_0$.*

Proof. Let Λ be the highest weight of $\mathfrak{M}$, and let $U\neq 0$ be an element of $\mathfrak{M}_\Lambda$. By our remark above, for every positive root α, $\Lambda(H_\alpha)\geqq 0$. By [7, pp. 51, 52], the elements $UZ(0, 0, R)$, $R=(k_1, \cdots, k_m)$, $0\leqq k_j\leqq\Lambda(H_{\alpha_j})$, where α_j is the positive root such that X_{m+l+j} belongs to $-\alpha_j$, form a set of C-generators of $\mathfrak{M}$. A close inspection of the argument shows that these elements form a set of $\mathfrak{o}$-generators for the $\mathfrak{o}$-module $\mathfrak{M}_0$ consisting of all $\mathfrak{o}$-linear combinations of the elements $UZ(P, Q, R)$, $(P, Q, R$ arbitrary). Since the elements $Z(P, Q, R)$ form an $\mathfrak{o}$-basis for $\mathfrak{B}$, we have $\mathfrak{M}_0\mathfrak{B}\subseteq\mathfrak{M}_0$, and the lemma is proved.

COROLLARY. *The module $\mathfrak{M}_0/\mathfrak{M}_0\mathfrak{X}$ is an $\mathfrak{a}$-module, finite dimensional over the field $\overline{K}$.*

Proof. The assertion follows from the facts that $\mathfrak{M}_0$ is a finitely generated $\mathfrak{o}$-module such that $\mathfrak{M}_0\mathfrak{B}\subseteq\mathfrak{M}_0$, and that $\mathfrak{X}$ is the kernel of the homomorphism $\tilde{T}$ of $\mathfrak{B}$ onto $\mathfrak{a}$.

We shall call the $\mathfrak{a}$-module $\mathfrak{M}_0/\mathfrak{M}_0\mathfrak{X}$ associated with an irreducible $\mathfrak{A}$-module $\mathfrak{M}$ a *ϕ-module* belonging to $\mathfrak{M}$.

Let $\mathfrak{n}$ be the radical of $\mathfrak{a}$ (if $\mathfrak{l}$ is not commutative then $\mathfrak{n}\neq 0$ by a result of Hochschild [8]). Let $f\rightarrow f^*$ be the natural mapping of $\mathfrak{a}\rightarrow\mathfrak{a}/\mathfrak{n}=\mathfrak{a}^*$, and let $\mathfrak{a}^*=\sum e_i^*\mathfrak{a}^*$ be a decomposition of $\mathfrak{a}^*$ into minimal right ideals, where the e_i^* are mutually orthogonal idempotents. Since $\mathfrak{a}$ has an identity element, Theorem 9.3C of [1] implies that there exist mutually orthogonal idempotents e_i such that $e_i+\mathfrak{n}=e_i^*$ for each i, and such that $\mathfrak{a}=\sum e_i\mathfrak{a}$ is a decomposition of $\mathfrak{a}$ into indecomposable right ideals. By Theorem 9.2G of [1], $e_i\mathfrak{a}$ is a-isomorphic to $e_j\mathfrak{a}$ if and only if $e_i^*\mathfrak{a}^*$ and $e_j^*\mathfrak{a}^*$ are $\mathfrak{a}$-isomorphic. We can partition the e_i appearing in the decomposition $\mathfrak{a}=\sum e_i\mathfrak{a}$ into equivalence classes, e_i being equivalent to e_j if $e_i\mathfrak{a}$ and $e_j\mathfrak{a}$ are $\mathfrak{a}$-isomorphic. Let $e^{(1)},\cdots,e^{(k)}$ be the idempotents in $\mathfrak{a}$ which are the sums of the elements in the distinct equivalence classes. It follows that $(e^{(1)})^*,\cdots,(e^{(k)})^*$ are central, mutually orthogonal idempotents in $\mathfrak{a}^*$, which are the identity elements of the distinct simple ideals in the two sided Wedderburn decomposition of $\mathfrak{a}^*$. If $\mathfrak{m}$ is any irreducible $\mathfrak{a}$-module, then since $\mathfrak{m}$ is $\mathfrak{a}$-isomorphic to one of the $e_i^*\mathfrak{a}^*$, there exists one of the $e^{(j)}$ such that $ue^{(j)}=u$ for all $u\in\mathfrak{m}$. Since the $e^{(j)}$ are mutually orthogonal by construction, $\mathfrak{m}e^{(k)}=0$ if $k\neq j$, and we shall say that $\mathfrak{m}$ belongs to the jth class. It is easily proved that an irreducible $\mathfrak{a}$-module $\mathfrak{m}_1$ belongs to the jth class if and only if $\mathfrak{m}_1e^{(j)}\neq 0$, and that an arbitrary $\mathfrak{a}$-module $\mathfrak{m}_2$ has a composition factor of the jth class if and only if $\mathfrak{m}_2e^{(j)}\neq 0$.

Now let $\mathfrak{M}$ be an arbitrary irreducible $\mathfrak{A}$-module, and let $\mathfrak{M}_0$ be the $\mathfrak{o}$-submodule of $\mathfrak{M}$ constructed in Lemma 3. Let F_j be any element of $\mathfrak{B}$ such that $F_j\tilde{T}=e^{(j)}$. Then if $u=U+\mathfrak{M}_0\mathfrak{X}$ is an element of the ϕ-module $\mathfrak{M}_0/\mathfrak{M}_0\mathfrak{X}$, we have $ue^{(j)}=UF_j+\mathfrak{M}_0\mathfrak{X}$. We have proved the following lemma.

LEMMA 4. *A ϕ-module $\mathfrak{M}_0/\mathfrak{M}_0\mathfrak{X}$ has a composition factor in the jth class if and only if $\mathfrak{M}_0F_j\not\subseteq\mathfrak{M}_0\mathfrak{X}$, where F_j is any element of $\mathfrak{B}$ such that $F_j\tilde{T}=e^{(j)}$.*

7. **The Cartan-Weyl theory of weights of representations of a modular Lie algebra.** We begin with some general remarks on the representations of associative algebras (see [10] for a complete discussion). Let $\mathfrak{a}$ be a finite dimensional algebra over a field E. An extension field $F\supseteq E$ is called a *splitting field* if every irreducible $\mathfrak{a}^F$-module is *absolutely irreducible*, that is, it remains irreducible for arbitrary extensions of the field F. Let $\mathfrak{n}$ be the radical of $\mathfrak{a}^F$. Then F is a splitting field if and only if $\mathfrak{a}^F/\mathfrak{n}$ is a direct sum of full matrix algebras over F. If F is a splitting field and $\Omega\supseteq F$, then Ω is a splitting field. If $F\subseteq\Omega$, F a splitting field, then every irreducible $\mathfrak{a}^\Omega$-module $\mathfrak{q}$ is equal to $\mathfrak{m}^\Omega$,

where $\mathfrak{m}$ is an $\mathfrak{a}$-F submodule of $\mathfrak{q}$. This property is characteristic of splitting fields.

LEMMA 5. *Let E be a perfect field, and let $\Omega \supseteq E$ be a splitting field. Then E is a splitting field if every irreducible $\mathfrak{a}^\Omega$-module $\mathfrak{q}$ is equal to $\mathfrak{m}^\Omega$, where $\mathfrak{m}$ is an $\mathfrak{a}$-E-submodule of $\mathfrak{q}$.*

Proof. Let $\mathfrak{n}$ be the radical of $\mathfrak{a}$. Then $\mathfrak{a}/\mathfrak{n}$ is a separable algebra, and it follows that $\mathfrak{n}^\Omega$ is the radical of $\mathfrak{a}^\Omega$, so that

$$(\mathfrak{a}/\mathfrak{n})^\Omega \cong \mathfrak{a}^\Omega/\mathfrak{n}^\Omega \cong \Omega_{h_1} \oplus \cdots \oplus \Omega_{h_r} \tag{18}$$

where Ω_h is the algebra of $h \times h$ matrices over Ω. For each i, $1 \leqq i \leqq r$, there exists a minimal right ideal $\mathfrak{q}_i$ in $\mathfrak{a}^\Omega/\mathfrak{n}^\Omega$ of dimension h_i over Ω (corresponding to the ith direct summand Ω_{h_i}), which, by the hypothesis, has the form $\mathfrak{q}_i = (\mathfrak{m}_i)^\Omega$, where the $\mathfrak{m}_i$ are irreducible $\mathfrak{a}$-E-modules of dimension h_i over E. Clearly no two of the $\mathfrak{m}_i$ can be $\mathfrak{a}$-isomorphic. Therefore, if t_i is the dimension over E of the centralizer of $\mathfrak{m}_i$, it follows that the dimension d over E of $\mathfrak{a}/\mathfrak{n}$ is not less than $\sum h_i^2 t_i$. On the other hand $d = \sum h_i^2$ by (18). Therefore $\sum h_i^2 \geqq \sum h_i^2 t_i$, and hence $t_i = 1$ for all i. It now follows from Burnside's Theorem that $\mathfrak{a}/\mathfrak{n}$ is a direct sum of full matrix algebras over E, and that E is a splitting field.

THEOREM 3. *Let $\mathfrak{l}$ be a separable modular algebra $\Sigma/\mathfrak{p}\Sigma$, where $\mathfrak{p}$ is a nonexceptional prime ideal in K. Then $\overline{K}$ is a splitting field for the u-algebra $\mathfrak{a}$ of $\mathfrak{l}$. Every irreducible $\mathfrak{a}$-module $\mathfrak{m}$ is a direct sum of weight spaces $\mathfrak{m}_\lambda$ belonging to the distinct weights of $\mathfrak{m}$.*

Proof. Let Ω be the algebraic closure of $\overline{K}$; obviously Ω is a splitting field. Moreover $\overline{K}$ is a finite field and hence perfect. By Lemma 5, $\overline{K}$ is a splitting field if we can prove that an arbitrary irreducible $\mathfrak{a}^\Omega$-module $\mathfrak{q}$ is equal to $\mathfrak{m}^\Omega$, where $\mathfrak{m}$ is an $\mathfrak{a}$-$\overline{K}$-submodule of $\mathfrak{q}$. Since $\mathfrak{h}$ is a finite dimensional commutative subalgebra of $\mathfrak{l}$, it is immediate that $\mathfrak{q}$ has at least one weight λ; let $u \neq 0$ belong to λ. If $x_{\bar{\alpha}}$ is one of the root elements among the (x_i) then $ux_{\bar{\alpha}}$ is either zero, or belongs to the weight $\lambda + \bar{\alpha}$. Consider the $\overline{K}$ subspace $\mathfrak{m}$ generated by the elements

$$ux_{i_1} \cdots x_{i_r}, \qquad r \geqq 0, \tag{19}$$

where either $1 \leqq i_j \leqq m$ or $m+l+1 \leqq i_j \leqq n$; each of these elements is either a weight vector or zero. We observe that if w is any weight vector belonging to a weight μ, then because of (13), $\mu(x_i)^p = \mu(x_i)$, $m+1 \leqq i \leqq m+l$, and hence $\mu(x_i) \in \overline{K}_0$, where $\overline{K}_0$ is the prime field contained in $\overline{K}$, for $m+1 \leqq i \leqq m+l$. It follows from this remark that $\mathfrak{m}\mathfrak{a} \subseteq \mathfrak{m}$, and $\mathfrak{m}^\Omega \mathfrak{a}^\Omega \subseteq \mathfrak{m}^\Omega$. By the irreducibility of $\mathfrak{q}$, we have $\mathfrak{m}^\Omega = \mathfrak{q}$, and the first part of the theorem is proved.

Now let $\mathfrak{m}$ be an irreducible $\mathfrak{a}$-module, Ω the algebraic closure of $\overline{K}$; then $\mathfrak{m}^\Omega$ is irreducible, and hence $\mathfrak{m}^\Omega = \mathfrak{m}_1^\Omega$, where $\mathfrak{m}_1$ is an $\mathfrak{a}$-submodule generated by weight vectors of the form (19). By the remarks preceding Lemma 4,

$\mathfrak{m}$ and $\mathfrak{m}_1$ are $\mathfrak{a}$-isomorphic. But since $\mathfrak{m}_1$ has a basis consisting of weight vectors, we have $\mathfrak{m}_1 = \sum(\mathfrak{m}_1)_\lambda$ where the λ are the distinct weights of $\mathfrak{m}_1$. Since $\mathfrak{m} \cong \mathfrak{m}_1$, the same statement applies to $\mathfrak{m}$, and the theorem is proved.

REMARK. Let $\mathfrak{m}$ be an arbitrary $\mathfrak{a}$-module such that $\mathfrak{m}$ is spanned by weight vectors. If $\lambda_1, \cdots, \lambda_s$ are the distinct weights of $\mathfrak{m}$, then $\mathfrak{m} = \sum_{i=1}^{s} \mathfrak{m}\lambda_i$ (direct sum). From this we see that if $\mathfrak{m}$ has a basis consisting of weight vectors belonging to weights $\lambda_1, \cdots, \lambda_s$, then every weight of $\mathfrak{m}$ appears among the λ_i. The proofs of these facts are easy, and we omit them.

The (1-1) mapping $\alpha \rightarrow \bar{\alpha}$ of the roots of $\mathfrak{L}$ onto the roots of $\mathfrak{l}$ defines a linear order relation among the roots of $\mathfrak{l}$; thus we shall write $\bar{\alpha} > 0$ if $\alpha > 0$, and $\bar{\alpha} < \bar{\beta}$ if $\alpha < \beta$.

LEMMA 6. *Let* $\mathfrak{m}$ *be a* $\mathfrak{a}$*-module, and let* $\mathfrak{m}$ *have a weight* λ *such that for some weight vector* $u \neq 0$ *belonging to* λ, $ux_i = 0$, *for* $1 \leqq i \leqq m$. *Then the subspace* $\mathfrak{m}_1$ *generated by all elements* $uz(0, 0, R)$ *is an* $\mathfrak{a}$*-submodule.*

Proof. Clearly $\mathfrak{m}_1 x_i \subseteq \mathfrak{m}_1$ for $m+1 \leqq i \leqq n$. Let $x_{\bar{\alpha}}$ be a root vector belonging to a positive root $\bar{\alpha}$, and let $uz(0, 0, R) = ux_{i_1} \cdots x_{i_r}$ be a generator of $\mathfrak{m}_1$. Since $ux_{\bar{\alpha}} = 0$, we can assume that $uz(0, 0, R')x_{\bar{\alpha}} = ux_{i_1} \cdots x_{i_s} x_\alpha \in \mathfrak{m}_1$ whenever $s < r$. If $\bar{\alpha}$ is the least positive root, then, if $x_{i_r} = x_{\bar{\beta}}$, we have

$$ux_{i_1} \cdots x_{i_r} x_{\bar{\alpha}} = ux_{i_1} \cdots x_{i_{r-1}} x_{\bar{\alpha}} x_{i_r} + ux_{i_1} \cdots x_{i_{r-1}} [x_{\bar{\beta}} x_{\bar{\alpha}}], \tag{20}$$

which is in $\mathfrak{m}_1$ because of our induction hypothesis, and because $[x_{\bar{\beta}} x_{\bar{\alpha}}]$ is either zero, or in $\mathfrak{h}$, or a multiple of $x_{\bar{\beta}+\bar{\alpha}}$ where $\bar{\beta}+\bar{\alpha} < 0$, otherwise $0 < \beta+\alpha < \alpha$, and $0 < \bar{\beta}+\bar{\alpha} < \bar{\alpha}$ since the mapping $\alpha \rightarrow \bar{\alpha}$ preserves sums of roots and the order relation. Thus we can also assume that $\mathfrak{m}_1 x_\gamma \subseteq \mathfrak{m}_1$ for all $\bar{\gamma} < \bar{\alpha}$. Then by (20), $ux_{i_1} \cdots x_{i_r} x_{\bar{\alpha}} \equiv ux_{i_1} \cdots x_{i_{r-1}} [x_{\bar{\beta}} x_{\bar{\alpha}}]$ (mod $\mathfrak{m}_1$), where $[x_{\bar{\beta}} x_{\bar{\alpha}}]$ is either zero, or in $\mathfrak{h}$, or a multiple of $x_{\bar{\beta}+\bar{\alpha}}$, where $\bar{\beta}+\bar{\alpha} < \bar{\alpha}$. In all cases, $ux_{i_1} \cdots x_{i_r} x_{\bar{\alpha}} \in \mathfrak{m}_1$ by our induction hypothesis, and the lemma is proved.

We shall call a weight λ of an $\mathfrak{a}$-module $\mathfrak{m}$ a *leading weight* of $\mathfrak{m}$ if there exists a nonzero vector u belonging to λ such that

$$ux_i = 0, \qquad 1 \leqq i \leqq m, \tag{21}$$

$$ux_{i_1} \cdots x_{i_r} = 0 \tag{22}$$

whenever $r > 0$ and the x_{i_j} belong to negative roots $\bar{\alpha}_j$ such that $\sum_{j=1}^{r} \bar{\alpha}_j = 0$. Even though the system of weights of an $\mathfrak{a}$-module $\mathfrak{m}$ may not admit a linear order relation, we shall call λ a *highest weight* of $\mathfrak{m}$ if $\lambda + \bar{\alpha}$ is not a weight for all roots $\bar{\alpha} > 0$.

We remark first that if λ is a highest weight of $\mathfrak{m}$, then λ is a leading weight of $\mathfrak{m}$. Obviously condition (21) is satisfied. If an expression of the form (22) is different from zero, then $ux_{i_1} \cdots x_{i_{r-1}} \neq 0$ belongs to the weight

$$\lambda + \bar{\alpha}_1 + \cdots + \bar{\alpha}_{r-1} = \lambda - \bar{\alpha}_r,$$

where $-\bar{\alpha}_r > 0$ since $-\bar{\alpha}_r$ corresponds to $-\alpha_r$, and this contradicts our assumption that λ is a highest weight.

It is possible to verify that the three dimensional simple modular Lie algebra $\mathfrak{l}$ of characteristic p obtained from the three dimensional unimodular Lie algebra of characteristic zero at a nonexceptional prime has exactly p inequivalent irreducible restricted representations (counting the trivial one dimensional representation), of degrees $1, 2, \cdots, p$. The representations of degree $1, 2, \cdots, p-1$ all have a highest weight, while the representation of degree p has a leading weight which is not a highest weight.

The significance of the concept of leading weight is clarified by the following result.

THEOREM 4. *Let $\mathfrak{m}$ be an irreducible $\mathfrak{a}$-module which possesses a leading weight λ. Then the dimension of $\mathfrak{m}_\lambda$ is equal to one. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be irreducible $\mathfrak{a}$-modules which have leading weights λ and λ' respectively. Then $\mathfrak{m}$ and $\mathfrak{m}'$ are $\mathfrak{a}$-isomorphic if and only if $\lambda=\lambda'$.*

Proof. Let $u\neq 0$ be a vector in $\mathfrak{m}$ belonging to λ which satisfies conditions (21) and (22). Since $\mathfrak{m}$ is irreducible, $\mathfrak{m}$ has a basis consisting of elements of the form (19), each of which is a weight vector. The first assertion of the theorem will be proved if we can show that any vector of the form (19) which has weight λ is a multiple of u. Actually we prove somewhat more, namely, that if $w=ux_{i_1}\cdots x_{i_r}$ is an element of the form (19) of weight λ, then $w=\bar{a}u$, where $\bar{a}$ is an element of $\overline{K}$ which depends only upon λ, and the sequence of root vectors $x_{i_1}, \cdots, x_{i_r}$, and not upon the action of $\mathfrak{a}$ upon $\mathfrak{m}$. Let $\bar{\beta}_1, \cdots, \bar{\beta}_r$ be the roots corresponding to $x_{i_1}, \cdots, x_{i_r}$. Then $\sum\bar{\beta}_i=0$. If all $\bar{\beta}_i<0$, then $w=0$ by (22). We have thus reduced the problem to the situation considered by Cartan and Weyl (see [13, p. 282]), so that if $w\neq 0$, then at least one of the $\bar{\beta}_i>0$. The argument of Cartan and Weyl, together with the properties (21) and (22) of a leading weight, can be applied to prove the first assertion.

Now let $\mathfrak{m}$ and $\mathfrak{m}'$ be irreducible $\mathfrak{a}$-modules having the same leading weight. The result established in the first part of the proof, and Weyl's method [13, p. 283] lead at once to the statement that $\mathfrak{m}$ and $\mathfrak{m}'$ are $\mathfrak{a}$-isomorphic. It is not completely trivial, however, to prove that if $\mathfrak{m}$ and $\mathfrak{m}'$ are $\mathfrak{a}$-isomorphic irreducible modules which possess leading weights λ and λ', then $\lambda=\lambda'$. Suppose that $\lambda\neq\lambda'$, and suppose that there exists an $\mathfrak{a}$-isomorphism S of $\mathfrak{m}'$ onto $\mathfrak{m}$. Let $u\neq 0$ belong to λ, and let $u'\neq 0$ belong to λ', where both u and u' satisfy the defining properties (21) and (22) of a leading weight. Then $u'S$ belongs to λ', and it follows that both λ and λ' are leading weights of $\mathfrak{m}$. Since $\mathfrak{m}$ is irreducible, by Lemma 6 and the remark after Theorem 3, there exist root vectors $x_{i_1}, \cdots, x_{i_r}$ belonging to negative roots such that $u_1=ux_{i_1}\cdots x_{i_r}$ is a nonzero element of $\mathfrak{m}_{\lambda'}$. Moreover $r>0$ since $\lambda\neq\lambda'$. Because λ' is a leading weight, and $\mathfrak{m}_{\lambda'}$ is one dimensional, it follows that $u_1x_i=0$, $1\leqq i\leqq m$. We can apply Lemma 6 again, and obtain negative root vectors $x_{j_1}, \cdots, x_{j_s}$, $s>0$, such that $ux_{i_1}\cdots x_{i_r}x_{j_1}\cdots x_{j_s}$ is a nonzero element of $\mathfrak{m}_\lambda$. This statement contradicts our assumption that λ is a leading weight, and the theorem is proved.

We emphasize that all the statement in Theorem 4 are valid if the words "leading weight" are replaced by "highest weight."

8. **The action of the Weyl group of $\mathfrak{l}$ upon the system of weights of an $\mathfrak{a}$-module.** The Weyl group of $\mathfrak{L}$ with respect to $\mathfrak{H}$ is the group of l.t. in the dual space $\mathfrak{H}^*$ of $\mathfrak{H}$ generated by the reflections S_α, where $\Lambda S_\alpha = \Lambda - \Lambda(H_\alpha)\alpha$, $\Lambda \in \mathfrak{H}^*$, and α is a root. It is known that the reflections determined by a fundamental system of roots generate the Weyl group, and that if α and β are roots, then αS_β is a root. Similarly we define the Weyl group of $\mathfrak{l}$ with respect to $\mathfrak{h}$ to be the group of l.t. in the dual $\mathfrak{h}^*$ of $\mathfrak{h}$ generated by the l.t. $s_{\bar\alpha}$, $\bar\alpha$ a root, where $\lambda s_{\bar\alpha} = \lambda - \lambda(h_{\bar\alpha})\bar\alpha$, and $h_{\bar\alpha} = H_\alpha T$. We observe that $s_{\bar\alpha}^2 = 1$ and that $s_{-\bar\alpha} = s_{\bar\alpha}$. Moreover, if $\bar\alpha$ and $\bar\beta$ are roots, then $\bar\alpha s_{\bar\beta}$ is a root. Since $\bar\alpha(h_{\bar\beta}) = \phi(\alpha(H_\beta)$ by (10), we have

$$\phi((\alpha S_\beta)(H_i)) = \phi(\alpha(H_i)) - \phi(\alpha(H_\beta))\phi(\beta(H_i)) = (\bar\alpha s_{\bar\beta})(H_i T)$$

for $1 \leq i \leq l$, proving that $\bar\alpha s_{\bar\beta}$ is the root of $\mathfrak{l}$ corresponding to the root αS_β of $\mathfrak{L}$.

The following result is based on a theorem of E. Cartan [3, p. 360] for representations of complex semi-simple algebras. As in the classical theory, a weight λ of an $\mathfrak{a}$-module $\mathfrak{m}$ is called *extreme* if it is impossible to find a root $\bar\alpha$ such that both $\lambda + \bar\alpha$ and $\lambda - \bar\alpha$ are weights.

THEOREM 5. *Let $\mathfrak{m}$ be an irreducible $\mathfrak{a}$-module. If $\mathfrak{m}$ has an extreme weight, then $\mathfrak{m}$ has a highest weight, and the Weyl group of $\mathfrak{l}$ acts transitively upon the set of extreme weights of $\mathfrak{m}$.*

Before giving the proof, we establish some preliminary results.

LEMMA 7. *If λ is a weight of an $\mathfrak{a}$-module $\mathfrak{m}$, then so is $\lambda s_{\bar\alpha}$ for every root $\bar\alpha$. If λ is extreme, then $\lambda s_{\bar\alpha}$ is extreme. If λ is extreme, and if $\lambda + \bar\alpha$ is a weight, then for any vector u belonging to λ, the weights belonging to $ux_{\bar\alpha}^i$, $i = 0, 1, \cdots$, where x is the root vector among the x_i belonging to $\bar\alpha$, include $\lambda s_{\bar\alpha}$.*

Proof(9). Since H_α is a linear combination of the H_i with coefficients in $Q \cap \mathfrak{o}$ for all roots α, it follows that $\lambda(h_{\bar\alpha}) = \lambda(H_\alpha T) \in \overline{K}_0$. If $\lambda + k\bar\alpha$ is a weight for all $k \in \overline{K}_0$ then $\lambda s_{\bar\alpha}$ is a weight since $\lambda(h_{\bar\alpha}) \in \overline{K}_0$. If not all $\lambda + k\bar\alpha$ are weights, then by Lemma 5.1 [12], the weights of this form lie in disjoint arithmetic progressions, each symmetric about $\lambda - 2^{-1}\lambda(h_{\bar\alpha})\bar\alpha$. Since λ and $\lambda s_{\bar\alpha}$ are symmetric, $\lambda s_{\bar\alpha}$ is a weight.

If $\lambda s_{\bar\alpha}$ is not extreme, then $\lambda s_{\bar\alpha} \pm \bar\beta$ are weights for some root $\bar\beta$. Applying $s_{\bar\alpha}$, and using the first statement of the lemma, we infer that $(\lambda s_{\bar\alpha} \pm \bar\beta)s_{\bar\alpha} = \lambda \pm \bar\beta s_{\bar\alpha}$ are both weights. But we have shown that $\bar\beta s_{\bar\alpha}$ is a root, hence λ is not extreme, and the second assertion is proved.

(9) This lemma is well known (see [13; 12]); we include the argument in order to emphasize those facts which we need for the proof of Theorem 5.

Finally let λ be extreme, and let $\lambda+\bar{\alpha}$ be a weight. If $u\neq 0$ belongs to λ, then $ux_{-\bar{\alpha}}=0$ since λ is extreme. We form $u_i=ux_{\bar{\alpha}}^i$, $i=0, 1, 2, \cdots$, and prove by induction that $u_ix_{-\bar{\alpha}}=c_iu_{i-1}$, where $c_i=-i\lambda(h_{\bar{\alpha}})-i(i-1)$. For some $r<p-1$ we have $u_r\neq 0$, $u_{r+1}=0$, and it follows that $c_{r+1}=-(r+1)\lambda(h_{\bar{\alpha}})-(r+1)r=0$. Since $r+1\neq 0$, $r=-\lambda(h_{\bar{\alpha}})$, and u_r belongs to $\lambda s_{\bar{\alpha}}$. This completes the proof.

LEMMA 8. *Let $\mathfrak{a}$ be the u-algebra of $\mathfrak{l}$. Then the subalgebra $\mathfrak{s}$ of $\mathfrak{a}$ generated by the root vectors x_i, $1\leq i\leq m$, belonging to the positive roots, is a nilpotent algebra.*

Proof. $\mathfrak{s}$ is the enveloping algebra of the subspace $\mathfrak{g}$ of $\mathfrak{l}$ generated by the x_i, $1\leq i\leq m$, and will be nilpotent by a result of Jacobson [11] if we can prove that $\mathfrak{g}$ is a (Lie) subalgebra of $\mathfrak{l}$ all of whose elements are nilpotent in $\mathfrak{a}$. Now $\mathfrak{g}=\mathfrak{G}T$, where $\mathfrak{G}$ is the $\mathfrak{o}$-submodule of Σ generated by the X_i, $1\leq i\leq m$. Since $[X_iX_j]$ is either zero or a multiple of a root vector belonging to a positive root, for $1\leq i, j\leq m$, $\mathfrak{G}$ is closed under the bracket operation, and hence $\mathfrak{g}$ is a subalgebra of $\mathfrak{l}$.

We prove now that a p-power of every element of $\mathfrak{G}$ is in $\mathfrak{X}$, the kernel of $\tilde{T}$. By (13), $X_i^p\in\mathfrak{X}$ for $1\leq i\leq m$. We shall use the identity (see [16, p. 91])

$$(X+Y)^p\equiv X^p+Y^p+s(X, Y) \pmod{\mathfrak{p}\mathfrak{B}} \tag{23}$$

where $X, Y\in\mathfrak{B}$, and $s(X, Y)$ is a sum of commutators of p-factors which are either X or Y. Now let $Y=\sum a_iX_i$ be an element of $\mathfrak{G}$; then from (23) we have

$$\begin{aligned} Y^p &\equiv \sum a_i^p X_i^p + Y^{(1)} \pmod{\mathfrak{p}\mathfrak{B}} \\ &\equiv Y^{(1)} \pmod{\mathfrak{X}}, \end{aligned}$$

where $Y^{(1)}\in\mathfrak{G}$, and $Y^{(1)}$ has the property that the minimum root α_i whose coefficient in $Y^{(1)}$ is not zero is greater than the minimum root whose coefficient in Y is not zero. If we iterate this process, and use the fact that the number of roots is finite, we obtain $Y^{p^t}\in\mathfrak{X}$ for some integer $t\geq 0$. This proves the lemma.

Proof of Theorem 5. Let λ be an extreme weight of $\mathfrak{m}$. We prove that there exists an elements s of the Weyl group of $\mathfrak{l}$ such that λs is a highest weight of $\mathfrak{m}$. Since $\mathfrak{m}$ is irreducible, it follows from Theorem 4 that $\mathfrak{m}$ has at most one highest weight, and we shall have proved that all the extreme weights of $\mathfrak{m}$ lie in one system of transitivity relative to the Weyl group, namely the one that contains a highest weight.

If λ is a highest weight, there is nothing to prove. Suppose that $\lambda+\bar{\alpha}$ is a weight for some $\bar{\alpha}>0$, and let $u\neq 0$ be a vector belonging to λ. By Lemma 7, there exists an integer $r\geq 0$ such that $ux_{\bar{\alpha}}^r$ belongs to $\lambda s_{\bar{\alpha}}$, which is again an extreme weight. We assert that $r>0$, for if $r=0$, $\lambda s_{\bar{\alpha}}=\lambda$, and the center of symmetry for the arithmetic progressions of weights of the form $\lambda+k\bar{\alpha}$ is λ. Therefore since $\lambda-\bar{\alpha}$ and $\lambda+\bar{\alpha}$ are symmetric about λ, $\lambda-\bar{\alpha}$ is a weight, contrary to our assumption that λ is extreme.

We now repeat the argument with $\lambda s_{\bar{\alpha}}$, and the vector $ux_{\bar{\alpha}}^r$, $r>0$, belonging to $\lambda s_{\bar{\alpha}}$. If a highest weight is not obtained by this process, then the construction yields products $x_{\bar{\alpha}_1}\cdots x_{\bar{\alpha}_r}\neq 0$, where the $\bar{\alpha}_i>0$, containing an arbitrarily large number of factors. But this is contrary to the fact that the subalgebra $\mathfrak{s}$ generated by the x_i, $1\leqq i\leqq m$, is nilpotent, by Lemma 8, and the theorem is proved.

9. **Every irreducible $\mathfrak{a}$-module with a leading weight is a constituent of a ϕ-module.** The main theorem can be stated as follows.

THEOREM 6. *Let $\mathfrak{m}$ be an irreducible $\mathfrak{a}$-module which has a leading weight $\lambda\neq 0$. Let Λ be the dominant integral function on H such that $\Lambda(H_i)$ is the rational integer, $0\leqq\Lambda(H_i)\leqq p-1$ such that $\phi(\Lambda(H_i))=\lambda(H_iT)$, $1\leqq i\leqq l$, and let $\mathfrak{M}$ be an irreducible $\mathfrak{A}$-module whose highest weight is Λ. Then $\mathfrak{m}$ is $\mathfrak{a}$-isomorphic to a composition factor of a ϕ-module $\mathfrak{M}_0/\mathfrak{M}_0\mathfrak{X}$ belonging to $\mathfrak{M}$.*

Proof. For simplicity we shall write h_i for H_iT, and H_i for X_{m+i}, $1\leqq i\leqq l$. Find h_{i_0}, $1\leqq i_0\leqq l$, such that $uh_{i_0}\neq 0$, where u is a fixed vector belonging to λ. Let $h=\lambda(h_{i_0})^{-1}h_{i_0}$; then $uh=u$. Let $e^{(j)}$ be the idempotent element of $\mathfrak{a}$ such that $ve^{(j)}=v$ for all v in $\mathfrak{m}$, which was constructed in the discussion preceding Lemma 4. Let $(0:u)=\{f\mid f\in\mathfrak{a},\ uf=0\}$. Then there exists $g\in(0:u)$ such that $e^{(j)}=h+g$. Let $g=\sum_{i\in I}\bar{a}_iz(P_i,\ Q_i,\ R_i)$, $\bar{a}_i\in\overline{K}$.

Let U be an element of weight Λ in $\mathfrak{M}$ such that the elements $UZ(0,0,R)$ generate $\mathfrak{M}_0$. Let $H=cH_{i_0}$, where $\phi(c)=\lambda(h_{i_0})^{-1}$; then $\phi(c\Lambda(H_{i_0}))=1$. Let $G=\sum_{i\in I}a_iZ(P_i,\ Q_i,\ R_i)$, where the a_i are elements of $\mathfrak{o}$ such that $\phi(a_i)=\bar{a}_i$, and let $E=H+G$; then $H\tilde{T}=h$, $G\tilde{T}=g$, and $E\tilde{T}=h+g=e^{(j)}$. By Lemma 4, it is sufficient to prove that $UE\notin\mathfrak{M}_0\mathfrak{X}$.

We write $Y_j=a_jZ(P_j,\ Q_j,\ R_j)$, and $y_j=\bar{a}_jz(P_j,\ Q_j,\ R_j)$; then $G=\sum_{j\in I}Y_j$; $g=\sum_{j\in I}y_j$. We define two subsets J and J' of I as follows:

$$J=\{\nu\mid\nu\in I,\ UY_\nu\neq 0,\ UY_\nu\in\mathfrak{M}_\lambda\},$$

$$J'=\{\nu\mid\nu\in I,\ uy_\nu\neq 0,\ uy_\nu\in\mathfrak{m}_\lambda\}.$$

We prove: (i) if $\nu\in J$ then $P_\nu=R_\nu=0$, and $Y_\nu=a_\nu Z(0,\ Q_\nu,\ 0)$; and (ii) $J'\subseteq J$. First we observe that if $P_\nu=R_\nu=0$, and if $Q_\nu=(j_1,\cdots,j_l)$, then

$$UZ(0,Q_\nu,0)=\Lambda(H_1)^{j_1}\cdots\Lambda(H_l)^{j_l}U$$

and

$$uz(0,\ Q_\nu,\ 0)=\lambda(h_1)^{j_1}\cdots\lambda(h_l)^{j_l}u=\phi(\Lambda(H_1)^{j_1}\cdots\Lambda(H_l)^{j_l})u \tag{24}$$

since $\phi(\Lambda(H_i))=\lambda(h_i)$.

Now let $\nu\in J'$, and consider $uy_\nu=\bar{a}_\nu uz(P_\nu,\ Q_\nu,\ R_\nu)$, $uy_\nu\in\mathfrak{m}_\lambda$, $uy_\nu\neq 0$. If $P_\nu\neq 0$, then $uy_\nu=0$. If $P_\nu=0$, $R_\nu\neq 0$, then

$$uy_\nu = \bar{a}_\nu \lambda(h_1)^{i_1} \cdots \lambda(h_l)^{i_l} uz(0, 0, R_\nu) \in m_\lambda,$$

and $uy_\nu = 0$ by (22), since λ is a leading weight of $\mathfrak{m}$. Therefore $P_\nu = R_\nu = 0$. Similarly if $\nu \in J$, then $P_\nu = R_\nu = 0$, proving (i). If $\nu \in J'$, then $UY_\nu = a_\nu UZ(0, Q_\nu, 0) \in \mathfrak{M}_\Lambda$, and by (24),

$$uz(0, Q_\nu, 0) = \phi(\Lambda(H_1)^{i_1} \cdots \Lambda(H_l)^{i_l})u \neq 0$$

and $a_\nu \neq 0$, hence $UY_\nu = a_\nu \Lambda(H_1)^{i_1} \cdots \Lambda(H_l)^{i_l} U \neq 0$, and (ii) is proved.

If $\nu \in J$, then $P_\nu = R_\nu = 0$ by (i), and hence $uy_\nu \in \mathfrak{m}_\lambda$.

Now let $Y = \sum_{\nu \in J} Y_\nu$; we prove that $UY \in \mathfrak{p}\mathfrak{M}_0 \subseteq \mathfrak{M}_0\mathfrak{X}$. By (i) we have $UY = dU$, where

$$d = \sum_{\nu \in J} a_\nu \Lambda(H_1)^{i_1} \cdots \Lambda(H_l)^{i_l}, \qquad Q_\nu = (j_1, \cdots, j_l).$$

Let $y = \sum_{\nu \in J} y_\nu$; then $uy \in \mathfrak{m}_\lambda$, and since $J' \subseteq J$ by (ii), uy is the component of ug of weight λ in the expression of ug as a sum of vectors belonging to distinct weights. Since $ug = 0$, $uy = 0$ because vectors belonging to distinct weights are linearly independent. On the other hand, $uy = \bar{e}u$, where

$$\bar{e} = \sum_{\nu \in J} \bar{a}\lambda(h_1)^{i_1} \cdots \lambda(h_l)^{i_l}, \qquad Q_\nu = (j_1, \cdots j_l),$$

and $\bar{e} = \phi(d) = 0$, and $d \in \mathfrak{p}$.

Now write $G = Y + Y'$, where $Y' = \sum_{\nu \in I-J} Y_\nu$. Since $E = H + G$ we have $UE \doteq UH + UY + UY' = (c\Lambda(H_{i_0}) + d)U + UY'$, and $c\Lambda(H_{i_0}) + d \equiv 1 \pmod{\mathfrak{p}}$. From the definition of J it follows that if UY' is expressed as an $\mathfrak{o}$-linear combination of the generators $UZ(0, 0, R)$ of $\mathfrak{M}_0$, the coefficient of U is zero. If $W \in \mathfrak{M}_0$, then although an expression $W \doteq \sum a_i UZ(0, 0, R_i)$, $a_i \in \mathfrak{o}$, is not uniquely determined, since U is the only generator of weight Λ, the coefficient of U is uniquely determined, and will be called the Λ-component of W. We have shown that the Λ-component of UE is $\equiv 1 \pmod{\mathfrak{p}}$. The theorem will be proved if we can show that the Λ-component of any element of $\mathfrak{M}_0\mathfrak{X}$ is in $\mathfrak{p}$, and this we shall do by using the generators of $\mathfrak{X}$ (see Lemma 2). An arbitrary element of $\mathfrak{M}_0\mathfrak{X}$ is a sum of terms of the following types, and it is sufficient to verify in each case that the Λ-component is in $\mathfrak{p}$.

(a) $W \in \mathfrak{p}\mathfrak{M}_0$ implies that the Λ-component is in $\mathfrak{p}$.

(b) $W = UFX_i^pG$, $F, G \in \mathfrak{B}$, $1 \leqq i \leqq m$; then $W \equiv UX_i^pFG \pmod{\mathfrak{p}\mathfrak{M}_0}$ by (17), and hence $W \equiv 0 \pmod{\mathfrak{p}\mathfrak{M}_0}$.

(c) $W = UF(H_i^p - H_i)G$, $1 \leqq i \leqq l$; then

$$\begin{aligned} W &\equiv U(H_i^p - H_i)FG \pmod{\mathfrak{p}\mathfrak{M}_0} \\ &\equiv (\Lambda(H_i)^p - \Lambda(H_i))UFG \pmod{\mathfrak{p}\mathfrak{M}_0} \\ &\equiv 0 \pmod{\mathfrak{p}\mathfrak{M}_0} \end{aligned}$$

by (17).

(d) $W = UFX_i^pG$, $m + l \leqq i \leqq n$; then

$$
\begin{aligned}
W &\equiv UFGX_i^p \pmod{\mathfrak{p}\mathfrak{M}_0} \\
&\equiv \sum a_k UZ(0, 0, R_k) X_i^p \pmod{\mathfrak{p}\mathfrak{M}_0}, \qquad a_k \in \mathfrak{o},
\end{aligned}
$$

and the Λ-component of $\sum a_k UZ(0, 0, R_k)X_i^p$ is zero. This completes the proof of the theorem.

REMARKS. In a subsequent paper we plan to show how a theorem analogous to Theorem 6, in combination with results of Seligman [12] and Harish-Chandra [7, Theorems 1 and 2], can be applied to prove that the Weyl matrix of a modular separable algebra determines the algebra up to (restricted) isomorphism, and that every separable algebra of characteristic p which satisfies certain conditions is isomorphic to a modular Lie algebra.

The following problem may be raised in connection with Theorem 6, but remains unsolved. Find necessary and sufficient conditions in order that a linear function λ on a Cartan subalgebra $\mathfrak{h}$ of a modular separable Lie algebra $\mathfrak{l}$ be a leading weight of an irreducible $\mathfrak{a}$-module, where $\mathfrak{a}$ is the u-algebra of $\mathfrak{l}$.

REFERENCES

1. E. Artin, C. J. Nesbitt, and R. M. Thrall, *Rings with minimum condition*, University of Michigan Publications in Mathematics, No. 1, 1944.
2. G. Birkhoff, *Representability of Lie groups and Lie algebras by matrices*, Ann. of Math. vol. 38 (1937) pp. 526–532.
3. E. Cartan, *Les groupes projectifs qui ne laissent invariante aucune multiplicité plane*, Oeuvres Completes, Partie I, vol. 1, pp. 355–398.
4. C. Chevalley, *An algebraic proof of a property of Lie groups*, Amer. J. Math. vol. 63 (1941) pp. 785–793.
5. F. Gantmacher, *Canonical representation of the automorphisms of a complex semi-simple Lie group*, Rec. Math. (Mat. Sbornik) N. S. vol. 5 (1939) pp. 101–144.
6. Harish-Chandra, *On representations of Lie algebras*, Ann. of Math. vol. 50 (1949) pp. 900–915.
7. ———, *On some applications of the universal enveloping algebra of a semi-simple Lie algebra*, Trans. Amer. Math. Soc. vol. 70 (1951) pp. 28–96.
8. G. Hochschild, *Representations of restricted Lie algebras of characteristic p*, Proc. Amer. Math. Soc. vol. 5 (1954) pp. 603–605.
9. N. Jacobson, *Restricted Lie algebras of characteristic p*, Trans. Amer. Math. Soc. vol. 50 (1941) pp. 15–25.
10. ———, *The theory of rings*, Mathematical Surveys, no. 2, New York, 1943.
11. ———, *Une generalisation du théorème d'Engel*, C.R. Acad. Sci. Paris vol. 234 (1952) pp. 679–681.
12. G. Seligman, *On Lie algebras of prime characteristic*, Memoirs of the American Mathematical Society, no. 19.
13. H. Weyl, *Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen* I, Math. Zeit. vol. 23 (1925) pp. 271–309.
14. ———, *Theorie der Darstellung* . . . II, Math. Zeit. vol. 24 (1926) pp. 328–376.
15. E. Witt, *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. vol. 177 (1937) pp. 152–160.
16. H. Zassenhaus, *Über Lie'sche Ringe mit Primzahlcharakteristik*, Abh. Math. Sem. Hansischen Univ. vol. 13 (1940) pp. 1–100.

UNIVERSITY OF WISCONSIN,
MADISON, WIS.