MODULAR LIE ALGEBRAS II

BY

CHARLES W. CURTIS

1. **Introduction.** Let $\mathfrak{g}$ be a Lie algebra over an algebraically closed field Ω of characteristic $p>7$, whose Killing form trace (ad x)(ad y) is nondegenerate. Seligman has proved that $\mathfrak{g}$ is a direct sum of simple Lie algebras, each of which has a nondegenerate Killing form, and is the analogue of one of the simple Lie algebras over the complex field. This analogy is sharpened by the main result of the present paper, which states that there exists a modular Lie algebra $\mathfrak{l}$ over the prime field Z_p in Ω, and an isomorphism H of $\mathfrak{l}$ into $\mathfrak{g}$ such that $\mathfrak{g}$ is obtained by extension of the base field to Ω from the image $\mathfrak{l}H$ of $\mathfrak{l}$ in $\mathfrak{g}$. The proof of the theorem is based upon the first part (§§1–5) of Seligman's thesis [5], on a theorem of Chevalley and Harish-Chandra [4] concerning the existence of a semi-simple Lie algebra over the complex field with a prescribed Weyl matrix, and on the construction of modular Lie algebras from semi-simple Lie algebras of characteristic zero given in [2]. The argument does not involve the explicit determination of the root systems of the algebras $\mathfrak{g}$ given by Seligman [5, §§6–14], and therefore provides a new approach to the problem of classifying the simple Lie algebras of characteristic $p>7$ with nondegenerate Killing forms. This application is outlined in the last section of the paper.

In brief, the contents of the paper are as follows. §2 is devoted to preliminary results. In §3, the concept of a simple system of roots is introduced, and the existence of a maximal simple system of roots of $\mathfrak{g}$ with respect to a Cartan subalgebra is established. Seligman proved this result by calculating all possible root systems. In §4, the Weyl matrix of $\mathfrak{g}$ relative to a maximal simple system of roots is defined, and it is proved that the Weyl matrix of $\mathfrak{g}$ is obtained from the Weyl matrix of a semi-simple Lie algebra $\mathfrak{L}$ over the complex field by reduction modulo p. It is then proved that the system of roots of $\mathfrak{L}$ is isomorphic in a certain sense to the system of roots of $\mathfrak{g}$. Chevalley's recent work [1] on simple groups makes it possible to give a more satisfactory approach to the construction of an admissible basis (see [2]) of $\mathfrak{L}$ than was outlined in [2]. In particular it is possible to select the rational field as a coefficient field in every case. This improvement is sketched in the last section, and the existence of a modular Lie algebra satisfying the requirements of the main theorem is proved.

The author is indebted to Dr. G. Seligman for reading an earlier draft of the manuscript.

Received by the editors July 18, 1956.

2. **Summary of known results.** The statements given without proof in this section are proved in §§1–5 of Seligman's paper [5]. Throughout the paper, $\mathfrak{g}$ denotes a Lie algebra over an algebraically closed field Ω of characteristic $p>7$ whose Killing form $(u, v) = \text{trace (ad } u)(\text{ad } v)$ is nondegenerate. We remark that the results of §§2.a, b, and the first part of §2.c are proved in [5] for any restricted Lie algebra $\mathfrak{g}$ over Ω which possesses a restricted representation $x \to U(x)$ for which the form $\text{trace}(U(x)U(y))$ is nondegenerate. Later we shall observe that the results of §§3 and 4 are actually valid for a Lie algebra satisfying this weaker condition.

2.a. Let $\mathfrak{c}$ be a Cartan subalgebra of $\mathfrak{g}$. For each linear function ρ on $\mathfrak{c}$, we let

$$\mathfrak{g}_\rho = \{u \mid u \in \mathfrak{g},\ [uc] = \rho(c)u \text{ for all } c \in \mathfrak{c}\}.$$

A linear function $\rho \neq 0$ such that $\mathfrak{g}_\rho \neq 0$ is called a *root* of $\mathfrak{g}$ (with respect to $\mathfrak{c}$), and the set of roots of $\mathfrak{g}$ will be denoted by $R(\mathfrak{g})$. Then $\mathfrak{g}$ is a vector space direct sum

$$\mathfrak{g} = \mathfrak{c} + \sum \mathfrak{g}_\rho.$$

The spaces $\mathfrak{g}_\rho$ are one dimensional. For each root ρ, $\pm\rho$ are the only multiples of ρ which are roots. For all roots ρ and σ we have

$$[\mathfrak{g}_\rho \mathfrak{g}_\sigma] = \mathfrak{g}_{\rho+\sigma}, \qquad \rho + \sigma \neq 0; \qquad [\mathfrak{g}_{-\rho}, \mathfrak{g}_\rho] \subseteq \mathfrak{c};$$
$$(\mathfrak{g}_\rho, \mathfrak{g}_\sigma) = 0, \qquad \rho + \sigma \neq 0; \qquad (\mathfrak{g}_\rho, \mathfrak{c}) = 0; \qquad (\mathfrak{g}_{-\rho}, \mathfrak{g}_\rho) \neq 0.$$

The results listed so far are Theorems 3.1, 3.2, 3.4, 5.1, 5.2, 5.3, and 5.5 of [5].

2.b. The restriction of the Killing form (u, v) to $\mathfrak{c}$ is nondegenerate; hence for each root ρ, there exists a unique element of $\mathfrak{c}$, which we shall denote by c_ρ', such that $(c_\rho', c) = \rho(c)$ for all c in $\mathfrak{c}$. For all roots ρ, we have

$$\rho(c_\rho') = (c_\rho', c_\rho') \neq 0,$$

by Theorem 4.2 of [5]. Moreover, by Corollary 3.2 of [5],

$$[e_{-\rho}, e_\rho] = (e_{-\rho}, e_\rho)c_\rho' \tag{1}$$

for all roots ρ, and for arbitrary $e_{-\rho}$ in $g_{-\rho}$, e_ρ in $\mathfrak{g}_\rho$. For each root ρ, we set $c_\rho = 2(c_\rho', c_\rho')^{-1}c_\rho'$; then $\rho(c_\rho) = 2$.

2.c. The prime field Z_p in Ω may be identified with $Z/(p)$, where Z is the ring of rational integers, and p is the characteristic of Ω. We shall write r^* for the image of an element r in Z under the natural mapping of $Z \to Z_p$; however, to simplify the notation, we shall frequently write 2, $2^2 = 4$, etc. for the images in Z_p of the powers of 2.

For each pair of roots (ρ, σ), $\rho \neq \sigma$, there exist uniquely determined rational integers $r_{\rho,\sigma}$ and $s_{\rho,\sigma}$ such that $-3 \leqq r_{\rho,\sigma} \leqq 0 \leqq s_{\rho,\sigma} \leqq 3$, with the property that for any integer k between $\pm(p-1)/2$, $\rho + k^*\sigma$ is a root if and only if $r_{\rho,\sigma} \leqq k \leqq s_{\rho,\sigma}$. It is known that for each pair of roots ρ, σ,

$$-r_{\rho,\sigma} + s_{\rho,\sigma} \leqq 3,$$

and that(1)

$$\rho(c_\sigma) = \frac{2(c_\rho', c_\sigma')}{(c_\sigma', c_\sigma')} = -(r^*_{\rho,\sigma} + s^*_{\rho,\sigma}) \in \{0, \pm 1^*, \pm 2^*, \pm 3^*\}. \tag{2}$$

The roots of the form $\rho + k^*\sigma$ form an arithmetic progression, symmetric about $\rho - \rho(c_\sigma)\sigma/2$. Since ρ and $\rho - \rho(c_\sigma)\sigma$ are symmetric about $\rho - \rho(c_\sigma)\sigma/2$, it follows that $\rho - \rho(c_\sigma)\sigma$ is a root. We define a linear transformation s_σ acting in the dual space $\mathfrak{c}^*$ of $\mathfrak{c}$ by

$$s_\sigma: \lambda \to \lambda - \lambda(c_\sigma)\sigma, \qquad \lambda \in \mathfrak{c}^*.$$

Then each of these transformations maps $R(\mathfrak{g})$ into itself.

We shall need the following explicit formula for (c_ρ', c_ρ'). If we compute $(c_\rho', c_\rho') = \text{trace } (adc_\rho')^2$ relative to any basis of $\mathfrak{g}$ consisting of a basis of $\mathfrak{c}$ together with elements $e_\rho \in \mathfrak{g}_\rho$ for each root ρ, then we obtain(2)

$$(c_\rho', c_\rho') = \sum_{\sigma \in R(\mathfrak{g})} \sigma(c_\rho')^2. \tag{3}$$

Substitution of (2) in the right hand side of (3) yields the formula

$$(c_\rho', c_\rho') = \frac{1}{4} \sum_\sigma (r^*_{\sigma,\rho} + s^*_{\sigma,\rho})^2 (c_\rho', c_\rho')^2. \tag{4}$$

Since $(c_\rho', c_\rho') \neq 0$, we obtain

$$(c_\rho', c_\rho') = 4\Big(\sum_\sigma (r^*_{\sigma,\rho} + s^*_{\sigma,\rho})^2\Big)^{-1}.$$

3. **Simple systems of roots**(3). A nonempty set $\Delta \subseteq R(\mathfrak{g})$ is called a *simple system of roots* if and only if the difference of any two elements of Δ is not a root. A *chain* of roots (from Δ) $C = C(\rho_1, \cdots, \rho_r)$ is an ordered set of roots $(\rho_1, \cdots, \rho_r)$, $\rho_i \in \Delta$, such that for each k, $1 \leqq k \leqq r$, $\sum_{i \leqq k} \rho_i$ is a root; the roots ρ_i, $1 \leqq i \leqq r$, are called the *links* of the chain; the number of times a root $\rho \in \Delta$ appears in a chain C is called the multiplicity of ρ in C; and the total number of links in C is called the *length* of C. The roots $\sum_{i \leqq k} \rho_i$, $1 \leqq k \leqq r$, are said to be *generated* by the chain C; a root ρ is generated by a chain of length r if there is at least one chain $C(\rho_1, \cdots, \rho_r)$ such that $\rho = \sum_{i=1}^r \rho_i$. The set of

(1) Because 0 is not counted as a root, we define $r_{\rho,\rho} = -2$ and $s_{\rho,\rho} = 0$ for all roots ρ, so that formula (2) is valid in all cases.

(2) It is in the derivation of formula (3), and hence in the applications of this formula which appear later in the paper (see Proposition 6) that the assumption that the Killing form of $\mathfrak{g}$ be nondegenerate is used in an essential way.

(3) The proofs of the results in §§3 and 4 (Propositions 1–5) make no use of formula (3), and consequently are valid for any restricted Lie algebra $\mathfrak{g}$ over Ω with a restricted representation $x \to U(x)$ such that the form trace $U(x)U(y)$ is nondegenerate.

all roots generated by chains with links in a simple system Δ will be denoted by $\Gamma(\Delta)$.

We shall derive some elementary properties of chains. Once for all we select basis elements u_ρ for the root spaces $\mathfrak{g}_\rho$ such that for every root ρ,

$$[u_{-\rho}, u_\rho] = c_\rho;$$

that such a choice is possible follows from (1). The results of 2.a imply that if $C(\rho_1, \cdots, \rho_r)$ is a chain, then $[\cdots [u_{\rho_1}, u_{\rho_2}] \cdots u_{\rho_r}]$ is a nonzero multiple of u_ρ where $\rho = \sum_1^r \rho_i$.

LEMMA 1. *Let Δ be a simple system such that $\rho \in \Delta$ implies $-\rho \notin \Gamma(\Delta)$. Let ρ and σ be roots in $\Gamma(\Delta)$ which are generated by chains of lengths r and s respectively. If $[u_\rho u_\sigma] \neq 0$, then $\rho+\sigma$ is a root; and if $\rho+\sigma$ is a root, then $\rho+\sigma \in \Gamma(\Delta)$ and is generated by at least one chain of length $r+s$.*

Proof. We use induction on s. Both statements are obvious if $s=1$, because of the hypothesis of the Lemma. Assume that $s>1$, and that both results hold for all pairs of roots ρ', σ', where σ' is generated by a chain of length less than or equal to $s-1$. The root vector u_σ is a nonzero multiple of $[u_{\sigma'}, u_\tau]$ where σ' is a root generated by a chain of length $s-1$, and $\tau \in \Delta$. Now suppose that

$$0 \neq [u_\rho u_\sigma] = \alpha[u_\rho [u_{\sigma'}, u_\tau]] = \alpha[[u_\rho u_{\sigma'}] u_\tau] + \alpha[u_{\sigma'} [u_\rho u_\tau]], \tag{5}$$

where $\alpha \neq 0$ is in Ω. If $\rho+\sigma$ is not a root, then $\rho+\sigma=0$, and the results of §2.a imply that both summands on the right are in $\mathfrak{c}$. If the first is different from zero, then the induction hypothesis implies that $\rho+\sigma' \in \Gamma(\Delta)$, and $(\rho+\sigma')+\tau = 0$, contrary to the hypothesis of the lemma. If the second is not zero, then $\rho+\tau \in \Gamma(\Delta)$, and $(\rho+\tau)+\sigma' = 0$ contradicts the induction hypothesis. Thus we may assume that $\rho+\sigma$ is a root. Then by the hypothesis of the Lemma, $\rho+\tau \neq 0$, and hence either $\rho+\tau$ is a root; or $\rho+\tau$ is neither zero nor a root, and $[u_\rho u_\tau] = 0$. If $\rho+\tau$ is a root, then $\rho+\sigma = (\rho+\tau)+\sigma' \in \Gamma(\Delta)$ and is generated by a chain of length $(r+1)+(s-1)$, by the induction hypothesis. If on the other hand, $[u_\rho u_\tau] = 0$, then $[u_\rho u_{\sigma'}] \neq 0$, and by the induction hypothesis, $\rho+\sigma' \in \Gamma(\Delta)$, and is generated by a chain of length $r+s-1$. Then $\rho+\sigma = (\rho+\sigma')+\tau$ is generated by a chain of length $r+s$, and the proof is complete.

REMARK. The proof of Lemma 1 establishes the further result that $\rho+\sigma$ is generated by a chain whose links are the combined links of the chains generating ρ and σ.

LEMMA 2. *Let Δ be a simple system such that $\rho \in \Delta$ implies $-\rho \notin \Gamma(\Delta)$. Then $\tau \in \Gamma(\Delta)$ implies $-\tau \notin \Gamma(\Delta)$.*

Proof. Suppose, to the contrary, that τ and $-\tau$ both belong to $\Gamma(\Delta)$. Then $[u_{-\tau} u_\tau] \neq 0$, and $-\tau+\tau=0$ in contradiction to Lemma 1.

LEMMA 3. *Let $C = C(\rho_1, \cdots, \rho_r)$ and $C' = C(\rho_1', \cdots, \rho_s')$ be chains with*

links in a simple system Δ *such that* $\rho\in\Delta$ *implies* $-\rho\notin\Gamma(\Delta)$. *If* $\sum_{i\leq r}\rho_i = \sum_{i\leq s}\rho_i'$, *then* $r=s$, *and for all* $\rho\in\Delta$, *the multiplicity of* ρ *in* C *is equal to the multiplicity of* ρ *in* C'.

Proof. If $r=1<s$, then $\rho_1-\rho_s' = \sum_{j\leq s-1}\rho_j'$ is a root, contrary to our assumption that Δ is a simple system. To prove that $r=s$, it is sufficient to prove that if both r and s are greater than one, then there exist chains of lengths $r-1$ and $s-1$ respectively which generate the same root, and which are obtained from the original chains by deleting a single root. Because $\sum_1^r\rho_i = \sum_1^s\rho_i'$, the fact that the root spaces are one dimensional implies that

$$w = [\cdots[u_{\rho_1}u_{\rho_2}]\cdots u_{\rho_r}] = \alpha[\cdots[u_{\rho_1'}u_{\rho_2'}]\cdots u_{\rho_s'}], \qquad \alpha\in\Omega.$$

Then by 2.a, $[wu_{-\rho_s'}]$ is not zero, and belongs to $\mathfrak{g}_{\rho'}$, where $\rho'=\sum_1^{s-1}\rho_i'$ is a root. On the other hand, ad $u_{-\rho_s'}$: $w\to[wu_{-\rho_s'}]$ is a derivation, and we obtain

$$0\neq[wu_{-\rho_s'}] = \sum_{i=1}^{r}[\cdots[u_{\rho_1}u_{\rho_2}]\cdots u_{\rho_{i-1}}]u^*_{\rho_i}]u_{\rho_{i+1}}]\cdots u_{\rho_r}], \tag{6}$$

where since $\rho_i-\rho_s'$ is not a root,

$$u^*_{\rho_i} = [u_{\rho_i}u_{-\rho_s'}] = \begin{cases}0 & \text{if } \rho_i\neq\rho_s',\\ c_i\in\mathfrak{c} & \text{if } \rho_i=\rho_s'.\end{cases} \tag{7}$$

By 2.a, the terms on the right side of (6) must either belong to root spaces $\mathfrak{g}_\rho$ or to $\mathfrak{c}$. Because $\mathfrak{g}$ is a vector space direct sum of $\mathfrak{c}$ and the spaces $\mathfrak{g}_\rho$, it follows from the fact that $[wu_{-\rho_s'}]\in\mathfrak{g}_{\rho'}$ that for some i, $1\leqq i\leqq r$, and for some $c_i\in\mathfrak{c}$ defined by (7), we have

$$0\neq(\rho_1+\cdots+\rho_{i-1})(c_i)[\cdots[u_{\rho_1}u_{\rho_2}]\cdots u_{\rho_{i-1}}]u_{\rho_{i+1}}]\cdots u_{\rho_r}]\in\mathfrak{g}_{\rho'}. \tag{8}$$

By (8) and Lemma 1, we infer that ρ' is generated by the chains $C_1'(\rho_1',\cdots,\rho_{s-1}')$ and $C_1(\rho_1,\cdots,\rho_{i-1},\rho_{i+1},\cdots,\rho_r)$ of lengths $s-1$ and $r-1$ respectively, both of which are obtained by deleting ρ_s' from the original chains. Therefore $r=s$. Since we may assume by induction that the multiplicities of any root ρ in Δ in the chains of lengths $r-1$ and $s-1$ are equal, the statement concerning the multiplicities is also proved.

If Δ is a simple system of roots, then we shall denote the set of roots $\{-\rho\,|\,\rho\in\Delta\}$ by Δ^-. Then Δ^- is a simple system. Now we shall prove, by an argument similar to one given by Dynkin [3], that there exists a simple system of roots Δ which satisfies the hypotheses of Lemmas 1, 2, and 3, and which has the property that every root of $\mathfrak{g}$ relative to $\mathfrak{c}$ belongs either to $\Gamma(\Delta)$ or $\Gamma(\Delta^-)$.

Seligman has proved (see [5, p. 20]) that there exists a system of $l=\operatorname{rank}\mathfrak{g}=\dim\mathfrak{c}$ linearly independent roots $\epsilon_1,\cdots,\epsilon_l$ of $\mathfrak{g}$ with respect to $\mathfrak{c}$. Then $c_{\epsilon_1}',\cdots,c_{\epsilon_s}'$ and hence $c_{\epsilon_1},\cdots,c_{\epsilon_l}$ form a basis of $\mathfrak{c}$, so that a root ρ is uniquely determined by the numbers $\rho(c_{\epsilon_i})$, $1\leqq i\leqq l$. By formula (2), the num-

bers $\rho(c_{\epsilon_i}) \in \{0^*, \pm 1^*, \pm 2^*, \pm 3^*\}$, $1 \leqq i \leqq l$. We shall introduce a lexicographic order among the roots of $\mathfrak{g}$ based upon the ordered set $\epsilon_1, \cdots, \epsilon_l$ as follows. For each root ρ, let $\rho^{(i)}$ be the natural number $0, \pm 1, \pm 2, \pm 3$ according as $\rho(c_{\epsilon_i})$ is $0^*, \pm 1^*, \pm 2^*, \pm 3^*$; then $\rho^{(i)}$ is uniquely determined since the characteristic of Ω is greater than 7. We define $\rho < \sigma$ if the first nonzero difference $\sigma^{(i)} - \rho^{(i)}$ is positive, and shall call ρ positive ($\rho > 0$) if the first nonzero $\rho^{(i)}$ is positive. We summarize some simple properties of the order relation.

LEMMA 4. *The order relation $\rho < \sigma$ introduced among the roots of $\mathfrak{g}$ has the following properties.*

(i) *the principle of trichotony holds;*

(ii) *$\rho < \sigma$, $\sigma < \tau$ implies $\rho < \tau$;*

(iii) *if $\rho > 0$, $\sigma > 0$, and if $\rho + \sigma$ is a root, then $\rho + \sigma > 0$;*

(iv) *$\rho < 0$ if and only if $-\rho < 0$;*

(v) *if ρ, σ, and $\rho - \sigma$ are roots, then $\rho > \sigma$ if and only if $\rho - \sigma > 0$; and*

(vi) *the roots belonging to a sequence $\{\rho_i\}$ such that*

$$\rho_1 > \rho_2 > \rho_3 > \cdots$$

are distinct, and any such sequence is finite.

Proof. (i) is clear since a root is uniquely determined by the ordered set of natural numbers $(\rho^{(1)}, \cdots, \rho^{(l)})$; (ii) follows from the observation that for each i, $\tau^{(i)} - \rho^{(i)} = (\tau^{(i)} - \sigma^{(i)}) + (\sigma^{(i)} - \rho^{(i)})$. (iii), (iv), and (v) follow from the fact that if $\rho \pm \sigma$ is a root (where to include (iv), ρ may be zero) then $(\rho \pm \sigma)^{(i)} = \rho^{(i)} \pm \sigma^{(i)}$. The finiteness of the properly descending chain (vi) is a consequence of the fact that there exist only a finite number of roots; this descending chain condition is of course equivalent to the statement that the roots are well ordered, in the sense that every set of roots contains a root which is less than all the other roots in the set.

Now we shall prove the main result of this section. We might remark that this proof, based upon Lemma 1, and applied to semi-simple Lie algebras of characteristic zero, is a slight variation of the usual proof of the corresponding result.

PROPOSITION 1. *There exists a simple system of roots Δ of $\mathfrak{g}$ with respect to $\mathfrak{c}$ with the following properties:*

(i) $\Gamma(\Delta) \cap \Gamma(\Delta^-) = \phi$;

(ii) $R(\mathfrak{g}) = \Gamma(\Delta) \cup \Gamma(\Delta^-)$.

Proof. Following Dynkin [3], a positive root ρ is called *simple* if ρ cannot be expressed as the sum of two positive roots. There exist simple roots, for example the least positive root ρ with respect to the order relation, which exists by Lemma 4, (vi). In fact, $\rho = \rho_1 + \rho_1'$, where ρ_1 and ρ_1' are positive, implies, since $\rho - \rho_1 = \rho_1'$ is a positive root, that $\rho_1 < \rho$, by Lemma 4, (v), and hence

ρ is a simple root. The set of all simple roots will be denoted by Δ; by Lemma 4, Δ is a simple system.

Since the simple roots are positive, the roots belonging to $\Gamma(\Delta)$ are also positive, by Lemma 4, (iii). Similarly the roots belonging to $\Gamma(\Delta^-)$ are negative, by Lemma 4, (iv), and hence $\Gamma(\Delta)$ and $\Gamma(\Delta^-)$ have no roots in common.

Finally, every root will belong to $\Gamma(\Delta)\cup\Gamma(\Delta^-)$ if we can prove that every positive root ρ belongs to $\Gamma(\Delta)$. This we shall do using induction on the order relation we have introduced among the roots. We have already shown that the least positive root belongs to Δ. Now assume that every positive root $\sigma<\rho$ belongs to $\Gamma(\Delta)$. If ρ is not simple, then $\rho=\sigma+\tau$, where σ and τ are both positive roots which are less than ρ. By our induction hypothesis, σ and τ belong to $\Gamma(\Delta)$, and ρ belongs to $\Gamma(\Delta)$ by an application of Lemma 1.

DEFINITION. A simple system of roots Δ satisfying (i) and (ii) of Proposition 1 will be called a *maximal simple system* of roots. A set Δ of roots is *decomposable* if $\Delta=\Delta'\cup\Delta''$, where Δ' and Δ'' are *orthogonal* in the sense that $\rho'(c_{\rho''})=\rho''(c_{\rho'})=0$ for all $\rho'\in\Delta'$, $\rho''\in\Delta''$; otherwise Δ is said to be *indecomposable*. If Δ' and Δ'' are orthogonal then we shall write $\Delta'\perp\Delta''$. Evidently orthogonal sets of roots are disjoint.

PROPOSITION 2. *The dimension of the space spanned by any maximal simple system of roots is l, where $l=\dim \mathfrak{c}=\operatorname{rank}\mathfrak{g}$.*

Much later (in §5) it is proved under stronger assumptions that the number of roots in a maximal simple system is exactly l.

Proof. Lemma 5.4 of [5] implies, since $[\mathfrak{g}\mathfrak{g}]=\mathfrak{g}$, that there exist $l=\dim\mathfrak{c}$ linearly independent roots $\epsilon_1, \cdots, \epsilon_l$ of $\mathfrak{g}$ with respect to $\mathfrak{c}$. Let Δ be any maximal simple system of roots. By Proposition 1, the ϵ_i are all linear combinations of the elements of Δ with coefficients in Ω. Hence the linear space spanned by the elements of Δ has dimension l, and the assertion of Proposition 2 is proved.

PROPOSITION 3. *Let Δ be a maximal simple system of roots of $\mathfrak{g}$. Then there exist indecomposable, mutually orthogonal, simple systems of roots $\Delta_i\subseteq\Delta$ such that $\Delta=\bigcup_{i=1}^s\Delta_i$. If $i\neq j$ then $\Gamma(\Delta_i)\perp\Gamma(\Delta_j)$, and $\Gamma(\Delta)=\bigcup_{i=1}^s\Gamma(\Delta_i)$. For each i, $\Gamma(\Delta_i)\cup\Gamma(\Delta_i^-)$ is the complete set of roots of an ideal $\mathfrak{g}_i$ in $\mathfrak{g}$ such that $\mathfrak{g}=\mathfrak{g}_1\oplus\cdots\oplus\mathfrak{g}_s$. The ideals $\mathfrak{g}_i$ are simple Lie algebras.*

Proof. It is immediate that $\Delta=\bigcup_{i=1}^s\Delta_i$, where the Δ_i are indecomposable and mutually orthogonal, and that $\Gamma(\Delta_i)\perp\Gamma(\Delta_j)$ if $i\neq j$. Now suppose, in the hope of arriving at a contradiction, that $\bigcup_{i=1}^s\Gamma(\Delta_i)$ is properly contained in $\Gamma(\Delta)$. Then there will exist a chain $C(\rho_1, \cdots, \rho_k)$, $\rho_i\in\Delta$, such that $\rho_1, \cdots, \rho_{k-1}\in\Delta_i$ and $\rho_k\in\Delta_j$ for some $j\neq i$. Then $\sum_{i\leq k}\rho_i\notin\bigcup_{i=1}^s\Gamma(\Delta_i)$ by the uniqueness of the links of the chain $C(\rho_1, \cdots, \rho_k)$ proved in Lemma 3. Clearly $k>1$, and if $\sigma=\sum_{i\leq k-1}\rho_i$, then σ is orthogonal to ρ_k. Since $\sigma+\rho_k$ is a root and $\sigma(c_{\rho_k})=0$, the results stated in §2.c imply that $\sigma-\rho_k$ is a root, and hence

$$[u_\sigma u_{-\rho_k}] = [[\cdots [u_{\rho_1} u_{\rho_2}] \cdots u_{\rho_{k-1}}] u_{-\rho_k}] \neq 0.$$

But $\rho_k \notin \Delta_i$, hence $[u_{\rho_i} u_{-\rho_k}] = 0$ for $1 \leqq i \leqq k-1$. These statements are contradictory, and hence $\Gamma(\Delta) = \bigcup_{i=1}^{s} \Gamma(\Delta_i)$.

Now let $\mathfrak{g}_i$ be the subspace of $\mathfrak{g}$ spanned by the elements u_ρ, c'_ρ, $\rho \in \Gamma(\Delta_i) \cup \Gamma(\Delta_i^-)$. It is easy to prove that $\mathfrak{g}_i$ is an ideal in $\mathfrak{g}$ with Cartan subalgebra $\mathfrak{c}_i$ spanned by the c'_ρ, $\rho \in \Gamma(\Delta_i) \cup \Gamma(\Delta_i^-)$, and that Δ_i is a maximal simple system of roots of $\mathfrak{g}_i$ with respect to $\mathfrak{c}_i$. Then $\mathfrak{g}$ is the direct sum of the $\mathfrak{g}_i$, and the $\mathfrak{g}_i$ are simple algebras. These facts have been established by Seligman [5, Theorem 15.2] in a context which is applicable to the present situation, and we shall not give the proofs here.

4. **Existence of a semi-simple Lie algebra of characteristic zero whose root diagram is isomorphic to the root diagram of $\mathfrak{g}$.**

PROPOSITION 4. *Let $\Delta = (\rho_1, \cdots, \rho_m)$ be a maximal simple system of roots of $\mathfrak{g}$. Then there exists a uniquely determined m by m matrix (a_{ij}) with integer coefficients a_{ij} such that* (1) $a_{ij}^* = -\rho_i(c_{\rho_j})$, $|a_{ij}| \leqq 3$, $a_{ii} = -2$, $a_{ij} \geqq 0$ *if $i \neq j$, and $a_{ij} = 0$ if and only if $a_{ji} = 0$. This matrix has the further properties:* (2) *the group W generated by the linear transformations S_i, $1 \leqq i \leqq m$, and defined by $x_i S_j = x_i + a_{ij} x_j$, $1 \leqq i \leqq m$, is finite, and* (3), $\det(a_{ij}) \neq 0$.

Proof. We shall call the matrix $(-\rho_i(c_{\rho_j}))$, $1 \leqq i, j \leqq m$, the *Weyl matrix* of $\mathfrak{g}$ associated with Δ. By (2), §2, there exists a matrix (a_{ij}) with integer coefficients such that $a_{ij}^* = -\rho_i(c_{\rho_j})$, and $|a_{ij}| \leqq 3$, $a_{ii} = -2$. Since Δ is a simple system, (2) implies that $a_{ij} \geqq 0$ if $i \neq j$. Since the characteristic of Ω is greater than 5, the matrix (a_{ij}) is uniquely determined by these properties. The last statement of (1) is a consequence of the fact that $\rho_i(c_{\rho_j})$ is a nonzero multiple of $\rho_j(c_{\rho_i})$.

Now let V be a vector space of dimension m over the real field, and let $x_1, \cdots, x_m$ be a basis of V. Let us define linear functions $\Lambda_1, \cdots, \Lambda_m$ on V by the equations $\Lambda_i(x_j) = -a_{ji}$, $1 \leqq i, j \leqq m$, then the linear transformations S_i defined in the statement of Proposition 4 are given by

$$xS_i = x - \Lambda_i(x) x_i, \quad x \in V, \qquad 1 \leqq i \leqq m. \tag{9}$$

By Proposition 1, every root of $\mathfrak{g}$ with respect to $\mathfrak{c}$ is either generated by a chain C or is the negative of such a root. To each root ρ in $\Gamma(\Delta)$ generated by the chain $C(\rho_{i_1}, \cdots, \rho_{i_r})$ we assign the vector $X(\rho) = x_{i_1} + \cdots + x_{i_r}$ in V; to the root ρ in $\Gamma(\Delta^-)$ we assign the vector $X(\rho) = -X(-\rho)$. Because $\Gamma(\Delta) \cap \Gamma(\Delta^-) = \phi$ by Proposition 1, and because the multiplicity with which ρ in Δ appears in the chain C is uniquely determined by Lemma 3, we conclude that the mapping $\rho \to X(\rho)$ is a single valued mapping of $R(\mathfrak{g})$ into V.

We prove next that if ρ, σ, and $\rho + \sigma$ are roots, then

$$X(\rho + \sigma) = X(\rho) + X(\sigma). \tag{10}$$

By the remark following Lemma 1, and the definition of the vectors $X(\rho)$,

(10) is valid provided that both ρ and σ belong to either $\Gamma(\Delta)$ or $\Gamma(\Delta^-)$. For the other case, we may assume that $\rho\in\Gamma(\Delta)$, and $\sigma\in\Gamma(\Delta^-)$. We use induction on the length of a chain generating $-\sigma$. If that length is one, so that $-\sigma=\sigma_1\in\Delta$, then

$$u_{\rho-\sigma_1} = \xi[u_\rho u_\sigma] = \xi[u_\rho u_{-\sigma_1}], \qquad \xi\in\Omega,$$

and as in the proof of Lemma 3, it follows that $\rho-\sigma_1$ is generated by a chain whose links are the links of a chain generating ρ with the exception of a single σ_1. Thus (10) holds in this case. If the length is greater than one, then $\sigma=-(\sigma'+\rho')$, $\rho'\in\Delta$, $\sigma'\in\Gamma(\Delta)$, where σ' is generated by a shorter chain than σ. Then

$$u_{\rho+\sigma} = \xi[u_\rho[u_{-\sigma'}u_{-\rho'}]] = \xi[[u_\rho u_{-\sigma'}]u_{-\rho'}] + \xi[u_{-\sigma'}[u_\rho u_{-\rho'}]],$$

where $\xi\in\Omega$. Since the root spaces $\mathfrak{g}_\rho$ are one dimensional, $u_{\rho+\sigma}$ must be a multiple of one summand or the other. In the first case, $\rho-\sigma'$ is a root, and by induction we have

$$X(\rho-\sigma') = X(\rho) + X(-\sigma').$$

By the first part of the argument,

$$\begin{aligned} X(\rho+\sigma) &= X(\rho-\sigma') + X(-\rho') = X(\rho) + X(-\sigma') + X(-\rho') \\ &= X(\rho) + X(\sigma). \end{aligned}$$

The argument in the second case is similar, and will be omitted. Thus (10) is valid in general.

Because $a_{ii}=-2$, we have $S_i^2=1$, $1\leqq i\leqq m$, and the S_i generate a group of linear transformations. Since $x_1, \cdots, x_m$ form a basis of V, the finiteness of this group will follow if we can prove that the set $\{X(\rho)\,|\,\rho\in R(g)\}$ is mapped into itself by all the linear transformations S_i. For this it is sufficient to prove that if $\rho\in\Gamma(\Delta)$ then

$$X(\rho)S_i = X(\rho s_{\rho_i}), \qquad 1\leqq i\leqq m, \tag{11}$$

where s_{ρ_i} is the reflection $\lambda\to\lambda-\lambda(c_{\rho_i})\rho_i$ investigated in §2.c. We recall that ρs_{ρ_i} is a root whenever ρ is a root. To prove (11), first assume that $\rho=\rho_j\in\Delta$. Then $X(\rho_j)S_j = -X(\rho_j)$. If $i\neq j$, then $X(\rho_j)S_i = X(\rho_j) - \Lambda_i(X(\rho_j))x_i = x_j+a_{ji}x_i$. Since ρ_j, $\rho_j+\rho_i$, $\cdots$, $\rho_j+a_{ji}^*\rho_i=\rho_j s_{\rho_i}$ are roots([4]), it follows that $x_j+a_{ji}x_i=X(\rho_j s_{\rho_i})$. If $\rho\in\Gamma(\Delta)$ is generated by a chain of length greater than one, then $\rho=\sigma+\rho'$, where $\rho'\in\Delta$, and σ is generated by a shorter chain than ρ. Assuming by induction that (11) holds for σ, we have, by two applications of (10),

$$\begin{aligned} X(\rho)S_i &= (X(\sigma) + X(\rho'))S_i = X(\sigma s_{\rho_i}) + X(\rho' s_{\rho_i}) \\ &= X((\sigma+\rho')s_{\rho_i}) = X(s_{\rho_i}). \end{aligned}$$

([4]) Cf. [5, Theorem 5.7].

This completes the proof that the group W is finite.

In order to prove that $\det(a_{ij}) \neq 0$, we observe first that since the linear transformations belonging to W have real coefficients, it follows (see [6, p. 153]) that there exists a positive definite quadratic form $Q(x)$ on the vector space V such that the operations of W are orthogonal transformations relative to the form Q. The bilinear form $\beta(x, y) = Q(x+y) - Q(x) - Q(y)$ associated with Q is nondegenerate, and has the property that $\beta(x, x) = 2Q(x) \neq 0$ whenever $x \neq 0$. By (9) the operations S_i of W are reflections in the hyperplanes E_i: $\Lambda_i(x) = 0$, and the vectors x_i have the property that $x_i S_i = -x_i$. We shall prove that

$$\Lambda_i(x) = 2\beta(x, x_i)\beta(x_i, x_i)^{-1}, \qquad x \in V,\ 1 \leqq i \leqq m. \tag{12}$$

Since all the S_i are orthogonal transformations, we have

$$\begin{aligned} \beta(x, x_i) &= \beta(xS_i, x_iS_i) = \beta(x - \Lambda_i(x)x_i, -x_i) \\ &= -\beta(x, x_i) + \Lambda_i(x)\beta(x_i, x_i). \end{aligned}$$

But $\beta(x_i, x_i) \neq 0$, and hence we obtain (12). Finally we have

$$a_{ij} = -\Lambda_j(x_i) = -\frac{2\beta(x_i, x_j)}{\beta(x_j, x_j)}, \qquad 1 \leqq i \leqq m,$$

and because $\det(\beta(x_i, x_j)) \neq 0$ by the nondegeneracy of β, $\det(a_{ij}) \neq 0$, and Proposition 4 is proved.

By Proposition 4 and Theorem 1 of [4], there exists a semi-simple Lie algebra $\mathfrak{L}$ over the complex field, and a Cartan subalgebra $\mathfrak{H}$ of $\mathfrak{L}$ such that the following statements are valid. It is possible to find a set of linear functions α_i, $1 \leqq i \leqq m$ on $\mathfrak{H}$ such that $\alpha_1, \cdots, \alpha_m$ is a fundamental system of roots of $\mathfrak{L}$ with respect to $\mathfrak{H}$, and the Weyl reflections S_{α_i} corresponding to the α_i are given by the formulas $\alpha_j S_{\alpha_i} = \alpha_j + a_{ji}\alpha_i$, $1 \leqq i, j \leqq m$. Then every root α of $\mathfrak{L}$ with respect to $\mathfrak{H}$ can be expressed in the form $\alpha = \sum_{i=1}^{m} d_i\alpha_i$, where the d_i are rational integers which are either all non-negative or all nonpositive. The former are called the positive roots; they are the positive roots with respect to the lexicographic ordering of the roots relative to the set $\alpha_1, \cdots, \alpha_m$. As in the case of $R(\mathfrak{g})$, the concept of a chain $C = C(\alpha_{i_1}, \cdots, \alpha_{i_r})$ can be introduced, and it is known that every positive root is generated by a chain (cf. [3, Theorem XV]).

PROPOSITION 5. *The mapping $\alpha_i \to \rho_i$ of the set $\alpha_1, \cdots, \alpha_m$ onto the maximal simple system Δ can be extended to a (1-1) mapping $\alpha \to f(\alpha)$ of the set $R(\mathfrak{L})$ of all roots of $\mathfrak{L}$ onto the set $R(\mathfrak{g})$ in such a way that the following conditions are satisfied.* (1) *If $\alpha, \beta, \alpha+\beta$ are roots of $\mathfrak{L}$ then $f(\alpha)+f(\beta)$ is a root of $\mathfrak{g}$, and $f(\alpha+\beta) = f(\alpha) + f(\beta)$*; (2) *If $\rho, \sigma, \rho+\sigma$ are roots of $\mathfrak{g}$ then $f^{-1}(\rho)+f^{-1}(\sigma)$ is a root of $\mathfrak{L}$, and $f^{-1}(\rho+\sigma) = f^{-1}(\rho)+f^{-1}(\sigma)$.*

Proof. Every root α of $\mathfrak{L}$ can be expressed in the form(5)

$$\alpha = \alpha_i S_{\alpha_{j_1}} \cdots S_{\alpha_{j_r}} = \sum_{i=1}^{m} d_i \alpha_i, \tag{13}$$

where $1 \leqq i \leqq m$, $1 \leqq j_k \leqq m$, $d_i \in Z$. We define the mapping f by

$$f(\alpha) = \rho_i s_{\rho_{j_1}} \cdots s_{\rho_{j_r}}; \tag{14}$$

then $f(\alpha)$ is a root by the results of §2.c. We prove first, by induction on r, that if $\alpha_i S_{\alpha_{j_1}} \cdots S_{\alpha_{j_r}} = \sum_1^m d_i \alpha_i$, then $\rho_i s_{\rho_{j_1}} \cdots s_{\rho_{j_r}} = \sum_1^m d^* \rho_i$. The result is evidently true if $r=1$. Assume that if $\beta = \alpha_i S_{\alpha_{j_1}} \cdots S_{\alpha_{j_{r-1}}} = \sum e_i \alpha_i$, then $\sigma = \rho_i s_{\rho_{j_1}} \cdots s_{\rho_{j_{r-1}}} = \sum e_i^* \rho_i$. Then $\beta S_{\alpha_{j_r}} = \sum e_i \alpha_i + (\sum e_i a_{ir}) \alpha_r$ while $\sigma s_{\rho_{j_r}} = \sum e_i^* \rho_i + (\sum e_i^* a_{ir}^*) \rho_r$, and our assertion is proved. From this fact it follows that the mapping f is single valued, and that if $\alpha = \sum d_i \alpha_i$, then

$$f(\alpha) = \sum_1^m d_i^* \rho_i. \tag{15}$$

From (15) we infer that if α, β, $\alpha+\beta$ are roots, then $f(\alpha+\beta) = f(\alpha) + f(\beta)$, and (1) is proved.

From (1) we deduce that if $C(\alpha_{i_1}, \cdots, \alpha_{i_r})$ is a chain generating the positive root α, then the root $f(\alpha)$ of $\mathfrak{g}$ belongs to $\Gamma(\Delta)$, and is generated by the chain $C(\rho_{i_1}, \cdots, \rho_{i_r})$. If α and β are distinct positive roots, then α and β are generated by chains in which some α_i appears with different multiplicities. By the preceding remark, it follows that $f(\alpha)$ and $f(\beta)$ are generated by chains in which ρ_i appears with different multiplicities, and hence $f(\alpha) \neq f(\beta)$ by Lemma 3. If $\alpha > 0$ and $\beta < 0$ then $f(\alpha) \neq f(\beta)$ since $\Gamma(\Delta) \cap \Gamma(\Delta^-) = \phi$. Therefore f is a (1-1) mapping of $R(\mathfrak{L})$ into $R(\mathfrak{g})$.

Let R_1 be the set of images $f(\alpha)$ of the roots of $\mathfrak{L}$; then f^{-1} is defined on R_1. We prove (2) for roots in R_1. First let ρ, σ, $\rho+\sigma \in R_1 \cap \Gamma(\Delta)$, and let $\alpha = f^{-1}(\rho)$, $\beta = f^{-1}(\sigma)$, and $\gamma = f^{-1}(\rho+\sigma)$. From what has been established it follows that the multiplicity with which a root α_i appears in a chain generating γ is equal to the multiplicity of ρ_i in a chain generating $\rho+\sigma$, and we conclude that $\gamma = \alpha+\beta$. A similar argument applies in case ρ, σ, $\rho+\sigma \in R_1 \cap \Gamma(\Delta^-)$. Finally if $\rho \in \Gamma(\Delta) \cap R_1$, $\sigma \in \Gamma(\Delta^-) \cap R_1$, $\rho+\sigma \in R_1$, then we may assume that $\rho+\sigma \in \Gamma(\Delta)$. Then $\rho+\sigma$, $-\sigma$, $\rho \in R_1 \cap \Gamma(\Delta)$, and by the first case, $f^{-1}(\rho+\sigma) + f^{-1}(-\sigma) = f^{-1}(\rho)$. Since $f^{-1}(-\sigma) = -f^{-1}(\sigma)$, (2) is proved for roots in R_1.

It remains to prove that $R_1 = R(\mathfrak{g})$. Let $\tau \in \Gamma(\Delta)$ be a root generated by a chain of length greater than one, and assume as an induction hypothesis that all roots in $\Gamma(\Delta)$ generated by shorter chains than τ belong to R_1. Then $\tau = \sigma + \rho_i$, $\rho_i \in \Delta$, and $\sigma = f(\beta) \in R_1$. Let u and v be the rational integers, $u \leqq 0 \leqq v$, such that $\beta + k\alpha_i$ is a root if and only if $u \leqq k \leqq v$. Then $|u+v| \leqq 3$,

(5) See Sataki, *On a theorem of E. Cartan*, Journal of the Mathematical Society of Japan vol. 2 (1951) pp. 284–304, Corollary 1 to Proposition 3.

and if $\beta = \sum d_k\alpha_k$, then it is known that $u+v = \sum d_k a_{ki}$. By (15) we have $\sigma = f(\beta) = \sum d_k^*\rho_k$, and by the results of §2.c we obtain $\sum d_k^* a_{ki}^* = (r_{\sigma,\rho_i}+s_{\sigma,\rho_i})^*$. Thus the numbers $u+v$ and $r_{\sigma,\rho_i}+s_{\sigma,\rho_i}$ are congruent modulo p. Since both have absolute value $\leqq 3$ and $p \geqq 7$, the numbers are equal. Since $\sigma+\rho_i$ is a root, $s_{\sigma,\rho_i} \geqq 1$, and we have $v \geqq (r_{\sigma,\rho_i}-u)+1$. By the proof of Lemma 3, the roots σ, $\sigma-\rho_i$, $\cdots$, $\sigma-(-r_{\sigma,\rho_i}^*)\rho_i$ are all generated by shorter chains than σ, and hence belong to R_1. Applying f^{-1} by the special case of (2) already established, we see that β, $\beta-\alpha_i$, $\cdots$, $\beta-(-r_{\sigma,\rho_i}^*)\alpha_i$ are roots of $\mathfrak{L}$, and hence $r_{\sigma,\rho_i}-u \geqq 0$, and $v \geqq 1$. Then $\beta+\alpha_i$ is a root, and by (1), $f(\beta+\alpha_i) = \tau$. Since we have proved that $R_1 = R(\mathfrak{g})$, 2) is valid for all roots, and the Proposition is completely proved.

COROLLARY. *If Δ is a maximal simple system of roots, then every root of $\mathfrak{g}$ is an image of an element of Δ by a transformation of the group generated by the reflections s_ρ determined by the roots ρ belonging to Δ.*

5. **Construction of a modular Lie algebra isomorphic to $\mathfrak{g}$.** We begin by selecting an admissible basis of $\mathfrak{L}$, taking into account the results of Chevalley [1] on the properties of the constants of structure $N_{\alpha\beta}$. Let $\mathfrak{H}$ be a Cartan subalgebra of $\mathfrak{L}$, α, β, $\cdots$ the roots of $\mathfrak{L}$ with respect to $\mathfrak{H}$, $B(X, Y)$ the Killing form on $\mathfrak{L}$, H_α' the unique element of $\mathfrak{H}$ corresponding to a root α such that $B(H_\alpha', H) = \alpha(H)$ for all $H \in \mathfrak{H}$, and $H_\alpha = 2B(H_\alpha', H_\alpha')^{-1}H_\alpha'$, so that $\alpha(H_\alpha) = 2$. Then $\mathfrak{L}$ has a basis consisting of root elements E_α in (1-1) correspondence with the roots, and a basis of $\mathfrak{H}$. Then E_α can be chosen so that for each root α,

$$[E_\alpha E_{-\alpha}] = H_\alpha, \qquad B(E_\alpha, E_{-\alpha}) = -2B(H_\alpha', H_\alpha')^{-1}. \tag{16}$$

Then we have the following multiplication table for $\mathfrak{L}$.

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

$$[E_\alpha E_\beta] = \begin{cases} 0 \text{ if } \alpha+\beta \text{ is not a root,} \\ N_{\alpha\beta}E_{\alpha+\beta} \text{ if } \alpha+\beta \text{ is a root (0 is not counted as a root),} \\ H_\alpha \text{ if } \alpha+\beta = 0. \end{cases} \tag{17}$$

It is with the elements $N_{\alpha\beta}$ that we shall be concerned. In [2] it is stated that the $N_{\alpha\beta}$ could be selected so that $N_{\alpha\beta}^2 \in Z$, the ring of rational integers; the reference given in [2] to Weyl's paper shows only that $N_{\alpha\beta}^2$ can be assumed to be a positive rational number, if different from zero. The coefficient field K defined in [2] is the algebraic number field generated by the $N_{\alpha\beta}$; it contains the constants of structure of the admissible basis consisting of the E_α and elements $H_{\alpha_1}, \cdots, H_{\alpha_m}$ corresponding to a fundamental system of roots of $\mathfrak{L}$. Without further analysis, the set of exceptional primes defined in §4 of [2] would have to be enlarged to include those primes $\mathfrak{p}$ for which $N_{\alpha\beta} \notin \mathfrak{o}_\mathfrak{p}$.

Chevalley has shown, however, that for a suitable choice of the E_α, the

$N_{\alpha\beta}$ are rational integers [1, pp. 21–23]. If we replace the E_α by $E'_\alpha = \xi_\alpha E_\alpha$, $\xi_\alpha \in C$, then (16) will hold provided that $\xi_\alpha \xi_{-\alpha} = 1$; we shall assume that this condition is always satisfied. Then Chevalley proves [1, p. 22] that for any choice of the ξ_α,

$$N_{\alpha\beta}N_{-\alpha,-\beta} = N'_{\alpha\beta}N'_{-\alpha,-\beta}.$$

He then calculates this uniquely determined number, and obtains

$$N_{\alpha\beta}N_{-\alpha,-\beta} = -(p+1)^2,$$

where p is the integer such that $\beta + i\alpha$ is a root for $-p \leqq i \leqq 0$. Then for a suitable choice of the E_α,

$$N_{\alpha\beta} = -N_{-\alpha,-\beta}$$

and hence if $N_{\alpha\beta} \neq 0$,

$$N_{\alpha\beta} = \pm (p+1). \tag{18}$$

Now we define a *rational basis* (X_i) of $\mathfrak{L}$ as a set of the E_α for which (16) and (18) are satisfied, together with elements $H_{\alpha_1}, \cdots, H_{\alpha_m}$ belonging to a fundamental system of roots of $\mathfrak{L}$ with respect to $\mathfrak{H}$. A rational basis is admissible in the sense of [2], but not every admissible basis need be rational. Some remarks in [2] concerning the uniqueness of the coefficient field, and which refer to a particular method of normalizing the E_α, of course can be ignored if we restrict ourselves to rational bases, for if (X_i) is a rational basis, then the constants of structure c_{ijk} defined by $[X_iX_j] = \sum c_{ijk}X_k$ are rational numbers (the H_α are not necessarily integral linear combinations of the H_{α_i}, $1 \leqq i \leqq m$.) The set of exceptional primes is defined as before (see [2]) to be the primes 2, 3, and any primes for which the determinant of the Killing matrix $(B(X_i, X_j))$ is not a unit.

Now let p be a rational prime. A *p-integral subring* Σ of $\mathfrak{L}$ is the set of all linear combinations with p-adic integer coefficients of the elements of a rational basis (X_i), provided that Σ is closed under the bracket operation. By [2, §4], a sufficient condition that $\sum \mathfrak{o}_p X_i$, where $\mathfrak{o}_p$ is the ring of p-adic integers r/s, $s \notin (p)$, form a p-integral subring is that $p \neq 2, 3$, and that for each root α, $B(E_\alpha, E_{-\alpha})$ be a unit in $\mathfrak{o}_p$. A *modular Lie algebra* $\mathfrak{l}$ is the Lie ring $\Sigma/p\Sigma$, viewed as a Lie algebra over the prime field $Z_p = \mathfrak{o}_p/(p)$ in the natural way.

The following result makes use of formula (3), §2, and hence, for the first time, the assumption that the Killing form of $\mathfrak{g}$ be nondegenerate is indispensable.

PROPOSITION 6. *Let p be the characteristic of Ω $(p > 7)$, and let $\mathfrak{o}$ be the ring of p-adic integers. Then the set Σ of linear combinations with coefficients in $\mathfrak{o}$ of the elements of a rational basis (X_i) is closed under the bracket operation.*

Proof. It is sufficient to prove that for each root α, $B(E_{-\alpha}, E_\alpha)$ is a unit in $\mathfrak{o}$. By (6) of [2] we have the formula

$$B(E_{-\alpha}, E_\alpha) = -2B(H'_\alpha, H'_\alpha)^{-1} = -\frac{1}{2}\left(\sum_\beta (u_{\beta,\alpha} + v_{\beta,\alpha})^2\right),$$

where $u_{\beta,\alpha}$ and $v_{\beta,\alpha}$ are the integers, $u_{\beta,\alpha} \leqq 0 \leqq v_{\beta,\alpha}$, such that $\beta + k\alpha$ is a root if and only if $u_{\beta,\alpha} \leqq k \leqq v_{\beta,\alpha}$. Since $p > 7$, this formula implies that each $B(E_{-\alpha}, E_\alpha) \in \mathfrak{o}$. Let f be the mapping of $R(\mathfrak{L})$ onto $R(\mathfrak{g})$ constructed in Proposition 5; then by (1) and (2) of Proposition 5, we have

$$r_{f(\alpha),f(\beta)} = u_{\alpha,\beta}, \qquad s_{f(\alpha),f(\beta)} = v_{\alpha,\beta},$$

where r and s are the integers defined in §2.c. Because

$$\sum_\beta (\overset{*}{r}_{f(\beta),f(\alpha)} + \overset{*}{s}_{f(\beta),f(\alpha)})^2 \neq 0$$

in Ω by formula (4), §2, we conclude that $B(E_{-\alpha}, E_\alpha)$ is a unit in $\mathfrak{o}$, and Proposition 6 is proved.

Now we come to the main result of the paper.

THEOREM. *Let $\mathfrak{g}$ be a Lie algebra over an algebraically closed field Ω of characteristic $p > 7$, whose Killing form is nondegenerate. There exists a semi-simple Lie algebra $\mathfrak{L}$ over the complex field whose Weyl matrix (a_{ij}) has the property that (a^*_{ij}) is the Weyl matrix of $\mathfrak{g}$ associated with a maximal simple system of roots. Then there exists a modular Lie algebra $\mathfrak{l}$ over the prime field Z_p in Ω belonging to a p-integral subring of $\mathfrak{L}$, and an isomorphism H of $\mathfrak{l}$ into $\mathfrak{g}$ such that $\mathfrak{g}$ is obtained from $\mathfrak{l}H$ by extension of the base field from Z_p to Ω.*

Let $\Delta = \{\rho_1, \cdots, \rho_m\}$ be a maximal simple system of roots of $\mathfrak{g}$ with Weyl matrix (a^*_{ij}). The existence of the Lie algebra $\mathfrak{L}$ with Weyl matrix (a_{ij}) follows from Proposition 4, and from Theorem 1 of [4]. Let (X_i) be a rational basis of $\mathfrak{L}$, and let $\mathfrak{o}$ be the ring of p-adic integers. By Proposition 6, the set $\Sigma = \sum \mathfrak{o} X_i$ is a p-integral subring.

We review some of the properties of the modular Lie algebra $\mathfrak{l} = \Sigma/p\Sigma$, most of which were established in the course of the proofs of Theorems 1 and 2 of [2]. We let ϕ be the natural mapping of $\mathfrak{o}$ onto Z_p, and let T be the natural mapping of Σ onto $\mathfrak{l}$. Then T maps $\mathfrak{H} \cap \Sigma$ onto a Cartan subalgebra $\mathfrak{h}$ of dimension m in $\mathfrak{l}$. For each root element E_α appearing in the basis (X_i), we write $e_{\alpha'}$ for $E_\alpha T$. We write h_i for $H_{\alpha_i} T$, where the H_{α_i} are the basis elements of $\mathfrak{H}$ among the (X_i), and $h_{\alpha'}$ for $H_\alpha T$. For each root α of $\mathfrak{L}$, let α' be the unique linear function on $\mathfrak{h}$ whose value on $H_{\alpha_i} T$ is $\phi(\alpha(H_{\alpha_i}))$, $1 \leqq i \leqq m$. Then for all $H \in \mathfrak{H} \cap \Sigma$, we have

$$\phi(\alpha(H)) = \alpha'(HT),$$

and in particular, since $H_\alpha \in \mathfrak{H} \cap \Sigma$ by (17), $\alpha'(H_\alpha T) = \phi(2) \neq 0$ in Z_p, so that the linear functions α' are different from zero. If we use the fact that for all the roots α of $\mathfrak{L}$, $\alpha(H_{\alpha_i}) = 2\alpha(H'_{\alpha_i})\alpha_i(H'_{\alpha_i})^{-1}$ is a rational integer such that $|\alpha(H_{\alpha_i})| \leqq 3$, then $\alpha(H_{\alpha_i}) \equiv \beta(H_{\alpha_i}) \pmod{p}$ for $1 \leqq i \leqq m$ implies that $\alpha(H_{\alpha_i}) = \beta(H_{\alpha_i})$ since $p > 7$. Therefore the mapping $\alpha \to \alpha'$ is a (1-1) mapping.

The table (17) yields the following multiplication table for $\mathfrak{l}$.

$$[hh'] = 0; \quad [e_{\alpha'} h] = \alpha'(h) e_{\alpha'} \quad h, h' \in \mathfrak{h};$$

$$[e_{\alpha'} e_{\beta'}] = \begin{cases} 0 \text{ if } \alpha + \beta \neq 0 \text{ and if } \alpha + \beta \text{ is not a root,} \\ n_{\alpha'\beta'} e_{\alpha'+\beta'} \text{ if } \alpha + \beta \text{ is a root,} \\ h_{\alpha'} = H_\alpha T \text{ if } \alpha + \beta = 0, \end{cases} \tag{19}$$

where $n_{\alpha,\beta,} = \phi(N_{\alpha\beta})$ is a nonzero element of Z_p whenever $N_{\alpha\beta} \neq 0$ for the following reason. Let $\beta + i\alpha$ be a root for $-p \leqq i \leqq q$. Then by (18), $N_{\alpha\beta} = \pm(p+1)$. On the other hand, $p + q \leqq 3$ (see [1, p. 19]), and hence $\phi(N_{\alpha\beta}) \neq 0$ in Z_p since the characteristic p is greater than 7.

From the formulae (19) it follows that the linear functions α' are roots of $\mathfrak{l}$ with respect to $\mathfrak{h}$. The mapping $\alpha \to \alpha'$ is a (1-1) mapping of the set of roots of $\mathfrak{L}$ with respect to $\mathfrak{H}$ onto the set of roots of $\mathfrak{l}$ with respect to $\mathfrak{h}$. The biuniqueness of the mapping has been proved, and the mapping is onto by the argument used in the first part of the proof of Theorem 2 of [2]. Evidently the mapping $\alpha \to \alpha'$ has the following additional properties.

$$\begin{aligned} \alpha, \beta, \alpha + \beta \in R(\mathfrak{L}) &\text{ implies } \alpha', \beta', (\alpha + \beta)' \in R(\mathfrak{l}) \\ &\text{and } (\alpha + \beta)' = \alpha' + \beta', \\ \alpha', \beta', \alpha' + \beta' \in R(\mathfrak{l}) &\text{ implies } \alpha + \beta \in R(\mathfrak{L}), \\ \alpha \in R(\mathfrak{L}) &\text{ implies } (-\alpha)' = -\alpha'. \end{aligned} \tag{20}$$

The sets $\Delta_0 = \{\alpha_1, \cdots, \alpha_m\}$ and $\Delta_1 = \{\alpha'_1, \cdots, \alpha'_m\}$ of roots of $\mathfrak{L}$ and $\mathfrak{l}$ respectively are simple systems of roots, and the definitions of chains etc. given in §3 can be applied to Δ_0 and Δ_1. It is known(6) that if α is a root of $\mathfrak{L}$ then either α or $-\alpha$ belongs to a chain with generators in Δ_0. By (20) the same remark applies to the roots of $\mathfrak{l}$. Moreover, the length of a chain which generates α' is uniquely determined, and is equal to the length of a chain which generates α.

Using the mapping f constructed in Proposition 5, it follows that the mapping $\alpha'_i \to \rho_i$, $1 \leqq i \leqq m$, can be extended to a (1-1) mapping $\alpha' \to \alpha \to f(\alpha) = \alpha''$ of $R(\mathfrak{l})$ onto $R(\mathfrak{g})$ with the property that the mapping $\alpha' \to \alpha''$ and the inverse mapping preserve sums, and a chain $C(\alpha'_{i_1}, \cdots, \alpha'_{i_r})$ with links in Δ_1 is mapped onto the chain $C(\alpha''_{i_1}, \cdots, \alpha''_{i_r})$ with links in Δ. Since $\alpha(H_\beta)$ and $\alpha''(c_{\beta''})$ can be calculated from the lengths of corresponding strings of roots of $\mathfrak{L}$ and $\mathfrak{g}$ respectively, it follows that if $\alpha' \to \alpha''$, $\beta' \to \beta''$, then $\alpha'(h_{\beta'}) = \alpha''(c_{\beta''})$.

(6) This statement can be proved by an argument similar to the proof of Proposition 1.

We prove next that every ideal $\mathfrak{b} \neq 0$ in $\mathfrak{l}$ contains at least one of the $e_{\alpha'}$. For this we choose an infinite field $F \supseteq Z_p$, and consider the nonzero ideal $\mathfrak{b}^F$ in $\mathfrak{l}^F$(7). Since the linear functions α' are distinct and different from zero, there exists an element h in $\mathfrak{h}^F$ such that $\alpha'(h) \neq 0$, and $\alpha'(h) - \beta'(h) \neq 0$ for all α' and β'. By assumption there exists in $\mathfrak{b}^F$ a nonzero element

$$w = \sum_{i=1}^{m} \xi_i h_i + \sum \eta_{\alpha'} e_{\alpha'}$$

such that $\eta_{\alpha'} \neq 0$ for some α'. Then

$$w(\operatorname{ad} h)^q = \sum \eta_{\alpha'} \alpha'(h)^q e_{\alpha'} \in \mathfrak{b}^F$$

for all $q \geqq 1$, and by using an appropriate Vandermonde determinant, we obtain

$$\delta \eta_{\alpha'} e_{\alpha'} \in \mathfrak{b}^F, \qquad \eta_{\alpha'} \neq 0,$$

where

$$\delta = (\prod_{\alpha'} \alpha'(h))(\prod_{\alpha<\beta} (\alpha'(h) - \beta'(h))) \neq 0$$

by the choice of h. Thus $e_{\alpha'} \in \mathfrak{b}^F \cap \mathfrak{l} = \mathfrak{b}$.

Now we shall construct a homomorphism H of $\mathfrak{l}$ into $\mathfrak{g}$, where $\mathfrak{g}$ is, for the purposes of this construction, viewed as a Lie algebra over Z_p. We recall that $\mathfrak{g}$ is a vector space direct sum $\mathfrak{g} = \mathfrak{c} + \sum_\rho \mathfrak{g}_\rho$, and that $\mathfrak{g}$ possesses a basis consisting of the root elements $u_{\alpha''}$ normalized so that $[u_{-\beta''} u_{\beta''}] = c_{\beta''}$, together with a basis for $\mathfrak{c}$. For each $i > 0$, let $\mathfrak{l}_i$ and $\mathfrak{g}_i$ be the subspaces of $\mathfrak{l}$ and $\mathfrak{g}$ respectively spanned by the root elements $e_{\alpha'}$ (resp. $u_{\alpha''}$) and the corresponding elements $h_{\alpha'}$ (resp. $c_{\alpha''}$) which belong to roots generated by chains of length $\leqq i$.

We sketch a proof by induction on i that there exists a linear mapping H of $\mathfrak{U}_{i>0} \mathfrak{l}_i$ onto $\mathfrak{U}_{i>0} \mathfrak{g}_i$ with the following properties: $\mathfrak{h}H = \mathfrak{c}$; $\mathfrak{l}_{\alpha'} H = \mathfrak{g}_{\alpha''}$, where $\mathfrak{l}_{\alpha'} = Z_p e_{\alpha'}$; $x \in \mathfrak{l}_{\alpha'} \cap \mathfrak{l}_i$, $y \in \mathfrak{l}_{\beta'} \cap \mathfrak{l}_i$, $[xy] \in \mathfrak{l}_{\alpha'+\beta'} \cap \mathfrak{l}_i$, implies xH, yH, $[xy]H \in \mathfrak{g}_i$ and $[xH, yH] = [xy]H$; and $x \in \mathfrak{l}_{\alpha'} \cap \mathfrak{l}_i$, $h \in \mathfrak{h}$, implies $[xH, hH] = [xh]H$ in $\mathfrak{g}_i$.

We define H on $\mathfrak{l}_1$ by setting $e_{\pm\alpha_i'} H = \pm u_{\pm\alpha_i''}$, $h_{\alpha_i'} H = c_{\alpha_i''}$, $1 \leqq i \leqq m$, and extending H by linearity to a mapping of $\mathfrak{l}_1$ onto $\mathfrak{g}_1$. Then H is single valued on $\mathfrak{l}_1$, and maps $\mathfrak{h}$ onto $\mathfrak{c}$. Since $\alpha_i' - \alpha_j'$ is not a root, and since $\alpha_i' + \alpha_j'$, if a root, has length greater than one, the fact that H preserves the bracket operation can be shown by the following calculation. From $[e_{-\alpha_i'} e_{\alpha_i'}] = -h_{\alpha_i'}$, we have $[e_{-\alpha_i'} e_{\alpha_i'}]H = -h_{\alpha_i'} H = -c_{\alpha_i''} = [e_{-\alpha_i'} H,\ e_{\alpha_i'} H]$, $1 \leqq i \leqq m$, and $[e_{\pm\alpha_i'},\ h_{\alpha_j'}] = \mp a_{ij}^* e_{\pm\alpha_i'}$ implies that $[e_{\pm\alpha_i'} H,\ h_{\alpha_j'} H] = \mp a_{ij}^* (e_{\pm\alpha_i'} H)$.

Now assume that for some $i > 1$, H has been extended to a mapping of $\mathfrak{U}_i \mathfrak{l}_i$ onto $\mathfrak{U}_i \mathfrak{g}_i$ with the required properties. For any root α' of $\mathfrak{l}$ generated by a chain of length $i+1$ with links in Δ_1, we have $\alpha' = \beta' + \alpha_k'$, where β' is gener-

(7) We use the notation $\mathfrak{b}^F$ for the vector space $\mathfrak{b} \otimes F$ (viewed as an algebra or as an ideal) obtained by extension of the base field from Z^p to F.

ated by a chain of length i, and $\alpha_k' \in \Delta_1$. We have shown previously that $n_{\beta',\alpha_k'} \neq 0$; therefore $[\mathfrak{l}_{\beta'}\mathfrak{l}_{\alpha_k'}] = \mathfrak{l}_{\alpha'}$ since the root spaces $\mathfrak{l}_{\alpha'}$ are one dimensional, and any $u \in \mathfrak{l}_{\alpha'}$ can be expressed in the form $u = [vw]$, where $v \in \mathfrak{l}_{\beta'}$, $w \in \mathfrak{l}_{\alpha_k'}$. Then we define $uH = [vH, wH]$. By construction, $vH \in \mathfrak{g}_{\beta''}$, $wH \in \mathfrak{g}_{\rho_k}$, and $uH = [vH, wH] \in \mathfrak{g}_{\alpha''}$, so that $\mathfrak{l}_{\alpha'}H = \mathfrak{g}_{\alpha''}$. The action of H upon $\mathfrak{l}_{-\alpha'}$ is defined in a similar manner, and H is defined on $\mathfrak{l}_{i+1}$ by linearity. The verification that H is defined independently of the representation of α' as a sum $\beta' + \alpha_k'$, and that H possesses the homomorphism property on $\mathfrak{l}_{i+1}$ is identical with the argument given by Seligman [5, §16], and we shall not repeat the details. Then H is a homomorphism of $\mathfrak{l}$ into $\mathfrak{g}$, and $\mathfrak{l}H$ contains a basis of $\mathfrak{g}$ over Ω because for every root ρ of $\mathfrak{g}$, either ρ or $-\rho$ belongs to $\Gamma(\Delta)$ by Proposition 1. Therefore $(\mathfrak{l}H)^{\Omega} = \mathfrak{g}$. By construction the kernel of H contains no root space $\mathfrak{l}_{\alpha'}$, and by a result established earlier in the proof, the kernel of H is zero, and H is an isomorphism. This completes the proof of the theorem.

COROLLARY 1. *Let Δ be a maximal simple system of roots of a Lie algebra $\mathfrak{g}$ over an algebraically closed field of characteristic $p > 7$ whose Killing form is non-degenerate. Then Δ is a linearly independent set of l roots, where l is the rank of $\mathfrak{g}$.*

Proof. By Proposition 2, Δ contains at least l linearly independent roots. In the proof of the theorem we have shown that the number of roots in Δ is equal to the dimension of the Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{l}$. Since H is an isomorphism mapping $\mathfrak{h}$ onto $\mathfrak{c}$, the dimension of $\mathfrak{c}$ is equal to the number of roots in Δ, and the Corollary is proved.

COROLLARY 2. *Two Lie algebras $\mathfrak{g}$ and $\mathfrak{g}'$ satisfying the hypotheses of Corollary 1 are isomorphic if the Weyl matrices A and A' associated with maximal simple systems of roots of $\mathfrak{g}$ and $\mathfrak{g}'$ are identical.*

Proof. The main theorem implies that there exists a modular Lie algebra $\mathfrak{l}$, and isomorphisms H and H' of $\mathfrak{l}$ onto $\mathfrak{g}$ and $\mathfrak{g}'$ such that $\mathfrak{g} = (\mathfrak{l}H)^{\Omega}$, $\mathfrak{g}' = (\mathfrak{l}H')^{\Omega}$. Then the mapping $H^{-1}H'$ can be extended to an isomorphism of $\mathfrak{g}$ onto $\mathfrak{g}'$.

According to Corollary 2, a Lie algebra $\mathfrak{g}$ over Ω with a nondegenerate Killing form is determined within isomorphism by the Weyl matrix belonging to a maximal simple system of roots of $\mathfrak{g}$ with respect to a Cartan subalgebra $\mathfrak{c}$. Therefore the classification of the algebras $\mathfrak{g}$ is equivalent to the explicit determination of all possible Weyl matrices. The main theorem gives a partial solution to this problem. By Proposition 3 it is sufficient to consider the case of a simple algebra. Let $\mathfrak{g}$ be a simple Lie algebra over Ω whose Killing form is nondegenerate, and let Δ be a maximal simple system of roots of $\mathfrak{g}$ relative to a Cartan subalgebra. By Proposition 3, Δ is an indecomposable simple system. Then by the main theorem there exists a semi-simple Lie algebra $\mathfrak{L}$ of characteristic zero with the following properties. There exists a Cartan subalgebra $\mathfrak{H}$ of $\mathfrak{L}$, and a fundamental simple system of roots $\alpha_1, \cdots, \alpha_l$ of $\mathfrak{L}$ relative to $\mathfrak{H}$ such that if $\alpha_i \to \alpha_i + a_{ij}\alpha_j$, $1 \leqq i \leqq l$, is the Weyl reflection deter-

mined by the root α_j, $1 \leqq j \leqq l$, then (a_{ij}^*) is the Weyl matrix of $\mathfrak{g}$ belonging to Δ. Let $B(X, Y)$ be the Killing form on $\mathfrak{L}$, and for each root α, let H'_α be the unique element of $\mathfrak{H}$ such that $B(H'_\alpha, H) = \alpha(H)$ for all $H \in \mathfrak{H}$. Let $H_\alpha = 2B(H'_\alpha, H'_\alpha)^{-1}H'_\alpha$. Then $H_{\alpha_1}, \cdots, H_{\alpha_l}$ is a basis for $\mathfrak{H}$, and $\alpha_i(H_{\alpha_j}) = -a_{ij}$, $1 \leqq i, j \leqq l$. Then it follows from the way the matrix (a_{ij}) was selected (see Proposition 4) that the fundamental system of roots $\alpha_1, \cdots, \alpha_l$ is indecomposable in the sense that for each i, $1 \leqq i \leqq l$, there exists a $j \neq i$ such that $\alpha_i(H_{\alpha_j}) \neq 0$. It is well known that the indecomposability of the system $\alpha_1, \cdots, \alpha_l$ implies that $\mathfrak{L}$ is a simple Lie algebra. The Weyl matrices of the simple Lie algebras $\mathfrak{L}$ can be constructed explicitly, for example, from the classification of the indecomposable simple systems of roots given by Dynkin [3]. Thus the Weyl matrix of a simple Lie algebra over an algebraically closed field of characteristic $p > 7$ whose Killing form is nondegenerate is obtained by reduction modulo p from the Weyl matrix of a simple Lie algebra over an algebraically closed field of characteristic zero, and the Weyl matrices of the latter are known explicitly. The following problem is not settled by our results, however, and is discussed from a different point of view by Seligman [5, pp. 77–83]. Let (a_{ij}) be the Weyl matrix of a simple Lie algebra over an algebraically closed field of characteristic zero, and let p be a prime number. The problem is to find necessary and sufficient conditions on (a_{ij}) in order that the matrix of residue classes of the a_{ij} modulo p be the Weyl matrix of a simple Lie algebra over an algebraically closed field of characteristic p with nondegenerate Killing form.

References

1. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. vol. 7 (1955) pp. 14–66.

2. C. W. Curtis, *Modular Lie algebras* I, Trans. Amer. Math. Soc. vol. 82 (1956) pp. 160–179.

3. E. B. Dynkin, *The structure of semi-simple algebras*, American Mathematical Society Translations, No. 17.

4. Harish-Chandra, *On some applications of the universal enveloping algebra of a semi-simple Lie algebra*, Trans. Amer. Math. Soc. vol. 70 (1951) pp. 28–96.

5. G. Seligman, *On Lie algebras of prime characteristic*, Memoirs of the American Mathematical Society, No. 19, 1956.

6. A Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, 3d ed., Berlin, 1937.

University of Wisconsin,
Madison, Wis.