Lie Algebras of Classical Type

W. H. MILLS & G. B. SELIGMAN

Communicated by N. JACOBSON

The purpose of this paper is to present a unified technique for the classification of those semi-simple Lie algebras to which the methods of KILLING and CARTAN are applicable. Five axioms for such a classification theory are presented, and from them the customary sets of invariants (matrices of integers or Schläfli diagrams) are developed and their completeness proved. The argument from the axioms to the isomorphism (completeness) theorem is elementary, involving only some familiarity with finite-dimensional vector spaces. The first two axioms require that the algebra have no center and that it be its own derived algebra. The other three require the existence of a Cartan decomposition with certain special properties. Among the algebras satisfying these axioms are all semi-simple Lie algebras over algebraically closed fields of characteristic zero (see [5]) and those algebras over algebraically closed fields of characteristic $p > 7$ that are treated in [8]. In particular, the axioms are satisfied by all Lie algebras with non-degenerate Killing forms over algebraically closed fields of characteristic different from 2, 3, 5.

The previous treatments of the classification theory all depend heavily on the existence of a non-degenerate bilinear form with certain properties, but unfortunately it is not clear whether or not a suitable form actually exists for all the Lie algebras obtained. Thus it is desirable to have a complete treatment that does not depend on such a form. Our present paper provides such a treatment.

Apart from giving the theory a basis which seems close to the most general setting in which it is applicable, it is to be hoped that the authors have achieved sufficient conciseness to make the results of [8] for non-zero characteristic more accessible. It will be noted that the multiplicity of case distinctions of that paper has been considerably reduced by the development of more general principles.

The existence of a full collection of algebras, one for each system of invariants, has long been known for characteristic zero ([1], [5], [7], [9], [11]). A complete answer to this question for $p \neq 0$ was not supplied in [8]. Using some of CHEVALLEY'S results on the choice of structure constants at characteristic

zero [2], one of us has now solved this problem. The results are contained in a short note immediately following this paper.

Our results, with one minor exception, all hold for characteristic 5 and 7. This is demonstrated in a second short note following this paper.

1. Axioms and simple consequences. A finite-dimensional *Lie algebra* $\mathfrak{L}$ over a field $\mathfrak{F}$ is a finite-dimensional vector space over $\mathfrak{F}$ in which there is defined a bilinear product $[ab]$: $[ab] \in \mathfrak{L}$ for all $a, b \in \mathfrak{L}$, and $[ab]$ satisfies the following identities:

Anticommutativity: $[aa] = 0$ for all $a \in \mathfrak{L}$, and

Jacobi identity: $[[ab]c] + [[bc]a] + [[ca]b] = 0$ for all $a, b, c \in \mathfrak{L}$.

From the first of these we obtain

$$\begin{aligned} 0 &= [a + b, a + b] = [aa] + [ab] + [ba] + [bb] \\ &= [ab] + [ba] \end{aligned}$$

or $[ab] = -[ba]$ for all $a, b \in \mathfrak{L}$. The *center* of $\mathfrak{L}$ is the set of all $a \in \mathfrak{L}$ such that $[a] = 0$. An *abelian Cartan subalgebra* of $\mathfrak{L}$ is a subspace $\mathfrak{S}$ of $\mathfrak{L}$ such that $[\mathfrak{S}\mathfrak{S}] = 0$ and such that $[a\mathfrak{S}] \subset \mathfrak{S}$, $a \in \mathfrak{L}$, implies $a \in \mathfrak{S}$. Let $\mathfrak{S}$ be such a subalgebra. For any $\alpha \in \mathfrak{S}^*$, the dual space of $\mathfrak{S}$, let $\mathfrak{L}_\alpha$ denote the set of all $a \in \mathfrak{L}$ such that $[ah] = \alpha(h)a$ for all $h \in \mathfrak{S}$. If $\mathfrak{L}_\alpha \neq 0$, α is called a *root* with respect to $\mathfrak{S}$. Clearly $\mathfrak{L}_0 = \mathfrak{S}$. If $a \in \mathfrak{L}_\alpha$, $b \in \mathfrak{L}_\beta$, then the Jacobi identity yields

$$[[ab]h] = [[ah]b] + [a[bh]] = (\alpha(h) + \beta(h))[ab],$$

so that $[\mathfrak{L}_\alpha \mathfrak{L}_\beta] \subset \mathfrak{L}_{\alpha+\beta}$.

Let $\mathfrak{L}$ be a finite-dimensional Lie algebra over a field $\mathfrak{F}$ of characteristic not 2, 3, 5, or 7.¹ Let p denote the characteristic of $\mathfrak{F}$. We shall assume that $\mathfrak{L}$ contains an abelian Cartan subalgebra $\mathfrak{S}$ and that $\mathfrak{L}$ and $\mathfrak{S}$ satisfy the following five axioms:

- (i) $[\mathfrak{L}\mathfrak{L}] = \mathfrak{L}$.
- (ii) The center of $\mathfrak{L}$ consists of 0 alone.
- (iii) $\mathfrak{L}$ is the direct sum of the subspaces $\mathfrak{L}_\alpha$.
- (iv) If α is a non-zero root, then $[\mathfrak{L}_\alpha \mathfrak{L}_{-\alpha}]$ is one-dimensional.
- (v) If α is a non-zero root and $\beta \in \mathfrak{S}^*$, then there is a positive integer m such that $\beta + m\alpha$ is not a root.

In particular, $\mathfrak{L}$ satisfies these conditions if $\mathfrak{F}$ is algebraically closed and if either (a) $p = 0$ and $\mathfrak{L}$ is semi-simple (for example, see [5]) or (b) $p > 7$ and $\mathfrak{L}$ is a restricted Lie algebra containing no abelian ideals and possessing a restricted representation with non-degenerate trace form [8]. If $\mathfrak{F}$ is algebraically closed,

¹ The only use in this paper of the assumption that the characteristic is not 7 is made in the proof of Lemma 3. The assumption that it is not 5 is used only in the proofs of Property (xvii), Lemma 3, and Theorem 6. For a full discussion of characteristic 5 and 7 see the second short note following this paper. The axioms imply that the characteristic is neither 2 nor 3.

$p \neq 2, 3, 5, 7$, and $\mathfrak{L}$ has non-degenerate Killing form, then either (a) or (b) holds so that our axioms apply.²

We adopt the notation of using the first eight lower case roman letters for elements of $\mathfrak{L}$ (and, in §2, for elements of the representation space $\mathfrak{V}$). The remaining lower case roman letters will denote real numbers—usually rational integers. Lower case Greek letters, except ϵ , will denote roots, elements of $\mathfrak{F}$, and homomorphisms.

We next derive some consequences of the axioms. From (iii) and (iv), respectively, we obtain

(vi) *There are only a finite number of roots.*

(vii) *If α is a root, then $-\alpha$ is also a root.*

For each non-zero root α , let h_α be a fixed non-zero element of $[\mathfrak{L}_\alpha \mathfrak{L}_{-\alpha}]$. Then from (i) and (iv) we obtain

(viii) *$\mathfrak{L}$ is spanned by the elements h_α .*

Now let $h \in \mathfrak{L}$ be such that $\alpha(h) = 0$ for all roots α . Then $[\mathfrak{L}_\alpha h] = 0$ for all roots α . Hence $[\mathfrak{L}h] = 0$ by (iii) and $h = 0$ by (ii). Thus we have

(ix) *The roots span the dual space $\mathfrak{L}^*$.*

From (v) and (vii) we have

(x) *If α is a non-zero root and $\beta \in \mathfrak{L}^*$, then there is a positive integer m such that $\beta - m\alpha$ is not a root.*

2. The Weyl-Jacobson Lemma. Let $\mathfrak{V}$ be a finite-dimensional vector space over $\mathfrak{F}$, let $\mathfrak{E}(\mathfrak{V})$ be the associative algebra of all endomorphisms of $\mathfrak{V}$, and let $\mathfrak{L}_1$ be a finite-dimensional Lie algebra over $\mathfrak{F}$. A linear mapping U of $\mathfrak{L}_1$ into $\mathfrak{E}(\mathfrak{V})$ is called a *representation* of $\mathfrak{L}_1$ in $\mathfrak{V}$ if $U([ab]) = U(a)U(b) - U(b)U(a)$ for all $a, b \in \mathfrak{L}_1$. If $\mathfrak{L}_1$ is a subalgebra of $\mathfrak{L}$, we may take $\mathfrak{V}$ to be the vector space $\mathfrak{L}$. It follows from the Jacobi identity that the mapping R of $\mathfrak{L}_1$ into $\mathfrak{E}(\mathfrak{L})$ given by $aR(b) = [ab]$, $a \in \mathfrak{L}$, $b \in \mathfrak{L}_1$ is a representation. This representation is called the *adjoint* representation of $\mathfrak{L}_1$ on $\mathfrak{L}$.

Let $\mathfrak{L}_1$ be a Lie algebra spanned by an abelian Cartan subalgebra $\mathfrak{H}$ and by two one-dimensional root-spaces $\mathfrak{L}_\alpha$ and $\mathfrak{L}_{-\alpha}$, $0 \neq \alpha \in \mathfrak{H}^*$. Let $e_\alpha \in \mathfrak{L}_\alpha$, $e_{-\alpha} \in \mathfrak{L}_{-\alpha}$, and assume that $[e_\alpha e_{-\alpha}] = h_\alpha \neq 0$. Let U be a representation of $\mathfrak{L}_1$ in a finite-dimensional vector space $\mathfrak{V}$. For any $\beta \in \mathfrak{H}^*$ let $\mathfrak{V}_\beta$ be the set of all $a \in \mathfrak{V}$ such that $a(\beta(h) - U(h))^m = 0$ for all $h \in \mathfrak{H}$ when m is sufficiently large. If $\mathfrak{V}_\beta \neq 0$, β is called a *weight* of the representation U .

Now

$$U(e_\alpha)U(h) = U(h)U(e_\alpha) + U([e_\alpha h]) = U(h)U(e_\alpha) + \alpha(h)U(e_\alpha)$$

² N. JACOBSON has recently shown that if $\mathfrak{L}$ is a Lie algebra with a non-degenerate invariant form over an algebraically closed field such that (1) $\mathfrak{L}$ has an abelian Cartan sub-algebra $\mathfrak{H}$; (2) every root with respect to $\mathfrak{H}$ is non-isotropic; and (3) for every $h \in \mathfrak{H}$, $\text{ad } h$ acts diagonally in $\mathfrak{L}$; then the derived algebra $[\mathfrak{L}\mathfrak{L}]$ modulo its center satisfies the axioms. In particular, these conditions hold if $\mathfrak{L}$ has a non-degenerate restricted trace form. The results of JACOBSON are not yet published.

for all $h \in \mathfrak{H}$. Hence for any $\beta \in \mathfrak{H}^*$, $h \in \mathfrak{H}$ we have

$$U(e_\alpha)(\beta(h) + \alpha(h) - U(h)) = (\beta(h) - U(h))U(e_\alpha),$$

and by induction on r

$$U(e_\alpha)(\beta(h) + \alpha(h) - U(h))^r = (\beta(h) - U(h))^r U(e_\alpha)$$

for all $r \geq 1$. It follows that $\mathfrak{B}_\beta U(e_\alpha) \subset \mathfrak{B}_{\beta+\alpha}$, and by symmetry $\mathfrak{B}_\beta U(e_{-\alpha}) \subset \mathfrak{B}_{\beta-\alpha}$.

Lemma 1. *If β is a weight, if $a_0 \in \mathfrak{B}_\beta$ is such that $a_0 U(h_\alpha) = \beta(h_\alpha) a_0$, and if $a_i = a_0 (U(e_\alpha))^i$, $i \geq 1$, $a_{-1} = 0$, then for all $i \geq 0$, $a_i U(h_\alpha) = (\beta + i\alpha)(h_\alpha) a_i$ and*

$$a_i U(e_{-\alpha}) = i \left(\beta + \frac{i-1}{2} \alpha \right) (h_\alpha) a_{i-1} + a_0 U(e_{-\alpha}) (U(e_\alpha))^i.$$

Proof. The lemma is immediate for $i = 0$. Suppose $i \geq 1$ and that the lemma holds for $i - 1$. Then

$$\begin{aligned} a_i U(h_\alpha) &= a_{i-1} U(e_\alpha) U(h_\alpha) = a_{i-1} U(h_\alpha) U(e_\alpha) + a_{i-1} U([e_\alpha h_\alpha]) \\ &= (\beta + (i-1)\alpha)(h_\alpha) a_{i-1} U(e_\alpha) + \alpha(h_\alpha) a_{i-1} U(e_\alpha) \\ &= (\beta + i\alpha)(h_\alpha) a_i, \end{aligned}$$

and

$$\begin{aligned} a_i U(e_{-\alpha}) &= a_{i-1} U(e_\alpha) U(e_{-\alpha}) = a_{i-1} U(e_{-\alpha}) U(e_\alpha) + a_{i-1} U(h_\alpha) \\ &= (i-1) \left(\beta + \frac{i-2}{2} \alpha \right) (h_\alpha) a_{i-1} + (\beta + (i-1)\alpha)(h_\alpha) a_{i-1} \\ &\quad + a_0 U(e_{-\alpha}) (U(e_\alpha))^i \\ &= i \left(\beta + \frac{i-1}{2} \alpha \right) (h_\alpha) a_{i-1} + a_0 U(e_{-\alpha}) (U(e_\alpha))^i. \end{aligned}$$

Lemma 2 (WEYL-JACOBSON). *If $\alpha(h_\alpha) \neq 0$ and if β is a weight such that $\beta - \alpha$ is not a weight, if $(j+1)$ is a positive integer such that $\beta + (j+1)\alpha$ is not a weight, and if $\beta + i\alpha$ is a weight for $0 \leq i \leq j$ then*

$$(1) \quad \bar{j} = -\frac{2\beta(h_\alpha)}{\alpha(h_\alpha)}$$

where $\bar{j}$ is the element in the prime field of $\mathfrak{F}$ corresponding to j . Moreover, if $0 \leq i < j$ then $\mathfrak{B}_{\beta+i\alpha} U(e_\alpha) \neq 0$.

Proof. Let $a_0 \in \mathfrak{B}_\beta$ be as in Lemma 1. Form the sequence of a_i as in Lemma 1. Since not all $\beta + i\alpha$ are weights by assumption, we have $a_i \neq 0$, $a_{i+1} = 0$ for some $i \geq 0$. Thus $i \leq j$. Now $a_0 U(e_{-\alpha}) = 0$ since $\beta - \alpha$ is not a weight, and from the second formula of Lemma 1

$$a_{i+1}U(e_{-\alpha}) = 0 = (i+1)\left(\beta + \frac{i}{2}\alpha\right)(h_{\alpha})a_i.$$

Now if $i+1 \equiv 0 \pmod{p}$, we have $p \neq 0$, and all $\beta + k\alpha$ are weights. Therefore $i+1 \equiv 0 \pmod{p}$ and

$$(2) \quad \bar{i} = -\frac{2\beta(h_{\alpha})}{\alpha(h_{\alpha})}.$$

It remains to show $i = j$. Both parts of the lemma will then be immediate. We need only show that $\beta + (i+1)\alpha$ is not a weight. Now suppose $\beta + (i+1)\alpha$ is a weight. Then there is a non-zero $b \in \mathfrak{B}_{\beta+(i+1)\alpha}$ such that $bU(h_{\alpha}) = (\beta + (i+1)\alpha)(h_{\alpha})b$. Since $\beta - \alpha$ is not a weight we have $b(U(e_{-\alpha}))^{i+2} = 0$. Let $n+1$ be the smallest positive integer such that $b(U(e_{-\alpha}))^{n+1}(U(e_{\alpha}))^{n+1} = 0$. We note that $0 \leq n \leq i+1$. Since not all $\beta + k\alpha$ are weights we have $b(U(e_{-\alpha}))^n \cdot (U(e_{\alpha}))^m = 0$ for some positive integer m , and we suppose that m is the smallest such integer. We have $m < p$ if $p > 0$. Furthermore $m > n$ by our choice of n and thus $b(U(e_{-\alpha}))^{n+1}(U(e_{\alpha}))^m = 0$. From the first statement of Lemma 1, with α replaced by $-\alpha$, we obtain

$$b(U(e_{-\alpha}))^n U(h_{\alpha}) = (\beta + (i+1-n)\alpha)(h_{\alpha})b(U(e_{-\alpha}))^n.$$

By an application of the second statement of Lemma 1 we now have

$$\begin{aligned} 0 &= b(U(e_{-\alpha}))^n (U(e_{\alpha}))^m U(e_{-\alpha}) \\ &= m\left(\beta + \left(i+1-n + \frac{m-1}{2}\right)\alpha\right)(h_{\alpha})b(U(e_{-\alpha}))^n (U(e_{\alpha}))^{m-1}. \end{aligned}$$

Consequently

$$\beta(h_{\alpha}) + \left(i+1-n + \frac{m-1}{2}\right)\alpha(h_{\alpha}) = 0.$$

Applying (2) we obtain $-i+2(i+1-n)+m-1 \equiv 0 \pmod{p}$ or $m-2n+i+1 \equiv 0 \pmod{p}$. Since $m > n$ and $n \leq i+1$ we have $m-2n+i+1 > 0$ and $p > 0$. Therefore $p > m$, $p > i+1$, and $m-2n+i+1 = p$ or $m = p+2n-i-1 > p+n-i-2$. But then the non-zero $b(U(e_{-\alpha}))^n (U(e_{\alpha}))^k$, $0 \leq k \leq p+n-i-2$, belong to the following weights:

$$\beta + (i+1-n)\alpha, \beta + (i+2-n)\alpha, \dots, \beta + (p-1)\alpha,$$

and, since $\beta, \beta + \alpha, \dots, \beta + (i-n)\alpha$ are known to be weights, all $\beta + k\alpha$ are weights, contrary to assumption. Therefore $\beta + (i+1)\alpha$ is not a weight, and the lemma is proved.

Lemma 2 is essentially equivalent to Lemma 5.1 of [8]. The proof given in [8] is incomplete in that the assumption is made, without proof, that $\beta + (i+1)\alpha$ is not a weight. The above argument completes the proof of Lemma 5.1 of [8].

3. Consequences of the lemmas. We now apply Lemmas 1 and 2 to the Lie algebra $\mathfrak{L}$ of §1 to prove some additional properties.

(xi) *If α is a non-zero root, then $\alpha(h_\alpha) \neq 0$.*

Proof. Since $[\mathfrak{L}_\alpha \mathfrak{L}_{-\alpha}]$ is one-dimensional, $h_\alpha = [e_\alpha e_{-\alpha}]$ for some $e_\alpha \in \mathfrak{L}_\alpha$, $e_{-\alpha} \in \mathfrak{L}_{-\alpha}$. Since $h_\alpha \neq 0$ there is a root γ such that $\gamma(h_\alpha) \neq 0$ by (ix). By (x) there is a non-negative integer r such that $\beta = \gamma - r\alpha$ is a root and $\beta - \alpha$ is not a root. Let a_0 be a non-zero element of $\mathfrak{L}_\beta$, and let $\mathfrak{L}_1$ be the subalgebra spanned by $\mathfrak{L}$, e_α , and $e_{-\alpha}$. We apply Lemma 1 with U the adjoint representation: $aU(b) = [ab]$. The weights of this representation are the roots of $\mathfrak{L}$ with respect to $\mathfrak{L}$. Since $a_k \in \mathfrak{L}_{\beta+k\alpha}$ it follows from (v) that there is a positive integer i such that $a_{i-1} \neq 0$, $a_i = 0$, and we have either $p = 0$ or $i < p$. Furthermore $[a_0 e_{-\alpha}] \in \mathfrak{L}_{\beta-\alpha} = 0$. By Lemma 1,

$$0 = [a_i e_{-\alpha}] = i \left(\beta + \frac{i-1}{2} \alpha \right) (h_\alpha) a_{i-1},$$

or

$$\beta(h_\alpha) + \frac{i-1}{2} \alpha(h_\alpha) = 0,$$

and

$$\gamma(h_\alpha) = \beta(h_\alpha) + r\alpha(h_\alpha) = -\frac{i-1}{2} \alpha(h_\alpha) + r\alpha(h_\alpha).$$

Since $\gamma(h_\alpha) \neq 0$ we have $\alpha(h_\alpha) \neq 0$, and (xi) is established.

(xii) *If α is a non-zero root, then $\mathfrak{L}_\alpha$ is one-dimensional.*

Proof. If the dimension of $\mathfrak{L}_\alpha$ is not one, it follows from (iv) that there is a non-zero $a_0 \in \mathfrak{L}_\alpha$ such that $[a_0 e_{-\alpha}] = 0$, where e_α and $e_{-\alpha}$ are as above. Using e_α , we form the sequence of a_k as before, and again for some i we have $a_{i-1} \neq 0$, $a_i = 0$, $i < p$ if $p \neq 0$. Hence

$$i \left(\alpha + \frac{i-1}{2} \alpha \right) (h_\alpha) = 0,$$

giving $\frac{1}{2}(i+1)\alpha(h_\alpha) = 0$. Since $\alpha(h_\alpha) \neq 0$ by (xi), we have $p > 0$, $i = p-1$, and $\alpha, 2\alpha, \dots, \alpha + (p-2)\alpha = -\alpha$ are roots, contrary to (v). Thus (xii) is proved.

(xiii) *If $\alpha, \beta, \alpha + \beta$ are non-zero roots, $[\mathfrak{L}_\alpha \mathfrak{L}_\beta] = \mathfrak{L}_{\alpha+\beta}$.*

Proof. By an application of the second part of Lemma 2, $[\mathfrak{L}_\alpha \mathfrak{L}_\beta] \neq 0$. Since $\mathfrak{L}_{\alpha+\beta}$ is one-dimensional and since $[\mathfrak{L}_\alpha \mathfrak{L}_\beta] \subset \mathfrak{L}_{\alpha+\beta}$, we have the result.

(xiv) *Let β be a root and α a non-zero root. Let $i+1$ be the smallest positive integer such that $\beta - (i+1)\alpha$ is not a root. Let $j+1$ be the smallest positive integer such that $\beta + (j+1)\alpha$ is not a root. Let $A_{\beta,\alpha}$ denote the rational integer $i-j$ and let $\bar{A}_{\beta,\alpha}$ denote the corresponding element of the prime field of $\mathfrak{F}$. Then*

$$\bar{A}_{\beta,\alpha} = \frac{2\beta(h_\alpha)}{\alpha(h_\alpha)}.$$

Proof. Apply Lemma 2 with β replaced by $\beta - i\alpha$. This gives

$$\bar{i} + \bar{j} = -\frac{2(\beta - i\alpha)(h_\alpha)}{\alpha(h_\alpha)} = -\frac{2\beta(h_\alpha)}{\alpha(h_\alpha)} + 2\bar{i}.$$

Hence

$$\bar{A}_{\beta, \alpha} = \bar{i} - \bar{j} = \frac{2\beta(h_\alpha)}{\alpha(h_\alpha)}.$$

The $A_{\beta, \alpha}$ are called *root-integers*.

(xv) If α is a non-zero root, then 2α is not a root.

Proof. Use (xii), (xiii), and $[e_\alpha e_\alpha] = 0$.

(xvi) If α is a non-zero root, then $\pm\alpha$ and 0 are the only integral multiples of α that are roots.

Proof. Suppose $r \neq \pm 1$, 0 is an integer such that $r\alpha$ is a root. By (vii) and (xv) we may suppose $r \geq 3$, $r\alpha - \alpha$ is not a root, and either $p = 0$ or $r < \frac{1}{2}p$. By (xiv), $\bar{A}_{r\alpha, \alpha} = 2r$, so $A_{r\alpha, \alpha} \equiv 2r \pmod{p}$; but $A_{r\alpha, \alpha} \leq 0$, since $r\alpha - \alpha$ is not a root. Hence $p \neq 0$ and $A_{r\alpha, \alpha} \leq 2r - p < 0$. This implies that $r\alpha$, $(r+1)\alpha$, $\dots$, $-r\alpha$ are roots. In particular, $\frac{1}{2}(p+1)\alpha = \frac{1}{2}\alpha$ is a root, contradicting (xv).

(xvii) If α is a non-zero root and $\beta \in \mathfrak{S}^*$, then β , $\beta + 2\alpha$, $\beta + 4\alpha$ are not all roots.

Proof. Suppose all three are roots. By (xvi), $\beta \neq 0$ and $\beta + 4\alpha \pm \beta$ are not roots. Hence $A_{\beta+4\alpha, \beta} = 0$. Therefore $(\beta + 4\alpha)(h_\beta) = 0$.

$$\bar{A}_{\beta+2\alpha, \beta} = \frac{2\beta(h_\beta) + 4\alpha(h_\beta)}{\beta(h_\beta)} = 1.$$

$A_{\beta+2\alpha, \beta} \equiv 1 \pmod{p}$. Since not all $\beta + 2\alpha + k\beta$ are roots, $A_{\beta+2\alpha, \beta} = 1$ and $\beta + 2\alpha - \beta = 2\alpha$ is a root, contrary to (xv).

(xviii) $-3 \leq A_{\beta, \alpha} \leq 3$.

Proof. By (xvii), the i and j of (xiv) are at most 3. Hence $-3 \leq i - j \leq 3$.

(xix) If α and β are non-zero roots, then $A_{\alpha, \beta} = 0$ if and only if $A_{\beta, \alpha} = 0$.

Proof. Suppose $A_{\alpha, \beta} = 0$, $A_{\beta, \alpha} \neq 0$. Then $\beta \neq \pm\alpha$. Replacing β by $-\beta$ if necessary, we may assume $A_{\beta, \alpha} < 0$. Then $\beta + \alpha$ is a non-zero root. Since $A_{\alpha, \beta} = 0$ this implies that $\alpha - \beta$ and therefore $\beta - \alpha$ are roots. Since $A_{\beta, \alpha} < 0$, it follows that $\beta + 2\alpha$ is a root. By (xv), $\beta + 2\alpha \pm \beta$ are not roots, so $A_{\beta+2\alpha, \beta} = 0$, giving $2\alpha(h_\beta) = -\beta(h_\beta) \neq 0$. Thus $A_{\alpha, \beta} \neq 0$, a contradiction.

4. Root-integers and strings of roots.

Lemma 3. If α , β , $\alpha + \beta$, and γ are roots and $\gamma \neq 0$, then

$$A_{\alpha+\beta, \gamma} = A_{\alpha, \gamma} + A_{\beta, \gamma}.$$

Proof. By (xiv), $\bar{A}_{\alpha+\beta, \gamma} = \bar{A}_{\alpha, \gamma} + \bar{A}_{\beta, \gamma}$, i.e.,

$$A_{\alpha+\beta, \gamma} \equiv A_{\alpha, \gamma} + A_{\beta, \gamma} \pmod{p}.$$

Since either $p = 0$ or $p > 9$ and since each term in the congruence lies between -3 and 3 , the congruence must be an equality. This proves the lemma.

Theorem 1. *Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be non-zero roots such that the determinant $|A_{\alpha_i, \alpha_j}| \neq 0$. Let β be a root. Then every sequence of roots of the form*

$$\beta_0 = \beta, \quad \beta_1 = \beta - \alpha_{k_1}, \quad \beta_2 = \beta - \alpha_{k_1} - \alpha_{k_2}, \dots$$

($1 \leq k_i \leq n$) terminates in a root γ such that $\gamma - \alpha_i$ is not a root for $1 \leq i \leq n$.

Proof. Suppose $\beta_0, \beta_1, \dots$ is an infinite sequence of this type. Then we can write

$$(3) \quad \beta_m = \beta_0 - \sum_{i=1}^m s_i^{(m)} \alpha_i$$

where $s_i^{(m)}$ is the number of times α_i occurs among $\alpha_{k_1}, \alpha_{k_2}, \dots, \alpha_{k_m}$. Using Lemma 3 and induction on m we obtain

$$(4) \quad A_{\beta_m, \alpha_j} = A_{\beta, \alpha_j} - \sum_{i=1}^m s_i^{(m)} A_{\alpha_i, \alpha_j}$$

for all m, j . Since there are only a finite number of roots by (vi), $\beta_u = \beta_v$ for some $u > v$. Substitution in (4) gives

$$\sum_{i=1}^n s_i^{(u)} A_{\alpha_i, \alpha_j} = \sum_{i=1}^n s_i^{(v)} A_{\alpha_i, \alpha_j},$$

and the system of equations

$$\sum_{i=1}^n x_i A_{\alpha_i, \alpha_j} = 0, \quad 1 \leq j \leq n,$$

has the non-trivial solution $x_i = s_i^{(u)} - s_i^{(v)}$, contradicting the hypothesis that the determinant is not zero.

Now if we did not arrive at a root γ such that $\gamma - \alpha_i$ is not a root, $1 \leq i \leq n$, then we could form such an infinite sequence. This completes the proof.³

Lemma 4. *If $\alpha_1, \alpha_2, \dots, \alpha_n$ are linearly dependent non-zero roots, then $|\bar{A}_{\alpha_i, \alpha_j}| = 0$.*

Proof. Suppose $\lambda_i \in \mathfrak{F}$, λ_i not all zero, $\sum \lambda_i \alpha_i = 0$. Then

$$\frac{2}{\alpha_j(h_{\alpha_j})} \sum_{i=1}^n \lambda_i \alpha_i(h_{\alpha_j}) = 0, \quad 1 \leq j \leq n,$$

or

$$\sum_{i=1}^n \lambda_i \bar{A}_{\alpha_i, \alpha_j} = 0, \quad 1 \leq j \leq n.$$

This implies $|\bar{A}_{\alpha_i, \alpha_j}| = 0$.

³ In the case of characteristic zero Theorem 1 is an immediate consequence of Lemma 4 and the fact that there are only a finite number of roots. The proof of Lemma 4 does not use Theorem 1.

5. A theorem on real matrices and its application.

Lemma 5. Let $M = (m_{ij})$ be an $n \times n$ real matrix such that:

(a) $m_{ij} \leq 0$ if $i \neq j$.

(b) Every proper principal minor of M is non-negative.

If there exist non-negative real numbers $t_1, t_2, \dots, t_n$, not all zero, such that

$$\sum_{i=1}^n t_i m_{ij} \geq 0, \quad 1 \leq j \leq n,$$

then $|M| \geq 0$.

Proof. If $n = 1$, then $t_1 > 0$, $t_1 m_{11} \geq 0$. Hence $|M| = m_{11} \geq 0$. Now let $n > 1$ and assume that the lemma holds for all $r \times r$ matrices with $r < n$. Suppose $\sum_{i=1}^n t_i m_{ij} = 0$ for exactly k values of j . If $k = n$, then $|M| = 0$ because the corresponding linear equations have a non-trivial solution. We proceed by induction downward on k . Suppose that $k < n$ and that the conclusion of the lemma holds for all $n \times n$ matrices M' satisfying (a), (b) and such that for the same t_i as above $\sum_{i=1}^n t_i m'_{ij} = 0$ for $k + 1$ values of j . Without loss of generality assume $\sum_{i=1}^n t_i m_{i1} > 0$. Since all $t_i \geq 0$ and $m_{i1} \leq 0$ if $i > 1$, we have $t_1 > 0$. Set

$$(5) \quad m'_{11} = -\frac{1}{t_1} \sum_{i=2}^n t_i m_{i1}.$$

Then $m_{11} t_1 > m'_{11} t_1 \geq 0$, or $m_{11} > m'_{11} \geq 0$. Define a new $n \times n$ matrix M' by (5) and by $m'_{ij} = m_{ij}$ if $(i, j) \neq (1, 1)$.

Case 1. Some proper principal minor P of M' is negative. We may suppose P chosen of minimal size. Since P is of minimal size, P satisfies (b); (a) is also satisfied by P . Furthermore, since P is negative it cannot be a principal minor of M . Hence P contains the element m'_{11} . Without loss of generality we may assume P to consist of elements in the first r rows and the first r columns of M' . But then

$$\sum_{i=1}^r t_i m'_{ij} \geq -\sum_{i=r+1}^n t_i m'_{ij} \geq 0, \quad 1 \leq j \leq r,$$

and $t_1 > 0$. By the induction hypothesis $P \geq 0$, a contradiction.

Case 2. Every proper principal minor of M' is non-negative. Then M' satisfies (a) and (b). Moreover,

$$|M| - |M'| = (m_{11} - m'_{11})M_{11},$$

where M_{11} is the cofactor of m_{11} in M (all other terms in the expansions of $|M|$ and $|M'|$ by the first row cancel). Since M_{11} is a principal minor, $M_{11} \geq 0$, and since $m_{11} > m'_{11}$, we have $(m_{11} - m'_{11})M_{11} \geq 0$. Therefore $|M'| \leq |M|$. Furthermore $\sum_{i=1}^n t_i m'_{ij} \geq 0$, $1 \leq j \leq n$, and $\sum_{i=1}^n t_i m'_{ij} = 0$ for $k + 1$ values of j . Hence $|M'| \geq 0$ by the induction hypothesis. It follows at once that $|M| \geq 0$, and the proof by induction is complete.

Theorem 2. Let $M = (m_{ij})$ be a real $n \times n$ matrix such that:

- (a) $m_{ii} \leq 0$ if $i \neq j$.
- (b) Every proper principal minor of M is positive.
- (c) $|M| \leq 0$.

If $t_1, t_2, \dots, t_n$ are non-negative real numbers such that

$$\sum_{i=1}^n t_i m_{ij} \geq 0, \quad 1 \leq j \leq n,$$

then

$$\sum_{i=1}^n t_i m_{ij} = 0, \quad 1 \leq j \leq n.$$

Proof. Suppose the theorem is false. Then without loss of generality we can assume $\sum_{i=1}^n t_i m_{i1} > 0$. Put $m'_{11} = m_{11} - \epsilon$, $m'_{ij} = m_{ij}$ for $(i, j) \neq (1, 1)$. Then, for sufficiently small positive ϵ , M' satisfies (a) and (b) of the hypotheses of Lemma 5. As in the proof of Lemma 5 we have

$$|M| - |M'| = (m_{11} - m'_{11})M_{11} = \epsilon M_{11},$$

where M_{11} is the cofactor of m_{11} in M . Since $M_{11} > 0$, $|M'| < |M| \leq 0$. Now $\sum_{i=1}^n t_i m_{i1} > 0$, so not all t_i are zero; and for ϵ sufficiently small we have all $\sum_{i=1}^n t_i m'_{ij} \geq 0$; $1 \leq j \leq n$. By Lemma 5, $|M'| \geq 0$, a contradiction. This completes the proof.

Theorem 3. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be non-zero roots. Suppose there exist real numbers A'_{ij} , $1 \leq i, j \leq n$, such that $A_{\alpha_i, \alpha_j} \leq A'_{ij} \leq 0$ for all $i \neq j$ and $A'_{ii} = 2$ ($= A_{\alpha_i, \alpha_i}$), $1 \leq i \leq n$. Suppose $|A'_{ij}| \leq 0$ and that every proper principal minor of the matrix (A'_{ij}) is positive. Then $A_{\alpha_i, \alpha_j} = A'_{ij}$ for all i, j and $|A_{\alpha_i, \alpha_i}| = 0$. Furthermore, there exist positive integers x_i such that

$$\sum_{i=1}^n x_i A_{\alpha_i, \alpha_j} = 0, \quad 1 \leq j \leq n,$$

and for any such integers

$$\sum_{i=1}^n x_i \alpha_i = 0.$$

Finally, $\alpha_1, \alpha_2, \dots, \alpha_n$ are linearly dependent.

Proof. We first show that any sequence of roots of the type $\beta_0 = 0, \beta_1 = \alpha_{k_1}, \beta_2 = \beta_1 + \alpha_{k_2}, \dots, \beta_r = \beta_{r-1} + \alpha_{k_r}$ can be extended. Let $\beta_0, \beta_1, \dots, \beta_r$ be such a sequence, $r \geq 1$. Then for all m such that $0 \leq m \leq r$ we have $\beta_m = \sum_{i=1}^n s_i^{(m)} \alpha_i$, where $s_i^{(m)}$ is the number of times i occurs among $k_1, k_2, \dots, k_m$. Now if $\sum_{i=1}^n s_i^{(r)} A'_{ij} < 0$ for some j then, by repeated application of Lemma 3,

$$A_{\beta_r, \alpha_j} = \sum_{i=1}^n s_i^{(r)} A_{\alpha_i, \alpha_j} \leq \sum_{i=1}^n s_i^{(r)} A'_{ij} < 0$$

and $\beta_r + \alpha_j$ is a root. If $\sum_{i=1}^n s_i^{(r)} A'_{ij} \geq 0$ for all j , then by Theorem 2 $\sum_{i=1}^n s_i^{(r)} A'_{ij} = 0$, $1 \leq j \leq n$, and

$$A_{\beta_r, \alpha_j} \leq \sum_{i=1}^n s_i^{(r)} A'_{ij} = 0, \quad 1 \leq j \leq n.$$

Now $r - 1 \geq 0$ so that $\beta_{r-1} = \beta_r - \alpha_{k_r}$ is a root and $A_{\beta_r, \alpha_{k_r}} \leq 0$. Hence $\beta_r + \alpha_{k_r}$ is a root. Thus in every case we can find a root β_{r+1} of the desired type. Hence we can form an infinite sequence of roots

$$\beta_0 = 0, \beta_1 = \alpha_1, \beta_2 = \beta_1 + \alpha_{k_2}, \dots, \beta_r = \beta_{r-1} + \alpha_{k_r}, \dots$$

Since there are only a finite number of roots we have $\beta_u = \beta_v$ for some $u > v$, $A_{\beta_u, \alpha_j} = A_{\beta_v, \alpha_j}$, $1 \leq j \leq n$, and $x_i = s_i^{(u)} - s_i^{(v)}$, $1 \leq i \leq n$, are non-negative integers, not all zero, satisfying

$$(6) \quad \sum_{i=1}^n x_i A_{\alpha_i, \alpha_j} = 0, \quad 1 \leq j \leq n.$$

It follows that $|A_{\alpha_i, \alpha_j}| = 0$. Furthermore

$$(7) \quad \sum_{i=1}^n x_i A'_{ij} \geq \sum_{i=1}^n x_i A_{\alpha_i, \alpha_j} = 0, \quad 1 \leq j \leq n.$$

By Theorem 2, $\sum_{i=1}^n x_i A'_{ij} = 0$ for all j . Moreover if $x_k = 0$ for some k , then $\sum_{i \neq k} x_i A'_{ij} = 0$, $j \neq k$, contradicting the assumption that the $(n-1)$ -rowed principal minors are positive. Hence all $x_i > 0$ and (7) yields $A_{\alpha_i, \alpha_j} = A'_{ij}$ for all i, j .

Now let $x_1, x_2, \dots, x_n$ be a positive integral solution of (6), and put $u = \sum x_i$. We will show that the sequence of roots

$$(8) \quad \beta_0 = 0, \beta_1 = \alpha_{k_1}, \beta_2 = \beta_1 + \alpha_{k_2}, \dots, \beta_m = \beta_{m-1} + \alpha_{k_m}, \dots$$

can be chosen in such a way that $\beta_u = \sum_{i=1}^n x_i \alpha_i$. For any root β we have either $A_{\beta, \alpha_j} \geq 0$, $1 \leq j \leq n$, or $A_{\beta, \alpha_k} < 0$ for some k . If $A_{\beta, \alpha_k} < 0$ for some k , then $\beta + \alpha_k$ is a root. Hence we can choose the sequence (8) so that for every m we have either $A_{\beta_m, \alpha_j} \geq 0$ for all j or $A_{\beta_m, \alpha_{k_{m+1}}} < 0$, where $\beta_{m+1} = \beta_m + \alpha_{k_{m+1}}$. As before, $\beta_m = \sum_{i=1}^n s_i^{(m)} \alpha_i$ where $s_i^{(m)}$ is the number of times i occurs among $k_1, k_2, \dots, k_m$. We shall show by induction on m that $s_i^{(m)} \leq x_i$ for $1 \leq i \leq n$, $0 \leq m \leq u$. This is immediate for $m = 0$. Suppose $1 \leq m \leq u$ and that $s_i^{(m-1)} \leq x_i$, $1 \leq i \leq n$. There are two cases:

Case 1. $A_{\beta_{m-1}, \alpha_j} < 0$ for some j . Then $\beta_m = \beta_{m-1} + \alpha_r$ where $r = k_m$ and $A_{\beta_{m-1}, \alpha_r} < 0$ by the choice of the sequence (8). In this case if $s_r^{(m-1)} = x_r$ then

$$0 > A_{\beta_{m-1}, \alpha_r} = \sum_{i=1}^n s_i^{(m-1)} A_{\alpha_i, \alpha_r} \geq \sum_{i=1}^n x_i A_{\alpha_i, \alpha_r} = 0$$

since $A_{\alpha_i, \alpha_r} \leq 0$ for $i \neq r$. Therefore $s_r^{(m-1)} < x_r$, so that $s_r^{(m)} \leq x_r$. For $i \neq r$ we have $s_i^{(m)} = s_i^{(m-1)} \leq x_i$.

Case 2. $A_{\beta_{m-1}, \alpha_j} \geq 0$ for all values of j . Here $\sum_{i=1}^n s_i^{(m-1)} A_{\alpha_i, \alpha_j} \geq 0$ for all j . By Theorem 2 we have $\sum_{i=1}^n s_i^{(m-1)} A_{\alpha_i, \alpha_j} = 0$ for all j . Now the rank of (A_{α_i, α_j}) is $n - 1$, since it has non-zero $(n - 1)$ -rowed principal minors. Hence $(s_1^{(m-1)}, \dots, s_n^{(m-1)})$ is a rational multiple of $(x_1, \dots, x_n)$. Since

$$\sum_{i=1}^n s_i^{(m-1)} = m - 1 < u = \sum_{i=1}^n x_i,$$

we have $s_i^{(m-1)} < x_i$ for all i . Hence $s_i^{(m)} \leq s_i^{(m-1)} + 1 \leq x_i$ for all i .

It follows that $\sum x_i \alpha_i = \beta_u$ is a root, since it belongs to the sequence (8).

Now $2x_1, 2x_2, \dots, 2x_n$ is also a solution of (6). Hence $\sum 2x_i \alpha_i = 2 \sum x_i \alpha_i$ is also a root. Therefore $\sum x_i \alpha_i = 0$ by (xv). Finally we note that (6) has a positive solution with not all x_i divisible by the characteristic p of $\mathfrak{F}$. Therefore $\alpha_1, \alpha_2, \dots, \alpha_n$ are linearly dependent.

6. Systems of roots. A set $\alpha_1, \alpha_2, \dots, \alpha_m$ of non-zero roots will be called a *system* of roots if $\alpha_i - \alpha_j$ is not a root for $i \neq j$. We see that in any system the roots are distinct and that $A_{\alpha_i, \alpha_j} \leq 0$ if $i \neq j$. A system $\alpha_1, \alpha_2, \dots, \alpha_m$ of roots will be called *semi-simple* if $\alpha_1, \alpha_2, \dots, \alpha_m$ are linearly independent.

Lemma 6. *If $\alpha_1, \alpha_2, \dots, \alpha_m$ is a semi-simple system of roots, then $|A_{\alpha_i, \alpha_i}| > 0$.*

Proof. First note that any subset of a semi-simple system is a semi-simple system. The assertion is true for $m = 1$. Assume the lemma holds for all semi-simple systems of fewer than m roots and that $|A_{\alpha_i, \alpha_i}| \leq 0$. Then every proper principal minor of this matrix is positive and we can apply Theorem 3 with $A'_{ij} = A_{\alpha_i, \alpha_j}$ to conclude that $\alpha_1, \dots, \alpha_m$ are linearly dependent, a contradiction. Hence $|A_{\alpha_i, \alpha_i}| > 0$ for all semi-simple systems by induction.

A set of non-zero roots is called *decomposable* if it is the union of two disjoint subsets S_1, S_2 such that $A_{\alpha_i, \alpha_j} = 0$ for all $\alpha_i \in S_1, \alpha_j \in S_2$. Otherwise $\alpha_1, \dots, \alpha_m$ is called *indecomposable*. A system of roots is called *simple*⁴ if it is semi-simple and indecomposable.

Lemma 7. *Let $S = \{\alpha_1, \dots, \alpha_r\}$ be a semi-simple system of roots which is the union of simple systems, each of which is maximal in the complete set of roots of $\mathfrak{L}$ with respect to $\mathfrak{S}$. Let β be a root such that $\beta, \alpha_1, \dots, \alpha_r$ are linearly independent. Then $A_{\beta, \alpha_i} = 0$ and $\beta + \alpha_i$ is not a root, $1 \leq i \leq r$.*

Proof.

Case 1. No $\beta - \alpha_i$ is a root. If $A_{\beta, \alpha_i} \neq 0$ for some i in this case, we could adjoin β to the simple component containing α_i , contradicting its maximality. Therefore $A_{\beta, \alpha_i} = 0$ for all i . Since no $\beta - \alpha_i$ is a root, no $\beta + \alpha_i$ is a root, $1 \leq i \leq r$.

Case 2. $\beta - \alpha_j$ is a root for some j . By Lemma 6, $|A_{\alpha_i, \alpha_i}| > 0$. Hence by Theorem 1 there is a finite sequence of roots

⁴ This is a slightly different terminology from the one used in [5] and [8].

$$\beta_0 = \beta, \beta_1 = \beta_0 - \alpha_i, \dots, \beta_u = \beta_{u-1} - \alpha_{k_u}$$

such that $u \geq 1$ and $\beta_u - \alpha_i$ is not a root, $1 \leq i \leq r$. Now $\beta_u, \alpha_1, \dots, \alpha_r$ are linearly independent. Hence $\beta_{u-1} = \beta_u + \alpha_{k_u}$ is not a root by Case 1 above. Therefore Case 2 is impossible, and the proof is complete.

Lemma 8. *Let S be as in Lemma 7. Let $T = \{\beta_1, \dots, \beta_t\}$ be a simple system of roots with respect to $\mathfrak{S}$. Then either*

- (a) $S \cup T$ is linearly independent, and $A_{\beta_i, \alpha_i} = 0$ for all β_i, α_i ; or
- (b) every β_i is a linear combination of the α_i , and for every β_i there is an α_i such that $A_{\beta_i, \alpha_i} \neq 0$.

Proof. Without loss of generality suppose there is an integer k , $0 \leq k \leq t$, such that $A_{\beta_j, \alpha_i} = 0$ for all α_i if $j \leq k$ and $A_{\beta_j, \alpha_i} \neq 0$ for some α_i if $j > k$. By Lemma 7, β_j is a linear combination of the α_i whenever $j > k$. For $j' \leq k < j$ we have $A_{\beta_j, \beta_{j'}} = 0$ by (xix) and (xiv), and hence $A_{\beta_{j'}, \beta_{j'}} = 0$ by (xviii). Since T is simple, it is indecomposable, and hence either $k = 0$ or $k = t$. If $k = 0$, the situation (b) holds.

Now suppose $k = t$ and that (a) does not hold, i.e., all $A_{\beta_i, \alpha_i} = 0$ and $S \cup T$ is linearly dependent. Since S and T separately are linearly independent sets, there is a non-zero $\gamma \in \mathfrak{S}^*$ such that $\gamma = \sum_{i=1}^r \lambda_i \alpha_i = \sum_{j=1}^t \mu_j \beta_j$, where $\lambda_i, \mu_j \in \mathfrak{F}$. Let α be a non-zero root that is a linear combination of the α_i . Then $A_{\alpha, \beta_i} = 0$ for all β_i by (xix) and (xiv); by (xviii) all $A_{\alpha, \beta_i} = 0$, and hence all $A_{\beta_i, \alpha} = 0$ by (xix). Thus all $\beta_i(h_\alpha) = 0$ by (xiv), and therefore $\gamma(h_\alpha) = 0$. Next let β be a root that is not a linear combination of the α_i . Then $A_{\beta, \alpha_i} = 0$ for all i by Lemma 7. Hence $A_{\alpha, \beta} = 0$ and $\alpha(h_\beta) = 0$ for all i . Therefore $\gamma(h_\beta) = 0$. By (viii), $\gamma(h) = 0$ for all $h \in \mathfrak{S}$. Thus $\gamma = 0$, a contradiction, and Lemma 8 is established.

If S and T are semi-simple systems that span the same subspace of $\mathfrak{S}^*$, we shall write $S \sim T$. Any root, or more generally any simple system of roots, can be embedded in a maximal simple system. By Lemma 8, there is a collection $S_1, S_2, \dots, S_s$ of disjoint maximal simple systems such that $S = S_1 \cup S_2 \cup \dots \cup S_s$ is a basis for $\mathfrak{S}^*$. Let $S = \{\alpha_1, \dots, \alpha_r\}$ and let $T = \{\beta_1, \dots, \beta_t\}$ be any simple system. By Lemma 8, $A_{\beta_i, \alpha_i} \neq 0$ for some i . Suppose $\alpha_i \in S_k$. Then by Lemma 8 with S replaced by S_k we see that every β_i belongs to the space spanned by S_k . If T is a maximal simple system, another application of Lemma 8 shows that $T \sim S_k$. On the other hand, when T consists of a single root we conclude that every root is a linear combination of one of the S_i .

Theorem 4. *Let the system S be a basis for $\mathfrak{S}^*$, where*

$$S = S_1 \cup S_2 \cup \dots \cup S_s,$$

S_i maximal simple systems. Then every root α is a linear combination of one of the S_i . Let T_i be the set of all non-zero roots that are linear combinations of S_i . Let

$\mathfrak{L}_i$ denote the subspace of $\mathfrak{L}$ spanned by all $\mathfrak{L}_\alpha$, $\alpha \in T_i$, and by all h_α , $\alpha \in T_i$. Then $\mathfrak{L}_i$ is an ideal of $\mathfrak{L}$ and

$$\mathfrak{L} = \mathfrak{L}_1 \oplus \mathfrak{L}_2 \oplus \cdots \oplus \mathfrak{L}_s.$$

Proof. Clearly $[\mathfrak{L}_i, \mathfrak{L}] \subset \mathfrak{L}_i$. If $\alpha \in T_i$, $\beta \in T_j$, $j \neq i$, then $\alpha + \beta$ is not a root so that $[\mathfrak{L}_\alpha, \mathfrak{L}_\beta] = 0$, and $[h_\alpha, \mathfrak{L}_\beta] = 0$ since $A_{\beta, \alpha} = 0$. Hence $[\mathfrak{L}_i, \mathfrak{L}_\beta] = 0$. Since we evidently have $[\mathfrak{L}_i, \mathfrak{L}_\alpha] \subset \mathfrak{L}_i$ for all $\alpha \in T_i$, we see that $[\mathfrak{L}_i, \mathfrak{L}] \subset \mathfrak{L}_i$ and $\mathfrak{L}_i$ is an ideal. Clearly $\mathfrak{L} = \mathfrak{L}_1 + \cdots + \mathfrak{L}_s$. If this sum is not direct we must have a relation of the form

$$\sum_{\alpha \in T_i} \lambda_\alpha h_\alpha = \sum_{\alpha \notin T_i} \lambda_\alpha h_\alpha = h \neq 0, \quad \lambda_\alpha \in \mathfrak{F}.$$

Now there is a root β such that $\beta(h) \neq 0$. If $\beta \in T_i$, we see from the second representation of h that $\beta(h) = 0$. If $\beta \notin T_i$, the first representation gives $\beta(h) = 0$. In either case we have a contradiction, and hence $\mathfrak{L} = \mathfrak{L}_1 \oplus \cdots \oplus \mathfrak{L}_s$.

Now each $\mathfrak{L}_i$ is a Lie algebra satisfying (i)–(v) with $\mathfrak{S}$ replaced by $\mathfrak{S} \cap \mathfrak{L}_i$. Thus we may restrict ourselves to the case $s = 1$, i.e., where every maximal simple system spans $\mathfrak{S}^*$.

7. Systems of roots. Diagrams and determinants. In the sequel we shall use $A_{i,j}$ (or $A_{i,i}$) as an abbreviation for A_{α_i, α_j} .

Lemma 9. If α_1, α_2 is a system of two roots then $0 \leq A_{12}A_{21} \leq 4$.

Proof. Since $\alpha_1 - \alpha_2$ and $\alpha_2 - \alpha_1$ are not roots we have $-3 \leq A_{12} \leq 0$, $-3 \leq A_{21} \leq 0$. If $A_{12} \leq -2$ and $A_{21} \leq -2$ we apply Theorem 3 with $n = 2$, $A'_{12} = A'_{21} = -2$ to obtain $A_{12} = A_{21} = -2$ and $A_{12}A_{21} = 4$. If either A_{12} or A_{21} is -1 then $1 \leq A_{12}A_{21} \leq 3$, and if either A_{12} or A_{21} is 0 then $A_{12}A_{21} = 0$. This establishes the lemma.

Systems of roots are represented by diagrams consisting of dots and lines; the dots represent the roots and the lines their relationships as follows: If α_1 and α_2 are roots we connect their dots by a single line if $A_{12}A_{21} = 1$, a double line if $A_{12}A_{21} = 2$, a triple line if $A_{12}A_{21} = 3$, and a quadruple line if $A_{12}A_{21} = 4$. We recall that $A_{12} = 0$ if and only if $A_{21} = 0$. In this case the dots of α_1 and α_2 are not directly connected by a line.

Lemma 10. Let $n \geq 2$, let $\alpha_1, \dots, \alpha_n$ be a system of roots such that $A_{n,j} = 0$ for $j < n - 1$, and let $A^{(s)}$ represent the $s \times s$ matrix $(A_{i,j})$, $1 \leq i, j \leq s$, $|A^{(0)}| = 1$. Then

$$|A^{(n)}| = 2 |A^{(n-1)}| - A_{n,n-1}A_{n-1,n} |A^{(n-2)}|.$$

Proof. By (xix), $A_{i,n} = 0$ for $j < n - 1$. Hence if we expand $|A^{(n)}|$ by the n -th row we obtain the desired result.

We next use Lemma 10 to compute the determinants of the root-integers for systems that correspond to certain diagrams, which are prominent in the classical theory and whose significance will become clear later. They are the diagrams

FIGURE 1.

shown in Figure 1. In these diagrams the dot corresponding to the root α_i is labeled i . B_r denotes a system with $A_{r-1,r} = -2$ and C_r a system with $A_{r,r-1} = -2$. For F_4 we take $A_{23} = -2$ and for G_2 we take $A_{12} = -3$.

Lemma 11. *If we denote by $|X|$ the determinant $|A_{ij}|$ for a system having the diagram X in Figure 1, then:*

$$\begin{aligned} |A_r| &= r + 1; & |B_r| &= |C_r| = 2; & |D_r| &= 4; \\ |E_r| &= 9 - r; & |F_4| &= |G_2| = 1. \end{aligned}$$

Proof. Evidently $|A_1| = 2$. By Lemma 10, $|A_2| = 2 \cdot 2 - 1 = 3$, $|C_2| = 2 \cdot 2 - 2 = 2$, and $|G_2| = 2 \cdot 2 - 3 = 1$. Lemma 10 yields $|A_r| = 2 |A_{r-1}| - |A_{r-2}|$. By induction on r we obtain $|A_r| = r + 1$. For $r \geq 3$, Lemma 10 gives us $|B_r| = |C_r| = 2 |A_{r-1}| - 2 |A_{r-2}| = 2$. For $r \geq 4$ we have $|D_r| = 2 |A_{r-1}| - |A_{r-3}| \cdot |A_1| = 2r - 2(r - 2) = 4$. For E_r we have $|E_r| = 2 |A_{r-1}| - |A_{r-4}| = 2r - 3(r - 3) = 9 - r$. Finally, $|F_4| = 2 |B_3| - |A_2| = 4 - 3 = 1$.

8. Systems with cycles. A system $\alpha_1, \dots, \alpha_n$ of roots (or its diagram) will be called *exact* if $|A_{ii}| = 0$ and if all proper principal minors of (A_{ij}) are positive. Since the determinant of a decomposable system is the product of the determinants of its components, it follows that an exact system is indecomposable. By Theorem 3, the roots in an exact system are linearly dependent, and we can read off a linear relation among the roots from a non-trivial relation among the rows of the matrix of root-integers.

We shall say that the ordered system of roots $\alpha_1, \dots, \alpha_r$ ($r \geq 3$) forms a cycle if $A_{i,i+1} \neq 0$, $1 \leq i \leq r-1$, and if $A_{1r} \neq 0$.

Lemma 12. *Let $\alpha_1, \dots, \alpha_r$ form a cycle. Then this system has diagram H_r . (See Figure 2.) Furthermore H_r is exact and*

$$(9) \quad \sum_{i=1}^r \alpha_i = 0.$$

H_r ($r \geq 3$)

FIGURE 2.

Proof. Let $A'_{i,i+1} = A'_{i+1,i} = -1 = A'_{1r} = A'_{r1}$, $1 \leq i \leq r-1$, $A'_{ii} = 2$, $1 \leq i \leq r$, all other $A'_{ij} = 0$, $1 \leq i, j \leq r$. Then every proper principal minor of (A'_{ij}) is the product of certain $|A_s|$ and hence is positive by Lemma 11. Evidently $\sum_{i=1}^r A'_{ij} = 0$, $1 \leq j \leq r$. Hence $|A'_{ij}| = 0$. Since $A_{ii} \leq A'_{ij} \leq 0$ for $i \neq j$, and since $A'_{ii} = 2$, we can apply Theorem 3 to conclude that $A_{ij} = A'_{ij}$ for all i, j and that $\sum \alpha_i = 0$. This completes the proof.

Theorem 5. *The indecomposable systems containing cycles are precisely those corresponding to the diagrams H_r , $r \geq 3$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be an indecomposable system containing a cycle. If $\alpha_1, \dots, \alpha_n$ is a cycle, the result is immediate from Lemma 12. Otherwise let $r < n$ be the minimal number of roots forming a cycle, which we may assume to be the ordered system $\alpha_1, \dots, \alpha_r$. Since $\alpha_1, \dots, \alpha_n$ is indecomposable, $A_{ts} \neq 0$ for some $t \leq r < s$. But, by Lemma 12, $\sum_{i=1}^r \alpha_i = 0$. Hence $\sum_{i=1}^r \alpha_i(h_{\alpha_s}) = 0$. Since $\alpha_i(h_{\alpha_s}) \neq 0$ we have $\alpha_i(h_{\alpha_s}) \neq 0$, and hence $A_{ts} \neq 0$ for at least two values of $i \leq r$, say $A_{ts} \neq 0$, $A_{us} \neq 0$, $1 \leq t < u \leq r$. Then the ordered system $\alpha_t, \alpha_{t+1}, \dots, \alpha_u, \alpha_s$ forms a cycle C . Since r is minimal, C consists of either r or $r+1$ roots. If C contains $r+1$ roots, then $t=1$, $u=r$, and $A_{1r} = 0$, contrary to assumption. Therefore C contains r roots and either $t=1$, $u=r-1$ or $t=2$, $u=r$. In either case, $\alpha_t + \dots + \alpha_u + \alpha_s = \alpha_1 + \alpha_2 + \dots + \alpha_r$ by (9). Thus either $\alpha_s = \alpha_r$ or $\alpha_s = \alpha_1$. Since the roots in any system are distinct, this contradicts the assumption $s > r$ and completes the proof.

9. Systems without cycles.

Lemma 13. *Every system containing a quadruple line has I_2 as a subdiagram. (See Figure 3.) I_2 is exact, and if α_1, α_2 are the roots of I_2 , then*

$$(10) \quad \alpha_1 + \alpha_2 = 0.$$

Proof. The matrix of I_2 is

$$\begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix}.$$

FIGURE 3.

Hence its determinant is zero, the proper principal minors are positive, and by Theorem 3 we have $\alpha_1 + \alpha_2 = 0$.

Lemma 14. *If $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is an indecomposable system containing a triple line then either $n = 2$ and $S = G_2$ or S contains a subsystem with diagram G_3 (Figure 3). G_3 is exact and has $A_{23} = -3$ and*

$$(11) \quad \alpha_1 + 2\alpha_2 + 3\alpha_3 = 0.$$

Proof. The only system of two roots containing a triple line is G_2 . If $n \geq 3$, then S contains an indecomposable subsystem $\alpha_1, \alpha_2, \alpha_3$ with a triple line, say $A_{23}A_{32} = 3$, $A_{12} \neq 0$. Set $A'_{12} = A'_{21} = -1$, $A'_{23} = A_{23}$, $A'_{32} = A_{32}$, $A'_{11} = A'_{22} = A'_{33} = 2$, $A'_{13} = A'_{31} = 0$. Then we can associate with (A'_{ij}) the diagram G_3 which has determinant $2|A_2| - 3|A_1| = 0$ by Lemma 10. The proper principal minors of (A'_{ij}) are positive and $A_{ii} \leq A'_{ii} \leq 0$ for $i \neq j$, $1 \leq i, j \leq 3$. By Theorem 3 we have $A_{ii} = A'_{ii}$, $1 \leq i, j \leq 3$, so that $\alpha_1, \alpha_2, \alpha_3$ has diagram G_3 .

Now if $A_{32} = -3$ then

$$(A_{ij}) = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -3 & 2 \end{bmatrix}$$

so that $A_{1j} + 2A_{2j} + A_{3j} = 0$, $1 \leq j \leq 3$. By Theorem 3, $\alpha_1 + 2\alpha_2 + \alpha_3 = 0$, or $-\alpha_1 = \alpha_3 + 2\alpha_2$. Since $A_{32} = -3$, it follows that $\alpha_3 + 3\alpha_2 = \alpha_2 - \alpha_1$ is a root, a contradiction. Hence we must have $A_{23} = -3$, and $\alpha_1, \alpha_2, \alpha_3$ has diagram G_3 with matrix

$$\begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -3 \\ 0 & -1 & 2 \end{bmatrix}.$$

We note that $A_{1i} + 2A_{2i} + 3A_{3i} = 0$, $1 \leq i \leq 3$. Hence by Theorem 3, $\alpha_1 + 2\alpha_2 + 3\alpha_3 = 0$. This completes the proof.

If $\alpha_1, \dots, \alpha_n$ is a set of non-zero roots we shall use $A^{(r)}$ to denote the $r \times r$ matrix (A_{ij}) , $1 \leq i, j \leq r$, and $|A^{(r)}|$ to denote the corresponding determinant.

Lemma 15. *Let $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be an indecomposable system containing a double line, but no triple or quadruple lines. Then either $S = F_4$, or $S = C_n$ ($n \geq 2$),*

or $S = B_n (n \geq 3)$; or S has a subsystem with one of the diagrams $CC_r (r \geq 3)$, $BD_r (r \geq 4)$, or F_5 . (See Figure 4.) CC_r , BD_r , and F_5 are exact. Furthermore we have

$$(12) \quad A_{12} = A_{r, r-1} = -2 \quad \text{and} \quad \alpha_1 + 2 \sum_{i=2}^{r-1} \alpha_i + \alpha_r = 0,$$

$$(13) \quad A_{21} = -2 \quad \text{and} \quad 2 \sum_{i=1}^{r-2} \alpha_i + \alpha_{r-1} + \alpha_r = 0,$$

$$(14) \quad A_{34} = -2 \quad \text{and} \quad \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 2\alpha_5 = 0$$

for CC_r , BD_r , F_5 , respectively.

$CC_r (r \geq 3)$

$BD_r (r \geq 4)$

F_5

FIGURE 4.

Proof. By Theorem 5, S does not contain a cycle. Suppose first that S contains two double lines. Then, since S is indecomposable, S contains a subsystem, say $\alpha_1, \alpha_2, \dots, \alpha_r$, with diagram $CC_r (r \geq 3)$. We may suppose that the roots of this subsystem are labeled as in Figure 4 and that $A_{21} \leq A_{r-1, r}$. Note that all proper principal minors of $A^{(r)}$ are positive by Lemma 11. There are three cases:

Case 1. $A_{21} = A_{r-1, r} = -2$. In this case $\sum_{i=1}^r A_{ij} = 0, 1 \leq j \leq r$. Hence $|A^{(r)}| = 0$, and, by Theorem 3, $\alpha_1 + \alpha_2 + \dots + \alpha_r = 0$. Recalling the definition of the $A_{ij} = A_{\alpha_i, \alpha_j}$ and Lemma 3, we observe that the following are roots:

$$\alpha_2, \alpha_2 + \alpha_3, \alpha_2 + \alpha_3 + \alpha_4, \dots, \alpha_2 + \alpha_3 + \dots + \alpha_{r-1},$$

$$\alpha_2 + \alpha_3 + \dots + \alpha_{r-1} + 2\alpha_r = \alpha_r - \alpha_1,$$

a contradiction. Hence this case is impossible.

Case 2. $A_{21} = -2 = A_{r, r-1}$. In this case $2A_{1j} + 2A_{2j} + \dots + 2A_{r-1, j} + A_{rj} = 0, 1 \leq j \leq r$. Hence $|A^{(r)}| = 0$, and $2\alpha_1 + \dots + 2\alpha_{r-1} + \alpha_r = 0$ by Theorem 3. Once again we apply the definition of the A_{ij} to show that $\alpha_1, \alpha_1 + \alpha_2, \dots, \alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_{r-1}$ are roots. Now $2(\alpha_1 + \alpha_2 + \dots + \alpha_{r-1}) = -\alpha_r$ is a root and is not zero by assumption. This contradicts (xv), and this case is therefore also impossible. Thus we have:

Case 3. $A_{12} = A_{r,r-1} = -2$. Here $A_{1j} + 2A_{2j} + 2A_{3j} + \cdots + 2A_{r-1,j} + A_{rj} = 0$, $1 \leq j \leq r$, so that $|A^{(r)}| = 0$. Thus CC_r is exact, and (12) follows from Theorem 3.

Next suppose that S contains only one double line and a branch point, i.e., a point directly connected to at least three other points. Then S contains a subsystem, say $\alpha_1, \alpha_2, \dots, \alpha_r$ ($r \geq 4$), with diagram BD_r . We may suppose that the roots of this subsystem are labeled as in Figure 4. All principal minors of $A^{(r)}$ are positive by Lemma 11. Here there are two cases to be considered:

Case i. $A_{12} = -2$. In this case

$$A_{1j} + 2A_{2j} + 2A_{3j} + \cdots + 2A_{r-2,j} + A_{r-1,j} + A_{rj} = 0,$$

$1 \leq j \leq r$. Hence $|A^{(r)}| = 0$, and by Theorem 3, $\alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_{r-2} + \alpha_{r-1} + \alpha_r = 0$. However the roots include

$$\alpha_1, \alpha_1 + 2\alpha_2, \alpha_1 + 2\alpha_2 + 2\alpha_3, \dots,$$

$$\alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_{r-1} = \alpha_{r-1} - \alpha_r,$$

contrary to assumption. Thus this case is impossible.

Case ii. $A_{21} = -2$. Here

$$2A_{1j} + 2A_{2j} + \cdots + 2A_{r-2,j} + A_{r-1,j} + A_{rj} = 0, \quad 1 \leq j \leq r.$$

Again $|A^{(r)}| = 0$, and (13) follows by Theorem 3.

Finally we have the case where S contains only one double line and has no branch points. Either $S = B_n$ or $S = C_n$ or S contains F_4 as a subsystem. (See Figure 1.) Since B_2 and C_2 are indistinguishable, it follows that either $S = B_n$ ($n \geq 3$); $S = C_n$ ($n \geq 2$); $S = F_4$; or S contains a subsystem with diagram F_5 , where we suppose the roots labeled as in Figure 4. For such a subsystem there are two cases:

Case I. $A_{43} = -2$. Here $A_{1j} + 2A_{2j} + 3A_{3j} + 2A_{4j} + A_{5j} = 0$, $1 \leq j \leq 5$, and $|A^{(5)}| = 0$. Every proper subsystem of $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ has a positive determinant by Lemma 11, so Theorem 3 yields $\alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5 = 0$. However, the following are roots:

$$\alpha_5, \alpha_4 + \alpha_5, 2\alpha_3 + \alpha_4 + \alpha_5, 2\alpha_2 + 2\alpha_3 + \alpha_4 + \alpha_5,$$

$$2\alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5, 2\alpha_2 + 4\alpha_3 + 2\alpha_4 + \alpha_5 = \alpha_3 - \alpha_1,$$

a contradiction. Thus this case is impossible.

Case II. $A_{34} = -2$. Every proper subsystem of $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ has positive determinant by Lemma 11 and $A_{1j} + 2A_{2j} + 3A_{3j} + 4A_{4j} + 2A_{5j} = 0$, $1 \leq j \leq 5$. Hence $|A^{(5)}| = 0$, and (14) follows from Theorem 3.

Lemma 16. Let $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be an indecomposable system of roots containing no multiple lines and no cycles. Then either $S = A_n$ ($n \geq 1$); or $S = D_n$

FIGURE 5.

($n \geq 4$); or $S = E_n$ ($n = 6, 7, 8$); or S contains a subsystem $\alpha_1, \alpha_2, \dots, \alpha_r$ with one of the diagrams DD_r ($r \geq 5$), J_7 , J_8 or E_9 . (See Figure 5.) The systems DD_r ($r \geq 5$), J_7 , J_8 , and E_9 are exact. We have

$$(15) \quad \alpha_1 + \alpha_2 + 2 \sum_{i=3}^{r-2} \alpha_i + \alpha_{r-1} + \alpha_r = 0,$$

$$(16) \quad \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5 + 2\alpha_6 + \alpha_7 = 0,$$

$$(17) \quad \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7 + 2\alpha_8 = 0,$$

$$(18) \quad \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 4\alpha_7 + 2\alpha_8 + 3\alpha_9 = 0,$$

in cases DD_r , J_7 , J_8 , E_9 , respectively.

Proof. If S contains a point incident with four or more lines, then S contains DD_5 as a subdiagram. If S contains two or more distinct branch points, then S contains DD_r as a subdiagram with $r \geq 6$. If S contains only one branch point, and that point is not incident with four lines, then either S contains J_7 , J_8 , or E_9 as a subdiagram; or $S = D_n$ ($n \geq 4$); or $S = E_6$, E_7 , or E_8 . If S contains no branch point then $S = A_n$. By Lemma 11, every proper subsystem of DD_r ($r \geq 5$), J_7 , J_8 , E_9 has positive determinant. For DD_r we have

$$A_{1j} + A_{2j} + 2A_{3j} + 2A_{4j} + \dots + 2A_{r-2,j} + A_{r-1,j} + A_{r,j} = 0,$$

$1 \leq j \leq r$. Hence $|A^{(r)}| = 0$, so that DD_r is exact; (15) follows from Theorem 3. To see that J_7 , J_8 , and E_9 are exact and to verify (16), (17), (18), one need only observe that the same combinations of the rows of the matrices corresponding to these systems are zero. Exactness and (16)–(18) then follow, the latter equations by Theorem 3.

Theorem 6. *The only indecomposable systems of roots are the non-exact systems A_r ($r \geq 1$); B_r ($r \geq 3$); C_r ($r \geq 2$); D_r ($r \geq 4$); E_6 ; E_7 ; E_8 ; F_4 ; G_2 ; and the exact systems H_r ($r \geq 3$); I_2 ; G_3 ; CC_r ($r \geq 3$); BD_r ($r \geq 4$); DD_r ($r \geq 5$); F_5 ; J_7 ; J_8 ; and E_9 . The roots in these exact systems satisfy (9), (10), (11), (12), (13), (15), (14), (16), (17), and (18), respectively.*

Proof. Let $S = \{\alpha_1, \dots, \alpha_n\}$ be an indecomposable system of roots that is not one of those listed above. By Theorem 5, S does not contain a cycle. By Lemmas 13–16, S contains an exact system $S' = \{\alpha_1, \dots, \alpha_r\}$ that is one of the exact systems listed, and $r < n$. In the corresponding relation among the elements of S' from (9)–(18), we note that every root has a non-zero coefficient from the prime field of $\mathfrak{F}$. Thus there exist $\lambda_i \in \mathfrak{F}$, all $\lambda_i \neq 0$, such that $\sum_{i=1}^r \lambda_i \alpha_i = 0$. Now we apply the reasoning of the proof of Theorem 5. We have another root α_{r+1} in S such that $A_{i,r+1} \neq 0$ for some $i \leq r$. Now

$$\sum_{i=1}^r \lambda_i \alpha_i (h_{\alpha_{r+1}}) = 0, \quad \sum_{i=1}^r \lambda_i \bar{A}_{i,r+1} = 0,$$

and therefore $A_{i,r+1} \neq 0$ for at least two $j \leq r$. But this implies that S contains a cycle, a contradiction. Thus Theorem 6 is established.

Corollary 1. *Every indecomposable non-exact system has positive determinant.*

Proof. Use Theorem 6 and Lemma 11.

Corollary 2. *If $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is an indecomposable system that is neither simple nor exact, then S is of type A_n and $p \mid n + 1$.*

Proof. The system S must be one of the indecomposable non-exact systems listed in Theorem 6. Furthermore $|\bar{A}_{\alpha_i, \alpha_j}| = 0$ by Lemma 4. Since $p \neq 2, 3$, it follows from Lemma 11 that S is of type A_n and $p \mid n + 1$.

10. Fundamental systems of roots. Let $S = \{\alpha_1, \dots, \alpha_r\}$ be a system of roots. A root β is called a *minimal* root with respect to S if β is a linear combination of S and if $\beta - \alpha_i$ is not a root, $1 \leq i \leq r$. An indecomposable non-exact system of roots S is called a *fundamental* system if S spans $\mathfrak{S}^*$ and if there is a unique minimal root with respect to S . From Corollary 1 of Theorem 6 it follows that any fundamental system has positive determinant.

Theorem 7. *If there is a simple system of roots that spans $\mathfrak{S}^*$, then there is a fundamental system of roots with respect to $\mathfrak{S}$.*

Proof. Let T be a simple system spanning $\mathfrak{S}^*$. By Lemma 6, T is not exact. By Lemma 8 any system containing T is indecomposable. Embed T in a maximal non-exact system $S = \{\alpha_1, \dots, \alpha_r\}$. Clearly S spans $\mathfrak{S}^*$. By Corollary 2 of Theorem 6, if $S \neq T$, then S is of type A_r , $p \mid r + 1$, and T is of type A_{r-1} . In any case S is one of the types A, B, C, D, E, F, G by Theorem 6. We suppose the roots of S labeled as in Figure 1. By Theorem 1 and Corollary 1 of Theorem

6 there is at least one minimal root with respect to S . Let α_{r+1} be such a minimal root. Then $S' = \{\alpha_1, \dots, \alpha_r, \alpha_{r+1}\}$ is a system, hence is exact. Thus S' is an (indecomposable) exact system of $r + 1$ roots containing S . We investigate the possibilities:

Case 1. S is of type C_r , $r \geq 2$. By Theorem 6, CC_{r+1} is the only exact system of $r + 1$ roots containing C_r . Hence S' is of type CC_{r+1} . Applying (12) with r replaced by $r' = r + 1$ and noting that the roots are permuted we obtain $\alpha_{r+1} = -2 \sum_{i=1}^{r-1} \alpha_i - \alpha_r$, so that the minimal root α_{r+1} is unique. Hence S is a fundamental system.

Case 2. S is of type G_2 . G_3 is the only exact system containing G_2 , so that S' is of type G_3 . By (11), with the roots permuted, $\alpha_3 = -2\alpha_1 - 3\alpha_2$. Thus α_3 is uniquely determined by S , and S is a fundamental system.

Case 3. S is of type F_4 . F_5 is the only exact system containing F_4 , so that S' is of type F_5 . By (14), with the roots permuted, $\alpha_5 = -2\alpha_1 - 3\alpha_2 - 4\alpha_3 - 2\alpha_4$ is uniquely determined by S , and S is a fundamental system.

Case 4. S is of type E_6 . Since J_7 is the only exact system of seven roots containing E_6 , we have S' of type J_7 . Hence α_7 is uniquely determined by (16), and S is fundamental.

Case 5. S is of type E_7 . Since J_8 is the only exact system of eight roots containing E_7 , S' is of type J_8 , (17) gives $\alpha_8 = -\alpha_1 - 2\alpha_2 - 3\alpha_3 - 4\alpha_4 - 3\alpha_5 - 2\alpha_6 - 2\alpha_7$, and once again S is fundamental.

Case 6. S is of type E_8 . Here S' must be of type E_9 . By (18)

$$\alpha_9 = -2\alpha_1 - 3\alpha_2 - 4\alpha_3 - 5\alpha_4 - 6\alpha_5 - 4\alpha_6 - 2\alpha_7 - 3\alpha_8,$$

and S is again a fundamental system.

From cases 1—6 we note that if $\mathfrak{S}^*$ is spanned by a simple system S^* of type C , E , F , or G then we may take $S = T = S^*$ and have a fundamental system. In what follows, therefore, we may assume that $\mathfrak{S}^*$ is not spanned by a simple system of type C , E , F , or G .

Now suppose that S' is of one of the six types CC_{r+1} , G_3 , F_5 , J_7 , J_8 , E_9 . Then S' contains a subsystem S^* of r roots of type C_r , G_2 , F_4 , E_6 , E_7 , or E_8 , respectively. By Lemmas 4 and 11, S^* is linearly independent and hence simple. Since the dimension of $\mathfrak{S}$ is at most r , S^* spans $\mathfrak{S}^*$, contrary to assumption. Thus we see that S' cannot be one of these six types.

Case 7. S is type B_r , $r \geq 3$. The only possible systems for S' are BD_{r+1} and F_5 . We have eliminated the latter. Hence S' is of type BD_{r+1} , (13) gives $\alpha_{r+1} = -\alpha_1 - 2 \sum_{i=2}^r \alpha_i$, and S is again fundamental. As above, this result enables us to assert the existence of a fundamental system whenever S' is of type BD_{r+1} , and thus to assume in the sequel that S' is not of this type.

Case 8. S is of type A_1 . Here S' must be of type I_2 , since I_2 is the only exact system of two roots. In this case (10) gives $\alpha_2 = -\alpha_1$, so α_2 is unique and S is fundamental.

Case 9. S is of type A_r , $r \geq 2$. The only exact systems of $r + 1$ roots containing A_r as a subsystem are H_{r+1} , G_3 , J_8 , E_9 , BD_4 . Hence S' is of type H_{r+1} and (9) gives $\alpha_{r+1} = -\sum_{i=1}^r \alpha_i$, so that α_{r+1} is unique and S is fundamental.

Case 10. S is of type D_r , $r \geq 4$. The only exact systems of $r + 1$ roots containing subsystems of type D_r are BD_{r+1} , DD_{r+1} , E_9 . Hence S' is of type DD_{r+1} . From (15) $\alpha_{r+1} = -\alpha_1 - 2\sum_{i=2}^{r-2} \alpha_i - \alpha_{r-1} - \alpha_r$. Thus α_{r+1} is unique and S is fundamental. This completes the proof of Theorem 7.

11. Levels of roots. Henceforth let $S = \{\alpha_1, \dots, \alpha_n\}$ be a fixed fundamental system of roots. Let δ be the unique minimal root with respect to S . In every case δ is a linear combination of $\alpha_1, \dots, \alpha_n$ with coefficients which are negative integers t_i , $-6 \leq t_i \leq -1$. Now if β is any root, then by Theorem 1 there is a finite sequence of roots

$$\beta_0 = \beta, \beta_1 = \beta_0 - \alpha_{k_1}, \beta_2 = \beta_1 - \alpha_{k_2}, \dots, \beta_u = \beta_{u-1} - \alpha_{k_u}$$

where $\beta_u - \alpha_i$ is not a root, $1 \leq j \leq r$. Hence $\beta_u = \delta$. As before $\beta_i = \beta - \sum_{j=1}^n s_j^{(i)} \alpha_j$, where $s_j^{(i)}$ is the number of times j occurs among $k_1, k_2, \dots, k_i$, and

$$A_{\delta, \alpha_i} = A_{\beta_u, \alpha_i} = A_{\beta, \alpha_i} - \sum_{j=1}^n s_j^{(u)} A_{\alpha_j}.$$

Since $|A_{\alpha_i}| \neq 0$, the integers $s_j^{(u)}$ are uniquely determined by the root β and the system S . Hence the non-negative integer $N(\beta) = u = \sum_{j=1}^n s_j^{(u)}$ is also uniquely determined by β . We shall call the integer

$$L(\beta) = N(\beta) - N(0)$$

the *level* of the root β . We see at once that $N(\delta) = 0$ and that if $\beta \neq \delta$ then $N(\beta) > 0$ and $L(\beta) > L(\delta)$. If β and $\beta - \alpha_i$ are both roots ($\alpha_i \in S$), then $N(\beta) = N(\beta - \alpha_i) + 1$, and hence $L(\beta) = L(\beta - \alpha_i) + 1$. Moreover $L(0) = 0$ and $L(\alpha_i) = -L(-\alpha_i) = 1$, $1 \leq i \leq n$. Furthermore $-\delta$ is the unique root such that no $-\delta + \alpha_i$ is a root; $N(-\delta) = 2N(0)$ so that $L(-\delta) = -L(\delta)$; $L(\delta) = -N(0) < 0$ and $L(-\delta) > 0$.

For every non-zero root β , let $0 \neq e_\beta \in \mathfrak{L}_\beta$. Let $\langle \alpha, \beta, \gamma, \dots, \omega \rangle$ denote the element $[\dots [[e_\alpha e_\beta] e_\gamma] \dots e_\omega]$ of $\mathfrak{L}_{\alpha+\beta+\gamma+\dots+\omega}$. If $\langle \alpha, \beta, \dots, \omega \rangle \neq 0$, then $\alpha, \alpha + \beta, \dots, \alpha + \beta + \dots + \omega$ are all roots. If $\alpha, \alpha + \beta, \dots, \alpha + \beta + \dots + \omega$ are all non-zero roots, then $\langle \alpha, \beta, \dots, \omega \rangle \neq 0$.

Lemma 17. *If β is a non-zero root, then $\langle \beta, -\alpha_{i_1}, \dots, -\alpha_{i_k}, \alpha_i \rangle$, $1 \leq i_k, j \leq n$, is a linear combination of*

$$(19) \quad \langle \beta, \alpha_i, -\alpha_{i_1}, \dots, -\alpha_{i_k} \rangle$$

and terms of the form

$$(20) \quad \langle \beta, -\alpha_{i_1}, \dots, -\hat{\alpha}_{i_a}, \dots, -\alpha_{i_k} \rangle, \quad i_a = j,$$

where the circumflex indicates an omitted factor. All terms belong to $\mathfrak{L}_\gamma$, where $\gamma = \beta + \alpha_j - \alpha_{i_1} - \alpha_{i_2} - \dots - \alpha_{i_k}$.

Proof. For $k = 0$, $\langle \beta, \alpha_j \rangle$ is evidently of the form (19). Assuming the result for $k - 1$, we have by the Jacobi identity

$$\begin{aligned} \langle \beta, -\alpha_{i_1}, \dots, -\alpha_{i_k}, \alpha_j \rangle &= [\langle \beta, -\alpha_{i_1}, \dots, -\alpha_{i_{k-1}} \rangle, \langle -\alpha_{i_k}, \alpha_j \rangle] \\ &\quad + \langle \beta, -\alpha_{i_1}, \dots, -\alpha_{i_{k-1}}, \alpha_j, -\alpha_{i_k} \rangle. \end{aligned}$$

By the inductive hypothesis (applied to $\langle \beta, -\alpha_{i_1}, \dots, -\alpha_{i_{k-1}}, \alpha_j \rangle$) the second term is of the required form. If $j \neq i_k$ then the first term is zero. If $j = i_k$, then $\langle -\alpha_{i_k}, \alpha_j \rangle \in \mathfrak{S}$ and the first term is a scalar multiple of $\langle \beta, -\alpha_{i_1}, \dots, -\alpha_{i_{k-1}} \rangle$. Together with the observation that all terms of the forms (19) and (20) belong to the root-space of $\beta + \alpha_j - \alpha_{i_1} - \dots - \alpha_{i_k}$, this completes the proof.

Lemma 18. *If β is a root and $L(\beta) = 0$, then $\beta = 0$.*

Proof. There is a relation of the form

$$(21) \quad \beta - \alpha_{i_1} - \dots - \alpha_{i_k} = 0 - \alpha_{i_1} - \dots - \alpha_{i_k}$$

where all partial sums are roots—for example take $k = N(0)$. Now suppose the relation (21) chosen with minimal k . We proceed by induction on k . If $k = 0$, we are done. Assume $k > 0$ and that the result holds for all integers less than k . Now if 0 occurs as a partial sum on the left side of the above equation, we must have $\beta = 0$, since otherwise we get two values for $N(0)$. Therefore we may assume 0 does not occur as a partial sum there. Then

$$\langle \beta, -\alpha_{i_1}, \dots, -\alpha_{i_k}, \alpha_{i_k} \rangle \neq 0.$$

By Lemma 17, one of the terms (19) or (20), with j replaced by j_k , is non-zero. Now if one of the terms (20) is non-zero we have

$$\beta - \alpha_{i_1} - \dots - \hat{\alpha}_{i_k} - \dots - \alpha_{i_k} = 0 - \alpha_{i_1} - \dots - \alpha_{i_{k-1}},$$

all partial sums being roots, which is impossible by the minimality of k . Therefore the term (19) is different from zero, and it follows from the result for $k - 1$ that $\beta + \alpha_{i_k} - \alpha_{i_1} = 0$, or $\beta = \alpha_{i_1} - \alpha_{i_k}$. But this is not a root unless $i_1 = j_k$. Therefore $\beta = 0$, and the proof is complete.

Lemma 19. *If $L(\beta) > 0$, then there is an $\alpha_i \in S$ such that $\beta - \alpha_i$ is a root. If $L(\beta) < 0$, there is an $\alpha_i \in S$ such that $\beta + \alpha_i$ is a root.*

Proof. If $L(\beta) > 0$, then $\beta \neq \delta$, and therefore some $\beta - \alpha_i$ is a root. If $L(\beta) < 0$, then $\beta \neq -\delta$, and therefore some $\beta + \alpha_i$ is a root.

Lemma 20. *If $L(\alpha) = 1$, then $\alpha \in S$. If $L(\alpha) = -1$, then $-\alpha \in S$.*

Proof. Suppose $L(\alpha) = 1$. By Lemma 19 there is an $\alpha_i \in S$ such that $\alpha - \alpha_i$ is a root. Then $L(\alpha - \alpha_i) = 0$, and $\alpha = \alpha_i \in S$ by Lemma 18. Similarly if $L(\alpha) = -1$, then there is an $\alpha_i \in S$ such that $\alpha + \alpha_i$ is a root, $L(\alpha + \alpha_i) = 0$, and $-\alpha = \alpha_i \in S$.

Lemma 21. *If α, β , and $\alpha + \beta$ are roots, then*

$$L(\alpha + \beta) = L(\alpha) + L(\beta).$$

Proof. If $L(\alpha) = 0$ or if $L(\beta) = 0$ the result follows immediately from Lemma 18. We suppose that $L(\alpha) \neq 0$, $L(\beta) \neq 0$ and proceed by induction on $|L(\alpha)|$, the absolute value of $L(\alpha)$. If $L(\alpha) = 1$, then, by Lemma 20, $\alpha = \alpha_i$ for some i , and $L(\alpha + \beta) = 1 + L(\beta) = L(\alpha) + L(\beta)$. Similarly if $L(\alpha) = -1$, then $\alpha = -\alpha_i$ for some i , and $L(\beta) = L(\beta - \alpha_i) + 1 = L(\alpha + \beta) - L(\alpha)$. Now suppose $|L(\alpha)| \geq 2$ and that $L(\gamma + \beta) = L(\gamma) + L(\beta)$ for all roots γ such that $|L(\gamma)| < |L(\alpha)|$. By Lemma 19 there is an $\alpha' = \pm\alpha_i$ such that $\gamma = \alpha - \alpha'$ is a root and $|L(\gamma)| = |L(\alpha)| - 1$. Now

$$\langle \alpha', \gamma, \beta \rangle = \langle \alpha', \beta, \gamma \rangle + \langle \beta, \gamma, \alpha' \rangle$$

is a non-zero element of $\mathfrak{L}_{\alpha+\beta}$, whether or not $\alpha + \beta = 0$. Hence either $\langle \alpha', \beta, \gamma \rangle \neq 0$ or $\langle \beta, \gamma, \alpha' \rangle \neq 0$. In the former case $\alpha' + \beta$ is a root and

$$L(\alpha + \beta) = L(\gamma) + L(\alpha' + \beta) = L(\gamma) + L(\alpha') + L(\beta) = L(\alpha) + L(\beta)$$

by three applications of the induction hypothesis. In the latter case $\beta + \gamma$ is a root and

$$L(\alpha + \beta) = L(\alpha') + L(\beta + \gamma) = L(\alpha') + L(\gamma) + L(\beta) = L(\alpha) + L(\beta),$$

which completes the proof.

An immediate consequence of Lemma 21 is

$$(22) \quad L(-\alpha) = -L(\alpha)$$

for all roots α .

12. Simplicity.

Theorem 8. *$\mathfrak{L}$ is simple if and only if there is a simple system of roots that spans $\mathfrak{L}^*$.*

Proof. Suppose that $\mathfrak{L}^*$ is spanned by a simple system of roots. By Theorem 7 there is a fundamental system of roots $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ with respect to $\mathfrak{L}$. Thus the results of §11 apply. Let $\mathfrak{A}$ be a non-zero ideal of $\mathfrak{L}$. Let $0 \neq b \in \mathfrak{A}$. We write $b = \sum b_\alpha$, where $b_\alpha \in \mathfrak{L}_\alpha$ and the sum runs over all roots α . Let β be a root of maximum level such that $b_\beta \neq 0$. Then, if δ is the minimal root, there is a non-zero element of $\mathfrak{L}_\delta$ of the form

$$d = [\dots [[b_\beta e_{-\alpha_{i(1)}}] e_{-\alpha_{i(2)}}] \dots e_{-\alpha_{i(k)}}],$$

where $1 \leq i(j) \leq n$, $k = L(\beta) - L(\delta)$. Then $\mathfrak{U}$ contains

$$[\cdots [[be_{-\alpha_{i(1)}}]e_{-\alpha_{i(2)}}] \cdots e_{-\alpha_{i(k)}}] = d.$$

Hence $e_\delta \in \mathfrak{U}$. Now if α is an arbitrary non-zero root, then e_α is a scalar multiple of an expression of the form $\langle \delta, \alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_m} \rangle$. Hence $e_\alpha \in \mathfrak{U}$ for all non-zero roots α . It follows from (viii) that $\mathfrak{S} \subset \mathfrak{U}$. Hence $\mathfrak{U} = \mathfrak{L}$. Therefore $\mathfrak{L}$ is simple. The converse is an immediate consequence of Theorem 4.

Corollary. *If $\mathfrak{L}$ is simple then $\mathfrak{L}$ remains simple under any extension of the base field $\mathfrak{F}$.*

13. The isomorphism theorem.

Lemma 22. *Let $\zeta \in \mathfrak{S}^*$, let $\alpha, \beta, \alpha + \beta$ be non-zero roots, and let $\zeta(h_\alpha) = \zeta(h_\beta) = 0$. Then $\zeta(h) = 0$ for all $h \in [\mathfrak{L}_{\alpha+\beta}\mathfrak{L}_{-\alpha-\beta}]$.*

Proof. Let $0 \neq e_{\alpha} \in \mathfrak{L}_{\alpha}$, $0 \neq e_{\beta} \in \mathfrak{L}_{\beta}$, such that $h_\alpha = [e_\alpha e_{-\alpha}]$ and $h_\beta = [e_\beta e_{-\beta}]$. We may suppose $h_{\alpha+\beta} = [[e_\alpha e_\beta][e_{-\beta} e_{-\alpha}]] \neq 0$. Since $[\mathfrak{L}_{\alpha+\beta}\mathfrak{L}_{-\alpha-\beta}]$ is one-dimensional and $h_{\alpha+\beta} \in [\mathfrak{L}_{\alpha+\beta}\mathfrak{L}_{-\alpha-\beta}]$, it is sufficient to show that $\zeta(h_{\alpha+\beta}) = 0$. By the Jacobi identity

$$h_{\alpha+\beta} = [[[e_\alpha e_\beta]e_{-\beta}]e_{-\alpha}] + [[[e_\beta e_\alpha]e_{-\alpha}]e_{-\beta}].$$

Now $[[e_\alpha e_\beta]e_{-\beta}] = \lambda e_\alpha$, $\lambda \in \mathfrak{F}$, since it is in the one-dimensional space $\mathfrak{L}_\alpha$. Thus $[[[e_\alpha e_\beta]e_{-\beta}]e_{-\alpha}] = \lambda h_\alpha$. Similarly $[[[e_\beta e_\alpha]e_{-\alpha}]e_{-\beta}] = \mu h_\beta$ for some $\mu \in \mathfrak{F}$. Then $h_{\alpha+\beta} = \lambda h_\alpha + \mu h_\beta$, and evidently $\zeta(h_{\alpha+\beta}) = 0$.

Now let $S = \{\alpha_1, \cdots, \alpha_n\}$ be a fundamental system of roots. Let $0 \neq e_{\alpha_i} \in \mathfrak{L}_{\alpha_i}$, $h_i = [e_{\alpha_i} e_{-\alpha_i}]$. Then $0 \neq h_i \in \mathfrak{S}$.

Lemma 23. *If $\zeta \in \mathfrak{S}^*$ and if $\zeta(h_i) = 0$, $1 \leq i \leq n$, then $\zeta = 0$.*

Proof. Let α be a root of positive level. We prove that $\zeta(h_\alpha) = 0$, where $0 \neq h_\alpha \in [\mathfrak{L}_\alpha \mathfrak{L}_{-\alpha}]$. Since for any non-zero root β either $L(\beta) > 0$ or $L(-\beta) > 0$ by (22) and Lemma 18, it follows from (viii) that $\mathfrak{S}$ is spanned by the one-dimensional subspaces $[\mathfrak{L}_\alpha \mathfrak{L}_{-\alpha}]$, $L(\alpha) > 0$, and we shall be able to conclude that $\zeta = 0$. We proceed by induction on $L(\alpha)$. If $L(\alpha) = 1$, $\alpha = \alpha_i$ for some i , and the result is true by assumption. If $L(\alpha) > 1$, we have $\alpha = \alpha' + \alpha_i$, $L(\alpha') > 0$ by Lemma 19, and $\zeta(h_{\alpha'}) = \zeta(h_{\alpha_i}) = 0$ by the inductive hypothesis. We now apply Lemma 22 to conclude that $\zeta(h_\alpha) = 0$ and finish the proof.

Lemma 24. *S is a basis for $\mathfrak{S}^*$ except in case S is of type A_n where $p \mid n + 1$. In the latter case,*

$$\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + n\alpha_n = 0,$$

where the roots are labeled as in Figure 1, and $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ is a basis for $\mathfrak{S}^*$.

Proof. By definition S spans $\mathfrak{S}^*$. By Corollary 2 of Theorem 6 either S is independent or S is of type A_n and $p \mid n + 1$. Let us consider this case. Label

the roots as in Figure 1 and set $\zeta = \alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + n\alpha_n$. Now

$$\sum_{i=1}^n iA_{ii} = \begin{cases} 0 & \text{if } 1 \leq j \leq n-1 \\ n+1 & \text{if } j = n. \end{cases}$$

Hence

$$\zeta(h_j) = \sum_{i=1}^n i\alpha_i(h_j) = \frac{1}{2}\alpha_j(h_j) \sum_{i=1}^n i\bar{A}_{ij} = 0, \quad 1 \leq j \leq n.$$

Therefore $\zeta = 0$ by Lemma 23. Now $\alpha_1, \dots, \alpha_{n-1}$ is of type A_{n-1} with determinant n . Since $p \mid (n+1)$, $p \nmid n$, and this is a linearly independent system by Lemma 4. Since S spans $\mathfrak{S}^*$ and is linearly dependent it follows that $\alpha_1, \dots, \alpha_{n-1}$ is a basis for $\mathfrak{S}^*$ in this case.

Theorem 9. *Let $\mathfrak{L}$ and $\mathfrak{L}'$ be finite-dimensional Lie algebras over $\mathfrak{F}$ with Cartan subalgebras $\mathfrak{S}$ and $\mathfrak{S}'$, respectively, both satisfying (i)–(v). Let $\mathfrak{S}^*$ be spanned by the fundamental (indecomposable) system $S = \{\alpha_1, \dots, \alpha_n\}$ and let $\mathfrak{S}'^*$ be spanned by the fundamental system $S' = \{\alpha'_1, \dots, \alpha'_n\}$. Suppose $A_{ij} = A_{\alpha_i, \alpha_j} = A_{\alpha'_i, \alpha'_j}$, $1 \leq i, j \leq n$, so that S and S' have the same type. Then $\mathfrak{L}$ and $\mathfrak{L}'$ are isomorphic.*

We begin the proof by proving the following lemma, subject to the hypotheses of Theorem 9:

Lemma 25. *There is a vector space isomorphism τ of $\mathfrak{S}^*$ onto $\mathfrak{S}'^*$ such that $\tau(\alpha_i) = \alpha'_i$, $1 \leq i \leq n$. If $\zeta \in \mathfrak{S}^*$, then ζ is a root if and only if $\tau(\zeta)$ is a root. If ζ is a root then $L(\zeta) = L(\tau(\zeta))$.*

Proof. It follows from Lemma 24 that there is a unique vector space isomorphism τ of $\mathfrak{S}^*$ onto $\mathfrak{S}'^*$ such that $\tau(\alpha_i) = \alpha'_i$, $1 \leq i \leq n$. Now let ζ be a root of $\mathfrak{L}$. We show that $\tau(\zeta)$ is a root of $\mathfrak{L}'$, that $L(\zeta) = L(\tau(\zeta))$, and that $A_{\zeta, \alpha_j} = A_{\tau(\zeta), \alpha'_j}$, $1 \leq j \leq n$. By (vii), (22), and the identity $A_{-\alpha, \beta} = -A_{\alpha, \beta}$ it is sufficient to treat the case $L(\zeta) \geq 0$. We proceed by induction on $L(\zeta)$. If $L(\zeta) = 0$, then $\zeta = 0$, $\tau(\zeta) = 0$ is a root, $L(\tau(\zeta)) = 0 = L(\zeta)$, and $A_{\tau(\zeta), \alpha'_j} = 0 = A_{\zeta, \alpha_j}$. If $L(\zeta) = 1$, then, by Lemma 20, $\zeta = \alpha_i$ for some i , $\tau(\zeta) = \alpha'_i$ which is a root, and $L(\tau(\zeta)) = 1 = L(\zeta)$. Furthermore $A_{\tau(\zeta), \alpha'_j} = A_{\zeta, \alpha_j}$ by hypothesis. Now let $L(\zeta) > 1$ and suppose that the assertion is true for all roots β of $\mathfrak{L}$ such that $0 \leq L(\beta) < L(\zeta)$. For some i , $\zeta - \alpha_i$ is a root. Let $k+1$ be the least positive integer such that $\zeta - (k+1)\alpha_i$ is not a root. Put $\beta = \zeta - k\alpha_i$. Then $L(\beta) > 0$, for otherwise either $\zeta - 2\alpha_i = 0$ or $\zeta - 3\alpha_i = 0$, and both are impossible by (xvi). Thus $0 < L(\beta) < L(\zeta)$. By the induction hypothesis, $\tau(\beta)$ is a root, $L(\tau(\beta)) = L(\beta)$, and $A_{\tau(\beta), \alpha'_i} = A_{\beta, \alpha_i} \leq -k$. Therefore $\tau(\zeta) = \tau(\beta) + k\alpha'_i$ is a root. Furthermore $L(\tau(\zeta)) = L(\tau(\beta)) + k = L(\beta) + k = L(\zeta)$. By Lemma 3 we have $A_{\tau(\zeta), \alpha'_j} = A_{\zeta, \alpha_j}$, $1 \leq j \leq n$.

By symmetry, if $\tau(\zeta)$ is a root, then ζ is a root, and the proof is complete.

Proof of the isomorphism theorem. Denote by $\mathfrak{L}_k$ the subspace of $\mathfrak{L}$ spanned by all $\mathfrak{L}_\alpha$ such that $0 \leq |L(\alpha)| \leq k$ and by $\mathfrak{L}'_k$, the corresponding subspace of

$\mathfrak{X}'$. By Lemma 25, $\mathfrak{S}$ and $\mathfrak{S}'$ have the same dimension. Furthermore $\mathfrak{X}_\alpha \subset \mathfrak{X}_k$ if and only if $\mathfrak{X}'_{\tau(\alpha)} \subset \mathfrak{X}'_k$. Hence $\mathfrak{X}_k$ and $\mathfrak{X}'_k$ have the same dimension. By induction on k , we now construct a one-to-one linear transformation η of $\mathfrak{X}_k$ onto $\mathfrak{X}'_k$ such that if $e_\alpha \in \mathfrak{X}_\alpha \subset \mathfrak{X}_k$, $e_\beta \in \mathfrak{X}_\beta \subset \mathfrak{X}_k$, $h \in \mathfrak{S}$, then $[e_\alpha h]\eta = [e_\alpha \eta, h\eta]$ and $[e_\alpha e_\beta]\eta = [e_\alpha \eta, e_\beta \eta]$ provided $\mathfrak{X}_{\alpha+\beta} \subset \mathfrak{X}_k$. Once this is done, we can let $k = -L(\delta)$, and η becomes the desired isomorphism.

First let $k = 1$. We may assume $\alpha_1, \dots, \alpha_n$ so ordered that the subsystem $S_i = \{\alpha_1, \dots, \alpha_i\}$ is indecomposable, $1 \leq i \leq n$. (The ordering of Figure 1 has this property.) Then since S does not contain a cycle, whenever $2 \leq j \leq n$ there is a unique $i < j$ such that $A_{ij} \neq 0$. Now let h_i, h'_i be non-zero elements of $[\mathfrak{X}_{\alpha_i}, \mathfrak{X}_{-\alpha_i}]$ and $[\mathfrak{X}'_{\alpha'_i}, \mathfrak{X}'_{-\alpha'_i}]$, respectively, such that $\alpha_i(h_i) = \alpha'_i(h'_i)$. We now define non-zero h_i, h'_i in $[\mathfrak{X}_{\alpha_i}, \mathfrak{X}_{-\alpha_i}]$, $[\mathfrak{X}'_{\alpha'_i}, \mathfrak{X}'_{-\alpha'_i}]$, respectively, such that $\alpha_i(h_i) = \alpha'_i(h'_i) = \alpha_i(h_i) = \alpha'_i(h'_i)$, $1 \leq i, j \leq n$. We proceed by induction on j . Suppose h_m, h'_m have been defined for $m < j$ such that $\alpha_i(h_m) = \alpha'_i(h'_m)$ for $1 \leq i, m \leq j-1$. For the single value of $i < j$ such that $A_{ij} \neq 0$ we have $\alpha_i(h_i) \neq 0$. Let h_i be the unique (non-zero) element of $[\mathfrak{X}_{\alpha_i}, \mathfrak{X}_{-\alpha_i}]$ such that $\alpha_i(h_i) = \alpha_i(h_i)$. Similarly, select h'_i in $[\mathfrak{X}'_{\alpha'_i}, \mathfrak{X}'_{-\alpha'_i}]$ such that $\alpha'_i(h'_i) = \alpha'_i(h'_i)$. Then for $q < j$, $q \neq i$, we have $\alpha_i(h_q) = \alpha_q(h_i) = 0 = \alpha'_i(h'_q) = \alpha'_q(h'_i)$. It remains only to verify that $\alpha_i(h_j) = \alpha'_i(h'_j)$, $\alpha_i(h_j) = \alpha'_i(h'_j) = \alpha_j(h_i) = \alpha'_j(h'_i)$. But

$$\frac{2\alpha_i(h_i)}{\alpha_i(h_i)} = \bar{A}_{ji} = \frac{2\alpha'_i(h'_i)}{\alpha'_i(h'_i)}.$$

Since $\alpha_i(h_i) = \alpha'_i(h'_i)$ by induction, we have $\alpha_i(h_i) = \alpha'_i(h'_i) = \alpha_i(h_i) = \alpha'_i(h'_i)$, the last by the definition of h_i, h'_i . Also

$$\frac{2\alpha_i(h_j)}{\alpha_j(h_i)} = \bar{A}_{ij} = \frac{2\alpha'_i(h'_j)}{\alpha'_j(h'_i)}$$

so that $\alpha_i(h_j) = \alpha'_i(h'_j)$. Thus the h_i, h'_i are defined by induction with the desired properties, $1 \leq j \leq n$.

Now suppose $\lambda_1 h_1 + \dots + \lambda_n h_n = 0$, $\lambda_i \in \mathfrak{F}$. Then

$$\sum_{i=1}^n \lambda_i \alpha_i(h_i) = \sum_{i=1}^n \lambda_i \alpha_i(h_i) = \alpha_j(\sum_{i=1}^n \lambda_i h_i) = 0, \quad 1 \leq j \leq n.$$

Hence $\lambda_1 \alpha_1 + \dots + \lambda_n \alpha_n = 0$ by Lemma 23. Applying τ we have $\lambda_1 \alpha'_1 + \dots + \lambda_n \alpha'_n = 0$ and thus

$$\alpha'_j(\sum_{i=1}^n \lambda_i h'_i) = \sum_{i=1}^n \lambda_i \alpha'_j(h'_i) = \sum_{i=1}^n \lambda_i \alpha'_i(h'_i) = 0, \quad 1 \leq j \leq n.$$

Since the α'_i span $\mathfrak{S}'^*$ we have $\lambda_1 h'_1 + \dots + \lambda_n h'_n = 0$. By symmetry we see that $\lambda_1 h_1 + \dots + \lambda_n h_n = 0$ if and only if $\lambda_1 h'_1 + \dots + \lambda_n h'_n = 0$.

Let $e_{\alpha_i}, e_{-\alpha_i}, e_{\alpha'_i}, e_{-\alpha'_i}$ be non-zero elements of $\mathfrak{X}_{\alpha_i}, \mathfrak{X}_{-\alpha_i}, \mathfrak{X}'_{\alpha'_i}, \mathfrak{X}'_{-\alpha'_i}$, respectively, such that $[e_{\alpha_i}, e_{-\alpha_i}] = h_i, [e_{\alpha'_i}, e_{-\alpha'_i}] = h'_i, 1 \leq i \leq n$. Let η be the vector space isomorphism of $\mathfrak{X}_1$ onto $\mathfrak{X}'_1$ such that $e_{\pm \alpha_i} \eta = e_{\pm \alpha'_i}, h_i \eta = h'_i$. Then

$$[e_{\alpha_i} h_i] \eta = \alpha_i(h_i)(e_{\alpha_i} \eta) = \alpha'_i(h'_i) e_{\alpha'_i} = [e_{\alpha'_i} h'_i] = [e_{\alpha_i} \eta, h_i \eta],$$

and similarly for $[e_{-\alpha_i} h_i]$. If $i \neq j$ then $[e_{\alpha_i} e_{-\alpha_j}] \eta = 0 = [e_{\alpha_i} \eta, e_{-\alpha_j} \eta]$, and $[e_{\alpha_i} e_{-\alpha_i}] \eta = h_i \eta = h'_i = [e_{\alpha_i} \eta, e_{-\alpha_i} \eta]$. If $\alpha_i + \alpha_j$ is not a root, then $[e_{\pm \alpha_i} e_{\pm \alpha_j}] \eta = 0 = [e_{\pm \alpha_i} \eta, e_{\pm \alpha_j} \eta]$ by Lemma 25, while if $\alpha_i + \alpha_j$ is a root then $\mathfrak{L}_{\pm(\alpha_i + \alpha_j)}$ is not contained in $\mathfrak{L}_1$. This completes the case $k = 1$.

Next let $k > 1$ and suppose η is defined from $\mathfrak{L}_{k-1}$ to $\mathfrak{L}'_{k-1}$ with the desired properties. For every root β such that $L(\beta) = k$ select an $\alpha_i \in S$ such that $\alpha = \beta - \alpha_i$ is a root. Then $L(\alpha) = k - 1$. Let $0 \neq e_{\pm \alpha} \in \mathfrak{L}_{\pm \alpha}$. Put

$$\begin{aligned} e_{\beta} &= [e_{\alpha} e_{\alpha_i}], & e_{\tau(\beta)} &= e_{\beta} \eta = [e_{\alpha} \eta, e_{\alpha_i} \eta], \\ e_{-\beta} &= [e_{-\alpha} e_{-\alpha_i}], & e_{-\tau(\beta)} &= e_{-\beta} \eta = [e_{-\alpha} \eta, e_{-\alpha_i} \eta]. \end{aligned}$$

Now if γ is a root of $\mathfrak{L}$ such that $0 < L(\gamma) \leq k$ then either $\beta + \gamma$ is not a root, in which case $[e_{\beta} e_{\gamma}] \eta = 0 = [e_{\beta} \eta, e_{\gamma} \eta]$, or $\beta + \gamma$ is a root, in which case $\mathfrak{L}_{\beta + \gamma}$ is not in $\mathfrak{L}_k$. Now suppose $\beta = \lambda_1 \alpha_1 + \cdots + \lambda_n \alpha_n$. Then $\tau(\beta) = \sum \lambda_i (\tau(\alpha_i))$ and

$$\begin{aligned} [e_{\beta} h_i] \eta &= \beta(h_i) e_{\beta} \eta = (\lambda_1 \alpha_1(h_i) + \cdots + \lambda_n \alpha_n(h_i)) e_{\beta} \eta \\ &= (\lambda_1 \alpha'_1(h'_i) + \cdots + \lambda_n \alpha'_n(h'_i)) e_{\beta} \eta \\ &= [e_{\beta} \eta, h_i \eta], \quad 1 \leq j \leq n. \end{aligned}$$

If γ is a root of $\mathfrak{L}$ such that $-k < L(\gamma) < 0$, then

$$\begin{aligned} [e_{\beta} e_{\gamma}] \eta &= [[e_{\alpha} e_{\alpha_i}] e_{\gamma}] \eta = [[e_{\alpha} e_{\gamma}] e_{\alpha_i}] \eta + [e_{\alpha} [e_{\alpha_i} e_{\gamma}]] \eta \\ &= [[e_{\alpha} \eta, e_{\gamma} \eta] e_{\alpha_i} \eta] + [e_{\alpha} \eta [e_{\alpha_i} \eta, e_{\gamma} \eta]] \\ &= [[e_{\alpha} \eta, e_{\alpha_i} \eta] e_{\gamma} \eta] = [e_{\beta} \eta, e_{\gamma} \eta]. \end{aligned}$$

If γ is a root of $\mathfrak{L}$ such that $-k = L(\gamma)$ then either $\beta + \gamma$ is not a root in which case $[e_{\beta} \eta, e_{\gamma} \eta] = 0 = [e_{\beta} e_{\gamma}] \eta$, or $\beta + \gamma$ is a root of level 0, $\beta = -\gamma$, and

$$\begin{aligned} [e_{\beta} e_{\gamma}] \eta &= [e_{\beta} [e_{-\alpha} e_{-\alpha_i}]] \eta \\ &= [[e_{\beta} e_{-\alpha}] e_{-\alpha_i}] \eta - [[e_{\beta} e_{-\alpha_i}] e_{-\alpha}] \eta \\ &= [[e_{\beta} \eta, e_{-\alpha} \eta] e_{-\alpha_i} \eta] - [[e_{\beta} \eta, e_{-\alpha_i} \eta] e_{-\alpha} \eta] \\ &= [e_{\beta} \eta [e_{-\alpha} \eta, e_{-\alpha_i} \eta]] = [e_{\beta} \eta, e_{\gamma} \eta] \end{aligned}$$

by the previous calculation and the induction hypothesis.

By symmetry $[e_{-\beta} e_{\gamma}] \eta = [e_{-\beta} \eta, e_{\gamma} \eta]$ for all $e_{\gamma} \in \mathfrak{L}_k$ such that $\mathfrak{L}_{-\beta + \gamma} \subset \mathfrak{L}_k$ and $[e_{-\beta} h_i] \eta = [e_{-\beta} \eta, h_i \eta]$ for all j .

Finally, suppose that γ and ζ are roots of positive level and that $\gamma + \zeta = \beta$ is a root of level k . Then $[e_{\gamma} e_{\zeta}]$ is a non-zero scalar multiple λe_{β} of e_{β} , and $[e_{\gamma} \eta, e_{\zeta} \eta]$ is a non-zero scalar multiple $\mu e_{\tau(\beta)}$ of $e_{\tau(\beta)} = e_{\beta} \eta$. Then $e_{\beta} = [e_{\alpha} e_{\alpha_i}]$, $e_{\beta} \eta = [e_{\alpha} \eta, e_{\alpha_i} \eta]$, and $[e_{\beta} e_{-\alpha_i}] \eta = [e_{\beta} \eta, e_{-\alpha_i} \eta]$ by the above. Hence

$$0 \neq \mu [[e_{\gamma} e_{\zeta}] e_{-\alpha_i}] \eta = \mu \lambda [e_{\beta} e_{-\alpha_i}] \eta = \mu \lambda [e_{\beta} \eta, e_{-\alpha_i} \eta] = \lambda [[e_{\gamma} \eta, e_{\zeta} \eta] e_{-\alpha_i} \eta].$$

Application of the Jacobi identity and the assumption for $\mathfrak{L}_{k-1}$ yields $\mu = \lambda$ or $[e_\gamma e_\delta]\eta = [e_\gamma\eta, e_\delta\eta]$, as in [8]. Similarly $[e_{-\gamma}e_{-\delta}]\eta = [e_{-\gamma}\eta, e_{-\delta}\eta]$. This completes the proof that η has the desired properties on $\mathfrak{L}_k$, and with it the proof of the theorem.

14. Summary. We have shown that if $\mathfrak{L}$ is a finite dimensional Lie algebra over a field $\mathfrak{F}$ of characteristic not 2, 3, 5, 7, if $\mathfrak{L}$ contains an abelian Cartan subalgebra $\mathfrak{H}$, and if $\mathfrak{L}$ and $\mathfrak{H}$ satisfy the axioms (i)–(v), then $\mathfrak{L}$ is the direct sum of simple Lie algebras with the same properties (Theorems 4 and 8). Thus it is sufficient to treat the case $\mathfrak{L}$ simple. If $\mathfrak{L}$ satisfies this additional condition of simplicity, then $\mathfrak{H}^*$ is spanned by a fundamental system of roots S , and S has one of the diagrams of Figure 1 (Theorems 7 and 6). The algebra $\mathfrak{L}$ is uniquely determined (up to isomorphism) by $\mathfrak{F}$ and the diagram of S (Theorem 9).

The algebras corresponding to the diagrams of Figure 1 all actually exist. This question has been treated elsewhere and we shall not discuss it here. For characteristic zero the existence of these algebras is well known. For characteristic $p > 7$ see [8, pp. 77–83] and the following paper.

BIBLIOGRAPHY

- [1] CARTAN, E. *Thèse*. Paris 1894. 2nd ed. Vuibert, Paris 1933.
- [2] CHEVALLEY, C. Sur certains groupes simples. *Tohoku Math. Jour.* **7** (1955), 14–66.
- [3] CURTIS, C. W. Modular Lie algebras I. *Trans. Amer. Math. Soc.* **82** (1956), 160–179.
- [4] CURTIS, C. W. Modular Lie algebras II. To appear in *Trans. Amer. Math. Soc.*
- [5] DYNKIN, E. B. *The structure of semi-simple algebras*. A. M. S. Translation No. 17.
- [6] JACOBSON, N. Classes of restricted Lie algebras of characteristic p . I. *Amer. J. Math.* **63** (1941), 481–515.
- [7] KILLING, W. Die Zusammensetzung der stetigen endlichen Transformationsgruppen. *Math. Ann.* **31** (1888), 252–290; **33** (1889), 1–48; **34** (1889), 57–122; **36** (1890), 161–189.
- [8] SELIGMAN, G. B. *On Lie algebras of prime characteristic*. A. M. S. Memoir No. 19.
- [9] VAN DER WAERDEN, B. L. Die Klassifikation der einfachen Lieschen Gruppen. *Math. Zeit.* **37** (1933), 446–462.
- [10] WEYL, H. Theorie der Darstellung kontinuierlicher halbeinfacher Gruppen durch lineare Transformationen. *Math. Zeit.* **23** (1925), 271–309; **24** (1926), 328–395.
- [11] WITT, E. Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe. *Abh. Math. Sem. Hamburg Univ.* **14** (1941), 289–337.

Yale University
New Haven, Connecticut