

UNIVERSAL
LIBRARY

OU_166430

UNIVERSAL
LIBRARY

MEMOIRS
OF THE
AMERICAN MATHEMATICAL SOCIETY

NUMBER 19

ON LIE ALGEBRAS OF PRIME CHARACTERISTIC

BY

GEORGE B. SELIGMAN

PUBLISHED BY THE
AMERICAN MATHEMATICAL SOCIETY

80 Waterman St., Providence, R.I.

1956

ON LIE ALGEBRAS OF PRIME CHARACTERISTIC

George B. Seligman
Princeton University

In no respect has the structure theory of Lie algebras of prime characteristic achieved the degree of completeness of the theory for characteristic zero. Almost as inadequate is our knowledge concerning those Lie algebras which are restricted in the sense of Jacobson [13]¹. In particular, the definition of semi-simplicity as the absence of non-trivial solvable ideals is insufficient to assure a direct decomposition into simple ideals. It is to be hoped that many of the unsolved problems would be brought closer to solution by the determination of the simple Lie algebras of prime characteristic. In any case, their determination is generally regarded as a problem of the highest interest in the field. The purpose of the present memoir is to demonstrate the applicability, under certain restrictions on the algebra and the base field, of the techniques used in the determination of all simple Lie algebras of characteristic zero. The more general problem remains unsolved, although it is known that the classification presented here is incomplete even for restricted Lie algebras ([3], [8], [9], [16]; the algebra of [8] is restricted, although the author does not discuss it from this aspect).

It follows from the work of Killing [21] and Cartan [2] that a semi-simple Lie algebra over an algebraically closed field of characteristic zero is a direct sum of simple ideals, and that all simple algebras can be determined. A seemingly indispensable tool in this theory is a symmetric bilinear form, the KILLING FORM, which is non-degenerate on every semi-simple algebra of characteristic zero.

When we pass to base fields of prime characteristic, we find that the Killing form of a semi-simple algebra may be degenerate; in fact, this is the case for an entire class of (restricted) simple Lie algebras, the

* The research described here is essentially that presented to the faculty of the Graduate School of Yale University in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

¹ The numbers in brackets refer to the bibliography at the end of the paper.

WITT ALGEBRAS [3], [9]. However, if we confine our attention to those algebras with non-degenerate Killing forms, much of the effectiveness of the classical techniques is restored. It is a generalization of this class of algebras that the author has treated, namely those restricted Lie algebras L possessing no abelian ideals and having a restricted representation $x \rightarrow U(x)$ such that the form $(x, y) = \text{Tr}(U(x)U(y))$ is non-degenerate on L . The base field is required to be algebraically closed and of characteristic $p > 7$. Of these last restrictions, the former is natural in order to make possible the root-system technique; the latter could probably be replaced by " $p > 3$ ", in which case the work of §§6-14 would become even more cumbersome.

In §§1 and 2, we show that it follows from work of Zassenhaus [33] and Dieudonné [6] that this class of algebras is actually a generalization of those with non-degenerate Killing form. In §3, the Cartan decomposition is introduced and hitherto unpublished proofs by Zassenhaus and Jacobson of some of its properties are presented. §4 is devoted to two important observations by Jacobson on representations of low-dimensional algebras, and to their use in the reconstruction of essential portions of the classical root-theory. The remaining portions are reproduced by elementary considerations in §5, up to the expression of all roots as linear combinations, with coefficients in the prime field, of a linearly independent subset of roots.

In §6, we introduce and classify SIMPLE systems of roots analogous to those of Dynkin [7]. Suitably chosen, these will eventually be the invariants by means of which the simple algebras are classified. The existence of simple systems is shown in §7 by giving a procedure for enlarging a given simple system. This procedure is also useful in §§8-14, where it is shown that if a simple system of roots is INDECOMPOSABLE in the sense of Dynkin and is MAXIMAL in a certain sense, then it determines, with a single exception, the complete set of roots which can be written as linear combinations of its members. §15 gives a procedure for choosing a maximal simple system of roots in any algebra subject to our conditions and includes a proof that such a system for a simple algebra is necessarily indecomposable. In §16 we show that the complete system of roots determines a simple algebra up to isomorphism, hence that the maximal simple system also determines the algebra, with the exception mentioned above. §§17 and 18 consist of discussions of examples of algebras in the isomorphism classes previously determined. The bibliography includes several

references which may be regarded as superfluous with regard to the content of this paper, but which are listed for the sake of completeness.

It might be mentioned that while the internal structure of algebras subject to our assumptions is fairly well determined, their behavior relative to representations and extensions displays properties which create special problems. For instance, each of them has a restricted representation which is not completely reducible [10]. Recent unpublished work of C. W. Curtis on the irreducible restricted representations has revealed further complications in that respect as well.

It is to be hoped that part of the author's debt to Professor Nathan Jacobson will be indicated by acknowledging the key steps in the argument for which he is responsible. Also very beneficial were several conversations with Professor Hans Zassenhaus. Finally, the author wishes to thank C. W. Curtis, W. H. Mills and H. C. Wang for reading the manuscript and for many helpful suggestions.

I. DEFINITIONS

A LIE ALGEBRA L over a field F is a finite-dimensional vector space over F in which there is defined a bilinear product $[xy]: [xy] \in L$ for all $x, y \in L$, and $[xy]$ satisfies the following identities:

Anticommutativity: $[xx] = 0$ for all $x \in L$.

Jacobi identity: $[[xy]z] + [[yz]x] + [[zx]y] = 0$ for all $x, y, z \in L$.

From $[xx] = 0$, we see that $[xy] = -[yx]$ for all $x, y \in L$. For $0 = [x + y, x + y] = [xx] + [xy] + [yx] + [yy] = [xy] + [yx]$.

Let V be a finite-dimensional vector space over F , and let $E(V)$ be the associative algebra of all endomorphisms of V . A linear mapping U of L into $E(V)$ is called a REPRESENTATION of L in V if $U([xy]) = [U(x)U(y)] = U(x)U(y) - U(y)U(x)$ for all $x, y \in L$.

If $x \in L$, the mapping $\text{ad}(x): y \rightarrow [yx]$ is a linear mapping of L into itself, and is in fact a representation of L , called the ADJOINT REPRESENTATION of L . Moreover, $\text{ad}(x)$ has the property of being a DERIVATION of L , i.e., a mapping D satisfying $[yz]D = [yD, z] + [y, zD]$ for all $y, z \in L$. For the powers of a derivation D we have the identity

$$[yz]D^n = \sum_{i=0}^n \binom{n}{i} [yD^i, zD^{n-i}].$$

Therefore if F has prime characteristic p , we have

$$[yz]D^p = [yD^p, z] + [y, zD^p],$$

or D^p is a derivation. If $D = \text{ad}(x)$ for some $x \in L$, D is called an INNER DERIVATION.

An IDEAL J in L is a subspace such that $[JL] \subseteq J$, where $[JL]$ denotes the set of all sums $\sum [x_i y_i]$, $x_i \in J$, $y_i \in L$. J is ABELIAN if $[JJ] = (0)$. L is called SEMI-SIMPLE if L contains no non-zero abelian ideals. L is SIMPLE if L contains no ideals other than L and (0) , and if $[LL] = L$.

Dieudonné has recently published the following result: ([6])

THEOREM 1.1. (Dieudonné). Let L be a semi-simple Lie algebra over a field F . Let there be defined on L a non-degenerate symmetric bilinear form (x, y) such that $([xy], z) = (x, [yz])$ for all x, y, z in L . Then L is a direct sum of simple ideals L_i :

$$L = L_1 + L_2 + \dots + L_k.$$

When F is of characteristic zero, L is semi-simple if and only if the KILLING FORM $\text{Tr}(\text{ad}(x)\text{ad}(y))$ is non-degenerate on L . Since this form is ASSOCIATIVE in the sense of Th. 1.1, L is a direct sum of simple ideals. The classical structure theory for semi-simple Lie algebras is thus reduced to the determination of all simple Lie algebras. In the case where F is algebraically closed, the theory has been completed in this sense (Killing [21]; Cartan [2]; van der Waerden [26]; Witt [28]; Dynkin [7]). Nearly complete results in the general case have been obtained by Landherr [22], [23]; Jacobson [11], [14], [19], [20]; and Tomber [25].

It is well known that the Killing form of an ideal J in L is the restriction to J of the Killing form of L . If L has non-degenerate Killing form, the simple direct summands of Th. 1.1 are pairwise orthogonal with respect to this form. It follows that each L_i has non-degenerate Killing form. Another property of algebras with non-degenerate Killing form is the following, proved by Zassenhaus [33]:

THEOREM 1.2. (Zassenhaus). If L has non-degenerate Killing form, then every derivation of L is inner.

The CENTER C of L is the set of all $x \in L$ such that $[xy] = 0$ for all $y \in L$. C is evidently an abelian ideal in L . Since algebras with non-degenerate Killing forms are semi-simple, $C = (0)$ if L has non-degenerate Killing form.

II. RESTRICTED LIE ALGEBRAS

Let us assume now that F is of prime characteristic p . The Lie algebra L is called RESTRICTED if it is closed under an operation $x \rightarrow x^{[p]}$, satisfying the following conditions:

- (1) $(\alpha x)^{[p]} = \alpha^p x^{[p]}$, $\alpha \in F$, $x \in L$;
- (2) $[x, y^{[p]}] = x(\text{ad}(y))^p$, $x, y \in L$;
- (3) $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x, y)$, $x, y \in L$,

where $s_i(x, y)$ is the coefficient of λ^{i-1} in $x(\text{ad}(\lambda x + y))^{p-1}$.

In keeping with the motivation for its definition, we shall write x^p instead of $x^{[p]}$. The notions of restricted ideal, restricted homomorphism, etc., are now clear. We shall use the term ORDINARY to refer to ideals, homomorphisms, etc., for which the properties of p -closure and preservation of the p -th powers are not required. In particular, a representation U of L is a RESTRICTED REPRESENTATION if $U(x^p) = (U(x))^p$ for all $x \in L$.

We shall be concerned in this paper with restricted Lie algebras L which are semi-simple (in either the ordinary or the restricted sense) and which possess a restricted representation U such that the form $(x, y) = \text{Tr}(U(x)U(y))$ is non-degenerate on L . If L is semi-simple in the ordinary sense, it clearly contains no restricted abelian ideals. Conversely, let A be an ordinary abelian ideal in L . Then $a^p \in C$ for all $a \in A$, and $A + C$ is a restricted abelian ideal. Thus the two senses of semi-simplicity coincide. By Th. 1.1, if L satisfies our conditions L is a direct sum of simple ordinary ideals $L_1 + L_2 + \dots + L_k$. Let $x_1 \in L_1$, and let $x_1^p = y_1 + \dots + y_k$, $y_1 \in L_1$. If $y_j \neq 0$ for some $j > 1$, then $[x_j y_j] \neq 0$ for some $x_j \in L_j$. Thus

$$0 = [x_j x_1] = x_j \text{ad}(x_1) = x_j \text{ad}(x_1)^p = [x_j x_1^p] = [x_j y_j],$$

a contradiction. Consequently each L_i is restricted.

The restriction of U to each of the L_i defines a restricted representation of L_i with non-degenerate trace form. Thus the problem of the structure of semi-simple algebras subject to the above conditions is reduced to the determination of all simple Lie algebras subject to these conditions. We shall present a solution to the latter problem for algebraically closed fields of sufficiently high characteristic.

These results will have as corollary the structure of ordinary semi-simple Lie algebras with non-degenerate Killing form. For if L is such an algebra with $x \in L$, then $\text{ad}(x)^p$ is a derivation of L . By Th. 1.2, there exists a (unique) $y \in L$ such that $\text{ad}(x)^p = \text{ad}(y)$. If we set $y = x^p$, L becomes a restricted Lie algebra, and the adjoint representation is restricted and has non-degenerate trace form. The simple ideals in the direct decomposition of L again have non-degenerate Killing forms.

III. THE CARTAN DECOMPOSITION

The base field is now assumed to be algebraically closed. A Lie algebra H is called NILPOTENT if the sequence

$$H, [HH], [[HH]H], [[[HH]H]H], \dots$$

terminates in (0). A subalgebra H of a Lie algebra L is called a CARTAN SUBALGEBRA if

- (1) H is nilpotent;
- (2) $x \in L$, $[xH] \subseteq H$ implies $x \in H$.

The existence and properties of Cartan subalgebras are summarized in the following theorem, one proof of which may be found in [33]:

THEOREM 3.1. Let L be a Lie algebra over F . Then L contains a Cartan subalgebra H . We can write $L = H + L_\alpha + \dots + L_\lambda$, a direct sum of spaces L_λ , where λ is a function on H to F and L_λ is the set of all $x \in L$ such that $x(\lambda(h) - \text{ad}(h))^m = 0$ for some $m \geq 0$ and all $h \in H$. For $\lambda = 0$ we have $L_0 = H$, and $[L_0 L_\lambda] = L_\lambda$, $\lambda \neq 0$. $[L_\lambda L_\alpha] \subseteq L_{\lambda+\alpha}$. If $L_\lambda \neq 0$, λ is called a root of L with respect to H and L_λ is called the root-space belonging to

the root λ . If H is abelian, all roots λ are linear functions on H to F .

THEOREM 3.2 (Zassenhaus). Let L be a Lie algebra over F , and let U be a representation of L such that the form $\text{Tr}(U(x)U(y))$ is non-degenerate on L . Then every Cartan subalgebra of L is abelian.

PROOF. Let H be a Cartan subalgebra. $L = H + \sum_{\alpha} a_{\alpha} \text{root } L_{\alpha}$. Write (x, y) for $\text{Tr}(U(x)U(y))$. Let $h \in H$, $e_{\alpha} \in L_{\alpha}$, $\alpha \neq 0$. By Th. 3.1, $e_{\alpha} = \sum [h_1 e_{\alpha}^{(1)}]$, $h_1 \in H$, $e_{\alpha}^{(1)} \in L_{\alpha}$. Therefore

$$(h, e_{\alpha}) = (h, \sum [h_1 e_{\alpha}^{(1)}]) = \sum ([hh_1], e_{\alpha}^{(1)}).$$

Similarly, $([hh_1], e_{\alpha}^{(1)}) = \sum_j ([hh_1]h_j, e_{\alpha}^{(1,j)})$, and one can eventually express (h, e_{α}) as a sum of terms (z, f_{α}) , $f_{\alpha} \in L_{\alpha}$, $z \in H^m = [[\overbrace{[HH] \dots H]^m} \dots H]$. But $H^m = (0)$ for some m . Therefore $(h, e_{\alpha}) = 0$. It follows that the restriction to H of the form (x, y) is non-degenerate on H .

If $[HH] \neq (0)$, there is an element $z \neq 0$ in $[HH]$ such that $[zH] = (0)$. Let U_1 be an irreducible representation of H of degree f_1 . By Schur's lemma $U_1(z) = \lambda_1 I_{f_1}$ is a scalar. Zassenhaus [30] has also shown that each $U_1(h)$, $h \in H$, has a single eigenvalue $\mu_1(h)$.

We can choose a basis for the representation space V relative to which

$$U(h) = \begin{pmatrix} U_1(h) & & 0 \\ & \cdot & \\ * & & U_r(h) \end{pmatrix}$$

for all $h \in H$, where the U_1 are irreducible representations of H . Now $(z, h) = \sum_1 \text{Tr}(U_1(z)U_1(h)) = \sum_1 \lambda_1 \text{Tr}(U_1(h)) = \sum_1 f_1 \lambda_1 \mu_1(h)$. Since $z \in [HH]$, $\text{Tr}(U_1(z)) = f_1 \lambda_1 = 0$. Thus $(z, H) = (0)$, contradicting the non-degeneracy of the form on H . Consequently H is abelian.

THEOREM 3.3 (Jacobson). If L is a restricted Lie algebra and U is a restricted representation with non-degenerate trace form, the mapping $h \rightarrow h^p$ is a semi-linear automorphism of any Cartan subalgebra

H , i.e., $h^p = 0$ only if $h = 0$ ($h \in H$).

PROOF. Choosing a basis for V as in the proof of Th. 3.2, we have

$$U(h^p) = U(h)^p = \begin{pmatrix} U_1(h)^p & & 0 \\ & \ddots & \\ * & & U_r(h)^p \end{pmatrix}.$$

Thus if $z^p = 0$, we have $U_1(z)^p = 0$, and the single eigenvalue $\mu_1(z) = 0$. Since H is commutative, by Th. 3.2, $U_1(z) = \mu_1(z)I_{F_1} = 0$. Thus $\text{Tr}(U_1(z)U_1(h)) = 0$ and $(z, h) = 0$ for all $h \in H$. Therefore $z = 0$, as in the proof of Th. 3.2.

THEOREM 3.4 (Jacobson). Let L be a restricted Lie algebra over F , and let U be a restricted representation of L with non-degenerate trace form. Then $[x_\alpha h] = \alpha(h)x_\alpha$ for all $x_\alpha \in L_\alpha$, $h \in H$.

PROOF. For sufficiently large k , we have $x_\alpha(\alpha(h) - \text{ad}(h))^{p^k} = 0$ for all $h \in H$, or $\alpha(h)^{p^k} x_\alpha = [x_\alpha h^{p^k}]$, where $h^{p^k} = (h^{p^{k-1}})^p$, $k > 1$. It follows from Th. 3.3 and recent work of Jacobson [17] that H has a basis h_1, \dots, h_r such that $h_i^p = h_i$, $1 \leq i \leq r$. Thus $\alpha(h_i)^{p^k} x_\alpha = [x_\alpha h_i]$, $1 \leq i \leq r$, and since $\text{ad}(h_i)^p = \text{ad}(h_i)$, the eigenvalue $\alpha(h_i)$ of $\text{ad}(h_i)$ satisfies $\alpha(h_i)^p = \alpha(h_i)$. Therefore $[x_\alpha h_i] = \alpha(h_i)x_\alpha$, $1 \leq i \leq r$, and the theorem is proved.

COROLLARY 3.1. If $\alpha \neq 0$ is a root, $-\alpha$ is also a root. L_α and $L_{-\alpha}$ have the same dimension.

PROOF. Let $0 \neq x_\alpha \in L_\alpha$, $0 \neq x_\lambda \in L_\lambda$. Now $x_\alpha = [x_\alpha h]$ for some $h \in H$, and $(x_\lambda, x_\alpha) = (x_\lambda, [x_\alpha h]) = ([x_\lambda x_\alpha], h) = 0$ unless $\lambda = -\alpha$, since $[x_\lambda x_\alpha] \in L_{\lambda+\alpha}$ (by the first step in the proof of Th. 3.2, $(L_\alpha, H) = (0)$ if $\alpha \neq 0$). If $L_{-\alpha} = (0)$, we have $(L_\alpha, L) = (0)$, a contradiction. For each non-zero $x_\alpha \in L_\alpha$, there is $x_{-\alpha} \in L_{-\alpha}$ such that $(x_\alpha, x_{-\alpha}) \neq 0$. Thus L_α and $L_{-\alpha}$ are dual spaces and have the same dimension.

For each linear function λ on H to F , the non-degeneracy of (x, y) on H implies the existence of an element $h_\lambda \in H$ such that

$(h_\lambda, h) = \lambda(h)$ for all $h \in H$. In particular, this is true if λ is a root with respect to H . We observe also that $h_{-\lambda} = -h_\lambda$, $h_{\lambda+\alpha} = h_\lambda + h_\alpha$, $h_{k\lambda} = kh_\lambda$ if k is an element of F .

COROLLARY 3.2. If $e_\alpha \in L_\alpha$, $e_{-\alpha} \in L_{-\alpha}$, then
 $[e_{-\alpha}e_\alpha] = (e_{-\alpha}, e_\alpha)h_\alpha$.

PROOF. $[e_{-\alpha}e_\alpha] \in L_0 = H$. For all $h \in H$, $(h, [e_{-\alpha}e_\alpha]) = ((he_{-\alpha}), e_\alpha) = \alpha(h)(e_{-\alpha}, e_\alpha) = (h, (e_{-\alpha}, e_\alpha)h_\alpha)$. Therefore $[e_{-\alpha}e_\alpha] = (e_{-\alpha}, e_\alpha)h_\alpha$, by the proof of Th. 3.2.

IV. LEMMAS ON REPRESENTATIONS AND THEIR APPLICATIONS

In this section we give two lemmas of Jacobson on the nature of irreducible representations of Lie algebras of dimensions two and three. These are then used to obtain useful information about Lie algebras of the type under investigation.

LEMMA 4.1 (Jacobson). Let L be a two-dimensional Lie algebra (not necessarily restricted) over F with basis elements e and h and multiplication $[eh] = e$. Let U be an irreducible representation of L . Then either $U(e)^p = 0$ or U is equivalent to the p -dimensional representation W :

$$W(e) = \begin{pmatrix} 0 & \mathfrak{I} & 0 & \dots & 0 & 0 \\ 0 & 0 & \mathfrak{I} & 0 & \dots & 0 \\ & & & \vdots & & \\ & & & \vdots & & \\ 0 & 0 & \dots & 0 & 0 & \mathfrak{I} \\ \mathfrak{I} & 0 & \dots & & & 0 \end{pmatrix},$$

$$W(h) = \begin{pmatrix} \lambda & 0 & \dots & 0 & 0 & 0 \\ 0 & \lambda+1 & 0 & \dots & 0 & 0 \\ & & & \vdots & & \\ & & & \vdots & & \\ 0 & \dots & 0 & \lambda+p-2 & 0 & \\ 0 & 0 & \dots & 0 & 0 & \lambda+p-1 \end{pmatrix}$$

where λ and δ are elements of F .

PROOF. Since $[U(h), U(e)^p] = \overbrace{[[[U(h)U(e)]U(e)] \dots U(e)]}^p = -[[U(e)U(e)] \dots U(e)] = 0$, we have $U(e)^p = \sigma I$, a scalar. Similarly, $U(h)^p - U(h) = \rho I$ is a scalar. If $\sigma = 0$, we are done. We may therefore assume $\sigma \neq 0$.

In the Birkhoff-Witt algebra $A = A(L)$, let B be the ideal generated by $e^p - \sigma$ and $h^p - h - \rho$. Then A/B is an associative algebra of dimension p^2 over F . U can be extended to a representation of A such that $U(1) = I$. Since its kernel contains B , U induces a representation of A/B . Since L can be embedded in A/B , this representation is irreducible. Now take $\delta \in F$ such that $\delta^p = \sigma$, take λ such that $\lambda^p - \lambda = \rho$, and form W as above. W induces an irreducible representation of A/B of degree p , which is therefore the only irreducible representation of A/B . Therefore U is equivalent to W . To see that the representation W is irreducible, observe that $W(h)$ has p distinct eigenvalues $\lambda, \lambda + 1, \dots, \lambda + p - 1$. Let x_1, \dots, x_p be a basis for the representation space such that $x_1 W(h) = (\lambda + 1)x_1$, $1 \leq i \leq p$, $x_i W(e) = \delta x_{i+1}$, $1 \leq i < p$, $x_p W(e) = \delta x_1$. Let \mathfrak{L} be a non-zero invariant subspace. Then \mathfrak{L} contains an eigenvector v of $W(h)$, which must be of the form βx_i for some x_i , $1 \leq i \leq p$, and some scalar $\beta \neq 0$. Hence $x_i \in \mathfrak{L}$, and by operating upon x_i with powers of $W(e)$, we see that \mathfrak{L} contains the entire basis x_1, x_2, \dots, x_p .

LEMMA 4.2 (Jacobson). Let L be a three-dimensional Lie algebra (not necessarily restricted) over F with basis e, f, h , and $[ef] = h, [fh] = 0 = [eh]$. Let U be a non-zero irreducible representation of L such that $U(e)^p = 0 = U(f)^p$. Then U is equivalent to W :

$$W(f) = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 2 & 0 & \dots & 0 & 0 \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ 0 & 0 & \dots & 0 & p-1 & 0 \end{pmatrix},$$

$$W(e) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ & & & \ddots & & \\ & & & & \ddots & \\ 0 & \dots & 0 & 1 & & \\ 0 & 0 & \dots & 0 & 0 & \end{pmatrix},$$

$$W(h) = \lambda I_p, \quad \lambda \in F.$$

PROOF. $U(h) = \lambda I$ is a scalar. If $\lambda = 0$, then $[U(e)U(f)] = 0$, and $U(e) = \rho I, U(f) = \sigma I$. But $U(e)^p = \rho^p I = 0$, or $\rho = 0$. Also $\sigma = 0$, and U would have to be the zero representation. Thus $\lambda \neq 0$. Let B be the ideal in $A = A(L)$ generated by e^p, f^p , and $h - \lambda$. A/B has dimension p^2 , and U induces an irreducible representation of A/B . However, W defines an irreducible representation of A/B of degree p . Therefore U is equivalent to W . To see that W is irreducible, let x_1, x_2, \dots, x_p be a basis for the representation space such that $x_1 W(f) = 0, x_i W(f) = (i - 1)x_{i-1}, i > 1; x_i W(e) = x_{i+1}, i < p; x_p W(e) = 0$. Let \mathfrak{S} be an invariant subspace and let $0 \neq v \in \mathfrak{S}$. Let $v = \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_p x_p$. Let γ_1 be the first non-zero component, and consider $vW(e)^{p-1} = \gamma_1 x_p \in \mathfrak{S}$. Thus $x_p \in \mathfrak{S}$. Now $x_p W(f)^k = (p - 1) \dots (p - k) x_{p-k} \in \mathfrak{S}, 0 \leq k \leq p - 1$, or \mathfrak{S} contains the entire basis x_p, x_{p-1}, \dots, x_1 . Thus the representation is irreducible.

THEOREM 4.1 (Jacobson). Let L be as in Th. 3.4, and let $0 \neq \alpha$ be a root. Then if $e_\alpha \in L_\alpha, e_\alpha^p = 0$.

PROOF. If $h \in H, [he_\alpha^p] = 0$; therefore $e_\alpha^p \in H$. Let $h \in H, \alpha(h) = 1$. Then e_α and h form a two-dimensional algebra L_1 as in Lemma 4.1. Now $(e_\alpha^p, h) = \text{Tr}(U(e_\alpha)^p U(h))$, and we can write the restriction of U to L_1 in the form

$$\begin{pmatrix} U_1 & & 0 \\ & \ddots & \\ * & & U_r \end{pmatrix},$$

where the U_1 are irreducible representations of L_1 . By Lemma 4.1, either $U_1(e_\alpha)^P = 0$ or U_1 is equivalent to the representation W of that lemma for suitable λ, δ . In either case, $\text{Tr}(U_1(e_\alpha)^P U_1(h)) = 0$, so that $(e_\alpha^P, h) = 0$. It follows that $(e_\alpha^P, h) = 0$ whenever $\alpha(h) \neq 0$. If $\alpha(h) = 0$, let $h' \in H$, $\alpha(h') \neq 0$. Then $\alpha(h + h') \neq 0$, and $(e_\alpha^P, h) = (e_\alpha^P, h + h') - (e_\alpha^P, h') = 0$. Therefore $(e_\alpha^P, H) = (0)$, or $e_\alpha^P = 0$.

COROLLARY 4.1. If e_α and x_α are in L_α , then

$$[[[x_\alpha e_\alpha] e_\alpha] \dots e_\alpha] = 0.$$

PROOF. For $\lambda \in F$, $\lambda e_\alpha + x_\alpha \in L_\alpha$. Therefore we have

$$0 = (\lambda e_\alpha + x_\alpha)^P = \lambda^P e_\alpha^P + \lambda^{P-1} [[x_\alpha e_\alpha] \dots e_\alpha] + \lambda^{P-2} S_2(x_\alpha, e_\alpha) + \dots + x_\alpha^P,$$

where the coefficients $S_1(x_\alpha, e_\alpha) \in L$. Since F is infinite, all coefficients are zero, in particular that of λ^{P-1} . (For details of the expansion used, see [13].)

THEOREM 4.2 (Jacobson). If $\alpha \neq 0$ is a root, then $\alpha(h_\alpha) \neq 0$.

PROOF. Suppose $\alpha(h_\alpha) = 0$. Let $0 \neq e_\alpha \in L_\alpha$, $0 \neq e_{-\alpha} \in L_{-\alpha}$, such that $(e_{-\alpha}, e_\alpha) = 1$. By Cor. 3.2, $[e_{-\alpha}, e_\alpha] = h_\alpha$. Let L_1 be the 3-dimensional algebra spanned by $e_\alpha, e_{-\alpha}, h_\alpha$. For each irreducible constituent U_1 of the restriction to L_1 of the representation U of L , we have $U_1(e_\alpha)^P = 0$, since $U(e_\alpha)^P = U(e_\alpha^P) = 0$. Also, $U_1(e_{-\alpha})^P = 0$. Thus the algebra L_1 and the representation U_1 are as in Lemma 4.2. Either U_1 is a zero representation or U_1 is equivalent to a representation of the type of W . In either case, $\text{Tr}(U_1(e_{-\alpha})U_1(e_\alpha)) = 0$. Therefore $(e_{-\alpha}, e_\alpha) = \text{Tr}(U(e_{-\alpha})U(e_\alpha)) = 0$, a contradiction, and the theorem is proved.

V. WEIGHTS AND ROOTS

Let H be an abelian Lie algebra over F , U a representation of H in V . As in the case of the adjoint representation, we can decompose V into a direct sum .

$$V = V_0 + \sum_{\Lambda} V_{\Lambda},$$

where Λ runs through a finite set of linear functions on H to F and V_{Λ} is the set of $v \in V$ such that $v(\Lambda(h) - U(h))^m = 0$ for all $h \in H$ when m is sufficiently large. The non-zero functions Λ with $V_{\Lambda} \neq (0)$ are called the WEIGHTS of the representation U . We shall assume in the following that F is algebraically closed and of characteristic $p > 2$.

LEMMA 5.1 (Weyl-Jacobson). Let $L_1 = H + \{e_{\alpha}, e_{-\alpha}\}$, where H is an abelian restricted Lie algebra, and where $[e_{\alpha}h] = \alpha(h)e_{\alpha}$, $[e_{-\alpha}h] = -\alpha(h)e_{-\alpha}$, α a linear function on H . Assume also that $[e_{-\alpha}e_{\alpha}] = h_{\alpha} \in H$ and that $\alpha(h_{\alpha}) \neq 0$. Let Λ be a weight of a representation U of L_1 . Then either all linear forms $\Lambda - k\alpha$ ($k = 0, 1, \dots, p-1$) are weights, or the set of weights of this form consists of disjoint arithmetic progressions with difference α , each symmetric about $\Lambda - \frac{\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha$, in the follow-

ing sense: If $\Lambda - k\alpha$ is a weight, then

$$\begin{aligned} \left(\Lambda - \frac{\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha\right) + \left(\left(\Lambda - \frac{\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha\right) - (\Lambda - k\alpha)\right) &= \\ &= \Lambda + k\alpha - \frac{2\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha \end{aligned}$$

is also a weight, and either all the quantities

$$\Lambda - k\alpha, \Lambda - k\alpha + \alpha, \Lambda - k\alpha + 2\alpha, \dots, \Lambda + k\alpha - \frac{2\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha$$

are weights, or all the quantities

$$\Lambda - k\alpha, \Lambda - k\alpha - \alpha, \Lambda - k\alpha - 2\alpha, \dots, \Lambda + k\alpha - \frac{2\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha$$

are weights. In either of these situations,

$\Lambda - \frac{\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha$ will be called the MIDPOINT of the corresponding string of weights.

PROOF. Assume that not all $\Lambda - k\alpha$ are weights. Let $\mathbf{M} = \Lambda - k\alpha$ be a weight such that $\mathbf{M} - \alpha$ is not a weight. Let $0 \neq x \in V$, the representation space, such that $xU(h) = \mathbf{M}(h)x$ for all $h \in H$. Then

$$\begin{aligned} xU(e_{-\alpha})U(h) &= x([U(e_{-\alpha})U(h)] + U(h)U(e_{-\alpha})) = \\ &= -\alpha(h)xU(e_{-\alpha}) + \mathbf{M}(h)xU(e_{-\alpha}) = \\ &= (\mathbf{M} - \alpha)(h)xU(e_{-\alpha}), \end{aligned}$$

or $xU(e_{-\alpha}) \in V_{\mathbf{M} - \alpha}$. Thus $xU(e_{-\alpha}) = 0$.

Set $x_0 = x$, $x_1 = xU(e_{-\alpha})$, \dots , $x_1 = xU(e_{-\alpha})^1$, \dots . Then $x_1U(h) = (\mathbf{M} + \alpha)(h)x_1$ for all $h \in H$, and one also proves that

$$x_1U(e_{-\alpha}) = -1(\mathbf{M} + \frac{(1-1)}{2}\alpha)(h_{\alpha})x_{1-1}, \quad 1 > 0.$$

Since not all $\mathbf{M} + j\alpha$ are weights, there exists $r < p - 1$ such that $x_r \neq 0$, $x_{r+1} = 0$. Then

$$0 = x_{r+1}U(e_{-\alpha}) = -(r+1)(\mathbf{M}(h_{\alpha}) + \frac{r}{2}\alpha(h_{\alpha}))x_r.$$

Since $r < p - 1$, $r = -\frac{2\mathbf{M}(h_{\alpha})}{\alpha(h_{\alpha})}\alpha$, and the following are weights:

$$\mathbf{M} = \Lambda - k\alpha, \mathbf{M} + \alpha, \dots, \mathbf{M} + r\alpha = \Lambda - (k - r)\alpha.$$

The midpoint is $\Lambda - k\alpha + \frac{r}{2}\alpha = \Lambda - k\alpha - \frac{\mathbf{M}(h_{\alpha})}{\alpha(h_{\alpha})}\alpha = \Lambda - \frac{\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha$.

Similarly, if $\mathbf{N} = \Lambda + j\alpha$ is a weight such that $\mathbf{N} + \alpha$ is not a weight, and if $yU(h) = \mathbf{N}(h)y$ for all h , the weights include

$$\mathbf{N} = \Lambda + j\alpha, \mathbf{N} - \alpha, \dots, \mathbf{N} - s\alpha = \Lambda + (j - s)\alpha,$$

where $s = \frac{2\mathbf{N}(h_{\alpha})}{\alpha(h_{\alpha})}$. The midpoint is again $\Lambda - \frac{\Lambda(h_{\alpha})}{\alpha(h_{\alpha})}\alpha$. If the two strings of weights are not disjoint, then they must coincide; for otherwise one of the following is the case: Either one of $\mathbf{M} + (r+1)\alpha$, $\mathbf{M} - \alpha$ is a member of the second string, or one of $\mathbf{N} + \alpha$, $\mathbf{N} - (s+1)\alpha$ is a member of the first string. But $\mathbf{M} - \alpha$ and $\mathbf{N} + \alpha$ are not weights by assumption. If $\mathbf{M} + (r+1)\alpha$ is in the second string, then

so is

$$\begin{aligned}
 & \left(\mathbf{A} - \frac{\mathbf{A}(h_\alpha)}{\alpha(h_\alpha)} \alpha \right) + \left(\mathbf{A} - \frac{\mathbf{A}(h_\alpha)}{\alpha(h_\alpha)} \alpha - (\mathbf{M} + (r+1)\alpha) \right) = \\
 & = 2\mathbf{A} - \frac{2\mathbf{A}(h_\alpha)}{\alpha(h_\alpha)} \alpha - \mathbf{M} - \left(-\frac{2\mathbf{M}(h_\alpha)}{\alpha(h_\alpha)} + 1 \right) \alpha = \\
 & = 2\mathbf{A} - \frac{2\mathbf{A}(h_\alpha)}{\alpha(h_\alpha)} \alpha - \mathbf{A} + k\alpha + \frac{2\mathbf{A}(h_\alpha)}{\alpha(h_\alpha)} \alpha - 2k\alpha - \alpha = \\
 & = \mathbf{A} - k\alpha - \alpha = \mathbf{M} - \alpha,
 \end{aligned}$$

a contradiction. The remaining case is eliminated in similar fashion, completing the proof of the lemma.

COROLLARY 5.1. If L is as in Th. 3.4, α is a root and $k\alpha$ is a weight for a representation of $L_1 = H + \{e_\alpha, e_{-\alpha}\}$ (constructed to fulfill the conditions of Lemma 5.1), then $-k\alpha$ is also a weight.

PROOF. We may assume not all $k\alpha$ are weights. Then the string of weights of this form is symmetric about 0. Therefore it contains $-k\alpha$.

LEMMA 5.2. Under the conditions of Th. 3.4, either all multiples $k\alpha$ ($k = 0, 1, \dots, p-1$) of a root α are roots, or 2α is not a root.

PROOF. Suppose not all $k\alpha$ are roots, and that 2α is a root. Let L_1 be as above, and let $2\alpha, 3\alpha, \dots, r\alpha$ be roots, $(r+1)\alpha$ not a root. Let $L_2 = L_1 + \sum_{k=1}^r L_{k\alpha}$. Since $[L_2, L_1] \subseteq L_2$, L_2 may be regarded as a representation space for L_1 . 2α is a weight for this representation, but -2α is not. This contradicts Cor. 5.1.

THEOREM 5.1 (Jacobson). If not all multiples $k\alpha$ of a root α are roots, then L_α is one-dimensional.

PROOF. Choose $e_\alpha \in L_\alpha, e_{-\alpha} \in L_{-\alpha}$, such that $(e_{-\alpha}, e_\alpha) = 1$. If $\dim L_\alpha > 1$, there is a vector $u_\alpha \neq 0$ in L_α such that $(e_{-\alpha}, u_\alpha) = 0$. By Cor. 3.2, $[u_\alpha, e_{-\alpha}] = 0$. Now $[u_\alpha, e_\alpha] \in L_{2\alpha} = (0)$ by Lemma 5.2. Thus

$$\begin{aligned} 0 &= [[u_\alpha e_\alpha] e_{-\alpha}] = - [[e_\alpha e_{-\alpha}] u_\alpha] - [[e_{-\alpha} u_\alpha] e_\alpha] = \\ &= - [u_\alpha h_\alpha] = - \alpha(h_\alpha) u_\alpha, \end{aligned}$$

a contradiction. Thus the theorem is proved.

THEOREM 5.2 (Jacobson). If $p > 3$, not all multiples of α are roots.

PROOF. Suppose all $k\alpha$ are roots, $k = 1, 2, \dots, p-1$. Let

$$L_1 = (h_\alpha) + \sum_{k=1}^{p-1} L_{k\alpha}.$$

Since $h_{k\alpha} = kh_\alpha$, L_1 is a subalgebra of L , and the restriction of U to L_1 defines a non-degenerate trace form on L_1 . L_1 has the Cartan subalgebra $K = (h_\alpha)$.

Now let $0 \neq e_{-\alpha} \in L_{-\alpha}$, $0 \neq x_{k\alpha} \in L_{k\alpha}$, $1 < k < p-1$, and suppose that $[x_{k\alpha} e_{-\alpha}] = 0$. Let $e_\alpha \in L_\alpha$ be such that $(e_{-\alpha}, e_\alpha) = 1$. Let $x_1 = x_{k\alpha} (\text{ad}(e_\alpha))^{k-1}$. By induction, $x_1 \in L_{(k+1)\alpha}$, and

$$[x_1 e_{-\alpha}] = -i(k + \frac{1-1}{2})\alpha(h_\alpha)x_{1-1}.$$

In particular, $x_{p-k} \in K$, and $(h_\alpha, x_{p-k}) = (h_\alpha, [[x_{p-k-2} e_\alpha] e_\alpha]) = \alpha(h_\alpha)(e_\alpha, [x_{p-k-2} e_\alpha]) = -\alpha(h_\alpha)([e_\alpha e_\alpha], x_{p-k-2}) = 0$. Hence $x_{p-k} = 0$. Therefore $x_j \neq 0$ implies $j < p-k$. Suppose $x_j \neq 0$, $x_{j+1} = 0$. Then as in the proof of Lemma 5.1,

$$0 = [x_{j+1} e_{-\alpha}] = -(j+1)(k + \frac{j}{2})\alpha(h_\alpha)x_j.$$

Therefore either $j = p-1$ or $j \equiv -2k \pmod{p}$. But $j = p-1$ is impossible, since $j < p-k$. Therefore $j \equiv -2k \pmod{p}$.

Next suppose $[x_{2\alpha} e_{-\alpha}] = 0$ for some $x_{2\alpha} \neq 0$ in $L_{2\alpha}$. Set

$$\delta = -2\alpha. \text{ Then } [e_{-\delta} x_{2\alpha}^{-1} \delta] = 0, \text{ where } e_{-\delta} = x_{2\alpha}, x_{2\alpha}^{-1} \delta = e_{-\alpha}.$$

Letting $k = \frac{p+1}{2}$ in the sequence above and replacing α by δ , we have

$j \equiv -2(\frac{p+1}{2}) \equiv -1$, or $j = p-1$, which is impossible. Thus the mapping $x_{2\alpha} \rightarrow [x_{2\alpha} e_{-\alpha}]$ is one-to-one of $L_{2\alpha}$ into L_α . Therefore $\underline{\dim} L_\alpha \geq \underline{\dim} L_{2\alpha}$. By repetition,

$$\underline{\dim} L_\alpha \geq \underline{\dim} L_{2\alpha} \geq \underline{\dim} L_{4\alpha} \geq \dots \geq \underline{\dim} L_\alpha,$$

or $\underline{\dim} L_\alpha = \underline{\dim} L_{2\alpha}$. Therefore the mapping $\text{ad}(e_{-\alpha})$ carries $L_{2\alpha}$ onto L_α . In particular, $e_\alpha = [y_{2\alpha} e_{-\alpha}]$ for some $y_{2\alpha} \in L_{2\alpha}$. But

$$1 = (e_\alpha, e_{-\alpha}) = ([y_{2\alpha} e_{-\alpha}], e_{-\alpha}) = (y_{2\alpha}, [e_{-\alpha} e_{-\alpha}]) = 0,$$

a contradiction. This completes the proof.

THEOREM 5.3. Only 0 and $\pm \alpha$ are roots among the integral multiples of a root α .

PROOF. Suppose some $k\alpha$ is a root, $k \neq 0, 1, -1$. Since 2α is not a root, we may assume that $k\alpha - \alpha$ is not a root. Now let $k\alpha, (k+1)\alpha, \dots, r\alpha$ be roots, $(r+1)\alpha$ not a root; then $\sum_{j=k}^r J_j \alpha$ is a representation space for L_1 , as defined before. Moreover, $j=0$ is excluded from this sum; for if $j=0$ were in the sum, so would be either all of $j=1, 2, \dots, k$, or all of $j=k, k+1, \dots, -2, -1, 0$. But neither of $\pm 2\alpha$ is a root, so this is impossible. However, 0 is the midpoint of the string of roots $k\alpha, (k+1)\alpha, \dots, r\alpha$; in particular, this string contains with every root its negative. Assume $\frac{p+1}{2}\alpha$ is not a member; then neither is $-\frac{p+1}{2}\alpha = \frac{p-1}{2}\alpha$. We observe further that the string must contain some $j\alpha, 2 < j < \frac{p-1}{2}$, and we may assume j is the largest integer with this property. Then $(j+1)\alpha$ is not a member of the string. Therefore we must have $j=r$, and the string is $j\alpha, (j-1)\alpha, \dots, k\alpha$. But now $-j\alpha$ is a member of the string, and $-j \not\equiv 1 \pmod{p}$ for $0 \leq i \leq j$. Therefore the string contains more than $(j+1)$ entries; in particular, it contains $(j-j)\alpha = 0$, and this is a contradiction. Therefore $\frac{p+1}{2}\alpha = 2^{-1}\alpha$ is a root, and $\alpha = 2(2^{-1}\alpha)$ is also a root, in contradiction to Lemma 5.2. This completes the proof.

LEMMA 5.3. Let $p > 3$. Let α, β be roots, $0 \neq e_\alpha \in L_\alpha, 0 \neq e_{\pm\beta} \in L_{\pm\beta}$. Let $[e_\alpha e_\beta] = 0 = [e_\alpha e_{-\beta}]$. Then $(h_\alpha, h_\beta) = 0$.

PROOF. By Ths. 5.1 and 5.2, we may assume $(e_\beta, e_{-\beta}) = 1$. Then

$$\begin{aligned}
0 &= [[e_\alpha e_\beta] e_{-\beta}] = - [[e_\beta e_{-\beta}] e_\alpha] - [[e_{-\beta} e_\alpha] e_\beta] = \\
&= - [e_\alpha h_\beta] = - \alpha(h_\beta) e_\alpha = - (h_\alpha, h_\beta) e_\alpha.
\end{aligned}$$

Thus $(h_\alpha, h_\beta) = 0$.

THEOREM 5.4. If α and β are roots, and if $p > 3$, not all of the following are roots: $\alpha - 2\beta$, $\alpha - \beta$, α , $\alpha + \beta$, $\alpha + 2\beta$. Therefore no "connected" string of the form $\alpha + k\beta$ contains more than four roots.

PROOF. If all the above are roots, then $2\beta = (\alpha + 2\beta) - \alpha$ and $2(\alpha + \beta) = (\alpha + 2\beta) + \alpha$ are not roots. By Lemma 5.3, $(h_{\alpha+2\beta}, h_\alpha) = 0$, or $(h_\alpha, h_\alpha) = -2(h_\alpha, h_\beta)$. Also $(\alpha - 2\beta) \pm \alpha$ are not roots, and $(h_\alpha, h_\alpha) = 2(h_\alpha, h_\beta)$. Therefore $4(h_\alpha, h_\beta) = 0$, or $(h_\alpha, h_\beta) = 0$. But then $\alpha(h_\alpha) = (h_\alpha, h_\alpha) = 0$, a contradiction. The second assertion is an immediate consequence.

THEOREM 5.5. Let $p > 3$, and let α and β be roots, $\alpha \neq -\beta$. Then $[L_\alpha L_\beta] = L_{\alpha+\beta}$.

PROOF. All root-spaces L_α are one-dimensional, and $[L_\alpha L_\beta] \subseteq L_{\alpha+\beta}$. Therefore if $\alpha + \beta$ is not a root, $[L_\alpha L_\beta] = (0) = L_{\alpha+\beta}$. If $\alpha + \beta$ is a root, it suffices to show $[e_\alpha e_\beta] \neq 0$ for non-zero $e_\alpha \in L_\alpha$, $e_\beta \in L_\beta$.

Since there are at most four consecutive roots of the form $\alpha + k\beta$, we can apply Lemma 5.1 to assert that the connected string containing α is an arithmetic progression with difference β . If $\alpha - j\beta$ is a member of this string, while $\alpha - (j+1)\beta$ is not a root, let $0 \neq x_0 \in L_{\alpha-j\beta}$, and let $x_1 = x_0 \text{ad}(e_\beta)^1$, $i > 0$. As in the proof of Lemma 5.1, $x_1 \in L_{\alpha-(j-1)\beta}$ and $x_1 = 0$ only when $\alpha - (j-1)\beta$ is no longer a root. (For suppose $\alpha - j\beta, \alpha - (j-1)\beta, \dots, \alpha - (j-1)\beta$ are roots, $\alpha - (j-1-1)\beta$ not a root; this string of roots has the same midpoint $\alpha - \frac{\alpha(h_\beta)}{\beta(h_\beta)}$ as does the string $\alpha - j\beta, \alpha - (j-1)\beta, \dots, \alpha - (j-t)\beta$ of those roots $\alpha - (j-s)\beta$ for which $x_s \neq 0$. Hence the strings coincide.) In particular, $x_j \neq 0$, $x_{j+1} \neq 0$. Now $x_j = \lambda e_\alpha \in L_\alpha$, $\lambda \neq 0$, and $x_{j+1} = \lambda [e_\alpha e_\beta] \neq 0$. Therefore

$[e_\alpha e_\beta] \neq 0$, and the theorem is proved.

THEOREM 5.6. Let α and β be roots, and let the progression of roots of the form $\alpha + k\beta$ containing α be

$$\alpha - r\beta, \dots, \alpha - \beta, \alpha, \alpha + \beta, \dots, \alpha + q\beta.$$

Then if $p > 3$, $\frac{2(h_\alpha, h_\beta)}{(h_\beta, h_\beta)} = r - q$.

PROOF. Let $0 \neq x_0 \in L_{\alpha - r\beta}$, and let $x_i = x_0 \text{ad}(e_\beta)^i$, $i > 0$, where $0 \neq e_\beta \in L_\beta$. Let $e_{-\beta} \in L_{-\beta}$, $(e_{-\beta}, e_\beta) = 1$. Then $x_i \in L_{\alpha - (r-i)\beta}$, and as in the proof of Lemma 5.1,

$$[x_{i+1} e_{-\beta}] = - (i + 1)(\alpha - r\beta + \frac{1}{2}\beta)(h_\beta)x_i, \quad i \geq 0.$$

Now $r + q + 1 \leq 4$, $x_{r+q} \neq 0$ by Th. 5.5, and $x_{r+q+1} = 0$. Thus

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

or $\frac{2(h_\alpha, h_\beta)}{(h_\beta, h_\beta)} = r - q$.

THEOREM 5.7. If α and β are roots and $p > 5$, all roots of the form $\alpha + k\beta$ lie in the connected string containing α .

PROOF. Let $\alpha + k\beta$ be a root not in this string. We may assume that $\alpha + (k - 1)\beta$ is not a root. The string $\alpha + k\beta, \alpha + (k + 1)\beta, \dots, \alpha + n\beta$ is symmetric about $\alpha - \frac{\alpha(h_\beta)}{\beta(h_\beta)}\beta$. By Ths. 5.4 and 5.6, $\frac{2\alpha(h_\beta)}{\beta(h_\beta)}$ is among $0, \pm 1, \pm 2, \pm 3$.

If $\alpha(h_\beta) = 0$, then as in the proof of Th. 5.3, $\alpha \pm 2^{-1}\beta$ are roots. However,

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

which means by Th. 5.6, and the fact that $p > 5$ that $\alpha + 2^{-1}\beta - \alpha = 2^{-1}\beta$ is a root, a contradiction. A similar contradiction is reached by

assuming that $\frac{2(h_\alpha, h_\beta)}{(h_\beta, h_\beta)} = \pm 2$, in the case of $+ 2$ by replacing α by

$\alpha - \beta$, and in the case of -2 by replacing α by $\alpha + \beta$ (which we know to be roots in these cases by Th. 5.6) and then applying the reasoning of the case $\alpha(h_\beta) = 0$.

Now when $\frac{2(h_\alpha, h_\beta)}{(h_\beta, h_\beta)} = 1$, any string of this type is symmetric about $\alpha - \frac{1}{2}\beta$. As in the proof of Th. 5.3, either $\alpha - \frac{1}{2}\beta$ is a member of such a string or the string contains $(\alpha - \frac{1}{2}\beta) + \frac{p+1}{2}\beta = \alpha$. In the latter case, we have the connected string about α . Therefore $\alpha - \frac{1}{2}\beta$ is a member of the string $\alpha + k\beta, \dots, \alpha + n\beta$, and is in fact the midpoint. Now replace α by $\alpha - \frac{1}{2}\beta$ and apply the case $\alpha(h_\beta) = 0$ to obtain the same contradiction as before. One treats the cases $\frac{2(h_\alpha, h_\beta)}{(h_\beta, h_\beta)} = -1, 3, -3$ in similar fashion.

Let $\alpha_1, \alpha_2, \dots, \alpha_r$ be a maximal set of linearly independent roots. Then every root can be expressed as a linear combination of these α_i . Moreover, $h_i = h_{\alpha_i}$ are linearly independent elements of H , and every h_α (α a root) can be expressed as a linear combination of the h_i . Let H_0 be the subspace of H spanned by the h_i , and let

$$L_0 = H_0 + \sum_{\alpha \text{ a root}} L_\alpha.$$

LEMMA 5.4. $L_0 = [LL]$.

PROOF. Let $h_{r+1}, \dots, h_j \in H$ be such that h_1, \dots, h_j is a basis for H . Then every $x \in L$ is uniquely expressible in the form

$$x = \sum_{i=1}^j \lambda_i h_i + \sum_{\alpha} \lambda_{\alpha} e_{\alpha},$$

where the λ 's are in F and $[e_{-\alpha} e_{\alpha}] = h_{\alpha}$. Now

$$[xh_1] = \sum_{\alpha} \lambda_{\alpha} \alpha(h_1) e_{\alpha} \in L_0,$$

and

$$[xe_{\alpha}] = - \sum_i \lambda_i \alpha(h_i) e_{\alpha} + \lambda_{-\alpha} h_{\alpha} + \sum_{\beta \neq -\alpha} \lambda_{\beta} N_{\beta\alpha} e_{\alpha+\beta} \in L_0,$$

where $N_{\beta\alpha} \in F$, $N_{\beta\alpha} = 0$ if and only if $\alpha + \beta$ is not a root. Thus $[LL] \subseteq L_0$. Since $h_i = [e_{-\alpha_i} e_{\alpha_i}] \in [LL]$, $1 \leq i \leq r$, and since $e_{\alpha} = \alpha(h_{\alpha})^{-1} [e_{\alpha} h_{\alpha}] \in [LL]$ for all α , $L_0 \subseteq [LL] = L_0$.

By Th. 1.1, $L = [LL] = L_0$ whenever L contains no abelian ideals (and has non-degenerate trace form, of course). We shall assume that this is the case in all that follows.

THEOREM 5.8. Let $p > 3$, and let $\alpha_1, \alpha_2, \dots, \alpha_r$ be a maximal set of linearly independent roots with respect to $H (= H_0)$. Then any root α with respect to H is a linear combination of the α_i with coefficients in the prime field contained in F .

PROOF. Let $\alpha = \sum \lambda_i \alpha_i$, $\lambda_i \in F$. By Th. 5.6, the quantities $\frac{2\alpha(h_i)}{\alpha_i(h_i)}$ and $\frac{2\alpha_j(h_i)}{\alpha_i(h_i)}$, $1 \leq i, j \leq r$, are integers modulo p , or are in the prime field contained in F . Since the h_i span H , and since (x, y) is non-degenerate on H , the matrix

$$\frac{2\alpha_j(h_i)}{\alpha_i(h_i)} = \frac{2(h_i, h_j)}{(h_i, h_i)}$$

is non-singular. Thus the system of equations

$$\frac{2\alpha(h_i)}{\alpha_i(h_i)} = \sum_{j=1}^r \lambda_j \frac{2\alpha_j(h_i)}{\alpha_i(h_i)}, \quad 1 \leq i \leq r,$$

has a unique solution in F , in fact, in the prime field Z_p . Thus the theorem is proved.

VI. SIMPLE SYSTEMS OF ROOTS

Throughout the following it will be assumed that the characteristic p of F is greater than 7, in order to avoid ambiguities in the application of Th. 5.6. Further distinguishing of cases will make the techniques applicable at characteristics 5 and 7.

LEMMA 6.1. Let α_1, α_2 be roots, $\alpha_1 \neq \pm \alpha_2$.

Let

$$A_{ij} = \frac{2\alpha_i(h_j)}{\alpha_j(h_j)}, \quad i, j = 1, 2,$$

where $h_j = h_{\alpha_j}$ as before. Then one of the

following is the case:

$$A_{12} = 0 = A_{21};$$

$$A_{12} = 1 = A_{21}; A_{12} = -1 = A_{21};$$

$$A_{12} = 2, A_{21} = 1; A_{12} = -2, A_{21} = -1;$$

$$A_{12} = 1, A_{21} = 2; A_{12} = -1, A_{21} = -2;$$

$$A_{12} = 3, A_{21} = 1; A_{12} = -3, A_{21} = -1;$$

$$A_{12} = 1, A_{21} = 3; A_{12} = -1, A_{21} = -3.$$

PROOF. If $A_{12} = 0$, then $A_{21} = 0$, since $\alpha_1(h_j) = \alpha_j(h_1)$. Now if $A_{12} \neq 0$, then $A_{12} = \pm 1, \pm 2$, or ± 3 . If $A_{12} = 2$ or 3 , then by Th. 5.6, $\alpha_1 - \alpha_2$ and $\alpha_1 - 2\alpha_2$ are roots, and as in the proof of Th. 5.4, $A_{21} = 1$. Likewise, if $A_{12} = -2$, or -3 , $A_{21} = -1$. By symmetry, we need only eliminate the possibility $A_{12} = 1 = -A_{21}$. But then $\alpha_1 - \alpha_2$ is a root by Th. 5.6, as is $-(\alpha_1 - \alpha_2) = \alpha_2 - \alpha_1$. But $A_{\alpha_2 - \alpha_1, \alpha_1} = -3$, where the notation is an extension of that used above; by Th. 5.6, $\alpha_2 - \alpha_1 + 3\alpha_1 = \alpha_2 + 2\alpha_1$ is a root, and by the proof of Th. 5.4, $A_{12} = -1$, a contradiction. Thus the lemma is proved.

Let $\alpha_1, \alpha_2, \dots, \alpha_k$ be a set of linearly independent roots with respect to the Cartan subalgebra H . This system is called SIMPLE if $\alpha_1 - \alpha_j$ is not a root for any $1 \neq j$, $1 \leq i, j \leq k$. A simple system of roots is DECOMPOSABLE if it splits into two subsystems S_1, S_2 , such that $\alpha_1(h_2) = 0$ for all $\alpha_1 \in S_1, \alpha_2 \in S_2$. Simple systems of roots are represented by diagrams consisting of dots and lines, using dots to indicate the roots of the system and lines their relationships, as follows:

If α_1, α_2 are roots (dots), we connect them by

a single line if $A_{12}A_{21} = 1$,

a double line if $A_{12}A_{21} = 2$,

a triple line if $A_{12}A_{21} = 3$.

α_1 and α_2 are not connected directly by a line (passing through no intermediate dot) if and only if $A_{12} = 0$. From the definition of a simple system, it follows that A_{1j} is among $0, -1, -2, -3$ if

$i \neq j$. Thus Lemma 6.1 specializes to

LEMMA 6.2. There are three possible indecomposable simple systems (i.s.s.) consisting of two roots, namely:

$$A_2: \circ \text{---} \circ; \quad B_2: \circ \text{====} \circ; \quad G_2: \circ \text{=====} \circ.$$

LEMMA 6.3. The only possible i.s.s. of three roots are:

$$A_3: \circ \text{---} \circ \text{---} \circ; \quad B_3, C_3: \circ \text{---} \circ \text{====} \circ.$$

PROOF. Let $\alpha_1, \alpha_2, \alpha_3$ be an i.s.s. Suppose first that $\alpha_1 + \alpha_2$ is not a root. By Lemma 5.3, $A_{12} = A_{21} = 0$. By indecomposability, $A_{13} \neq 0, A_{23} \neq 0$.

CASE 1: $A_{13}A_{31} = 1 = A_{23}A_{32}$. This gives the diagram A_3 .

CASE 2: $A_{13}A_{31} = 2, A_{23}A_{32} = 1$, or $A_{13}A_{31} = 1, A_{23}A_{32} = 2$. These give the diagram B_3, C_3 .

CASE 3: $A_{13}A_{31} = 2 = A_{23}A_{32}$. Assume first that $A_{13} = -2, A_{23} = -2$. Then $A_{31} = -1 = A_{32}$. Here and in the sequel we shall write $(\lambda_1 \dots \lambda_k)$ for $\sum_{i=1}^k \lambda_i \alpha_i, \lambda_i \in F$. By repeated applications of Th. 5.6, we see that the following are roots:

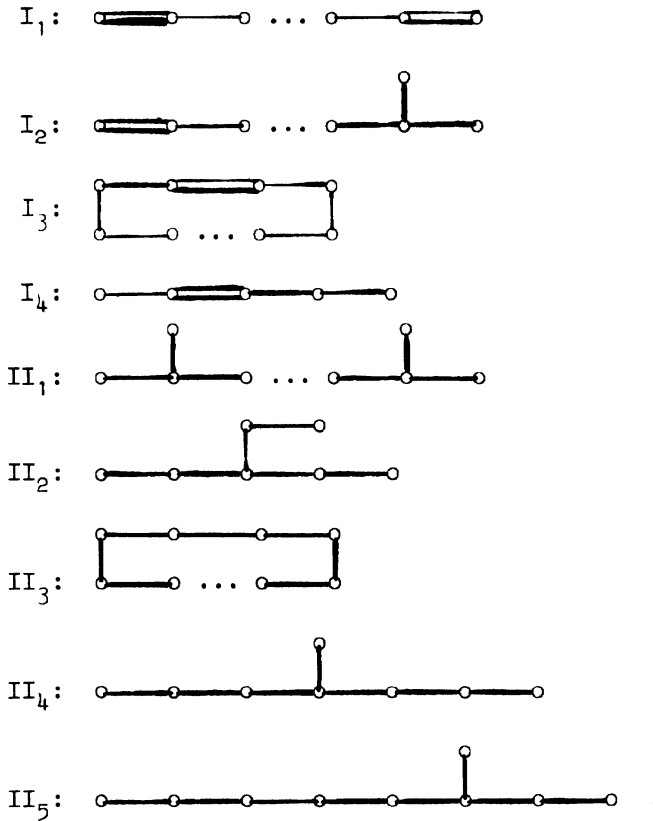
$$(1 \ 0 \ 1), (1 \ 0 \ 2), (1 \ 1 \ 2), (1 \ 2 \ 2), (0 \ 1 \ 2), (2 \ 1 \ 2), \\ (2 \ 1 \ 4), (2 \ 2 \ 4) = 2(1 \ 1 \ 2), \text{ a contradiction.}$$

Now assume $A_{13} = -2 = A_{32}$. Then $A_{31} = -1 = A_{23}$, and the roots include

$$(1 \ 0 \ 1), (1 \ 0 \ 2), (0 \ 1 \ 1), (0 \ 2 \ 1), (1 \ 1 \ 1), (1 \ 1 \ 2), (1 \ 2 \ 2), \\ (1 \ 3 \ 2), (1 \ 3 \ 3), (2 \ 3 \ 3), (2 \ 3 \ 4), (2 \ 4 \ 4) = 2(1 \ 2 \ 2), \text{ a} \\ \text{contradiction. The case } A_{31} = -2 = A_{23} \text{ is eliminated} \\ \text{by symmetry.}$$

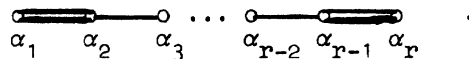
Finally let $A_{31} = -2 = A_{32}, A_{13} = -1 = A_{23}$. The roots include

LEMMA 6.4. There is no i.s.s. of the form:



PROOF. The proof will consist of showing that in each case we obtain two roots, one of which is twice the other. The techniques are those of the proof of Lemma 6.3, involving repeated use of Th. 5.6. We suppress monotonous computations, writing only the final steps.

I₁. Label the diagram as shown:



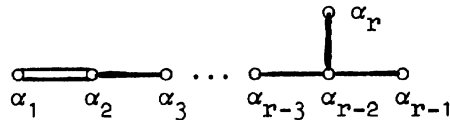
There are four possible cases: a) $A_{12} = -2 = A_{r,r-1}$; b) $A_{12} = -2 = A_{r-1,r}$; c) $A_{21} = -2 = A_{r-1,r}$; d) $A_{21} = -2 = A_{r,r-1}$. Cases b) and d) are equivalent by symmetry.

a) The roots include $(1\ 2\ 2\ \dots\ 2\ 1)$ and $2(1\ 2\ 2\ \dots\ 2\ 1)$, a contradiction.

b) The roots include $(1\ 2\ \dots\ 2)$ and $2(1\ 2\ \dots\ 2)$, a contradiction.

c) The roots include $(1\ 1\ \dots\ 1)$ and $2(1\ 1\ \dots\ 1)$, a contradiction. Thus I_1 is eliminated.

I_2 . Label the diagram as shown:



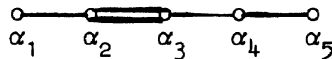
There are two cases: a) $A_{12} = -2$; b) $A_{21} = -2$.

a) The roots include $(1\ 2\ 2\ \dots\ 2\ 1\ 1)$ and $2(1\ 2\ 2\ \dots\ 2\ 1\ 1)$, a contradiction.

b) The roots include $(2\ 2\ \dots\ 2\ 1\ 1)$ and $2(2\ 2\ \dots\ 2\ 1\ 1)$, a contradiction. Thus I_2 is eliminated.

I_3 . Since all quantities which are roots in the case of the diagram II_3 are roots in this case, we refer to II_3 for the elimination of both cases I_3 and II_3 .

I_4 . Label the diagram as shown:

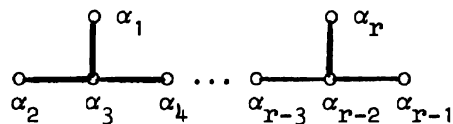


There are two cases: a) $A_{23} = -2$; b) $A_{32} = -2$.

a) The roots include $(1\ 2\ 3\ 2\ 1)$ and $2(1\ 2\ 3\ 2\ 1)$, a contradiction.

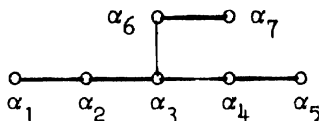
b) The roots include $(2\ 4\ 3\ 2\ 1)$ and $2(2\ 4\ 3\ 2\ 1)$, a contradiction. Thus I_4 is eliminated.

II_1 . Label the diagram as shown:



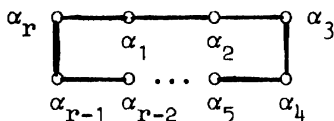
The roots include $(1\ 1\ 2\ 2\ \dots\ 2\ 1\ 1)$ and $2(1\ 1\ 2\ 2\ \dots\ 2\ 1\ 1)$, a contradiction. This eliminates II_1 .

II_2 . Label the diagram as shown:



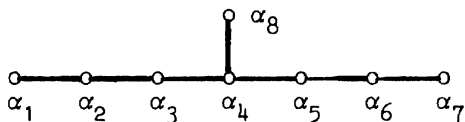
The roots include $(1\ 2\ 3\ 2\ 1\ 2\ 1)$ and $2(1\ 2\ 3\ 2\ 1\ 2\ 1)$, a contradiction. This eliminates II_2 .

II_3 . Label the diagram as shown:



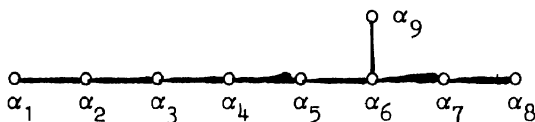
The roots include $(1\ 1\ \dots\ 1)$ and $2(1\ 1\ \dots\ 1)$, a contradiction. This eliminates II_3 (and with it, I_3).

II_4 . Label the diagram as shown:



The roots include $(1\ 2\ 3\ 4\ 3\ 2\ 1\ 2)$ and $2(1\ 2\ 3\ 4\ 3\ 2\ 1\ 2)$, a contradiction. This eliminates II_4 .

II_5 . Label the diagram as shown:

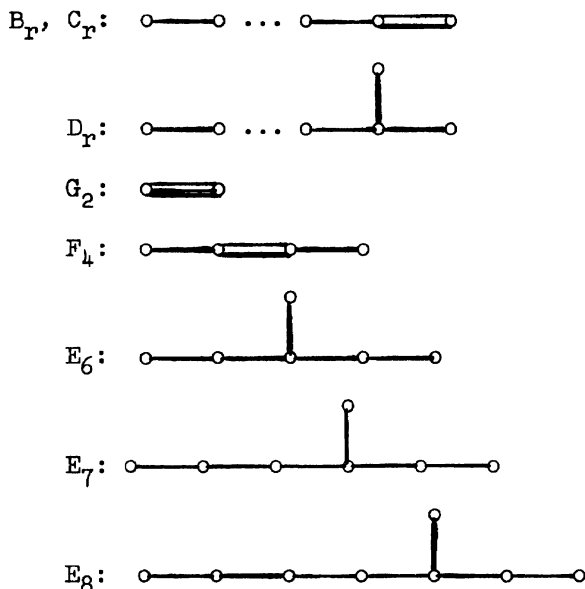


The roots include $(1\ 2\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$ and $2(1\ 2\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$, a contradiction. This eliminates II_5 and completes the proof.

From Lemmas 6.2, 6.3 and 6.4 the following theorem is an easy consequence ([7], p. 139).

THEOREM 6.1. Every i.s.s. must have one of the following diagrams:





VII. EXISTENCE OF SIMPLE SYSTEMS

We next demonstrate that L possesses a FUNDAMENTAL simple system of roots, i.e., a simple system $\alpha_1, \dots, \alpha_r$ such that h_1, \dots, h_r form a basis for H . The existence of such a system will follow from the following lemma, which we shall use again later.

LEMMA 7.1. Let $\alpha_1, \dots, \alpha_k$ be a simple system of roots in L , and let α be a root independent of $\alpha_1, \dots, \alpha_k$. Then we can form a string of roots $\alpha, \alpha - \alpha_{i_1}, \alpha - \alpha_{i_1} - \alpha_{i_2}, \dots, \beta$, $1 \leq i_s \leq k$, such that $\beta - \alpha_{i_1}$ is not a root for $1 \leq i \leq k$.

PROOF. Assume first that $\alpha_1, \dots, \alpha_k$ is indecomposable. If $k = 1$, we form the string $\alpha, \alpha - \alpha_1, \alpha - 2\alpha_1, \alpha - 3\alpha_1$, and let β be the last entry which is a root.

Now let $k = 2$. Then α_1, α_2 is of type A_2, B_2 , or G_2 . In case B_2 , we may assume $A_{12} = -2$, and in case G_2 , that $A_{12} = -3$. We may also assume that γ is a root obtained by α by subtracting α_2 a sufficient number of times so that $\gamma - \alpha_2$ is no longer a root. Then γ and α_2 form a simple system, which by Lemma 6.2 is one of the following:

- 0) $\begin{array}{c} \circ \\ \mathfrak{Y} \end{array} \quad \begin{array}{c} \circ \\ \alpha_2 \end{array}$ 1) $\begin{array}{c} \circ \text{---} \circ \\ \mathfrak{Y} \quad \alpha_2 \end{array}$
- 2) $\begin{array}{c} \text{---} \\ \mathfrak{Y} \quad \alpha_2 \end{array}$, $A_{\mathfrak{Y},2} = -2$; 3) $\begin{array}{c} \text{---} \\ \mathfrak{Y} \quad \alpha_2 \end{array}$, $A_{2,\mathfrak{Y}} = -2$;
- 4) $\begin{array}{c} \text{---} \\ \mathfrak{Y} \quad \alpha_2 \end{array}$, $A_{\mathfrak{Y},2} = -3$; 5) $\begin{array}{c} \text{---} \\ \mathfrak{Y} \quad \alpha_2 \end{array}$, $A_{2,\mathfrak{Y}} = -3$.

A similar notation will be used throughout; e.g., $A_2 0$) will refer to the case

$$\begin{array}{c} \circ \text{---} \circ \\ \alpha_1 \quad \alpha_2 \end{array}, \quad \begin{array}{c} \circ \\ \mathfrak{Y} \end{array} \quad \begin{array}{c} \circ \\ \alpha_2 \end{array}$$

and we shall put

$$A_{\mathfrak{Y},1} = \frac{2\mathfrak{Y}(h_1)}{\alpha_1(h_1)}, \quad A_{1,\mathfrak{Y}} = \frac{2\mathfrak{Y}(h_1)}{\mathfrak{Y}(h_{\mathfrak{Y}})}, \quad 1 \leq i \leq k.$$

Then all the quantities of the form A_{ij} , $A_{1,\mathfrak{Y}}$, $A_{\mathfrak{Y},1}$ are determined by the specification of the case (such as $A_2 0$) except for $A_{1,\mathfrak{Y}}$ and $A_{\mathfrak{Y},1}$. We must subdivide further to treat all possible values for these quantities as indicated in Lemma 6.1.

$A_2 0$) If $A_{\mathfrak{Y},1} = -2$ or -3 , or if $A_{1,\mathfrak{Y}} = -2$ or -3 , then $\mathfrak{Y} - \alpha_1$ is not a root, and we can take $\rho = \mathfrak{Y}$. (Since $\mathfrak{Y}, \alpha_1, \alpha_2$ form an i.s.s., $A_{\mathfrak{Y},1} = -3$ and $A_{1,\mathfrak{Y}} = -3$ are impossible; however, we shall in general omit observations of this nature.) Now suppose $A_{\mathfrak{Y},1} = -1 = A_{1,\mathfrak{Y}}$. If $\mathfrak{Y} - \alpha_1$ is a root, so is $\mathfrak{Y} - \alpha_1 - \alpha_2$ by Th. 5.6, and by another application of Th. 5.6, $\mathfrak{Y} - \alpha_2$ is a root, a contradiction. A similar contradiction results from assuming that $\mathfrak{Y} - \alpha_1$ is a root in the case $A_{\mathfrak{Y},1} = 0 = A_{1,\mathfrak{Y}}$. In these cases, we take $\rho = \mathfrak{Y}$.

Next let $A_{\mathfrak{Y},1} = 1$. Then $\mathfrak{Y} - \alpha_1$ is a root, as is $\mathfrak{Y} - \alpha_1 - \alpha_2$. If $\mathfrak{Y} - 2\alpha_1 - \alpha_2$ is a root, so is $\mathfrak{Y} - \alpha_2$, a contradiction. If $\mathfrak{Y} - \alpha_1 - 2\alpha_2$ is a root, so are $\mathfrak{Y} - \alpha_1 + \alpha_2$, $\mathfrak{Y} + \alpha_2$, and $\mathfrak{Y} - \alpha_2$, a contradiction. Thus we take $\rho = \mathfrak{Y} - \alpha_1 - \alpha_2$.

Now let $A_{\mathfrak{Y},1} = 2$. $\mathfrak{Y} - 2\alpha_1$ is a root, as is $\mathfrak{Y} - 2\alpha_1 - 2\alpha_2$. If $\mathfrak{Y} - 3\alpha_1 - 2\alpha_2$ is a root, so are $\mathfrak{Y} - \alpha_1 - 2\alpha_2$, $\mathfrak{Y} - \alpha_1 + \alpha_2$, $\mathfrak{Y} + \alpha_2$, $\mathfrak{Y} - \alpha_2$, a contradiction. If $\mathfrak{Y} - 2\alpha_1 - 3\alpha_2 = \delta$ is a root, then

$A_{\delta,2} = -4$, a contradiction. Thus we take $\beta = \gamma - 2\alpha_1 - 2\alpha_2$. Similarly if $A_{\gamma,1} = 3$, we can take $\beta = \gamma - 3\alpha_1 - 3\alpha_2$.

A_2^1) Here $\gamma(h_\gamma) = \alpha_2(h_2) = \alpha_1(h_1)$. Thus $A_{\gamma,1} = A_{1,\gamma} = 1, 0$ or -1 , by Lemma 6.1. First let $A_{\gamma,1} = -1$. If $\gamma - \alpha_1$ is a root, we know by Th. 5.6 that $\gamma - 2\alpha_1$ is not a root. If $\gamma - \alpha_1 - \alpha_2$ is a root, so is $\gamma - \alpha_2$, a contradiction. Thus we take $\beta = \gamma$ if $\gamma - \alpha_1$ is not a root and $\beta = \gamma - \alpha_1$ if $\gamma - \alpha_1$ is a root.

When $A_{\gamma,1} = 0$, either $\gamma - \alpha_1$ is a root or we take $\beta = \gamma$. In the former case we can take $\beta = \gamma - \alpha_1$, as above. Now let $A_{\gamma,1} = 1$. Then $\gamma - \alpha_1$ is a root. If $\gamma - 2\alpha_1$ is a root, so are $\gamma - 2\alpha_1 - \alpha_2$ and $\gamma - \alpha_2$, a contradiction. Thus either $\gamma - \alpha_1 - \alpha_2$ is a root or we can take $\beta = \gamma - \alpha_1$. In the former case, one may show in similar fashion that we can take $\beta = \gamma - \alpha_1 - \alpha_2$.

A_2^2) Here $\gamma(h_\gamma) = 2\alpha_2(h_2) = 2\alpha_1(h_1)$. Therefore $A_{\gamma,1} = -2, 0$ or 2 . If $A_{\gamma,1} = -2$, we can take $\beta = \gamma$. If $A_{\gamma,1} = 0$, we take $\beta = \gamma$ or $\beta = \gamma - \alpha_1$ as in the corresponding subcase of A_2^1). If $A_{\gamma,1} = 2$, we show as above that we can take $\beta = \gamma - 2\alpha_1$ or $\beta = \gamma - 2\alpha_1 - \alpha_2$.

A_2^3) Here $2\gamma(h_\gamma) = \alpha_2(h_2) = \alpha_1(h_1)$, and $A_{\gamma,1} = -1, 0$ or 1 . β can be taken by the procedure of case A_2^1). The same choice suffices in the case A_2^5).

A_2^4) $\gamma(h_\gamma) = 3\alpha_2(h_2) = 3\alpha_1(h_1)$, and $A_{\gamma,1} = -3, 0$ or 3 . The first is impossible by Lemma 6.3. If $A_{\gamma,1} = 0$, we obtain either $\beta = \gamma$ or $\beta = \gamma - \alpha_1$. When $A_{\gamma,1} = 3$, we take $\beta = \gamma - 3\alpha_1$. However, all these contradict Lemma 6.3, so the case A_2^4) cannot occur.

B_2^0) (As indicated before, this is the case $A_{1,2} = -2, A_{2,\gamma} = 0$.) As in the case A_2^0), we can restrict our attention to the cases $A_{\gamma,1} = 1, 2, 3$. When $A_{\gamma,1} = 1$, $\gamma - 2\alpha_1 - 2\alpha_2$ is a root, and we can take $\beta = \gamma - 2\alpha_1 - 2\alpha_2$. This gives an i.s.s. not allowable under Lemma 6.3. When $A_{\gamma,1} = 2$ or 3 , $\gamma - 2\alpha_1$ is a root, and $A_{\gamma-2\alpha_1,\alpha_2} = 4$, a contradiction.

B_2^1) $\gamma(h_\gamma) = \alpha_2(h_2) = \frac{1}{2}\alpha_1(h_1)$. Hence $A_{\gamma,1} = -1, 0$ or 1 . In the first two cases, we can take $\beta = \gamma$, and obtain a system in the first case which is impossible by Lemma 6.3. In case $A_{\gamma,1} = 1$, we can take $\beta = \gamma - \alpha_1 - \alpha_2$.

B_2^2) $\gamma(h_\gamma) = 2\alpha_2(h_2) = \alpha_1(h_1)$. Therefore $A_{\gamma,1} = -1, 0$ or 1 .

By Lemma 6.3, we cannot have $\beta = \gamma$. Therefore $\gamma - \alpha_1$ is a root. If $A_{\gamma,1} = -1$ or 0 we can take $\beta = \gamma - \alpha_1$. If $A_{\gamma,1} = +1$, then either we can take $\beta = \gamma - \alpha_1$, or $\gamma - \alpha_1 - \alpha_2$ is a root and we can take $\beta = \gamma - \alpha_1 - \alpha_2$.

B₂3) $2\gamma(h_{\gamma}) = \alpha_2(h_2) = \frac{1}{2}\alpha_2(h_1)$. Thus either $A_{\gamma,1} = 0$, or $p = 11$ and $A_{\gamma,1} = \pm 3$. If $A_{\gamma,1} = 0$ and $\gamma - \alpha_1$ is a root, we can take $\beta = \gamma - \alpha_1$, otherwise $\beta = \gamma$. $A_{\gamma,1} = -3$ is impossible by Lemma 6.3. If $A_{\gamma,1} = 3$, $\gamma - 3\alpha_1$ is a root, and $A_{\gamma-3\alpha_1,\alpha_2} = 4$, a contradiction.

B₂4) $\gamma(h_{\gamma}) = 3\alpha_2(h_2) = \frac{3}{2}\alpha_2(h_1)$. Then $A_{\gamma,1} = 0$, and if $\gamma - \alpha_1$ is a root, we take $\beta = \gamma - \alpha_1$; otherwise $\beta = \gamma$.

B₂5) $3\gamma(h_{\gamma}) = \alpha_2(h_2) = \frac{1}{2}\alpha_1(h_1)$. Then $A_{\gamma,1} = 0$, or $p = 11$ and $A_{\gamma,1} = \pm 2$, or $p = 17$ and $A_{\gamma,1} = \pm 3$. $A_{\gamma,1} = -2$ and -3 are impossible by Lemma 6.3. By the same lemma, $\gamma - \alpha_1$ is a root. When $A_{\gamma,1} = 0$, $\gamma - \alpha_2$ is also a root, a contradiction. If $A_{\gamma,1} = 2$, we can take $\beta = \gamma - 3\alpha_1 - 3\alpha_2$. If $A_{\gamma,1} = 3$, $\gamma - 3\alpha_1$ is a root, and $A_{\gamma-3\alpha_1,\alpha_2} = 5$, a contradiction.

G₂0) As in A₂0) and B₂0), we need only consider $A_{\gamma,1} = 1, 2, 3$. Now $A_{\gamma-2\alpha_1,\alpha_2} = 6$, so $\gamma - 2\alpha_1$ is not a root and $A_{\gamma,1} = 1$. Then $\beta = \gamma - 4\alpha_1 \stackrel{\alpha_2}{=} 6\alpha_2$ is a root, and $\beta - \alpha_1$ is not a root for $1 = 1, 2$.

G₂1) $\gamma(h_{\gamma}) = \alpha_2(h_2) = \frac{1}{3}\alpha_1(h_1)$. Thus $A_{\gamma,1} = -1, 0$ or 1 . By Lemma 6.3, we may assume that $\gamma - \alpha_1$ is a root. Also, $\gamma - 2\alpha_1$ is not a root. It follows that $A_{\gamma,1} = 1$, and we find $\beta = \gamma - 2\alpha_1 - 3\alpha_2$.

G₂2) Since $\gamma(h_{\gamma}) = \frac{2}{3}\alpha_1(h_1)$, we must have $A_{\gamma,1} = 0$. As before, $\beta = \gamma$ is impossible. Thus $\gamma - \alpha_1$, and therefore $\gamma - \alpha_2$, is a root, a contradiction.

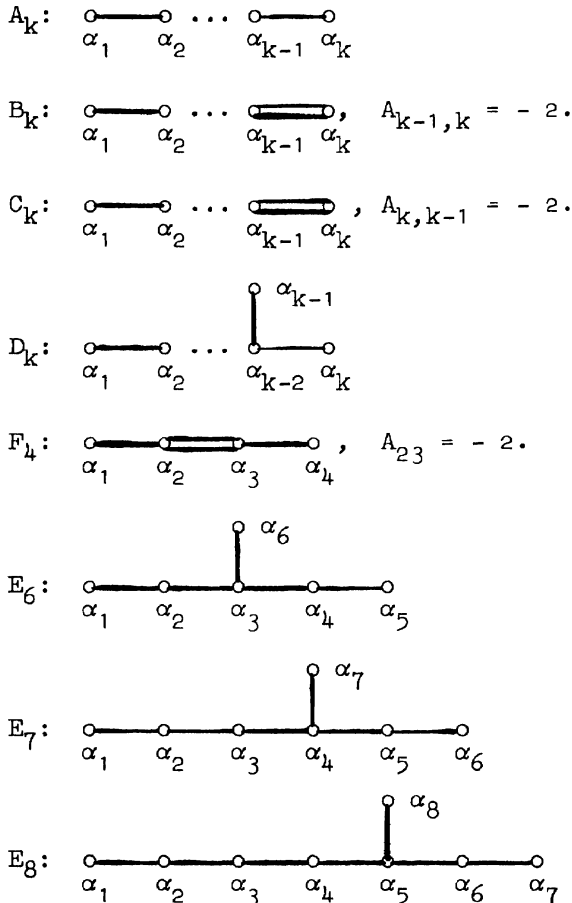
G₂3) $2\gamma(h_{\gamma}) = \alpha_2(h_2) = \frac{1}{3}\alpha_1(h_1)$. Either $A_{\gamma,1} = 0$, or $p = 11$ and $A_{\gamma,1} = \pm 2$, or $p = 17$ and $A_{\gamma,1} = \pm 3$. $A_{\gamma,1} = -2$ or -3 contradicts Lemma 6.3. $A_{\gamma,1} = 2$ or 3 implies that $\gamma - 2\alpha_1$ is a root. But $A_{\gamma-2\alpha_1,\alpha_2} = 5$, a contradiction. If $A_{\gamma,1} = 0$, we may assume $\gamma - \alpha_1$ is a root. But then so is $\gamma - \alpha_2$, a contradiction.

G₂4) $\gamma(h_{\gamma}) = 3\alpha_2(h_2) = \alpha_1(h_1)$, or $A_{\gamma,1} = -1, 0$ or 1 . As before, we may assume that $A_{\gamma,1} = 1$ and that $\gamma - 2\alpha_1$ is not a root. Then we find $\beta = \gamma - \alpha_1$.

G₂5) $3\gamma(h_{\gamma}) = \alpha_2(h_2) = \frac{1}{3}\alpha_1(h_1)$. Either $A_{\gamma,1} = 0$, or $p = 17$ and $A_{\gamma,1} = \pm 2$, or $p = 13$ and $A_{\gamma,1} = \pm 3$. As in G₂3) we must have $A_{\gamma,1} = 0$. But then $\gamma - \alpha_1$ cannot be a root, and we have an i.s.s. which

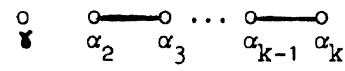
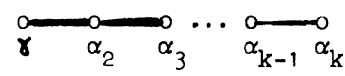
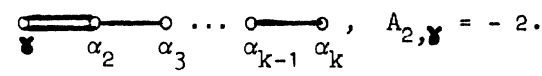
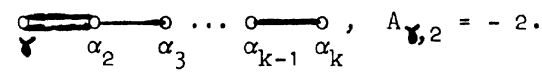
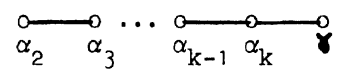
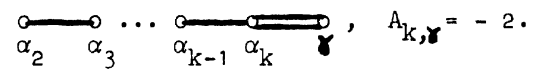
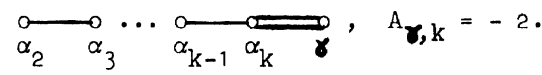
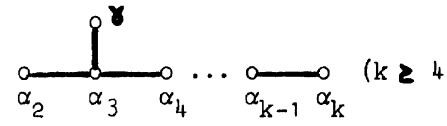
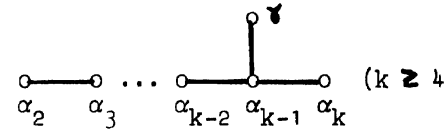
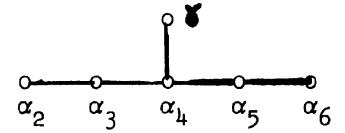
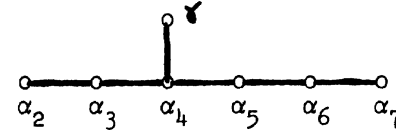
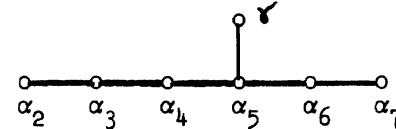
contradicts Lemma 6.3. This completes the proof for $k = 2$.

Now assume we have proved that it is possible to carry out the process of the lemma for all i.s.s. of $(k - 1)$ roots ($k \geq 3$) and let $\alpha_1, \dots, \alpha_k$ be an i.s.s. which we shall label as shown:

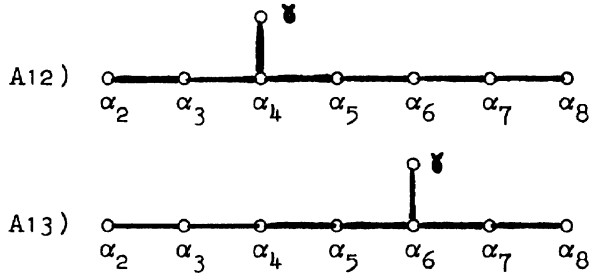


Let α be a root independent of $\alpha_1, \dots, \alpha_k$. Since $\alpha_2, \dots, \alpha_k$ is an i.s.s. of $k - 1$ roots, we can find a string of roots $\alpha - \alpha_{1_1}, \alpha - \alpha_{1_1} - \alpha_{1_2}, \dots, \gamma, 2 \leq i_3 \leq k$, such that $\gamma - \alpha_{1_1}$ is not a root for $2 \leq i \leq k$. Then $\gamma, \alpha_2, \dots, \alpha_k$ form a simple system, which is indecomposable unless $A_{\gamma,1} = 0, 2 \leq i \leq k$.

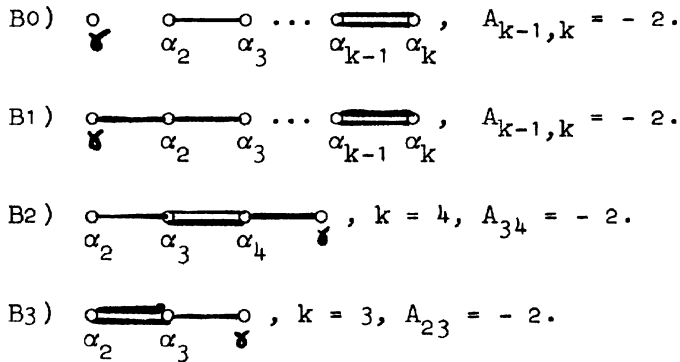
Suppose first that $\alpha_1, \dots, \alpha_k$ is of type A_k . By Th. 6.1, the system $\gamma, \alpha_2, \dots, \alpha_k$ has one of the following diagrams:

- A0) 
- A1) 
- A2)  , $A_{2, \gamma} = -2$.
- A3)  , $A_{\gamma, 2} = -2$.
- A4) 
- A5)  , $A_{k, \gamma} = -2$.
- A6)  , $A_{\gamma, k} = -2$.
- A7)  ($k \geq 4$)
- A8)  ($k \geq 4$)
- A9) 
- A10) 
- A11) 

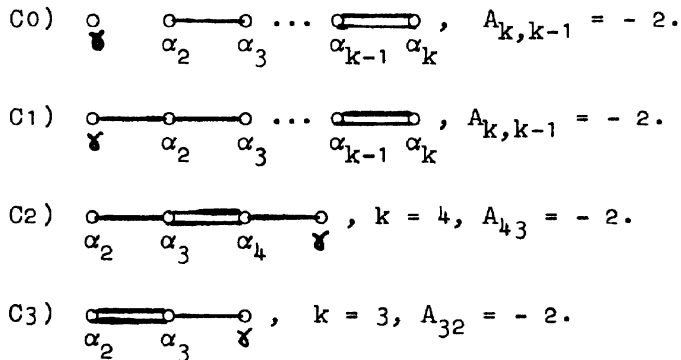
*



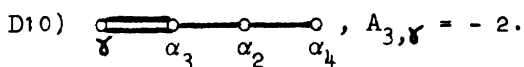
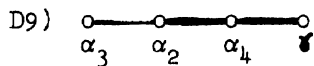
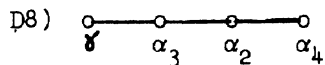
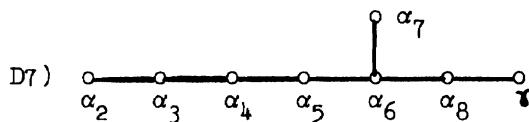
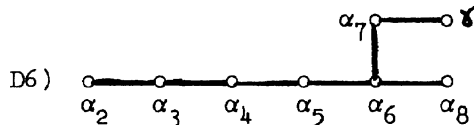
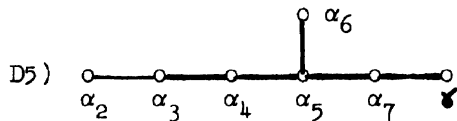
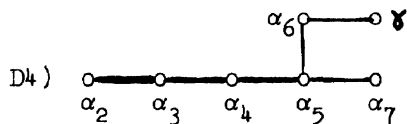
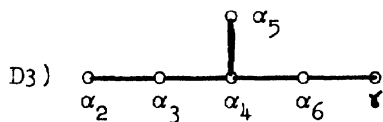
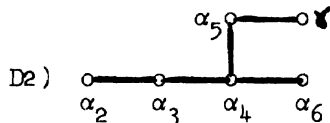
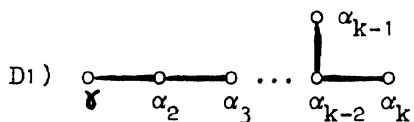
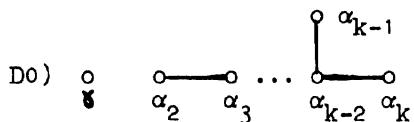
If $\alpha_1, \dots, \alpha_k$ is of type B_k , then $\gamma, \alpha_2, \dots, \alpha_k$ must have one of the following diagrams:



If $\alpha_1, \dots, \alpha_k$ is of type C_k , $\gamma, \alpha_2, \dots, \alpha_k$ has one of the following diagrams:



If $\alpha_1, \dots, \alpha_k$ is of type D_k ($k \geq 4$), then $\gamma, \alpha_2, \dots, \alpha_k$ is one of the following:



*

$$D11) \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_2 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array} \text{---} \begin{array}{c} \circ \\ \gamma \end{array}, A_{4,\gamma} = -2.$$

$$D12) \begin{array}{c} \circ \\ \gamma \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_2 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array}, A_{\gamma,3} = -2.$$

$$D13) \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_2 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array} \text{---} \begin{array}{c} \circ \\ \gamma \end{array}, A_{\gamma,4} = -2.$$

$$D14) \begin{array}{c} \alpha_4 \\ \circ \end{array} \text{---} \begin{array}{c} \circ \\ \gamma \end{array} \\ \circ \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_5 \end{array} \\ \alpha_2 \end{array}$$

$$D15) \begin{array}{c} \circ \\ \alpha_4 \end{array} \\ \circ \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_5 \end{array} \text{---} \begin{array}{c} \circ \\ \gamma \end{array}$$

If $\alpha_1, \dots, \alpha_k$ is of type F, then $\gamma, \alpha_2, \alpha_3, \alpha_4$ is one of the following:

$$F0) \begin{array}{c} \circ \\ \gamma \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_2 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array}, A_{23} = -2.$$

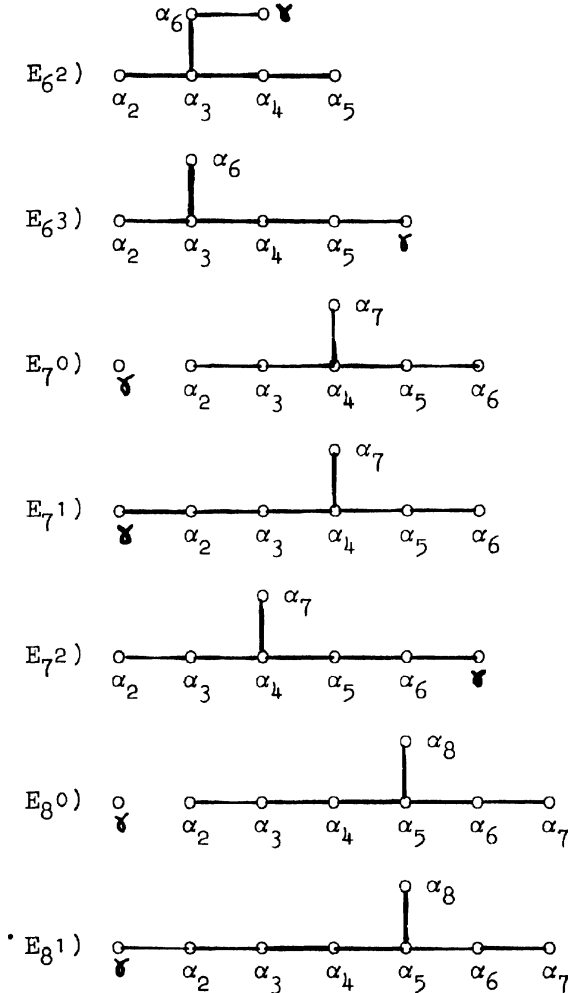
$$F1) \begin{array}{c} \circ \\ \alpha_2 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array} \text{---} \begin{array}{c} \circ \\ \gamma \end{array}, A_{23} = -2.$$

$$F2) \begin{array}{c} \circ \\ \gamma \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_2 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array}, A_{23} = -2.$$

If $\alpha_1, \dots, \alpha_k$ is of type E, then $\gamma, \alpha_2, \dots, \alpha_k$ is one of the following:

$$E_6 0) \begin{array}{c} \circ \\ \alpha_6 \end{array} \\ \circ \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_5 \end{array} \\ \gamma \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_2 \end{array}$$

$$E_6 1) \begin{array}{c} \circ \\ \alpha_6 \end{array} \\ \circ \text{---} \begin{array}{c} \circ \\ \alpha_3 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_4 \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_5 \end{array} \\ \gamma \end{array} \text{---} \begin{array}{c} \circ \\ \alpha_2 \end{array}$$



In each case, we demonstrate a root β obtained from γ through a string of roots $\gamma - \alpha_{i_1}, \gamma - \alpha_{i_1} - \alpha_{i_2}, \dots, \beta, 1 \leq i_s \leq k$, such that $\beta, \alpha_1, \alpha_2, \dots, \alpha_k$ form a simple system.

A0) In case $A_{\gamma,1} = -2$, we have $\beta = \gamma$. If $A_{\gamma,1} = -1$ or 0 , and $\gamma - \alpha_1$ is a root, $\gamma - \alpha_1 - \alpha_2$ is also a root, as is $\gamma - \alpha_2$, a contradiction. Thus we have $\beta = \gamma$. There remain the cases $A_{\gamma,1} = 1, 2$ or 3 . In each such case, $\gamma - A_{\gamma,1}\alpha_1$ is a root, but $\gamma - (A_{\gamma,1} + 1)\alpha_1$ is not. This is clear if $A_{\gamma,1} = 2$ or 3 ; when $A_{\gamma,1} = 1$, $\gamma - 2\alpha_1$ a root implies that $\gamma - 2\alpha_1 - \alpha_2$ is a root, as is $\gamma - \alpha_2$, a contradiction. A string of the prescribed form can be formed using Th. 5.6,

leading to the root $\gamma - A_{\gamma,1}(\alpha_1 + \dots + \alpha_k)$.

Now suppose $\gamma - (A_{\gamma,1} + 1)\alpha_1 - A_{\gamma,1}(\alpha_2 + \dots + \alpha_k)$ is a root. Then so are $\gamma - (A_{\gamma,1} + 1)\alpha_1 - A_{\gamma,1}(\alpha_2 + \dots + \alpha_{k-1})$, ..., $\gamma - (A_{\gamma,1} + 1)\alpha_1 - A_{\gamma,1}\alpha_2$, $\gamma - (A_{\gamma,1} - 1)\alpha_1 - A_{\gamma,1}\alpha_2$, $\gamma - (A_{\gamma,1} - 1)\alpha_1 + \alpha_2$, $\gamma + \alpha_2$ and $\gamma - \alpha_2$, a contradiction. By similar reasoning, we see that we can take $\beta = \gamma - A_{\gamma,1}(\alpha_1 + \dots + \alpha_k)$ (and thus that $A_{\gamma,1} \neq 3$).

A1), A2) As in A₂1), A₂3), $A_{\gamma,1} = -1, 0$ or 1 . If $A_{\gamma,1} = -1$ or 0 , we can take $\beta = \gamma$ unless $\gamma - \alpha_1$ is a root. In the latter case, if $\gamma - \alpha_1 - \alpha_j$ is a root, $j > 1$, so is $\gamma - \alpha_j$, and we can take $\beta = \gamma - \alpha_1$. Now let $A_{\gamma,1} = 1$. If $\gamma - 2\alpha_1$ is a root, so are $\gamma - 2\alpha_1 - \alpha_2$ and $\gamma - \alpha_2$, a contradiction. If $\gamma - \alpha_1 - \alpha_2$ is a root, so are $\gamma - \alpha_1 - \alpha_2 - \alpha_3$, $\gamma - \alpha_1 - \alpha_3$, $\gamma - \alpha_3$, a contradiction. It is clearly impossible that $\gamma - \alpha_1 - \alpha_j$ be a root for $j > 2$. Thus we take $\beta = \gamma - \alpha_1$.

A3) Here $A_{\gamma,1} = -2, 0$ or 2 . In case $A_{\gamma,1} = -2$, we take $\beta = \gamma$. In case $A_{\gamma,1} = 0$, we take $\beta = \gamma$ unless $\gamma - \alpha_1$ is a root, in which case we have $\beta = \gamma - \alpha_1$. Next let $A_{\gamma,1} = 2$. As in A1), A2), we see that we can take $\beta = \gamma - 2\alpha_1$.

A4), A5) Here $A_{\gamma,1} = -1, 0$ or 1 . If $A_{\gamma,1} = -1$ or 0 , the assumption that $\gamma - \alpha_1$ is a root leads to the conclusion that $\gamma - \alpha_2$ is a root, as in A0). Thus $\beta = \gamma$ in these cases. When $A_{\gamma,1} = 1$, $\gamma - 2\alpha_1$ cannot be a root, and we can form a string to arrive at $\gamma - \alpha_1 - \dots - \alpha_{k-1}$, which can be taken as our β unless $\gamma - \alpha_1 - \dots - \alpha_{k-1} - \alpha_k$ is a root. In the latter case, we take $\beta = \gamma - \alpha_1 - \dots - \alpha_{k-1} - \alpha_k$.

A6) Here $A_{\gamma,1} = -2, 0$ or 2 . $A_{\gamma,1} = -2$ is impossible. If $A_{\gamma,1} = 0$, we have $\beta = \gamma$ as in A4), A5). If $A_{\gamma,1} = 2$, we form a string of roots of the desired type to arrive at $\delta = \gamma - 2\alpha_1 - \dots - 2\alpha_{k-1}$. It is readily checked that $\delta - \alpha_j$ is not a root for $1 \leq j \leq k-1$. If $\delta - \alpha_k$ is not a root, then $\delta, \alpha_1, \dots, \alpha_k$ form an impossible i.s.s. Let $\beta = \delta - \alpha_k = \gamma - 2\alpha_1 - \dots - 2\alpha_{k-1} - \alpha_k$. Then $\beta, \alpha_1, \dots, \alpha_k$ form an i.s.s. of a type impossible by Lemma 6.4.

A7) Here $A_{\gamma,1} = -1, 0$ or 1 , and we can again take $\beta = \gamma$ unless $A_{\gamma,1} = 1$. In this case, $\gamma - \alpha_1 - \alpha_2$ is a root δ ; either we can take $\beta = \delta$ or $\delta - \alpha_3$ is a root. If $\delta - \alpha_3$ is a root, so are $\delta - \alpha_3 - \alpha_4$, $\delta - \alpha_4 = \gamma - \alpha_1 - \alpha_2 - \alpha_4$, $\gamma - \alpha_1 - \alpha_4$ and $\gamma - \alpha_4$, a contradiction. Thus we take $\beta = \delta$.

A8) Again $A_{\gamma,1} = -1, 0$ or 1 , and $\beta = \gamma$ unless $A_{\gamma,1} = 1$. When $A_{\gamma,1} = 1$, we form a string leading to $\gamma - \alpha_1 - \alpha_2 - \dots - \alpha_{k-2} = \delta$. $\delta - \alpha_j$ is not a root for $j \neq k-1$. If $\delta - \alpha_{k-1}$ is a root, so are $\delta - \alpha_{k-1} - \alpha_k$ and therefore $\delta - \alpha_k$, in contradiction to the preceding remark. Thus we take $\beta = \delta$.

A9) $A_{\gamma,1} = -1, 0$ or 1 ; $A_{\gamma,1} = -1$ is impossible, and we have $\beta = \gamma$ if $A_{\gamma,1} = 0$. When $A_{\gamma,1} = 1$, we find $\beta = \gamma - \alpha_1 - \alpha_2 - \alpha_3$.

A10) As in A9), either $A_{\gamma,1} = 0$, $\beta = \gamma$ (which is impossible), or $A_{\gamma,1} = 1$, $\beta = \gamma - \alpha_1 - \alpha_2 - \alpha_3$.

A11) Here either $A_{\gamma,1} = 0$, $\beta = \gamma$, or $A_{\gamma,1} = 1$, $\beta = \gamma - \alpha_1 - \dots - \alpha_4$, and the latter is impossible.

A12) Here either $A_{\gamma,1} = 0$, $\beta = \gamma$, or $A_{\gamma,1} = 1$, $\beta = \gamma - \alpha_1 - \alpha_2 - \alpha_3$; both are impossible.

A13) Either $A_{\gamma,1} = 0$, $\beta = \gamma$, or $A_{\gamma,1} = 1$, $\beta = \gamma - \alpha_1 - \dots - \alpha_5$; both are impossible.

B0) $A_{\gamma,1} = -2, -3$ are impossible. If $A_{\gamma,1} = -1$ or 0 , we have $\beta = \gamma$ as in A0). If $A_{\gamma,1}$ is among $1, 2, 3$, the roots include $\gamma - A_{\gamma,1}(\alpha_1 + \dots + \alpha_{k-1}) = \delta$, and $A_{\delta,k} = 2A_{\gamma,1}$. This is impossible unless $A_{\gamma,1} = 1$. Then we have a string leading to $\gamma - \alpha_1 - \dots - \alpha_{k-1}$, $\gamma - \alpha_1 - \dots - \alpha_{k-1} - 2\alpha_k$, $\gamma - \alpha_1 - \dots - \alpha_{k-2} - 2\alpha_{k-1} - 2\alpha_k$, ..., $\gamma - 2\alpha_1 - \dots - 2\alpha_k = \beta$, and $\beta - \alpha_1$ is not a root for $1 \leq i \leq k$.

B1) Here $A_{\gamma,1} = -1, 0$ or 1 . If $A_{\gamma,1} = -1$ or 0 and $\gamma - \alpha_1$ is a root, we can take $\beta = \gamma - \alpha_1$. This gives an impossible system in either case. Hence either $\beta = \gamma$ or $A_{\gamma,1} = 1$. In the latter case, $\gamma - \alpha_1$ is a root, and $\gamma - \alpha_1 - \alpha_j$ is not a root for $j \neq 2$. If $\gamma - \alpha_1 - \alpha_2$ is a root, so are $\gamma - \alpha_1 - \alpha_2 - \alpha_3$ and $\gamma - \alpha_1 - \alpha_3$, a contradiction. Thus we have $\beta = \gamma - \alpha_1$ in this case.

B2) Again $A_{\gamma,1} = -1, 0$ or 1 , and $\gamma - \alpha_1$ is not a root if $A_{\gamma,1} \neq 1$. But then $\gamma, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ form an impossible i.s.s., so we can assume $A_{\gamma,1} = 1$. Then we form a string of the desired type leading to $\gamma - \alpha_1 - \alpha_2 - \alpha_3 - \alpha_4 = \beta$, and are done.

B3) Again $A_{\gamma,1} = -1, 0$ or 1 . If $A_{\gamma,1} = -1$ or 0 , we have $\beta = \gamma$. If $A_{\gamma,1} = 1$, the roots include $\gamma - \alpha_1 - \alpha_2 - \alpha_3$. We can take $\beta = \gamma - \alpha_1 - \alpha_2 - \alpha_3$ unless $\gamma - \alpha_1 - \alpha_2 - 2\alpha_3$ is a root; but then so are $\gamma - \alpha_1 - 2\alpha_2 - 2\alpha_3$, $\gamma - \alpha_1 - 2\alpha_2 - \alpha_3$, $\gamma - \alpha_1 - \alpha_3$, $\gamma - \alpha_3$, a contradiction.

C0) As in B0), we eliminate $A_{\gamma,1} = -3, -2, -1, 0$ (in the latter two cases by taking $\beta = \gamma$). When $A_{\gamma,1} = 1, 2, 3$, we find a string of the desired type leading to $\beta = \gamma - A_{\gamma,1}(2\alpha_1 + \dots + 2\alpha_{k-1} + \alpha_k)$, and $\beta - \alpha_j$ is not a root for any j . This is only possible, by Lemma 6.4, when $A_{\gamma,1} = 1$.

C1) $A_{\gamma,1} = -1, 0$ or 1 . As in B1), $\gamma - \alpha_1$ is not a root unless $A_{\gamma,1} = 1$, and we have $\beta = \gamma$. $A_{\gamma,1} \neq 1$ is therefore impossible by Lemma 6.4. If $A_{\gamma,1} = 1$ and $k > 3$, we have $\beta = \gamma - \alpha_1$ as a suitable root. When $k = 3$ and $\gamma - \alpha_1 - \alpha_2$ is a root, so is $\gamma - \alpha_1 - \alpha_2 - \alpha_3$, and we can take $\beta = \gamma - \alpha_1 - \alpha_2 - \alpha_3$ in this case.

C2) $A_{\gamma,1} = -2, 0$ or 2 . $A_{\gamma,1} = -2$ is impossible. If $A_{\gamma,1} = 0$, $\gamma - \alpha_1$ cannot be a root, and we again have an impossible system. Thus $A_{\gamma,1} = 2$, and we can form a string of the desired type leading to $\beta = \gamma - 2\alpha_1 - 2\alpha_2 - 2\alpha_3 - \alpha_4$, and $\beta, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ form an i.s.s. impossible by Th. 6.1. Therefore C2) is eliminated.

C3) $A_{\gamma,1} = -2, 0$ or 2 , and $A_{\gamma,1} = -2$ is impossible. If $A_{\gamma,1} = 0$, we can take $\beta = \gamma$. If $A_{\gamma,1} = 2$, we can form a string to arrive at $\gamma - 2\alpha_1 - 2\alpha_2 - \alpha_3 = \delta$. If $\delta - \alpha_1$ is not a root, we take $\beta = \delta$. Otherwise, we can take $\beta = \delta - \alpha_1 - \alpha_2 = \gamma - 3\alpha_1 - 3\alpha_2 - \alpha_3$.

D0) As in B0), C0), $A_{\gamma,1} = -2$ or -3 is impossible. If $A_{\gamma,1} = -1$ or 0 , we have $\beta = \gamma$. Otherwise, $A_{\gamma,1} = 1, 2, 3$, and we can form a string of roots leading to $\gamma - A_{\gamma,1}(2\alpha_1 + \dots + 2\alpha_{k-2} + \alpha_{k-1} + \alpha_k)$, and take this root as our β . By Lemma 6.4, this implies that $A_{\gamma,1} = 1$.

D1) $A_{\gamma,1} = -1, 0$ or 1 . If $A_{\gamma,1} = -1$ or 0 and $\gamma - \alpha_1$ is a root, $\gamma - \alpha_1 - \alpha_2$ must be a root, by Lemma 6.4. Then $\gamma - \alpha_1 - \alpha_2 - \alpha_3$, $\gamma - \alpha_1 - \alpha_3$ are roots, a contradiction. Thus $\beta = \gamma$ if $A_{\gamma,1} = -1$ or 0 . Now let $A_{\gamma,1} = 1$. Then take $\beta = \gamma - \alpha_1$. If $\gamma - \alpha_1 - \alpha_2$ is a root, so are $\gamma - \alpha_1 - \alpha_2 - \alpha_3$, $\gamma - \alpha_1 - \alpha_3$, $\gamma - \alpha_3$, a contradiction. Clearly, $\beta - \alpha_j$ is not a root for $j \neq 2$.

D2), D3) By symmetry, we need only treat D2). $A_{\gamma,1} = -1, 0$ or 1 . Now $A_{\gamma,1} = -1$ is impossible, and when $A_{\gamma,1} = 0$ we have $\beta = \gamma$. Next let $A_{\gamma,1} = 1$. Then we have a string leading to $\beta = \gamma - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_6)$, and $\beta - \alpha_j$ is not a root for any j .

D4), D5) We treat D4). $A_{\gamma,1} = -1, 0$ or 1 . $A_{\gamma,1} = -1$ is again impossible, and $\beta = \gamma$ when $A_{\gamma,1} = 0$. When $A_{\gamma,1} = 1$, we find $\beta = \gamma - \alpha_1 - \alpha_2 - \alpha_3 - \alpha_4 - \alpha_5 - \alpha_7$.

D6), D7) Here only $A_{\mathfrak{Y},1} = 1$ is possible, giving $\mathfrak{B} = \mathfrak{Y} - \alpha_1 - \dots - \alpha_6 - \alpha_8$ in D6). But this system also violates Lemma 6.4.

D8)-D11) $A_{\mathfrak{Y},1} = -1, 0$ or 1 . If $A_{\mathfrak{Y},1} = -1$ or 0 , we see that $\mathfrak{Y} - \alpha_1$ cannot be a root. Now let $A_{\mathfrak{Y},1} = 1$. In D8) and D10), we obtain $\mathfrak{B} = \mathfrak{Y} - \alpha_1 - \alpha_2 - \alpha_4$. D9) and D11) are symmetric with these cases.

D12), D13) $A_{\mathfrak{Y},1} = -2, 0$ or 2 . The first two are impossible. In D12), we arrive at $\mathfrak{B} = \mathfrak{Y} - 2\alpha_1 - 2\alpha_2 - 2\alpha_4$, which is also impossible. D13) is treated symmetrically.

D14), D15) $A_{\mathfrak{Y},1} = -1, 0$ or 1 . Of the first two, only 0 is possible, and there $\mathfrak{B} = \mathfrak{Y}$. For $A_{\mathfrak{Y},1} = 1$, we obtain $\mathfrak{B} = \mathfrak{Y} - \alpha_1 - \alpha_2 - \alpha_3 - \alpha_5$ in D14) and $\mathfrak{B} = \mathfrak{Y} - \alpha_1 - \alpha_2 - \alpha_3 - \alpha_4$ in D15).

F0) $A_{\mathfrak{Y},1} = -2, -3$ are impossible. If $A_{\mathfrak{Y},1} = -1$ or 0 , we can take $\mathfrak{B} = \mathfrak{Y}$; by Lemma 6.4, this eliminates $A_{\mathfrak{Y},1} = -1$. If $A_{\mathfrak{Y},1} = 2$ or 3 , $\mathfrak{Y} - 2\alpha_1$ and $\mathfrak{Y} - 2\alpha_1 - 2\alpha_2 = \delta$ are roots, and $A_{\delta,3} = 4$, a contradiction. Thus $A_{\mathfrak{Y},1} = 1$ remains, and here we find $\mathfrak{B} = \mathfrak{Y} - 4\alpha_1 - 6\alpha_2 - 8\alpha_3 - 4\alpha_4$.

F1) $A_{\mathfrak{Y},1} = -1, 0$ or 1 , the former two being impossible. When $A_{\mathfrak{Y},1} = 1$, we arrive at $\mathfrak{B} = \mathfrak{Y} - 2\alpha_1 - 3\alpha_2 - 4\alpha_3 - 2\alpha_4$. But this also gives an impossible i.s.s.

F2) $A_{\mathfrak{Y},1} = -1, 0$ or 1 . If $A_{\mathfrak{Y},1} = -1$ or 0 , $\mathfrak{Y} - \alpha_1$ cannot be a root. But $\mathfrak{B} = \mathfrak{Y}$ is likewise impossible. Therefore $A_{\mathfrak{Y},1} = 1$, and we can take $\mathfrak{B} = \mathfrak{Y} - \alpha_1$. However, this i.s.s. is again impossible.

E₆0) $A_{\mathfrak{Y},1} = -2, -3$ are impossible. If $A_{\mathfrak{Y},1} = -1$ or 0 , take $\mathfrak{B} = \mathfrak{Y}$. If $A_{\mathfrak{Y},1} = 1, 2, 3$, we arrive at $\mathfrak{B} = \mathfrak{Y} - A_{\mathfrak{Y},1}(2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 3\alpha_4 + 2\alpha_5 + 2\alpha_6)$, and this implies that $A_{\mathfrak{Y},1} = 1$.

E₆1) $A_{\mathfrak{Y},1} = -1, 0$ or 1 . $A_{\mathfrak{Y},1} = -1$ is impossible. In case $A_{\mathfrak{Y},1} = 0$, we have $\mathfrak{B} = \mathfrak{Y} - \alpha_1$, since $\mathfrak{B} = \mathfrak{Y}$ gives an impossible i.s.s. But $\mathfrak{B} = \mathfrak{Y} - \alpha_1$ also gives an impossible i.s.s. Thus only $A_{\mathfrak{Y},1} = 1$ is possible, and in this case we have $\mathfrak{B} = \mathfrak{Y} - \alpha_1$.

E₆2) Only $A_{\mathfrak{Y},1} = 0$ is possible, as in E₆1). Then we arrive at $\mathfrak{B} = \mathfrak{Y} - \alpha_1 - \alpha_2 - \alpha_3 - \alpha_4 - \alpha_5$.

E₆3) $A_{\mathfrak{Y},1} = 0$ is possible, with $\mathfrak{B} = \mathfrak{Y}$. If this is not the case, then $A_{\mathfrak{Y},1} = 1$, and we can take $\mathfrak{B} = \mathfrak{Y} - 2\alpha_1 - 2\alpha_2 - 2\alpha_3 - \alpha_4 - \alpha_6$.

E₇0) Either $A_{\mathfrak{Y},1} = -1$ or 0 and $\mathfrak{B} = \mathfrak{Y}$, or $A_{\mathfrak{Y},1} = 1, 2$ or 3 , and we obtain $\mathfrak{B} = \mathfrak{Y} - A_{\mathfrak{Y},1}(3\alpha_1 + 4\alpha_2 + 5\alpha_3 + 6\alpha_4 + 4\alpha_5 + 2\alpha_6 + 3\alpha_7)$. This is only possible if $A_{\mathfrak{Y},1} = 1$, by Lemma 6.4.

E₇1) As in E₆1), $A_{\gamma,1} = -1$ or 0 is impossible. If $A_{\gamma,1} = 1$, we have $\beta = \gamma - \alpha_1$.

E₇2) Here $A_{\gamma,1} = -1$ or 0 is impossible. If $A_{\gamma,1} = 1$, we arrive at $\beta = \gamma - 2\alpha_1 - 2\alpha_2 - 2\alpha_3 - 2\alpha_4 - \alpha_5 - \alpha_7$.

E₈0) The only possible case is $A_{\gamma,1} = 0$, $\beta = \gamma$. For $A_{\gamma,1} = -1, -2, -3$ are eliminated as above, and otherwise we find $\beta = \gamma - A_{\gamma,1}(4\alpha_1 + 6\alpha_2 + 8\alpha_3 + 10\alpha_4 + 12\alpha_5 + 8\alpha_6 + 4\alpha_7 + 6\alpha_8)$. But this gives an impossible i.s.s. for $A_{\gamma,1} = 1, 2, 3$.

E₈1) As in E₇1), the only tentative situation possible is $A_{\gamma,1} = 1$, $\beta = \gamma - \alpha_1$. But this contradicts Lemma 6.4.

Thus the conclusions of the lemma hold by induction when $\alpha_1, \dots, \alpha_k$ is indecomposable. We observe also that in case $\gamma, \gamma - \alpha_1, \gamma - \alpha_1 - \alpha_2, \dots, \gamma - \alpha_1 - \dots - \alpha_{1_s} = \beta$ is the string of roots by which β was obtained from γ , we can return from β to γ in the sense that the value of $A_{\beta,1_s}$ assures us that $\beta + \alpha_{1_s}$ is a root, either that of $A_{\beta+\alpha_{1_s},1_{s-1}}$ or that of $A_{\beta,1_s}$ (the latter used only if $\alpha_{1_{s-1}} = \alpha_{1_s}$) assures us that $\beta + \alpha_{1_s} + \alpha_{1_{s-1}}$ is a root, until finally we arrive at γ by such reasoning. This observation is verified by examining the process by which β is obtained from γ in each of the above cases. It follows that if δ is a root such that $\delta(h_{1_i}) = 0$, $1 \leq i \leq k$, and if $\beta + \delta$ is a root, then $\gamma + \delta$, and consequently $\alpha + \delta$, is also a root.

Now assume that the simple system $\alpha_1, \dots, \alpha_k$ decomposes into j "pairwise orthogonal" indecomposable components. If $j = 1$, we have already proved the lemma. Suppose that we have proved the lemma for systems with $(j - 1)$ indecomposable components, and let $\alpha_1, \dots, \alpha_m$ be an indecomposable component of $\alpha_1, \dots, \alpha_k$. Let $\alpha - \alpha_{1_1}, \alpha - \alpha_{1_1} - \alpha_{1_2}, \dots, \alpha - \alpha_{1_1} - \dots - \alpha_{1_s} = \gamma$ be a string of roots, $m + 1 \leq i_q \leq k$, such that $\gamma, \alpha_{m+1}, \dots, \alpha_k$ form a simple system. Since $\alpha_1, \dots, \alpha_m$ is indecomposable, we can form a string $\gamma, \gamma - \alpha_{j_1}, \gamma - \alpha_{j_1} - \alpha_{j_2}, \dots, \gamma - \alpha_{j_1} - \dots - \alpha_{j_r} = \beta$ of roots according to the procedures of the first part of this proof, $1 \leq j_1 \leq m$, such that $\beta, \alpha_1, \dots, \alpha_m$ form a simple system.

Now suppose that $\beta - \alpha_t$ is a root, $t > m$. Since $\alpha_t(h_1) = 0$ for $1 \leq i \leq m$, we can apply the observation above to show that $\gamma - \alpha_t$ is a root, in contradiction to the construction of γ . Therefore, $\beta, \alpha_1, \dots, \alpha_k$ is a simple system, and Lemma 7.1 is proved. An immediate consequence is the following theorem:

THEOREM 7.1. Let L be a restricted Lie algebra over F having a restricted representation with non-degenerate trace form. If $[LL] = L$, then L possesses a fundamental simple system of roots with respect to any given Cartan subalgebra H .

VIII. SYSTEMS OF TYPE A

THEOREM 8.1. Let $\alpha_1, \dots, \alpha_r$ be an i.s.s. of type A_r , labeled as in the proof of Lemma 7.1. Suppose there is no i.s.s. β_1, \dots, β_r of r roots, each linearly dependent on $\alpha_1, \dots, \alpha_r$, of type other than A_r . Suppose also that the matrix $(\alpha_1(h_j))$, $1 \leq i, j \leq r$, is non-singular. Then $p \nmid (r+1)$, and every root expressible as a linear combination of $\alpha_1, \dots, \alpha_r$ is among the following and their negatives, where we use the conventions of §6 in writing $(\lambda_1 \lambda_2 \dots \lambda_r)$ for $\lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \dots + \lambda_r \alpha_r$:

$$\begin{aligned} & (1 \ 0 \ \dots \ 0), (0 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1); \\ & (1 \ 1 \ 0 \ \dots \ 0), (0 \ 1 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1 \ 1); \\ & (1 \ 1 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1 \ 1 \ 1); \\ & \quad \vdots \\ & (1 \ 1 \ \dots \ 1 \ 0), (0 \ 1 \ 1 \ \dots \ 1); \\ & (1 \ 1 \ \dots \ 1); \end{aligned}$$

except possibly when $p \mid (r+2)$, when the following and their negatives may be roots:

$$\begin{aligned} \alpha_0 = & (1 \ 2 \ 3 \ \dots \ r), (1 \ 2 \ \dots \ r-1 \ r+1), (1 \ 2 \ \dots \ r-2 \ r \ r+1), \\ & \dots, (1 \ 3 \ 4 \ \dots \ r+1), (2 \ 3 \ \dots \ r \ r+1). \end{aligned}$$

In the former case there are $r(r+1)$ such roots: in

the latter, $(r + 1)(r + 2)$.

PROOF. Let $\alpha \neq 0$ be a root, $\alpha = (\rho_1 \dots \rho_r)$. If $\rho_i = 0$, let ρ_{k+1} be the first non-zero coefficient. Then $A_{\alpha, k} = -\rho_{k+1} \neq 0$. Hence either $\alpha + \alpha_k$ or $\alpha - \alpha_k$ is a root. By replacing α by $-\alpha$ if necessary, we may assume that $\alpha - \alpha_k$ is a root. Now $A_{\alpha - \alpha_k, k-1} = 1$, so $\alpha - \alpha_k - \alpha_{k-1}$ is a root. We repeat to arrive at a root $\beta = \alpha - \alpha_k - \alpha_{k-1} - \dots - \alpha_1$ such that the coefficient of α_1 in β is -1 . If $\rho_1 \neq 0$, we take $\beta = \alpha$. Thus in any case β is linearly independent of $\alpha_2, \dots, \alpha_r$. By Lemma 7.1, we can form a string of roots $\beta - \alpha_{i_1}$, $\beta - \alpha_{i_1} - \alpha_{i_2}$, \dots , $\beta - \alpha_{i_1} - \dots - \alpha_{i_s} = \gamma$, $2 \leq i_j \leq r$, such that $\gamma, \alpha_2, \dots, \alpha_r$ form a simple system. If this system is indecomposable, it must be of type A_r by assumption, and therefore is one of the following:

$$A1) \quad \begin{array}{ccccccc} \circ & \text{---} & \circ & \text{---} & \circ & \dots & \circ & \text{---} & \circ \\ \gamma & & \alpha_2 & & \alpha_3 & & \alpha_{r-1} & & \alpha_r \end{array}$$

$$A2) \quad \begin{array}{ccccccc} \circ & \text{---} & \circ & \dots & \circ & \text{---} & \circ & \text{---} & \circ \\ \alpha_2 & & \alpha_3 & & \alpha_{r-1} & & \alpha_r & & \gamma \end{array}$$

The only other possibility is the decomposable system

$$A0) \quad \begin{array}{ccccccc} \circ & & \circ & \text{---} & \circ & \dots & \circ & \text{---} & \circ \\ \gamma & & \alpha_2 & & \alpha_3 & & \alpha_{r-1} & & \alpha_r \end{array}$$

Now if $p \mid (r + 1)$, let $h_0 = h_1 + 2h_2 + \dots + rh_r$. Then $h_0 \neq 0$, but $\alpha_1(h_0) = 0$, $1 \leq i \leq r$. The matrix $(\alpha_1(h_j))$ is singular in this case, contrary to assumption. Thus we see that $p \nmid (r + 1)$. Let $\gamma = (\lambda_1 \dots \lambda_r)$, $\lambda_1 \neq 0$. Since $-\alpha_1 - \alpha_2$ is a root, $\gamma \neq -\alpha_1$. If $\gamma \neq \alpha_1$, the pair $(A_{\gamma, 1}, A_{1, \gamma})$ must be one of the following, as in the proof of Lemma 7.1:

$$A1) \quad (A_{\gamma, 1}, A_{1, \gamma}) = (-1, -1), (0, 0) \text{ or } (1, 1).$$

$$A2) \quad (A_{\gamma, 1}, A_{1, \gamma}) = (-1, -1), (0, 0) \text{ or } (1, 1).$$

$$A0) \quad (A_{\gamma, 1}, A_{1, \gamma}) = (-1, -1), (0, 0), (1, 1), (1, 2), (2, 1), \\ (-1, -2), (-2, -1), (1, 3), (3, 1), \\ (-1, -3), (-3, -1).$$

$$A1) \quad A_{\gamma, 1} = 2\lambda_1 - \lambda_2$$

$$\begin{aligned} A_{\mathfrak{Y},2} &= -1 = -\lambda_1 + 2\lambda_2 - \lambda_3 \\ A_{\mathfrak{Y},3} &= 0 = -\lambda_2 + 2\lambda_3 - \lambda_4 \\ &\vdots \\ A_{\mathfrak{Y},r} &= 0 = -\lambda_{r-1} + 2\lambda_r. \end{aligned}$$

Hence $\lambda_{r-1} = 2\lambda_r$, $\lambda_{r-2} = 3\lambda_r$, ..., $\lambda_2 = (r-1)\lambda_r$, $\lambda_1 = r\lambda_r + 1$, and $A_{\mathfrak{Y},1} = (r+1)\lambda_r + 2$. Therefore $\lambda_r = \frac{1}{r+1}(A_{\mathfrak{Y},1} - 2)$. $A_{\mathfrak{Y},1} = 1$: $\lambda_r = \frac{-1}{r+1}$, $\lambda_{r-1} = \frac{-2}{r+1}$, ..., $\lambda_2 = -\frac{r-1}{r+1}$, $\lambda_1 = \frac{1}{r+1}$. Now $A_{1,\mathfrak{Y}} = 1$, $2 = A_{\mathfrak{Y},\mathfrak{Y}} = \sum \lambda_1 A_{1,\mathfrak{Y}} = \lambda_1 - \lambda_2 = \frac{r}{r+1}$. Therefore $r \equiv -2 \pmod{p}$, and $\mathfrak{Y} = - (1 \ 3 \ 4 \ \dots \ r \ r+1)$.

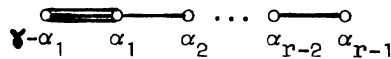
$$A_{\mathfrak{Y},1} = 0: \lambda_r = \frac{-2}{r+1}, \lambda_{r-1} = \frac{-4}{r+1}, \dots, \lambda_2 = -2\frac{r-1}{r+1}, \lambda_1 = -\frac{r-1}{r+1}.$$

As before, $2 = A_{\mathfrak{Y},\mathfrak{Y}} = -\lambda_2 = 2\frac{r-1}{r+1}$, $r-1 = r+1$, $2 = 0$, a contradiction.

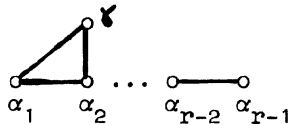
$$A_{\mathfrak{Y},1} = -1: \lambda_r = \frac{-3}{r+1}, \dots, \lambda_2 = -3\frac{r-1}{r+1}, \lambda_1 = \frac{-2r+1}{r+1}.$$

$2 = -\lambda_1 - \lambda_2 = \frac{5r-4}{r+1}$; $3r = 6$, or $p \mid (r-2)$. If $r = 2$, we have

$\mathfrak{Y} = -\alpha_1 - \alpha_2$. If $r > 2$ and $\mathfrak{Y} - \alpha_1$ is a root, we see as in the case A1) of the proof of Lemma 7.1 that $\mathfrak{Y} - \alpha_1, \alpha_1, \dots, \alpha_{r-1}$ form an i.s.s.



of a type impossible by Th. 6.1. Therefore $\mathfrak{Y} - \alpha_1$ is not a root, and $\mathfrak{Y}, \alpha_1, \dots, \alpha_{r-1}$ form the impossible i.s.s.



A2) As in A1), we find $\lambda_r = \frac{1}{r+1}(A_{\mathfrak{Y},1} - r)$, $\lambda_{r-1} = \frac{1}{r+1}(2A_{\mathfrak{Y},1} - r + 1)$, ..., $\lambda_2 = \frac{1}{r+1}((r-1)A_{\mathfrak{Y},1} - 2)$, $\lambda_1 = \frac{1}{r+1}(rA_{\mathfrak{Y},1} - 1)$.

$$\begin{aligned} A_{\mathfrak{Y},1} = 1: \lambda_r &= \frac{1-r}{r+1}, \lambda_1 = \frac{r-1}{r+1}. \quad 2 = A_{\mathfrak{Y},\mathfrak{Y}} = \sum \lambda_1 A_{1,\mathfrak{Y}} = \lambda_1 - \lambda_r \\ &= 2\frac{r-1}{r+1}; \quad r-1 = r+1, \quad \text{a contradiction.} \end{aligned}$$

$$A_{\gamma,1} = 0: \lambda_r = \frac{-r}{r+1} = A_{\gamma,\gamma} = 2; p \nmid (r+2), \text{ and } \gamma = (1 \ 2 \ \dots \ r) = \alpha_0.$$

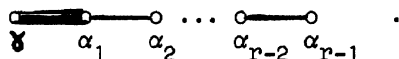
$$A_{\gamma,1} = -1: \gamma = -(1 \ 1 \ \dots \ 1).$$

$$A_0) \lambda_r = \frac{1}{r+1} A_{\gamma,1}, \lambda_{r-1} = \frac{2}{r+1} A_{\gamma,1}, \dots, \lambda_1 = \frac{r}{r+1} A_{\gamma,1}.$$

$$A_{\gamma,1} = 0: \text{Then } \gamma = 0, \text{ contrary to the choice of } \gamma.$$

$$A_{\gamma,1} = -1: 2 = A_{\gamma,\gamma} = \frac{-r}{r+1} A_{1,\gamma}.$$

$A_{1,\gamma} = -3: \gamma - \alpha_1$ is not a root, $\lambda_r \neq 0$, and $\gamma, \alpha_1, \dots, \alpha_{r-1}$ form the system



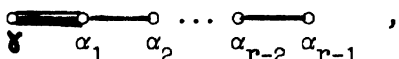
This is impossible if $r > 2$ and contrary to assumption if $r = 2$.

$$A_{1,\gamma} = -2: r = r+1, \text{ a contradiction.}$$

$$A_{1,\gamma} = -1; p \nmid (r+2), \text{ and } \gamma = -(2 \ 3 \ \dots \ r \ r+1).$$

$$A_{\gamma,1} = -2: 2 = A_{\gamma,\gamma} = \frac{-2r}{r+1} A_{1,\gamma} = \frac{2r}{r+1}; r = r+1, \text{ a contradiction.}$$

$A_{\gamma,1} = -3: \lambda_r \neq 0, \gamma - \alpha_1$ is not a root, and $\gamma, \alpha_1, \dots, \alpha_{r-1}$ form the i.s.s.



which is impossible as in the case $A_{1,\gamma} = -3$.

For $A_{\gamma,1} = 1, 2, 3$, we obtain the negatives of these roots. Thus among the possible values for γ when α_0 is not a root, we have only α_1 and $-(1 \ 1 \ \dots \ 1)$.

$\gamma = \alpha_1: \gamma + \alpha_2$ is a root, but $\gamma + \alpha_j$ is not a root for $j > 2$. $\gamma + \alpha_2 + \alpha_3$ is a root, but $\gamma + \alpha_2 + \alpha_j$ is not a root for $j > 4, j \neq 3$. (For $j = 2, \gamma + 2\alpha_2$ a root would imply $\gamma - \alpha_2$ a root; for $j > 3, \gamma + \alpha_2 + \alpha_j$ a root would imply $\gamma + \alpha_j$ a root.) By successive application of this type of reasoning, we obtain the string of roots

$$[1] \quad \gamma, \gamma + \alpha_2, \gamma + \alpha_2 + \alpha_3, \dots, \gamma + \alpha_2 + \dots + \alpha_r$$

in which each member after γ is the only root obtainable from its immediate predecessor by adding some $\alpha_j, 1 < j \leq r$. If

$$\gamma + \alpha_2 + \dots + \alpha_r + \alpha_j \text{ is a root, } 1 < j < r, \text{ so are } \gamma + \alpha_2 + \dots + \alpha_r - \alpha_j = (1 \ \dots \ 1 \ 0 \ 1 \ \dots \ 1), (1 \ \dots \ 1 \ 0 \ 0 \ 1 \ \dots \ 1), \dots,$$

$(1 \ 0 \ \dots \overset{j}{0} \ 1 \ \dots \ 1), \dots, (1 \ 0 \ \dots \ 0 \ 1) = \alpha_1 + \alpha_r$, a contradiction if $r > 2$. (If $r = 2$, it is clear that $\gamma + 2\alpha_2$ is not a root.) If $\gamma + \alpha_2 + \dots + \alpha_r + \alpha_r$ is a root, so are $(1 \ \dots \ 1 \ -1), (1 \ \dots \ 1 \ 0 \ -1), \dots, (1 \ 0 \ \dots \ 0 \ -1) = \alpha_1 - \alpha_r$, a contradiction. Therefore the root β is among the string [1]. In our construction of β , the coefficient of α_1 was -1 except when $\beta = \alpha$. Therefore $\beta = \alpha$ is among the roots

$$(1 \ 0 \ \dots \ 0), (1 \ 1 \ 0 \ \dots \ 0), (1 \ 1 \ 1 \ 0 \ \dots \ 0), \dots, (1 \ \dots \ 1).$$

$\gamma = -(1 \ \dots \ 1)$: By the kind of reasoning applied above, we find that β is among the string

$$[2] \quad -(1 \ \dots \ 1), -(1 \ \dots \ 1 \ 0), \dots, -(1 \ 0 \ \dots \ 0).$$

Now either $\alpha = \beta$, or $\alpha = \beta + \alpha_1 + \dots + \alpha_k, k < r$. If $\alpha = \beta$, we are done. If $\alpha = \beta + \alpha_1 + \dots + \alpha_k$, then since the first non-zero coefficient of α was assumed to be among $-1, -2, -3$, we must have $k < m$, where m is the number of non-zero coefficients of β in the string [2]. Thus $\alpha = -(0 \ \dots \ 0 \overset{k}{1} \ \dots \ \overset{m}{1} \ 0 \ \dots \ 0)$, and α is among the negatives of the roots listed.

Suitable application of Th. 5.6 shows that all quantities listed in the "non-exceptional" list actually are roots.

When $p \mid (r + 2)$, the following possible values for γ were also encountered: $-(1 \ 3 \ 4 \ \dots \ r + 1), \alpha_0 = (1 \ 2 \ \dots \ r), \pm(2 \ 3 \ 4 \ \dots \ r + 1)$. In each case, applications of Th. 5.6 show that α_0 is a root.

$\gamma = -(1 \ 3 \ 4 \ \dots \ r + 1)$: As before, β is among

$$[3] \quad \gamma, \gamma + \alpha_2, \gamma + \alpha_2 + \alpha_3, \dots, \gamma + \alpha_2 + \alpha_3 + \dots + \alpha_r.$$

Now either $\alpha = \beta$, or $\beta + \alpha_1$ is a root. In the latter case, if

$\beta = \gamma + \alpha_2 + \dots + \alpha_{j-1}, j > 3, \beta + \alpha_1 = -(0 \ 2 \ \dots \ j - 1 \overset{j}{j} + 1 \ \dots \ r + 1)$. Also roots are $\beta - \alpha_1 = -(2 \ 2 \ 3 \ \dots \ j - 1 \overset{j}{j} + 1 \ \dots \ r + 1),$
 $-(2 \ 2 \ 3 \ \dots \ j - 2 \ j \ j + 1 \ \dots \ r + 1), \dots, -(2 \ 2 \ 3 \ 5 \ \dots \ r + 1),$
 $-(2 \ 3 \ 3 \ 5 \ \dots \ r + 1), -(2 \ 3 \ 5 \ 5 \ \dots \ r + 1), -(1 \ 3 \ 5 \ 5 \ \dots \ r + 1) =$
 $\gamma - \alpha_3$, a contradiction. If $\beta = \gamma + \alpha_2 = -(1 \ 2 \ 4 \ \dots \ r + 1)$, and $\beta + \alpha_1$ is a root, so are $\beta - \alpha_1 = -(2 \ 2 \ 4 \ 5 \ \dots \ r + 1),$
 $-(2 \ 2 \ 3 \ 5 \ \dots \ r + 1), -(2 \ 3 \ 3 \ 5 \ \dots \ r + 1), -(2 \ 3 \ 5 \ 5 \ \dots \ r + 1),$
 $-(1 \ 3 \ 5 \ 5 \ \dots \ r + 1) = \gamma - \alpha_3$, again a contradiction. If $\beta = \gamma$ and $\beta + \alpha_1$ is a root, so are $\beta + \alpha_1 + 2\alpha_2 = -(0 \ 1 \ 4 \ \dots \ r + 1),$

$-(1 \ 1 \ 4 \ \dots \ r + 1)$, $-(1 \ 4 \ 4 \ \dots \ r + 1) = \gamma - \alpha_2$, a contradiction. Thus $\alpha = \beta$, and all possible values for α are negatives of members of the list.

$\gamma = \alpha_0$: β must be among

$$\gamma, \gamma + \alpha_r, \gamma + \alpha_r + \alpha_{r-1}, \dots, \gamma + \alpha_r + \alpha_{r-1} + \dots + \alpha_2.$$

Since the coefficient of α_1 in β is not -1 , $\alpha = \beta$, and has been included in our listing.

$\gamma = \pm (2 \ 3 \ 4 \ \dots \ r + 1)$: $\gamma + \alpha_j$ is not a root for any $j > 1$, so $\beta = \gamma$. Since the first coefficient of β is not -1 , $\alpha = \beta = \gamma$.

If α_0 is a root, all the "exceptional" quantities are roots. This completes the proof of the theorem. In succeeding theorems of this type, the observation that all listed quantities are roots will be omitted. It follows in each case by Th. 5.6.

IX. SYSTEMS OF TYPE D

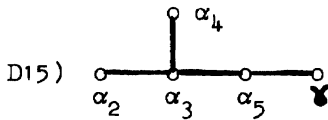
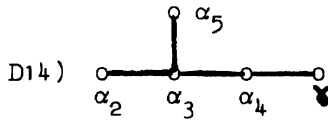
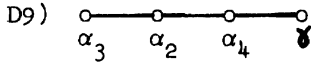
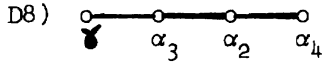
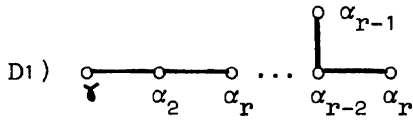
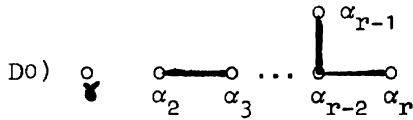
THEOREM 9.1. Let $\alpha_1, \dots, \alpha_r$ be an i.s.s. of type $D_r (r \geq 4)$, and suppose there is no i.s.s. β_1, \dots, β_r of r roots, each linearly dependent on $\alpha_1, \dots, \alpha_r$, of type B, C, E or F. Then every root which is a linear combination of $\alpha_1, \dots, \alpha_r$ is among the following and their negatives, where $\alpha_1, \dots, \alpha_r$ is labeled as in the proof of Lemma 7.1:

$$\begin{aligned} &(1 \ 0 \ \dots \ 0), (0 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1); \\ &(1 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1 \ 1 \ 0), (0 \ \dots \ 0 \ 1 \ 0 \ 1); \\ &(1 \ 1 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1 \ 1 \ 1 \ 0), (0 \ \dots \ 0 \ 1 \ 1 \ 0 \ 1), \\ &\quad (0 \ \dots \ 0 \ 1 \ 1 \ 1); \\ &(1 \ 1 \ 1 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1 \ 1 \ 1 \ 1 \ 0), (0 \ \dots \ 0 \ 1 \ 1 \ 1 \ 0 \ 1), \\ &\quad (0 \ \dots \ 0 \ 1 \ 1 \ 1 \ 1), (0 \ \dots \ 0 \ 1 \ 2 \ 1 \ 1); \\ &\quad \vdots \\ &\quad \vdots \\ &(1 \ \dots \ 1 \ 0), (1 \ \dots \ 1 \ 0 \ 1), (0 \ 1 \ \dots \ 1), (0 \ 1 \ \dots \ 1 \ 2 \ 1 \ 1), \\ &\quad \dots, (0 \ 1 \ 2 \ \dots \ 2 \ 1 \ 1); \\ &(1 \ \dots \ 1), (1 \ \dots \ 1 \ 2 \ 1 \ 1), (1 \ \dots \ 1 \ 2 \ 2 \ 1 \ 1), \dots, \\ &\quad (1 \ 2 \ \dots \ 2 \ 1 \ 1). \end{aligned}$$

There are $2r(r - 1)$ roots in all.

PROOF. Let α be a root dependent on $\alpha_1, \dots, \alpha_r$. If the coefficient of α_1 in α is not zero, take $\beta = \alpha$. Otherwise, if α_j has the first non-zero coefficient, we proceed as in the proof of Th. 8.1 if $j \leq r - 2$; i.e., replacing α by $-\alpha$ if necessary, we form a string of roots $\alpha - \alpha_{j-1}, \dots, \alpha - \alpha_{j-1} - \dots - \alpha_1 = \beta$. A similar procedure is possible except when $\alpha = \rho_{r-1}\alpha_{r-1} + \rho_r\alpha_r$, with $\rho_r = -\rho_{r-1}$. In this case, replacing α by $-\alpha$ if necessary, we may assume that $\alpha - \alpha_{r-1}$ is a root, and then form the string $\alpha, \alpha - \alpha_{r-1}, \dots, \alpha - \alpha_{r-1} - \dots - \alpha_1 = \beta$.

Now proceed according to Lemma 7.1 to obtain a root γ such that $\gamma, \alpha_2, \dots, \alpha_r$ form a simple system. By the hypotheses, this can only be one of the following:



D0) Solving the equations obtained from the relations, we find that $\gamma = (\lambda_1 \dots \lambda_r)$ is given by $\lambda_{r-1} = \lambda_r, \lambda_{r-2} = 2\lambda_r = \lambda_{r-3} = \dots = \lambda_1, \lambda_1 = A_{\gamma,1}$, and $\gamma = \frac{1}{2} A_{\gamma,1} (2 \dots 2 \ 1 \ 1)$. Thus $A_{\gamma,1} \neq 0$.

$A_{\gamma,1} = -1: 2 = A_{\gamma,\gamma} = -A_{1,\gamma}$, or $A_{1,\gamma} = -2$. Then $\gamma - \alpha_1$ is not a root, and $\gamma, \alpha_1, \dots, \alpha_{r-1}$ form an i.s.s. of type B_r , contrary

to assumption.

$A_{\gamma,1} = -2$: Here $\gamma, \alpha_1, \dots, \alpha_{r-1}$ form an i.s.s. of type C_r , a contradiction.

$A_{\gamma,1} = -3$: $2 = A_{\gamma,\gamma} = -3A_{1,\gamma} = 3$, a contradiction.

For $A_{\gamma,1} = 1, 2, 3$, replace γ by $-\gamma$. Then $-\gamma, \alpha_2, \dots, \alpha_r$ form a simple system, with $A_{-\gamma,1} = -1, -2, -3$. But this has just been proved impossible.

D1) Unless $\gamma = \alpha_1$, $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0)$ or $(-1, -1)$. We find $\lambda_{r-1} = \lambda_r$, $\lambda_{r-2} = 2\lambda_r = \dots = \lambda_2$, $\lambda_1 = 2\lambda_r + 1$, $A_{\gamma,1} = 2\lambda_r + 2$.

$A_{\gamma,1} = 1$: $\lambda_r = -\frac{1}{2}$, $\lambda_1 = 0$, a contradiction.

$A_{\gamma,1} = 0$: $\gamma = -(1 \ 2 \ \dots \ 2 \ 1 \ 1)$.

$A_{\gamma,1} = -1$: $\lambda_r = \frac{3}{2}$, $\lambda_2 = -3$, $\lambda_1 = -2$; $2 = A_{\gamma,\gamma} = -2A_{1,\gamma} - 3A_{2,\gamma} = 5$, a contradiction.

D8) $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0)$ or $(-1, -1)$. $\lambda_4 = \lambda_3 + \frac{1}{2}$, $\lambda_2 = 2\lambda_3 + 1$, $\lambda_1 = 2\lambda_3 + \frac{3}{2}$, $A_{\gamma,1} = 2\lambda_3 + 2$.

$A_{\gamma,1} = 1$: $\lambda_3 = -\frac{1}{2}$, $\lambda_1 = \frac{1}{2}$, $\lambda_2 = \lambda_4 = 0$. $2 = A_{\gamma,\gamma} = \frac{1}{2}A_{1,\gamma} - \frac{1}{2}A_{3,\gamma} = \frac{1}{2} + \frac{1}{2} = 1$, a contradiction.

$A_{\gamma,1} = 0$: $\lambda_3 = -1$; $2 = A_{\gamma,\gamma} = -A_{3,\gamma} = 1$, a contradiction.

$A_{\gamma,1} = -1$: $\lambda_3 = -\frac{3}{2} = \lambda_1$; $2 = A_{\gamma,\gamma} = -\frac{3}{2}A_{1,\gamma} - \frac{3}{2}A_{3,\gamma} = 3$, a contradiction.

D14) $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0)$ or $(-1, -1)$. $\lambda_5 = \lambda_4 + \frac{1}{2}$, $\lambda_3 = 2\lambda_4 + 1$, $\lambda_2 = 2\lambda_4 + \frac{3}{2}$, $\lambda_1 = 2\lambda_4 + 2$, $\lambda_4 = \frac{1}{2}A_{\gamma,1} - \frac{5}{4}$.

$A_{\gamma,1} = 1$: $\lambda_4 = -\frac{3}{4}$, $\lambda_1 = \frac{1}{2}$; $2 = A_{\gamma,\gamma} = \frac{1}{2}A_{1,\gamma} - \frac{3}{4}A_{4,\gamma} = \frac{5}{4}$, a contradiction.

$A_{\gamma,1} = 0$: $\lambda_4 = -\frac{5}{4}$; $2 = A_{\gamma,\gamma} = -\frac{5}{4}A_{4,\gamma} = \frac{5}{4}$, a contradiction.

$A_{\gamma,1} = -1$: $\lambda_4 = -\frac{7}{4}$, $\lambda_1 = -\frac{3}{2}$; $2 = A_{\gamma,\gamma} = -\frac{3}{2}A_{1,\gamma} - \frac{7}{4}A_{4,\gamma} = \frac{13}{4}$, a contradiction.

D9) and D15) are impossible by symmetry with D8) and D14). Thus we have either $\gamma = \alpha_1$ or $\gamma = -(1 \ 2 \ \dots \ 2 \ 1 \ 1)$.

$\gamma = \alpha_1$: In the following string of roots, a root immediately following another is the only root which can be obtained from it by adding some α_j , $j > 1$. If there are two or more such roots, all of them will be

enclosed in a bracket, and the next entry in the string is a bracket containing all roots obtainable from these by adding a single α_j , $j > 1$, if more than one such root exists. The reasoning follows the lines of the proof of Th. 8-1, and β is among these roots:

$$\begin{aligned} \gamma = & (1 \ 0 \ \dots \ 0), (1 \ 1 \ 0 \ \dots \ 0), \dots, (1 \ \dots \ 1 \ 0 \ 0), \\ & [(1 \ \dots \ 1 \ 1 \ 0), (1 \ \dots \ 1 \ 0 \ 1)], (1 \ \dots \ 1 \ 1), \\ & (1 \ \dots \ 1 \ 2 \ 1 \ 1), \dots, (1 \ 2 \ \dots \ 2 \ 1 \ 1). \end{aligned}$$

Since the first coefficient of β is not -1 , we have $\alpha = \beta$.

$$\begin{aligned} \gamma = & -(1 \ 2 \ \dots \ 2 \ 1 \ 1): \text{ As above, } \beta \text{ is a member of the string} \\ \gamma = & -(1 \ 2 \ \dots \ 2 \ 1 \ 1), -(1 \ 1 \ 2 \ \dots \ 2 \ 1 \ 1), \dots, \\ & -(1 \ \dots \ 1 \ 2 \ 1 \ 1), -(1 \ \dots \ 1), [-(1 \ \dots \ 1 \ 0), -(1 \ \dots \ 1 \ 0 \ 1)], \\ & -(1 \ \dots \ 1 \ 0 \ 0), \dots, -(1 \ 0 \ \dots \ 0) = -\alpha_1. \end{aligned}$$

If $\alpha = \beta$, α is among the negatives of the roots listed in the statement of the theorem. Now let $\alpha = \beta + \alpha_1 + \dots + \alpha_k$, $k \leq r - 1$. If no coefficient of β is -2 , then α is a root of the list if it is a root, as in the proof of Th. 8.1. If some coefficient of β is -2 , then α is among the roots listed except when

$\beta = -(1 \ \dots \ 1 \ 2 \ \dots \ 2 \ 1 \ 1)$. In this case, $k \leq r - 2$, and $\alpha = -(0 \ \dots \ 0 \ 2 \ \dots \ 2 \ 1 \ 1)$. Also roots are $-(0 \ \dots \ 0 \ 2 \ \dots \ 2 \ 1 \ 1)$, \dots , $-(0 \ \dots \ 0 \ 1 \ 1)$, $(0 \ \dots \ 0 \ 1 \ 1) = \alpha_{r-1} + \alpha_r$, a contradiction. If $k = r - 1$, the coefficient of α_{r-1} in α is non-zero, and we must have $\beta = -(1 \ \dots \ 1 \ 0 \ 1)$, $\alpha = \alpha_{r-1} - \alpha_r$, which is impossible. Thus α is among the roots cited in the theorem, and the theorem is proved.

X. SYSTEMS OF TYPE B

THEOREM 10.1. Let $\alpha_1, \dots, \alpha_r$ be an i.s.s. of type B_r and suppose there is no i.s.s. β_1, \dots, β_r of r roots, each linearly dependent on $\alpha_1, \dots, \alpha_r$, of type C, G or F. Then if the system $\alpha_1, \dots, \alpha_r$ is labeled as in the proof of Lemma 7.1, every root dependent on $\alpha_1, \dots, \alpha_r$ is among the following and their negatives:

$$\begin{aligned} & (1 \ 0 \ \dots \ 0), (0 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1); \\ & (1 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1 \ 1), (0 \ \dots \ 0 \ 1 \ 2); \\ & (1 \ 1 \ 1 \ 0 \ \dots \ 0), \dots, (0 \ \dots \ 0 \ 1 \ 1 \ 1), (0 \ \dots \ 0 \ 1 \ 1 \ 2), \end{aligned}$$

$$\begin{array}{c}
 (0 \dots 0 \ 1 \ 2 \ 2); \\
 \vdots \\
 (1 \dots 1 \ 0), (0 \ 1 \dots 1), (0 \ 1 \dots 1 \ 2), \dots, (0 \ 1 \ 2 \dots 2); \\
 (1 \dots 1), (1 \dots 1 \ 2), \dots, (1 \ 2 \dots 2).
 \end{array}$$

There are $2r^2$ roots in all.

PROOF. As in the proof of Th. 8.1, we find a root β : $\beta = \alpha$ or $\beta = \alpha - \alpha_k - \dots - \alpha_1$, $k < r$, such that the coefficient of α_1 in β is non-zero. Then by Lemma 7.1 we find a string $\beta, \beta - \alpha_{1_1}, \beta - \alpha_{1_1} - \alpha_{1_2}, \dots, \beta - \alpha_{1_1} - \dots - \alpha_{1_s} = \gamma$, $2 \leq 1_j \leq r$, such that $\gamma, \alpha_2, \dots, \alpha_r$ form a simple system. We shall assume for the present that $\gamma \neq \alpha_1$. If $r = 2$, we can have:

$$\begin{array}{ll}
 B_2^0) \begin{array}{c} \circ \\ \gamma \\ \circ \\ \alpha_2 \end{array} & B_2^1) \begin{array}{c} \circ \text{---} \circ \\ \gamma \qquad \alpha_2 \end{array} \\
 B_2^2) \begin{array}{c} \text{---} \circ \\ \gamma \qquad \alpha_2 \end{array}, A_{\gamma,2} = -2; & B_2^3) \begin{array}{c} \text{---} \circ \\ \gamma \qquad \alpha_2 \end{array}, A_{2,\gamma} = -2.
 \end{array}$$

B_2^0) If $\gamma = (\lambda_1 \lambda_2)$, we have $\lambda_1 = \lambda_2 = A_{\gamma,1}$, from the equations obtained as in earlier cases. Since $\alpha_1 + \alpha_2$ is a root, $A_{\gamma,1} = \pm 1$, $\gamma = \pm (1 \ 1)$. But then $\gamma - \alpha_2$ is a root, contrary to choice of γ .

$$B_2^1) (A_{\gamma,1}, A_{1,\gamma}) = (1, 2), (0, 0) \text{ or } (-1, -2). \quad \lambda_1 = \lambda_2 + \frac{1}{2}, \lambda_2 = A_{\gamma,1} - 1.$$

$$A_{\gamma,1} = 1: \lambda_2 = 0, \lambda_1 = \frac{1}{2}, \gamma = \frac{1}{2} \alpha_1, \text{ a contradiction.}$$

$$A_{\gamma,1} = 0: \lambda_2 = -1, \lambda_1 = -\frac{1}{2}, \gamma = -\frac{1}{2}(\alpha_1 + 2\alpha_2), \text{ a contradiction.}$$

$$A_{\gamma,1} = -1: \lambda_2 = -2, \lambda_1 = -\frac{3}{2}; 2 = A_{\gamma,\gamma} = -\frac{3}{2} A_{1,\gamma} - 2A_{2,\gamma} = 5, \text{ a contradiction.}$$

$$B_2^2) (A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0) \text{ or } (-1, -1). \quad \lambda_1 = \lambda_2 + 1, \lambda_2 = A_{\gamma,1} - 2.$$

$$A_{\gamma,1} = 1: \lambda_2 = -1, \lambda_1 = 0, \text{ contrary to choice of } \gamma.$$

$$A_{\gamma,1} = 0: \lambda_2 = -2, \lambda_1 = -1, \gamma = -(1 \ 2).$$

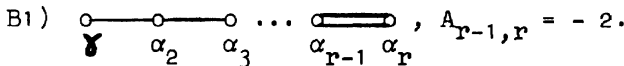
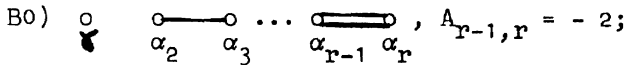
$$A_{\gamma,1} = -1: \lambda_2 = -3, \lambda_1 = -2; 2 = A_{\gamma,\gamma} = -2A_{1,\gamma} - 3A_{2,\gamma} = 5, \text{ a contradiction.}$$

$$B_2^3) \text{ Here } \gamma(h_\gamma) = \frac{1}{4} \alpha_1(h_1), \text{ or } A_{1,\gamma} = 4A_{\gamma,1}. \text{ Thus either}$$

$A_{\gamma,1} = 0 = A_{1,\gamma}$ or $p = 11$ and $(A_{\gamma,1}, A_{1,\gamma}) = (3, 1)$ or $(-3, -1)$. In the former case we find $\gamma = -\frac{1}{2}(\alpha_1 + 2\alpha_2)$, a contradiction. In the latter cases, either $-\gamma$ and α_1 or γ and α_1 form an i.s.s. of type G_2 , contrary to assumption.

Thus $\gamma = \alpha_1$ or $\gamma = -(1\ 2)$. If $\gamma = \alpha_1$, $\beta = \alpha_1$, $\alpha_1 + \alpha_2$ or $\alpha_1 + 2\alpha_2$, and $\alpha = \beta$ is among the roots listed. If $\gamma = -(1\ 2)$, then $\beta = \gamma$, $\gamma + \alpha_2$ or $\gamma + 2\alpha_2$. If $\beta = \gamma$, then $\alpha = \beta$. If $\beta = \gamma + \alpha_2$, then $\alpha = \beta = -(1\ 1)$ or $\alpha = \beta + \alpha_1 = -(0\ 1)$. If $\beta = \gamma + 2\alpha_2$, then $\beta + \alpha_1 = 0$, or $\alpha = \beta = -(1\ 0)$. In each case, α is among the roots mentioned.

For $r > 2$, $\gamma, \alpha_2, \dots, \alpha_r$ has one of the following diagrams:



B0) $\lambda_r = \lambda_{r-1} = \dots = \lambda_1 = A_{\gamma,1}$. Since $\alpha_1 + \alpha_2 + \dots + \alpha_r$ is a root, $A_{\gamma,1} = \pm 1$, $\gamma = \pm (1\ 1 \dots 1)$. But then $\gamma - \alpha_r$ is a root, a contradiction.

B1) $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0)$ or $(-1, -1)$. $\lambda_{r-1} = \lambda_r = \dots = \lambda_2$, $\lambda_1 = \lambda_r + 1$, $\lambda_r + 2 = A_{\gamma,1}$.

$A_{\gamma,1} = 1$: $\lambda_r = -1$, $\lambda_1 = 0$, a contradiction.

$A_{\gamma,1} = 0$: $\gamma = -(1\ 2 \dots 2)$.

$A_{\gamma,1} = -1$: $\lambda_2 = -3$, $\lambda_1 = -2$; $2 = A_{\gamma,\gamma} = -2A_{1,\gamma} - 3A_{2,\gamma} = 5$, a contradiction. Thus either $\gamma = \alpha_1$ or $\gamma = -(1\ 2 \dots 2)$.

$\gamma = \alpha_1$: As in the proof of Th. 8.1, β is in the following string:

- $\gamma = (1\ 0 \dots 0), (1\ 1\ 0 \dots 0), \dots, (1 \dots 1), (1 \dots 1\ 2), \dots, (1\ 2 \dots 2)$.

Since the leading coefficient of β is not -1 , $\alpha = \beta$.

$\gamma = -(1\ 2 \dots 2)$: β is among the following roots:

- $\gamma = -(1\ 2 \dots 2), -(1\ 1\ 2 \dots 2), \dots, -(1 \dots 1), -(1 \dots 1\ 0), \dots, -(1\ 0 \dots 0) = -\alpha_1$.

If $\alpha = \beta$, we are done. If $\alpha = \beta + \alpha_1 + \dots + \alpha_k$, the first k coefficients of β must be -1 . If the $(k+1)$ st coefficient of β is

- 2, then $\alpha = -2(0 \dots 0 \overset{k}{1} \dots 1)$, a contradiction. Therefore α is either of the form $-(0 \dots 0 \overset{k}{1} \dots 1 \ 2 \dots 2)$, of the form $-(0 \dots 0 \overset{k}{1} \dots 1)$ or of the form $-(0 \dots 0 \overset{k}{1} \dots 1 \ 0 \dots 0)$. But all roots of each of these forms are included in the statement of the theorem.

XI. SYSTEMS OF TYPE C

THEOREM 11.1. Let $\alpha_1, \dots, \alpha_r$ be an i.s.s. of type C_r ($r \geq 3$), and suppose there is no i.s.s. β_1, \dots, β_r or r roots, linearly dependent on $\alpha_1, \dots, \alpha_r$, of type F. Then every root dependent on $\alpha_1, \dots, \alpha_r$ is among the following and their negatives:

- (1 0 ... 0), (0 1 0 ... 0), ..., (0 ... 0 1);
- (1 1 0 ... 0), ..., (0 ... 0 1 1), (0 ... 0 2 1);
- (1 1 1 0 ... 0), ..., (0 ... 0 1 1 1), (0 ... 0 1 2 1),
(0 ... 0 2 2 1);
- ⋮
- (1 ... 1 0), (0 1 ... 1), (0 1 ... 1 2 1), ...,
(0 2 ... 2 1);
- (1 ... 1), (1 ... 1 2 1), ..., (2 ... 2 1).

There are $2r^2$ roots in all.

PROOF. Let α be such a root. As in the proofs of Ths. 8.1 and 10.1, we find a root $\gamma = (\lambda_1 \dots \lambda_r)$ such that $\gamma, \alpha_2, \dots, \alpha_r$ form a simple system. This must be one of the following:

C0) $\begin{matrix} \circ & \text{---} & \circ & \dots & \text{---} & \text{---} & \circ & \circ \\ \gamma & & \alpha_2 & & \alpha_3 & & \alpha_{r-1} & \alpha_r \end{matrix}, A_{r,r-1} = -2;$

C1) $\begin{matrix} \circ & \text{---} & \circ & \dots & \text{---} & \text{---} & \circ & \circ \\ \gamma & & \alpha_2 & & \alpha_3 & & \alpha_{r-1} & \alpha_r \end{matrix}, A_{r,r-1} = -2;$

C3) $\begin{matrix} \text{---} & \text{---} & \circ \\ \alpha_2 & \alpha_3 & \gamma \end{matrix}, A_{32} = -2.$

C0) $\lambda_{r-1} = 2 \lambda_r = \lambda_{r-2} = \dots = \lambda_1 = A_{\gamma,1}, \gamma = \frac{1}{2} A_{\gamma,1} (2 \dots 2 \ 1).$

Since $(2 \dots 2 \ 1)$ is a root, $\gamma = \pm(2 \dots 2 \ 1)$.

C1) If $\gamma \neq \alpha_1$, then $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0)$ or $(-1, -1)$.

We find $\lambda_{r-1} = 2\lambda_r = \lambda_{r-2} = \dots = \lambda_2$, $\lambda_1 = 2\lambda_r + 1$,
 $A_{\gamma,1} = 2\lambda_r + 2$.

$A_{\gamma,1} = 1$: $\lambda_r = -\frac{1}{2}$, $\lambda_1 = 0$, contrary to assumption.

$A_{\gamma,1} = 0$: $\lambda_r = -1$, $\gamma = -(1\ 2 \dots 2\ 1)$.

$A_{\gamma,1} = -1$: $\lambda_r = -\frac{3}{2}$, $\lambda_2 = -3$, $\lambda_1 = -2$.

$2 = A_{\gamma,\gamma} = -2A_{1,\gamma} - 3A_{2,\gamma} = 5$, a contradiction.

C3) $(A_{\gamma,1}, A_{1,\gamma}) = (2, 1), (0, 0)$ or $(-2, -1)$. $\lambda_2 = 2\lambda_3 + 1$,

$\lambda_1 = 2\lambda_3 + 2$, $A_{\gamma,1} = 2\lambda_3 + 3$.

$A_{\gamma,1} = 2$: $\lambda_3 = -\frac{1}{2}$, $\lambda_2 = 0$, $\lambda_1 = 1$; $2 = A_{\gamma,\gamma} = A_{1,\gamma} - \frac{1}{2}A_{3,\gamma} = \frac{3}{2}$,
 a contradiction.

$A_{\gamma,1} = 0$: $\lambda_3 = -\frac{3}{2}$; $2 = A_{\gamma,\gamma} = -\frac{3}{2}A_{3,\gamma} = \frac{3}{2}$, a contradiction.

$A_{\gamma,1} = -2$: $\lambda_3 = -\frac{5}{2}$, $\lambda_1 = -3$; $2 = -3A_{1,\gamma} - \frac{5}{2}A_{3,\gamma} = \frac{11}{2}$, a
 contradiction.

Thus γ is one of $\alpha_1 = (1\ 0 \dots 0)$, $-(1\ 2 \dots 2\ 1)$, $\pm(2 \dots 2\ 1)$.

$\gamma = \alpha_1$: As in the preceding proofs the intermediate root β must
 be among

$\gamma = (1\ 0 \dots 0), (1\ 1\ 0 \dots 0), \dots, (1 \dots 1), (1 \dots 1\ 2\ 1),$
 $(1 \dots 1\ 2\ 2\ 1), \dots, (1\ 2 \dots 2\ 1)$.

Since the first coefficient of β is not -1 , we have $\alpha = \beta$.

$\gamma = \pm(2 \dots 2\ 1)$: Since $\gamma + \alpha_j$ is not a root for any $j > 1$, and
 since the first coefficient of γ is not -1 , $\gamma = \beta = \alpha$.

$\gamma = -(1\ 2 \dots 2\ 1)$: As in previous cases, β is among

$\gamma = -(1\ 2 \dots 2\ 1), -(1\ 1\ 2 \dots 2\ 1), \dots, -(1 \dots 1\ 2\ 1),$
 $-(1 \dots 1), -(1 \dots 1\ 0), \dots, -(1\ 0 \dots 0) = -\alpha_1$.

Either $\alpha = \beta$ or $\alpha = \beta + \alpha_1 + \dots + \alpha_k$, where the first k co-
 efficients of β are -1 and the $(k+1)$ st is non-zero. But all such
 quantities α are among the roots mentioned in the statement of the
 theorem. Thus all possible roots α are mentioned, and the theorem is
 proved.

XII. SYSTEMS OF TYPE G

THEOREM 12.1. Let α_1, α_2 be an i.s.s. of type G.
 Then any root dependent on α_1 and α_2 is among the
 following and their negatives:

(1 0), (0 1), (1 1), (1 2), (1 3), (2 3).

There are 12 such roots in all.

PROOF. If $\alpha = (\rho_1, \rho_2)$ is such a root, we may assume $\rho_1 \neq 0$, since otherwise $\alpha = \pm \alpha_2$. Then one of $\alpha, \alpha - \alpha_2, \alpha - 2\alpha_2, \alpha - 3\alpha_2$ is a root γ such that γ and α_2 form a simple system. This is one of the following:

$$G0) \begin{array}{c} \circ \\ \gamma \end{array} \quad \begin{array}{c} \circ \\ \alpha_2 \end{array}$$

$$G1) \begin{array}{c} \circ \text{---} \circ \\ \gamma \quad \alpha_2 \end{array}$$

$$G2) \begin{array}{c} \text{---} \circ \\ \gamma \quad \alpha_2 \end{array}, A_{\gamma,2} = -2;$$

$$G3) \begin{array}{c} \text{---} \circ \\ \gamma \quad \alpha_2 \end{array}, A_{2,\gamma} = -2;$$

$$G4) \begin{array}{c} \text{---} \circ \\ \gamma \quad \alpha_2 \end{array}, A_{\gamma,2} = -3;$$

$$G5) \begin{array}{c} \text{---} \circ \\ \gamma \quad \alpha_2 \end{array}, A_{2,\gamma} = -3.$$

We assume for the present that $\gamma \neq \alpha_1$. Let $\gamma = (\lambda_1, \lambda_2)$.

G0) $\lambda_1 = \frac{2}{3}\lambda_2, \lambda_2 = 3A_{\gamma,1}, \gamma = A_{\gamma,1}(2\ 3)$. Since (2 3) is a root, $\gamma = \pm(2\ 3)$.

G1) $(A_{\gamma,1}, A_{1,\gamma}) = (1,3), (0,0)$ or $(-1, -3)$. $\lambda_1 = \frac{2}{3}\lambda_2 + \frac{1}{3}, \lambda_2 = 3A_{\gamma,1} - 2$.

$A_{\gamma,1} = 1: \lambda_2 = 1 = \lambda_1, \gamma = (1\ 1)$. Then $\gamma - \alpha_2$ is a root, a contradiction.

$A_{\gamma,1} = 0: \gamma = -(1\ 2)$, and $\gamma - \alpha_2$ is a root, a contradiction.

$A_{\gamma,1} = -1: \gamma = -(3\ 5); \gamma + \alpha_1 = \delta$ is a root, and $A_{\delta,2} = -4$, a contradiction.

G2) Here $3A_{\gamma,1} = 2A_{1,\gamma}$, or $A_{\gamma,1} = A_{1,\gamma} = 0$. Then $\gamma = -2(1\ 2)$, a contradiction.

G3) The coefficients λ_1, λ_2 are obtained from the same equations as in G1), but now $A_{1,\gamma} = 6A_{\gamma,1}$. From G1), $A_{\gamma,1} = 0$ is impossible. Thus either $p = 11$ and $(A_{\gamma,1}, A_{1,\gamma}) = (2, 1)$ or $(-2, -1)$, or $p = 17$ and $(A_{\gamma,1}, A_{1,\gamma}) = (3, 1)$ or $(-3, -1)$.

$A_{\gamma,1} = 2: \gamma = (3\ 4)$; also a root is $(2\ 4) = 2(1\ 2)$, a contradiction.

$A_{\gamma,1} = -2: \gamma = -(5\ 8)$; also a root is $-(4\ 8) = -4(1\ 2)$, a contradiction.

$A_{\gamma,1} = 3: \gamma = (5\ 7); (5\ 8)$ is also a root, contradicting the last step above.

$A_{\gamma,1} = -3: \gamma = -(7\ 11);$ also a root is $\gamma + \alpha_1 = \delta$, and $A_{\delta,2} = -4$, a contradiction.

G4) Here $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0)$ or $(-1, -1)$.

$$\lambda_1 = \frac{2}{3}\lambda_2 + 1, \quad \lambda_2 = 3A_{\gamma,1} - 6.$$

$$A_{\gamma,1} = 1: \gamma = -(1\ 3).$$

$$A_{\gamma,1} = 0: \gamma = -(3\ 6) = -3(1\ 2), \text{ a contradiction.}$$

$A_{\gamma,1} = -1: \gamma = -(5\ 9);$ also a root is $-(5\ 8)$, impossible by G3).

G5) The equations are those of G1) and G3), with $A_{1,\gamma} = 9A_{\gamma,1}$.

We must have either $A_{\gamma,1} = 0$, or $p = 17$ and $(A_{\gamma,1}, A_{1,\gamma}) = (2, 1)$ or $(-2, -1)$, or $p = 13$ and $(A_{\gamma,1}, A_{1,\gamma}) = (3, 1)$ or $(-3, -1)$. But all these possibilities have been eliminated in G3).

Thus γ is among $\alpha_1 = (1\ 0)$, $-(1\ 3)$ and $\pm(2\ 3)$.

$\gamma = (1\ 0): \alpha$ is among $(1\ 0), (1\ 1), (1\ 2), (1\ 3)$.

$\gamma = -(1\ 3): \alpha$ is among $-(1\ 3), -(1\ 2), -(1\ 1), -(1\ 0)$.

$\gamma = \pm(2\ 3): \alpha = \gamma = \pm(2\ 3)$. Thus the theorem is proved.

XIII. SYSTEMS OF TYPE F

THEOREM 13.1. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be an i.s.s. of type F. Then every root dependent on $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ is among the following their negatives:

$$(1\ 0\ 0\ 0), (0\ 1\ 0\ 0), (0\ 0\ 1\ 0), (0\ 0\ 0\ 1),$$

$$(1\ 1\ 0\ 0), (0\ 1\ 1\ 0),$$

$$(0\ 0\ 1\ 1), (0\ 1\ 2\ 0), (1\ 1\ 1\ 0), (0\ 1\ 1\ 1),$$

$$(1\ 1\ 2\ 0), (1\ 2\ 2\ 0),$$

$$(0\ 1\ 2\ 1), (0\ 1\ 2\ 2), (1\ 1\ 1\ 1), (1\ 1\ 2\ 1),$$

$$(1\ 1\ 2\ 2), (1\ 2\ 2\ 1),$$

$$(1\ 2\ 2\ 2), (1\ 2\ 3\ 1), (1\ 2\ 3\ 2), (1\ 2\ 4\ 2),$$

$$(1\ 3\ 4\ 2), (2\ 3\ 4\ 2).$$

There are 48 such roots in all.

PROOF. Let α be a root, and proceed from α to a root γ as in the proofs of Ths. 8.1-11.1. $\gamma, \alpha_2, \alpha_3, \alpha_4$ form a simple system, one of the following:

$$F0) \quad \begin{array}{c} \circ \\ \gamma \end{array} \quad \begin{array}{c} \text{---} \text{---} \text{---} \\ \alpha_2 \quad \alpha_3 \end{array} \quad \begin{array}{c} \circ \\ \alpha_4 \end{array}, \quad A_{23} = -2;$$

$$F1) \quad \begin{array}{c} \circ \\ \gamma \end{array} \quad \begin{array}{c} \text{---} \text{---} \text{---} \\ \alpha_2 \quad \alpha_3 \end{array} \quad \begin{array}{c} \circ \\ \alpha_4 \end{array}, \quad A_{23} = -2;$$

$$F2) \quad \begin{array}{c} \text{---} \text{---} \text{---} \\ \alpha_2 \quad \alpha_3 \end{array} \quad \begin{array}{c} \circ \\ \alpha_4 \end{array} \quad \begin{array}{c} \circ \\ \gamma \end{array}, \quad A_{23} = -2.$$

Let $\gamma = (\lambda_1 \lambda_2 \lambda_3 \lambda_4)$, $\gamma \neq \alpha_1$.

F0) $\lambda_3 = 2\lambda_4$, $\lambda_2 = \frac{3}{2}\lambda_4$, $\lambda_1 = \lambda_4$, $\lambda_4 = 2A_{\gamma,1}$.
 $\gamma = A_{\gamma,1}(2 \ 3 \ 4 \ 2)$. Since we know that $(2 \ 3 \ 4 \ 2)$ is a root,
 $\gamma = \pm(2 \ 3 \ 4 \ 2)$.

F1) $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0)$ or $(-1, -1)$. $\lambda_3 = 2\lambda_4$,
 $\lambda_2 = \frac{3}{2}\lambda_4$, $\lambda_1 = \lambda_4 + 1$, $\lambda_4 = 2(A_{\gamma,1} - 2)$.

$A_{\gamma,1} = 1$: $\gamma = -(1 \ 3 \ 4 \ 2)$.

$A_{\gamma,1} = 0$: $\lambda_2 = -6$; $2 = A_{\gamma,\gamma} = -6A_{2,\gamma} = 6$, a contradiction.

$A_{\gamma,1} = -1$: $\lambda_2 = -9$, $\lambda_1 = -5$; $2 = A_{\gamma,\gamma} = -5A_{1,\gamma} - 9A_{2,\gamma} = 14$,
 a contradiction.

F2) $(A_{\gamma,1}, A_{1,\gamma}) = (1, 2), (0, 0)$ or $(-1, -2)$. $\lambda_3 = 2\lambda_4 + 1$,
 $\lambda_2 = \frac{3}{2}\lambda_4 + 1$, $\lambda_1 = \lambda_4 + 1$, $\lambda_4 = 2(A_{\gamma,1} - 1)$.

$A_{\gamma,1} = 1$: $\gamma = (1 \ 1 \ 1 \ 0)$, and $\gamma - \alpha_3$ is a root, a contradiction.

$A_{\gamma,1} = 0$: $\gamma = -(1 \ 2 \ 3 \ 2)$; again $\gamma - \alpha_3$ is a root.

$A_{\gamma,1} = -1$: $\gamma = -(3 \ 5 \ 7 \ 4)$; $2 = A_{\gamma,\gamma} = -4A_{4,\gamma} - 3A_{1,\gamma} = 10$, a
 contradiction.

Thus γ is among $\alpha_1 = (1 \ 0 \ 0 \ 0)$, $-(1 \ 3 \ 4 \ 2)$, $\pm(2 \ 3 \ 4 \ 2)$.

$\gamma = (1 \ 0 \ 0 \ 0)$: Using the conventions of the proof of Th. 9.1, the
 intermediate root β must be one of the following:

$(1 \ 0 \ 0 \ 0)$, $(1 \ 1 \ 0 \ 0)$, $(1 \ 1 \ 1 \ 0)$, $[(1 \ 1 \ 2 \ 0), (1 \ 1 \ 1 \ 1)]$,
 $[(1 \ 2 \ 2 \ 0), (1 \ 1 \ 2 \ 1)]$, $[(1 \ 2 \ 2 \ 1), (1 \ 1 \ 2 \ 2)]$,
 $[(1 \ 2 \ 2 \ 2), (1 \ 2 \ 3 \ 1)]$, $(1 \ 2 \ 3 \ 2)$, $(1 \ 2 \ 4 \ 2)$, $(1 \ 3 \ 4 \ 2)$.

$\alpha = \beta$ is among the roots listed.

$\gamma = - (1 \ 3 \ 4 \ 2)$; As above, β is one of the following:

$- (1 \ 3 \ 4 \ 2)$, $- (1 \ 2 \ 4 \ 2)$, $- (1 \ 2 \ 3 \ 2)$, $[- (1 \ 2 \ 2 \ 2), -(1 \ 2 \ 3 \ 1)]$,
 $[- (1 \ 1 \ 2 \ 2)$, $- (1 \ 2 \ 2 \ 1)]$, $[- (1 \ 1 \ 2 \ 1)$, $- (1 \ 2 \ 2 \ 0)]$,
 $[- (1 \ 1 \ 2 \ 0)$, $- (1 \ 1 \ 1 \ 1)]$, $- (1 \ 1 \ 1 \ 0)$, $- (1 \ 1 \ 0 \ 0)$, $- (1 \ 0 \ 0 \ 0)$.

Moreover, whenever $\beta + \alpha_1 + \dots + \alpha_k$ is a root, $k \leq 4$, it is among the roots expressible in terms of the system $\alpha_2, \alpha_3, \alpha_4$ of type C_3 . By Th. 11.1, it is given in the statement of that theorem. But all such quantities are included in the statement of this theorem.

$\gamma = \pm (2 \ 3 \ 4 \ 2)$: Here $\beta = \gamma$, and $\alpha = \beta$.

This completes the proof of the theorem.

XIV. SYSTEMS OF TYPE E

THEOREM 14.1. Let $\alpha_1, \dots, \alpha_r$ be an i.s.s. of type E, and let α be a root dependent on $\alpha_1, \dots, \alpha_r$. Then α is one of the roots listed below for the corresponding value of r , or one of their negatives:

E_6 : $(1 \ 0 \ 0 \ 0 \ 0 \ 0)$, $(0 \ 1 \ 0 \ 0 \ 0 \ 0)$, $(0 \ 0 \ 1 \ 0 \ 0 \ 0)$, $(0 \ 0 \ 0 \ 1 \ 0 \ 0)$,
 $(0 \ 0 \ 0 \ 0 \ 1 \ 0)$, $(0 \ 0 \ 0 \ 0 \ 0 \ 1)$, $(1 \ 1 \ 0 \ 0 \ 0 \ 0)$, $(0 \ 1 \ 1 \ 0 \ 0 \ 0)$,
 $(0 \ 0 \ 1 \ 1 \ 0 \ 0)$, $(0 \ 0 \ 0 \ 1 \ 1 \ 0)$, $(0 \ 0 \ 1 \ 0 \ 0 \ 1)$, $(1 \ 1 \ 1 \ 0 \ 0 \ 0)$,
 $(0 \ 1 \ 1 \ 1 \ 0 \ 0)$, $(0 \ 0 \ 1 \ 1 \ 1 \ 0)$, $(0 \ 1 \ 1 \ 0 \ 0 \ 1)$, $(0 \ 0 \ 1 \ 1 \ 0 \ 1)$,
 $(1 \ 1 \ 1 \ 1 \ 0 \ 0)$, $(0 \ 1 \ 1 \ 1 \ 1 \ 0)$, $(1 \ 1 \ 1 \ 0 \ 0 \ 1)$, $(0 \ 0 \ 1 \ 1 \ 1 \ 1)$,
 $(0 \ 1 \ 1 \ 1 \ 0 \ 1)$, $(0 \ 1 \ 2 \ 1 \ 0 \ 1)$, $(1 \ 1 \ 1 \ 1 \ 1 \ 0)$, $(1 \ 1 \ 1 \ 1 \ 0 \ 1)$,
 $(1 \ 1 \ 2 \ 1 \ 0 \ 1)$, $(1 \ 2 \ 2 \ 1 \ 0 \ 1)$, $(0 \ 1 \ 1 \ 1 \ 1 \ 1)$, $(0 \ 1 \ 2 \ 1 \ 1 \ 1)$,
 $(0 \ 1 \ 2 \ 2 \ 1 \ 1)$, $(1 \ 1 \ 1 \ 1 \ 1 \ 1)$, $(1 \ 1 \ 2 \ 1 \ 1 \ 1)$, $(1 \ 1 \ 2 \ 2 \ 1 \ 1)$,
 $(1 \ 2 \ 2 \ 1 \ 1 \ 1)$, $(1 \ 2 \ 2 \ 2 \ 1 \ 1)$, $(1 \ 2 \ 3 \ 2 \ 1 \ 1)$, $(1 \ 2 \ 3 \ 2 \ 1 \ 2)$.

There are 72 roots in all.

E_7 : (1 0 0 0 0 0 0), (0 1 0 0 0 0 0), (0 0 1 0 0 0 0), (0 0 0 1 0 0 0),
 (0 0 0 0 1 0 0), (0 0 0 0 0 1 0), (0 0 0 0 0 0 1), (1 1 0 0 0 0 0),
 (0 1 1 0 0 0 0), (0 0 1 1 0 0 0), (0 0 0 1 1 0 0), (0 0 0 0 1 1 0),
 (0 0 0 1 0 0 1), (1 1 1 0 0 0 0), (0 1 1 1 0 0 0), (0 0 1 1 1 0 0),
 (0 0 0 1 1 1 0), (0 0 1 1 0 0 1), (0 0 0 1 1 0 1), (1 1 1 1 0 0 0),
 (0 1 1 1 1 0 0), (0 0 1 1 1 1 0), (0 1 1 1 0 0 1), (0 0 0 1 1 1 1),
 (0 0 1 1 1 0 1), (0 0 1 2 1 0 1), (1 1 1 1 1 0 0), (0 1 1 1 1 1 0),
 (1 1 1 1 0 0 1), (0 1 1 1 1 0 1), (0 1 1 2 1 0 1), (0 1 2 2 1 0 1),
 (0 0 1 1 1 1 1), (0 0 1 2 1 1 1), (0 0 1 2 2 1 1), (1 1 1 1 1 1 0),
 (1 1 1 1 1 0 1), (1 1 1 2 1 0 1), (1 1 2 2 1 0 1), (1 2 2 2 1 0 1),
 (0 1 1 1 1 1 1), (0 1 1 2 1 1 1), (0 1 2 2 1 1 1), (0 1 1 2 2 1 1),
 (0 1 2 2 2 1 1), (0 1 2 3 2 1 1), (0 1 2 3 2 1 2), (1 1 1 1 1 1 1),
 (1 1 1 2 1 1 1), (1 1 2 2 1 1 1), (1 1 1 2 2 1 1), (1 2 2 2 1 1 1),
 (1 1 2 2 2 1 1), (1 1 2 3 2 1 1), (1 2 2 2 2 1 1), (1 2 2 3 2 1 1),
 (1 1 2 3 2 1 2), (1 2 3 3 2 1 1), (1 2 2 3 2 1 2), (1 2 3 3 2 1 2),
 (1 2 3 4 2 1 2), (1 2 3 4 3 1 2), (1 2 3 4 3 2 2).

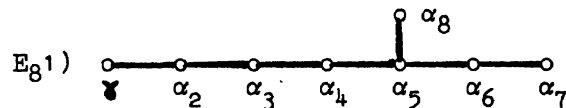
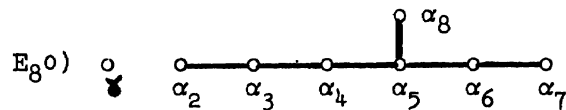
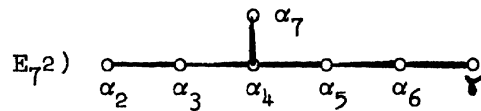
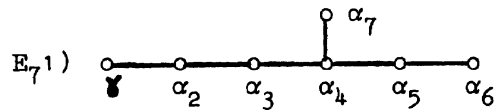
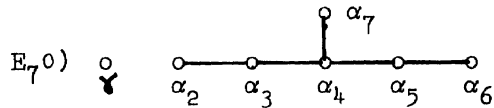
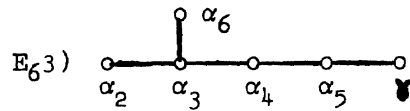
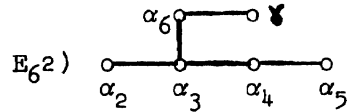
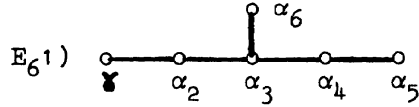
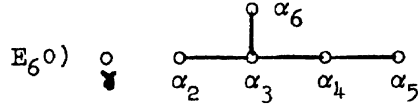
There are 126 roots in all.

E_8 : (1 0 0 0 0 0 0 0), (0 1 0 0 0 0 0 0), (0 0 1 0 0 0 0 0),
 (0 0 0 1 0 0 0 0), (0 0 0 0 1 0 0 0), (0 0 0 0 0 1 0 0),
 (0 0 0 0 0 0 1 0), (0 0 0 0 0 0 0 1), (1 1 0 0 0 0 0 0),
 (0 1 1 0 0 0 0 0), (0 0 1 1 0 0 0 0), (0 0 0 1 1 0 0 0),
 (0 0 0 0 1 1 0 0), (0 0 0 0 0 1 1 0), (0 0 0 0 1 0 0 1),
 (1 1 1 0 0 0 0 0), (0 1 1 1 0 0 0 0), (0 0 1 1 1 0 0 0),
 (0 0 0 1 1 1 0 0), (0 0 0 0 1 1 1 0), (0 0 0 1 1 0 0 1),
 (0 0 0 0 1 1 0 1), (1 1 1 1 0 0 0 0), (0 1 1 1 1 0 0 0),
 (0 0 1 1 1 1 0 0), (0 0 0 1 1 1 1 0), (0 0 1 1 1 0 0 1),
 (0 0 0 0 1 1 1 1), (0 0 0 1 1 1 0 1), (0 0 0 1 2 1 0 1),
 (1 1 1 1 1 0 0 0), (0 1 1 1 1 1 0 0), (0 0 1 1 1 1 1 0),
 (0 1 1 1 1 0 0 1), (0 0 1 1 1 1 0 1), (0 0 1 1 2 1 0 1),

(0 0 1 2 2 1 0 1), (0 0 0 1 1 1 1 1), (0 0 0 1 2 1 1 1),
 (0 0 0 1 2 2 1 1), (1 1 1 1 1 1 0 0), (0 1 1 1 1 1 1 0),
 (1 1 1 1 1 0 0 1), (0 1 1 1 1 1 0 1), (0 1 1 1 2 1 0 1),
 (0 1 1 2 2 1 0 1), (0 1 2 2 2 1 0 1), (0 0 1 1 1 1 1 1),
 (0 0 1 1 2 1 1 1), (0 0 1 2 2 1 1 1), (0 0 1 1 2 2 1 1),
 (0 0 1 2 2 2 1 1), (0 0 1 2 3 2 1 1), (0 0 1 2 3 2 1 2),
 (1 1 1 1 1 1 1 0), (1 1 1 1 1 1 0 1), (1 1 1 1 2 1 0 1),
 (1 1 1 2 2 1 0 1), (1 1 2 2 2 1 0 1), (1 2 2 2 2 1 0 1),
 (0 1 1 1 1 1 1 1), (0 1 1 1 2 1 1 1), (0 1 1 2 2 1 1 1),
 (0 1 1 1 2 2 1 1), (0 1 2 2 2 1 1 1), (0 1 1 2 2 2 1 1),
 (0 1 1 2 3 2 1 1), (0 1 1 2 3 2 1 2), (0 1 2 2 2 2 1 1),
 (0 1 2 2 3 2 1 1), (0 1 2 3 3 2 1 1), (0 1 2 2 3 2 1 2),
 (0 1 2 3 3 2 1 2), (0 1 2 3 4 2 1 2), (0 1 2 3 4 3 1 2),
 (0 1 2 3 4 3 2 2), (1 1 1 1 1 1 1 1), (1 1 1 1 2 1 1 1),
 (1 1 1 2 2 1 1 1), (1 1 1 1 2 2 1 1), (1 1 2 2 2 1 1 1),
 (1 1 1 2 2 2 1 1), (1 2 2 2 2 1 1 1), (1 1 2 2 2 2 1 1),
 (1 1 1 2 3 2 1 1), (1 2 2 2 2 2 1 1), (1 1 2 2 3 2 1 1),
 (1 1 1 2 3 2 1 2), (1 2 2 2 3 2 1 1), (1 1 2 2 3 2 1 2),
 (1 1 2 3 3 2 1 1), (1 2 2 2 3 2 1 2), (1 2 2 3 3 2 1 1),
 (1 1 2 3 3 2 1 2), (1 2 2 3 3 2 1 2), (1 2 3 3 3 2 1 1),
 (1 1 2 3 4 2 1 2), (1 2 3 3 3 2 1 2), (1 2 2 3 4 2 1 2),
 (1 1 2 3 4 3 1 2), (1 2 3 3 4 2 1 2), (1 2 2 3 4 3 1 2),
 (1 1 2 3 4 3 2 2), (1 2 3 4 4 2 1 2), (1 2 3 3 4 3 1 2),
 (1 2 2 3 4 3 2 2), (1 2 3 4 4 3 1 2), (1 2 3 3 4 3 2 2),
 (1 2 3 4 5 3 1 2), (1 2 3 4 4 3 2 2), (1 2 3 4 5 3 2 2),
 (1 2 3 4 5 3 1 3), (1 2 3 4 5 4 2 2), (1 2 3 4 5 3 2 3),
 (1 2 3 4 5 4 2 3), (1 2 3 4 6 4 2 3), (1 2 3 5 6 4 2 3)
 (1 2 4 5 6 4 2 3), (1 3 4 5 6 4 2 3), (2 3 4 5 6 4 2 3),

There are 240 roots in all.

PROOF. As in the proof of Th. 9.1, we can obtain from the given root α (or its negative) a root β with non-zero first coefficient, and from β a root γ such that $\gamma, \alpha_2, \dots, \alpha_r$ form a simple system. This is one of the following:



Let $\gamma = (\lambda_1 \dots \lambda_r)$, and assume for the present that $\gamma \neq \alpha_1$.

$$E_6^0) \quad \lambda_5 = \frac{2}{3} \lambda_6, \quad \lambda_4 = \frac{4}{3} \lambda_6, \quad \lambda_3 = 2 \lambda_6, \quad \lambda_2 = \frac{5}{3} \lambda_6, \quad \lambda_6 = A_{\gamma,1}.$$

$A_{\gamma,1} = -1$: $\lambda_6 = -1$, $\lambda_1 = -\frac{4}{3}$; $2 = A_{\gamma,\gamma} = -\frac{4}{3} A_{1,\gamma} = \frac{4}{3}, \frac{8}{3}$ or 4 ; each of these is impossible.

$$A_{\gamma,1} = -2: \quad \lambda_1 = -\frac{8}{3}; \quad 2 = -\frac{8}{3} A_{1,\gamma} = \frac{8}{3}, \quad \text{a contradiction.}$$

$$A_{\gamma,1} = -3: \quad \lambda_1 = -4; \quad 2 = -4 A_{1,\gamma} = 4, \quad \text{a contradiction.}$$

$$A_{\gamma,1} = 0: \quad \gamma = 0, \quad \text{contrary to assumption.}$$

Since $A_{\gamma,1} = 1, 2, 3$ give the negatives of the quantities shown impossible above, they are also impossible.

$$E_6^1) \quad (A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0) \text{ or } (-1, -1). \quad \lambda_5 = \frac{2}{3} \lambda_6,$$

$$\lambda_4 = \frac{4}{3} \lambda_6, \quad \lambda_3 = 2 \lambda_6, \quad \lambda_2 = \frac{5}{3} \lambda_6, \quad \lambda_1 = \frac{4}{3} \lambda_6 + 1, \quad \lambda_6 = A_{\gamma,1} - 2.$$

$$A_{\gamma,1} = 1: \quad \lambda_1 = -\frac{1}{3}, \quad \lambda_2 = -\frac{5}{3}; \quad 2 = A_{\gamma,\gamma} = -\frac{1}{3} A_{1,\gamma} - \frac{5}{3} A_{2,\gamma} = \frac{4}{3},$$

and this is impossible.

$$A_{\gamma,1} = 0: \quad \lambda_2 = -\frac{10}{3}; \quad 2 = A_{\gamma,\gamma} = -\frac{10}{3} A_{2,\gamma} = \frac{10}{3}, \quad \text{impossible.}$$

$$A_{\gamma,1} = -1: \quad \lambda_1 = -3, \quad \lambda_2 = -5; \quad 2 = A_{\gamma,\gamma} = -3 A_{1,\gamma} - 5 A_{2,\gamma} = 8,$$

impossible.

$$E_6^2) \quad (A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0) \text{ or } (-1, -1). \quad \lambda_5 = \frac{2}{3} \lambda_6 + \frac{1}{3},$$

$$\lambda_4 = 2 \lambda_5, \quad \lambda_3 = 3 \lambda_5, \quad \lambda_2 = \frac{5}{3} \lambda_6 + \frac{4}{3}, \quad \lambda_1 = \frac{4}{3} \lambda_6 + \frac{5}{3}, \quad \lambda_6 = A_{\gamma,1} - 2.$$

$$A_{\gamma,1} = 1: \quad \lambda_6 = -1, \quad \lambda_1 = \frac{1}{3}; \quad 2 = A_{\gamma,\gamma} = \frac{1}{3} A_{1,\gamma} - A_{6,\gamma} = \frac{4}{3},$$

impossible.

$$A_{\gamma,1} = 0: \quad \gamma = -(1 \ 2 \ 3 \ 2 \ 1 \ 2).$$

$$A_{\gamma,1} = -1: \quad \lambda_6 = -3, \quad \lambda_1 = -\frac{7}{3}; \quad 2 = A_{\gamma,\gamma} = -\frac{7}{3} A_{1,\gamma} - 3 A_{6,\gamma} = \frac{16}{3},$$

which is impossible.

$$E_6^3) \quad (A_{\gamma,1}, A_{1,\gamma}) = (1, 1), (0, 0) \text{ or } (-1, -1). \quad \lambda_5 = \frac{2}{3} \lambda_6 - \frac{2}{3},$$

$$\lambda_4 = \frac{4}{3} \lambda_6 - \frac{1}{3}, \quad \lambda_3 = 2 \lambda_6, \quad \lambda_2 = \frac{5}{3} \lambda_6 + \frac{1}{3}, \quad \lambda_1 = \frac{4}{3} \lambda_6 + \frac{2}{3}, \quad \lambda_6 = A_{\gamma,1} - 1.$$

$$A_{\gamma,1} = 1: \quad \lambda_5 = -\frac{2}{3}, \quad \lambda_1 = \frac{2}{3}; \quad 2 = \frac{2}{3} A_{1,\gamma} - \frac{2}{3} A_{5,\gamma} = \frac{4}{3}, \quad \text{impossible.}$$

$$A_{\gamma,1} = 0: \quad \lambda_5 = -\frac{4}{3}; \quad 2 = -\frac{4}{3} A_{5,\gamma} = \frac{4}{3}, \quad \text{impossible.}$$

$$A_{\gamma,1} = -1: \quad \lambda_5 = -2 = \lambda_1; \quad 2 = -2 A_{1,\gamma} - 2 A_{5,\gamma} = 4, \quad \text{impossible.}$$

Thus either $\gamma = \alpha_1$ or $\gamma = -(1 \ 2 \ 3 \ 2 \ 1 \ 2)$.

$\gamma = \alpha_1$: With the convention of Th. 9.1, β is among:

$$(1 \ 0 \ 0 \ 0 \ 0 \ 0), (1 \ 1 \ 0 \ 0 \ 0 \ 0), (1 \ 1 \ 1 \ 0 \ 0 \ 0) [(1 \ 1 \ 1 \ 1 \ 0 \ 0),$$

(1 1 1 0 0 1)], [(1 1 1 1 1 0), (1 1 1 1 0 1)], [(1 1 1 1 1 1), (1 1 2 1 0 1)], [(1 1 2 1 1 1), (1 2 2 1 0 1)], [(1 2 2 1 1 1), (1 1 2 2 1 1)], (1 2 2 2 1 1), (1 2 3 2 1 1), (1 2 3 2 1 2).

As before, $\alpha = \beta$.

$\gamma = -(1 2 3 2 1 2)$: β is among the following:

$-(1 2 3 2 1 2)$, $-(1 2 3 2 1 1)$, $-(1 2 2 2 1 1)$, $[-(1 2 2 1 1 1)$,
 $-(1 1 2 2 1 1)]$, $[-(1 1 2 1 1 1)$, $-(1 2 2 1 0 1)]$, $[-(1 1 1 1 1 1)$,
 $-(1 1 2 1 0 1)]$, $[-(1 1 1 1 1 0)$, $-(1 1 1 1 0 1)]$, $[-(1 1 1 1 0 0)$,
 $-(1 1 1 0 0 1)]$, $-(1 1 1 0 0 0)$, $-(1 1 0 0 0 0)$, $-(1 0 0 0 0 0)$.

If $\alpha = \beta$, the theorem holds for α . Otherwise, $\beta + \alpha_1$ is a root; this is only the case when $\beta = -(1 1 2 2 1 1)$, $-(1 1 2 1 1 1)$, $-(1 1 1 1 1 1)$, $-(1 1 2 1 0 1)$, $-(1 1 1 1 1 0)$, $-(1 1 1 1 0 1)$, $-(1 1 1 1 0 0)$, $-(1 1 1 0 0 1)$, $-(1 1 1 0 0 0)$, $-(1 1 0 0 0 0)$. In each case, the theorem holds if $\alpha = \beta + \alpha_1$. Otherwise $\beta + \alpha_1 + \alpha_2$ is a root, and we continue to apply this reasoning to show that the theorem holds for α in any case.

$$E_7 0) \text{ Assume } \gamma \neq \alpha_1. \quad \lambda_6 = \frac{2}{3} \lambda_7, \quad \lambda_5 = \frac{4}{3} \lambda_7, \quad \lambda_4 = 2 \lambda_7, \\ \lambda_3 = \frac{5}{3} \lambda_7, \quad \lambda_2 = \frac{4}{3} \lambda_7, \quad \lambda_1 = \lambda_7 = \frac{3}{2} A_{\gamma, 1}.$$

$$A_{\gamma, 1} = 0: \gamma = 0, \text{ impossible.}$$

$$A_{\gamma, 1} = -1: \lambda_1 = -\frac{3}{2}; 2 = -\frac{3}{2} A_{1, \gamma} = \frac{3}{2}, 3 \text{ or } \frac{9}{2}, \text{ impossible.}$$

$$A_{\gamma, 1} = -2: \lambda_1 = -3; 2 = -3 A_{1, \gamma} = 3, \text{ impossible.}$$

$$A_{\gamma, 1} = -3: \lambda_1 = -\frac{9}{2}; 2 = -\frac{9}{2} A_{1, \gamma} = \frac{9}{2}, \text{ impossible.}$$

As in previous cases, the above implies that $A_{\gamma, 1} = 1, 2, 3$ are impossible.

$$E_7 1) (A_{\gamma, 1}, A_{1, \gamma}) = (1, 1), (0, 0) \text{ or } (-1, -1). \quad \lambda_6 = \frac{2}{3} \lambda_7, \\ \lambda_5 = \frac{4}{3} \lambda_7, \quad \lambda_4 = 2 \lambda_7, \quad \lambda_3 = \frac{5}{3} \lambda_7, \quad \lambda_2 = \frac{4}{3} \lambda_7, \quad \lambda_1 = \lambda_7 + 1, \\ \lambda_7 = \frac{3}{2} (A_{\gamma, 1} - 2).$$

$$A_{\gamma, 1} = 1: \lambda_1 = -\frac{1}{2}, \quad \lambda_2 = -2; 2 = -\frac{1}{2} A_{1, \gamma} - 2 A_{2, \gamma} = \frac{3}{2}, \text{ impossible.}$$

$$A_{\gamma, 1} = 0: \lambda_2 = -4; 2 = -4 A_{2, \gamma} = 4, \text{ impossible.}$$

$$A_{\gamma, 1} = -1: \lambda_1 = -\frac{7}{2}, \quad \lambda_2 = -6; 2 = -\frac{7}{2} A_{1, \gamma} - 6 A_{2, \gamma} = \frac{19}{2}, \\ \text{impossible.}$$

$$E_7 2) (A_{\gamma, 1}, A_{1, \gamma}) = (1, 1), (0, 0) \text{ or } (-1, -1). \quad \lambda_6 = \frac{2}{3} \lambda_7 - \frac{2}{3},$$

$$\lambda_5 = \frac{4}{3} \lambda_7 - \frac{1}{3}, \quad \lambda_4 = 2 \lambda_7, \quad \lambda_3 = \frac{5}{3} \lambda_7 + \frac{1}{3}, \quad \lambda_2 = \frac{4}{3} \lambda_7 + \frac{2}{3},$$

$$\lambda_1 = \lambda_7 + 1, \quad \lambda_7 = \frac{3}{2} A_{\gamma,1} - 2.$$

$$A_{\gamma,1} = 1: \lambda_6 = -1, \quad \lambda_1 = \frac{1}{2}; \quad 2 = \frac{1}{2} A_{1,\gamma} - A_{6,\gamma} = \frac{3}{2}, \quad \text{impossible.}$$

$$A_{\gamma,1} = 0: \gamma = - (1 \ 2 \ 3 \ 4 \ 3 \ 2 \ 2).$$

$$A_{\gamma,1} = -1: \lambda_6 = -3, \quad \lambda_1 = -\frac{5}{2}; \quad 2 = -\frac{5}{2} A_{1,\gamma} - 3A_{6,\gamma} = \frac{11}{2},$$

impossible.

Thus either $\gamma = \alpha_1$ or $\gamma = - (1 \ 2 \ 3 \ 4 \ 3 \ 2 \ 2)$.

$\gamma = \alpha_1$: β is among the following roots:

$$(1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0), (1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0), (1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0), (1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0),$$

$$[(1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0), (1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1)], [(1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0), (1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1)],$$

$$[(1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1), (1 \ 1 \ 1 \ 2 \ 1 \ 0 \ 1)], [(1 \ 1 \ 1 \ 2 \ 1 \ 1 \ 1), (1 \ 1 \ 2 \ 2 \ 1 \ 0 \ 1)],$$

$$[(1 \ 1 \ 1 \ 2 \ 2 \ 1 \ 1), (1 \ 1 \ 2 \ 2 \ 1 \ 1 \ 1), (1 \ 2 \ 2 \ 2 \ 1 \ 0 \ 1)],$$

$$[(1 \ 1 \ 2 \ 2 \ 2 \ 1 \ 1), (1 \ 2 \ 2 \ 2 \ 1 \ 1 \ 1)], [(1 \ 2 \ 2 \ 2 \ 2 \ 1 \ 1), (1 \ 1 \ 2 \ 3 \ 2 \ 1 \ 1)],$$

$$[(1 \ 2 \ 2 \ 3 \ 2 \ 1 \ 1), (1 \ 1 \ 2 \ 3 \ 2 \ 1 \ 2)], [(1 \ 2 \ 3 \ 3 \ 2 \ 1 \ 1), (1 \ 2 \ 2 \ 3 \ 2 \ 1 \ 2)],$$

$$(1 \ 2 \ 3 \ 3 \ 2 \ 1 \ 2), (1 \ 2 \ 3 \ 4 \ 2 \ 1 \ 2), (1 \ 2 \ 3 \ 4 \ 3 \ 1 \ 2), (1 \ 2 \ 3 \ 4 \ 3 \ 2 \ 2).$$

The grouping in brackets follows the established rule, and $\alpha = \beta$.

$\gamma = -(1 \ 2 \ 3 \ 4 \ 3 \ 2 \ 2)$: β is among the following roots:

$$-(1 \ 2 \ 3 \ 4 \ 3 \ 2 \ 2), -(1 \ 2 \ 3 \ 4 \ 3 \ 1 \ 2), -(1 \ 2 \ 3 \ 4 \ 2 \ 1 \ 2),$$

$$-(1 \ 2 \ 3 \ 3 \ 2 \ 1 \ 2), [-(1 \ 2 \ 2 \ 3 \ 2 \ 1 \ 2), -(1 \ 2 \ 3 \ 3 \ 2 \ 1 \ 1)],$$

$$[(1 \ 1 \ 2 \ 3 \ 2 \ 1 \ 2), -(1 \ 2 \ 2 \ 3 \ 2 \ 1 \ 1)], [-(1 \ 1 \ 2 \ 3 \ 2 \ 1 \ 1),$$

$$-(1 \ 2 \ 2 \ 2 \ 2 \ 1 \ 1)], [-(1 \ 1 \ 2 \ 2 \ 2 \ 1 \ 1), -(1 \ 2 \ 2 \ 2 \ 1 \ 1 \ 1)],$$

$$[-(1 \ 1 \ 1 \ 2 \ 2 \ 1 \ 1), -(1 \ 1 \ 2 \ 2 \ 1 \ 1 \ 1), -(1 \ 2 \ 2 \ 2 \ 1 \ 0 \ 1)],$$

$$[-(1 \ 1 \ 1 \ 2 \ 1 \ 1 \ 1), -(1 \ 1 \ 2 \ 2 \ 1 \ 0 \ 1)], [-(1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1),$$

$$-(1 \ 1 \ 1 \ 2 \ 1 \ 0 \ 1)], [-(1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0), -(1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1)],$$

$$[-(1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0), -(1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1)], -(1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0),$$

$$-(1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0), -(1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0), -(1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0).$$

If $\alpha = \beta$, α is among the roots given in the statement of the theorem. If $\alpha = \beta + \alpha_1 + \dots + \alpha_k$, α is a linear combination of $\alpha_2, \dots, \alpha_7$, a system of type E_6 , and therefore is among the roots given in the statement of the theorem for systems of type E_6 . All such roots are also given under the heading E_7 . Thus the theorem is true for

systems of type E_7 .

E_{80}) $\lambda_7 = \frac{2}{3} \lambda_8$, $\lambda_6 = \frac{4}{3} \lambda_8$, $\lambda_5 = 2 \lambda_8$, $\lambda_4 = \frac{5}{3} \lambda_8$, $\lambda_3 = \frac{4}{3} \lambda_8$,
 $\lambda_2 = \lambda_8$, $\lambda_1 = \frac{2}{3} \lambda_8$, $\lambda_8 = 3A_{\gamma,1}$. $\gamma = A_{\gamma,1}(2\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$. Since
 $(2\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$ is readily shown to be a root, $A_{\gamma,1} = \pm 1$.

E_{81}) If $\gamma \neq \alpha_1$, $(A_{\gamma,1}, A_{1,\gamma}) = (1, 1)$, $(0, 0)$ or $(-1, -1)$.
 $\lambda_7 = \frac{2}{3} \lambda_8$, $\lambda_6 = \frac{4}{3} \lambda_8$, $\lambda_5 = 2 \lambda_8$, $\lambda_4 = \frac{5}{3} \lambda_8$, $\lambda_3 = \frac{4}{3} \lambda_8$,
 $\lambda_1 = \frac{2}{3} \lambda_8 + 1$, $\lambda_8 = 3A_{\gamma,1} - 6$.

$A_{\gamma,1} = 1$: $\gamma = -(1\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$.

$A_{\gamma,1} = 0$: $\lambda_2 = -6$; $2 = -6A_{2,\gamma} = 6$, impossible.

$A_{\gamma,1} = -1$: $\lambda_2 = -9$, $\lambda_1 = -5$; $2 = -5A_{1,\gamma} - 9A_{2,\gamma} = 14$, impossible

Thus γ is among $\pm(2\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$, $-(1\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$ and α_1 .

$\gamma = \pm(2\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$: $\alpha = \beta = \gamma$ is among the roots listed.

$\gamma = -(1\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$: β is among the following roots:

$-(1\ 3\ 4\ 5\ 6\ 4\ 2\ 3)$, $-(1\ 2\ 4\ 5\ 6\ 4\ 2\ 3)$, $-(1\ 2\ 3\ 5\ 6\ 4\ 2\ 3)$,
 $-(1\ 2\ 3\ 4\ 6\ 4\ 2\ 3)$, $-(1\ 2\ 3\ 4\ 5\ 4\ 2\ 3)$, $[-(1\ 2\ 3\ 4\ 5\ 3\ 2\ 3)]$,
 $-(1\ 2\ 3\ 4\ 5\ 4\ 2\ 2)$, $[-(1\ 2\ 3\ 4\ 5\ 3\ 1\ 3)]$, $-(1\ 2\ 3\ 4\ 5\ 3\ 2\ 2)$,
 $[-(1\ 2\ 3\ 4\ 5\ 3\ 1\ 2)]$, $[-(1\ 2\ 3\ 4\ 4\ 3\ 2\ 2)]$,
 $[-(1\ 2\ 3\ 4\ 4\ 3\ 1\ 2)]$, $[-(1\ 2\ 3\ 3\ 4\ 3\ 2\ 2)]$,
 $[-(1\ 2\ 2\ 3\ 4\ 3\ 1\ 2)]$, $[-(1\ 2\ 3\ 3\ 4\ 2\ 1\ 2)]$, $[-(1\ 1\ 2\ 3\ 4\ 3\ 2\ 2)]$,
 $[-(1\ 1\ 2\ 3\ 4\ 3\ 1\ 2)]$, $[-(1\ 2\ 2\ 3\ 4\ 2\ 1\ 2)]$, $[-(1\ 2\ 3\ 3\ 3\ 2\ 1\ 2)]$,
 $[-(1\ 1\ 2\ 3\ 4\ 2\ 1\ 2)]$, $[-(1\ 2\ 2\ 3\ 3\ 2\ 1\ 2)]$, $[-(1\ 2\ 3\ 3\ 3\ 2\ 1\ 1)]$,
 $[-(1\ 1\ 2\ 3\ 3\ 2\ 1\ 2)]$, $[-(1\ 2\ 2\ 3\ 2\ 1\ 2)]$, $[-(1\ 2\ 2\ 3\ 3\ 2\ 1\ 1)]$,
 $[-(1\ 1\ 2\ 2\ 3\ 2\ 1\ 2)]$, $[-(1\ 1\ 2\ 3\ 3\ 2\ 1\ 1)]$, $[-(1\ 2\ 2\ 2\ 3\ 2\ 1\ 1)]$,
 $[-(1\ 1\ 1\ 2\ 3\ 2\ 1\ 2)]$, $[-(1\ 1\ 2\ 2\ 3\ 2\ 1\ 1)]$, $[-(1\ 2\ 2\ 2\ 2\ 2\ 1\ 1)]$,
 $[-(1\ 1\ 1\ 2\ 3\ 2\ 1\ 1)]$, $[-(1\ 1\ 2\ 2\ 2\ 2\ 1\ 1)]$, $[-(1\ 2\ 2\ 2\ 2\ 1\ 1\ 1)]$,
 $[-(1\ 1\ 1\ 2\ 2\ 2\ 1\ 1)]$, $[-(1\ 1\ 2\ 2\ 2\ 1\ 1\ 1)]$, $[-(1\ 2\ 2\ 2\ 2\ 1\ 0\ 1)]$,
 $[-(1\ 1\ 1\ 1\ 2\ 2\ 1\ 1)]$, $[-(1\ 1\ 1\ 2\ 2\ 1\ 1\ 1)]$, $[-(1\ 1\ 2\ 2\ 2\ 1\ 0\ 1)]$,
 $[-(1\ 1\ 1\ 1\ 2\ 1\ 1\ 1)]$, $[-(1\ 1\ 1\ 2\ 2\ 1\ 0\ 1)]$, $[-(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)]$,
 $[-(1\ 1\ 1\ 1\ 2\ 1\ 0\ 1)]$, $[-(1\ 1\ 1\ 1\ 1\ 1\ 1\ 0)]$, $[-(1\ 1\ 1\ 1\ 1\ 1\ 0\ 1)]$,

$$\begin{aligned} &[-(1\ 1\ 1\ 1\ 1\ 1\ 0\ 0), -(1\ 1\ 1\ 1\ 1\ 0\ 0\ 1)], -(1\ 1\ 1\ 1\ 1\ 0\ 0\ 0), \\ &-(1\ 1\ 1\ 1\ 0\ 0\ 0\ 0), -(1\ 1\ 1\ 0\ 0\ 0\ 0\ 0), -(1\ 1\ 0\ 0\ 0\ 0\ 0\ 0), \\ &-(1\ 0\ 0\ 0\ 0\ 0\ 0\ 0) = -\alpha_1. \end{aligned}$$

Either $\alpha = \beta$ or α is expressible in terms of the system $\alpha_2, \dots, \alpha_8$ of type E_7 . In either case, α is among the roots of the statement of the theorem.

$\forall = \alpha_1$: $\alpha = \beta$ is among the following roots:

$$\begin{aligned} &(1\ 0\ 0\ 0\ 0\ 0\ 0\ 0), (1\ 1\ 0\ 0\ 0\ 0\ 0\ 0), (1\ 1\ 1\ 0\ 0\ 0\ 0\ 0), \\ &(1\ 1\ 1\ 1\ 0\ 0\ 0\ 0), (1\ 1\ 1\ 1\ 1\ 0\ 0\ 0), [(1\ 1\ 1\ 1\ 1\ 1\ 0\ 0), \\ &(1\ 1\ 1\ 1\ 1\ 0\ 0\ 1)], [(1\ 1\ 1\ 1\ 1\ 1\ 1\ 0), (1\ 1\ 1\ 1\ 1\ 1\ 0\ 1)], \\ &[(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1), (1\ 1\ 1\ 1\ 2\ 1\ 0\ 1)], \\ &[(1\ 1\ 1\ 1\ 2\ 1\ 1\ 1), (1\ 1\ 1\ 2\ 2\ 1\ 0\ 1)], \\ &[(1\ 1\ 1\ 2\ 2\ 1\ 1\ 1), (1\ 1\ 1\ 1\ 2\ 2\ 1\ 1), (1\ 1\ 2\ 2\ 2\ 1\ 0\ 1)], \\ &[(1\ 1\ 2\ 2\ 2\ 1\ 1\ 1), (1\ 1\ 1\ 2\ 2\ 2\ 1\ 1), (1\ 2\ 2\ 2\ 2\ 1\ 0\ 1)], \\ &[(1\ 2\ 2\ 2\ 2\ 1\ 1\ 1), (1\ 1\ 2\ 2\ 2\ 2\ 1\ 1), (1\ 1\ 1\ 2\ 3\ 2\ 1\ 1)], \\ &[(1\ 2\ 2\ 2\ 2\ 2\ 1\ 1), (1\ 1\ 2\ 2\ 3\ 2\ 1\ 1), (1\ 1\ 1\ 2\ 3\ 2\ 1\ 2)], \\ &[(1\ 2\ 2\ 2\ 3\ 2\ 1\ 1), (1\ 1\ 2\ 3\ 3\ 2\ 1\ 1), (1\ 1\ 2\ 2\ 3\ 2\ 1\ 2)], \\ &[(1\ 2\ 2\ 3\ 3\ 2\ 1\ 1), (1\ 1\ 2\ 3\ 3\ 2\ 1\ 2), (1\ 2\ 2\ 2\ 3\ 2\ 1\ 2)], \\ &[(1\ 2\ 3\ 3\ 3\ 2\ 1\ 1), (1\ 2\ 2\ 3\ 3\ 2\ 1\ 2), (1\ 1\ 2\ 3\ 4\ 2\ 1\ 2)], \\ &[(1\ 2\ 3\ 3\ 3\ 2\ 1\ 2), (1\ 2\ 2\ 3\ 4\ 2\ 1\ 2), (1\ 1\ 2\ 3\ 4\ 3\ 1\ 2)], \\ &[(1\ 2\ 3\ 3\ 4\ 2\ 1\ 2), (1\ 2\ 2\ 3\ 4\ 3\ 1\ 2), (1\ 1\ 2\ 3\ 4\ 3\ 2\ 2)], \\ &[(1\ 2\ 3\ 4\ 4\ 2\ 1\ 2), (1\ 2\ 3\ 3\ 4\ 3\ 1\ 2), (1\ 2\ 2\ 3\ 4\ 3\ 2\ 2)], \\ &[(1\ 2\ 3\ 4\ 4\ 3\ 1\ 2), (1\ 2\ 3\ 3\ 4\ 3\ 2\ 2)], [(1\ 2\ 3\ 4\ 5\ 3\ 1\ 2), \\ &(1\ 2\ 3\ 4\ 4\ 3\ 2\ 2)], [(1\ 2\ 3\ 4\ 5\ 3\ 2\ 2), (1\ 2\ 3\ 4\ 5\ 3\ 1\ 3)], \\ &[(1\ 2\ 3\ 4\ 5\ 4\ 2\ 2), (1\ 2\ 3\ 4\ 5\ 3\ 2\ 3)], (1\ 2\ 3\ 4\ 5\ 4\ 2\ 3), \\ &(1\ 2\ 3\ 4\ 6\ 4\ 2\ 3), (1\ 2\ 3\ 5\ 6\ 4\ 2\ 3), (1\ 2\ 4\ 5\ 6\ 4\ 2\ 3), \\ &(1\ 3\ 4\ 5\ 6\ 4\ 2\ 3). \end{aligned}$$

Then $\alpha = \beta$, and α is listed in the statement of the theorem. Thus the proof of Th. 14.1 is complete.

XV. MAXIMAL SIMPLE SYSTEMS

THEOREM 15.1. Let $\alpha_1, \dots, \alpha_r$ be a simple system of roots such that the matrix $(\alpha_1(h_j))$ is non-singular. Then there exists a simple system of roots $\delta_1, \dots, \delta_r$, each dependent on $\alpha_1, \dots, \alpha_r$, such that every root expressible as a linear combination of roots $\alpha_1, \dots, \alpha_r$ is expressible as a linear combination of roots in an indecomposable subsystem of $\delta_1, \dots, \delta_r$. Since each indecomposable component of $\delta_1, \dots, \delta_r$ has the property that the matrix $(\delta_i(h_j))$, formed for δ_i, δ_j in the given component, is non-singular, we can even choose $\delta_1, \dots, \delta_r$ in such a fashion that any root is among the roots of Ths. 8.1-14.1, corresponding to the type A-G of the indecomposable component involved in its expression.

PROOF. Among all simple systems of r roots linearly dependent on $\alpha_1, \dots, \alpha_r$, consider only those which have an indecomposable component of maximal rank, i.e., consisting of a maximal number of roots. Among such systems, consider only those in which the subsystem of all roots orthogonal to such a maximal component contains in its turn an indecomposable component of maximal rank, and repeat the procedure until it terminates. Denote any final system by β_1, \dots, β_r .

Now suppose $\gamma_1, \dots, \gamma_s$ is an i.s.s. Among the i.s.s.'s consisting of s roots each dependent on $\gamma_1, \dots, \gamma_s$ we introduce a partial ordering according to the type of the system, as follows:

$$s = 2: A < B < G.$$

$$s = 3: A < B < C.$$

$$s = 4: A < D < B < C < F.$$

$$s = 5, s > 8: A < D < B < C.$$

$$s = 6, 7, 8: A < D < B < C < E.$$

If β_1, \dots, β_k is any indecomposable component of β_1, \dots, β_r , and β_1, \dots, β_k is maximal in the above ordering among i.s.s.'s dependent on β_1, \dots, β_k , take $(\delta_1, \dots, \delta_k) = (\beta_1, \dots, \beta_k)$. Otherwise replace $(\beta_1, \dots, \beta_k)$ by an i.s.s. $(\delta_1, \dots, \delta_k)$ which is maximal among such systems. We must show that $\delta_1, \dots, \delta_k$,

$\beta_{k+1}, \dots, \beta_r$ is a simple system. This is trivial when $(\delta_1, \dots, \delta_k) = (\beta_1, \dots, \beta_k)$.

In any other case, the choice of $\delta_1, \dots, \delta_k$ and Ths. 8.1-14.1 assure that any root dependent on $\delta_1, \dots, \delta_k$ is a member of the set of roots given in the theorem corresponding to the type of $\delta_1, \dots, \delta_k$. If $\delta_1, \dots, \delta_k$ is of type A, then $(\delta_1, \dots, \delta_k) = (\beta_1, \dots, \beta_k)$; thus the exceptional case where $p \nmid (k+2)$ is not encountered.

Now suppose that $\beta_1 - \delta_j$ is a root for some $i > k$. Since $\delta_j(n_{\beta_1}) = 0$ for all j , $1 \leq j \leq k$, $\beta_1 + \delta_j$ is also a root, as are $-\beta_1 \pm \delta_j$. By repeated use of the formula of Th. 5.6, we see that $\delta - \beta_1$ is a root for each δ in the roots of Ths. 8.1-14.1 for a system of the type of $\delta_1, \dots, \delta_k$. For instance, if δ is a positive root, we observe from the statements of those theorems that we can arrive at δ from δ_j by a sequence of additions and subtractions of roots δ_s , $1 \leq s \leq k$, with each addition or subtraction being justified by Th. 5.6 in the sense that the value $\delta^*(n_{\delta_s})$ tells us how many times δ_s may be added to a given term δ^* of the sequence. Since $(\delta^* - \beta_1)(n_{\delta_s}) = \delta^*(n_{\delta_s})$, we may add δ_s to $\delta^* - \beta_1$ as many times as to δ^* . Thus we can arrive at $\delta - \beta_1$ from $\delta_j - \beta_1$ by the same sequence of additions and subtractions used to arrive at δ from δ_j . A similar procedure may be used if δ is negative. In particular, $\beta_j - \beta_1$ is a root for some j , $1 \leq j \leq k$. This is a contradiction, and so $\delta_1, \dots, \delta_k, \beta_{k+1}, \dots, \beta_r$ are a simple system.

If we carry out this replacement procedure for each indecomposable component of the simple system β_1, \dots, β_r , we obtain a new simple system $\delta_1, \dots, \delta_r$ satisfying the requirements by which the system β_1, \dots, β_r was chosen. We shall call any simple system obtained by this process a maximal simple system.

Let α be a root dependent on $\alpha_1, \dots, \alpha_r$, therefore also on $\delta_1, \dots, \delta_r$. If $\delta_1, \dots, \delta_r$ is indecomposable, the first part of the theorem is trivial; the second part follows from Ths. 8.1-14.1. Now suppose the theorem has been proved for maximal systems which decompose into $j-1$ indecomposable components, and suppose that $\delta_1, \dots, \delta_r$ decomposes into j indecomposable components. Let $\delta_1, \dots, \delta_k$ be an indecomposable component of maximal rank. Then $\delta_{k+1}, \dots, \delta_r$ is a maximal system with $j-1$ indecomposable components. If α is not dependent on $\delta_1, \dots, \delta_k$, we can apply Lemma 7.1 to perform successive

subtractions (in some order) of $\delta_1, \dots, \delta_k$ from α and obtain a string of roots leading to a root α' such that $\alpha', \delta_1, \dots, \delta_k$ form a simple system. Since k was the maximal rank for an indecomposable component of any simple system, $\alpha'(h_{\delta_j}) = 0$, $1 \leq j \leq k$. It follows that α' is expressible purely in terms of $\delta_{k+1}, \dots, \delta_r$, and consequently in terms of a single indecomposable component of this system. This is the only case we need consider further, since if α is dependent on $\delta_1, \dots, \delta_k$ alone, the conclusions of the theorem hold for α by Ths. 8.1-14.1.

Let α' be dependent on the indecomposable component $\delta_{k+1}, \dots, \delta_m$, hence among the roots given for this system in Ths. 8.1-14.1. Now either α is dependent on $\delta_{k+1}, \dots, \delta_m$ alone, or $\alpha' + \delta_1$ is a root for some $1 \leq k$. In the latter case, $\alpha' - \delta_1$ is also a root, contradicting the construction of α' . This completes the proof of the theorem.

THEOREM 15.2. Let L be a restricted Lie algebra over an algebraically closed field of characteristic $p > 7$ such that L contains no abelian ideals and has a restricted representation with non-degenerate trace form. Let $\alpha_1, \dots, \alpha_r$ be a fundamental simple system of roots with respect to a Cartan subalgebra H in L , and assume that $\alpha_1, \dots, \alpha_r$ is maximal in the sense of Th. 15.1. Then L is simple (in both the ordinary and the restricted sense) if and only if the system $\alpha_1, \dots, \alpha_r$ is indecomposable.

PROOF. Suppose $\alpha_1, \dots, \alpha_r$ decomposes. Let $\alpha_1, \dots, \alpha_m$ be an indecomposable component of maximal rank. Let J be the subspace of L spanned by $h_{\alpha_1}, \dots, h_{\alpha_m}$ and by some $e_\alpha \neq 0$ in each L_α such that α is a (non-zero) linear combination of $\alpha_1, \dots, \alpha_m$. Then J is an ideal in L . For if $h \in H$,

$$[h_{\alpha_i}, h] = 0, \quad 1 \leq i \leq m,$$

and

$$[e_\alpha, h] = \alpha(h)e_\alpha \in J \quad \text{if } e_\alpha \in J.$$

Thus $[JH] \subseteq J$.

If β is a root, then by Th. 15.1 either β is a linear

combination of $\alpha_1, \dots, \alpha_m$ or β is a linear combination of $\alpha_{m+1}, \dots, \alpha_r$. In the first case,

$$[e_\beta h_{\alpha_1}] = \beta(h_{\alpha_1})e_\beta \in J;$$

$$[e_\alpha e_\beta] \in L_{\alpha+\beta} \subseteq J \text{ if } e_\alpha \in J, \beta \neq -\alpha;$$

$$[e_\alpha e_{-\alpha}] = -(e_\alpha, e_{-\alpha})h_\alpha \in J \text{ if } e_\alpha \in J.$$

In the second case,

$$[h_{\alpha_1} e_\beta] = -\beta(h_{\alpha_1})e_\beta = 0 \in J;$$

$$[e_\alpha e_\beta] = c \in J \text{ if } e_\alpha \in J,$$

since $L_{\alpha+\beta} = 0$ by Th. 15.1.

Thus $[JL_\beta] \subseteq J$ for all roots β , and $[JL] \subseteq J$. Since $h_{\alpha_{m+1}} \notin J$, $0 \notin J \neq L$. Therefore the direct decomposition of L involves at least two (restricted) ideals, and L is not simple in either sense of the word.

Conversely, if L is not simple, $L = L_1 \bullet L_2$, where L_1, L_2 are restricted ideals in L . If α is a root and $0 \neq e_\alpha \in L_\alpha$,

$$e_\alpha = e_\alpha^{(1)} + e_\alpha^{(2)}, e_\alpha^{(1)} \in L_1.$$

If $h \in H$, $[e_\alpha^{(1)}h] + [e_\alpha^{(2)}h] = \alpha(h)e_\alpha = \alpha(h)e_\alpha^{(1)} + \alpha(h)e_\alpha^{(2)}$, or $[e_\alpha^{(1)}h] - \alpha(h)e_\alpha^{(1)} = \alpha(h)e_\alpha^{(2)} - [e_\alpha^{(2)}h] \in L_1 \cap L_2 = (0)$. Thus each $e_\alpha^{(1)} \in L_\alpha$. Since L_α is one-dimensional, either $e_\alpha^{(1)} = 0$ or $e_\alpha^{(2)} = 0$, and each root-space is contained in one or the other of the ideals L_1, L_2 .

Suppose $e_{\alpha_1}, \dots, e_{\alpha_r}$ are all in the same ideal L_1 . Then so are $h_1 = [e_{-\alpha_1} e_{\alpha_1}]$. Since for each root α there is an h_1 such that $\alpha(h_1) = 0$, $e_\alpha = \alpha(h_1)^{-1}[e_\alpha h_1] \in L_1$, and $L_1 = L$. Therefore we may assume that $e_{\alpha_1}, \dots, e_{\alpha_k} \in L_1$, $e_{\alpha_{k+1}}, \dots, e_{\alpha_r} \in L_2$. As above, h_1, \dots, h_k and $e_{-\alpha_1}, \dots, e_{-\alpha_k}$ are in L_1 , while h_{k+1}, \dots, h_r and $e_{-\alpha_{k+1}}, \dots, e_{-\alpha_r}$ are in L_2 . Therefore

$$[e_{\alpha_i} e_{\alpha_j}] = 0 = [e_{\alpha_i} e_{-\alpha_j}]$$

for all $i \leq k < j$. By Lemma 5.3, $\alpha_i(h_j) = 0 = \alpha_j(h_i)$, $i \leq k < j$, and $\alpha_1, \dots, \alpha_r$ decomposes. This completes the proof.

XVI. CLASSIFICATION OF THE SIMPLE ALGEBRAS

THEOREM 16.1. Let L be a simple restricted Lie algebra of characteristic $p > 7$ possessing a restricted representation with non-degenerate trace form. Let $\alpha_1, \dots, \alpha_r$ be a maximal fundamental simple system of roots with respect to a Cartan subalgebra H of L . Then $\alpha_1, \dots, \alpha_r$ is indecomposable, and the algebra L is determined up to restricted isomorphisms by the type $A_r, B_r, C_r, D_r, G_2, F_4, E_6, E_7, E_8$ of $\alpha_1, \dots, \alpha_r$, except in the case where $\alpha_1, \dots, \alpha_r$ is of type A_r and $p \nmid (r+2)$. In this case, L is determined if we know whether $\alpha_0 = \alpha_1 + 2\alpha_2 + \dots + r\alpha_r$ is a root, where $\alpha_1, \dots, \alpha_r$ is labeled in the customary manner.

PROOF. $\alpha_1, \dots, \alpha_r$ is an i.s.s. by Th. 15.2. We agree to call a root α positive if it is among the set of roots actually listed in Ths. 8.1-14.1 for a system of the type of $\alpha_1, \dots, \alpha_r$, as opposed to the negatives of these roots. In the case of $A_r, p \nmid (r+2)$, we define $\alpha_0, \alpha_0 + \alpha_r, \dots, \alpha_0 + \alpha_r + \dots + \alpha_1$ to be positive. From Ths. 8.1-14.1, we observe that if the sum of two positive roots is a root, this root is positive. We also see that any positive root α except $\alpha_1, \dots, \alpha_r$ (and α_0 , if it is a root) can be written in the form $\beta + \alpha_i$, where β is a positive root and $1 \leq i \leq r$.

Now let L' be another simple algebra over the same (algebraically closed) field with a non-degenerate trace form. Suppose that L' has a maximal fundamental simple system of the same type (and rank) as that of L , and that α_0 is a root for L' if and only if it is a root for L (here we identify the systems of roots of L and L' , as permitted by Ths. 8.1-14.1). Let H' be the corresponding Cartan subalgebra of L' . If $h_\alpha \in H, h'_\alpha \in H'$ are defined as before, then

$$\frac{2\alpha(h_\beta)}{\beta(h_\beta)} = \frac{2\alpha(h'_\beta)}{\beta(h'_\beta)}$$

for all roots α, β . For these numbers depend only on the systems of roots, which we know to coincide.

Let $e_{\alpha_1}, \dots, e_{\alpha_r}$ (and possibly e_{α_0}) be non-zero elements of $L_{\alpha_1}, \dots, L_{\alpha_r}$ (L_{α_0}), respectively, and choose $e'_{\alpha_1}, \dots, e'_{\alpha_r}$ (e'_{α_0}) similarly in L' . Choose $e_{-\alpha_1} \in L_{-\alpha_1}, e'_{-\alpha_1} \in L'_{-\alpha_1}$ such that

$$[e_{-\alpha_1} e_{\alpha_1}] = \frac{2}{\alpha_1(h_{\alpha_1})} h_{\alpha_1} = h_1,$$

$$[e'_{-\alpha_1} e'_{\alpha_1}] = \frac{2}{\alpha_1(h'_{\alpha_1})} h'_{\alpha_1} = h'_1,$$

$0 \leq i \leq r$. Define a linear mapping η of the subspace L_0 of L spanned by the $e_{\pm\alpha_i}, 0 \leq i \leq r$, onto the subspace L'_0 of L' spanned by the $e'_{\pm\alpha_i}, 0 \leq i \leq r$, by $e_{\pm\alpha_i} \eta = e'_{\pm\alpha_i}$. This mapping is one-to-one, and if we set $h_i \eta = h'_i, 1 \leq i \leq r$, we can extend η to a linear mapping of $L^* = H + L_0$ onto $L'^* = H' + L'_0$. Moreover, we have

$$(1) \quad [e_{\pm\alpha_i} \eta, h_j \eta] = [e_{\pm\alpha_i} h_j] \eta,$$

$$(2) \quad [e_{-\alpha_i} \eta, e_{\alpha_j} \eta] = [e_{-\alpha_i} e_{\alpha_j}] \eta, \quad 1 \leq j \leq r, \quad 0 \leq i \leq r.$$

$$[e_{\pm\alpha_i} \eta, h_j \eta] = [e'_{\pm\alpha_i} h'_j] = \pm \frac{2\alpha_1(h'_{\alpha_j})}{\alpha_j(h'_{\alpha_j})} e'_{\pm\alpha_i}, \quad \text{while}$$

(1):

$$[e_{\pm\alpha_i} h_j] \eta = \pm \frac{2\alpha_1(h_{\alpha_j})}{\alpha_j(h_{\alpha_j})} e_{\pm\alpha_i} \eta = \pm \frac{2\alpha_1(h'_{\alpha_j})}{\alpha_j(h'_{\alpha_j})} e'_{\pm\alpha_i}.$$

(2): Except when $i = 0$, this is a trivial consequence of the definition of η . When α_0 is a root, we have

$$\begin{aligned}
 [e_{-\alpha_0}\eta, e_{\alpha_0}\eta] &= [e_{-\alpha_0}e_{\alpha_0}'] = h_0' = \frac{2}{\alpha_0(h_{\alpha_0}')} h_{\alpha_0}' \\
 &= \frac{2}{\alpha_0(h_{\alpha_0}')} (h_{\alpha_1}' + 2h_{\alpha_2}' + \dots + rh_{\alpha_r}').
 \end{aligned}$$

Now $\alpha_0(h_{\alpha_0}') = \alpha_1(h_{\alpha_1}') = \dots = \alpha_r(h_{\alpha_r}')$, so that

$$h_0' = h_1' + 2h_2' + \dots + rh_r'.$$

Similarly, $h_0 = h_1 + 2h_2 + \dots + rh_r$, and $h_0\eta = h_0'$, or

$$[e_{-\alpha_0}\eta, e_{\alpha_0}\eta] = [e_{-\alpha_0}e_{\alpha_0}']\eta.$$

If α is a positive root other than $\alpha_0, \alpha_0 + \alpha_r, \dots, \alpha_0 + \alpha_r + \dots + \alpha_1$, define the level of α to be the sum of the natural numbers which represent its coefficients in the lists of Ths. 8.1-14.1. If α_0 is a root, let α_0 have level 1, $\alpha_0 + \alpha_r$ have level 2, $\dots, \alpha_0 + \alpha_r + \dots + \alpha_1$ have level $r + 1$. If α has level $n > 1$, we see that we can find a positive root $\alpha - \alpha_1$ of level $n - 1$ for some $i, 1 \leq i \leq r$.

Let

$$\begin{aligned}
 L_n &= H + \sum_{\alpha} \text{positive of level } \leq n L_{\pm\alpha}, \\
 L_n' &= H' + \sum_{\alpha} \text{positive of level } \leq n L_{\pm\alpha}'.
 \end{aligned}$$

Then $L_1 = L^*, L_1' = L'^*$, and for n sufficiently large, $L_n = L, L_n' = L'$. We assert that the mapping η can be extended to a one-to-one linear mapping of L_n onto L_n' , mapping L_{β} onto L_{β}' if $L_{\beta} \subseteq L_n$, such that if $L_{\alpha}, L_{\beta}, L_{\alpha+\beta} \subseteq L_n$, then $[e_{\alpha}e_{\beta}]\eta = [e_{\alpha}\eta, e_{\beta}\eta]$ in L_n' , where $0 \neq e_{\alpha} \in L_{\alpha}, 0 \neq e_{\beta} \in L_{\beta}$ (we allow α, β , or $\alpha + \beta$ to be zero, in which case the corresponding root-vector can be replaced by arbitrary $h \in H$). Such an extension has already been obtained for $n = 1$. Assume there exists an extension to L_{n-1} with these properties.

Let α be a positive root of level n , and suppose that $\alpha = \beta + \alpha_1$, where β is a positive of level $n - 1, 1 \leq i \leq r$. Let $0 \neq e_{\beta} \in L_{\beta}, 0 \neq e_{\alpha_1} \in L_{\alpha_1}$. Then $0 \neq [e_{\beta}e_{\alpha_1}] = e_{\alpha} \in L_{\alpha}$. Define $e_{\alpha}\eta = [e_{\beta}\eta, e_{\alpha_1}\eta] \in L_{\alpha}' \subseteq L_n'$. Similarly, if $e_{-\alpha} = [e_{-\beta}e_{-\alpha_1}] \in L_{-\alpha}$, define $e_{-\alpha}\eta = [e_{-\beta}\eta, e_{-\alpha_1}\eta] \in L_n'$. Extend η to L_n by linearity. Then

η is one-to-one from L_n to L'_n , and maps H onto H' , L_β onto L'_β for $L_\beta \subseteq L_n$. It remains only to prove the homomorphism property. It will be evident from the proof that the definition of $e_\alpha \eta$ is independent of the representation of α as $\beta + \alpha_1$, and of that of e_α as $[e_\beta e_{\alpha_1}]$. That is, if we represent α in any way as a sum $\gamma + \alpha_j$ of a root γ and a root α_j of the fundamental simple system and if we represent the same vector e_α in any way as $[e_\gamma e_{\alpha_j}]$, where e_γ and e_{α_j} are in the corresponding root-spaces, our definition of $e_\alpha \eta$ will imply that $e_\alpha \eta = [e_\gamma \eta, e_{\alpha_j} \eta]$.

Now

$$[e_{+\alpha} h_1] \eta = \pm \alpha(h_1)(e_{+\alpha} \eta) = \pm \frac{2\alpha(h_{\alpha_1})}{\alpha_1(h_{\alpha_1})} (e_{+\alpha} \eta),$$

while

$$[e_{+\alpha} \eta, h_1 \eta] = [e_{+\alpha} \eta, h_1'] = \pm \frac{2\alpha(h_{\alpha_1}')}{\alpha_1(h_{\alpha_1}')} (e_{+\alpha} \eta) = [e_{+\alpha} h_1] \eta,$$

$$e_{+\alpha} \in L_n, \quad 1 \leq i \leq r.$$

If α is positive of level n and γ is positive, then either $[e_\gamma e_\alpha] = 0$ or $[e_\gamma e_\alpha] \notin L_n$. If $e_\gamma \in L_n$ and $[e_\gamma e_\alpha] = 0$, then $\gamma + \alpha$ is not a root, and $[e_\gamma \eta, e_\alpha \eta] = 0 = [e_\gamma e_\alpha] \eta$.

Next let γ be positive of level less than n . Then

$$[e_{-\gamma} e_\alpha] = [e_{-\gamma} [e_\beta e_{\alpha_1}]] = - [e_\beta [e_{\alpha_1} e_{-\gamma}]] - [e_{\alpha_1} [e_{-\gamma} e_\beta]],$$

and

$$\begin{aligned} [e_{-\gamma} e_\alpha] \eta &= - [e_\beta [e_{\alpha_1} e_{-\gamma}]] \eta - [e_{\alpha_1} [e_{-\gamma} e_\beta]] \eta \\ &= - [e_\beta \eta [e_{\alpha_1} e_{-\gamma}]] \eta - [e_{\alpha_1} \eta [e_{-\gamma} e_\beta]] \eta \\ &= - [e_\beta \eta [e_{\alpha_1} \eta, e_{-\gamma}]] - [e_{\alpha_1} \eta [e_{-\gamma} \eta, e_\beta \eta]] \\ &= [e_{-\gamma} \eta [e_\beta \eta, e_{\alpha_1} \eta]] = [e_{-\gamma} \eta, e_\alpha \eta], \end{aligned}$$

since all quantities to which η is applied are root-vectors in L_{n-1} , for which the homomorphism property holds by assumption.

If γ is positive of level n , we have $e_{-\gamma} = [e_{-\lambda} e_{-\alpha_j}]$, where λ

is positive of level $n - 1$, and $e_{-\gamma}\eta = [e_{-\lambda}\eta, e_{-\alpha_j}\eta]$ ($1 \leq j \leq r$). By reasoning similar to the above,

$$\begin{aligned}
[e_{-\gamma}e_{\alpha}\eta] &= - [e_{\beta}[e_{\alpha_1}e_{-\gamma}]]\eta - [e_{\alpha_1}[e_{-\gamma}e_{\beta}]]\eta \\
&= - [e_{\beta}[e_{\alpha_1}[e_{-\lambda}e_{-\alpha_j}]]]\eta - [e_{\alpha_1}[[e_{-\lambda}e_{-\alpha_j}]e_{\beta}]]\eta \\
&= [e_{\beta}[e_{-\lambda}[e_{-\alpha_j}e_{\alpha_1}]]]\eta + [e_{\beta}[e_{-\alpha_j}[e_{\alpha_1}e_{-\lambda}]]]\eta \\
&\quad + [e_{\alpha_1}[[e_{-\alpha_j}e_{\beta}]e_{-\lambda}]]\eta + [e_{\alpha_1}[[e_{\beta}e_{-\lambda}]e_{-\alpha_j}]]\eta \\
&= [e_{\beta}\eta[e_{-\lambda}\eta[e_{-\alpha_j}\eta, e_{\alpha_1}\eta]]] + [e_{\beta}\eta[e_{-\alpha_j}\eta[e_{\alpha_1}\eta, e_{-\lambda}\eta]]] \\
&\quad + [e_{\alpha_1}\eta[[e_{-\alpha_j}\eta, e_{\beta}\eta]e_{-\lambda}\eta]] + [e_{\alpha_1}\eta[[e_{\beta}\eta, e_{-\lambda}\eta]e_{-\alpha_j}\eta]] \\
&= [e_{-\gamma}\eta, e_{\alpha}\eta].
\end{aligned}$$

A similar argument shows that $[e_{-\alpha}e_{\gamma}\eta] = [e_{-\alpha}\eta, e_{\gamma}\eta]$ whenever α is positive of level n and γ is positive.

Finally, suppose that γ and δ are positive, and that $\gamma + \delta$ is a root. Then $\gamma + \delta$ is positive; if it is of level less than n , then both γ and δ are of level less than n , and by hypothesis, $[e_{\gamma}\eta, e_{\delta}\eta] = [e_{\gamma}e_{\delta}]\eta$. There remains only the case $[e_{\gamma}e_{\delta}] = ke_{\alpha}$, $k \in F$, where $\alpha = \beta + \alpha_1$ is positive of level n , and $[e_{\beta}\eta, e_{\alpha_1}\eta] = e_{\alpha}\eta$. Since L'_{α} is one-dimensional, $[e_{\gamma}\eta, e_{\delta}\eta] = k'(e_{\alpha}\eta)$, and

$$\begin{aligned}
[[e_{\gamma}e_{\delta}]\eta, e_{-\alpha_1}\eta] &= [[e_{\gamma}e_{\delta}]e_{-\alpha_1}]\eta \\
&= - [[e_{\delta}e_{-\alpha_1}]e_{\gamma}]\eta - [[e_{-\alpha_1}e_{\gamma}]e_{\delta}]\eta \\
&= - [[e_{\delta}\eta, e_{-\alpha_1}\eta]e_{\gamma}\eta] - [[e_{-\alpha_1}\eta, e_{\gamma}\eta]e_{\delta}\eta] \\
&= [[e_{\gamma}\eta, e_{\delta}\eta]e_{-\alpha_1}\eta] = k'[e_{\alpha}\eta, e_{-\alpha_1}\eta].
\end{aligned}$$

Meanwhile, $[[e_{\gamma}e_{\delta}]\eta, e_{-\alpha_1}\eta] = k[e_{\alpha}\eta, e_{-\alpha_1}\eta]$. Since $[e_{\alpha}\eta, e_{-\alpha_1}\eta] \neq 0$, $k = k'$, and $[e_{\gamma}\eta, e_{\delta}\eta] = [e_{\gamma}e_{\delta}]\eta$. A repetition of the procedure shows that $[e_{-\gamma}\eta, e_{-\delta}\eta] = [e_{-\gamma}e_{-\delta}]\eta$. Thus η is extended to L_n with the desired homomorphism property.

In particular, when $L_n = L$, $L'_n = L'$, η can be extended to a one-to-one linear mapping of L onto L' such that $[x\eta, y\eta] = [xy]\eta$ for all $x, y \in L$, i.e., to an (ordinary) isomorphism of L onto L' . When

$x \in L$, the quantity $(x\eta)^p - x^p\eta$ is in the center of L' , therefore is zero. Consequently η is a restricted isomorphism of L onto L' . This completes the proof.

Let us summarize the results so far obtained on the classification problem:

THEOREM 16.2. Let L be a simple restricted Lie algebra over an algebraically closed field of prime characteristic $p > 7$, and let L possess a restricted representation with non-degenerate trace form. Then L has a maximal fundamental simple system of roots which is indecomposable, therefore is among the systems of roots of Theorem 6.1, with distinction drawn between systems of type B and those of type C. Moreover, this system determines the algebra up to restricted isomorphism, except when the system is of type A_p and $p \nmid (r + 2)$; in this case there may be two non-isomorphic algebras with the same type of maximal fundamental simple system.

XVII. THE CLASSICAL SIMPLE ALGEBRAS

The classical simple algebras, that is, those of types A - D, are realized as matrices of trace zero (type A) or as matrices which are skew with respect to a certain involution in a full matrix algebra (types B, C, D). The proofs of simplicity for these realizations, as well as the demonstration of the absence of isomorphisms among them, are to be found in [15]. Although we shall not, in general, use their Killing forms, remarks are added as to the conditions under which the Killing form is non-degenerate. The source for these remarks is the work of Dynkin [7], except for the special case of type A, which has been computed by the author.

Consider first the Lie algebra \bar{A}_r of all $(r + 1)$ by $(r + 1)$ matrices of trace zero over the field F . If $p \nmid (r + 1)$, \bar{A}_r is a restricted Lie algebra containing no ordinary ideals. It has a basis given by

$$H_i = E_{ii} - E_{r+1, r+1}, \quad 1 \leq i \leq r,$$

$$E_{ij}, \quad i \neq j, \quad 1 \leq i, j \leq r + 1,$$

where E_{1j} is the matrix with 1 at the intersection of the i -th row and j -th column, and 0 in all other positions. Also,

$$H_1^p = H_1, E_{1j}^p = 0.$$

By observing the effect on this basis, we see that $\text{Tr}(XY)$ is a non-degenerate form on \bar{A}_r when $p \nmid (r+1)$. The H_1 span a Cartan subalgebra H with respect to which the E_{1j} are root-vectors. H has dimension r , and that of \bar{A}_r is $r^2 + 2r$. From this we see that any maximal fundamental simple system of roots with respect to H must be of type A_r . Such a system is obtained if we let $E_{r+1,1}$ belong to the root α_1 , E_{12} to α_2 , ..., $E_{r-1,1}$ to α_r . Then $E_{1,r+1}$ belongs to $-\alpha_1$, E_{21} to $-\alpha_2$, ..., $E_{r,r-1}$ to $-\alpha_r$. By forming the commutators of these elements, we see that $\alpha_1, \dots, \alpha_r$ form a maximal fundamental i.s.s. of type A_r . By Th. 15.2 and the non-degeneracy of the form $\text{Tr}(XY)$, this would provide another proof of simplicity if we only knew that \bar{A}_r is semi-simple. But we get both a non-degenerate trace form and the semi-simplicity from the fact that the Killing form of this algebra is non-degenerate, and from these the simplicity is a consequence of Th. 15.2. Any simple restricted Lie algebra of the class A_r with the property that the quantity α_0 is not a root if $p \mid (r+2)$ is isomorphic to the algebra \bar{A}_r , by Th. 16.1.

Next let $p \mid (r+2)$, and let L^* be the restricted Lie algebra of all $(r+2)$ by $(r+2)$ matrices of trace zero over F . Let C be its (one-dimensional) center. Then $L = L^*/C$ is a restricted Lie algebra containing no ordinary ideals and having the basis

$$\begin{aligned} & \bar{H}_1, \bar{H}_2, \dots, \bar{H}_r \\ & \bar{E}_{1j}, 1 \neq j, 1 \leq i, j \leq r+2, \end{aligned}$$

where $X \rightarrow \bar{X}$ is the natural homomorphism of L^* onto L , and the H_1 and E_{1j} have already been defined. $\bar{H}_1, \dots, \bar{H}_r$ span a Cartan subalgebra, relative to which the \bar{E}_{1j} are root-vectors. Let $\bar{E}_{r+2,1}$ belong to the root α_1 , \bar{E}_{12} to α_2 , ..., $\bar{E}_{r-1,r}$ to α_r . Then we see as above that $\alpha_1, \dots, \alpha_r$ form a fundamental simple system of roots. Moreover, if we define $\bar{H}_{\alpha_1} = [\bar{E}_{1,r+2}, \bar{E}_{r+2,1}]$, ..., $\bar{H}_{\alpha_r} = [\bar{E}_{r,r-1}, \bar{E}_{r-1,r}]$, then $\alpha_j(\bar{H}_{\alpha_j}) \neq 0$, $1 \leq j \leq r$. By a similar definition of \bar{H}_{α} for each root α , we can duplicate all the results of §5 in this case. $\alpha_1, \dots, \alpha_r$ form an i.s.s. of type A_r , and the root to which $\bar{E}_{r,r+1}$

belongs is $\alpha_0 = \alpha_1 + 2\alpha_2 + \dots + r\alpha_r$. The complete system of roots is exactly that displayed for the exceptional case in Th. 8.1. Thus the system $\alpha_1, \dots, \alpha_r$ is maximal for L .

Now L satisfies all the conditions used in the proof of Th. 16.1 to prove the uniqueness of an algebra of type A_r with α_0 as a root, even though we have not shown that L has a non-degenerate trace form. Therefore any algebra of this type is isomorphic to the algebra L . It is unknown to the author whether this algebra has a restricted representation with non-degenerate trace form. It is known that the Killing form fails in this respect.

Next let \bar{B}_r be the Lie algebra of all $(2r + 1)$ by $(2r + 1)$ matrices M over F satisfying $M = -S^{-1}M'S$, where M' denotes the transpose of M , and

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I_r \\ 0 & I_r & 0 \end{pmatrix} .$$

Then \bar{B}_r is a restricted Lie algebra containing no ordinary ideals, and has as a basis

$$\begin{aligned} H_1 &= E_{1+1,1+1} - E_{1+r+1,1+r+1}; \\ E_{(1,-j)} &= E_{j+1,1+1} - E_{1+r+1,j+r+1}, \quad 1 \neq j; \\ E_{(-1,-j)} &= E_{j+1,1+r+1} - E_{1+1,j+r+1}, \quad 1 < j; \\ E_{(1,j)} &= E_{1+r+1,j+1} - E_{j+r+1,1+1}, \quad 1 < j; \\ E_i &= E_{1,1+1} - E_{1+r+1,1}; \quad E_{-1} = E_{1+1,1} - E_{1,1+r+1}; \\ &1 \leq i, j \leq r. \end{aligned}$$

The form $\text{Tr}(XY)$ is non-degenerate on \bar{B}_r . The quantities H_1 span a Cartan subalgebra of \bar{B}_r , and the $E_{(1,-j)}$, $E_{(-1,-j)}$, $E_{(1,j)}$, E_i , E_{-1} are root-vectors corresponding to distinct roots with respect to this Cartan subalgebra. Let $E_{(1,-1)}$ belong to the root α_1 , $1 \leq i \leq r - 1$, and let E_r belong to the root α_r . Then $E_{(1+1,1)}$ belongs to $-\alpha_1$, $1 \leq i \leq r - 1$, and E_{-r} belongs to $-\alpha_r$. From this we see that $\alpha_1, \dots, \alpha_r$ form a simple system of roots which is indecomposable of type B_r . This system is in fact maximal; for the dimension of \bar{B}_r is $2r^2 + r$,

and there are $2r^2$ distinct roots. The only systems which are greater in our ordering and which could give this number of roots are those of type C_r and that of type E_6 when $r = 6$. In the next paragraphs we show an algebra with a maximal system of type C_r , which Jacobson has proved is not isomorphic to \bar{B}_r . It can be shown that \bar{B}_r has non-degenerate Killing form except when $p \mid (2r - 1)$ [7]. The possibility of a system of roots of type E_6 in \bar{B}_6 will be eliminated in §18.

Suppose next that \bar{C}_r is the algebra of all $2r$ by $2r$ matrices M over F satisfying $M = -S^{-1}M'S$, where

$$S = \begin{pmatrix} 0 & I_r \\ -I_r & 0 \end{pmatrix} .$$

\bar{C}_r is a restricted Lie algebra containing no ordinary ideals, and has the basis

$$\begin{aligned} H_1 &= E_{11} - E_{1+r,1+r} ; \\ E_{(-1,j)} &= E_{1j} - E_{j+r,1+r}, \quad 1 \neq j ; \\ E_{(-1,-j)} &= E_{1,j+r} + E_{j,1+r}, \quad 1 < j ; \\ E_{(1,j)} &= E_{1+r,j} + E_{j+r,1}, \quad 1 < j ; \\ E_{(-21)} &= E_{1,1+r}; \quad E_{(21)} = E_{1+r,1}; \quad 1 \leq 1, j \leq r. \end{aligned}$$

The form $\text{Tr}(XY)$ is non-degenerate on \bar{C}_r . The H_1 span a Cartan subalgebra, and the $E_{(-1,-j)}$, $E_{(-1,j)}$, $E_{(1,j)}$, $E_{(-21)}$, $E_{(21)}$ are root-vectors corresponding to distinct roots. Since the dimension of \bar{C}_r is $2r^2 + r$, any maximal fundamental simple system must be of type B, C or E, with the last only possible when $r = 6$. The possibility of a maximal system of type E will be eliminated in the next section.

Let $E_{(2r)}$ belong to the root α_r , and let $E_{(-1-1,1)}$ belong to α_1 , $1 \leq 1 \leq r - 1$. Then $E_{(-2r)}$ belongs to $-\alpha_r$, $E_{(-1,1+1)}$ to $-\alpha_1$, $1 \leq 1 \leq r - 1$, and $\alpha_1, \dots, \alpha_r$ form a simple system of type C_r . If we assume the assertion to have been proved that this algebra cannot possess a simple system of type E when $r = 6$, the system $\alpha_1, \dots, \alpha_r$ is maximal. Thus \bar{C}_r is a representative of the isomorphism class

defined by the system C_r . Jacobson has shown that \bar{C}_r is not isomorphic to the algebra \bar{B}_r for $r \geq 3$. This shows that the simple system of type B_r found for that algebra was in fact maximal. Dynkin shows that \bar{C}_r has non-degenerate Killing form except when $p \mid (r+1)$.

Finally let \bar{D}_r be the algebra of all $2r$ by $2r$ matrices M over F satisfying $M = -S^{-1}M'S$, where

$$S = \begin{pmatrix} 0 & I_r \\ I_r & 0 \end{pmatrix}.$$

For $r \geq 4$, \bar{D}_r is a restricted Lie algebra containing no ordinary ideals, and has the basis

$$H_i = E_{ii} - E_{i+r, i+r};$$

$$E_{(i, -j)} = E_{ji} - E_{i+r, j+r}, \quad i \neq j;$$

$$E_{(-i, -j)} = E_{j, i+r} - E_{i, j+r}, \quad i < j;$$

$$E_{(i, j)} = E_{i+r, j} - E_{j+r, i}, \quad i < j; \quad 1 \leq i, j \leq r.$$

The form $\text{Tr}(XY)$ is non-degenerate on \bar{D}_r . The H_i span a Cartan subalgebra, relative to which the $E_{(i, -j)}$, $E_{(-i, -j)}$, $E_{(i, j)}$ are root-vectors. Let $E_{(i, -i-1)}$ belong to the root α_i , $1 \leq i < r$, and let $E_{(r-1, r)}$ belong to α_r . Then $E_{(i+1, -i)}$ belongs to $-\alpha_i$, $1 \leq i \leq r$, and $E_{(-r+1, -r)}$ belongs to $-\alpha_r$. $\alpha_1, \dots, \alpha_r$ form a simple system of roots, which is indecomposable of type D_r . Since \bar{D}_r has dimension $2r^2 - r$, this system is maximal, and \bar{D}_r is a representative of the isomorphism class defined by the system D_r . The Killing form of \bar{D}_r is non-degenerate except when $p \mid (r-1)$.

XVIII. THE FIVE EXCEPTIONAL ALGEBRAS

In the discussion of these algebras we borrow extensively from Cartan's thesis ([2], pp. 87-93). He demonstrates representatives of the corresponding classes over the complex field, but chooses bases for the algebras in such a fashion that the structural constants are rational numbers whose denominators are 1, 2, or 3. The determinant of the Killing form with respect to this basis is a non-zero rational number,

whose residue class (mod p) is well-defined for $p > 3$, and which is congruent to zero (mod p) for only a finite number of p . For the algebra \bar{G}_2 , the determinant of the Killing form is not congruent to zero (mod p) if $p > 3$. The other cases await calculation.

Cartan constructs a 14-dimensional simple complex Lie algebra L with a two-dimensional Cartan subalgebra and a simple system of roots of type G_2 . Reducing its (rational) structural constants to their residue classes (mod p), we obtain a 14-dimensional Lie algebra over the field Z_p of integers modulo p . We can consider Z_p as embedded in our field F and extend Z_p to F to obtain a 14-dimensional Lie algebra \bar{G}_2 over F . If the characteristic p of F is greater than 3, \bar{G}_2 has non-degenerate Killing form, hence is a restricted Lie algebra. \bar{G}_2 again has a two-dimensional Cartan subalgebra. If a maximal fundamental simple system for \bar{G}_2 were of type A_2 , of type B_2 , or decomposable, then \bar{G}_2 would have dimension 8, 10 or 6, respectively. Therefore any maximal fundamental simple system of roots for \bar{G}_2 is of type G_2 (such a system is easily found), and \bar{G}_2 is a representative of the isomorphism class G_2 .

Similarly, we can use Cartan's work to construct a Lie algebra \bar{F}_4 of dimension 52 over F with a Cartan subalgebra of dimension 4. For suitable values of p (almost all), the Killing form is non-degenerate, and one can display a simple system of roots of type F_4 . This system is therefore maximal, and \bar{F}_4 is a representative of the isomorphism class determined by the system F_4 .

The same procedure can be used to display representatives of the isomorphism classes determined by E_6, E_7, E_8 , at least for sufficiently large values of p . It remains to show that the algebra of type E_6 so obtained is not isomorphic to either of those algebras \bar{B}_6 and \bar{C}_6 which we have claimed as representatives of the types B_6 and C_6 . But if we observe the system of all roots for an algebra of type E_6 as listed in §14, we see that there are no two roots $\alpha, \beta, \alpha \neq -\beta$, such that $\alpha + \beta$ and $\alpha + 2\beta$ are roots. In each of the cases \bar{B}_6 and \bar{C}_6 there are such roots (for \bar{B}_6 , take $\alpha = \alpha_5, \beta = \alpha_6$; for \bar{C}_6 , take $\alpha = \alpha_6, \beta = \alpha_5$), and this property will be preserved under isomorphism. Thus the algebras cannot be isomorphic.

For $p > 7$, we may argue as in the exceptional case of type A (see §17) to show that if the class F_4, E_6, E_7 or E_8 is non-vacuous, the algebra formed by the above process must be representative. Therefore a

class is non-vacuous if and only if the algebra so obtained for that class has a restricted representation with non-degenerate trace form. It seems likely that this remark is unnecessary, i.e., that the Killing forms are already non-degenerate for $p > 7$.

As a corollary, we can state the following classification theorem for simple algebras with non-degenerate Killing form.

THEOREM 18.1. Let L be a Lie algebra over an algebraically closed field of characteristic $p > 7$. Suppose that L is simple and has non-degenerate Killing form. Then L is isomorphic to one of the algebras

$$\bar{A}_r, p \nmid (r + 1), r \geq 1;$$

$$\bar{B}_r, p \nmid (2r - 1), r \geq 2;$$

$$\bar{C}_r, p \nmid (r + 1), r \geq 3;$$

$$\bar{D}_r, p \nmid (r - 1), r \geq 4;$$

or to one of the algebras formed from the Killing-Cartan complex algebras of types E, F, G in the manner indicated. For the types E and F, there is an algebra of the respective type with non-degenerate Killing form if and only if the corresponding complex algebra has a Killing form whose determinant is not congruent to zero modulo p .

BIBLIOGRAPHY

- [1] BIRKHOFF, G., Representability of Lie algebras and Lie groups by matrices. *Ann. of Math.* 38 (1937), 526-532.
- [2] CARTAN, É., Thèse. Paris 1894. 2nd ed. Vuibert, Paris 1933.
- [3] CHANG, HO-JUI, Über Wittsche Lie-Ringe. *Abh. Math. Sem. Hamburg Univ.* 14 (1941), 151-184.
- [4] CURTIS, C. W., A note on the representations of nilpotent Lie algebras. *Proc. A. M. S.* 5 (1954), 813-824. Errata, ibid. p. 1001.
- [5] DIEUDONNÉ, J., Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$. *Comment. Math. Helv.* 28 (1954), 87-118.
- [6] ———, On semi-simple Lie algebras. *Proc. A. M. S.* 4 (1953), 931-932.
- [7] DYNKIN, E. B., The structure of semi-simple algebras. *A. M. S. Translation No.* 17.
- [8] FRANK, M. S., A new class of simple Lie algebras. *Proc. Nat. Acad. Sci. U.S.A.* 40 (1954), 713-719.
- [9] GLEASON, A. M. and others, The first Summer Mathematical Institute. *Bull. A. M. S.* 60 (1954), 457-471.
- [10] HOCHSCHILD, G., Representations of restricted Lie algebras of characteristic p . *Proc. A. M. S.* 5 (1954), 603-605.
- [11] JACOBSON, N., A class of normal simple Lie algebras of characteristic zero. *Ann. of Math.* 38 (1937), 508-517.
- [12] ———, A note on Lie algebras of characteristic p . *Amer. Jour. of Math.* 74 (1952), 357-359.
- [13] ———, Abstract derivation and Lie algebras. *Trans. A. M. S.* 42 (1937), 206-224.
- [14] ———, Cayley numbers and simple Lie algebras of type G. *Duke Math. Jour.* 5 (1939), 775-783.
- [15] ———, Classes of restricted Lie algebras of characteristic p . I. *Amer. Jour. of Math.* 63 (1941), 481-515.
- [16] ———, Classes of restricted Lie algebras of characteristic p . II. *Duke Math. Jour.* 10 (1943), 107-121.
- [17] ———, Commutative restricted Lie algebras. *Proc. A. M. S.* 6 (1955), 476-481.
- [18] ———, Restricted Lie algebras of characteristic p . *Trans. A. M. S.* 50 (1941), 15-25.
- [19] ———, Simple Lie algebras of type A. *Ann. of Math.* 39 (1938), 181-188.

- [20] JACOBSON, N., Simple Lie algebras over a field of characteristic zero. Duke Math. Jour. 4 (1938), 534-551.
- [21] 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.
- [22] LANDHERR, W., Liesche Ringe vom Typus A. Abh. Math. Sem. Hamburg Univ. 12 (1938), 200-241.
- [23] ———, Über einfache Liesche Ringe. Abh. Math. Sem. Hamburg Univ. 11 (1935), 41-64.
- [24] LAZARD, M., Sur les groupes nilpotents et les anneaux de Lie. Ann. École Norm. Sup. 71 (1954), 101-190.
- [25] TOMBER, M. L., Lie algebras of type F. Proc. A. M. S. 4 (1953), 759-768.
- [26] van der WAERDEN, B. L., Die Klassifikation der einfachen Lieschen Gruppen. Math. Zeitschr. 37 (1933), 446-462.
- [27] WEYL, H., Theorie der Darstellung kontinuierlicher halbeinfacher Gruppen durch lineare Transformationen. Math. Zeitschr. 23 (1925), 271-309; 24 (1926), 328-395.
- [28] WITT, E., Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe. Abh. Math. Sem. Hamburg Univ. 14 (1941), 289-337.
- [29] ———, Treue Darstellung Liescher Ringe. Jour. für Math. (Crelles J.) 177 (1937), 152-160.
- [30] ZASSENHAUS, H., Darstellungstheorie nilpotenter Lie-Ringe bei Charakteristik $p > 0$. Jour. für Math. (Crelles J.) 182 (1940), 150-155.
- [31] ———, Ein Verfahren, jeder endlichen p -Gruppe einen Lie-Ring mit der Charakteristik p zuzuordnen. Abh. Math. Sem. Hamburg Univ. 13 (1939), 200-207.
- [32] ———, The representations of Lie algebras of prime characteristic. Proc. Glasgow Math. Assoc. 2 (1954), 1-36.
- [33] ———, Über Lie'sche Ringe mit Primzahlcharakteristik. Abh. Math. Sem. Hamburg Univ. 13 (1939), 1-100.

OF THE
AMERICAN MATHEMATICAL SOCIETY

- | | | |
|-----|---|--------|
| 1. | G. T. Whyburn, <i>Open mappings on locally compact spaces</i> . ii, 25 pp. 1950. | \$0.75 |
| 2. | J. Dieudonné, <i>On the automorphisms of the classical groups</i> , with a supplement by L. K. Hua. viii, 122 pp. 1951. | 1.80 |
| 3. | H. D. Ursell and L. C. Young, <i>Remarks on the theory of prime ends</i> . 29 pp. 1951. | 1.00 |
| 4. | K. Ito, <i>On stochastic differential equations</i> . 51 pp. 1951. | 1.00 |
| 5. | O. Zariski, <i>Theory and applications of holomorphic functions on algebraic varieties over arbitrary ground fields</i> . 93 pp. 1951, reprinted 1956 | 1.40 |
| 6. | K. L. Chung, M. D. Donsker, P. Erdős, W. H. J. Fuchs, and M. Kac, <i>Four papers on probability</i> . ii, 12 + 19 + 11 + 12 pp. 1951, reprinted 1956. | 1.20 |
| 7. | R. V. Kadison, <i>A representation theory for commutative topological algebras</i> . 39 pp. 1951, reprinted 1956. | 1.00 |
| 8. | J. W. T. Youngs, <i>The representation problem for Fréchet surfaces</i> . 143 pp. 1951. | 1.80 |
| 9. | I. E. Segal, <i>Decompositions of operator algebras</i> . I and II. 67 + 66 pp. 1951. | 1.80 |
| 10. | S. C. Kleene, <i>Two papers on the predicate calculus</i> . 68 pp. 1952. | 1.30 |
| 11. | E. A. Michael, <i>Locally multiplicatively-convex topological algebras</i> . 79 pp. 1952. | 1.40 |
| 12. | S. Karlin and L. S. Shapley, <i>Geometry of moment spaces</i> . 93 pp. 1953. | 1.50 |
| 13. | Walter Strodt, <i>Contributions to the asymptotic theory of ordinary differential equations in the complex domain</i> . 81 pp. 1954. | 1.50 |
| 14. | <i>Lie algebras and Lie groups</i> . Five papers prepared in connection with the First Summer Mathematical Institute. vi, 54 pp. 1953. | 1.30 |
| 15. | I. I. Hirschman, <i>The decomposition of Walsh and Fourier series</i> . 65 pp. 1955. | 1.40 |
| 16. | Alexandre Grothendieck, <i>Produits tensoriels topologiques et espaces nucléaires</i> . 191 + 140 pp. 1955. | 2.80 |
| 17. | L. C. Young, <i>On generalized surfaces of finite topological types</i> . 63 pp. 1955. | 1.30 |
| 18. | L. H. Loomis, <i>The lattice theoretic background of the dimension theory of operator algebras</i> . 36 pp. 1955. | 1.30 |
| 19. | G. B. Seligman, <i>On Lie algebras of prime characteristic</i> . 85 pp. 1956. | 1.60 |

The price to members of the American Mathematical Society is 25% less than list.