

UNIVERSAL
LIBRARY

OU_166428

UNIVERSAL
LIBRARY

MEMOIRS
OF THE
AMERICAN MATHEMATICAL SOCIETY

NUMBER 14

LIE ALGEBRAS AND LIE GROUPS

**FIVE PAPERS PREPARED IN CONNECTION WITH
THE FIRST SUMMER MATHEMATICAL INSTITUTE**

**PUBLISHED BY THE
AMERICAN MATHEMATICAL SOCIETY**

80 Waterman St., Providence, R. I.

1955

OSMANIA UNIVERSITY LIBRARY

Call No. 510.6 / AMS — Accession No. 39917

Author *Memiors of the AMS No. 14 :*

Title *Lie algebras and Lie groups*

This book should be returned on or before the date last marked below.

Five papers prepared in connection with the First Summer Mathematical Institute of the American Mathematical Society, which was held at Colby College, Waterville, Maine, from June 20 to July 31, 1953.

The Institute was supported by a grant from the National Science Foundation.

TABLE OF CONTENTS

Foreword	v
By A. M. GLEASON	
The Betti Numbers of the Exceptional Groups	1
By A. BOREL and C. CHEVALLEY	
On a Simple Lie Algebra of Characteristic 2	11
By R. D. SCHAFER and M. L. TOMBER	
On the Derivation Algebra and the Holomorph of a Nilpotent Lie Algebra	15
By EUGENE SCHENKMAN	
On the Group of Automorphisms of a Locally Compact Connected Group	23
By MORIKUNI GOTO	
Some New Decomposition Theorems for Semi-Simple Groups	31
By G. D. MOSTOW	

FOREWORD

The American Mathematical Society, with the financial support of the National Science Foundation, held its First Summer Mathematical Institute from June 20 to July 31, 1953. The topic chosen was Lie Theory; twenty-nine mathematicians active in this area attended. The six-week period provided opportunity both for the interchange of ideas and for the subsequent shaping of ideas into theorems. The five papers collected in this Memoir present some results achieved by the participants.

We cannot yet assess the total effect of the Summer Institute. This volume, however, is witness that it has substantially increased our knowledge of Lie groups and Lie algebras.

A. M. Gleason
Editor

THE BETTI NUMBERS OF THE EXCEPTIONAL GROUPS

A. BOREL AND C. CHEVALLEY

The Betti numbers¹ of the classical groups have been known for a long time and can be obtained in several ways, (see e.g. [1], Chap. III, [8], and [9] for other references); those of the exceptional groups have been given only more recently ([4], [10])², with practically no proof, and the purpose of this Note is to describe the actual computations which allow us to derive them from general statements proved elsewhere. We will mainly use elementary divisibility considerations based on the Hirsch formula (1.4), on the knowledge of subgroups of maximal rank [2], and their Poincaré polynomials. Thus this method requires a certain amount of information and, in that respect, is less satisfactory than that of [4], based solely on the study of the invariants of the Weyl group, but it has the advantage of leading to simpler computations. However, the method is not sufficient to deal with E_8 , and there we shall also have to consider some invariants of the Weyl group.

1. Preliminaries. 1.1. G will always denote a compact connected Lie group, $r(G)$ or r its rank; we recall that $r(G)$ is the (common) dimension of the maximal toral subgroups of G . If T^r is one of them, the quotient by T^r of its normaliser in G is a finite group, the Weyl group $W(G)$ of G , whose order will be denoted $\text{ord } W(G)$; it may be identified in a natural way with the group of automorphisms of the Lie algebra \mathfrak{U}^r of T^r which are induced by inner automorphisms, and l_G will be the ring of polynomials over \mathfrak{U}^r with real coefficients which are fixed under the operations of $W(G)$.

The classes of locally isomorphic compact connected non abelian simple Lie groups are usually denoted by A_r , ($r \geq 1$), B_r , ($r \geq 2$), C_r , ($r \geq 3$), D_r , ($r \geq 4$), (the classical structures), G_2 , F_4 , E_6 , E_7 , E_8 , (the exceptional structures). Their respective dimensions are $r(r+2)$, $r(2r+1)$, $r(2r+1)$, $r(2r-1)$, 14 , 52 , 78 , 133 , 248 , and the orders of the respective Weyl groups are $(r+.)!$, $r! \cdot 2^r$, $r! \cdot 2^r$, $r! \cdot 2^{r-1}$, 12 , $2^7 \cdot 3^2$, $2^7 \cdot 3^4 \cdot 5$, $9! \cdot 8$, $10! \cdot 3 \cdot 2^6$; subscripts denote rank.

1.2. $H^*(X)$, (resp. $H^t(X)$), will denote the cohomology algebra, (resp. the t -th cohomology space) of the space X , with real coefficients, and

$$P(X, t) = \sum_{i \geq 0} \dim H^i(X) \cdot t^i$$

its Poincaré polynomial.

1. Only cohomology over the field of real numbers is considered in this Note.
2. except however of G_2 , (see [3]).

By Hopf's theorem [5], combined with [3], or with H. Hopf, *Comm. Math. Helv.* 13(1940-41), pp. 119-143, (see also [1], Prop. 26.1), $H^*(G)$ is the exterior algebra of an r -dimensional subspace P , graded by odd degrees; in particular

$$P(G, t) = (1+t^{s_1}) \cdot \dots \cdot (1+t^{s_r}),$$

the s_i 's being the degrees of a base of P ; by Samelson's theorem ([8], [7], [1]), one may take as P the subspace generated by primitive elements.

As well known, and as follows e.g. from (1.3), two compact connected locally isomorphic Lie groups have isomorphic cohomology algebras over the reals, so we can allow ourselves to speak about the Betti numbers of A_r , B_r , etc., meaning by that of course the Betti numbers of any representative of that structure. Recall that

$$P(A_r, t) = (1+t^3) \cdot (1+t^5) \cdot \dots \cdot (1+t^{2r+1}),$$

$$P(B_r, t) = P(C_r, t) = (1+t^3) \cdot (1+t^7) \cdot \dots \cdot (1+t^{4r-1}),$$

$$P(D_r, t) = (1+t^3) \cdot (1+t^7) \cdot \dots \cdot (1+t^{4r-5}) \cdot (1+t^{2r-1}).$$

1.3. The ring I_G of invariants of $\mathbb{W}(G)$ has r algebraically independent generators (to be called hereafter *primitive invariants*) of degrees m_1, \dots, m_r and

$$P(G, t) = (1+t^{2m_1-1}) \cdot \dots \cdot (1+t^{2m_r-1}),$$

([4], see [1], §26-27 for a topological proof).

1.4. Let U be a closed connected subgroup of G , having the same rank as G . Then the Euler-Poincaré characteristic $P(G/U, -1)$ of G/U is equal to the quotient of $\text{ord } \mathbb{W}(G)$ by $\text{ord } \mathbb{W}(U)$, (see [6]), and, by Hirsch formula, (proved e.g. in [1], §26):

$$P\left(\frac{G}{U}, t\right) = (1-t^{2m_1}) \cdot \dots \cdot (1-t^{2m_r}) \cdot (1-t^{2n_1})^{-1} \cdot \dots \cdot (1-t^{2n_r})^{-1},$$

where the m_i 's, (resp., the n_i 's), are the degrees of the primitive invariants of $\mathbb{W}(G)$, (resp. $\mathbb{W}(U)$).

In particular, if k different coefficients n_i are divisible by an integer c , the system (m_i) has the same property.

1.5. Applying (1.4) to G/T^r , one gets

$$2(m_1 + \dots + m_r) = \dim G + r, \quad m_1 \cdot \dots \cdot m_r = \text{ord } W(G).$$

Let now G be simple non abelian. Then, as well known, $W(G)$ is absolutely irreducible, therefore it has no linear invariant and only one quadratic invariant (up to a multiplicative constant), so we may assume in that case:

$$m_1 = 2, \quad m_i > 2, \quad (i \geq 2).$$

1.6. If $a = p_1 \cdot \dots \cdot p_n$ is the factorisation of an integer a into prime numbers p_1, \dots, p_n , we set

$$S(a) = \sum_{i=1}^{i=n} p_i, \quad E(a) = a - S(a);$$

we have $E(a) \geq 0$, $S(a \cdot b) = S(a) + S(b)$, whence $E(a \cdot b) \geq b(a-1) - S(a)$.

2. The Poincaré polynomials of G_2 and F_4 . For G_2 , (1.5) gives $m_1 - 2$, $m_2 = 6$, whence:

$$P(G_2, t) = (1 + t^3) \cdot (1 + t^{11}).$$

F_4 contains a subgroup of type B_4 , (see e.g. [2]); by (1.1) and (1.4), the co-set space F_4/B_4 has vanishing odd-dimensional Betti numbers, and its Euler-Poincaré characteristic is equal to 3; since it is a compact orientable manifold, we can apply Poincaré duality, and that shows

$$P(F_4/B_4, t) = 1 + t^8 + t^{16};$$

hence, if (m_i) are the degrees of the primitive invariants of $W(F_4)$:

$$\prod_{i=1}^{i=4} (1 - t^{2m_i}) = (1 + t^8 + t^{16}) \cdot \prod_{i=1}^{i=4} (1 - t^{4i}),$$

and finally, by (1.3):

$$P(F_4, t) = (1 + t^3) \cdot (1 + t^{11}) \cdot (1 + t^{15}) \cdot (1 + t^{23}).$$

3. The Poincaré polynomial of E_6 . E_6 has three maximal connected subgroups of rank 6 [2]:

$$T^1 \times D_5 : 1, 2, 4, 6, 8, 5$$

$$A_2 \times A_2 \times A_2 : 2, 3, 2, 3, 2, 3$$

$$A_1 \times A_5 : 2, 2, 3, 4, 5, 6$$

(On the right are given the degrees of the primitive invariants of the Weyl group, deduced from (1.1) and (1.3)). Therefore, by (1.4), there are among the m_i 's at least one multiple of 8, another multiple of 4, two more multiples of 2, as well as at least three multiples of 3.

By (1.5) we have

$$m_1 = 2, \quad \sum_2^6 m_i = 40, \quad \prod_2^6 m_i = 2^6 \cdot 3^4 \cdot 5,$$

whence

$$\sum_2^6 E(m_i) = 40 - S(2^6 \cdot 3^4 \cdot 5) = 11.$$

We may assume that $m_2 = 8n_2$; since one of m_3, \dots, m_6 is $\equiv 0 \pmod{4}$ and another one is even, n_2 is odd; moreover $7n_2 - 6 \leq E(m_2) \leq 11$, whence $n_2 = 1$, and

$$\sum_3^6 m_i = 32, \quad \prod_3^6 m_i = 2^3 \cdot 3^4 \cdot 5, \quad \sum_3^6 E(m_i) = 9.$$

Since $32 \not\equiv 0 \pmod{3}$, all of m_3, \dots, m_6 cannot be $\equiv 0 \pmod{3}$ and one of them is divisible by 9. Assume that $m_3 = 9n_3$, then $8n_3 - 6 \leq E(m_3) \leq 9$, whence $n_3 = 1$, and

$$\sum_3^6 m_i = 23, \quad \prod_3^6 m_i = 2^3 \cdot 3^2 \cdot 5, \quad \sum_3^6 E(m_i) = 6.$$

Set $m_4 = 5n_4$; then $4n_4 - 5 \leq E(m_4) \leq 6$, whence $n_4 \leq 2$. Were $n_4 = 2$, then we would have $m_5 + m_6 = 13$, which is impossible, since three of the m_i 's have to be multiples of 3. Thus $n_4 = 1$,

$$m_5 + m_6 = 18, \quad m_5 \cdot m_6 = 72$$

which gives for m_5, m_6 the values 6, 12; finally we get:

$$P(E_6, t) = (1+t^3) \cdot (1+t^9) \cdot (1+t^{11}) \cdot (1+t^{15}) \cdot (1+t^{17}) \cdot (1+t^{23}).$$

4. The Poincaré polynomial of E_7 . For the degrees of the primitive invari-

ants we have here

$$(4.1) \quad m_1 = 2, \quad \sum_2^7 m_i = 68, \quad \prod_2^7 m_i = 2^9 \cdot 3^4 \cdot 5 \cdot 7.$$

E_7 contains a subgroup of type $A_1 \times D_6$; by (1.1), (1.3), the degrees of the primitive invariants of the latter are 2, 2, 4, 6, 8, 10, 6; hence, by (1.4), all the m_i 's are even and, putting $m_i = 2n_i$, we get:

$$(4.2) \quad \sum_2^7 n_i = 34, \quad \prod_2^7 n_i = 2^3 \cdot 3^4 \cdot 5 \cdot 7, \quad \sum_2^7 E(n_i) = 4.$$

We may assume $n_2 = 7p_2$; then $6p_2 - 7 \leq E(n_2) \leq 4$, whence $p_2 = 1$ and

$$\sum_3^7 n_i = 27, \quad \prod_3^7 n_i = 2^3 \cdot 3^4 \cdot 5, \quad \sum_3^7 E(n_i) = 4.$$

Not all n_i 's may be $\equiv 0 \pmod{3}$; since their sum is divisible by 3, at least two of them are $\not\equiv 0 \pmod{3}$ and therefore another one must be $\equiv 0 \pmod{9}$. Set $n_3 = 9p_3$, then $8p_3 - 6 \leq E(n_4) \leq 4$, whence $n_3 = 1$ and

$$\sum_4^7 n_i = 18, \quad \prod_4^7 n_i = 2^3 \cdot 3^2 \cdot 5, \quad \sum_4^7 E(n_i) = 1.$$

Assume that $n_4 = 5p_4$, then $4p_4 - 5 \leq E(n_4) \leq 1$, whence $p_4 = 1$ and

$$\sum_5^7 n_i = 13, \quad \prod_5^7 n_i = 2^3 \cdot 3^2, \quad \sum_5^7 E(n_i) = 1.$$

Since the sum is $\not\equiv 0 \pmod{2}$, one of the remaining n_i 's, say n_5 , is odd; then n_5 is a power of 3, different from 9 since $E(n_5) \leq 1$; hence

$$n_5 = 3, \quad n_6 + n_7 = 10, \quad n_6 \cdot n_7 = 24,$$

which gives the values 4 and 6 for n_6 and n_7 . Thus we obtain

$$P(E_7, t) = (1+t^3) \cdot (1+t^{11}) \cdot (1+t^{15}) \cdot (1+t^{19}) \cdot (1+t^{23}) \cdot (1+t^{27}) \cdot (1+t^{35}).$$

5. The Poincaré polynomial of E_8 . 5.1. Let (x_i) , ($1 \leq i \leq 8$), be coordinates in the Lie algebra of a maximal torus of E_8 . Then the roots may be written

$$\pm x_i \pm x_j, \quad (i < j), \quad \frac{1}{2} \left(\sum_1^8 \epsilon_i \cdot x_i \right), \quad (\epsilon_i = \pm 1, \prod_1^8 \epsilon_i = 1).$$

The Killing form is then $\sum x_i^2$ up to a constant factor; we put moreover

$$s_j = \sum_I^8 x_i^j;$$

we will also use (overabundant) coordinates $z, y_i, (1 \leq i \leq 8)$, defined by

$$z = \frac{1}{8} \cdot \left(\sum_I^8 x_i \right); \quad y_i = x_i - z, \quad (1 \leq i \leq 8);$$

the y_i 's being therefore subject to the relation $\sum y_i = 0$; we put

$$t_j = \sum_I^8 y_i^j;$$

we denote by s the symmetry to the hyperplane $\sum x_i = 0$; it is defined either by

$$s(x_i) = x_i - 2z, \quad (1 \leq i \leq 8),$$

or by

$$s(z) = -z, \quad s(y_i) = y_i, \quad (1 \leq i \leq 8).$$

5.2. $W(E_8)$ is generated by the reflections to the hyperplanes obtained by equating to zero one root; the reflections to the hyperplanes $x_i \pm x_j = 0$ generate a subgroup W^* of $W(E_8)$, (in fact $W^* = W(D_8)$), which may be described as the group of permutations of the x_i 's combined with an even number of changes of signs. Thus the invariants of W^* , and therefore those of $W(E_8)$, will be polynomials in the functions $s_{2k}, (1 \leq k \leq 7)$, and in the product of the x_i 's; in particular *their degrees are all even*.

The proof of the following lemma will be given in (5.3) to (5.6).

LEMMA. *Let S_{2m} be the half-sum of the $2m$ -th powers of the roots of E_8 . Then S_8 and S_{12} are primitive invariants of $W(E_8)$. Moreover, $W(E_8)$ has no primitive invariant of degree 4 or 6.*

5.3. **Degree 4.** If there is a primitive invariant of degree 4, it must have the form $as_4 + bs_2^2$, (a, b real constants, $a \neq 0$), and s_4 is then also invariant; but

$$s_4 = t_4 + 4 \cdot z \cdot t_3 + 6 \cdot z^2 \cdot t_2 + 8 \cdot z^4, \quad (\text{since } t_1 = 0),$$

and $s(s_4) = s_4$ would imply that $t_3 = 0$ under the sole condition $t_1 = 0$, in other terms that t_3 is divisible by t_1 , which is not the case; hence a contradiction.

5.4. **Degree 6.** If there is a primitive invariant of degree 6, then there must

exist an invariant of the form

$$a \cdot s_6 + b \cdot s_4 \cdot s_2, \quad ((a, b) \neq (0, 0));$$

but the coefficient of z in that expression is

$$6 \cdot a \cdot t_5 + 4 \cdot b \cdot t_3 \cdot t_2$$

and is not divisible by t_1 , whence a contradiction.

5.5. Degree 8. Since there is no primitive invariant of degree 4, it will be enough to show that S_8 is not divisible by S_2 . We have

$$(5.5)^* \quad S_{2m} = \sum_{i < j} [(x_i - x_j)^{2m} + (x_i + x_j)^{2m}] + 2^{-2m-1} \cdot \sum_{(\epsilon_i)} \left(\sum_{l=1}^8 \epsilon_l \cdot \chi_l \right)^{2m}$$

the latter sum being extended to all systems (ϵ_i) such that $\epsilon_i = \pm 1$, $\prod_1^8 \epsilon_i = 1$. Putting $m = 4$, $x_i = 0$, ($3 \leq i \leq 8$), we get

$$12(x_1^8 + x_2^8) + (x_1 - x_2)^8 + (x_1 + x_2)^8 + 2^{-3} \cdot (x_1 - x_2)^8 + 2^{-3} \cdot (x_1 + x_2)^8$$

which, for the particular values $x_1 = 1$, $x_2 = i$, is a sum of strictly positive terms; thus S_8 is $\neq 0$ for a set of values of the x_i which annihilates S_2 , and therefore is not divisible by S_2 .

5.6. Degree 12. Since there are no primitive invariants of degrees 4, 6 it will be enough to show that S_{12} is not divisible by S_2 . Let j be a primitive cube root of unity, and let us put in (5.5)*:

$$m = 6, \quad x_1 = 1, \quad x_2 = j, \quad x_3 = j^2, \quad x_i = 0, \quad (i \geq 4).$$

The polynomial S_{12} becomes then a sum with positive coefficients of the numbers

$$1, \quad j^{12}, \quad j^{24}, \quad (1-j)^{12}, \quad (1-j^2)^{12}, \quad (j-j^2)^{12},$$

$$(1+j)^{12}, \quad (1+j^2)^{12}, \quad (j+j^2)^{12},$$

$$(-1+j+j^2)^{12}, \quad (1-j+j^2)^{12}, \quad (1+j-j^2)^{12},$$

each of which is > 0 , as one easily sees; thus $S_{12} > 0$ and $S_2 = 0$ for these values of the x_i and S_2 does not divide S_{12} , which concludes the proof of the lemma.

5.7. The foregoing and (1.5) already give

$$m_1 = 2, m_2 = 8, m_3 = 12, m_i = 2n_i > 2 \quad (i \geq 4).$$

Since $\text{ord} W(E_8) = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$, we get

$$(5.7)^* \quad \sum_4^8 n_i = 53, \quad \prod_4^8 n_i = 2^3 \cdot 3^4 \cdot 5^2 \cdot 7, \quad \sum_4^8 E(n_i) = 18.$$

Among the subgroups of rank 8 of E_8 , we have [2]:

$$A_1 \times E_7 : 2, 2, 6, 8, 10, 12, 14, 18$$

$$D_8 : 2, 4, 6, 8, 10, 12, 14, 8$$

$$A_8 : 2, 3, 4, 5, 6, 7, 8, 9$$

$$A_2 \times E_6 : 2, 3, 2, 5, 6, 8, 9, 12$$

$$A_4 \times A_4 : 2, 3, 4, 5, 2, 3, 4, 5$$

(following each group are the degrees of the corresponding primitive invariants).

For the n_i 's that gives by (1.4) the conditions:

- (a) two multiples of 5.
- (b) one multiple of 9, two more multiples of 3, no other factor 3.
- (c) one multiple of 4, another multiple of 2, no other factor 2.
- (d) one multiple of 7.

By (5.7)*, we have $E(n_i) \leq 18$, ($4 \leq i \leq 8$). Since

$$E(9p) \geq 8p - 6, \quad E(7p) \geq 6p - 7, \quad E(5p) \geq 4p - 5,$$

we see that, if some n_i is a product $a \cdot b$, then $a = 9$ implies $b \leq 3$, $a = 7$ implies $b \leq 4$, $a = 5$ implies $b \leq 5$; moreover, it is impossible that one of the n_i 's, say n_4 , is equal to 20, for $n_5 + n_6 + n_7 + n_8$ would then be 33, which is $\equiv 0 \pmod{3}$ while in virtue of (5.7) (b) exactly three of n_5, n_6, n_7, n_8 would be divisible by 3. Hence, none of n_4, n_5, n_6, n_7, n_8 is divisible by two of the factors 4, 5, 7, 9 and, in view of (5.7), we may assume:

$$n_4 = 9p_4, \quad n_5 = 7p_5, \quad n_6 = 5p_6, \quad n_7 = 5p_7, \quad n_8 = 4p_8$$

with

$$p_4 \leq 2, p_5 \leq 4, p_6 \leq 5, p_7 \leq 5, \prod_{i=1}^8 p_i = 2 \cdot 3^2.$$

Moreover, it follows from (5.7) (b), (c) that p_8 is odd and not divisible by 9. Thus, each of the p_i 's is 1, 2, or 3 and $\prod p_i = 2 \cdot 3^2$ implies $\sum p_i = 10$. On the other hand,

$$53 = \sum_4^8 n_i = 5 \cdot \sum_4^8 p_i + 4p_4 + 2p_5 - p_8,$$

whence

$$4p_4 + 2p_5 = 3 + p_8.$$

Since $p_8 \leq 3$, that gives $p_4 = p_5 = 1$, whence $p_8 = 3$, and one of p_6, p_7 is 2, the other 3. Finally we obtain

$$P(E_8, t) = (1+t^3) \cdot (1+t^{15}) \cdot (1+t^{23}) \cdot (1+t^{27}) \cdot (1+t^{35}) \cdot (1+t^{39}) \cdot (1+t^{47}) \cdot (1+t^{59}).$$

BIBLIOGRAPHY

1. A. Borel, *Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts*, Ann. of Math. vol. 57 (1953) pp. 115–207.
2. A. Borel and J. de Siebenthal, *Les sous-groupe fermés connexes de rang maximum des groupes de Lie clos*, Comment. Math. Helv. vol. 23 (1949–50) pp. 200–221.
3. E. Cartan, *Sur les invariants intégraux de certains espaces homogènes clos et les propriétés topologiques de ces espaces*, Ann. Soc. Polonaise Math. vol. 8 (1929) pp. 181–225; Oeuvres complètes, Part I, vol. 2, pp. 1081–1125.
4. C. Chevalley, *The Betti numbers of the exceptional simple Lie groups*, Proceedings of the International Congress of Mathematicians, 1950, Vol 2, 1952, pp. 21–24.
5. H. Hopf, *Ueber die Topologie der Gruppen-Mannigfaltigkeiten und ihrer Verallgemeinerungen*, Ann. of Math. vol. 42 (1941) pp. 22–52.
6. H. Hopf and H. Samelson, *Ein Satz über die Wirkungsräume geschlossener Liescher Gruppen*, Comment. Math. Helv. vol. 13 (1940–41) pp. 240–251.
7. J. L. Koszul, *Homologie et cohomologie des algèbres de Lie*, Bull. Soc. Math. France vol. 78 (1950) pp. 65–127.
8. H. Samelson, *Beiträge zur Topologie der Gruppen-Mannigfaltigkeiten*, Ann. of Math. vol. 42 (1941) pp. 1091–1137.
9. ———, *Topology of Lie groups*, Bull. Amer. Math Soc. vol. 58 (1952) pp. 2–37.
10. Chih-Ta Yen, *Sur les polynomes de Poincaré des groupes de Lie exceptionnels*, C. R. Acad. Sci. Paris vol. 228 (1949) pp. 628–630.

ON A SIMPLE LIE ALGEBRA OF CHARACTERISTIC 2

R. D. SCHAFER¹ AND M. L. TOMBER

Over a field Φ of characteristic 2 any special Jordan algebra is a Lie algebra since the products $X \circ Y = XY + YX$ and $[X, Y] = XY - YX$ coincide. In this note we show that certain 27-dimensional algebras \mathfrak{J} which, over a field of characteristic $\neq 2$, would be exceptional simple Jordan algebras are actually special Jordan algebras over Φ .

In each such \mathfrak{J} the set \mathfrak{J}_0 of elements of trace 0 is a simple Lie algebra of dimension 26. If Φ is algebraically closed, there is one \mathfrak{J}_0 and it is isomorphic to a known symplectic algebra.² \mathfrak{J}_0 provides another counterexample (over an arbitrary field of characteristic 2) to the conjecture of Zassenhaus [4, p. 80]³ that the algebra of outer derivations of a simple Lie algebra of characteristic p is solvable. For the algebra $\mathfrak{D}/\text{ad } \mathfrak{J}_0$ of outer derivations is simple, being isomorphic (if Φ is algebraically closed) to \mathfrak{J}_0 .

Let \mathfrak{C}_3 be the set of all 3×3 matrices with elements in any (generalized) Cayley algebra \mathfrak{C} over an arbitrary field Φ of characteristic 2, and \mathfrak{J} be the 27-dimensional subspace of \mathfrak{C}_3 consisting of all matrices

$$(1) \quad X = \begin{pmatrix} \xi_1 & x_3 & \bar{x}_2 \\ \bar{x}_3 & \xi_2 & x_1 \\ x_2 & \bar{x}_1 & \xi_3 \end{pmatrix}, \quad \xi_i \text{ in } \Phi, \quad x_i \text{ in } \mathfrak{C},$$

where \bar{x} is the conjugate of x in \mathfrak{C} . Define multiplication in \mathfrak{J} by $X \circ Y = XY + YX$ where XY denotes the ordinary matrix multiplication in \mathfrak{C}_3 . We write

Presented to the Society, October 24, 1953.

1. This research was supported in part by a grant from the National Science Foundation.

2. When these results were first announced in a seminar on the structure of Lie algebras of characteristic $p > 0$ at the Society's Summer Mathematical Institute on Lie groups and Lie algebras, we said that \mathfrak{J}_0 was, to the best of our knowledge, a new simple Lie algebra of characteristic 2. This was based on the fact that, by error, no algebra of dimension 26 appeared in the list of known simple Lie algebras of characteristic p which was presented in that seminar.

3. Numbers in brackets refer to references at the end of the paper. Jacobson [3, p. 515] gives a counterexample to Zassenhaus' conjecture over an imperfect field. At the seminar referred to in footnote 2, I. Kaplansky gave a counterexample of dimension 7 over any algebraically closed field of characteristic 3, in which the algebra of outer derivations is isomorphic to the 7-dimensional simple algebra. We are indebted to Kaplansky for his friendly interest and helpful suggestions.

$$(2) \quad X = \xi_1 e_1 + \xi_2 e_2 + \xi_3 e_3 + (x_1)_1 + (x_2)_2 + (x_3)_3$$

for X in (1), and $\mathfrak{X} = \mathfrak{X}_1 + \mathfrak{X}_2 + \mathfrak{X}_3$ where \mathfrak{X}_i is the set of all $T_i = (x_i)_i$. We note that multiplication in \mathfrak{X} is determined by commutativity and the following rules:

$$e_i \circ e_h = 0 \text{ for all } h, \quad e_i \circ T_i = 0,$$

$$e_i \circ T_h = T_h \text{ for } h \neq i,$$

$$(x)_i \circ (y)_i = t(x\bar{y})(e_j + e_k),$$

$$(x)_i \circ (y)_j = (\bar{x}y)_k,$$

where $t(x) = x + \bar{x}$ in Φ , and where we reserve i, j, k for a cyclic permutation of 1, 2, 3. Let $\text{Tr } X = \xi_1 + \xi_2 + \xi_3$, and $e = e_1 + e_2 + e_3$. Then $\mathfrak{X} = \Phi e \oplus \mathfrak{X}_0$, where \mathfrak{X}_0 is the subspace of all elements X satisfying $\text{Tr } X = 0$.

One may verify directly that \mathfrak{X} is a restricted⁴ Lie algebra of characteristic 2, where X^2 is the ordinary square of X in \mathbb{C}_3 . The derived algebra \mathfrak{X}_0 is a 26-dimensional central simple Lie algebra (also restricted) over Φ . It follows that \mathfrak{X} and \mathfrak{X}_0 are special Jordan algebras [2, Theorem 1]. If \mathbb{C} contains divisors of zero (as would be the case if Φ were algebraically closed), this simple algebra \mathfrak{X}_0 is not new, being isomorphic to a symplectic algebra, as may be seen as follows. The elements of \mathbb{C} may be represented as pairs (m, n) of 2×2 matrices m, n with elements in Φ , multiplication of pairs being defined by

$$(m_1, n_1)(m_2, n_2) = (m_1 m_2 + n_2 \bar{n}_1, \bar{m}_1 n_2 + m_2 n_1)$$

where the conjugate of $m = \begin{pmatrix} a & \beta \\ \gamma & \delta \end{pmatrix}$ in Φ_2 is $\bar{m} = \begin{pmatrix} \delta & -\beta \\ -\gamma & a \end{pmatrix}$. Let \mathfrak{Q} be the algebra of 8×8 symplectic matrices of the form

$$(3) \quad \bar{X} = \begin{pmatrix} (\sum_i \xi_i)l & m_1 & n_2 & \bar{m}_3 \\ \bar{m}_1 & \xi_1 l & n_3 & m_2 \\ \bar{n}_2 & \bar{n}_3 & \xi_2 l & \bar{n}_1 \\ m_3 & \bar{m}_2 & n_1 & \xi_3 l \end{pmatrix},$$

ξ_i in Φ , m_i, n_i in Φ_2 . It is known that $\mathfrak{Q}/\Phi l$ is a 26-dimensional simple Lie algebra over Φ . A vector space isomorphism between \mathfrak{X} and \mathfrak{Q} is given by

4. For the definition see [2].

$X = \sum_h \xi'_h e_h + \sum_h ((m_h, n_h))_h \leftrightarrow \bar{X}$ in (3). Computing $\overline{X \circ Y}$ where $Y = \sum_h \xi'_h e_h + \sum_h ((m'_h, n'_h))_h$, we see that

$$(4) \quad \overline{X \circ Y} = [\bar{X}, \bar{Y}] + t(m_1 \bar{m}'_1 + n_2 \bar{n}'_2 + m_3 \bar{m}'_3)I.$$

Hence $\mathfrak{Y}_0 \cong \mathfrak{Y} / \Phi e \cong \mathfrak{L} / \Phi I$.

One derivation D^* of \mathfrak{Y} is defined by $D^*e = e, D^*X = 0$ for every X in \mathfrak{Y}_0 . The derivation algebra $\mathfrak{D}(\mathfrak{Y})$ of \mathfrak{Y} is $\mathfrak{D}(\mathfrak{Y}) = \Phi D^* \oplus \tilde{\mathfrak{D}}$, where $\tilde{\mathfrak{D}}$ is the set of all \tilde{D} in $\mathfrak{D}(\mathfrak{Y})$ satisfying $\tilde{D}e = 0$.

THEOREM. *The derivation algebra $\mathfrak{D} = \mathfrak{D}(\mathfrak{Y}_0)$ of \mathfrak{Y}_0 is 52-dimensional, and the 26-dimensional algebra $\mathfrak{D}/\text{ad } \mathfrak{Y}_0$ of outer derivations of \mathfrak{Y}_0 is simple. If \mathfrak{C} has divisors of zero (as would be the case if Φ were assumed to be algebraically closed), then $\mathfrak{D}/\text{ad } \mathfrak{Y}_0 \cong \mathfrak{Y}_0$.*

The proof follows by the method of [1], where the derivation algebra of the exceptional Jordan algebra \mathfrak{Y} of characteristic 0 is shown to be the 52-dimensional simple Lie algebra F_4 . It is easy to see that $\mathfrak{D} \cong \tilde{\mathfrak{D}}$. For any \tilde{D} in $\tilde{\mathfrak{D}}$, write $\tilde{D}e_i = \sum_h \lambda_{ih} e_h + (x_{ii})_i + (x_{ij})_j + (x_{ik})_k$. Then $0 = \tilde{D}(e_i \circ e_j) = \tilde{D}e_i \circ e_j + e_i \circ \tilde{D}e_j = (x_{ii})_i + (x_{ik})_k + (x_{jj})_j + (x_{jk})_k$ implies $x_{ii} = 0$ and $x_{ih} = x_h$ for $h \neq i$. Hence $\tilde{D}e_i = \sum_h \lambda_{ih} e_h + (x_j)_j + (x_k)_k$. Writing $X = \sum_h (x_h)_h$ in \mathfrak{E} and $D_0 = \tilde{D} - \text{ad } X$ in $\tilde{\mathfrak{D}}$, we see that the derivation D_0 must map each e_i onto 0. Hence $\tilde{\mathfrak{D}} = \text{ad } \mathfrak{Y} \mathfrak{E} + \mathfrak{D}_0$, where \mathfrak{D}_0 is the subalgebra of $\tilde{\mathfrak{D}}$ consisting of all derivations D such that $De_i = 0$ for all $i = 1, 2, 3$. Let D be in \mathfrak{D}_0 . Then $DT_i - D(e_j \circ T_i) = e_j \circ DT_i$ implies DT_i is in $\mathfrak{E}_i + \mathfrak{E}_k$. Similarly DT_i is in $\mathfrak{E}_i + \mathfrak{E}_j$. Hence $D\mathfrak{E}_i \subseteq \mathfrak{E}_i$. Define A_i on \mathfrak{C} by

$$(5) \quad D(x)_i = (A_i x)_i \quad \text{for } D \text{ in } \mathfrak{D}_0.$$

Then $(A_i x)_i \circ (y)_j + (x)_i \circ (A_j y)_j = (A_k \bar{x} \bar{y})_k$. Writing S for the involution $x \rightarrow \bar{x} = SX$, we have

$$(6) \quad (A_i x)y + x(A_j y) = SA_k S(xy) \quad \text{for all } x, y \text{ in } \mathfrak{C}.$$

Let $A_i I = a_i$ in \mathfrak{C} . Then $a_i + a_j = \bar{a}_k$ implying $\sum_h a_h = 0$. Also $A_i x + x a_j = SA_k Sx$ implies $A_i + R_{a_j} = SA_k S$. Let $E = \sum_h A_h$. Then $E = SES$. Hence $(Ex)y + x(Ey) = SES(xy) = E(xy)$, or E is a derivation of \mathfrak{C} . Also $L_{a_i} y + A_j y = SA_k Sy$, implying $L_{a_i} + A_j = SA_k S = A_i + R_{a_j}$, or

$$(7) \quad A_k = E + L_{a_i} + R_{a_j}, \quad (\sum_h a_h = 0).$$

Now (7) implies $A_i + R_{a_j} = E + L_{a_j} + R_{a_k} + R_{a_l} = SA_kS = E + R_{a_i}^- + L_{a_j}^-$, or $t(a_j)I = t(a_i)I$, so that $0 = t(\sum_k a_k) = 3t(a_h) = t(a_h)$. Conversely, any D defined by $De_i = 0$ and (5), where the A_i satisfy (7) with $t(a_h) = 0$, is a derivation of \mathfrak{Y} . Hence \mathfrak{D}_0 (and therefore $\tilde{\mathfrak{D}} \cong \mathfrak{D}$) is determined.

The dimension of \mathfrak{D}_0 is 28, since $E + L_{a_i} + R_{a_j} = 0$ for $i = 1, 2, 3$ implies $a_i + a_j = 0$, or $a_k = 0$ for $k = 1, 2, 3$, and $E = 0$. The derivation algebra $\mathfrak{E} = \mathfrak{D}(\mathfrak{C})$ is known⁵ to have dimension 14. Hence \mathfrak{D}_0 has dimension $14 + 7 + 7 = 28$. It follows that the dimension of \mathfrak{D} , equal to the dimension of $\tilde{\mathfrak{D}}$, is $24 + 28 = 52$. Let \mathfrak{H} be the two-dimensional abelian subalgebra of \mathfrak{Y}_0 spanned by the elements $e_i + e_j$. Then $\text{ad}_{\mathfrak{Y}}\mathfrak{H} \subseteq \mathfrak{D}_0$ and $\text{ad}\mathfrak{Y} = \text{ad}_{\mathfrak{Y}}\mathfrak{H} + \text{ad}_{\mathfrak{Y}}\mathfrak{X}$. Hence $\mathfrak{D}/\text{ad}\mathfrak{Y}_0 \cong \tilde{\mathfrak{D}}/\text{ad}\mathfrak{Y} \cong \mathfrak{D}_0/\text{ad}_{\mathfrak{Y}}\mathfrak{H}$ is of dimension 26 over Φ .

Let \mathfrak{U} be the set of linear transformations on \mathfrak{C} consisting of all $A = E + L_a + R_b$ with $t(a) = t(b) = 0$, E in $\mathfrak{E} = \mathfrak{D}(\mathfrak{C})$. The dimension of \mathfrak{U} is 27, since $A = 0$ implies $a + b = 0$, or $E = L_a - R_a$ is a derivation of \mathfrak{C} , which implies, since the characteristic is $\neq 3$, that $a = al$. For each $i = 1, 2, 3$, the mapping $D \rightarrow A_i$ given by (5) is a homomorphism of \mathfrak{D}_0 onto \mathfrak{U} . ΦI is an ideal in \mathfrak{U} whose complete inverse image in \mathfrak{D}_0 is $\text{ad}_{\mathfrak{Y}}\mathfrak{H}$. Hence $\mathfrak{D}/\text{ad}\mathfrak{Y}_0 \cong \mathfrak{D}_0/\text{ad}_{\mathfrak{Y}}\mathfrak{H} \cong \mathfrak{U}/\Phi I$.

If \mathfrak{C} has divisors of zero, then $\mathfrak{U}/\Phi I \cong \mathfrak{Y}_0$. For the elements of \mathfrak{C} may be represented as pairs (m, n) of elements m, n in Φ_2 . Let e_{ij} be elements of a usual matrix basis for Φ_2 and $f_{ij} = (0, e_{ij})$. With respect to the basis $(e_{11}, e_{22}, e_{12}, e_{21}, f_{11}, f_{22}, f_{12}, f_{21})$ one may compute the matrices of the linear transformations in \mathfrak{U} and see that they all have the form (3). Since the dimensions of \mathfrak{U} and \mathfrak{Q} are both 27, we have $\mathfrak{U} \cong \mathfrak{Q}$. Hence $\mathfrak{U}/\Phi I \cong \mathfrak{Q}/\Phi I \cong \mathfrak{Y}_0$. It follows that $\mathfrak{D}/\text{ad}\mathfrak{Y}_0 \cong \mathfrak{U}/\Phi I$ is simple for an arbitrary Cayley algebra \mathfrak{C} over an arbitrary field Φ .

REFERENCES

1. C. Chevalley and R. D. Schafer, *The exceptional simple Lie algebras F_4 and E_6* , Proc. Nat. Acad. Sci. U. S. A. vol. 36 (1950) pp. 137-141.
2. N. Jacobson, *Restricted Lie algebras of characteristic p* , Trans. Amer. Math. Soc. vol 50 (1941) pp. 15-25.
3. ———, *Classes of restricted Lie algebras of characteristic p* , I, Amer. J. Math. vol. 63 (1941) pp. 481-515.
4. H Zassenhaus, *Über Liesche ringe mit primzahlcharakteristik*, Abh. Math. Sem. Hansischen Univ. vol. 13 (1939) pp. 1-100.

UNIVERSITY OF CONNECTICUT AND
AMHERST COLLEGE

5. In the seminar mentioned in footnote 2, Kaplansky announced that $\mathfrak{E} = \mathfrak{D}(\mathfrak{C})$ is 14-dimensional for all Φ and simple for Φ of characteristic $\neq 3$.

ON THE DERIVATION ALGEBRA AND THE HOLOMORPH OF A NILPOTENT ALGEBRA

EUGENE SCHENKMAN*

Introduction. In [2] Mills shows that the holomorph of an Abelian group determines the group up to isomorphism. We are interested here in the similar question of whether the holomorph of a Lie algebra determines the algebra up to isomorphism; and show that the answer is in the affirmative if the algebra is a free nilpotent Lie algebra of finite class generated by $q \neq 2$ elements.

In order to prove the above result it is necessary to make a study of derivations of nilpotent Lie algebras. It will be shown that a sequence of characteristic ideals of the derivation algebra of a nilpotent Lie algebra is determined in a natural manner by the members of the descending central series of the algebra. In particular those derivations which send the algebra into its commutator subalgebra form a nilpotent ideal of the derivation algebra which is actually the nil radical in case the algebra is a free nilpotent algebra of finite class.

It will also be shown that any map of a minimal set of generators of a free Lie algebra into the algebra can be extended in one and only one way to be a derivation of the algebra. From this it follows that the derivation algebra of an arbitrary Lie algebra L is the homomorphic image of a subalgebra of the derivation algebra of the free Lie algebra generated by the generators of L . Several related results will also be mentioned.

I should like to express my appreciation to Professors Amitsur, Goto, and Jacobson for conversations with them during the preparation of this paper.

1. Preliminaries. If L is a Lie algebra over a field Φ then \hat{d} is a derivation in L if \hat{d} is a linear map of L into L , and if for $l_1, l_2 \in L, [l_1, l_2]\hat{d} = [l_1\hat{d}, l_2] + [l_1, l_2\hat{d}]$. As is well known the set of derivations of L form a Lie algebra \hat{D} called the derivation algebra of L . The holomorph H of L is defined to be the semi direct sum of L and D (where D is an isomorphic copy of \hat{D}) in the following manner. As a vector space H is the direct sum of L and D ; that is, for $h \in H$ there is a unique representation $h = l + d$ where $l \in L, d \in D$. Finally commutation in H is given by $[h_1, h_2] = [l_1 + d_1, l_2 + d_2] = [l_1l_2 + l_1\hat{d}_2 - l_2\hat{d}_1 + d_1d_2]$ where $d_1d_2 \in D$ and $l_1l_2 + l_1\hat{d}_2 - l_2\hat{d}_1 \in L$; \hat{d}_1 and \hat{d}_2 being the elements of \hat{D} corresponding to d_1 and d_2 under the isomorphism between \hat{D} and D . It is easy to verify that the holomorph is a Lie algebra, that L is an ideal of H and that D is a subalgebra

* This research was supported in whole or in part by the U. S. Air Force under contract number AF18(600)-790 monitored by the Office of Scientific Research.

of H .

An inner derivation of L is given by the map $X \rightarrow [x, l]$, which we shall denote by \hat{l} or also in general by \hat{i} . Of course if l is in the center of L then $\hat{l} = 0$. If $i \in D$ and $l \in L$ correspond to the same derivation $\hat{i} = \hat{l}$ then $i - l$ is in the centralizer L^* of L in H . Conversely, if l^* is in the centralizer L^* then $l^* = l + d$ where $l \in L$, $d \in D$, and $\hat{l} = -\hat{d}$; whence \hat{d} is the inner derivation corresponding to $-l$. Thus L^* consists precisely of the elements $i - l$ where i corresponds to the inner derivation determined by l .

In fact there is an automorphism θ of period 2 of H given by $l\theta = i - l$ for $l \in L$ and $d\theta = d$ for $d \in D$. For θ is clearly a linear mapping and a direct check shows that $[(l_1 + d_1)\theta, (l_2 + d_2)\theta] = [l_1 + d_1, l_2 + d_2]\theta$. Since θ sends L into L^* we see that L^* is isomorphic to L , L is the centralizer of L^* , D is the derivation algebra and H is the holomorph of L^* as well as of L .

II. Some remarks on ideals of the holomorph. In what follows H will denote the holomorph of L and L^* ; L^* is centralizer of L , L^* centralizer of L ; \hat{D} will denote the derivation algebra of L and L^* , D the isomorphic copy of \hat{D} contained in H .

(1) If K is an ideal of H then $K \cap L^* \neq 0$ or else $[K, L^*] \subset K \cap L^* = 0$ and $K \subset L$. It follows that $K \cap \{L, L^*\} \neq 0$ where $\{L, L^*\}$ denotes the algebra generated by L and L^* .

(2) If $K \not\supset L$, L finite, then H is not the holomorph of K . For if so the centralizer K^* of K would be contained in $L^* \cong L$, a proper part of K ; on the other hand if H is the holomorph of K we know that the centralizer of K should be isomorphic to K ; this would be a contradiction.

From (1) and (2) we deduce the following result.

THEOREM 1. *If L is a finite Abelian Lie algebra with holomorph H then H is the holomorph of no other Lie algebra.*

PROOF. Suppose that H were also the holomorph of the Lie algebra K . Then by (1) K intersects L since $\{L, L^*\} = L$ when L is Abelian. On the other hand there are no ideals of H contained in L other than L since any linear transformation of an Abelian Lie algebra is a derivation. Hence $K \cap L = L$ and $K \supset L$. But then we know by (2) that $K = L$.

DEFINITION. If $h = l + d$ where $h \in H$, $l \in L$, $d \in D$ then we shall call l the first component, d the second component of h in the representation as an element of the holomorph of L .

(3) If K is an ideal of H then the set of first components of the elements of K is an ideal of H and the set of second components is an ideal of D .

III. Some remarks on derivation algebras and free nilpotent algebras.

(1) If L is a Lie algebra with characteristic ideal M and derivation algebra \hat{D} then the set of derivations \hat{D}_M which map L into M form an ideal of \hat{D} (characteristic ideal M means that $M\hat{D} \subset M$). For $L[\hat{D}_M, \hat{D}] \subset L\hat{D}_M\hat{D} + L\hat{D}\hat{D}_M \subset M$.

(2) If \hat{D}_M is an ideal of \hat{D} then $L\hat{D}_M$ is a characteristic ideal of L . For $(L\hat{D}_M)\hat{D} \subset L\hat{D}\hat{D}_M + L[\hat{D}_M, \hat{D}] \subset L\hat{D}_M$.

(3) If e_α are a minimal set of generators of a free Lie algebra L , then any map \hat{d} which sends e_α into elements of L can be extended in one and only one way to be a derivation of L . For (cf. [1], p. 20) \hat{d} can be extended in one and only one way to be a derivation of the free algebra F generated by the e_α and according to [3] L can be considered as a submodule of F closed under commutation $[a, b] = ab - ba$ for $a, b \in F$. Now \hat{d} induces a derivation in L since every element of L is of the form $\Sigma\gamma[\dots[e_i, e_j]\dots e_r]$ and $\Sigma\gamma[\dots[e_i, e_j]\dots e_r]\hat{d} = \Sigma\gamma[\dots[e_i, e_j]\dots e_p\hat{d}\dots e_r]$ which is in L since $e_p \in L$.

(4) If \hat{D} is the derivation algebra of L and if M is a subspace of L then \hat{D}_{LM} , the subset of derivations which map L into M , is a subalgebra of \hat{D} ; and so also is the set of derivations \hat{D}_M which map M into itself. In fact \hat{D}_{LM} is normal in \hat{D}_M ; for $L[\hat{D}_{LM}, \hat{D}_M] \subset (L\hat{D}_{LM})\hat{D}_M + (L\hat{D}_M)\hat{D}_{LM} \subset M$.

With the help of (3) and (4) we can prove the following result.

THEOREM 2. *If K is an arbitrary Lie algebra and if L is the free Lie algebra with the smallest possible number of generators such that $K = L/M$ then the algebra of derivations of K is isomorphic to \hat{D}_M/\hat{D}_{LM} where \hat{D}_M and \hat{D}_{LM} send M and L into M , respectively.*

PROOF. Let e_α be a minimal set of generators for L and $e_\alpha + M$ be a minimal set of generators for L/M . It is clear that if $\hat{d} \in \hat{D}_M$ then $(e_\alpha + M)\hat{d} = e_\alpha\hat{d} + M$ and \hat{d} induces a derivation in L/M , and in fact \hat{D}_M determines an algebra of derivations of L/M which is an homomorphic image of \hat{D}_M . On the other hand each derivation of L/M sends $e_\alpha + M$ into some $a_\alpha + M$. By (3) we know that there are derivations of L determined by the prescription that e_α maps into $a_\alpha + m_\alpha$, m_α arbitrary in M ; we shall call these the derivations of L associated with the given derivations of L/M . Since zero maps into zero under derivations it is clear that the associated derivations are all in \hat{D}_M and hence the algebra of derivations of L/M determined by \hat{D}_M is the full derivation algebra. Clearly the kernel of the homomorphism is \hat{D}_{LM} and the theorem follows.

COROLLARY. *The derivation algebra of a free nilpotent Lie algebra of class n (that is a free Lie algebra L modulo the $(n+1)$ st member of the descending central series L^{n+1}) generated by q elements has dimension q times the dimension*

of the Lie algebra. Consequently the dimension of the holomorph of such a Lie algebra is $q+1$ times that of the given Lie algebra.

For if $m_i, i=1, \dots, k$, constitute a basis of L then by (3) and the theorem, each derivation of L is determined by a map which holds $q-1$ generators fixed and sends the remaining generator into one of the m_i .

LEMMA 1. *The center of a free nilpotent Lie algebra L of class n generated by $q > 2$ elements has dimension equal to or greater than half the dimension of L . Equality holds only for $n=2, q=3$.*

The proof depends on the fact that the homogeneous expressions of degree k in the q generators form a module of dimension

$$f_q(k) = \frac{1}{k} \sum_{d|k} M(d)q^{\frac{k}{d}}$$

($M(d)$ the Moebius function; cf. [3]). Since the dimension of the center L^n of L is the same as the dimension of the module of homogeneous expressions of degree n , and since the dimension of L/L^n is the dimension of the module of homogeneous expressions of degree less than n , the lemma will be proved if we show that $f_q(n) \geq \sum_{r=1}^{n-1} f_q(r)$. We demonstrate the last statement by showing that $f_q(n) \geq 2f_q(n-1)$, equality holding only when $n=2, q=3$. We check this directly for $n = 2, 3, 4, 5, 6$ from the facts that $f_q(1) = q$; $f_q(2) = (1/2)(q^2 - q)$; $f_q(3) = (1/3)(q^3 - q)$; $f_q(4) = (1/4)(q^4 - q^2)$; $f_q(5) = (1/5)(q^5 - q)$; $f_q(6) = (1/6)(q^6 - q^3 - q^2 + q)$. For $n > 6, q \geq 3$ since $q^r > q^{r-1} = (q^{r-1} + \dots + q + 1)(q-1) \geq (2q^{r-1} + \dots + 2q + 2)$ we have

$$\begin{aligned} q^n &> \frac{n}{n-1} (2q^{n-1} + q^{\lfloor \frac{n}{2} \rfloor + 2}) \geq \frac{n}{n-1} (2q^{n-1} + 2q^{\lfloor \frac{n}{2} \rfloor} + 2q^{\lfloor \frac{n}{2} \rfloor - 1} + \dots + 2q^2 + 2q + 2q) \\ &= \frac{2n}{n-1} (q^{n-1} + q^{\lfloor \frac{n}{2} \rfloor} + q^{\lfloor \frac{n}{2} \rfloor - 1} + \dots + q + q). \end{aligned}$$

Therefore

$$\frac{1}{n} q^n > \frac{2}{n-1} (q^{n-1} + q^{\lfloor \frac{n}{2} \rfloor} + \dots + q + q)$$

and it can now be readily seen from the definition of $f_q(n)$ that $f_q(n) > 2f_q(n-1)$ since n and $n-1$ have no common factors other than 1. This completes the proof of the lemma.

(5) If L is any nilpotent Lie algebra with center Z then any linear mapping \hat{d} which sends any minimal set of generators of L into elements of Z can be extended in one and only one way to be a derivation of L . For if α_a are the genera-

tors such that $a_\alpha \hat{d} = z_\alpha, z_\alpha \in Z$ then $[a_\alpha, a_\beta] \hat{d} = [z_\alpha, a_\beta] + [a_\alpha, z_\beta] = 0$ and hence $L^2 d = 0$. Of course it is well known that no element of a minimal set of generators of a nilpotent Lie algebra can be in the commutator subalgebra.

LEMMA 2. *If L is a free nilpotent Lie algebra of class n then every characteristic ideal of L other than L and L^2 is contained in L^3 . If in addition the field is of characteristic other than 2 and 3, then L, L^2 , and L^3 are the only characteristic ideals properly containing L^4 .*

PROOF. Suppose M were a characteristic ideal containing L^2 and let $e \in M, e \notin L^2$ and let a be arbitrary in L . Then by (3) there is a derivation which maps e into a ; hence $a \in M$ and $L \subset M$; that is, there is no characteristic ideal between L^2 and L .

Now suppose M is a characteristic ideal properly containing L^3 but not L^2 . If e_1, \dots, e_q are a minimal set of generators of L and $[e_1, e_2] \in M$ then $[e_k, e_2] \in M, k = 3, \dots, q$; for by (3) there is a derivation such that e_1 maps to e_k and e_2 to zero whence $[e_1, e_2]$ maps into $[e_k, e_2]$. Similarly $[e_k, e_2] \in M$ implies that $[e_k, e_l] \in M$ and thus $L^2 \subset M$. Now if $\sum_{ij} \gamma [e_i, e_j] \in M$ then by (3) we know there is a derivation which maps e_{i_0} into e_{i_0} and all other e_i into zero; and hence there is an element of the form $\sum_j \gamma [e_{i_0}, e_j] \in M$. But again by a suitable derivation we know there is an element of the form $[e_{i_0}, e_{j_0}] \in M$ and hence from the above remarks $L^2 \subset M$.

Finally we must show that if M is a characteristic ideal in L^3 properly containing L^4 then $M = L^3$. If $[[e_{i_0}, e_{j_0}] e_{k_0}] \in M$ then as before we can readily see that $[[e_i, e_j] e_k] \in M$ for arbitrary ij, k and hence $L^3 \subset M$. If $\sum_{i,j,k} \gamma [[e_i, e_j] e_k] \in M$ then again as above this implies $\sum_{j,k} \gamma [[e_{i_0}, e_j] e_k] \in M$ which implies that $\sum_k \gamma [[e_{i_0}, e_{j_0}] e_k] + \sum_r \delta [[e_{i_0}, e_r] e_{j_0}] \in M$. But setting $\sum_k \gamma e_k = e_m$ and $\sum_r \delta e_r = e_n$ we have $[[e_{i_0}, e_{j_0}] e_m] + [[e_{i_0}, e_m] e_{j_0}] \in M$ whence $[[e_{i_0}, e_{j_0}] e_m]$ is in M if e_n is linearly independent of the space spanned by e_{i_0}, e_{j_0}, e_m . Otherwise there is an element in M either of the form $[[e_{i_0}, e_{i_1}] e_{i_1}]$ or of the form $[[e_{i_0}, e_{i_1}] e_{i_2}] + [[e_{i_0}, e_{i_2}] e_{i_1}]$. Now it is clear that there is a derivation which maps the first of these into the second and also a derivation mapping the second into the first when the characteristic of the underlying field is not 2. From this fact we can see that either type of element in M implies that for all i, j, k , all the elements of both types are in M . But if $[[e_i, e_j] e_k] + [[e_i, e_k] e_j] \in M$ and if $[[e_j, e_i] e_k] + [[e_j, e_k] e_i] \in M$ then by the Jacobi identity $3[[e_i, e_j] e_k] \in M$ and hence when the characteristic of the underlying field is not 3 all of $L^3 \subset M$ as was to be shown. This completes the proof of the lemma.

REMARK. If a, b, c are the generators of a free Lie algebra L over a field

of characteristic 3 then the subalgebra of L generated by L^4 , $[[a, b]b]$, $[[a, c]c]$, $[[b, c]c]$, $[[b, a]a]$, $[[c, b]b]$, $[[c, a]a]$ and $[[a, b]c] + [[a, c]b]$ is a characteristic ideal of L not equal to L^3 .

I was unable to determine whether all the characteristic ideals of the free Lie algebra L are formed from the powers of L by means of unions, intersections, and commutation in case the underlying field is of characteristic zero.

(6) If L is a nilpotent Lie algebra, for $k = 1, 2, \dots$, let \hat{D}_k be the set of derivations that map L into L^{k+1} . Then by (1) \hat{D}_k is an ideal of \hat{D} the derivation algebra of L ; and in fact it can readily be seen that $[\hat{D}_k, \hat{D}_l] \subset \hat{D}_{k+l}$. It follows that \hat{D}_1 is a nilpotent ideal of \hat{D} . Similarly when H is the holomorph of L then $D_1 + L$ is a nilpotent ideal of H ; if n is the class of L , L^n is the center of $L + D_1$.

(7) If L is a free nilpotent Lie algebra of class n then in the notation of (6) ($D_i \subset H$ corresponding to \hat{D}_i) we have $L^k, L^{k-1} + D_{k-1}, L^{k-2} + D_{k-2}, \dots, L + D_1$ are the members of the ascending central series of $L + D_1$ and hence are invariant under every automorphism of H because of the following theorem, which states that $L + D_1$ is the nil radical of H . It should be noted that the class of $L + D_1$ is the same as that of L .

THEOREM 3. *If L is a free nilpotent Lie algebra of class n generated by q elements then \hat{D}_1 as defined in (6) is the nil radical of \hat{D} ; $L + D_1$ is the nil radical of H the holomorph of L ; and the center of L is the center of $L + D_1$.*

PROOF. It follows from (6) that \hat{D}_1 is a nilpotent ideal and hence is contained in the nil radical of \hat{D} . Let \hat{j} be a derivation such that if for $i = 1, \dots, q$, e_i is a minimal set of generators of L then $e_i \hat{j} = e_i$. Then $\hat{D}_1 + (\hat{j})$ is the radical of \hat{D} . For $\hat{D}_1 + (\hat{j})$ is an ideal of \hat{D} since the mapping induced by \hat{j} in L/L^2 is the identity derivation and $\hat{D}/\hat{D}_1 + (\hat{j})$ is isomorphic to an image of \hat{D}/\hat{D}_1 ; but the latter is precisely the algebra of linear transformations of a vector space and from its structure we know $\hat{D}/\hat{D}_1 + (\hat{j})$ has no solvable ideal. Hence $\hat{D}_1 + (\hat{j})$ contains the radical of \hat{D} . On the other hand \hat{D}_1 is a nilpotent ideal of $\hat{D}_1 + (\hat{j})$ of one dimension less and hence $\hat{D}_1 + (\hat{j})$ is solvable. Hence $\hat{D}_1 + (\hat{j})$ is the radical of \hat{D} . Now $\hat{D}_1 + (\hat{j})$ is not nilpotent for if \hat{d}_1 is a derivation such that $e_1 \hat{d}_1 = [e_1, e_2]$ and for $i = 2, 3, \dots, q$, $e_i \hat{d}_1 = 0$ then $e_1 [\hat{d}_1, \hat{j}] = e_1 \hat{d}_1 \hat{j} - e_1 \hat{j} \hat{d}_1 = 2[e_1, e_2] - [e_1, e_2] = [e_1, e_2]$ and $e_i [\hat{d}_1, \hat{j}] = 0$ whence $[\hat{d}_1, \hat{j}] = \hat{d}_1$. (In fact by this type of argument $[\hat{D}_1, (\hat{j})] = \hat{D}_1$). Hence \hat{j} is not nilpotent in \hat{D} and hence is not in the nil radical. It follows that \hat{D}_1 is the nil radical of \hat{D} as the theorem asserts. Similarly it can be seen that $L + D_1$ is the nil radical of H . The last statement of the theorem follows from (6).

(8) It should be noted that under the assumptions of Theorem 2 if $\hat{r} \in \hat{R}$, the

radical of \hat{D} , $\hat{r} \notin \hat{N}$, \hat{N} the nil radical of \hat{D} , then \hat{R} is the smallest ideal of \hat{R} containing \hat{r} . For $\hat{r} = \hat{j} + \hat{n}$ where $\hat{n} \in \hat{N}$ and $[\hat{D}_1, \hat{r}] = [\hat{D}_1, \hat{j} + \hat{n}] = \hat{D}_1 \pmod{\hat{D}_2}$ whence $[[\hat{D}_1, \hat{r}] \xrightarrow{k \text{ times}} r] = \hat{D}_1 \pmod{\hat{D}_k}$ for all \hat{k} and \hat{D}_1 is in the smallest ideal containing \hat{r} as asserted.

IV. On the isomorphisms between Lie algebras having the same holomorph.

LEMMA 3. *If H is the holomorph of the finitely generated free nilpotent Lie algebra of finite class L and also of k then k is nilpotent.*

PROOF. K is normal in H . If it were not nilpotent then it would either have a simple non-Abelian factor in its composition series (which is impossible for then H should have at least two such non-Abelian factors, whereas we can see from II, (6) that H modulo the nilpotent ideal $L + D_1$ is isomorphic to the full algebra of linear transformations of a vector space and therefore H has only one non-Abelian factor); or else K contains an element r in the radical but not in the nil radical which is impossible in view of III, (8); for H cannot be the holomorph of its radical. Hence K must be nilpotent as the lemma asserts.

THEOREM 3. *If H is the holomorph of L , a free nilpotent Lie algebra of class n generated by $q \neq 2$ elements, then H cannot also be the holomorph of another Lie algebra K unless K is isomorphic to L .*

PROOF. We assume $q \geq 3$ since if $q = 1$, L is Abelian, and the statement follows from Theorem 1. Suppose K is another Lie algebra such that H is the holomorph of K . Then by the previous lemma K is in the nil radical of H .

Now if K were contained in $L^2 + D_2$ (cf. III, (6)) then $L^{n-1} + D_{n-1}$ would be in the centralizer K^* of K ; but K^* is sent into K by an automorphism of H and since by III, (7) $L^{n-1} + D_{n-1}$ is invariant under all automorphisms of H , $L^{n-1} + D_{n-1}$ is also in K and hence in the center of K . But then the center of K has a dimension greater than half the dimension of H (in case $n=2, q=3, L^2 + D_2 - L^2$ and K is Abelian whence Theorem 1 applies); for D_{n-1} has dimension equal to q times that of L^n the center of L and then the assertion follows by an application of the corollary to Theorem 2 and Lemma 1. It follows from III, (5) that there should be at least as many linearly independent derivations of K as the dimension of its center. But in the case under consideration H is not large enough for this and hence cannot be the holomorph of K if $K \subset L^2 + D_2$.

Accordingly we assume that there is an element $k \in K$ such that $k = l + d$ where either $l \notin L^2$ or $d \notin D_2$. If $l \notin L^2$ then by II, (3) and Lemma 2 the first components of K exhaust all of L . It follows that no $d \in D$ can be in the centralizer of L and hence the dimension of the derivation algebra of K is at least as

great as that of D . This means that the dimension of K can be at most that of L . Then if for $i = 1, \dots, r$, e_i are a basis for L wherein e_1, \dots, e_q are a minimal set of generators of L then $e_i + d_i$ are a basis for K and $e_1 + d_1, \dots, e_r + d_q$ are a set of generators of K . But then K is isomorphic to L since it is an image of L (L being free) of the same dimension as L and the theorem is true in this case.

Finally we consider the case where for all $k \in K$ the first components of K are in L^2 . Then for some $k, k = l + d, d \notin D_2$. But then for some $e \in L, e \notin L^2, [e, k] \in L, [e, k] \notin L^3$; hence by Lemma 2 and II, (3) again all of $L^2 \subset K$. But then $d \in K$ and then again by Lemma 1 there are not enough elements of L as there should be according to III, (5) to send d into every element of L^n which is in the center of K since it is in the center of the nil radical of H . With this the theorem is proved.

REMARK. It might be of interest to mention that if H is the holomorph of a semi-simple Lie algebra L over a field of characteristic zero and also of K , then K is isomorphic to L . For every derivation of L is inner and therefore H is the direct product of L and L^* where L^* is the centralizer of L isomorphic to L . Hence H is semi-simple and contains a copy of each simple direct factor an even number of times.

BIBLIOGRAPHY

1. C. Chevalley, *Théorie des Groupes de Lie*, Tome II, Paris, Hermann, 1951.
2. W. H. Mills, *On the non-isomorphism of certain holomorphs*, Trans. Amer. Math. Soc. vol. 74 (1953) pp. 428–443.
3. E. Witt, *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. vol. 177 (1937) pp. 152–160.

LOUISIANA STATE UNIVERSITY AND
THE INSTITUTE FOR ADVANCED STUDY

ON THE GROUP OF AUTOMORPHISMS OF A LOCALLY COMPACT CONNECTED GROUP

MORIKUNI GOTO

1. Introduction and preliminaries. The purpose of this note is to establish a tower theorem for locally compact connected groups, which is an analogue to the theorem proved by H. Wielandt [5] for finite groups and to that by C. Chevalley [1] and E. Schenkman [4] for Lie algebras, and to consider some related subjects. We begin with some preliminary remarks.

Automorphism group of a locally compact connected group. Let G be a locally compact group, and $\tilde{\mathfrak{A}}(G)$ the automorphism group, namely the group of all bi-continuous automorphisms, of G . We can introduce a natural topology (the so-called compact open topology) in $\tilde{\mathfrak{A}}(G)$ so that $\tilde{\mathfrak{A}}(G)$ becomes a topological group. If in particular, G is a connected Lie group, then this topology coincides with the topology of $\tilde{\mathfrak{A}}(G)$ as a linear Lie group over the Lie algebra of G . Now denote by $\mathfrak{A}(G)$ the connected component group of $\tilde{\mathfrak{A}}(G)$ containing the identity. In this note we limit ourselves to connected G 's. Then $\mathfrak{A}(G)$ contains the group $\mathfrak{I}(G)$ composed of all inner automorphisms of G , and we have a continuous homomorphism (adjoint representation in Lie group case) of G onto $\mathfrak{I}(G)$, the kernel of which coincides with the center of G . Now it is to be remarked that $\mathfrak{A}(G)$ is not always locally compact. (See Goto [2].)

Tower theorem of locally compact connected groups. Now our tower theorem, suggested by C. Chevalley and N. Jacobson, can be formulated as follows:

TOWER THEOREM. *Let G be a locally compact connected group with totally disconnected center. Then*

(1) $\mathfrak{A}(G)$ is locally compact, and has no center.

From (1), we can define the series $\mathfrak{A}^2(G) = \mathfrak{A}(\mathfrak{A}(G))$, ..., $\mathfrak{A}^{k+1}(G) = \mathfrak{A}(\mathfrak{A}^k(G))$ inductively, and we have

(2) *For some integer k on, all continuous automorphisms of $\mathfrak{A}^k(G)$ are inner:*

$$\mathfrak{A}^k(G) = \mathfrak{A}(\mathfrak{A}^k(G)) \cong \mathfrak{A}^{k+1}(G) \cong \mathfrak{A}^{k+2}(G) \cong \dots$$

Here, by the expression that a group G has no centers or G is with no center, we mean that the center of G is composed of the identity only.

Now we want to mention the following two theorems, which are essential for our proof.

Structure theorem of locally compact connected groups. The theorem established mainly by K. Iwasawa [3] and H. Yamabe [6], [7] is stated usually as follows:

THEOREM. *Let G be a locally compact connected group. Then we can find a neighborhood G_I of the identity e of G , a closed local Lie group L_I^* in G_I , and a compact subgroup K , such that G_I is the direct product of L_I^* and K :*

$$G_I = L_I^* \times K.$$

Here let us consider the group L^* which is generated by L_I^* in G . Then we can find a uniquely determined connected Lie group L which maps continuously and isomorphically onto L^* . It is obvious that

$$G = L^*K \quad [L^*, K] = e,$$

where $[L^*, K]$ denotes the commutator group of L^* and K .

Denote by D^* the intersection of L^* and K , and let D be the inverse image of D^* in L . Then from $L_I^* \cap K = e$ we see that D is a discrete normal, accordingly central, subgroup of L . We want to call a local decomposition of a locally compact connected group in the structure theorem a *canonical decomposition*, including the notions of L , L^* , D and D^* as stated above. It is to be remarked that L^* is a closed subgroup of G if and only if D , or D^* , is a finite group, and for some G , L^* can never be closed for any choice of canonical decompositions. (See Iwasawa [3] and Goto [2]).

Tower theorem of Lie algebras (see e.g., Schenkman [4]). Let \mathfrak{L} be a Lie algebra of finite rank over an arbitrary field, and let $\mathfrak{F}(\mathfrak{L})$ be the Lie algebra of all derivations of \mathfrak{L} . Denote by $\mathfrak{S}(\mathfrak{L})$ the subalgebra of $\mathfrak{F}(\mathfrak{L})$ composed of inner derivations. Then the theorem proved by Chevalley [1] and Schenkman [4] may be stated as follows:

THEOREM. *Let \mathfrak{L} be a Lie algebra with no center and of finite rank over a field. Consider the series of successive Lie algebras*

$$\mathfrak{L}, \mathfrak{F}(\mathfrak{L}), \mathfrak{F}^2(\mathfrak{L}) = \mathfrak{F}(\mathfrak{F}(\mathfrak{L})), \dots, \mathfrak{F}^{k+1}(\mathfrak{L}) = \mathfrak{F}(\mathfrak{F}^k(\mathfrak{L})), \dots$$

Then for some integer k on, all derivations of $\mathfrak{F}^k(\mathfrak{L})$ are inner, and we get

$$\mathfrak{F}^k(\mathfrak{L}) = \mathfrak{S}(\mathfrak{F}^k(\mathfrak{L})) \cong \mathfrak{F}^{k+1}(\mathfrak{L}) \cong \mathfrak{F}^{k+2}(\mathfrak{L}) \cong \dots$$

Now we want to add some known facts for later use. Let L be a connected Lie group, and \mathfrak{L} the corresponding Lie algebra (over the field of real numbers). Then the Lie algebra of the inner automorphism group $\mathfrak{A}(L)$ is $\mathfrak{A}(\mathfrak{L})$, and if in particular L is simply connected, then the Lie algebra of $\tilde{\mathfrak{A}}(L)$ (or $\mathfrak{A}(L)$) is $\mathfrak{E}(\mathfrak{L})$.

2. Lemmas.

LEMMA 1. *Let G be a locally compact connected group, and let $G = L^*K$ be a canonical decomposition. Then*

- (1) K is mapped onto itself by $\mathfrak{A}(G)$: $\mathfrak{A}(G)K = K$.
- (2) L^* is mapped onto itself by $\mathfrak{A}(G)$: $\mathfrak{A}(G)L^* = L^*$,

if either (a) K has totally disconnected center, or (b) L is perfect, i.e., $[L, L] = L$.

PROOF. (1) We can take L_l^* so small that it contains no subgroup other than the identity group. Then K is the largest subgroup in $G_l = L_l^* \times K$. Hence for a suitably chosen neighborhood \mathfrak{U} of the identity of $\tilde{\mathfrak{A}}(G)$, K is mapped onto itself by \mathfrak{U} . Therefore K is mapped onto itself by the open subgroup $\{\mathfrak{U}\}$ of $\tilde{\mathfrak{A}}(G)$ generated by \mathfrak{U} . Now since $\mathfrak{A}(G)$ is contained in $\{\mathfrak{U}\}$, K is mapped onto itself by $\mathfrak{A}(G)$.

(2) Let σ be an element of $\mathfrak{A}(G)$. We may find a connected neighborhood L_ρ of the identity of L so that

$$\sigma(L_\rho^*) \subseteq L_l^* \times K,$$

where L_ρ^* denotes the image of L_ρ in L^* . Then for x in L^* we have a continuous decomposition

$$\sigma(x) = l(x)k(x)$$

where

$$l(x) \in L^*, k(x) \in K.$$

Now from $xy = yx$ for $y \in K$ we have $\sigma(x)\sigma(y) = \sigma(y)\sigma(x)$, namely $l(x)k(x)\sigma(y) = \sigma(y)l(x)k(x)$, whence $k(x)\sigma(y) = \sigma(y)k(x)$. Since $\sigma(y)$ is arbitrary in K with y , $k(x)$ must be contained in the center of K . Now we consider two cases (a) and (b) separately.

(a) Because $\{k(x) \mid x \in L^*\}$ is connected, and is contained in the totally disconnected center of K ,

(b) Because $k(x)$ gives a continuous homomorphism from a perfect local Lie group L_ρ^* into a commutative group,

$k(x) = e$ in both cases. Namely $\mathfrak{U}(G)L_\rho^* \subseteq L_I^*$, whence $\mathfrak{U}(G)L^* = L^*$.

LEMMA 2. *Let L_0 be a connected Lie group with no center. Then the automorphism group $\tilde{\mathfrak{U}}(L_0)$ is the same as the automorphism group $\tilde{\mathfrak{U}}(\tilde{L})$ of the universal covering group \tilde{L} of L_0 acting as a linear group over the common Lie algebra \mathfrak{Q} of L and L_0 . In particular the Lie algebra of $\mathfrak{U}(L_0)$ coincides with the derivation algebra $\mathfrak{E}(\mathfrak{Q})$ of \mathfrak{Q} .*

PROOF. Every element of $\tilde{\mathfrak{U}}(\tilde{L})$ maps the center of \tilde{L} onto itself. On the other hand L_0 is the factor group of \tilde{L} modulo the center. Therefore $\tilde{\mathfrak{U}}(\tilde{L})$ induces a subgroup of $\tilde{\mathfrak{U}}(L_0)$, namely we have a continuous homomorphism from $\tilde{\mathfrak{U}}(\tilde{L})$ into $\tilde{\mathfrak{U}}(L_0)$.

But because \tilde{L} and L_0 are locally isomorphic and \tilde{L} is simply connected, every element of $\tilde{\mathfrak{U}}(L_0)$ induces an automorphism of \tilde{L} . Therefore this homomorphism is onto.

Let now $\tilde{\sigma}$ be an automorphism of \tilde{L} such that $\tilde{\sigma}(\tilde{x})\tilde{x}^{-1}$ is contained in the center for every element \tilde{x} of \tilde{L} . Then the set $\{\tilde{\sigma}(\tilde{x})\tilde{x}^{-1} \mid \tilde{x} \in \tilde{L}\}$ must be connected as a continuous image of a connected set. Hence it reduces to the identity, namely $\tilde{\sigma}(\tilde{x}) = \tilde{x}$. This implies that the homomorphism is one-to-one.

Now we know that the Lie algebra of $\mathfrak{U}(\tilde{L})$ is $\mathfrak{E}(\mathfrak{Q})$. Therefore the last assertion is obvious.

LEMMA 3. *Let L be a connected Lie group, D a discrete normal subgroup, and let $\tilde{\mathfrak{U}}_D = \tilde{\mathfrak{U}}_D(L)$ be the subgroup of $\tilde{\mathfrak{U}}(L)$ composed of elements which leave every element of D fixed. Denote by $\mathfrak{U}_D = \mathfrak{U}_D(L)$ the connected component of $\tilde{\mathfrak{U}}_D$. Then*

(1) $\tilde{\mathfrak{U}}_D$, accordingly \mathfrak{U}_D also, is a closed linear group over the Lie algebra \mathfrak{Q} of L .

(2) If in particular the center of L is discrete, $\tilde{\mathfrak{U}}_D$ and \mathfrak{U}_D have no center.

PROOF. (1) Let \tilde{L} be the universal covering group of L . Then $\tilde{\mathfrak{U}}(\tilde{L})$ is a closed linear group over \mathfrak{Q} , which can be identified with the automorphism group of \mathfrak{Q} . Now let f be the covering mapping, N the kernel, and \tilde{D} the complete inverse image of D in \tilde{L} . Then $\tilde{\mathfrak{U}}_D$ can be considered as the subgroup of $\tilde{\mathfrak{U}}(\tilde{L})$ composed of the elements satisfying

$$\sigma(N) = N \text{ and } \sigma(\tilde{d})\tilde{d}^{-1} \in N \text{ for } \tilde{d} \in \tilde{D}.$$

It is clear that these conditions define a closed subset of $\tilde{\mathfrak{U}}(\tilde{L})$. Therefore $\tilde{\mathfrak{U}}_D$, accordingly \mathfrak{U}_D , is a closed linear group over \mathfrak{Q} .

(2) Next let L_0 be the factor group of L modulo the center. Because the center of L is discrete, L_0 has no center. Then the isomorphism of $\tilde{\mathfrak{A}}_D$ into $\tilde{\mathfrak{U}}(\tilde{L})$ mentioned above can also be considered as an isomorphism of $\tilde{\mathfrak{A}}_D$ into $\tilde{\mathfrak{U}}(L_0)$ by application of Lemma 2. In this isomorphism the group $\mathfrak{A}(L)$ composed of all inner automorphisms of L goes onto $\mathfrak{A}(L_0)$. Therefore $\tilde{\mathfrak{A}}_D$ and \mathfrak{A}_D are mapped onto subgroups of $\tilde{\mathfrak{U}}(L_0)$ containing $\mathfrak{A}(L_0)$.

On the other hand by a well-known theorem of abstract group theory, every subgroup of the automorphism group of a group with no center has also no center, if it contains all inner automorphisms.

Hence $\tilde{\mathfrak{A}}_D$ and \mathfrak{A}_D have no center.

LEMMA 4. *Let K be a compact normal subgroup of a connected topological group G , and K^0 the connected component of K containing the identity. Denote by $\mathfrak{S}_G(K^0)$ and $\mathfrak{S}_K(K^0)$ the subgroups of the automorphism group of G and K respectively, composed of the inner automorphisms induced by the elements of K^0 . Then we have*

$$\mathfrak{U}(K) = \mathfrak{S}_K(K^0) \cong \mathfrak{S}_G(K^0) = \text{IIS}_\alpha,$$

where the isomorphism is induced by the same element of K^0 , and the last term is an (in general infinite) weak product of compact connected simple Lie groups with no center.

PROOF. By a theorem of Iwasawa [3], $\tilde{\mathfrak{U}}(K)/\mathfrak{A}(K)$ is totally disconnected, and it is obvious that $\mathfrak{A}(K)/\mathfrak{S}_K(K^0)$ is totally disconnected. Hence $\tilde{\mathfrak{U}}(K)/\mathfrak{S}_K(K^0)$ is totally disconnected. Therefore $\mathfrak{S}_K(K^0) \supseteq \mathfrak{U}(K)$. But as $\mathfrak{S}_K(K^0)$ is connected, we have $\mathfrak{U}(K) \supseteq \mathfrak{S}_K(K^0)$, whence we get the first equality.

Now let A be the center of K^0 . Then A is clearly a normal subgroup of G . On the other hand since a compact commutative normal subgroup of a connected topological group is central by [3], A is central in G . Therefore we have a natural isomorphism of $\mathfrak{S}_G(K^0)$ onto $\mathfrak{S}_K(K^0)$ by restricting the domain.

Next it is well known that a compact connected group reduces to the last form modulo the center.

3. Theorems.

Let G be a locally compact connected group and let $G = L^*K$ be a canonical decomposition. Since $\mathfrak{U}(G)K = K$ by Lemma 1 (1), every element of $\mathfrak{U}(G)$ determines an element of $\mathfrak{U}(K)$. On the other hand by Lemma 4, $\mathfrak{U}(K)$ is naturally isomorphic to $\mathfrak{S}_G(K^0)$. Therefore we have a continuous homomorphism ϕ from $\mathfrak{U}(G)$ into $\mathfrak{S}_G(K^0)$. Denote the kernel by \mathfrak{B} .

Now since K^0 is mapped onto itself by $\mathfrak{U}(G)$, $\mathfrak{S}_G(K^0)$ is a normal subgroup of $\mathfrak{U}(G)$. And ϕ is the identity mapping on $\mathfrak{S}_G(K^0)$. Therefore ϕ is onto, and we have the direct product decomposition of $\mathfrak{U}(G)$: $\mathfrak{U}(G) = \mathfrak{S}_G(K^0) \times \mathfrak{B}$. Now, since we can find a $\mathfrak{S}_G(K^0)$ -part of elements of $\mathfrak{U}(G)$ continuously, this decomposition is continuous. And we can see also that \mathfrak{B} is connected.

Next we shall retain the notations of L , D and D^* as in §1, and for $x \in L$, we shall denote by x^* the corresponding element of L^* . Now consider $\tilde{\mathfrak{U}}_D(L)$ and $\mathfrak{U}_D(L)$ in Lemma 3. Then by defining

$$\begin{cases} f(\sigma)x^* = (\sigma(x))^* & x^* \in L^*, \\ f(\sigma)y = y & y \in K, \end{cases}$$

for $\sigma \in \tilde{\mathfrak{U}}_D$, we have an automorphism $f(\sigma)$ of G . And since $f(\sigma)$ is continuous on a neighborhood $G_I = L_I^* \times K$, it is continuous on G , namely $f(\tilde{\mathfrak{U}}_D) \subseteq \tilde{\mathfrak{U}}(G)$.

Now the convergence of a sequence of $\tilde{\mathfrak{U}}(G)$ or $\tilde{\mathfrak{U}}(L)$ is equivalent to the uniform convergence in some definite compact neighborhood of the identity. This shows the bicontinuity of f . Hence $f(\mathfrak{U}_D)$ is connected with \mathfrak{U}_D , and we have that $f(\mathfrak{U}_D) \subseteq \mathfrak{U}(G)$.

Thus we get the following:

THEOREM 1. *Let G be a locally compact connected group with a canonical decomposition $G = L^*K$, and let K^0 be the connected component of the identity of K . Then*

- (1) $\mathfrak{U}(G) = \mathfrak{S}_G(K^0) \times \mathfrak{B}$ where $\mathfrak{B} = \{\sigma | \sigma \in \mathfrak{U}(G), \sigma(x) = x, x \in K\}$
- (2) *There exists a bicontinuous isomorphism from $\mathfrak{U}_D(L)$ into \mathfrak{B} :*

$$f(\mathfrak{U}_D(L)) \subseteq \mathfrak{B}.$$

Suppose now that L^* is mapped onto itself by $\mathfrak{U}(G)$. Then every element of \mathfrak{B} induces an automorphism of L^* , which makes every element of D^* fixed. Therefore we can get an isomorphism f' from \mathfrak{B} into $\tilde{\mathfrak{U}}_D$. This mapping f' is clearly the inverse mapping of f . Therefore we have $f(\mathfrak{U}_D(L)) = \mathfrak{B}$. Hence \mathfrak{B} is a Lie group. On the other hand as $\mathfrak{S}_G(K^0)$ is compact, we have the following:

THEOREM 2. *If L^* is mapped onto itself by $\mathfrak{U}(G)$ in Theorem 1, then $\mathfrak{U}(G)$ is locally compact and $f(\mathfrak{U}_D(L)) = \mathfrak{B}$.*

COROLLARY. *Let G be a locally compact connected perfect group. Then $\mathfrak{U}(G)$ is locally compact.*

PROOF. Since G is perfect, the factor group G/K is also perfect. On the other hand if a connected Lie group is perfect, then every connected locally isomorphic group is also perfect, and G/K is locally isomorphic with L . Therefore L is perfect. Hence by Lemma 1, (2) (b) and Theorem 2 we have the corollary.

Proof of the tower theorem. (1) Because the center of k is central in G , we can apply Lemma 1, (2) in this case. Thus we have $\mathfrak{U}(G)L^* - L^*$, which implies that $\mathfrak{U}(G) \cong \mathfrak{S}_G(K^0) \times \mathfrak{U}_D(L)$ by Theorem 2. On the other hand since the center of L is clearly discrete, by Lemma 3, (2) $\mathfrak{U}_D(L)$ has no center.

(2) From $\mathfrak{U}(G) = \text{PIS}_\alpha \times \mathfrak{B}$, we get easily that

$$\mathfrak{U}^2(G) = \mathfrak{U}(\text{PIS}_\alpha) \times \mathfrak{U}(\mathfrak{B}).$$

And by using $\mathfrak{U}(\text{PIS}_\alpha) \cong \text{PIS}_\alpha$, we may write inductively

$$\mathfrak{U}^{k+1}(G) \cong \text{PIS}_\alpha \times \mathfrak{U}^k(\mathfrak{B}).$$

Now, using Lemma 2, the Lie algebra of $\mathfrak{U}^k(\mathfrak{B})$ is \mathfrak{S}^k (Lie algebra of \mathfrak{B}). And since \mathfrak{B} has no center, the Lie algebra of \mathfrak{B} has no center. Therefore our assertion follows from the tower theorem of Lie algebras.

BIBLIOGRAPHY

1. C. Chevalley, *On groups of automorphisms of Lie groups*, Proc. Nat. Acad. Sci. U. S. A. vol. 30 (1944) pp. 274–275.
2. M. Goto, *Dense imbeddings of locally compact connected groups*, forthcoming shortly.
3. K. Iwasawa, *On some types of topological groups*, Ann. of Math. vol. 50 (1949) pp. 507–557.
4. E. Schenkman, *A theory of subinvariant Lie algebras*, Amer. J. Math. vol. 73 (1951) pp. 453–474.
5. H. Wielandt, *Eine Verallgemeinerung der invarianten Untergruppen*, Math. Zeit. vol. 45 (1939) pp. 209–244.
6. H. Yamabe, *On the conjecture of Iwasawa and Gleason*, Ann. of Math. vol. 58 (1953) pp. 48–54.
7. ———, *A generalization of a theorem of Gleason*, Ann. of Math. vol. 58 (1953) pp. 351–365.

SOME NEW DECOMPOSITION THEOREMS FOR SEMI-SIMPLE GROUPS

G. D. MOSTOW

1. Introduction. This paper arose out of an investigation of the topological structure of Klein spaces with semi-simple isotropy group. The main results are:

THEOREM 3. *Let \mathfrak{S} be the space of all $n \times n$ symmetric real matrices, let \mathfrak{E} be any linear subspace of \mathfrak{S} such that $[X[XY]] \in \mathfrak{E}$ for all $X, Y \in \mathfrak{S}$, and let $\mathfrak{F} = \{X | X \in \mathfrak{S}, \text{Tr} X = 0\}$. Then any positive definite symmetric real matrix can be represented uniquely and continuously as $e f e$ where $e \in \exp \mathfrak{E}$, and $f \in \exp \mathfrak{F}$.*

THEOREM 4. *Let $\mathfrak{E}, \mathfrak{F}$ be as before. Then any nonsingular real matrix can be represented uniquely and continuously as $k \cdot f \cdot e$ where k is orthogonal, $f \in \exp \mathfrak{F}$, $e \in \exp \mathfrak{E}$.*

The analogue of Theorem 3 for positive definite Hermitian complex matrices is also true, and in fact follows from it with the help of Theorem 1 (cf. below). The analogue of Theorem 4 for complex matrices is also true.

From Theorem 4, one can deduce:

THEOREM 5. *Let G be a connected semi-simple Lie group and let $\mathfrak{G} = \mathfrak{K} + \mathfrak{E}$ be a Cartan decomposition of its Lie algebra with \mathfrak{K} compact (cf. end of §2 for definitions). Let \mathfrak{E}' be a linear subspace of \mathfrak{E} such that $[X[XY]] \in \mathfrak{E}'$ for all $X, Y \in \mathfrak{E}'$. Let $\mathfrak{F} = \{X | B(X, \mathfrak{E}') = 0, X \in \mathfrak{E}\}$, where B is the fundamental bilinear form on \mathfrak{G} . Then G decomposes topologically into $K \cdot F \cdot E'$ where K is the analytic subgroup determined by \mathfrak{K} , $F = \exp \mathfrak{F}$, $E' = \exp \mathfrak{E}'$.*

THEOREM 6. *Let \mathfrak{G} be a real semi-simple Lie algebra, let \mathfrak{G}' be semi-simple subalgebra, and let $\mathfrak{K}' + \mathfrak{E}'$ be a Cartan decomposition for \mathfrak{G}' , \mathfrak{K}' being compact. Then there is a Cartan decomposition $\mathfrak{K} + \mathfrak{E}$ for \mathfrak{G} with $\mathfrak{K}' \subset \mathfrak{K}$ and $\mathfrak{E}' \subset \mathfrak{E}$.*

From Theorem 6 one deduces:

THEOREM 7. *Let $\mathfrak{G}_1 \subset \mathfrak{G}_2 \subset \dots \subset \mathfrak{G}_n$ be an ascending chain of semi-simple Lie algebras of endomorphisms of a real linear space V of finite dimension. Then a positive definite inner product B for V can be chosen in such a way that $\mathfrak{G}_i = \mathfrak{G}_i \cap \mathfrak{K} + \mathfrak{G}_i \cap \mathfrak{S}$ ($i = 1, \dots, n$) where \mathfrak{K} and \mathfrak{S} are respectively the skew-symmetric and symmetric endomorphisms of V with respect to B .*

A noteworthy special case is $n=1$.

Let \mathfrak{G}_i, B be as in Theorem 7, and let G_i denote the analytic group of matrices which \mathfrak{G}_i determines. Then $G_i = G_i \cap K \cdot G_i \cap P$ topologically ($i=1, \dots, n$), where K is the orthogonal group, and P is the set of positive definite symmetric matrices with respect to B , by a standard argument (cf. [3]).

These results enable one to prove that the factor space of a Lie group by a semi-simple subgroup is a fiber bundle whose fibers are euclidean and whose base space is the factor space of a compact group. The import of the above results for Klein spaces is discussed in a paper that shall appear elsewhere.

Another result that is included in this paper is a simplified version of E. Cartan's proof that maximal compact subgroups of a semi-simple analytic group are conjugate under inner automorphism. Although the proof given here is in essence Cartan's, it seems appropriate to present it, for in the setting of §2, Cartan's ideas can be executed with simplicity and rigor, and without a previous knowledge of symmetric Riemannian spaces. As a matter of fact, part of §2 can be considered as a novel exposition of Cartan's symmetric Riemannian spaces.

2. The space of positive definite matrices. Let \mathfrak{S} denote the space of real $n \times n$ symmetric matrices and let P denote the space of positive definite symmetric matrices. We will regard \mathfrak{S} as a linear space with inner product

$$\text{Tr } XY, \quad X, Y \in \mathfrak{S}$$

and we will regard P as a Riemannian space with infinitesimal metric

$$\left(\frac{ds}{dt}\right)^2 = \text{Tr}(p^{-1}\dot{p})^2$$

where $p(t)$ is a differentiable path in P , \dot{p} denotes dp/dt , and Tr denotes trace (cf. [4]). Clearly this metric on P is invariant under the transitive group of transformations $p \rightarrow x'px$, where x is any non-singular matrix and x' is its transpose. The inner product on \mathfrak{S} is positive definite, since all the eigenvalues of the elements of \mathfrak{S} are real. For any $X \in \mathfrak{S}$ we define the linear transformations

$$L_X: \quad g \rightarrow Xg$$

$$R_X: \quad g \rightarrow gX$$

on the linear space of all $n \times n$ matrices. We define $D_X = R_X - L_X$, and on \mathfrak{S} we define

$$\tau_X: \quad Y \rightarrow \exp -\frac{X}{2} \cdot \lim_{t \rightarrow 0} \frac{\exp(X+tY) - \exp Y}{t} \exp -\frac{X}{2}.$$

Clearly τ_X is a linear transformation of \mathfrak{G} into \mathfrak{G} .

LEMMA 1. For any $X \in \mathfrak{G}$, $t_X = (\sinh D_X/2)/(D_X/2)$ on \mathfrak{G} and is self-adjoint.

PROOF. Let $X(t)$ be a differentiable path in \mathfrak{G} . Differentiating both sides of the equation with respect to t ,

$$X(\exp X) = (\exp X)X$$

we obtain

$$\dot{X}(\exp X) + X(\dot{\exp X}) = (\dot{\exp X})X + (\exp X)\dot{X}$$

and thus

$$\dot{X}(\exp X) - (\exp X)\dot{X} = (\dot{\exp X})X - X(\dot{\exp X}).$$

Hence

$$\begin{aligned} \left(\exp -\frac{X}{2}\right)\dot{X}\left(\exp \frac{X}{2}\right) - \left(\exp \frac{X}{2}\right)\dot{X}\left(\exp -\frac{X}{2}\right) = \\ \left(\exp -\frac{X}{2}\right)(\dot{\exp X})\left(\exp -\frac{X}{2}\right)X - X\left(\exp -\frac{X}{2}\right)(\dot{\exp X})\left(\exp -\frac{X}{2}\right). \end{aligned}$$

Since L_X and R_X commute, $\exp D/2 = \exp -L/2 \cdot \exp R/2$, where D, L, R denote D_X, L_X , and R_X respectively. Hence

$$\left(\exp \frac{D}{2}\right)\dot{X} = D\tau_X\dot{X}.$$

Selecting for $X(t)$ the path $X + tY$, where $Y \in \mathfrak{G}$, we see that for all $Y \in \mathfrak{G}$,

$$\left(\exp \frac{D}{2} - \exp -\frac{D}{2}\right)Y = D\tau Y$$

where τ denotes τ_X .

We now prove that τ is the restriction to \mathfrak{G} of

$$\frac{\exp D/2 - \exp -D/2}{D} = \frac{\sinh D/2}{D/2} = \sum_{n=0}^{\infty} \frac{(D/2)^{2n}}{(2n+1)!}.$$

Observe first that τ is self-adjoint on \mathfrak{G} , for

$$\begin{aligned} \text{Tr}(\tau A)B &= \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{p+q=n-1} \text{Tr}(\exp -X/2)X^p A X^q (\exp -X/2)B = \\ \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{p+q=n-1} \text{Tr} A X^q (\exp -X/2)B X^p (\exp -X/2) &= \text{Tr} A(\tau B). \end{aligned}$$

Moreover the restriction of D^2 to \mathfrak{G} is also self-adjoint so that $\tau - (\sinh D/2)/(D/2)$ is self-adjoint on \mathfrak{G} . Let $\mathfrak{N} = \{A \mid A \in \mathfrak{G}, DA = 0\}$. We have seen that

$$D\left(\tau - \frac{\sinh D/2}{D/2}\right)Y = 0$$

for all $Y \in \mathfrak{G}$.

Thus $\tau - (\sinh D/2)/(D/2)$ maps \mathfrak{G} into \mathfrak{N} . Let \mathfrak{N}^\perp denote the orthogonal complement of \mathfrak{N} in \mathfrak{G} . Then $(\tau - (\sinh D/2)/(D/2))\mathfrak{N}^\perp \subset \mathfrak{N} \cap \mathfrak{N}^\perp = \{0\}$. On the other hand if $Y \in \mathfrak{N}$, then $XY = YX$, $\exp(X+tY) = \exp X \exp tY$, and $\tau X = X - (\sinh D/2)/(D/2)X$. Thus $\tau = (\sinh D/2)/(D/2)$ throughout \mathfrak{G} .

DEFINITION. Let f be a differentiable path in P . By $\rho_R(f)$ is meant the Riemannian length of f in the metric that we have introduced on P . By $\rho_{\mathfrak{G}}(f)$ is meant the ordinary euclidean length of the path $\log f$ which lies in the euclidean space \mathfrak{G} (the metric in \mathfrak{G} being derived from the positive definite inner product $\text{Tr}XY$).

LEMMA 2. Along any differentiable path $p(t)$ in P ,

$$\text{Tr}(\dot{\log p})^2 \leq \text{Tr}(p^{-1}\dot{p})^2;$$

thus, for any differentiable path f in P ,

$$\rho_{\mathfrak{G}}(f) \leq \rho_R(f).$$

PROOF. First we observe that

$$\text{Tr}(p^{-1}\dot{p})^2 = \text{Tr}(p^{-1/2}\dot{p}p^{-1/2})(p^{-1/2}\dot{p}p^{-1/2}) = \text{Tr}\tau(\dot{\log p})^2$$

by definition of τ , where τ denotes $\tau_{\log p}$. Now by Lemma 1, $\tau = (\sinh D/2)/(D/2)$, where D denotes $D_{\log p}$, and thus the eigenvalues of τ are

$$\frac{\sinh(\lambda_i - \lambda_j)/2}{(\lambda_i - \lambda_j)/2}$$

where $\lambda_1, \dots, \lambda_n$ are the eigenvalues of $\log p$. Since $\log p$ is symmetric its eigenvalues are real, and consequently the eigenvalues of τ are not less than 1. Since moreover, τ is self-adjoint with respect to the imposed inner product on \mathfrak{G} , we conclude immediately that

$$\text{Tr}(\dot{\log p})^2 \leq \text{Tr}[\tau(\dot{\log p})]^2 = \text{Tr}(p^{-1} \dot{p})^2.$$

Since $\text{Tr}(\dot{\log p})^2$ is the infinitesimal form of the euclidean metric in \mathfrak{G} , the second assertion of the lemma follows at once.

LEMMA 3. *$\exp t \log p$ ($0 \leq t \leq 1$) is the unique geodesic in P joining the identity 1 to the element $p \in P$. More generally, the geodesic between any two points is unique.*

PROOF. Let H denote $\log p$, and let f denote the path $\exp tH$, $0 \leq t \leq 1$. Since H and tH commute, $\rho_R(f)$ is clearly equal to $(\text{Tr} H^2)^{1/2}$, which in turn is the euclidean distance between $\log 1$ and $\log \exp H$. It follows immediately from the minimum property of geodesics in euclidean space that $(\text{Tr} H^2)^{1/2} = \rho_{\mathfrak{G}}(g)$ for any differentiable path g in P other than $\log f$. Thus for all differentiable paths in g other than f ,

$$\rho_R(f) < \rho_{\mathfrak{G}}(g) \leq \rho_R(g).$$

It follows at once that f is the unique geodesic from 1 to p . Since the group of isometries of P is transitive, geodesics between any two points are unique.

DEFINITION. Let $p, q \in P$. \overline{pq} shall denote the geodesic path joining p to q . $\rho_{\mathfrak{G}}(p, q)$ denotes the euclidean distance in \mathfrak{G} between $\log p$ and $\log q$.

LEMMA 4. *The Riemannian angle between two paths f and g intersecting at 1 is equal to the euclidean angle in \mathfrak{G} between the two paths $\log f$ and $\log g$ at 0 . Moreover, in any geodesic triangle ABC in P ,*

$$c^2 \geq a^2 + b^2 - 2ab \cos A$$

where a, b, c , are the lengths of sides opposite the angles A, B, C respectively.

PROOF. We may assume for convenience that $f(0) = g(0) = 1$. The Riemannian angle between f and g at 1 is by definition

$$\frac{\text{Tr}(f^{-1} \dot{f})(g^{-1} \dot{g})}{[\text{Tr}(f^{-1} \dot{f})^2]^{1/2} [\text{Tr}(g^{-1} \dot{g})^2]^{1/2}}$$

and at $f(0) = g(0) = l$, this reduces to

$$\frac{\text{Tr } \ddot{f}g}{[\text{Tr } \dot{f}^2]^{1/2} [\text{Tr } \dot{g}^2]^{1/2}}.$$

Since the mapping $p \rightarrow \log p$ is non-singular, the angle at 0 between $\log f$ and $\log g$ in \mathbb{G} depends only on the tangents to f and g at l . Thus we can assume for convenience of computation that

$$f(t) = \exp t \dot{f}(0), \quad g(t) = \exp t \dot{g}(0).$$

It is now clear that the Riemannian angle between f and g at l equals the euclidean angle between $\log f$ and $\log g$ at 0 .

We suppose now that ABC is a geodesic triangle in P . Translating the vertex C to l by an isometry, we may assume without loss of generality that C is at l .

Applying Lemma 2, we obtain

$$\begin{aligned} \rho_R(\overline{AB})^2 &\geq \rho_{\mathbb{G}}(\overline{AB})^2 \geq \rho_{\mathbb{G}}(A, B)^2 = \\ &\rho_{\mathbb{G}}(A, C)^2 + \rho_{\mathbb{G}}(A, C)^2 - 2\rho_{\mathbb{G}}(A, C) \rho_{\mathbb{G}}(B, C) \cos \sphericalangle C, \end{aligned}$$

the last equality being the law of cosines in the euclidean space \mathbb{G} . Now as seen in the Proof of Lemma 2,

$$\rho_{\mathbb{G}}(A, C) = \rho_{\mathbb{G}}(A, l) = \rho_R(\overline{AC}) = b,$$

and similarly $\rho_{\mathbb{G}}(B, C) = a$.

Applying the first part of Lemma 4, we have

$$c^2 = \rho_R(\overline{AB})^2 \geq a^2 + b^2 - 2ab \cos \sphericalangle C.$$

REMARK. From the inequality of Lemma 4 it follows readily that the sum of the three angles of a geodesic triangle in P is at most 180° . For let ABC be a geodesic triangle in P with a, b, c denoting the length of sides opposite the vertices A, B, C respectively. Since a, b, c satisfy the triangle inequality, there exists in euclidean space a triangle A_1, B_1, C_1 with the sides opposite A_1, B_1, C_1 being of length a, b, c respectively. Now $\cos \sphericalangle C_1 = (a^2 + b^2 - c^2) / 2ab \leq \cos \sphericalangle C$. Hence $\sphericalangle C \leq \sphericalangle C_1$. Similarly $\sphericalangle A \leq \sphericalangle A_1, \sphericalangle B \leq \sphericalangle B_1$. It follows that $\sphericalangle A + \sphericalangle B + \sphericalangle C \leq 180^\circ$.

LEMMA 5. Let $X \in \mathfrak{G}$. The mappings

$$\alpha_X : A \rightarrow A \cdot \exp X + \exp X \cdot A, \quad A \in \mathfrak{G}$$

$$\beta_X : A \rightarrow \left. \frac{d}{dt} \right|_{t=0} \exp(X + tA), \quad A \in \mathfrak{G}$$

are 1-1 linear transformations of \mathfrak{G} onto \mathfrak{G} . Let $\gamma_X = \beta_X^{-1} \circ \alpha_X$. Then

$$\gamma_X = D_X \coth(D_X/2).$$

PROOF. The mapping γ_X is obviously a linear transformation of \mathfrak{G} into \mathfrak{G} . To prove that it is 1-1 into, it suffices to conclude from $A \exp X + \exp X \cdot A = 0$ with $A \in \mathfrak{G}$ that $A = 0$. Suppose

$$A \exp X + \exp X \cdot A = 0.$$

Then

$$\left[\left(\exp -\frac{X}{2} \right) A \exp \frac{X}{2} \right]' = \exp \frac{X}{2} A \exp -\frac{X}{2} = - \left(\exp -\frac{X}{2} \right) A \exp \frac{X}{2}.$$

Thus $(\exp -X/2) A \exp X/2$ is skew-symmetric. On the other hand, its eigenvalues being eigenvalues of the symmetric matrix A , are all real. Hence it is zero and $A = 0$.

As for β_X , it is $\exp \frac{L_X}{2} \circ \exp \frac{R_X}{2} \circ \tau_X$ and is thus a 1-1 linear transformation of \mathfrak{G} onto \mathfrak{G} . Finally

$$\begin{aligned} \gamma_X &= (\exp L_X/2 \cdot (\exp R_X/2) \tau_X)^{-1} (\exp R_X + \exp L_X) \text{ on } \mathfrak{G} \\ &= \frac{D_X/2}{\sinh D_X/2} \cdot \exp(R_X - L_X)/2 + \exp(L_X - R_X)/2 \\ &= D_X \frac{\cosh D_X/2}{\sinh D_X/2} \\ &= D_X \coth D_X/2. \end{aligned}$$

THEOREM 1. Let \mathfrak{E} be a linear subspace of \mathfrak{G} and let $E = \exp \mathfrak{E}$. Then $[X, [X, Y]] \in \mathfrak{E}$ for all $X, Y \in \mathfrak{E}$ if and only if $e f e \in E$ for all $e, f \in E$.

PROOF. Assume first that $[X[X, Y]] \in \mathfrak{E}$ for all $X, Y \in \mathfrak{E}$. Then $D_X^2 Y \in \mathfrak{E}$

for all $X, Y \in \mathfrak{G}$. Let $f \in E$ and let $Y \in \mathfrak{G}$. Define the path $X(t)$ in \mathfrak{G} by the relationship $\exp X(t) = \exp tY \cdot f \cdot \exp tY$. Then

$$\begin{aligned} \beta_{X(t_0)}(\dot{X}(t_0)) &= \left. \frac{d}{ds} \right|_{s=0} \exp(X(t_0)) + s\dot{X}(t_0) = \left. \frac{d}{dt} \right|_{t=t_0} \exp X(t) \\ &= Y \exp X(t) + \exp X(t) \cdot Y. \end{aligned}$$

Thus

$$\dot{X}(t) = \beta_{X(t)}^{-1} \cdot \alpha_{X(t)}(Y) = \gamma_{X(t)}(Y) = D(\coth D/2)(Y) = f(X(t))$$

where $D = D_{X(t)}$, and $f(X)$ is a differentiable, in fact an analytic matrix valued function of the matrix X .

Moreover, since the Taylor-series expansion for $D \coth D/2$ involves only even powers of D , f has the additional property that $f(X) \in \mathfrak{G}$ when $X \in \mathfrak{G}$. We may therefore regard $\dot{X} = f(X)$ as a differential equation on \mathfrak{G} and by the fundamental existence theorem for differential equations there is a solution in \mathfrak{G} with initial point at $X(0)$. Applying now the uniqueness theorem for solutions of ordinary differential equations, we have $X(t) \in \mathfrak{G}$ for all t . On taking $t=1$ and $Y = \log e$ for $e \in E$, we conclude that for all $e, f \in E$, $efe \in E$.

Conversely, assume that $efe \in E$ whenever $e, f \in E$. Then for $f \in E$ and $Y \in \mathfrak{G}$, let $X(t)$ be the path in \mathfrak{G} defined by the relation

$$\exp X(t) = \exp tY f \exp tY.$$

Then $X(t) \in \mathfrak{G}$ for all t and thus $\dot{X}(t)$ as well as

$$Z = \lim_{t \rightarrow 0} \frac{\dot{X}(t) - \dot{X}(0)}{t^2} \in \mathfrak{G},$$

if the latter limit exists. But as seen above, $\dot{X}(t) = D(\coth D/2)(Y)$ where $D = D_{X(t)}$. Consequently

$$Z = \lim_{t \rightarrow 0} \left[\frac{(1 + (1/12)t^2 D^2)Y - Y}{t^2} + tW \right] = (1/12)D_{X(0)}^2 Y;$$

where W depends continuously on t .

Hence $D_{X(0)}^2(Y) \in \mathfrak{G}$. Taking $f = \exp X$, we have $[X, [X, Y]] = D^2(Y) \in \mathfrak{G}$. Proof of the theorem is now complete.

An immediate consequence of Theorem 1 is the

COROLLARY. *Let \mathfrak{E} be a linear subspace of \mathfrak{G} with the property $[X, [X, Y]] \in \mathfrak{E}$ for all $X, Y \in \mathfrak{E}$. Then $E = \exp \mathfrak{E}$ is a geodesic subspace of P .*

PROOF. By Lemma 3, E contains the geodesic joining the identity matrix 1 with any point $p \in E$. Since the family of isometries of P consisting of all transformations $x \rightarrow exe$ with $e \in E$ keeps E invariant and carries 1 into all points of E , the set E must contain the geodesic joining any two of its points, i.e., E is a geodesic subspace of P .

The converse to this corollary is also true. For consider the mapping $\sigma_p : x \rightarrow px^{-1}p$ of P onto P where $p \in P$. It is easy to verify that this preserves the infinitesimal metric on P and is thus an isometry. Clearly σ_p has p as a fixed point and it maps each geodesic $p^{1/2} \exp tX p^{1/2}$ through p onto $p^{1/2} \exp -tX p^{1/2}$, i.e., every geodesic through p is a subset invariant under σ_p . It follows that if $E = \exp \mathfrak{E}$ is a geodesic subspace, then $\sigma_p(E) \subset E$ for all $p \in E$. Now let τ_p denote the isometry $x \rightarrow p^{1/2}xp^{1/2}$ of P onto P for $p \in P$. Then for all $x \in P$,

$$\sigma_p \cdot \sigma_{p^{1/2}}(x) = p \cdot (p^{1/2}x^{-1}p^{1/2})^{-1}p = p^{1/2}xp^{1/2} = \tau_p(x)$$

that is, $\tau_p = \sigma_p \cdot \sigma_{p^{1/2}}$. Hence for all $e, f \in E$, $efe = t_e(f) = \sigma_e(\sigma_{e^{1/2}}(f)) \in E$. Applying the preceding theorem, we have for all $X, Y \in \mathfrak{E}$ that $[X, [X, Y]] \in \mathfrak{E}$.

REMARK. σ_p and τ_p are *symmetry* and *translation* respectively in the language of E. Cartan.

These last results can be described in a somewhat sharper way. Namely

THEOREM 2. *Let \mathfrak{E} be a linear subspace of \mathfrak{G} and let $E = \exp \mathfrak{E}$. The following are then equivalent:*

- (1) E is a geodesic subspace of P .
- (2) For all $e, f \in E$, $efe \in E$.
- (3) For all $X, Y \in \mathfrak{E}$, $[X, [X, Y]] \in \mathfrak{E}$.
- (4) \mathfrak{E} is a Lie triple system, i.e., for all $X, Y, Z \in \mathfrak{E}$, $[X, [Y, Z]] \in \mathfrak{E}$.

PROOF. We have already established above the equivalence of (1), (2), and (3). To complete proof of this theorem, it suffices to prove that (3) implies (4). Assume (3). By polarization

$$[Z, [X, Y]] + [X, [Z, Y]] \in \mathfrak{E}$$

for all X, Y, Z in \mathfrak{E} . Now applying the Jacobi identity

$$[Z, [X, Y]] = [[Z, X], Y] + [X, [Z, Y]]$$

we obtain after substitution

$$(A) \quad [[Z, X], Y] + 2[X, [Z, Y]] \in \mathfrak{G}$$

for all X, Y, Z in \mathfrak{G} . Interchanging X and Y , we have

$$[[Z, Y], X] + 2[Y, [Z, X]] \in \mathfrak{G}$$

and hence

$$(B) \quad 2[[Z, X], Y] + [X, [Z, Y]] \in \mathfrak{G}$$

for all $X, Y, Z \in \mathfrak{G}$. From (A) and (B) it follows that $[X, [Z, Y]] \in \mathfrak{G}$ for all $X, Y, Z \in \mathfrak{G}$. From this (4) follows at once. Proof of the theorem is now complete.

THEOREM 3. *Let \mathfrak{G} be a linear subspace of the space \mathfrak{S} of real symmetric $n \times n$ matrices such that $[X[X, Y]] \in \mathfrak{G}$ for all $X, Y \in \mathfrak{G}$. Let $\mathfrak{F} = \{X | X \in \mathfrak{G}, \text{tr} X = 0\}$. Let E, F denote $\exp \mathfrak{G}, \exp \mathfrak{F}$ respectively. Then any positive definite real symmetric matrix can be expressed uniquely and continuously as $e f e$ with $e \in E, f \in F$.*

PROOF. We consider the mapping $\phi : (e, f) \rightarrow e f e$ of the cartesian product $E \times F$ into P , the space of positive definite real symmetric matrices. ϕ is a one-to-one map of $E \times F$ into P . For suppose $e_1 f_1 e_1 = e_2 f_2 e_2$ with $e_i \in E, f_i \in F (i=1, 2)$. Then consider the geodesic triangle with vertices at $e_1 f_1 e_1, e_1^2$, and e_2^2 .

By Theorem 2, E is a geodesic subspace of P . Hence the geodesic joining e_1^2 to e_2^2 lies in E . On the other hand the geodesic joining $e_1 f_1 e_1$ to e_1^2 lies in $e_1 F e_1$. In as much as \mathfrak{F} is perpendicular to \mathfrak{G} (with respect to the inner product $\text{tr} XY$ on \mathfrak{S}) at zero, F is perpendicular to E at the identity matrix I by Lemma 4. Since $x \rightarrow e_1 x e_1$ is an isometry, $e_1 F e_1$ is perpendicular to $e_1 E e_1 = E$ at e_1^2 . Thus the angle at e_1^2 of the above geodesic triangle is 90° . Similarly, the angle at e_2^2 is 90° for it is formed by the geodesic joining e_2^2 to $e_1 f_1 e_1 = e_2 f_2 e_2$, which lies in $e_2 F e_2$ and by the geodesic joining e_2^2 to e_1^2 which lies in E . Denoting the lengths of the sides of the geodesic triangle by a, b, c we have by Lemma 4, $c^2 \geq a^2 + b^2$ and $b^2 \geq a^2 + c^2$, where a is the length of the side joining e_1^2 to e_2^2 . Hence $a=0$ and $e_1^2 = e_2^2$. It follows that $e_1 = e_2$ and thus $f_1 = f_2$. Thus ϕ is a one-to-one mapping.

We now denote by $|x|$ the Riemannian distance from X to the identity matrix I , where $x \in P$.

For any $e \in E, f \in F, |\phi(e, f)|$ is an upper bound for $|e|$ and $|f|$. For consider

the geodesic triangle with vertices at l , $e f e$, and e^2 . By the same reasoning that was just used, there is a right angle at e^2 . Hence by Lemma 4, $|e f e|^2 \geq |e^2|^2 + |f|^2$. Thus $|e f e| \geq \sup(2|e|, |f|)$ and from this the assertion follows.

Finally, let us consider the image set $\phi(E \times F)$. Since ϕ is continuous and one-to-one, it is a homeomorphism of each open set in $E \times F$ with compact closure into P . Since $E \times F$ and P are euclidean spaces of the same dimension, $\phi(E \times F)$ must be open in P by the well-known invariance-of-domain theorem for euclidean space. On the other hand suppose that x is a point in the closure of $\phi(E \times F)$. Then there exists a sequence $\{e_n\} \subset E$ and $\{f_n\} \subset F$ such that $x_n = e_n f_n e_n$ converges to x . Now since $|e_n f_n e_n| \geq \sup(|e_n|, |f_n|)$, $\{e_n\}$ and $\{f_n\}$ lie in compact subsets of E and F and have points of accumulation e and f (in E and F) respectively. Since ϕ is continuous, $x = e f e \in \phi(E \times F)$. Thus $\phi(E \times F)$ is closed. Since P is connected $\phi(E \times F) = P$. Since ϕ is continuous and one-to-one, it is a homeomorphism on each compact set of $E \times F$. Since ϕ^{-1} maps bounded sets of P into compact sets of $E \times F$, ϕ^{-1} must be continuous on each bounded set of P and is hence continuous on P . Consequently ϕ is a homeomorphism of $E \times F$ onto P . Proof of the theorem is now complete.

THEOREM 4. *Let \mathfrak{G} , \mathfrak{F} , e , f be as in Theorem 3. Then any non-singular $n \times n$ matrix can be expressed uniquely and continuously as $k \cdot f \cdot e$ where k is orthogonal, $e \in E$, $f \in F$.*

PROOF. Let K denote the group of orthogonal $n \times n$ matrices. Let θ denote the mapping $(k, f, e) \rightarrow k f e$ of $K \times F \times E$ into the full linear group.

θ is a one-to-one mapping. For if $k_1 f_1 e_1 = k_2 f_2 e_2$ with k_i, f_i, e_i in K, F, E ($i=1, 2$), then on multiplying by the transpose we obtain $e_1 f_1^2 e_1 = e_2 f_2^2 e_2$. By Theorem 3, $e_1 = e_2$, $f_1 = f_2$ and consequently $k_1 = k_2$.

The mapping θ is also onto. For given a non-singular matrix x , select $e \in E$ and $f \in F$ so as to satisfy $e f^2 e = {}^t x \cdot x$, which is certainly possible since ${}^t x \cdot x \in P$. Now $x(f e)^{-1}$ is orthogonal, for

$$\begin{aligned} {}^t(x(f e)^{-1}) \cdot x(f e)^{-1} &= {}^t(f e)^{-1} {}^t x x (f e)^{-1} \\ &= f^{-1} e^{-1} e f^2 e e^{-1} f^{-1} \\ &= I. \end{aligned}$$

Set $k = x(f e)^{-1}$. Then $x = k f e$ with $k \in K$, $f \in F$, $e \in E$.

Thus θ is a one-to-one onto mapping. The inverse θ^{-1} is also continuous. For in the representation $x = k f e$, e and f depend continuously on ${}^t x x$ by Theo-

rem 3 and thus depend continuously on x . It follows k too depends continuously on x . Hence θ^{-1} is continuous, and θ is a homeomorphism. Proof of theorem is now complete.

Let \mathfrak{G} be a real or complex Lie algebra. By its *adjoint group* or *group of inner automorphisms* is meant the linear Lie group on \mathfrak{G} that is generated by the Lie algebra of linear transformations $\text{ad } \mathfrak{G} - \text{ad } X$ denoting the transformation $Y \rightarrow [X, Y]$. A subalgebra \mathfrak{H} of a real Lie algebra \mathfrak{G} is said to be a *compact subalgebra* of \mathfrak{G} if the analytic subgroup of the adjoint group of \mathfrak{G} which is generated by the subalgebra $\{\text{ad } X \mid X \text{ in } \mathfrak{H}\}$ is compact. A real Lie algebra is called *compact* if its adjoint group is compact. If \mathfrak{H} is a compact subalgebra of \mathfrak{G} , then \mathfrak{H} is compact but not conversely.

By the *complexification* of a real Lie algebra is meant the Lie algebra over the complex numbers that is obtained upon augmenting the ground field to the field of complex numbers. By a *real form* of a complex Lie algebra \mathfrak{G} is meant a real linear subspace \mathfrak{H} which is closed under the formation of Poisson brackets and such that every element of \mathfrak{G} can be expressed uniquely as $X + \sqrt{-1}Y$ with X, Y in \mathfrak{H} . Thus it is a real Lie subalgebra whose complexification can be identified with \mathfrak{G} .

By a *compact real form* of a complex Lie algebra \mathfrak{G} is meant a real form which is compact. It is clear that this is a compact subalgebra of \mathfrak{G} regarded as a real Lie algebra.

It was first verified by E. Cartan and later proved by H. Weyl that every complex semi-simple Lie group has a compact real form. It is well known that in a compact semi-simple Lie algebra, that fundamental bilinear form is negative definite, i.e., the form $B(X, Y) = \text{Tr ad } X \text{ ad } Y$.

Let \mathfrak{G} be a real semi-simple Lie algebra, and let \mathfrak{G}_c denote its complexification. Let θ denote the conjugation of \mathfrak{G}_c with respect to \mathfrak{G} , that is, the correspondence $X + \sqrt{-1}Y \rightarrow X - \sqrt{-1}Y$ where X, Y are in \mathfrak{G} .

DEFINITION. A *Cartan decomposition* of \mathfrak{G} is a decomposition into the direct sum of a subalgebra \mathfrak{K} and a linear subspace \mathfrak{E} such that, for some compact real form \mathfrak{G}_K of \mathfrak{G}_c which is invariant under θ , $\mathfrak{K} = \mathfrak{G} \cap \mathfrak{G}_K$ and $\mathfrak{E} = \mathfrak{G} \cap \sqrt{-1}\mathfrak{G}_K$.

For existence of such a decomposition, cf. [3]. Since, in the above definition, $\mathfrak{G}_K = \mathfrak{K} + \sqrt{-1}\mathfrak{E}$, there is a one-to-one correspondence between Cartan decomposition of a real semi-simple Lie algebra \mathfrak{G} and compact real form of \mathfrak{G}_c which are invariant under the conjugation of \mathfrak{G}_c with respect to \mathfrak{G} . It is known in addition that \mathfrak{K} is a compact subalgebra of \mathfrak{G} .

Let now $\mathfrak{G}, \mathfrak{G}_c, \theta$ be as before, and let \mathfrak{G}_K be a compact real form of \mathfrak{G}_c that is invariant under θ . Since θ preserves Poisson brackets, its restriction to the

real form \mathfrak{G}_K is an automorphism of \mathfrak{G}_K . Let ϕ denote the extension of this automorphism to an automorphism of \mathfrak{G}_c . Then $\phi(X) = X$ for $X \in \mathfrak{G} \cap \mathfrak{G}_K$ and $\phi(X) = -X$ for $X \in \mathfrak{G} \cap \sqrt{-1} \mathfrak{G}_K$. Since ϕ is an automorphism of \mathfrak{G} it preserves the fundamental bilinear form, so that for any $X \in \mathfrak{R}$, $Y \in \mathfrak{G}$ we have $B(X, Y) = B(X, -Y)$ and hence $B(X, Y) = 0$. We can select a base (X_1, \dots, X_s) for \mathfrak{R} and a base (X_{s+1}, \dots, X_n) for \mathfrak{G} so that $B(X_i, X_j) = -\sqrt{ij}$ ($i, j \leq s$) and $B(X_i, X_j) = \sqrt{ij}$ for ($i, j > s$). Relative to the base (X_1, \dots, X_n) for \mathfrak{G} , it can be said the matrix representing $\text{ad} X$ is skew-symmetric or symmetric according as $X \in \mathfrak{R}$ or $X \in \mathfrak{G}$ respectively (cf. [3]). As a result, if we identify linear transformations on \mathfrak{G} with their matrices relative to the base (X_1, \dots, X_n) we have for any $X \in \mathfrak{G}$,

$$\text{ad} \phi(X) = -{}^t \text{ad} X.$$

With respect to this base, the matrices of $\text{ad} \mathfrak{R}$ are skew-symmetric and the matrices of $\text{ad} \mathfrak{G}$ are symmetric.

DEFINITION. Let $\mathfrak{R} + \mathfrak{G}$ be a Cartan decomposition of a real semi-simple Lie algebra \mathfrak{G} . By a $\mathfrak{R} + \mathfrak{G}$ base for \mathfrak{G} is meant any base with respect to which the matrices of $\text{ad} \mathfrak{R}$ and $\text{ad} \mathfrak{G}$ are respectively skew-symmetric and symmetric.

It is evident that with respect to a $\mathfrak{R} + \mathfrak{G}$ decomposition for a semi-simple algebra \mathfrak{G} , we have ${}^t \text{ad} \mathfrak{G} = \text{ad} \mathfrak{G}$, i.e., $\text{ad} \mathfrak{G}$ is a self-adjoint family of matrices.

THEOREM 5. Let G be a connected real semi-simple Lie group, let B denote the fundamental bilinear form on its Lie algebra \mathfrak{G} , and let $\mathfrak{R} + \mathfrak{G}$ be a Cartan decomposition of \mathfrak{G} (\mathfrak{R} being compact). Let \mathfrak{G}' be a linear subspace of \mathfrak{G} such that $[X, [X, Y]] \in \mathfrak{G}'$ for all $X, Y \in \mathfrak{G}'$. Let $\mathfrak{F} = \{X \mid B(X, \mathfrak{G}') = 0\}$. Then G decomposes topologically into $K \cdot F \cdot E'$ where K is the analytic subgroup determined by \mathfrak{R} , $F = \exp \mathfrak{F}$, $E' = \exp \mathfrak{G}'$.

PROOF. Let Ad denote the adjoint representation $x \rightarrow d\Gamma'_e(x)$ where $\Gamma'(x)$ denotes the inner automorphism $y \rightarrow xyx^{-1}$ of G and $d\Gamma'_e(x)$ is the differential of $\Gamma'(x)$ at the identity e . As is known, $\text{Ad} \exp X = \exp \text{ad} X$ for all X in the Lie algebra \mathfrak{G} (which is the tangent space to G at e). We select once and for all a fixed $\mathfrak{R} + \mathfrak{G}$ base in \mathfrak{G} , and we identify linear transformations on \mathfrak{G} with their matrix representations relative to the chosen base. For any $X \in \text{ad} \mathfrak{R}$, ${}^t X = -X$ where ${}^t X$ is the transpose of X ; for any $X \in \text{ad} \mathfrak{G}$, ${}^t X = X$. Hence ${}^t \text{ad} \mathfrak{G} = \text{ad} \mathfrak{G}$, and ${}^t \text{Ad} \exp \mathfrak{G} = \exp {}^t \text{ad} \mathfrak{G} = \exp \text{ad} \mathfrak{G} = \text{Ad} \exp \mathfrak{G}$. Since each element of the connected group $\text{Ad} G$ is a product of elements from $\text{Ad} \exp \mathfrak{G}$, it follows that ${}^t \text{Ad} G = \text{Ad} G$. Suppose now that $x \in \text{Ad} G$. By Theorem 4, $x = kfe$ where k is orthogonal, $e \in \exp \text{ad} \mathfrak{G}' = \text{Ad} E'$, and $f \in \exp \mathfrak{F}$, where $\mathfrak{F} = \{X \mid X \in \mathfrak{G}, \text{Tr} X \cdot \text{ad} \mathfrak{G}' = 0\}$ and \mathfrak{G} is the totality of real symmetric $n \times n$ matrices ($n = \dim \mathfrak{G}$). Consequently, $\text{Ad} G$

contains ${}^t x x = e f^2 e$. Since $e f^2 e$ is a positive definite symmetric matrix, in the semi-simple group $\text{Ad}G$, it is in the subset $\exp \text{ad} \mathfrak{G} = \text{Ad}E$ (cf. [3] Lemma 2.5 p. 976). Now by Theorem 3, $p = e f^2 e$ has a representation $e_1 f_1 e_1$ with $e_1 \in \exp \text{ad} \mathfrak{G}$. Hence $f_1 = e_1^{-1} p e_1^{-1} \in \exp \text{ad} \mathfrak{G}$ by Theorem 2. Applying the uniqueness part of Theorem 3, we conclude $f^2 = f_1 \in \exp \text{ad} \mathfrak{G} \cap \exp \tilde{\mathfrak{F}} = \exp(\tilde{\mathfrak{F}} \cap \text{ad} \mathfrak{G}) = \exp \mathfrak{F} = \text{Ad}F$. As a result $k = x e^{-1} f^{-1} \in \text{Ad}G$ and, being orthogonal, is in the analytic subgroup $\text{Ad}K$ (cf. [3], Lemma 2.5 p. 977). It now follows readily that $\text{Ad}G = \text{Ad}K \cdot \text{Ad}F \cdot \text{Ad}E'$ topologically. Repeating the argument in [3], Lemma 2.7 p. 978, we conclude that $G = K \cdot F \cdot E'$ topologically.

3. **Cartan's conjugacy theorem.** In §2 we have deduced simply and with rigor a number of properties of the Riemannian space P , which is a symmetric Riemannian space in the sense of Cartan. As a result, it is possible to present in a rigorous and simple way Cartan's proof that the maximal compact subgroup of a connected semi-simple group G are conjugate under inner automorphisms, (cf. [1]).

Let $\mathfrak{R} + \mathfrak{G}$ be a Cartan decomposition for \mathfrak{G} , the Lie algebra of G , and let K be the analytic subgroup of G that is determined by \mathfrak{R} . It is sufficient to prove that if K' is a compact subgroup of G , then there is an $x \in G$ such that $x^{-1} K' x \subset K$, i.e., $K' x K \subset x K$. This means that the subgroup K' operating on the space G/K of right cosets $[gK]$ by left translations has the coset $[xK]$ as a fixed point.

Let E denote the subspace $\exp \mathfrak{G}$ of G . Then the mapping $(e, k) \rightarrow ek$ of $E \times K$ into G is a homeomorphism and moreover the mapping $e \rightarrow \text{Ad}e$ is a homeomorphism of E into the space of linear transformations on \mathfrak{G} , (cf. [3]).

We choose once and for all a fixed $\mathfrak{R} - \mathfrak{G}$ base in \mathfrak{G} , and we identify linear transformations on \mathfrak{G} with their matrices relative to the chosen base. We denote by \mathfrak{S} and P the space of symmetric and positive definite matrices respectively. We regard P as a Riemannian space, the metric being the one adopted in §2, and we employ the same notation introduced in §2. Then $\text{ad} \mathfrak{G} \subset \mathfrak{S}$, $\text{Ad}E \subset P$, $\text{ad}X$ is skew-symmetric, and thus $\text{Ad}K$ is orthogonal.

Let ϕ denote the mapping $[xK] \rightarrow \text{Ad}e_x^2$ of G/K into $\text{Ad}E$ where by definition e_x is the unique element of E such that $e_x \cdot k = x$ for some $k \in K$. Let $t(g)$ denote the mapping which carries any g in G into the isometry $p \rightarrow \text{Ad}g \cdot p \cdot {}^t \text{Ad}g$. Then, ϕ is a homeomorphism of G/K into P which is equivariant with respect to the homomorphism t of G into the group of isometries on P . That ϕ is a homeomorphism follows immediately from the fact that $G = E \times K$ topologically, $e \rightarrow \text{Ad}e$ is a homeomorphism of E into P , and $p \rightarrow p^2$ is a homeomorphism of $\text{Ad}E$ onto $\text{Ad}E$. Since $\phi([xK]) = \text{Ad}e_x^2 = (\text{Ad}e_x)^2 = \text{Ad}x \cdot {}^t \text{Ad}x$, we have

$$\phi([g x K]) = \text{Ad}g x \cdot {}^t \text{Ad}x = \text{Ad}g \text{Ad}x \cdot {}^t \text{Ad}x \cdot {}^t \text{Ad}g = t(g) \cdot \phi([xK])$$

for all $g \in G$. Thus ϕ is equivariant with respect to t .

Accordingly, to prove that the compact subgroup K' has a fixed point in G/K is equivalent to proving that the compact group of isometries $\iota(K')$ has a fixed point in $\phi(G/K)$. Consequently, we can shift the fixed point investigation from G/K to $\text{Ad}E = \exp \text{ad} \mathfrak{E}$, and the conjugacy theorem will follow the result:

Let \mathfrak{E} be a linear subspace of \mathfrak{G} such that $(X, [X, Y]) \in \mathfrak{E}$ for all $X, Y \in \mathfrak{E}$ (i.e., such that $\exp \mathfrak{E}$ is a geodesic subspace; cf. Theorem 2). Let K be a compact group of isometries of P which keeps $E = \exp \mathfrak{E}$ invariant. Then K has a fixed point in E .

PROOF. Let x be any point of E , and let F be the function with E as domain such that $F(p) = \int_K \rho(p, k(x))^2 dk$ for $p \in E$. Let p_0 be a point of E which minimizes F . Clearly, there is such a p_0 . Since the family of isometries $p \rightarrow ep$ with $e \in E$ is transitive on E and keeps E invariant (Theorem 1) we can assume without loss of generality that p_0 is the identity I .

Now for any $p, q \in P$, $\rho(p, q) = \rho(p^{-1/2} p p^{-1/2}, p^{-1/2} q p^{-1/2}) = \rho_{\mathfrak{G}}(I, p^{-1/2} q p^{-1/2})$ by Lemma 3. Thus $\rho(p, q)^2 = \text{Tr}(\log p^{-1/2} q p^{-1/2})^2 = \text{Tr}(\log p^{-1} q)^2$, where by definition $\log m$ for any matrix m with only positive eigenvalues is $\log \text{Tr} m + L(m(\text{Tr} m)^{-1})$, $L(x)$ being the power series $\sum (-1)^{n+1} n^{-1} (x-1)^n$. It should be noted therefore that the eigenvalues of $p^{-1} q$ are the same as the eigenvalues of the positive definite matrix $p^{-1/2} q p^{-1/2}$. For letting $A = p^{-1/2} q$ and $B = p^{-1/2}$ the eigenvalues of AB and BA the solutions of the equations $|\lambda - AB| = 0$ and $|\lambda - BA| = 0$, and each is equivalent to $|\lambda B^{-1} - A| = 0$.

Let now p be a matrix, and let $\delta(t)$ be an analytic path of matrices with $\delta(0) = p$. We denote by δ the operator which assigns to matrix or scalar valued functions defined around p their derivatives with respect to t along $\delta(t)$ at $t=0$. Thus for example, if the power series $f(x) = \sum a_n x^n$ is convergent in a neighborhood of the matrix p , then

$$\begin{aligned} \delta \text{Tr} f(p) &= \text{Tr} \delta f(p) = \sum_n \sum_{r+s=n-1} n a_n p^r \delta p p^s \\ &= \text{Tr} \sum_n n a_n p^{n-1} \delta p \\ &= \text{Tr} f'(p) \cdot \delta p. \end{aligned}$$

Regarding now $\rho(p, q)$ as a function of its first argument, the point $q \in P$ being held fixed, and letting δ be an arbitrary analytic path emanating from the element $p \in P$, we have

$$\begin{aligned}\delta\rho(p, q)^2 &= \delta \operatorname{Tr}(\log pq^{-1})^2 = 2 \operatorname{Tr}[\log pq^{-1}](pq^{-1})^{-1} \delta p \cdot q^{-1} \\ &= 2 \operatorname{Tr} q^{-1}(\log pq^{-1}) q \cdot p^{-1} \cdot \delta p.\end{aligned}$$

Since $q^{-1} \log(pq^{-1}) q \cdot p^{-1}$ as a function of p is uniformly continuous on each compact set in P , the convergence of the difference-quotient to the derivative $\delta\rho(p, q)^2$ is uniform. As a result, $\delta F(p) = \int_K \delta\rho(p, k(x))^2 dk$, for any δ lying in E . Since F is a differentiable function of p , by Rolle's theorem $\delta F = 0$ for any δ in E which originates at l .

Thus for any such δ

$$0 = \delta F(l) = \int_K \delta\rho(l, k(x))^2 dk = \int_K 2 \operatorname{Tr} \log q^{-1} \cdot \delta p dk = -2 \int_K \operatorname{Tr} \log q \cdot \delta p dk.$$

On the other hand, $\delta\rho_{\mathbb{C}}(p, q)^2 = \delta \operatorname{Tr}(\log p - \log q)^2 = 2 \operatorname{Tr}(\log p - \log q) q^{-1} \delta p$ and for $p = l$ we get $\delta\rho_{\mathbb{C}}(l, q)^2 = -2 \operatorname{Tr} \log q \cdot \delta p$, δ being a path originating at l . As a result, l is an extremum for the function $G(p) = \int_K \rho_{\mathbb{C}}(p, k(x))^2 dk$ with $p \in F$. However, the correspondence $p \rightarrow \log p$ with $p \in E$ is an isometry of E onto \mathbb{C} relative to metrics $\rho_{\mathbb{C}}$ in E and euclidean distance in \mathbb{C} , and any extremum for $G(\exp X)$ with $X \in \mathbb{C}$ is the unique center of mass of the set $\log K(x)$, the point $k(x)$ being weighted by k .

More rigorously, if f is a continuous mapping of the compact group K into the euclidean space \mathbb{C} , then at the extrema of the function $h(X) = \int_K |X - f(k)|^2 dk$, we have $\int_K (X - f(k)) \cdot \delta X dk = 0$, the dot multiplication being inner product, for any δ in \mathbb{C} with origin at X . Thus $0 = \int_K (X - f(k)) dk \cdot \delta X$ by linearity and thus $\int_K (X - f(k)) dk = 0$. Consequently $X = \int_K f(k) dk / \int_K dk$ and $h(X)$ has but one extremum—its unique minimum. Taking f to be the mapping $k \rightarrow \log k(x)$ of K into \mathbb{C} , the minimum for $h(X)$ is $X = 0$, and thus $\int_K \rho_{\mathbb{C}}(l, k(x))^2 dk < \int_K \rho_{\mathbb{C}}(p, k(x))^2 dk$ if $p \neq l$.

Applying Lemma 2 of §2, we obtain

$$\int_K \rho(l, k(x))^2 dk = \int_K \rho_{\mathbb{C}}(l, k(x))^2 dk < \int_K \rho_{\mathbb{C}}(p, k(x))^2 dk \leq \int_K \rho(p, k(x))^2 dk$$

if $p \neq l$. That is, l is the unique minimum of $F(p)$. Now by the invariance of Haar measure in K under translations, we have

$$F(c(p)) = \int_K \rho(c(p), k(x))^2 dk = \int_K \rho(p, c^{-1}k(x))^2 dk = \int_K \rho(p, k(x))^2 dk = F(p)$$

so that $F(c(l)) = F(l)$ and thus $c(l) = l$ for all $c \in K$. Consequently, K admits a fixed point in E .

We have thus proved: if G is a real connected semi-simple Lie group, and if

$\mathfrak{R} + \mathfrak{C}$ is a Cartan decomposition of its Lie algebra (\mathfrak{R} the compact part), then any compact subgroup of G is conjugate under an inner automorphism to a subgroup of K , the analytic subgroup determined by \mathfrak{R} .

That is, any two maximal compact subalgebras of a real semi-simple algebra \mathfrak{G} are conjugate under an inner automorphism of \mathfrak{G} . If $\mathfrak{R} + \mathfrak{C}$ is a Cartan decomposition of \mathfrak{G} (with \mathfrak{R} the compact part), then \mathfrak{R} is a maximal compact subalgebra.

Now, $\text{Ad}K$ being compact, K has a unique maximal compact subgroup K_0 (cf. [3], pp. 979-980). Thus every maximal compact subgroup of G is conjugate to K_0 under an inner automorphism.

If $\mathfrak{R}_1 + \mathfrak{C}_1$ and $\mathfrak{R}_2 + \mathfrak{C}_2$ are Cartan decompositions for the real semi-simple algebra \mathfrak{G} , \mathfrak{R}_i being the compact part, then there is an inner automorphism T carrying \mathfrak{R}_1 into \mathfrak{R}_2 . Since automorphisms of \mathfrak{G} preserve the fundamental bilinear form B , T carries \mathfrak{C}_1 , the orthogonal complement to \mathfrak{R}_1 with respect to B , into \mathfrak{C}_2 . Thus any two Cartan decompositions of a real semi-simple algebra are conjugate under an inner automorphism.

4. Some preliminaries about automorphisms. Let \mathfrak{G}_K be a compact semi-simple Lie algebra, i.e., its fundamental bilinear form $B(X, Y) = \text{Tr} X \text{ad} Y$ is negative definite. Let \mathfrak{H}_K be a Cartan subalgebra of \mathfrak{G}_K , and let $\mathfrak{G}_c, \mathfrak{H}_c$ be the complexifications of $\mathfrak{G}_K, \mathfrak{H}_K$ respectively (cf. [3] §2). Then it is known that

(1) Modulo \mathfrak{H}_c , there is a base $\{e_\alpha \mid \text{all roots } \alpha \text{ defined on } \mathfrak{H}_c\}$ for \mathfrak{G}_c such that $[h, e_\alpha] = \alpha(h)e_\alpha$ for all $h \in \mathfrak{H}_c$, and for each α .

(2) To each root α , there corresponds a unique $h_\alpha \in \mathfrak{H}_c$ such that $B(h, h_\alpha) = \alpha(h)$, for all $h \in \mathfrak{H}_c$. $B(h_\alpha, h_\beta)$ is a real number invariant under automorphisms of the roots (i.e., correspondences between roots which preserves sums).

(3) The e_α can be chosen so as to satisfy $[e_\alpha, e_{-\alpha}] = h_\alpha$.

(4) $[e_\alpha, e_\beta] = \begin{cases} c_{\alpha\beta} e_{\alpha+\beta} & \text{if } \alpha+\beta \text{ is a root} \\ 0 & \text{otherwise.} \end{cases}$

$c_{\alpha, \beta} c_{-\alpha, -\beta}$ is a negative number invariant under root automorphisms.

(5) Let \mathfrak{H}_0 be the real linear span of $\{h_\alpha \mid \text{all roots } \alpha\}$, and let R_0 be the space of real linear functions on \mathfrak{H}_0 . Then each automorphism of the roots determines a unique linear transformation of R_0 .

(6) $\mathfrak{H}_K = \sqrt{-1} \mathfrak{H}_0$. The e_α can be so selected as to satisfy the additional conditions $c_{\alpha, \beta} = -c_{-\alpha, -\beta}$, and $ze_\alpha - \bar{z}e_{-\alpha} \in \mathfrak{G}_K$ for each complex number z and root α . In this case, \mathfrak{G}_K is spanned by \mathfrak{H}_K and $\{ze_\alpha - \bar{z}e_{-\alpha}\}$.

(7) Let Γ denote the set of automorphisms of \mathfrak{G}_c which keep \mathfrak{H}_c (and hence \mathfrak{H}_0 and \mathfrak{H}_K) invariant. If $\phi \in \Gamma$, let ϕ^* denote the linear transformation of R_0 such that $\phi^* \rho(\phi h) = \rho(h)$ for any $\rho \in R_0, h \in \mathfrak{H}_0$. Then $\phi \rightarrow \phi^*$ is a homeomor-

phism of Γ onto the group of linear transformations of R_0 which take roots into roots. The kernel of this homeomorphism consists of inner automorphisms of \mathfrak{G}_c . If S is a subset of Γ , S^* denotes $\{\phi^* | \phi \in S\}$.

(8) Let I be the totality of inner automorphisms in Γ . The group I^* is called the *Weyl group*. The group Γ^* is called the *Cartan group*. For any $\rho, \sigma \in R_0$, define $B^*(\rho, \sigma) = B(h_\rho, h_\sigma)$ where h_ρ is the element of \mathfrak{H}_0 satisfying $B(h, h_\rho) = \rho(h)$ for all $h \in \mathfrak{H}_c$. Then B^* is a positive definite metric on R_0 and the Weyl group contains a generating set of reflections with respect to B^* . By a *chamber* is meant the interior of a fundamental domain bounded by reflecting planes. Since I is normal in Γ , I^* is normal in Γ^* . Hence the family of reflecting planes of I^* and, thus, chambers are permuted by the Cartan group. Furthermore, $I^* = I_K^*$ where I_K is the subset of I keeping \mathfrak{G}_K invariant, ([6]).

(9) Each chamber C is bounded by s faces, where $s = \dim R_0 = \dim \mathfrak{H}_0 = \text{rank } \mathfrak{G}_c$; i.e., to each chamber, there corresponds a *fundamental system* of s roots β_1, \dots, β_s such that $C = \{\rho | B^*(\rho, \beta_i) > 0\}$. Each root $\alpha = n_1\beta_1 + \dots + n_s\beta_s$ where n_1, \dots, n_s are integers of the same sign or zero. In addition

$$\{e_{\beta_1}, \dots, e_{\beta_s}, e_{-\beta_1}, \dots, e_{-\beta_s}\}$$

generates \mathfrak{G}_c .

(10) An *admissible ordering* of the roots is an ordering such that if $\alpha \leq \alpha_1$ and $\beta \leq \beta_1$, then $\alpha + \beta \leq \alpha_1 + \beta_1$. If $\{\rho_1, \dots, \rho_s\}$ is any base for R_0 , then lexicographic ordering with respect to the components of roots relative to this base is an admissible ordering. A root is called *positive* relative to an admissible ordering if it is greater than 0. A root ρ is called *prime* under an admissible ordering if $\pm \rho \neq \alpha + \beta$ where $\mp \rho < \alpha, \beta < \pm \rho$. A positive root is prime if and only if it is not the sum of two positive roots. Assume $\alpha \rightarrow \alpha'$ is a root automorphism. Let

$$-a_n < -a_{n-1} < \dots < 0 < a_1 < \dots < a_n$$

be any admissible ordering of the roots. Define for each positive root ρ a complex number u_ρ by induction on the subscript of $\rho = a_k$:

$$u_\rho \text{ is } \begin{cases} \text{arbitrary if } \rho \text{ is prime} \\ \frac{c_{\alpha'\beta'}}{c_{\alpha\beta}} u_\alpha u_\beta \text{ if } \rho = \alpha + \beta \quad 0 < \alpha, \beta < \rho. \end{cases}$$

By a theorem of Weyl, the numbers u_ρ defined in this way are defined consistently and the linear transformation of \mathfrak{G}_c with $e_\alpha \rightarrow u_\alpha e_{\alpha'}, h_\alpha \rightarrow h_{\alpha'}$ (all roots α) is

an automorphism of \mathfrak{G}_c , where by definition $u_{-\alpha}u_\alpha = 1$.

(11) Any two Cartan subalgebras of a real compact or complex semi-simple Lie algebra are conjugate under an inner automorphism, (cf. [2], [5], or [6]).

5. Automorphisms of compact semi-simple algebra. Let \mathfrak{G}_K be a real semi-simple Lie algebra which is compact, and let it be imbedded in its complexification.

LEMMA 5. Suppose $X \in \mathfrak{G}_K$, $Y \in \sqrt{-1} \mathfrak{G}_K$ and $e = \exp \text{ad } Y$. If $e(X) \in \mathfrak{G}_K$ then $[Y, X] = 0$.

PROOF. $e(X) = \exp \text{ad } Y(X) = \cosh \text{ad } Y(X) + \sinh \text{ad } Y(X)$. Since $(\text{ad } Y)^n(X)$ is in $\sqrt{-1} \mathfrak{G}_K$ for all odd powers n , and in \mathfrak{G}_K for all even powers n , $\cosh \text{ad } Y(X) \in \mathfrak{G}_K$, $\sinh \text{ad } Y(X) \in \sqrt{-1} \mathfrak{G}_K$.

Since $e(X) \in \mathfrak{G}_K$ by hypothesis, $\sinh \text{ad } Y(X) = 0$. But $\text{ad } Y$ is a semi-simple linear transformation (i.e., minimal equations have no repeated factors) and its eigenvalues are all real (cf. § 2).

Since moreover $\sinh x$ is a one-to-one real valued function of the real number x , the subspaces of eigenvectors belonging to its various eigenvalues is the same for $\text{ad } Y$ and $\sinh \text{ad } Y$. As a result any eigenvector of $\sinh \text{ad } Y$ is an eigenvalue of $\text{ad } Y$. Since $\sinh^{-1} 0 = 0$, $\sinh \text{ad } Y(X) = 0$ implies $\text{ad } Y(X) = 0$, i.e., $[Y, X] = 0$.

REMARK. It is known (cf. [3]) that any inner automorphism of \mathfrak{G}_c can be represented as $e \cdot k$ where k is an inner automorphism generated by $\text{ad } \mathfrak{G}_K$ and $e \in \exp \text{ad } \sqrt{-1} \mathfrak{G}_K$. If ek keeps \mathfrak{G}_K invariant, then $e(\mathfrak{G}_K) \subset \mathfrak{G}_K$. By Lemma 4.1 e is the identity transformation on \mathfrak{G}_K and hence on \mathfrak{G}_c . Thus the only inner automorphisms keeping \mathfrak{G}_K invariant are the inner automorphisms of \mathfrak{G}_K . As a result $\text{Ad}(\mathfrak{G}_K)$, the adjoint group of \mathfrak{G}_K , can be identified with the subgroup of $\text{Ad}(\mathfrak{G}_c)$ which keeps \mathfrak{G}_K invariant.

Let \mathfrak{G}_K be a real semi-simple Lie algebra which is compact, let \mathfrak{H}_K be a Cartan subalgebra of \mathfrak{G}_K , let \mathfrak{G}_c denote the complexification of \mathfrak{G}_K , and let \mathfrak{H}_c denote the extension of \mathfrak{H}_K to \mathfrak{G}_c . Then \mathfrak{H}_c is a Cartan subalgebra of \mathfrak{G}_c (cf. [3], p. 969). We employ the notation introduced in § 4.

Select elements $\{e_\alpha | \text{all roots } \alpha\}$ so as to satisfy conditions (1) through (6) of § 4. Let C be a chamber defined by a fundamental system of roots $(\beta_1, \dots, \beta_s)$. Let O^* denote the subgroup of the Cartan group Γ^* which keeps the chamber C invariant. To each $\phi^* \in O^*$, we let correspond an automorphism ϕ_0 which is an extension of ϕ^* , and which is defined as follows: order the roots lexicographically with respect to β_1, \dots, β_s , apply Weyl's procedure to define for each root α the number u_α , and take care to define $u_\alpha = 1$ if α is a positive prime root (cf. Re-

mark 10 of §4). Then the numbers $\{u_\alpha \mid \text{all roots } \alpha\}$ are uniquely defined, and ϕ_0 is defined as the automorphism $h_\alpha \rightarrow h_{\phi^* \alpha}, e_\alpha \rightarrow u_\alpha e_{\phi^* \alpha}$ (all roots α). Let $0 = \{\phi_0 \mid \phi^* \in 0\}$. Then the correspondence $\phi^* \rightarrow \phi_0$ of 0^* into Γ is an isomorphism. For each root β_i of the fundamental system being prime in the selected ordering, $\phi_0 e_{\beta_i} = e_{\phi^* \beta_i}$ ($i=1, \dots, s$) for any $\phi_0 \in 0$. Thus $\phi_0 e_{-\beta_i} = e_{\phi^*(-\beta_i)}$ ($i=1, \dots, s$). In as much as ϕ^* permutes $\{\beta_1, \dots, \beta_s\}$, ϕ_0 effects a permutation of the generating set of root vectors $e_{\beta_1}, \dots, e_{\beta_s}, e_{-\beta_1}, \dots, e_{-\beta_s}$ (all $\phi^* \in 0^*$). It follows immediately that $\phi^* \rightarrow \phi_0$ is an isomorphism of 0^* into Γ . Since the chamber C is the interior of a fundamental domain for the Weyl group Γ^* , it is evident that the Cartan group $\Gamma^* = 0^* \cdot \Gamma^*$ (semi-direct). In view of the isomorphisms of 0^* onto 0 which is the inverse of the natural homomorphism of 0 onto 0^* , we have $\Gamma = 0 \cdot \Gamma$ (semi-direct).

Let us denote by $\text{Aut} \mathfrak{G}_c, \text{Aut} \mathfrak{G}_K, \text{Ad} \mathfrak{G}_c, \text{Ad}_c \mathfrak{G}_K$ the group of automorphisms of \mathfrak{G}_c , the subgroup of $\text{Aut} \mathfrak{G}_c$ keeping \mathfrak{G}_K invariant, the group of inner automorphism of \mathfrak{G}_c , the subgroup of $\text{Ad} \mathfrak{G}_c$ which keeps \mathfrak{G}_K invariant respectively. Let $\text{Aut} \mathfrak{G}_K$ and $\text{Ad} \mathfrak{G}_K$ denote the group of automorphisms of the real Lie algebra \mathfrak{G}_K and the subgroup of inner automorphisms respectively. Finally, let 0_K denote the set of restrictions of automorphisms in the set 0 to \mathfrak{G}_K .

LEMMA 5.2. 0 keeps \mathfrak{G}_K invariant. Moreover,

(a) $\text{Aut} \mathfrak{G}_c = 0 \cdot \text{Ad} \mathfrak{G}_c$ (semi-direct),

(b) $\text{Aut}_c \mathfrak{G}_K = 0 \cdot \text{Ad}_c \mathfrak{G}_K$ (semi-direct),

(c) $\text{Aut} \mathfrak{G}_K = 0_K \cdot \text{Ad} \mathfrak{G}_K$ (semi-direct).

PROOF. By choice of root vectors, \mathfrak{G}_K is spanned by \mathfrak{H}_K and $\{ze_\alpha - \bar{z}e_{-\alpha} \mid \text{all roots } \alpha, z \text{ any complex number}\}$ (cf. Remark 6 of §4). Let $\phi_0 \in 0$ and let a' denote $\phi^* a$ for any root a . Then $c_{\alpha, \beta}^2 = c_{\alpha', \beta'}^2$ for all roots α, β (remarks (4) and (6) of §4), so that $c_{\alpha', \beta'} / c_{\alpha, \beta} = \pm 1$. It follows that $u_\alpha = \pm 1$ for any α where u_α is the number defined by the relation $\phi_0(e_\alpha) = u_\alpha e_{\alpha'}$. Thus $u_{-\alpha} = u_\alpha = \bar{u}_\alpha$ for all roots α . Hence $\phi_0(ze_\alpha - \bar{z}e_{-\alpha}) = zu_\alpha e_{\alpha'} - \bar{z}u_{-\alpha} e_{-\alpha'} = zu_\alpha e_{\alpha'} - \bar{z}u_\alpha e_{-\alpha'}$ for each root α . In addition $\phi_0(\mathfrak{H}_K) \subset \mathfrak{H}_K$. Hence $\phi_0(\mathfrak{G}_K) \subset \mathfrak{G}_K$.

Assertion (a) now follows from the fact that Cartan subalgebras are permuted *transitively* by inner automorphisms.

Assertion (b) now follows from the fact that Cartan subalgebras of \mathfrak{G}_K are permuted *transitively* by inner automorphisms of \mathfrak{G}_K . And finally assertion (c) follows from the natural isomorphism between $\text{Ad}_c \mathfrak{G}_K$ and $\text{Ad} \mathfrak{G}_K$ that was pointed out above.

LEMMA 5.3. Let ϕ be an automorphism of the compact semi-simple Lie al-

gebra \mathfrak{G}_K such that ϕ^2 is inner. Then there exists an inner automorphism g of \mathfrak{G}_K such that $g\phi$ is of order two.

PROOF. We employ notation as above. Then by assertion (c), $\text{Aut } \mathfrak{G}_K = 0_K \cdot \text{Ad } \mathfrak{G}_K = \text{Ad } \mathfrak{G}_K \cdot 0_K$, the latter equality holding since $\text{Ad } \mathfrak{G}_K$ is a normal subgroup of $\text{Aut } \mathfrak{G}_K$. Select the element $g \in \text{Ad } \mathfrak{G}_K$ so that $g\phi \in 0_K$. Then $(g\phi)^2 = g\phi g\phi = g\phi(\phi^{-1}g\phi)$ is inner and is in 0_K . Let h denote the extension of $(g\phi)^2$ to an automorphism of \mathfrak{G}_c . Then $h \in 0$ and is inner. Hence $h \in 0 \cap I = \{\text{identity}\}$.

6. A normal form for semi-simple subalgebras. Let \mathfrak{G} be a real semi-simple Lie algebra, let \mathfrak{G}_c denote its complexification, and let θ denote the conjugation of \mathfrak{G}_c with respect to \mathfrak{G} . It is known that there is a compact real form of \mathfrak{G}_c invariant under θ (cf. [6] or [3]). We prove here a sharper result.

THEOREM. Let \mathfrak{G}' be a semi-simple subalgebra of \mathfrak{G} . Then any compact real form of \mathfrak{G}'_c invariant under θ can be extended to a compact real form of \mathfrak{G}_c invariant under θ .

PROOF. Let \mathfrak{G}'_K be a compact real form of \mathfrak{G}'_c which is invariant under θ . Let \mathfrak{G}_K^* be a maximal compact subalgebra of \mathfrak{G}_c which includes \mathfrak{G}'_K . Since $[\theta(X), \theta(Y)] = \theta([X, Y])$ for any $X, Y \in \mathfrak{G}_c$, $\mathfrak{A}(\mathfrak{G}_K)$ is a maximal compact subalgebra of \mathfrak{G}_c regarded as a real Lie algebra. By a theorem of Cartan (cf. §3), maximal compact subalgebras of a semi-simple algebra are conjugate under inner automorphisms. Since \mathfrak{G}_c is semi-simple as a real Lie algebra, there is an inner automorphism g of \mathfrak{G}_c such that $\theta(\mathfrak{G}_K) = g(\mathfrak{G}_K)$. Let ϕ denote the restriction of $g^{-1}\theta$ to \mathfrak{G}_K^* . Then ϕ is an automorphism of \mathfrak{G}_K^* with ϕ^2 inner. By Lemma 5.3 of §5, there is an inner automorphism \bar{g} of \mathfrak{G}_K^* such that $\bar{g}\phi$ is of order 2. Letting $h = \bar{g}g^{-1}$, and $a = h\theta$, we have $a = h\theta$ on \mathfrak{G}_K^* where h is an inner automorphism of \mathfrak{G}_c and a is an automorphism of \mathfrak{G}_K^* of order two. We now extend the domain of definition of a to all of \mathfrak{G}_c by defining $a = h\theta$. a is thus *not* an automorphism of \mathfrak{G}_c but rather a conjugation, i.e., $a(aX + bY) = \bar{a}a(X) + \bar{b}a(Y)$, $a([X, Y]) = [a(X), a(Y)]$.

Nevertheless, any conjugation of \mathfrak{G}_c is an automorphism of \mathfrak{G}_c when we regard \mathfrak{G}_c as a Lie algebra over the field of real numbers.

It is well known that any automorphism of a real Lie algebra \mathfrak{G} can be extended to an automorphism of the simply connected form \tilde{G} of \mathfrak{G} . Since any automorphism keeps the center of \tilde{G} invariant and \tilde{G} modulo its center can be identified with the adjoint group of \mathfrak{G} , i.e., the group of inner automorphisms of \mathfrak{G} , any automorphism of \mathfrak{G} induces in a natural way an automorphism of the adjoint group of \mathfrak{G} . Moreover, if \mathfrak{G}_c is a complex Lie algebra, then the adjoint group of \mathfrak{G}_c when regarded as a real Lie group is the same as the adjoint group of the real Lie algebra \mathfrak{G}_c . Thus the conjugations a and θ , as well as the automorphism h , induces

in a natural way real automorphisms of $\text{Ad}(\mathfrak{G}_c)$, the adjoint group of \mathfrak{G}_c . We denote these automorphisms of the adjoint group by the same letters a, θ, h respectively. We will take care to avoid confusing $\theta \cdot h$ and $\theta(h) = \theta h \theta^{-1} = \theta h \theta$. We also observe that h , as an automorphism of $\text{Ad}(\mathfrak{G}_c)$, is the transformation $h(g) = h g h^{-1}$.

We have

$$I = a^2 = h \theta h \theta = h \cdot \theta(h)$$

where I is the identity automorphism of \mathfrak{G}_c . Hence

$$\theta(h) = h^{-1}.$$

On the other hand, $a = h \theta$ implies $\theta = \theta^{-1} = a^{-1} h = a h$, so that

$$\theta(h) = a(h).$$

It is known that any element of $\text{Ad}(\mathfrak{G}_c)$ can be represented uniquely as $k \cdot e$, where $k \in \text{Ad}_c(\mathfrak{G}_K^*)$ and $e \in \exp \text{ad} \sqrt{-1} \mathfrak{G}_K$. Hence $\theta(h) = a(h) = a(k e) = a(k) a(e)$. Since $a(\mathfrak{G}_K^*) \subset \mathfrak{G}_K^*$ and a is a conjugation of \mathfrak{G}_c , $a(\sqrt{-1} \mathfrak{G}_K^*) \subset \sqrt{-1} \mathfrak{G}_K^*$. As a result $a(k) \in \text{Ad}_c(\mathfrak{G}_K)$ and $a(e) \in \exp \text{ad} \sqrt{-1} \mathfrak{G}_K$. But $\theta(h) = h^{-1} = e^{-1} k^{-1} = k^{-1} (h e^{-1} k^{-1})$. Since $k^{-1} \in \text{Ad}_c(\mathfrak{G}_K^*)$ and $k e^{-1} k^{-1} \in \exp \text{ad} \sqrt{-1} \mathfrak{G}_K^*$, we infer $a(k) = k^{-1}$, $a(e) = k e^{-1} k^{-1}$.

It is known that the correspondence $\text{ad} Y \rightarrow \exp \text{ad} Y$, $Y \in \sqrt{-1} \mathfrak{G}_K^*$, is a one-to-one mapping of $\text{ad} \sqrt{-1} \mathfrak{G}_K^*$ onto $\exp \text{ad} \sqrt{-1} \mathfrak{G}_K^*$. Since $a(\sqrt{-1} \mathfrak{G}_K^*) \subset \sqrt{-1} \mathfrak{G}_K^*$, it follows from the preceding remark that $a(e^t) = k e^{-t} k^{-1}$, where e^t denotes $\exp t \text{ad} Y$, and $Y \in \sqrt{-1} \mathfrak{G}_K^*$. Hence

$$\theta(e^t) = (h^{-1} a)(e) = h^{-1}(a(e^t)) = e^{-1} k^{-1} (k e^{-t} k^{-1}) k e = e^{-t}.$$

Let $\mathfrak{G}_K = e^{-1/2}(\mathfrak{G}_K^*)$. Then

$$\begin{aligned} \theta(\mathfrak{G}_K) &= (\theta \cdot e^{-1/2})(\mathfrak{G}_K^*) = \theta(e^{-1/2}) \theta(\mathfrak{G}_K^*) = e^{1/2} h^{-1} a(\mathfrak{G}_K^*) \\ &= e^{1/2} e^{-1} k^{-1} (\mathfrak{G}_K^*) = e^{-1/2}(\mathfrak{G}_K^*) = \mathfrak{G}_K. \end{aligned}$$

Thus \mathfrak{G}_K is invariant under θ . Furthermore $\mathfrak{G}'_K = \theta(\mathfrak{G}'_K) = h^{-1} a(\mathfrak{G}'_K) = e^{-1} k^{-1} a(\mathfrak{G}'_K)$, so that $e(\mathfrak{G}'_K) \subset \mathfrak{G}_K^*$. By Lemma 5.1 of § 5, it follows that $e^t(X) = X$ for all $X \in \mathfrak{G}'_K$. Thus $\mathfrak{G}'_K = e^{-1/2}(\mathfrak{G}'_K) \subset \mathfrak{G}_K$; that is, \mathfrak{G}'_K is a compact real form of \mathfrak{G}_c which is invariant under θ and which includes \mathfrak{G}_K .

Proof of the theorem is now complete.

An immediate corollary of the theorem is

COROLLARY 6.1. *Let $\mathfrak{G}_1 \subset \mathfrak{G}_2 \subset \dots \subset \mathfrak{G}_n = \mathfrak{G}$ be an ascending sequence of semi-simple subalgebras of the real semi-simple Lie algebra \mathfrak{G} . Let \mathfrak{G}_{ic} denote the complexification of $\mathfrak{G}_i (i=1, \dots, n)$ and let θ denote the conjugation of \mathfrak{G}_c with respect to \mathfrak{G} . Then there is a compact real form \mathfrak{G}_K of \mathfrak{G}_c such that $\mathfrak{G}_K \cap \mathfrak{G}_{ic}$ is a compact real form of $\mathfrak{G}_{ic} (i=1, \dots, n)$.*

PROOF. First select any compact real form of \mathfrak{G}_{1c} that is invariant under θ . Then extend it to an invariant compact real form of \mathfrak{G}_{2c} , extend this, etc. Take \mathfrak{G}_K to be the invariant compact form that is obtained for \mathfrak{G}_{nc} (after n extensions).

Associated with any Cartan decomposition $\mathfrak{R} + \mathfrak{G}$ of a real semi-simple Lie algebra \mathfrak{G} is a unique compact real form \mathfrak{G}_K of the complexification \mathfrak{G}_c such that (cf. § 2)

$$\mathfrak{R} = \mathfrak{G} \cap \mathfrak{G}_K, \quad \mathfrak{G} = \mathfrak{G} \cap \sqrt{-1} \mathfrak{G}_K.$$

Thus Theorem 6' can be restated as

THEOREM 6. *Let \mathfrak{G}' be a semi-simple subalgebra of \mathfrak{G} and let $\mathfrak{R}' + \mathfrak{G}'$ be a Cartan decomposition for \mathfrak{G}' . Then there is a Cartan decomposition $\mathfrak{R} + \mathfrak{G}$ for \mathfrak{G} with $\mathfrak{R}' \subset \mathfrak{R}$ and $\mathfrak{G}' \subset \mathfrak{G}$.*

7. A normal form for real semi-simple linear Lie algebras.

THEOREM 7. *Let $\mathfrak{G}_1 \subset \mathfrak{G}_2 \subset \dots \subset \mathfrak{G}_n$ be an ascending chain of semi-simple Lie algebras of endomorphisms of the real linear space \mathfrak{V} (of finite dimension). Then a positive definite inner product B for \mathfrak{V} can be so chosen that*

$$\mathfrak{G}_i = \mathfrak{G}_i \cap \mathfrak{R} + \mathfrak{G}_i \cap \mathfrak{G} \quad (i=1, \dots, n)$$

where \mathfrak{R} and \mathfrak{G} are the totality of skew-symmetric and symmetric endomorphisms with respect to B .

PROOF. Let γ be an arbitrary base in \mathfrak{V} , and let \mathfrak{G}_{n+1} denote the Lie algebra of all endomorphisms of \mathfrak{V} where trace is 0. Then $\mathfrak{G}_{n+1} \supset \mathfrak{G}_n$, \mathfrak{G}_{n+1} is semi-simple and $\mathfrak{R} + \mathfrak{G}$ is a Cartan decomposition for \mathfrak{G}_{n+1} where \mathfrak{R} and \mathfrak{G} are the totality of endomorphisms where matrices with respect to γ are respectively skew-symmetric and symmetric of trace 0.

It follows from Corollary 6.1 that there is a Cartan decomposition $\mathfrak{R} + \mathfrak{G}_0$ for \mathfrak{G}_{n+1} such that $\mathfrak{G}_i \cap \mathfrak{R} + \mathfrak{G}_i \cap \mathfrak{G}$ is a Cartan decomposition for $\mathfrak{G}_i (i=1, \dots, n+1)$.

Since any Cartan decompositions of a real semi-simple algebra are conjugate under an *inner* automorphism (cf. §3), there is an automorphism T of \mathfrak{B} in \mathfrak{G}_{n+1} such that $T\bar{\mathfrak{R}}T^{-1} = \mathfrak{R}$, $T\bar{\mathfrak{S}}T^{-1} = \mathfrak{S}_0$. Now let C denote the (unique) inner product on \mathfrak{B} such that γ is an orthonormal base with respect to C , and let B be the inner product on \mathfrak{B} such that $B(X, Y) = C(T^{-1}X, T^{-1}Y)$ for any X, Y in \mathfrak{B} . Then for any $k \in \bar{\mathfrak{R}}$, and X, Y in \mathfrak{B}

$$C(kX, Y) + C(X, kY) = 0,$$

$$B(TkT^{-1}X, Y) + B(X, TkT^{-1}Y) = C(kT^{-1}X, T^{-1}Y) + C(T^{-1}X, kT^{-1}Y) = 0$$

so that \mathfrak{R} is skew-symmetric with respect to B . Since \mathfrak{R} is a maximal compact subalgebra of \mathfrak{G}_{n+1} , it consists of the totality of skew-symmetric endomorphisms of \mathfrak{B} with respect to B . Similarly \mathfrak{S} is the totality of symmetric endomorphisms with respect to B whose trace is 0.

Now let \mathfrak{S} denote the totality of symmetric endomorphisms of \mathfrak{B} with respect to B . Then $\mathfrak{G}_i = \mathfrak{G}_i \cap \mathfrak{R} + \mathfrak{G}_i \cap \mathfrak{S}$ ($i=1, \dots, n$). Proof of the theorem is now complete.

BIBLIOGRAPHY

1. E. Cartan, *Groupes simples clos et ouvert*, J. Math. Pures Appl. vol. 8 (1929) pp. 1–33.
2. C. Chevalley, *An algebraic proof of a property of Lie groups*, Amer. J. Math. vol. 63 (1941) pp. 785–793.
3. G. D. Mostow, *A new proof of E. Cartan's theorem on the topology of semi-simple groups*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 969–980.
4. C. L. Siegel, *Symplectic geometry*, Amer. J. Math. vol. 63 (1943) pp. 1–86.
5. A. Weil, *Démonstration topologique d'un théorème fondamental de Cartan*, C. R. Acad. Sci. Paris vol. 200 (1935) pp. 518–520; Mat. Sbornik N. S. vol. 1 (1936) p. 779.
6. H. Weyl, *Zur theorie der Darstellung kontinuierlicher half-einfacher Gruppen I–III*, Math. Zeitsch. vol. 23–24 (1924–25).

THE JOHNS HOPKINS UNIVERSITY, BALTIMORE, MD. AND
 INSTITUTO DE MATEMATICA PURA E APLICADA, RIO DE JANEIRO, BRASIL.

MEMOIRS
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> . 90 pp. 1951. | 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. | 1.20 |
| 7. R. V. Kadison, <i>A representation theory for commutative topological algebras</i> . 39 pp. 1951. | 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. 1955. | 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 |

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