TREATISE ON ANALYSIS

Volume V
Volume 10

TREATISE ON ANALYSIS

10-II. Chapters XII–XV, enlarged and corrected printing, 1976
10-III. Chapters XVI–XVII, 1972
10-IV. Chapters XVIII–XX, 1974
10-V. Chapter XXI, 1977
SCHEMATIC PLAN OF THE WORK

I. Elements of the theory of sets
II. Real numbers
III. Metric spaces
IV. Additional properties of the real line
V. Normed spaces
VI. Hilbert spaces
VII. Spaces of continuous functions
VIII. Differential calculus
IX. Analytic functions
X. Existence theorems
XI. Elementary spectral theory
XII. Topology and topological algebra
XIII. Integration
XIV. Haar measure and convolution
XV. Normed algebras and spectral theory
XVI. Differential manifolds
XVII. Distributions and differential operators
XVIII. Differential systems
XIX. Lie groups
XX. Riemannian geometry
XXI. Compact Lie groups
XXII. Harmonic analysis
XXIII. Linear functional equations
XXIV. Elementary differential topology
XXV. Nonlinear problems
In the following definitions, the first number indicates the chapter in which the notation is introduced, and the second number indicates the section within the chapter.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U(\mu)$</td>
<td>$\int U(s) , d\mu(s)$, where $U$ is a continuous unitary representation of a group $G$ and $\mu$ is a bounded measure on $G$: 21.1</td>
</tr>
<tr>
<td>$U(f)$, $U(\tilde{f})$</td>
<td>$\int f(s) , U(s) , d\beta(s)$, where $\beta$ is a Haar measure on $G$, and $f \in \mathcal{L}^1_c(G, \beta)$: 21.1</td>
</tr>
<tr>
<td>$U_{\text{ext}}$</td>
<td>Mapping $\mu \mapsto U(\mu)$: 21.1</td>
</tr>
<tr>
<td>$R(s)$</td>
<td>Left regular representation $\tilde{f} \mapsto (\varepsilon \ast f) \tilde{\cdot}$: 21.1</td>
</tr>
<tr>
<td>$U_1 \oplus U_2$</td>
<td>Direct sum of two continuous linear representations: 21.1</td>
</tr>
<tr>
<td>$U^{(\mathbb{R})}$, $U^{(\mathbb{H})}$</td>
<td>Real (resp. quaternionic) linear representation corresponding to a complex linear representation $U$: 21.1, Problem 9</td>
</tr>
<tr>
<td>$\alpha_p (p \in R(G))$</td>
<td>Minimal two-sided ideals of the complete Hilbert algebra $L^2_\mathbb{C}(G)$, for $G$ compact: 21.2</td>
</tr>
<tr>
<td>$u_p$</td>
<td>Identity element of $\alpha_p$: 21.2</td>
</tr>
<tr>
<td>$n_p$</td>
<td>The integer such that $\alpha_p$ is isomorphic to $M_{n_p}(\mathbb{C})$: 21.2</td>
</tr>
<tr>
<td>$m_{l_k}^{(p)}$</td>
<td>Elements of $\alpha_p$: 21.2</td>
</tr>
<tr>
<td>$M_p(s)$</td>
<td>The matrix $(n_p^{-1} m_{l_k}^{(p)}(s))$: 21.2</td>
</tr>
<tr>
<td>$p_0$</td>
<td>Index of the trivial ideal $\alpha_{p_0} = \mathbb{C}$: 21.2</td>
</tr>
</tbody>
</table>
$\chi_{p}$
$n_{p}^{-1} u_{p}$: 21.3
the index such that $\chi_{p} = \overline{\chi}_{p}$: 21.3

$\bar{\rho}$

$\text{cl}(V)$
class $\sum_{\rho \in \mathbb{R}} d_{\rho} \cdot \rho$ of a finite-dimensional linear representation: 21.4
ring of classes of continuous linear representations of $G$: 21.4

$Z^{(R)}, Z^{(R(G))}$
bilinear form $(u, v) \mapsto \text{Tr}(U_{*}(u) \circ U_{*}(v))$ associated with a linear representation $U$ of a Lie group: 21.5
bilinear form $(u, v) \mapsto \text{Tr}(\rho(u) \circ \rho(v))$ associated with a homomorphism of Lie algebras $\rho : \mathfrak{g} \to \text{gl}(F)$: 21.5

$B_{U}$
Killing form $(u, v) \mapsto \text{Tr}(\text{ad}(u) \circ \text{ad}(v))$ of a Lie algebra $\mathfrak{g}$: 21.5

$B_{\rho}$
kernel $\exp^{-1}(e)$ of the exponential $\exp$ of $T$, where $t$ is the Lie algebra of the torus $T$: 21.7
dual of the lattice $\Gamma_{T}$, in $t^*$: 21.7

$\Gamma_{T}$
Weyl group $\mathcal{W}(T)/T$, where $T$ is a maximal torus of $G$: 21.7

$\mathfrak{w}, \lambda$
$\mathfrak{w}^{-1}(\lambda)$, for $w \in W$ and $\lambda \in t^*$: 21.8

$\mathcal{S}(G, T), \mathcal{S}(G), \mathcal{S}$
set of roots of $G$ with respect to $T$: 21.8

$\mathfrak{g}_{\mathfrak{x}}$
subspace of $\mathfrak{g}_{\mathfrak{g}}$ consisting of the vectors $x$ such that $[u, x] = \alpha(u)x$ for all $u \in t$: 21.8

$U_{\mathfrak{x}}$
subgroup $\chi_{\mathfrak{x}}^{-1}(1)$ of $T$, where $\chi_{\mathfrak{x}}(\exp(u)) = e^{\alpha(u)}$ for $u \in t$: 21.8

$u_{\mathfrak{x}}$
hyperplane $\alpha^{-1}(0)$ in $t$: 21.8

$s_{\mathfrak{x}}$
element of $W$ acting on $t$ by reflection in the hyperplane $u_{\mathfrak{x}}$: 21.8

$L_{m}$
simple $U(\mathfrak{sl}(2, \mathbb{C}))$-module of dimension $m+1$: 21.9

$\mathfrak{g} = \mathfrak{h} \bigoplus_{\alpha \in \mathcal{S}} \mathfrak{g}_{\alpha}$
root decomposition of a complex semisimple Lie algebra $\mathfrak{g}$: 21.10 and 21.20

$\mathfrak{h}_{\alpha}^{0}$
element of $\mathfrak{h}$ such that $\alpha(h) = \Phi(h, \mathfrak{h}_{\alpha}^{0})$: 21.10

$\mathfrak{h}_{\mathfrak{x}}$
element of $\mathfrak{h}$ such that $\alpha(h_{\mathfrak{x}}) = 2$ and $\mathfrak{h}_{\mathfrak{x}} \in [\mathfrak{g}_{\mathfrak{x}}, \mathfrak{g}_{-\mathfrak{x}}]$: 21.10

$\mathfrak{x}_{\mathfrak{x}}, \mathfrak{x}_{-\mathfrak{x}}$
elements of $\mathfrak{g}_{\mathfrak{x}}, \mathfrak{g}_{-\mathfrak{x}}$, respectively, such that $[\mathfrak{x}_{\mathfrak{x}}, \mathfrak{x}_{-\mathfrak{x}}] = \mathfrak{h}_{\mathfrak{x}}$: 21.10
\(\sigma_x\) bijection \(\lambda \mapsto \lambda - \lambda(h_x)\alpha\) of \(\mathfrak{h}^*\) onto itself: 21.10

\(s_x\) Lie subalgebra \(\mathfrak{ch}_x \oplus \mathfrak{cx}_x \oplus \mathfrak{cx}_{-x}\): 21.10

\(N_{\alpha, \beta}\) numbers such that \([x_\alpha, x_\beta] = N_{\alpha, \beta} x_{\alpha + \beta}\) when \(\alpha + \beta \in S\): 21.10

\(D(G)\) union of the hyperplanes in \(\mathfrak{t}\) with equations \(\alpha(u) = 2\pi in, n \in \mathbb{Z}\): 21.10, Problem 2

\(\sigma_x\) bijection \(\lambda \mapsto \lambda - v_\alpha(\lambda)\alpha\), for a reduced root system \(S\) in \(F\): 21.11

\(W_S\) Weyl group of \(S\), generated by the \(\sigma_x\); 21.11

\(n(\alpha, \beta)\) Cartan integers \(v_\beta(\alpha) = 2(\beta|\alpha)/(\beta|\beta)\) for \(\alpha, \beta \in S\): 21.11

\(S^+_x\) set of \(\alpha \in S\) such that \(\alpha(x) > 0\): 21.11

\(B_S\) basis of \(S\), namely the set of indecomposable elements of \(S^+_x\): 21.11

\(S^+\) set of positive roots, relative to a basis \(B\) of \(S\): 21.11

\(S'\) root system formed by the \(v_\alpha \in F^*\): 21.11

\(B'\) basis of \(S'\) consisting of the \(v_\alpha, \alpha \in B\): 21.11

\(\delta\) \[
\frac{1}{2} \sum_{\lambda \in S^+} \lambda : 21.11
\]

\(e_r\) linear form on \(\mathfrak{t} = \bigoplus_{s=1}^{n} \mathbb{R}E_{ss} < \mathfrak{m}_n(\mathbb{C})\) such that \(e_r(iE_{ss}) = i\delta_{rs}\): 21.12

\(\text{Sp}(2n, \mathbb{C}), \text{sp}(2n, \mathbb{C})\) complex symplectic group and its Lie algebra: 21.12

\(\text{SO}(m, \mathbb{C}), \text{so}(m, \mathbb{C})\) complex special orthogonal group and its Lie algebra: 21.12

\(A_n, B_n, C_n, D_n\) Lie algebras of the classical groups: 21.12

\(P(G, T), P(G), P\) lattice \(2\pi i \Gamma^P\) of weights of \(G\) with respect to \(T\): 21.13

\(e^p, s \mapsto e^{p(s)}\) character \(\exp(u) \mapsto e^{p(u)}\) of \(P\), where \(p \in P\): 21.13

\(S(\Pi)\) \[
\sum_{p \in \Pi} e^p, \text{ where } \Pi \text{ is an orbit of the Weyl group } W \text{ in } P : 21.13
\]

\( h_j \), \( P(\mathfrak{g}) \):

\( h_{\beta_j} \), where \( \{\beta_1, \ldots, \beta_l\} \) is a basis of \( \mathfrak{s} \); 21.14

set of \( \lambda \in t_\mathfrak{g}^* \) such that \( \lambda(h_j) \in \mathbb{Z} \) for all \( \alpha \in \mathfrak{s} \), or equivalently such that \( \lambda(h_j) \in \mathbb{Z} \) for \( 1 \leq j \leq l \); 21.14

\( C(\mathfrak{g}), C \):

Weyl chamber in \( \mathfrak{i}^* \), consisting of the \( \lambda \) such that \( \lambda(h_j) > 0 \) for \( 1 \leq j \leq l \); 21.14

order relation on \( \mathfrak{i}^* \), equivalent to \( \lambda = \mu \) or \( \mu - \lambda = \gamma + \sum c_j \beta_j \), with \( \gamma \in \mathfrak{i}^* \) and \( c_j \geq 0 \) and not all zero; 21.14

\( s_j \):

reflection \( s_{\beta_j} : \lambda \mapsto \lambda - \lambda(h_j)\beta_j \) for \( 1 \leq j \leq l \); 21.14

\( H_\alpha \):

hyperplane in \( \mathfrak{i}^* \) with equation \( \lambda(h_\alpha) = 0 \); 21.14

\( \mathbb{Z}[P]^{\mathbb{A}W} \):

set of \( W \)-anti-invariant elements of \( \mathbb{Z}[P] \); 21.14

\( J(e^p) \):

\[ \sum_{w \in W} \det(w)e^{w \cdot p} \text{, where } p \in P \]; 21.14

\( P_{\text{reg}} \):

set of weights \( \lambda \in P \) which are regular linear forms; 21.14

\( S(p) \):

\( S(\Pi) \), where \( \Pi \) is the \( W \)-orbit of \( p \in P \cap \bar{C} \); 21.14

\( \Delta \):

\( J(e^p) = \prod_{\alpha \in \mathfrak{S}^*} (e^{p/2} - e^{-p/2}) \); 21.14

\( T_{\text{reg}} \):

set of regular points of the maximal torus \( T \subset G \); 21.15

\( u_G, u_T, u_{G/T} \):

invariant volume-forms on \( G, T \) and \( G/T \); 21.15

\( m_G, m_T, m_{G/T} \):

invariant measures corresponding to the volume-forms \( u_G, u_T, u_{G/T} \); 21.15

\( \mu = n_1\beta_1 + \cdots + n_l\beta_l \):

highest root in \( \mathfrak{s} \), relative to the basis \( B = \{\beta_1, \ldots, \beta_l\} \); 21.15, Problem 10

\( \mathfrak{w} \):

affine Weyl group; 21.15, Problem 11

\( \mathfrak{w}^* \):

hyperplane with equation \( \alpha(u) = 2\pi k \) in \( \mathfrak{i}^* \); 21.15, Problem 11

\( \{p_1, p_2, \ldots, p_l\} \):

basis of \( \mathfrak{i}^* \) dual to \( \{\beta_1, \beta_2, \ldots, \beta_l\} \); 21.15, Problem 11

\( Q(\mathfrak{g}) \):

sublattice \( P(G/Z) \) of \( P(G) \) generated by the roots \( \alpha \in \mathfrak{s} \); 21.16

\( \omega \):

fundamental weights \( (1 \leq j \leq l) \) relative to the basis \( B \) of \( \mathfrak{s} \); 21.16

simply connected covering group of \( SO(m) \) (\( m \geq 3 \)); 21.16
\begin{itemize}
  \item \(a(E)\) \hspace{2cm} set of self-adjoint automorphisms of \(E\): 21.17
  \item \(a_+(E)\) \hspace{2cm} set of positive self-adjoint automorphisms of \(E\): 21.17
  \item \(\mathcal{G}_u, g_u, g, c_u\) \hspace{2cm} \(\mathcal{G}_u\) a simply connected compact semisimple Lie group; \(g_u = \text{Lie}(\mathcal{G}_u)\); \(g = (g_u)_G\); \(c_u\) the conjugation of \(g\) for which \(g_u\) is the set of fixed vectors: 21.18
  \item \(\mathcal{G}\) \hspace{2cm} simply connected complex Lie group with Lie algebra \(g\): 21.18
  \item \(c_0\) \hspace{2cm} conjugation of \(g\) which commutes with \(c_u\): 21.18
  \item \(l_0, i\rho_0\) \hspace{2cm} real vector subspaces of \(g_u\) on which \(c_0(x) = x\) and \(c_0(x) = -x\), respectively: 21.18
  \item \(g_0\) \hspace{2cm} subalgebra of invariants of \(c_0\): 21.18
  \item \(\check{P}\) \hspace{2cm} image of \(i\rho_0\) under the mapping \(iu \mapsto \exp_G(iu)\): 21.18
  \item \(G_0, K_0, P_0\) \hspace{2cm} \(G_0\) the Lie subgroup of \(\mathcal{G}_{IR}\) consisting of the fixed points of \(\sigma\) such that \(\sigma_\ast = c_0\); \(K_0 = G_0 \cap \mathcal{G}_u\); \(P_0 = G_0 \cap \check{P}\): 21.18
  \item \(G_1\) \hspace{2cm} \(\mathcal{G}_0/D\), a group locally isomorphic to \(\mathcal{G}_0\): 21.18
  \item \(K_1, P_1\) \hspace{2cm} \(K_1 = \mathcal{K}_0/D\); \(P_1 = \text{image of } \rho_0\) under \(\exp_{G_1}\): 21.18
  \item \(G_2\) \hspace{2cm} \(\mathcal{G}_u/(C \cap G_0), C\) the centre of \(\mathcal{G}_u\): 21.18
  \item \(K_2\) \hspace{2cm} \(K_0/(C \cap G_0)\): 21.18
  \item \(K'\) \hspace{2cm} subgroup of fixed points of \(\sigma_2\), the automorphism of \(G_2\) obtained from \(\sigma\) on passing to the quotient: 21.18
  \item \(P_2\) \hspace{2cm} image of \(i\rho_0\) under \(\exp_{G_2}\): 21.18
  \item \(\alpha < \beta\) \hspace{2cm} lexicographic ordering: 21.20
  \item \(a_0\) \hspace{2cm} maximal commutative subalgebra of \(P_0\): 21.21
  \item \(t\) \hspace{2cm} maximal commutative subalgebra of \(g_u\) containing \(a_0\): 21.21
  \item \(S'\) \hspace{2cm} subset of \(S\) consisting of the roots which vanish on \(ia_0\): 21.21
\end{itemize}
### NOTATION

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S''_+$</td>
<td>subset of $S'' = S - S'$ consisting of the $\alpha$ such that $\alpha(z_0) &gt; 0$: 21.21</td>
</tr>
<tr>
<td>$\mathfrak{n}, \mathfrak{n}_0$</td>
<td>$\mathfrak{n} = \bigoplus \mathfrak{g}_\alpha, \mathfrak{n} = \mathfrak{n}_0 \cap \mathfrak{g}_0$: 21.21</td>
</tr>
<tr>
<td>$\mathfrak{k}_k$</td>
<td>Lie algebra of matrices $(x_{hj})$ such that $x_{kj} = 0$ for $j + k &gt; h$: 21.21</td>
</tr>
</tbody>
</table>
CHAPTER XXI
COMPACT LIE GROUPS AND SEMISIMPLE LIE GROUPS

It is rarely the case in mathematics that one can describe explicitly all the objects endowed with a structure that is characterized by a few simple axioms. A classical (and elementary) example is that of finite commutative groups (A.26.4). By contrast, in spite of more than a century of effort and an enormous accumulation of results, mathematics is still very far from being able to describe all noncommutative finite groups, even when supplementary restrictions (such as simplicity or nilpotency) are imposed.

It is therefore all the more remarkable that, in the theory of Lie groups, all the compact simply connected Lie groups are explicitly known, and that, starting from these groups, the structure of compact connected Lie groups is reduced to a simple problem in the theory of finitely generated commutative groups ((16.30.2) and (21.6.9)). The compact simply connected Lie groups are finite products of groups that are either the universal covering groups of the “classical groups” SO(n), SU(n), and U(n, H) (16.11) (and therefore depend on an integral parameter) or the five “exceptional” groups, of dimensions 14, 52, 78, 133, and 248. We shall not get as far as this final result, but we shall develop the methods leading to it, up to the point where what remains to be done is an enumeration (by successive exclusion) of certain algebraic objects related to Euclidean geometry, subjected to very restrictive conditions of an arithmetic nature, which allow only a small number of possibilities (21.10.3) (see [79] or [85] for a complete account).

These methods are based in part on the elementary theory of Lie groups in Chapter XIX, and in part on a fundamental new idea, which dominates this chapter and the next, and whose importance in present-day mathematics cannot be overemphasized; the notion of a linear representation of a group. The first essential fact is that where compact groups are concerned (whether they are Lie groups or not) we may restrict our attention to finite-dimensional linear representations (21.2.3). The second unexpected
XXI COMPACT LIE GROUPS AND SEMISIMPLE LIE GROUPS

phenomenon is that where compact connected Lie groups are concerned, everything rests on the explicit knowledge of the representations of only two types of groups: the tori $T^n$ and the group $SU(2)$ (21.9). Roughly speaking, these are the "building blocks" with which we can "construct" all the other compact connected Lie groups and obtain not only their explicit structure but also an enumeration of all their linear representations (21.15.5).

The interest attached to the compact connected Lie groups arises not only from the esthetic attractions of the theory, which is one of the most beautiful and most satisfying in the whole of mathematics, but also from the central position they occupy in the welter of modern theories. In the first place, they are closely related to a capital notion in the theory of Lie groups, namely that of a semisimple group (compact or not), and in fact it turns out that a knowledge of the compact semisimple groups determines all the others (21.18). Since the time of F. Klein it has been recognized that classical "geometry" is essentially the study of certain semisimple groups; and E. Cartan, in his development of the notions of fiber bundle and connection, showed that these groups play an equally important role in differential geometry (see Chapter XX). From then on, their influence has spread into differential topology and homological algebra. We shall see in Chapter XXII how—again following E. Cartan—it has been realized over the last twenty-five years that the study of representations of semisimple groups (but now on infinite-dimensional spaces) is fundamental in many questions of analysis, not to speak of applications to quantum mechanics. But the most unexpected turn has been the invasion of the theory of semisimple groups into regions that appear completely foreign: "abstract" algebraic geometry, number theory, and the theory of finite groups. It has been known since the work of S. Lie and E. Cartan that semisimple groups are algebraic (that is, they can be defined by polynomial equations); but it is only since 1950 that it has come to be realized that this is no accidental fact, but rather that the theory of semisimple groups has two faces of equal importance: the analytic aspect, which gave birth to the theory, and the purely algebraic aspect, which appears when one considers a ground field other than $\mathbb{R}$ or $\mathbb{C}$. We have not, unfortunately, been able to take account of this second aspect; here we can only remark that its repercussions are increasingly numerous, and refer the reader to the works [80], [81], [74], [77], and [78] in the bibliography.

1. CONTINUOUS UNITARY REPRESENTATIONS OF LOCALLY COMPACT GROUPS

(21.1.1) Let $G$ be a topological group, $E$ a Hausdorff topological vector space over the field $\mathbb{C}$ of complex numbers. Generalizing the definition given in (16.9.7), we define a continuous linear representation of $G$ on $E$ to be a
mapping $s \mapsto U(s)$ of $G$ into the group $\text{GL}(E)$ of automorphisms of the topological vector space $E$, which satisfies the following conditions:

(a) $U(st) = U(s)U(t)$ for all $s, t \in G$;
(b) for each $x \in E$, the mapping $s \mapsto U(s) \cdot x$ of $G$ into $E$ is continuous.

It follows from (a) that $U(e) = 1_E$ (where $e$ is the identity element of $G$) and that, for all $s \in G$,

\[(21.1.1.1)\quad U(s^{-1}) = U(s)^{-1}.\]

If $E$ is of finite dimension $d$, the representation $U$ is said to be of dimension (or degree) $d$, and we sometimes write $d = \dim U$.

The mapping $U_0$ that sends each $s \in G$ to the identity automorphism $1_E$ is a continuous linear representation of $G$ on $E$, called the trivial representation.

A vector subspace $F$ of $E$ is said to be stable under a continuous linear representation $U$ of $G$ on $E$ if $U(s)(F) \subseteq F$ for all $s \in G$; in that case, the mapping $s \mapsto U(s) \mid F$ is a continuous linear representation of $G$ on $F$, called the subrepresentation of $U$ corresponding to $F$.

A continuous linear representation $U$ of $G$ on $E$ is said to be irreducible (or topologically irreducible) if the only closed vector subspaces $F$ of $E$ that are stable under $U$ are $\{0\}$ and $E$. For each $x \neq 0$ in $E$, the set $\{U(s) \cdot x : s \in G\}$ is then total in $E$ (12.13).

(21.1.2) In this chapter and the next, we shall be concerned especially with the case where $E$ is a separable Hilbert space. A continuous unitary representation of $G$ on $E$ is then a continuous linear representation $U$ of $G$ on $E$ such that for each $s \in G$ the operator $U(s)$ is unitary, or in other words (15.5) is an automorphism of the Hilbert space structure of $E$. This means that the operators $U(s)$ satisfy conditions (a) and (b) of (21.1.1), together with the following condition:

(c) $(U(s) \cdot x \mid U(s) \cdot y) = (x \mid y)$ for all $s \in G$ and all $x, y \in E$.

In particular, $U(s)$ is an isometry of $E$ onto $E$, for all $s \in G$, and we have

\[(21.1.2.1)\quad U(s)^{-1} = (U(s))^*.\]

for all $s \in G$.

(21.1.3) (i) When $E$ is finite-dimensional, condition (b) of (21.1.1) is equivalent to saying that $s \mapsto U(s)$ is a continuous mapping of $G$ into the normed algebra $L(E)$ (relative to any norm that defines the topology of $E$); for it is
equivalent to saying that if \((u_k(s))\) is the matrix of \(U(s)\) relative to some basis of \(E\), then the functions \(u_k\) are continuous on \(G\). On the other hand, if \(E\) is a separable Hilbert space of infinite dimension and \(U\) is a continuous unitary representation of \(G\) on \(E\), then \(U\) is not in general a continuous mapping of \(G\) into the normed algebra \(\mathcal{L}(E)\) (Problem 3).

(ii) When \(E\) is finite-dimensional, a continuous linear representation \(U\) of \(G\) on \(E\) is not necessarily a continuous unitary representation relative to any scalar product (6.2) on \(E\). For example, if \(G = \mathbb{R}\), the continuous linear representation

\[
U : x \mapsto \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}
\]

of \(G\) on \(C^2\) is not unitary, relative to any scalar product on \(C^2\), because any unitary matrix is similar to a diagonal matrix (15.11.14) (cf. Section 21.18, Problem 1).

(21.1.4) Throughout the rest of this chapter we shall consider only separable metrizable locally compact groups, and as in Chapter XIV the phrases "locally compact group" and "compact group" will mean "separable metrizable locally compact group" and "metrizable compact group," respectively.

Let \(G\) be a locally compact group, \(\mu\) a bounded complex measure (13.20) on \(G\), and \(U\) a continuous unitary representation of \(G\) on a separable Hilbert space \(E\). For each pair of vectors \(x, y\) in \(E\), the function \(s \mapsto (U(s) \cdot x \mid y)\) is continuous and bounded on \(G\), because \(\|U(s) \cdot x\| = \|x\|\); it is therefore \(\mu\)-integrable, and by (13.20.5) we have

\[
\left| \int (U(s) \cdot x \mid y) \, d\mu(s) \right| \leq \|\mu\| \cdot \|x\| \cdot \|y\|.
\]

Since \(E\) may be identified with its dual, it follows that there exists a unique vector \(U(\mu) \cdot x\) in \(E\) such that

\[
\int (U(s) \cdot x \mid y) \, d\mu(s) = (U(\mu) \cdot x \mid y)
\]

for all \(y \in E\), and this allows us to write (13.10.6)

\[
U(\mu) \cdot x = \int (U(s) \cdot x) \, d\mu(s).
\]

It is clear that this relation defines a continuous endomorphism \(U(\mu)\) of \(E\), since (21.1.4.1) implies that

\[
\|U(\mu)\| \leq \|\mu\|.
\]
In particular, we have

\[(21.1.4.4) \quad U(\varepsilon_s) = U(s)\]

for all \(s \in G\).

The relation (21.1.4.2) is sometimes written in the abridged form

\[(21.1.4.5) \quad U(\mu) = \int U(s) \, d\mu(s).\]

(21.1.5) We recall (15.4.9) that the set \(M_b^1(G)\) of bounded complex measures on \(G\) is an involutory Banach algebra over \(\mathbb{C}\), the multiplication being convolution of measures, and the involution \(\mu \mapsto \hat{\mu}\). When a left Haar measure \(\beta\) has been chosen on \(G\), the normed space \(L_c^1(G)\) may be canonically identified with a closed vector subspace of \(M_b^1(G)\), by identifying the class \(\mathcal{I}\) of a \(\beta\)-integrable function \(f\) with the bounded measure \(f \cdot \beta\), since \(\|f \cdot \beta\| = N_1(f)\) (13.20.3). By the definition of the convolution of two functions in \(L_c^1(G)\) (14.10.1), \(L_c^1(G)\) is a subalgebra of \(M_b^1(G)\) if we define the product of the classes of two functions \(f, g \in L_c^1(G)\) to be the class of \(f \ast g\). If in addition \(G\) is unimodular (14.3), \(L_c^1(G)\) is a two-sided ideal in \(M_b^1(G)\), and the transform of the measure \(f \cdot \beta\) under the involution \(\mu \mapsto \hat{\mu}\) is \(\mathcal{I} \cdot \beta\) (14.3.4.2). We may therefore consider \(L_c^1(G)\) as an involutory closed subalgebra of \(M_b^1(G)\), the involution being that which transforms the class of \(f\) into the class of \(\mathcal{I}\).

We deduce from this that if \(G\) is unimodular, then for each representation (15.5) \(V\) of the involutory Banach algebra \(L_c^1(G)\) on a Hilbert space \(E\), we have

\[(21.1.5.1) \quad \|V(\mathcal{I})\| \leq N_1(f)\]

for all \(f \in L_c^1(G)\). For if \(G\) is discrete, this is just (15.5.7) because the identity element \(\varepsilon_e\) of \(M_b^1(G)\) then belongs to \(L_c^1(G)\). If \(G\) is not discrete, it is immediately seen that \(V\) may be extended to a representation on \(E\) of the involutory Banach subalgebra \(A = L_c^1(G) \oplus C \varepsilon_e\) of \(M_b^1(G)\) by putting \(V(f \cdot \beta + \lambda \varepsilon_e) = V(\mathcal{I}) + \lambda \cdot 1_E\), and (15.5.7) can then be applied to this algebra with identity element.

(21.1.6) Under the assumptions of (21.1.4), the mapping \(\mu \mapsto U(\mu)\) is a representation (15.5) of the involutory Banach algebra \(M_b^1(G)\) on the Hilbert space \(E\). If in addition \(G\) is unimodular, the restriction of \(\mu \mapsto U(\mu)\) to \(L_c^1(G)\) is nondegenerate.

It follows immediately from (21.1.4.4) that \(U(\varepsilon_s) = 1_E\). To prove the first assertion, it remains to show that \(U(\mu \ast \nu) = U(\mu)U(\nu)\) and \(U(\hat{\mu}) = (U(\mu))^*\),
where $\mu$, $\nu$ are any two bounded measures on $G$. If $x$, $y$ are any two vectors in $E$ then by definition (14.5) we have

\[
(U(\mu \ast \nu) \cdot x \mid y) = \int (U(s) \cdot x \mid y) \, d(\mu \ast \nu)(s)
\]

\[
= \int \int (U(sw) \cdot x \mid y) \, d\mu(v) \, dv(w)
\]

\[
= \int \int (U(w) \cdot x \mid (U(v))^* \cdot y) \, d\mu(v) \, dv(w)
\]

\[
= \int (U(v) \cdot x \mid (U(v))^* \cdot y) \, d\mu(v)
\]

\[
= \int (U(v) \cdot (U(v) \cdot x) \mid y) \, d\mu(v)
\]

\[
= (U(\mu)U(v) \cdot x \mid y)
\]

by virtue of the Lebesgue–Fubini theorem, and this proves the first relation.

Next, using the fact that the operators $U(s)$ are unitary, we have

\[
((U(\mu))^* \cdot x \mid y) = \overline{(U(\mu) \cdot y \mid x)}
\]

\[
= \int \overline{(U(s) \cdot y \mid x)} \, d\mu(s)
\]

\[
= \int \overline{(U(s) \cdot y \mid x)} \, d\bar{\mu}(s)
\]

\[
= \int (U(s^{-1}) \cdot x \mid y) \, d\bar{\mu}(s)
\]

\[
= \int (U(t) \cdot x \mid y) \, d\bar{\mu}(t)
\]

\[
= (U(\hat{\mu}) \cdot x \mid y)
\]

by the definition of the measure $\hat{\mu}$ (15.4.9), and this proves the second relation.

In particular, for each $s \in G$ and each bounded measure $\mu$ on $G$, we have

(21.1.6.1) \quad U(\varepsilon_s \ast \mu) = U(s)U(\mu), \quad U(\mu \ast \varepsilon_s) = U(\mu)U(s).

Let $(V_n)$ be a decreasing sequence of neighborhoods of $e$ in $G$, forming a fundamental system of neighborhoods of $e$. For each $s \in G$ and each $n$, let $u_n$
be a positive-valued function belonging to $\mathcal{X}(G)$ with support contained in $sV_n$ and such that $\int u_n \, d\beta = 1$. For each $x \in E$ and each $\varepsilon > 0$, there exists an integer $n$ such that

\[(21.1.6.2) \| U(t) \cdot x - U(s) \cdot x \| \leq \varepsilon \]

for all $t \in sV_n$. We have then, for all $y \in E$,

\[ (U(u_n \cdot \beta)x - U(s) \cdot x \mid y) = \int (U(t) \cdot x - U(s) \cdot x \mid y) u_n(t) \, d\beta(t) \]

and the inequality (21.1.6.2) therefore implies that

\[ \| U(u_n \cdot \beta) \cdot x - U(s) \cdot x \| \leq \varepsilon. \]

If there existed a vector $x \neq 0$ such that $U(f \cdot \beta) \cdot x = 0$ for all functions $f \in \mathcal{L}^1(G)$, we should therefore have $U(s) \cdot x = 0$ for all $s \in G$, which is absurd (take $s = e$). The restriction of the representation $\mu \mapsto U(\mu)$ to $L^1_c(G)$ is therefore nondegenerate.

By abuse of language, we shall call the restriction of $\mu \mapsto U(\mu)$ to $L^1_c(G)$ the extension of $U$ to $L^1_c(G)$, and we shall denote it by $U_{\text{ext}}$. For $f \in \mathcal{L}^1_c(G)$, we shall write $U(f)$ instead of $U(f \cdot \beta)$ or $U(\tilde{f})$.

\[ (21.1.7) \quad \text{Let } G \text{ be a unimodular, separable, metrizable, locally compact group. Then the mapping } U \mapsto U_{\text{ext}} \text{ is a bijection of the set of continuous unitary representations of } G \text{ on } E \text{ onto the set of nondegenerate representations of the involutive Banach algebra } L^1_c(G) \text{ on } E. \text{ Furthermore, in order that a closed vector subspace } F \text{ of } E \text{ should be stable under all the operators } U(s) (s \in G), \text{ it is necessary and sufficient that it should be stable under all the operators } U(f) \text{ for } f \in \mathcal{L}^1_c(G) (\text{or just for } f \in \mathcal{X}(G)). \]

We have seen in the course of the proof of (21.1.6) that, for each $s \in G$ and $x \in E$, the vector $U(s) \cdot x$ is the limit of a sequence $U(u_n) \cdot x$ with $u_n \in \mathcal{X}(G)$. This shows already that the mapping $U \mapsto U_{\text{ext}}$ is injective, and that if a closed subspace $F$ of $E$ is stable under the operators $U(f)$ (where $f \in \mathcal{L}^1_c(G)$ or $f \in \mathcal{X}(G)$), then it is stable under the operators $U(s) (s \in G)$; and the converse follows directly from the definition of $U(\mu)$ (21.1.4). It remains to show that, for each nondegenerate representation $V$ of $L^1_c(G)$ on $E$, there exists a continuous unitary representation $U$ of $G$ on $E$ such that $V = U_{\text{ext}}$. Let $H$ be the vector subspace of $E$ spanned by the vectors $V(f) \cdot x$, where $f \in \mathcal{L}^1_c(G)$ and $x \in E$; then the hypothesis on $V$ signifies that
H is dense in $E$. Let $s \in G$, and define the sequence of functions $(u_n)$ as in the proof of (21.1.6); then for each $f \in \mathcal{L}^1_c(G)$ we have (14.11.1)

$$\lim_{n \to \infty} N_1(u_n \ast f - \varepsilon_s \ast f) = 0$$

and consequently (21.1.5.1)

$$\lim_{n \to \infty} \| V(u_n) V(f) - V(\varepsilon_s \ast f) \| = 0.$$ 

This shows that for each $y \in H$, i.e., each linear combination $\sum_k V(f_k) \cdot x_k$, the sequence $(V(u_n) \cdot y)$ has a limit in $E$, namely, $\sum_k V(\varepsilon_s \ast f_k) \cdot x_k$. Let $U(s) \cdot y$ denote this limit. It is clear that the mapping $U(s): H \to E$ so defined is linear and such that for each $f \in \mathcal{L}^1_c(G)$ we have

(21.1.7.1) 

$$U(s) \circ V(f) = V(\varepsilon_s \ast f),$$

which shows also that $U(s)$ maps $H$ into itself.

Also, by (21.1.5.1), we have $\| V(u_n) \| \leq N_1(u_n) = 1$ for all $n$, and therefore $\| U(s) \cdot y \| \leq \| y \|$ for all $y \in H$; hence $U(s)$ extends uniquely to a continuous operator on $E$, which we denote also by $U(s)$. Clearly we have $\| U(s) \| \leq 1$. We have to show that $s \mapsto U(s)$ is a continuous unitary representation of $G$ on $E$. If $s, t \in G$, then by virtue of (21.1.7.1) we have

$$U(st) \circ V(f) = V(\varepsilon_{st} \ast f) = V(\varepsilon_s \ast (\varepsilon_t \ast f))$$

$$= U(s) \circ V(\varepsilon_s \ast f) = U(s) \circ U(t) \circ V(f),$$

from which it follows immediately that $U(st) \cdot y = U(s) \cdot (U(t) \cdot y)$ for all $y \in H$ and hence, by continuity, $U(st) = U(s)U(t)$ in $\mathcal{L}(E)$. Next, it follows from (21.1.7.1) that $U(e)$ is equal to the identity mapping on $H$, and therefore also on $E$. Finally, since $\| U(s) \cdot x \| \leq \| x \|$ and $\| U(s^{-1}) \cdot x \| \leq \| x \|$, we have also $\| x \| \leq \| U(s) \cdot x \|$ and therefore $\| U(s) \cdot x \| = \| x \|$ for all $x \in E$, so that $U(s)$ is a unitary operator.

It remains to show that $V = U_{\text{ext}} \cdot$. Let $f, g \in \mathcal{L}^1_c(G)$; from the definition of convolution and the Lebesgue–Fubini theorem it follows that for each $h \in \mathcal{L}^{\infty}_c(G)$ we have

(21.1.7.2) 

$$\langle h, f \ast g \rangle = \int f(s) \langle h, \varepsilon_s \ast g \rangle \, d\beta(s).$$

For each pair of vectors $x, y \in E$, the function $f \mapsto (V(f) \cdot x \, | \, y)$ is a continuous linear form on $\mathcal{L}^1_c(G)$, hence is of the form $f \mapsto \langle h, f \rangle$ for some $h \in \mathcal{L}^{\infty}_c(G)$ (13.17.1). Hence, by virtue of (21.1.7.2), we may write
1. UNITARY REPRESENTATIONS OF LOCALLY COMPACT GROUPS

(21.1.8) The study of the continuous unitary representations of a unimodular group $G$ is therefore entirely equivalent to that of the nondegenerate representations of $L^1(G)$. Hence we may transfer to the former all the terminology introduced in (15.5) for the latter. In particular, two continuous unitary representations $U_1, U_2$ of $G$ on spaces $E_1, E_2$ are said to be equivalent if there exists an isomorphism $T$ of the Hilbert space $E_1$ onto the Hilbert space $E_2$ such that $U_2(s) = TU_1(s)T^{-1}$ for all $s \in G$. This is equivalent to saying that $U_2(f) = TU_1(f)T^{-1}$ for all functions $f \in L^1(G)$: in other words, $(U_1)_{\text{ext}}$ and $(U_2)_{\text{ext}}$ are equivalent in the sense of (15.5). To say that $U$ is irreducible is equivalent to saying, by virtue of (21.1.7), that $U_{\text{ext}}$ is topologically irreducible. Finally, if $E$ is the Hilbert sum of a sequence $(F_n)$ of closed subspaces stable under $U$, then $U$ is said to be the Hilbert sum of the subrepresentations corresponding to the $F_n$.

(21.1.9) Example. Suppose that $G$ is unimodular. For each $s \in G$ and each $f \in L^2(G)$, the function $\gamma(s)f = \varepsilon_s \ast f$ (14.8.5) belongs to $L^2(G)$, and we have $N_2(\varepsilon_s \ast f) = N_2(f)$. Hence we may define a unitary operator $R(s)$ on $L^2(G)$ by mapping the class of $f$ to the class of $\varepsilon_s \ast f$. Further, it follows from (14.10.6.3) that $s \mapsto R(s)$ is a continuous unitary representation of $G$ on $L^2(G)$. This representation is called the regular (or left regular) representation of $G$. It follows from (14.9.2) that for each bounded measure $\mu$ on $G$ we have $R(\mu) \cdot \tilde{g} = (\mu \ast g)^-$ for all $g \in L^2(G)$, and in particular that $R(f) \cdot \tilde{g} = (f \ast g)^-$ for all $f \in L^1(G)$. The representation $R_{\text{ext}}$ is called the regular (or left regular) representation of $L^1(G)$ on $L^2(G)$. It is injective, because it follows immediately from regularization (14.11.1) that if $f \ast g$ is negligible for all functions $g \in L^2(G)$, then $f$ is negligible.

(21.1.10) Let $E_1, E_2$ be two Hausdorff topological vector spaces over $\mathbb{C}$, and let $U_1, U_2$ be continuous linear representations of $G$ on $E_1, E_2$, respectively (21.1.1). Generalizing the terminology of (21.1.8), we say that $U_1$ and $U_2$ are equivalent if there exists an isomorphism $T : E_1 \to E_2$ of topological
vector spaces such that \( U_2(s) = TU_1(s)T^{-1} \) for all \( s \in G \). When \( E_1, E_2 \) are Hilbert spaces and \( U_1, U_2 \) are continuous unitary representations, it can be shown that this definition is equivalent to that given in (21.1.8) (Problem 4).

The **direct sum** of two arbitrary continuous linear representations \( U_1, U_2 \) of \( G \) is defined to be the continuous linear representation \( U \) of \( G \) on \( E_1 \times E_2 \) defined by \( U(s) \cdot (x_1, x_2) = (U_1(s) \cdot x_1, U_2(s) \cdot x_2) \). If \( E_1 \) and \( E_2 \) are finite-dimensional and \( U_1(s), U_2(s) \) are identified with their matrices relative to (arbitrary) bases of \( E_1, E_2 \), respectively, then \( U(s) \) is identified with the matrix \( \begin{pmatrix} U_1(s) & 0 \\ 0 & U_2(s) \end{pmatrix} \), and we write \( U = U_1 \oplus U_2 \). The direct sum of a finite number of continuous linear representations of \( G \) is defined in the same way. A continuous linear representation of \( G \) on a finite-dimensional space is said to be **completely reducible** if it is equivalent to a direct sum of irreducible representations.

**PROBLEMS**

1. Let \( E \) be a normed space, \( G \) a (separable, metrizable) locally compact group, and \( s \mapsto U(s) \) a mapping of \( G \) into the group \( \text{GL}(E) \) such that \( U(st) = U(s)U(t) \) for all \( s, t \in G \). Let \( A \) be a dense subset of \( E \) such that for each \( x \in A \) the mapping \( s \mapsto U(s) \cdot x \) is continuous on \( G \).
   
   (a) Show that the function \( s \mapsto \|U(s)\| \) is lower semicontinuous on \( G \) and that
   
   \[ \|U(st)\| \leq \|U(s)\| \cdot \|U(t)\| \]
   
   for all \( s, t \in G \).
   
   (b) Deduce from (a) that for each compact subset \( K \) of \( G \) the set \( \{ U(s) : s \in K \} \) is equicontinuous on \( E \) (use (12.16.2)). Deduce that the mapping \( (s, x) \mapsto U(s) \cdot x \) of \( G \times E \) into \( E \) is continuous.

2. Let \( E \) be a separable normed space and \( D \) a denumerable dense subset of \( E \); let \( G \) be a locally compact group and let \( s \mapsto U(s) \) be a mapping of \( G \) into \( \text{GL}(E) \) such that \( U(st) = U(s)U(t) \) for all \( s, t \in G \). Suppose also that for each \( x \in D \) the mapping \( s \mapsto U(s) \cdot x \) of \( G \) into \( E \) is **measurable** (relative to a Haar measure on \( G \)).

   Let \( V \) be a symmetric compact neighborhood of \( e \) in \( G \). Show that there exists a compact subset \( K \) of \( V \), with measure arbitrarily close to that of \( V \), such that the mapping \( s \mapsto \|U(s)\| \) is lower semicontinuous on \( K \) (13.9.5). Deduce that this mapping is bounded on \( K \) (same method as in Problem 1). Show, by using (14.10.8), that there exists a neighborhood \( W \subseteq V \) of \( e \) in \( G \) such that the mapping \( s \mapsto \|U(s)\| \) is bounded on \( W \), and deduce that the mapping \( (s, x) \mapsto U(s) \cdot x \) of \( G \times E \) into \( E \) is continuous.

3. Let \( G \) be an infinite (metrizable) compact group, endowed with normalized Haar measure. Show that for each \( s \neq e \) in \( G \) there exists a function \( f \in \mathcal{S}^2_G \) such that \( N_2(f) = 1 \) and \( N_2(y(s)f - f) = \sqrt{2} \). Deduce that the regular representation \( s \mapsto R(s) \) of \( G \) on \( L^2_G \) is not a continuous mapping of \( G \) into the Banach algebra \( \mathcal{S}(L^2_G) \).
4. Let $G$ be a locally compact group, let $E_1$ and $E_2$ be separable complex Hilbert spaces, $U_1$ and $U_2$ continuous unitary representations of $G$ on $E_1$, $E_2$, respectively, and let $T: E_1 \rightarrow E_2$ be an isomorphism of topological vector spaces such that $U_2(s) = TU_1(s)T^{-1}$ for all $s \in G$.

(a) There exists an isomorphism $T^*: E_2 \rightarrow E_1$ of topological vector spaces such that $(T^* \cdot x_1, x_2) = (x_1, T^* \cdot x_2)$ for all $x_1 \in E_1$ and $x_2 \in E_2$. ($T^*$ is the adjoint of $T$; cf. Section 15.12, Problem 1.) The operator $T^* \circ T$ on $E_1$ is self-adjoint, positive, and invertible, and there exists a unique self-adjoint positive invertible operator $A$ such that $A^2 = T^* \circ T$ (15.11.12). Show that $A^2U_1(s) = U_1(s)A^2$ for all $s \in G$, and deduce that $AU_1(s) = U_1(s)A$ for all $s \in G$. (Use the approximation of $t^{1/2}$ by polynomials, together with (15.11.8.1).)

(b) Show that $T \circ A^{-1} = S: E_1 \rightarrow E_2$ is an isomorphism of Hilbert spaces, such that $U_2(s) = SU_1(s)S^{-1}$ for all $s \in G$.

5. (a) Let $E$ be a separable Hilbert space and $A$ an unbounded self-adjoint operator on $E$. If $U$ is a unitary operator on $E$ that leaves $\text{dom}(A)$ stable and is such that $U \cdot (A \cdot x) = A \cdot (U \cdot x)$ for all $x \in \text{dom}(A)$, show that $U(\text{dom}(A)) = \text{dom}(A)$, and that for each bounded, uniformly measurable function $f$ on $\mathbb{R}$, the operator $U$ commutes with the continuous self-adjoint operator $f(A)$ (notation of (15.12.13)). In particular, if $A$ is not a homothety, there exists a closed vector subspace $F$ of $E$, other than $E$ and $[0]$, which is stable under $U$.

(b) Let $G$ be a locally compact group and let $s \mapsto U(s)$ be an irreducible continuous unitary representation of $G$ on $E$. Show that if $A$ is an unbounded self-adjoint operator on $E$, such that $\text{dom}(A)$ is stable under the representation $U$ and such that $U(s) \cdot (A \cdot x) = A \cdot (U(s) \cdot x)$ for all $s \in G$ and all $x \in \text{dom}(A)$, then $A$ is necessarily a homothety. (This is the topological version of Schur's lemma.)

6. Let $G$ be a locally compact group and let $U_1$, $U_2$ be continuous unitary representations of $G$ on separable Hilbert spaces $E_1$, $E_2$, respectively. A continuous linear mapping $T: E_1 \rightarrow E_2$ is an intertwining operator for $U_1$ and $U_2$ if $TU_1(s) = U_2(s)T$ for all $s \in G$. Then $T^*$ (Problem 4) is an intertwining operator for $U_2$ and $U_1$.

Suppose that $U_1$ is irreducible. Suppose also that there exists a nonzero unbounded closed operator $T$ from $E_1$ to $E_2$ (Section 15.12, Problem 1) such that $\text{dom}(T)$ is dense in $E_1$ and stable under $U_1$, and such that $T \cdot (U_1(s) \cdot x) = U_2(s) \cdot (T \cdot x)$ for all $x \in \text{dom}(T)$ and all $s \in G$. Show that $\text{dom}(T^*)$ is dense in $E_2$ and stable under $U_2$, that $\text{dom}(T^*T)$ is dense in $E_1$ and stable under $U_1$, and that $T^*T$ is self-adjoint. (Consider the Hilbert sum of $E_1$ and $E_2$, and the operator $S$ defined on $\text{dom}(T) \oplus E_2$, which is equal to $T$ on $\text{dom}(T)$ and zero on $E_2$.) Deduc from Problem 5 that there exists a constant $c \neq 0$ such that $T^*T = cI$, and hence that $\text{dom}(T) = E_1$ and that $T$ is an isometry of $E_1$ onto a closed subspace of $E_2$. Hence $U_1$ is equivalent to a subrepresentation of $U_2$.

7. Let $E$ be a finite-dimensional real vector space. If $G$ is a topological group, a continuous (real) linear representation of $G$ on $E$ is any continuous homomorphism of $G$ into $\text{GL}(E)$.

(a) Let $F = E_{(c)}$ be the complex vector space obtained from $E$ by extension of scalars; identify $E$ with the (real) subspace of $F$ consisting of all $x \otimes 1$ with $x \in E$. Then every $z \in F$ is uniquely of the form $z = x + iy$ where $x, y \in E$. Define a mapping $J: F \rightarrow F$ by $J \cdot (x + iy) = x - iy$, where $x, y \in E$; then $J$ is a semilinear bijection, and $J^2 = 1$; also $E$ is the set of $z \in F$ such that $J \cdot z = z$. If $s \mapsto U(s)$ is a continuous (real) linear representation of $G$ on $E$, the mapping $s \mapsto V(s) = U(s) \otimes 1_E$ is a continuous linear representation of $G$ on $F$, such that $V(s) \cdot J = J \cdot V(s)$ for all $s \in G$. 


12 **XXI COMPACT LIE GROUPS AND SEMISIMPLE LIE GROUPS**

(b) Conversely, let $F$ be a finite-dimensional complex vector space, and let $J$ be a semilinear bijection of $F$ onto $F$ such that $J^2 = I$. If $F_{1\mathbb{R}}$ is the real vector space obtained from $F$ by restriction of scalars, then $J$ is an involutory automorphism of $F_{1\mathbb{R}}$. If $E$ is the eigenspace of this automorphism for the eigenvalue $1$, then $iE$ is the eigenspace for the eigenvalue $-1$, and consequently $F$ may be identified with $E_{(i)}$. Show that if $s \mapsto V(s)$ is a continuous linear representation of $G$ on $F$ such that $V(s) \cdot J = J \cdot V(s)$ for all $s \in G$, then there exists a continuous (real) linear representation $U$ of $G$ on $E$ such that $V$ may be identified with $s \mapsto U(s) \otimes 1_E$.

8. Let $F$ be a finite-dimensional left vector space over $H$, the division ring of quaternions. If $G$ is any topological group, a **continuous (quaternionic) linear representation** of $G$ on $F$ is any continuous homomorphism of $G$ into $GL(F)$.

(a) Identify the quaternions of the form $a + bi$ ($a, b \in \mathbb{R}$) with complex numbers, so that every quaternion $a + bi + cj + dk$ is expressed as $(a + bi) + (c + di)$, and $H = \mathbb{C} \oplus \mathbb{C}$ is a left vector space of dimension 2 over $\mathbb{C}$. Let $E = F_{1\mathbb{C}}$ be the complex vector space obtained from $F$ by restriction of scalars. If we define $J \cdot z = jz$ for each vector $z \in E$, then we have $J \cdot (\lambda z) = J(\lambda \cdot z)$ for all $\lambda \in \mathbb{C}$, so that $J$ is a semilinear bijection of $E$ onto $E$ such that $J^2 = -I$. A quaternionic continuous linear representation $s \mapsto U(s)$ of $G$ on $F$ can be considered as a continuous linear representation of $G$ on $E$, and we have $U(s) \cdot J = J \cdot U(s)$ for all $s \in G$.

(b) Conversely, let $E$ be a finite-dimensional complex vector space, and let $J$ be a semilinear bijection of $E$ onto $E$ such that $J^2 = -I$. For each vector $z \in E$ and each quaternion $\lambda + \mu j$ (where $\lambda, \mu \in \mathbb{C}$), put $(\lambda + \mu j)z = \lambda z + \mu (J \cdot z)$. This defines on $E$ a structure of left vector space over $H$ such that if $F$ denotes this left vector space then $E = F_{1\mathbb{C}}$. If $U$ is a continuous linear representation of $G$ on $E$ such that $U(s) \cdot J = J \cdot U(s)$ for all $s \in G$, then $U$ can be regarded as a quaternionic continuous linear representation of $G$ on $F$.

9. For finite-dimensional real (resp. quaternionic) continuous linear representations of a topological group $G$, the notions of equivalent representations, direct sum of representations, and irreducible representations are defined exactly as in (21.1.1) and (21.1.10), by replacing the field $\mathbb{C}$ by $\mathbb{R}$ (resp. $\mathbb{H}$) throughout. If $U$ is a continuous linear representation of $G$ on a finite-dimensional complex vector space, satisfying the condition of Problem 7(b) (resp. 8(b)), we denote by $U^{(\mathbb{R})}$ (resp. $U^{(\mathbb{H})}$) the corresponding real (resp. quaternionic) linear representation.

(a) Let $U, V$ be two equivalent complex linear representations of $G$, so that if $E, F$ are the respective spaces of the representations $U, V$, there exists a linear bijection $T$ of $E$ onto $F$ such that $V(s) = TU(s)T^{-1}$ for all $s \in G$. Suppose that there exists a semilinear bijection $J_E$ (resp. $J_F$) of $E$ (resp. $F$) onto itself such that $J_E^2 = \varepsilon I_E$ and $J_F^2 = \varepsilon I_F$ (where $\varepsilon = \pm 1$) and $U(s)J_E = J_F U(s)$, $V(s)J_F = J_E V(s)$ for all $s \in G$. Show that there exists a linear bijection $S$ of $E$ onto $F$ such that $V(s) = SU(s)S^{-1}$ for all $s \in G$ and also $S J_E = J_F S$. (Put $T = \frac{1}{2}(T + J_F T J_E^{-1})$, $T'' = \frac{1}{2i}(T - J_F T J_E^{-1})$, and show that there exists a real number $\xi$ such that $T' + \xi T''$ is a bijection.) Deduce that if $\varepsilon = 1$, the representations $U^{(\mathbb{R})}$ and $V^{(\mathbb{R})}$ are equivalent, and that if $\varepsilon = -1$ the representations $U^{(\mathbb{H})}$ and $V^{(\mathbb{H})}$ are equivalent.

(b) Let $U$ be a complex linear representation of $G$ on a (finite-dimensional) complex vector space $E$, and identify each automorphism $U(s)$ with its matrix relative to a fixed basis of $E$. In order that $U$ should satisfy the condition of Problem 7(b) (resp. 8(b)), it is necessary and sufficient that there should exist an invertible complex matrix $P$ such that...
1. UNITARY REPRESENTATIONS OF LOCALLY COMPACT GROUPS

\[ U(s) = P\overline{U(s)}P^{-1} \text{ for all } s \in G, \text{ and such that } PP = PP = 1 \text{ (resp. } -I). \]  (For any complex matrix \( A = (a_{ij}) \), \( \overline{A} \) denotes the complex conjugate matrix \( (\overline{a_{ij}}) \).) In particular, the representation \( U \) is equivalent to the complex conjugate representation \( s \mapsto U(s) \) (denoted by \( \overline{U} \)).

(c) Conversely, let \( U \) be an irreducible complex linear representation of \( G \) on \( E \) that is equivalent to its complex conjugate. Then \( U \) satisfies one and only one of the conditions of Problems 7(b) and 8(b); in other words, one of the representations \( U^R, U^H \) is defined, but not the other. (Use (b) and Schur's lemma (A.22.4).) Moreover, whichever of the representations \( U^R, U^H \) is defined is irreducible.

10. (a) Let \( U \) be a complex linear representation of \( G \) on a finite-dimensional vector space \( E \). For each \( s \in G, U(s) \) is also an automorphism of the real vector space \( E_{\mathbb{R}} \) obtained from \( E \) by restriction of scalars; let \( U_{\mathbb{R}} \) denote the real linear representation so defined. Show that the complex linear representation \( s \mapsto U_{\mathbb{R}}(s) \otimes 1_c \) is equivalent to the direct sum of the representation \( U \) and its conjugate \( \overline{U} \).

(b) Deduce from (a) that if \( U \) is irreducible and not equivalent to its conjugate \( \overline{U} \), then \( U_{\mathbb{R}} \) is irreducible.

(c) Suppose that \( U \) satisfies the condition of Problem 8(b), so that the quaternionic linear representation \( U^H \) is defined. Show that if \( U \) is irreducible, then so also is \( U_{\mathbb{R}} \). (Use (a) and observe that if \( V \) is an irreducible real linear representation, then \( W = V \otimes 1_c \) is irreducible, and \( W^H \) is not defined.)

(d) If \( V_1, V_2 \) are inequivalent irreducible real linear representations of \( G \), show that there exists no irreducible complex linear representation that is equivalent to a subrepresentation of \( s \mapsto V_1(s) \otimes 1_c \) and also to a subrepresentation of \( s \mapsto V_2(s) \otimes 1_c \). (Use Schur's lemma (A.22.4).)

(e) Deduce from above that the finite-dimensional irreducible real linear representations of \( G \) are all obtained (up to equivalence) from the finite-dimensional irreducible complex linear representations \( U \) of \( G \), by taking \( U^R \) whenever this is defined, and otherwise taking \( U_{\mathbb{R}} \). Furthermore, if the irreducible complex representations considered are pairwise inequivalent, then the same is true of the irreducible real representations obtained from them.

(f) State and prove the analogous results for irreducible quaternionic linear representations.

11. Let \( U, V \) be two finite-dimensional continuous complex linear representations of \( G \), and let \( W(s) = U(s) \otimes V(s) \) (A.10.5). If the representations \( U^R \) and \( V^R \) (resp. \( U^H \) and \( V^H \)) are defined, then \( W^R \) is defined; and if \( U^R \) and \( V^H \) are defined, then \( W^H \) is defined. State and prove the analogous results for the representations \( s \mapsto \bigwedge^p U(s) \) (A.13.4), and the representations \( s \mapsto S^p U(s) \) defined by symmetric powers (A.17). If \( U^R \) (resp. \( U^H \)) is defined, then we have \( (U^R)^{-1} = (U^{-1})^R \) (resp. \( (U^H)^{-1} = (U^{-1})^H \)).

12. Let \( G \) and \( H \) be two topological groups and let \( (s, t) \mapsto U((s, t)) \) be a continuous linear representation of \( G \times H \) on a finite-dimensional complex vector space \( E \). Suppose that \( U \) is irreducible and that the representations \( s \mapsto U((s, e')) \) and \( t \mapsto U((e, t)) \) of \( G \) and \( H \), respectively, on \( E \) are completely reducible (\( e, e' \) being the identity elements of \( G, H \), respectively). Show that there exists an irreducible representation \( V \) of \( G \) and an irreducible representation \( W \) of \( H \) such that \( U \) is equivalent to the representation \( (s, t) \mapsto V(s) \otimes W(t) \).

(Use Schur's lemma.)
13. Let $G$ be a separable, metrizable, locally compact group and let $\Delta$ be its modulus $(14.3)$. If $\beta$ is a left Haar measure on $G$ and if for each function $f \in L^2_c(G)$ we put $f^* = f \cdot \Delta^{-1}$, show that the transform of the measure $f \cdot \beta$ under the involution $\mu \mapsto \hat{\mu}$ of $M^1_c(G)$ is $f^* \cdot \beta$.

Extend the results of Section 21.1 to nonunimodular locally compact groups.

2. THE HILBERT ALGEBRA OF A COMPACT GROUP

(21.2.1) In this section, $G$ denotes a (metrizable) compact group and $\beta$ the Haar measure on $G$ with total mass 1 (we recall that compact groups are unimodular $(14.3.3)$). If $f, g \in L^2_c(G)$, the function $f \ast g$ is continuous on $G$ and satisfies

\[(21.2.1.1) \quad \| f \ast g \| \leq N_2(f)N_2(g) \]

by virtue of $(14.10.7)$. It follows that

\[(21.2.1.2) \quad N_2(f \ast g) \leq N_2(f)N_2(g), \]

so that $L^2_c(G)$ is a separable Banach algebra with respect to convolution and its Hilbert space structure. Also we have $N_2(f^*) = N_2(f)$ since $G$ is unimodular, and therefore $L^2_c(G)$ is a Banach algebra with involution. In fact, it is a Hilbert algebra $(15.7.5)$, relative to the scalar product in $L^2_c(G)$. For the condition $(15.7.5.1)$ follows immediately from the definition of the involution and of the scalar product, having regard to $(14.3.4)$; and $(15.7.5.3)$ follows from $(21.2.1.2)$. The condition $(15.7.5.4)$ is a consequence of regularization $(14.11.1)$. Finally, condition $(15.7.5.2)$ takes the form

\[(21.2.1.3) \quad \langle f \ast g, h \rangle = \langle g, f^* \ast h \rangle \]

for all $f, g, h \in L^2_c(G)$; when $g$ is continuous, this formula is a special case of $(14.9.4.1)$, and for arbitrary $g$ the result follows by continuity, because of $(13.11.6)$ and $(21.2.1.2)$.

(21.2.2) A function $h \in L^2_c(G)$ is said to be central if its class in $L^2_c(G)$ belongs to the center of this algebra. This signifies that for all functions $f \in L^2_c(G)$, the functions $f \ast h$ and $h \ast f$ are equal almost everywhere; but they are continuous functions, and therefore they are equal (since $\beta$ has support $G (14.1.2)$). In other words, for all $s \in G$ we must have

\[ \int_G f(t^{-1})(h(st) - h(ts)) \, d\beta(t) = 0. \]
This is possible only if \( h(st) = h(ts) \) for all \( t \) in the complement of a negligible set (depending on \( s \)) (13.14.4); if in addition \( h \) is \textit{continuous}, then this negligible set is necessarily empty, again because the support of \( \beta \) is the whole of \( G \) (14.1.2). Hence the \textit{continuous central functions on} \( G \) are the \textit{continuous functions} \( h \) which satisfy

\[(21.2.2.1) \quad h(sts^{-1}) = h(t) \quad \text{for all} \quad s, t \in G.\]

We remark that the classes of these functions belong also to the \textit{center} of \( M_c(G) \); this follows immediately from (14.8.2) and (14.8.4).

\[(21.2.3) \quad \text{(Peter-Weyl theorem)} \quad \text{Let} \ G \text{ be a metrizable compact group. The complete Hilbert algebra} \ L_c^2(G) \text{ is the Hilbert sum of an at most denumerable family} \ (a_\rho)_{\rho \in \mathbb{R}} \text{ of finite-dimensional simple algebras; each} \ a_\rho \text{ is isomorphic to a matrix algebra} \ M_{n_\rho}(\mathbb{C}) \text{ and is a minimal two-sided ideal in} \ L_c^2(G). \text{The elements of} \ a_\rho \text{ are classes of continuous functions on} \ G; \text{the identity element of} \ a_\rho \text{ is the class of a continuous function} \ u_\rho \text{ such that} \ u_\rho^2 = u_\rho; \text{and the orthogonal projection of} \ L_c^2(G) \text{ onto} \ a_\rho \text{ (6.3.1) maps the class of a function} \ f \text{ to the class of} \ f \ast u_\rho = u_\rho \ast f. \text{Consequently, for all} \ f \in L_c^2(G) \text{ we have}

\[(21.2.3.1) \quad f = \sum_{\rho \in \mathbb{R}} (f \ast u_\rho)^\sim,

\text{the right-hand side being a convergent series in} \ L_c^2(G), \text{regardless of the way in which the elements of} \ \mathbb{R} \text{ are arranged as a sequence.}

Since \( L_c^2(G) \) is \textit{complete}, it is the Hilbert sum of an at most denumerable family \( (a_\rho)_{\rho \in \mathbb{R}} \) of distinct two-sided ideals that are topologically simple Hilbert algebras and annihilate each other in pairs (15.8.13). Everything therefore reduces to proving that each \( a_\rho \) is \textit{finite-dimensional}. For each \( a_\rho \) will then be the Hilbert sum of a finite number of minimal left ideals, each of which is generated by an irreducible self-adjoint idempotent, and the sum of these idempotents will be the identity element of the algebra \( a_\rho \). If \( v \) is a function whose class is this identity element, every element of \( a_\rho \) will be the class of a function of the form \( f \ast v \), hence \textit{continuous} (21.2.1). The remaining assertions of the theorem then follow from (15.8.11).

In view of (15.8.15), it will be enough to prove the following assertion:

\[(21.2.3.2) \quad \text{Each closed two-sided ideal} \ b \neq \{0\} \text{ in} \ L_c^2(G) \text{ contains a nonzero element of the center of} \ L_c^2(G).\]
We shall use the following remark:

(21.2.3.3) For a closed vector subspace \( b \) of \( L^2_c(G) \), the following conditions are equivalent:

(a) \( b \) is a left ideal in \( L^2_c(G) \);
(b) \( b \) is stable under the regular representation of \( L^2_c(G) \) on \( L^2_c(G) \) (21.1.9);
(c) for each function \( f \) whose class is in \( b \), and each \( s \in G \), the class of \( \varepsilon_s * f = \gamma(s) f \) lies in \( b \).

The equivalence of (b) and (c) is a particular case of (21.1.7), applied to the regular representation. It is clear that (b) implies (a); on the other hand, \( L^2_c(G) \) is dense in \( L^1_c(G) \) (13.11.6) and the mapping \( f \mapsto f * g \) of \( L^1_c(G) \) into \( L^2_c(G) \) is continuous for all \( g \in L^2_c(G) \) (14.10.6), whence (a) implies (b).

There is of course an analogous statement for right ideals in \( L^2_c(G) \).

We now come to the proof of (21.2.3.2). We shall first show that \( b \) contains the class of a continuous function \( f \), not identically zero. For if \( g \) is a nonnegligible function whose class belongs to \( b \), then the class of \( g * \check{g} \) also belongs to \( b \); but \( g * \check{g} \) is continuous (21.2.1) and \( (g * \check{g})(e) = (N_2(g))^2 > 0 \) (14.10.4). We may therefore take \( f = g * \check{g} \). Next consider the function

\[
(21.2.3.4) \quad h(t) = \int_G f(sts^{-1}) \, d\beta(s).
\]

Since the function \( (x, y, z) \mapsto f(xyz) \) is uniformly continuous on \( G \times G \times G \) (3.16.5), it follows immediately that \( h \) is continuous on \( G \), and since \( h(e) = f(e) \neq 0 \), \( h \) is not identically zero. For all \( x \in G \) we have

\[
(21.2.3.5) \quad h(xtx^{-1}) = \int_G f((sx)t(sx)^{-1}) \, d\beta(s)
\]

\[= h(t) \]

because \( \beta \) is right-invariant. It remains to show that the class of \( h \) belongs to \( b \). Now \( L^2_c(G) \) is the Hilbert sum of \( b \) and its orthogonal supplement \( b^\perp \),
which is also a two-sided ideal (15.8.2); hence it is enough to show that 
\((\hat{h} | \hat{w}) = 0 \) for all \( \hat{w} \in b^1 \). We have

\[
(\hat{h} | \hat{w}) = \int \hat{w}(t) \, d\beta(t) \int f(sts^{-1}) \, d\beta(s) \\
= \int d\beta(s) \int \hat{w}(t) f(sts^{-1}) \, d\beta(t) \\
= \int d\beta(s) \int \hat{w}(s^{-1}ts)f(t) \, d\beta(t)
\]

by the Lebesgue-Fubini theorem and the left- and right-invariance of \( \beta \).
Since \( \hat{w} \in b^1 \), the class of \( \varepsilon_\lambda * w * \varepsilon_{\lambda-1} \), also belongs to \( b^1 \) by virtue of (21.2.3.3), hence by definition we have \( \int \hat{w}(s^{-1}ts)f(t) \, d\beta(t) = 0 \), and the proof is complete.

(21.2.4) By virtue of (21.2.3) it is convenient to identify each element of an ideal \( a_\rho \) with the unique continuous function in the class, and this we shall do from now on.† For each \( \rho \in \mathbb{R} \), choose once and for all a decomposition of \( a_\rho \) as the Hilbert sum of \( n_\rho \) minimal left ideals \( l_j = a_\rho * m_j \) (also denoted by \( I^\rho_j \)), pairwise isomorphic and orthogonal, where each \( m_j \) \((1 \leq j \leq n_\rho)\) is a minimal self-adjoint idempotent, so that \( u_\rho = \sum_{j=1}^{n_\rho} m_j \). Also let \( (a_j)_{1 \leq j \leq n_\rho} \) be a Hilbert basis of \( l_1 \), such that \( a_j \in m_j * a_\rho * m_j \). Then from (15.8.14) we know that all the numbers \( (m_j | m_j) \) are equal to the same number \( \gamma > 0 \), and that

\[
a_j * \tilde{a}_j = \gamma m_j, \quad \tilde{a}_j * a_j = \gamma m_1.
\]

Now put, for each pair of indices \( j, k \),

\[
m_{jk} = \gamma^{-1} a_j * \tilde{a}_k
\]

(so that \( m_{jj} = m_j \)); then we have

(21.2.4.1) \[
m_{jk} * a_h = \delta_{kh} a_j
\]

where \( \delta_{kh} \) is the Kronecker delta. We shall also write \( m_{ij}^{(\rho)} \) in place of \( m_{ij} \).

† More generally, from now on we shall identify each continuous function \( f \) on a locally compact group \( G \), belonging to one or other of the spaces \( L^1(L^2)(G, \beta), L^2(L^2)(G, \beta), L^\infty(G, \beta) \) (where \( \beta \) is a left or right Haar measure on \( G \)), with its class in the corresponding space \( L^1(L^2)(G, \beta), L^2(L^2)(G, \beta), L^\infty(G, \beta) \). This can cause no confusion because \( f \) is the only continuous function in its class, since the support of \( \beta \) is the whole of \( G \).
With the notation of (21.2.4):

(a) For each index $j$, the $m_{ij}$ ($1 \leq i \leq n_p$) form an orthogonal basis of $l_j$.

(b) $m_{ij} = \delta_{ij}$, $m_{ij} \ast m_{ik} = \delta_{jk} m_{ik}$.

(c) $(m_{ij} | m_{ij}) = n_p$, $m_{ij}(e) = n_p \delta_{ij}$ for all pairs $(i, j)$ (so that $\gamma = n_p^{-1}$). The functions $n_p^{-1/2} m_{ij}^\rho (1 \leq i, j \leq n_p, \rho \in \mathbb{R})$ therefore form a Hilbert basis (6.5) of the Hilbert space $L^2_c(G)$.

(d) Let $M_\rho(s) = (n_p^{-1} m_{ij}(s))$ for all $s \in G$; then the matrices $M_\rho(s)$ satisfy the relations

(21.2.5.1) $M_\rho(st) = M_\rho(s) M_\rho(t)$, \quad $M_\rho(s^{-1}) = (M_\rho(s))^*$,

so that $s \mapsto M_\rho(s)$ is a continuous unitary representation of $G$ on $C^n_*$, relative to the Hermitian scalar product $\sum_j \xi_j \bar{\eta}_j$.

The assertions in (a) and (b) are immediate consequences of the definitions in (21.2.4), since the $a_j \in l_1$ and the $m_j$ are pairwise orthogonal. Since $a_\rho$ is a Hilbert algebra, we have

$$(m_{ij} | m_{ij}) = \gamma^{-2} (a_i \ast \bar{a}_j | a_i \ast \bar{a}_j) = \gamma^{-2} (\bar{a}_i \ast a_i | \bar{a}_j \ast a_j) = (m_1 | m_1).$$

To calculate this number we remark that for each index $k$ the function $t \mapsto m_{ik}(st)$ belongs to $l_k$ for each $s \in G$ (21.2.3.3) and can therefore be written in the form

(21.2.5.2) $m_{ik}(st) = \sum_{j=1}^{n_p} c_{ij}(s) m_{jk}(t)$.

On the other hand,

$$m_{jk}(t) = (m_{j1} \ast m_{1k})(t) = \int_G m_{j1}(tx) \overline{m_{k1}(x)} \, d\beta(x),$$

hence in particular $m_{jk}(e) = (m_{j1} | m_{1k})$, and by putting $t = e$ in (21.2.5.2) we obtain, using the orthogonality properties of the $m_{ij}$,

(21.2.5.3) $m_{ik}(s) = (m_1 | m_1) c_{ik}(s)$.

Next, putting $s = t^{-1}$ and $i = k = 1$ in (21.2.5.2), we obtain by use of (14.10.4)

$$(m_1 | m_1) = m_1(e) = \sum_{j=1}^{n_p} c_{1j}(s) \overline{m_{1j}(s)}.$$
and therefore, using (21.2.5.3)
\[ \sum_{j=1}^{n_{\rho}} m_{ij}(s)\overline{m_{ij}(s)} = (m_1 | m_1)^2. \]

Integrating over \( G \), we finally obtain
\[ (m_1 | m_1)^2 = n_{\rho}(m_1 | m_1) \]
which proves (c); and then the relations (21.2.5.1) follow immediately from (b) and (21.2.5.2) and (21.2.5.3).

(21.2.6) The center of the Hilbert algebra \( \mathbb{L}^2(c)(G) \) is the Hilbert sum of the 1-dimensional subspaces \( \mathbb{C} \rho_p \) \( (\rho \in \mathbb{R}) \). In particular, if \( G \) is commutative, all the ideals \( \alpha_p \) are of dimension \( n_{\rho} = 1 \).

That the \( u_{\rho} \) belong to the center of \( \mathbb{L}^2(c)(G) \) follows from the facts that \( u_{\rho} \) is the identity element of \( \alpha_{\rho} \) and that \( \alpha_{\rho} \ast \alpha_{\rho'} = [0] \) whenever \( \rho \neq \rho' \). Conversely, if the class \( f \) of a function \( f \) belongs to the center of \( \mathbb{L}^2(c)(G) \), then so also the class of \( f \ast u_{\rho} \in \alpha_{\rho} \), hence \( f \ast u_{\rho} = c_{\rho} u_{\rho} \) for some scalar \( c_{\rho} \in \mathbb{C} \); now apply the formula (21.2.3.1).

(21.2.7) The classes of the complex constant functions form a two-sided ideal of dimension 1 in \( \mathbb{L}^2(c)(G) \) (14.6.3), which is therefore of the form \( \alpha_{\rho_0} \). It is called the trivial ideal. The corresponding linear representation \( M_{\rho_0} \) of dimension 1 is such that \( M_{\rho_0}(s) = 1 \) for all \( s \in G \), that is to say, it is the trivial linear representation (21.1.1). For each \( \rho \neq \rho_0 \) in \( \mathbb{R} \), we have

\[ \int_G m_{ij}(p)(s) \, d\beta(s) = 0 \]
since the subspaces \( \alpha_{\rho} \) and \( \alpha_{\rho_0} \) are orthogonal.

(21.2.8) (i) If \( f \) and \( g \) are continuous complex-valued functions on \( G \), then

\[ f \ast g = \sum_{\rho \in \mathbb{R}} \left( \sum_{1 \leq i, j \leq n_{\rho}} n_{\rho}^{-1} (g \mid m_{ij}(\rho))(f \ast m_{ij}(\rho)) \right), \]
the series on the right being summable for the topology of uniform convergence.

(ii) The functions \( m_{ij}(\rho) \) \( (\rho \in \mathbb{R}, 1 \leq i, j \leq n_{\rho}) \) form a total system in the space of continuous functions on \( G \), for the topology of uniform convergence.
(i) Identifying continuous functions with their classes in $L^2_c(G)$, we may write
\[ g = \sum_{\rho \in \mathbb{R}, 1 \leq i, j \leq n} \frac{1}{n_{ij}^{\rho}} (m_{ij}^{\rho})^* m_{ij}^{\rho} \]
the series on the right being summable in $L^2_c(G)$, because the functions $n_{ij}^{\rho-1/2} m_{ij}^{\rho}$ form a Hilbert basis of this space. Now form the convolution product of both sides with $f$; since $u \mapsto f^\ast u$ is a continuous mapping of $L^2_c(G)$ into $\mathfrak{g}_c(G)$ (21.2.1.1), we obtain the formula (21.2.8.1).

(ii) It follows from regularization (14.11.1) that for each continuous function $g$ on $G$ there exists a continuous function $\tilde{f}$ on $G$ such that $\|f^\ast g - g\|$ is arbitrarily small. Now, for each $\rho \in \mathbb{R}$, the functions $f^\ast m_{ij}^{\rho}$ belong to $\mathfrak{g}_c(G)$, and therefore are linear combinations of the $m_{ij}^{\rho}$ (1 \leq h, k \leq n) with complex coefficients. This completes the proof.

PROBLEMS

1. Let $E$ be a finite-dimensional complex vector space, $E^*$ its dual, $G$ a topological group, and $U$ a continuous linear representation of $G$ on $E$. For each pair of vectors $x \in E$, $x^* \in E^*$, the function $s \mapsto \langle U(s) \cdot x, x^* \rangle$ is continuous on $G$; it is called the coefficient of $U$ relative to $(x, x^*)$ and is denoted by $c_{U}(x, x^*)$. For all $t \in G$ we have
\[ \gamma(t)c_{U}(x, x^*) = c_{U}(x, U(t)^{-1} \cdot x^*), \quad \delta(t)c_{U}(x, x^*) = c_{U}(U(t) \cdot x, x^*). \]
If we identify $U(s)$ with its matrix $(u_{jk}(s))$ relative to a fixed basis of $E$, then the functions $c_{U}(x, x^*)$ are linear combinations of the $u_{jk}$. We have
\[ c_{U^{-1}}(x^*, x) = c_{U}(x, x^*), \quad c_{U}(x, x^*) = c_{\tilde{U}}(x, x^*). \]

(a) Let $\mathfrak{g}_c(U)$ (or $\mathfrak{g}_{c,c}(U)$) denote the vector subspace of $\mathfrak{g}_c(G)$ spanned by the coefficients of the continuous linear representation $U$ of $G$. If $U_1$, $U_2$ are equivalent, then $\mathfrak{g}_c(U_1) = \mathfrak{g}_c(U_2)$; also $\mathfrak{g}_c(U^{-1}) = \mathfrak{g}_c(U)$ and $\mathfrak{g}_c(U_1) + \mathfrak{g}_c(U_2)$ and $\mathfrak{g}_c(U_1 \otimes U_2) = \mathfrak{g}_c(U_1) \mathfrak{g}_c(U_2)$, the vector subspace of $\mathfrak{g}_c(G)$ spanned by the products $c_1 c_2$, where $c_1 \in \mathfrak{g}_c(U_1)$ and $c_2 \in \mathfrak{g}_c(U_2)$. The vector subspace $\mathfrak{g}_c(U)$ has finite dimension $\leq (\dim U)^2$ and is stable under left and right translations $f \mapsto \gamma(s)f, f \mapsto \delta(s)f$ for all $s \in G$. Conversely, if $E$ is a vector subspace of $\mathfrak{g}_c(G)$ that is stable under left translations $f \mapsto \gamma(s)f$ and is finite-dimensional, and if we denote by $U(s)$ the endomorphism $f \mapsto \gamma(s)f$ of $E$, then $U$ is a continuous linear representation of $G$ on $E$, and $E \subset \mathfrak{g}_c(U)$. A function $f \in \mathfrak{g}_c(G)$ is called a representative function on $G$ if the vector subspace of $\mathfrak{g}_c(G)$ spanned by the left-translates $\gamma(s)f$ of $f$, for all $s \in G$, is finite-dimensional. The representative functions on $G$ form a subalgebra $\mathfrak{h}(G)$ (or $\mathfrak{h}_c(G)$) of $\mathfrak{g}_c(G)$, which is the same as the subalgebra generated by the coefficients of all the finite-dimensional continuous linear representations of $G$.

(b) Let $U$ be a continuous linear representation of $G$, of dimension $n < \infty$, and let $U'$ be the continuous linear representation of $G$ on $\mathfrak{g}_c(U)$ defined by $U'(s) \cdot f = \gamma(s)f$. Show that
2. THE HILBERT ALGEBRA OF A COMPACT GROUP

$U$ is equivalent to a subrepresentation of $U'$. If $U$ is irreducible, $U'$ is the direct sum of $n$ representations equivalent to $U$. Give an example of a reducible representation where this is not the case (cf. (21.1.3)). Deduce that if $U$ is irreducible and if $U_1$ is a finite-dimensional continuous linear representation such that $\gamma(U_1) \subset \gamma(U)$, then $U_1$ is the direct sum of $m$ representations equivalent to $U$, where $m \leq n$.

(c) Extend the above definitions and results to finite-dimensional continuous real linear representations (Section 21.1, Problem 7); in place of $\gamma_c(U)$ and $\mathscr{A}_c(G)$ we have $\gamma_r(U)$ and $\mathscr{A}_r(G)$.

2. Let $G$ be a metrizable compact group.

(a) Show that the algebra $\mathscr{A}_c(G)$ of complex representative functions is the direct sum of the two-sided ideals $a_p (p \in \mathbb{R})$, and that the algebra $\mathscr{A}_c(G)$ consists of the real and imaginary parts of the functions belonging to $\mathscr{A}_c(G)$.

(b) Let $M$ be a subset of $\mathscr{A}_c(G)$. The set $H$ of elements $t \in G$ such that $\delta(t)f = f$ for all $f \in M$ is a closed subgroup of $G$. Show that the set of functions $g \in \mathscr{A}_c(G)$ such that $\gamma(t)g = g$ for all $t \in H$ is the left ideal $b$ of $\mathscr{A}_c(G)$ generated by $M$. The functions belonging to $b$ may be canonically identified with continuous functions on $G/H$, and $b$ may be identified with the intersection of $\mathscr{A}_c(G)$ with $\mathcal{C}(G/H)$ (considered as a subalgebra of $\mathscr{A}_c(G)$); also $b$ is dense in $\mathcal{C}(G/H)$ (Use the Stone-Weierstrass theorem.)

(c) Let $K$ be a closed subgroup of $G$. Show that every function in $\mathcal{C}(K)$ is the restriction to $K$ of a function belonging to $\mathscr{A}_c(G)$. (Consider the set of functions in $\mathcal{C}(K)$ that are restrictions to $K$ of functions belonging to $\mathscr{A}_c(G)$ and use (a) above, with $G$ replaced by $K$.) If $b$ is the left ideal in $\mathscr{A}_c(G)$ that is the intersection of $\mathcal{C}(G)$ with $\mathcal{C}(G/K)$, show that $K$ is equal to the subgroup $H$ of elements $t \in G$ such that $\gamma(t)f = f$ for all $f \in b$. (Observe that a function belonging to $b$ that is constant on $K$ is constant on $H$.)

3. Let $G$ be an infinite compact group. With the notation of (21.2.3), if $p, q$ are two functions defined on $\mathbb{R}$, with values $> 0$, we write $p = o(q)$ to mean that for each $\epsilon > 0$ there exists a finite subset $J$ of $\mathbb{R}$ such that $p(p) \leq \epsilon q(p)$ for all $p \in \mathbb{R} - J$.

(a) Show that for each function $f \in \mathcal{L}_2^+(G)$, the operator $R(f)$ is a Hilbert-Schmidt operator on $L^2(G)$, and that the mapping $f \mapsto R(f)$ is an isometry of the Hilbert algebra $L_G^2$ onto a closed subalgebra of the Hilbert algebra $L^2(G)$ (15.4.8). In particular, for all $f, g \in \mathcal{L}_2^+(G)$, the operator $R(f)R(g)$ is nuclear (Section 15.11. Problem 7), and we have

$$\text{Tr}(R(f)R(g)) = \sum_{p \in R} \text{Tr}(R(f * g * u_p)) = (f | g).$$

(b) We have $\|R(f * u_p)\|_2 = N_2(f * u_p) = o(1)$ and $N_\alpha(f * u_p) = o(n_p)$ for all $f \in \mathcal{L}_2^+(G)$. (Use (a) above and the relation $f * u_p = f * u_{p + *}$.)

(c) Give an example of a continuous function on $G$ such that $R(f)$ is not nuclear. (Take $G = T$.)

(d) Show that $\|R(m_p^{(p)})\|_2 = 1$ and $\|R(m_p^{(p)})\|_1 = n_p$. (Observe that the eigenvalues of $R(m_p^{(p)}) \ast R(m_p^{(p)})$ are known.)

(e) Let $f \in \mathcal{L}_2^+(G)$. Show that $R(f)$ is a compact operator on $L^2(G)$ and that $\|R(f * u_p)\|_2 = o(1)$. (Use the fact that $L_G^2$ is dense in $L^2(G)$, the inequality (21.1.4.3), and (a) above.) Deduce that $\|R(f * u_p)\|_2 = N_2(f * u_p) = o(n_p)$ and that $N_\alpha(f * u_p) = o(n_p^\alpha)$.

4. Let $M$ be a compact differential manifold and $G$ a compact group acting continuously on $M$ such that, for each $s \in G$, the mapping $x \mapsto s \cdot x$ is a diffeomorphism of $M$. 

5. Let $M$ be a compact differential manifold and $G$ a compact Lie group acting differentiably on $M$; let $x$ be a point of $M$ and $S_x$ the stabilizer of $x$ in $G$.

(a) Show that there exists a submanifold $W$ of $M$, contained in a neighborhood of $x$ and containing $x$, which is stable under $S_x$ and which is such that $T_x(W)$ is a supplement in $T_x(M)$ to the tangent space $T_x(G \cdot x)$ to the orbit of $x$. (Use Problem 4 above, or Problem 6 of Section 19.1.)

(b) Let $V$ be a submanifold of $G$, passing through $e$ and such that the tangent space to $V$ at $e$ is supplementary in $g_e = T_e(G)$ to the Lie algebra $T_e(S_x)$ of $S_x$. Show that there exists a relatively compact open neighborhood $U$ of $e$ in $V$ and a relatively compact open neighborhood $K$ of $x$ in $W$ such that the mapping $(s, y) \mapsto s \cdot y$ of $U \times K$ into $M$ is a diffeomorphism onto a neighborhood of $x$ in $M$, and such that $K$ is stable under $S_x$. Deduce that $s \cdot K \cap K = \emptyset$ for all $s \in U$ not belonging to $S_x$.

(c) Deduce from (b) that there exists a relatively compact open neighborhood $K' \subset K$ of $x$ in $W$ having the following properties: (i) $K'$ is stable under $S_x$; (ii) the mapping $(s, y) \mapsto s \cdot y$ of $U \times K'$ into $M$ is a diffeomorphism onto a neighborhood of $x$ in $M$; (iii) $s \cdot K' \cap K' = \emptyset$ for $s \notin S_x$. (Use Problem 4.) Such a set $K'$ is called a slice of $M$ at the point $x$ (for the action of $G$ on $M$). Show that for all $z \in K'$ we have $S_z \subset S_x$.

6. If $M$ is a pure differential manifold and $G$ is a Lie group acting differentiably on $M$, let $L(G, M)$ denote the set of conjugacy classes in $G$ of the stabilizers of the points of $M$ (two stabilizers being in the same class if they stabilize two points of the same orbit). We shall show that, if $G$ and $M$ are compact, the set $L(G, M)$ is finite. The proof will be by induction on $\dim(M) = n$.

(a) Show that if the result is true for every differential manifold $M$ of dimension $n - 1$, then $L(G, \mathbb{R}^n)$ is finite for all compact subgroups $G$ of $O(n)$ (apply the hypothesis to $S_{n-1}$).

(b) There exists a finite number of slices $K_i$ ($1 \leq i \leq r$) of $M$ (Problem 5) relative to points $x_i$ of $M$, such that $M$ is the union of the sets $G \cdot K_i$. Deduce from (a) that each of the sets $L(S_{x_i}, K_i)$ is finite, and show that $L(G, G \cdot K_i)$ is finite by using Problem 5(c).
7. Let $G$ be a compact Lie group. Show that there are only finitely many conjugacy classes of normalizers of connected Lie groups immersed in $G$. (Consider the projective space $P(\Lambda(\mathfrak{g}_e))$ corresponding to the exterior algebra on the vector space $\mathfrak{g}_e$, and the action of $G$ on this compact manifold induced by the adjoint representation of $G$ on $\mathfrak{g}_e$, and apply the result of Problem 6.)

8. Let $G$ be a compact group and $\beta$ the Haar measure on $G$ for which the total mass is 1. In order that a sequence $(x_n)$ of points of $G$ should be equirepartitioned relative to the measure $\beta$ (Section 13.4, Problem 7) it is necessary and sufficient that, for each $\rho \neq \rho_0$ in $\mathbb{R}$, we should have

$$\lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} M_{\rho}(x_k) = 0.$$  

(Use (21.2.8) and (21.7.1).) In particular, for a point $s \in G$ to be such that the sequence $(s^n)_{n \geq 0}$ is equirepartitioned relative to $\beta$, it is necessary and sufficient that 1 is an eigenvalue of none of the matrices $M_{\rho}(s)$ for $\rho \neq \rho_0$. (This condition implies that $G$ is commutative.)

3. CHARACTERS OF A COMPACT GROUP

We retain the hypotheses and notation of (21.2). For each $\rho \in \mathbb{R}$ and each $s \in G$, let

$$\chi_\rho(s) = \frac{1}{n_\rho} u_\rho(s) = \frac{1}{n_\rho} \sum_{j=1}^{n_\rho} m_{jj}^{(\rho)}(s).$$

(21.3.1) The function $\chi_\rho$ is called the character of the compact group $G$ associated with the minimal two-sided ideal $\alpha_\rho$.

The character $\chi_{\rho_0}$ associated with $\alpha_{\rho_0}$ (21.2.7) is the constant function $\chi_{\rho_0}(s) = 1$ for all $s \in G$. It is called the trivial character of $G$.

The following properties are immediate consequences of (21.2.3) and (21.2.5):

$$\chi_\rho(sts^{-1}) = \chi_\rho(t) \quad \text{for all} \quad s, t \in G.$$  

(21.3.2.1) We have

$$\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)} \quad \text{for all} \quad s \in G,$$

(21.3.2.2) and

$$\chi_\rho \ast \chi_\rho = \frac{1}{n_\rho} \chi_\rho.$$  

(21.3.2.3)
The characters form a Hilbert basis of the center of $L^2(G)$, indexed by $R$. In other words,

$$\int \chi_{\rho}(s)\overline{\chi_{\rho}(s)} \, d\beta(s) = \begin{cases} 0 & \text{if } \rho' \neq \rho, \\ 1 & \text{if } \rho' = \rho, \end{cases}$$

and if $f$ is any central function in $L^2(G)$, then

$$f = \sum_{\rho \in R} (f | \chi_{\rho}) \chi_{\rho} = \sum_{\rho \in R} n_{\rho}(f * \chi_{\rho})$$

in $L^2(G)$. Furthermore, we have

$$\int \chi_{\rho}(s) \, d\beta(s) = 0 \quad \text{for all } \rho \neq \rho_0.$$ 

Finally, for each $s \in G$,

$$\chi_{\rho}(s) = \text{Tr}(M_{\rho}(s))$$

and in particular

$$\chi_{\rho}(e) = n_{\rho}.$$ 

If $f, g$ are continuous complex-valued central functions on $G$, then

$$f * g = \sum_{\rho \in R} (g | \chi_{\rho})(f * \chi_{\rho})$$

the series on the right being summable for the topology of uniform convergence.

This follows directly from (21.2.1.1) and the fact that the $\chi_{\rho}$ form a Hilbert basis of the center of $L^2(G)$ (21.3.2).

The functions $\chi_{\rho}$ ($\rho \in R$) form a total system in the space of continuous complex-valued central functions on $G$, for the topology of uniform convergence.

For each continuous central function $f, f * \chi_{\rho}$ is a scalar multiple of $\chi_{\rho}$. Taking account of (21.3.3), it is enough to show that for each continuous central function $g$, there exists a continuous central function $f$ such that $\|f * g - g\|$ is arbitrarily small. We shall first establish the following topological lemma:

(i) Let $G$ be a metrizable topological group and $K$ a compact subset of $G$. For each open neighborhood $U$ of the identity element $e$ of $G$, there exists a neighborhood $V \subset U$ of $e$, such that $tVt^{-1} \subset U$ for all $t \in K$. 

3. CHARACTERS OF A COMPACT GROUP

(ii) In a compact metrizable group $G$, there exists a fundamental system of neighborhoods of $e$ that are invariant under all inner automorphisms. If $T$ is such a neighborhood, there exists a continuous central function $h \geq 0$, with support contained in $T$, and such that $\int h(s) \, d\beta(s) = 1$.

(i) Let $U_0$ be a neighborhood of $e$ such that $U_0^3 \subseteq U$. For each $s \in G$, there exists a neighborhood $V_s$ of $e$ in $G$ such that $sV_s s^{-1} \subseteq U_0$; by continuity, there is therefore a neighborhood $W_s$ of $s$ such that $tV_s t^{-1} \subseteq U$ for all $t \in W_s$. There exist a finite number of points $s_j \in K (1 \leq j \leq m)$ such that the $W_{s_j}$ cover $K$; if we put $V = \bigcap_j V_{s_j}$, we shall have $tV t^{-1} \subseteq U$ for all $t \in K$.

(ii) We may apply (i) with $K = G$. The union $T$ of the $tV t^{-1}$ as $t$ runs through $G$ is then a neighborhood of $e$ contained in $U$ and invariant under all inner automorphisms.

To construct the function $h$, choose a continuous function $f \geq 0$, with support contained in $T$, and such that $f(e) > 0$; then let

$$h(t) = c \int_G f(st^{-1}) \, d\beta(s)$$

where $c$ is a suitably chosen positive constant. The proof that $h$ satisfies the required conditions is the same as in (21.2.3).

The proof that for any given continuous central function $g$, the number $\| h \ast g - g \|$ can be made arbitrarily small by suitable choice of a continuous central function $h$, now follows from the lemma (21.3.4.1) and regularization (14.11.1).

(21.3.5) (i) For each element $s \neq e$ in $G$, there exists $p \in \mathbb{R}$ such that $\chi_p(s) \neq \chi_p(e)$.

(ii) The intersection of the kernels $N_p$ of the homomorphisms $s \mapsto M_p(s)$, as $p$ runs through $\mathbb{R}$, consists of the identity element alone.

(i) If not, it would follow from (21.3.4) that $f(s) = f(e)$ for all continuous central functions $f$ on $G$, contradicting (21.3.4.1).

(ii) It is enough to remark that $s \in N_p$ implies that $\chi_p(s) = \chi_p(e)$.

(21.3.6) For all characters $\chi$ of $G$ we have

(21.3.6.1) $\chi(s)\chi(t) = \chi(e) \int \chi(usu^{-1}t) \, d\beta(u)$

for all $s, t \in G$. 
From the definition of $\chi_p$, we have

$$\chi_p(usu^{-1}t) = \frac{1}{n_p} \sum_i m_{ii}(usu^{-1}t)$$

by virtue of (21.2.5.1), and therefore

$$\int \chi_p(usu^{-1}t) \, d\beta(u) = \frac{1}{n_p} \sum_{i,j,h,k} m_{jh}(s)m_{hk}(u^{-1})m_{ki}(t)$$

making use of (21.2.5).

(21.3.7) The mapping that sends the class of a function $f \in L^2_c(G)$ to the class of its complex conjugate $\overline{f}$ is clearly a semilinear bijection of the algebra $L^2_c(G)$ onto itself, which is an automorphism of its ring structure. This automorphism therefore transforms each minimal two-sided ideal $\alpha_p$ into another minimal two-sided ideal, which we denote by $\alpha_p$. If in general $X$ denotes the matrix whose entries are the complex conjugates of those of a matrix $X$, then we have $M_p(s) = \overline{M_p(s)}$ for all $s \in G$, and for the corresponding characters we have

$$\chi_p = \overline{\chi_p}.$$  

The relation $\alpha_p = \alpha_p$ is therefore equivalent to the character $\chi_p$ taking only real values on $G$.

**Particular Cases:** 1. **Commutative Compact Groups**

(21.3.8) Let $f \in L^2_c(G)$ be nonnegligible and such that, for all $s \in G$, $f(st) = f(s)f(t)$ for almost all $t \in G$. This means that in $L^2_c(G)$ the subspace $C \cdot f$ is stable under all the mappings $g \mapsto (e_x * g)^{-}$, and hence is a minimal closed left ideal of dimension 1 (21.2.3.3). This is possible only if this ideal is one of the $\alpha_p$ such that $n_p = 1$, and then $f$ is equal almost everywhere to the corresponding character $\chi_p$. These characters are called the *abelian characters* of $G$. We have just seen that they are the only continuous homomorphisms of $G$ into $C^*$; the image of $G$ under such a homomorphism, being a
3. CHARACTERS OF A COMPACT GROUP 27

compact subgroup of $\mathbb{C}^*$, is necessarily contained in $U$ (the unit circle in $\mathbb{C}^*$), because $\mathbb{C}^* = U \times R_+^*$, and $R_+^*$ contains no compact subgroup other than $\{1\}$.

If the compact group $G$ is commutative, every character of $G$ is abelian, because the algebras $a_n$ are commutative. The classes of the characters of $G$ then form a Hilbert basis of $L^2_c(G)$ (21.2.5), and every continuous function on $G$ is the uniform limit of a sequence of linear combinations of characters (21.3.4).

(21.3.9) Every character of the group $U^n$ is of the form

\[(z_1, z_2, \ldots, z_n) \mapsto z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}\]

where $k_1, \ldots, k_n$ are integers (positive, negative, or zero). The only character of $U^n$ that takes only real values is the trivial character ($k_1 = \cdots = k_n = 0$).

The group $U^n$ is isomorphic to $T^n$, hence to $R^n/Z^n$. If $u$ is a continuous homomorphism of $R^n/Z^n$ into $T = R/Z$, and if $\varphi: R^n \to R^n/Z^n$ and $\psi: R \to R/Z$ are the canonical homomorphisms, then $u = \varphi$ is a continuous homomorphism of $R^n$ into $R/Z$, and therefore (16.30.3) factorizes as $\psi \circ v$, where $v$ is a continuous homomorphism of $R^n$ into $R$. By restricting $v$ to each of the subgroups $Re_j$ of $R^n$ (where $(e_j)$ is the canonical basis of $R^n$) and using (4.1.3), it follows that $v$ is a linear mapping of $R^n$ into $R$. Moreover, since $u(\varphi(Z^n)) = \{0\}$, we must have $v(Z^n) \subset Z$, and therefore each of the $v(e_j)$ must be an integer $k_j$. This completes the proof.

Observe that if we apply to the group $U^n$ the theorems (21.3.2) and (21.3.4) we regain, in view of (21.3.9), the facts that the orthogonal system $(z^n)_{n \in Z}$ is total in $L^2_c(U)$ (7.4.3), and that every continuous function on $U^n$ is a uniform limit of trigonometric polynomials (7.4.2).

**Particular Cases: II. Finite Groups**

(21.3.10) If $G$ is a finite group, the algebras $M^1_c(G)$, $L^1_c(G)$ and $L^2_c(G)$ all coincide with the group algebra of $G$ over $\mathbb{C}$, which is also denoted by $C[G]$ (14.7.4), and all the elements of this algebra may be considered as continuous functions on $G$. Let $C_1, \ldots, C_r$ denote the conjugacy classes of $G$ (with $C_1 = \{e\}$), that is to say, the equivalence classes for the relation:

there exists $t \in G$ such that $s' = t s t^{-1}$

between elements $s, s' \in G$. It follows from the definition (21.2.2.1) that each central function is constant on each set $C_j$, and from (21.3.4) that the central
functions are in this case linear combinations of characters. Since the latter are linearly independent, we see that the number \( r \) of conjugacy classes \( C_j \) is equal to the number of characters of \( G \) and to the dimension of the center of \( C[G] \).

Let \( \rho_1, \rho_2, \ldots, \rho_r \) denote the elements of \( R \), and for brevity let \( \chi_{ij} \) denote the value taken by the character \( \chi_{\rho_i} \) on the class \( C_j \). If \( g \) is the order of \( G \) and \( h_j \) the number of elements in the class \( C_j \), the orthogonality relations (21.3.2.4) take the form

\[
\frac{1}{g} \sum_{k=1}^{r} h_k \chi_{ik} \overline{\chi_{jk}} = \delta_{ij} \quad (1 \leq i, j \leq r).
\]

In other words, the \( r \times r \) matrix

\[
(21.3.10.2) \quad \left( h_k^{1/2} g^{-1/2} \chi_{ik}^{-1} \right)_{1 \leq i, k \leq r}
\]

is unitary. We obtain other orthogonality relations by expressing that the transpose of (21.3.10.2) is unitary:

\[
(21.3.10.3) \quad \sum_{i=1}^{r} \chi_{ik} \overline{\chi_{il}} = 0 \quad \text{if} \quad k \neq l,
\]

\[
(21.3.10.4) \quad \sum_{i=1}^{r} |\chi_{ik}|^2 = g/h_k.
\]

These formulas can also be written as

\[
(21.3.10.5) \quad \sum_{\rho \in R} \chi_{\rho}(s) \chi_{\rho}(t^{-1}) = 0
\]

if \( s, t \) are not conjugate in \( G \), and

\[
(21.3.10.6) \quad \sum_{\rho \in R} |\chi_{\rho}(s)|^2 = g/h_k
\]

if \( s \in C_k \).

Since \( e \) is not conjugate to any other element of \( G \), by putting \( t = e \) in (21.3.10.5) and taking account of (21.3.2.8) we obtain

\[
(21.3.10.7) \quad \sum_{\rho \in R} \eta_{\rho} \chi_{\rho}(s) = 0 \quad \text{if} \quad s \neq e.
\]
3. CHARACTERS OF A COMPACT GROUP

Of course, if we put \( s = e \) in (21.3.10.6) we obtain the relation

\[
\sum_{\rho \in \pi} n_{\rho}^2 = g, \tag{21.3.10.8}
\]

which also follows from the fact that \( L^2_c(G) \) is the direct sum of the \( \alpha_{\rho} \).

PROBLEMS

1. Let \( G \) be a metrizable compact group. Show that the center of the Banach algebra \( M_c(G) \) of measures on \( G \) is the closure of the center of \( L^2_c(G) \), in the vague topology.

2. Show that:
   
   (a) If the representations \( M_{\rho} \) and \( \tilde{M}_{\rho} = M_{\rho} \) are not equivalent, then \( \int \chi_{\rho}(s^2) \, d\beta(s) = 0. \)

   (b) If the representation \( M_{\rho}^{(R)} \) is defined (Section 21.1, Problem 9), then \( \int \chi_{\rho}(s^2) \, d\beta(s) = 1. \)

   (c) If the representation \( M_{\rho}^{(H)} \) is defined (Section 21.1, Problem 9), then \( \int \chi_{\rho}(s^2) \, d\beta(s) = -1. \)

(Use the orthogonality relations for characters and observe that if \( M_{\rho}^{(R)} \) (resp. \( M_{\rho}^{(H)} \)) is defined, there exists a unitary matrix \( U \) such that \( M_{\rho}(s) = UM_{\rho}(s)U^{-1} \) for all \( s \in G \), and \( 'U = U \) (resp. \( 'U = -U \)) (cf. Section 21.1, Problem 9).)

3. Let \( G \) be a finite group.

   (a) Show that for each character \( \chi \) of \( G \) and each \( s \in G \), the complex number \( \chi(s) \) is an algebraic integer.† (Consider the eigenvalues of \( U(s) \), where \( U \) is an irreducible representation of \( G \) with character \( \chi \), and remark that each element of \( G \) has finite order.)

   (b) Deduce from (a) that the number of elements of a conjugacy class \( C \) in \( G \) divides the order \( g \) of \( G \). Give a direct proof of this fact.

   (c) The characteristic functions \( \epsilon_j \) of the subsets \( C_j \) of \( G \) form a basis of the center of \( C[G] \) for which the coefficients in the multiplication table are rational integers \( \geq 0 \). Deduce that if we put \( M_{\rho}(\epsilon_j) = \lambda_j I_{n_{\rho}} \), then the complex numbers \( \lambda_j \) are algebraic integers (remark that the image of the center of \( C[G] \) under \( M_{\rho} \) is a finitely generated \( \mathbb{Z} \)-module). Show that for each conjugacy class \( C_j \) in \( G \) the number \( n_{\rho}^{-1} \sum_{s \in C_j} \chi_{\rho}(s) \) is an algebraic integer, for each \( \rho \in \pi \).

   (d) Deduce from (a) and (c) that each \( n_{\rho} \) divides the order \( g \) of \( G \) (use (21.3.10.1)).

4. Let \( G \) be a finite group. For each \( s \in G \), let \( t(s) \) denote the number of elements \( u \in G \) such that \( u^2 = s \). Show that

\[
t(s) = \sum_{\rho \in \pi} \nu(\rho) \chi_{\rho}(s)\]

where
\[ v(p) = \frac{1}{g} \sum_{s \in G} \chi_p(s^2) \]
(which is equal to 1, 0 or -1, by Problem 2).

5. Let \( G \) be a finite group. With the notation of (21.3.10), show that each of the numbers \( \sum_{k=1}^{r} x_{jk} \) is a rational integer \( \geq 0 \). (Decompose into irreducible representations the representation of degree \( g \) (the order of \( G \)) defined on the vector space \( C[G] = C^G \) by \( U(s) \cdot e_i = e_{i_{u(s)}} \).)

6. Let \( G \) be a finite group.
   (a) For each \( p \in \mathbb{R} \) and each \( s \in G \), we have \( |\chi_p(s)| \leq n_p \) (cf. (22.1.3.5)); we have \( \chi_p(s) = n_p \) if and only if \( s \) lies in the kernel \( N_p \) of \( M_p \); and \( |\chi_p(s)| = n_p \) if and only if the coset of \( s \) in \( G/N_p \) belongs to the center of this group. (Consider the eigenvalues of \( M_p(s) \).)
   (b) Suppose that for some conjugacy class \( C \) in \( G \), the number \( h_j \) of elements of \( C \) is prime to \( n_p \). Show that for each \( s \in C_j \), either \( \chi_p(s) = 0 \) or \( |\chi_p(s)| = n_p \). (Deduce from Problem 3(c) that the number \( \chi_p(s)/n_p \) is an algebraic integer, and use (a) above.)
   (c) Suppose that \( C_j \neq [e] \) and that the number of elements in \( C \) is a prime power. Show that there exists \( p \neq p_0 \) in \( \mathbb{R} \) such that \( |\chi_p(s)| = n_p \) for \( s \in C_j \). (Use (21.3.2.6) and the fact that \( n_p \chi_p(s) \) is an algebraic integer.) Deduce that \( G \) cannot be a noncommutative simple group.

7. Let \( G \) be a finite group of order \( p^aq^b \), where \( p \) and \( q \) are prime numbers. Then \( G \) is solvable (Burnside's theorem). (Argue by induction on the order of \( G \), by considering a Sylow \( p \)-subgroup of \( G \), which has a nontrivial center.† Consider the number of elements conjugate in \( G \) to an element \( \neq e \) of this center, and use Problem 6(c).)

4. CONTINUOUS UNITARY REPRESENTATIONS OF COMPACT GROUPS

(21.4.1) Let \( G \) be a compact group and let \( V \) be a continuous unitary representation of \( G \) on a separable complex Hilbert space \( E \). Then (with the notation of (21.2)): 

(i) For each \( p \in \mathbb{R} \), the operator \( V(u_p) \) (21.1.4.2) is an orthogonal projection of \( E \) onto a closed subspace \( E_p \) of \( E \), and \( E \) is the Hilbert sum of the \( E_p \).

(ii) Each subspace \( E_p \) is stable under \( V \), and the restriction of \( V \) to \( E_p \) is the Hilbert sum of a (finite or infinite) sequence of irreducible representations of \( G \), each equivalent to \( M_p \) (21.2.5) and (21.3.7)).

(i) Since \( u_p \ast u_p = u_p \) and \( \tilde{u}_p = u_p \) (21.2.3), \( V(u_p) \) is a continuous operator on \( E \) which is idempotent and Hermitian (21.1.6), hence (15.5.3.1) is an

orthogonal projection. Further, since \( u_{\rho} * u_{\rho'} = 0 \) if \( \rho' \neq \rho \), we have \( V(u_{\rho}) \circ V(u_{\rho'}) = 0 \), and therefore the images \( E_{\rho} \) of the projections \( V(u_{\rho}) \) are pairwise orthogonal closed subspaces. To show that \( E \) is the Hilbert sum of the \( E_{\rho} \), it is enough to show that the sum of the subspaces \( E_{\rho} \) is dense in \( E \). Now, we know that as \( f \) runs through \( L^1_{c}(G) \) and \( x \) runs through \( E \), the vectors \( V(f) \cdot x \) span a dense subspace of \( E \) (21.1.7). Since the continuous functions are dense in \( L^1_{c}(G) \), and since \( \| V(f) \| \leq N_1(f) \) (21.1.4.3), it follows that the \( V(f) \cdot x \) already span a dense subspace of \( E \) as \( x \) runs through \( E \) and \( f \) runs through the space \( C_c(G) \) of continuous functions on \( G \). But if \( f \) is continuous, then for each \( \varepsilon > 0 \) there exists a finite linear combination

\[
\sum_{i, j, \rho} c_{ij}^{(p)} m_{ij}^{(p)}
\]

such that \( \| f - \sum_{i, j, \rho} c_{ij}^{(p)} m_{ij}^{(p)} \| \leq \varepsilon \) (21.2.8), and a fortiori

\[
\left\| V(f) - \sum_{i, j, \rho} c_{ij}^{(p)} V(m_{ij}^{(p)}) \right\| \leq N_1 \left( f - \sum_{i, j, \rho} c_{ij}^{(p)} m_{ij}^{(p)} \right) \leq \varepsilon.
\]

Since \( m_{ij}^{(p)} = u_{\rho} \ast m_{ij}^{(p)} \), we have \( V(m_{ij}^{(p)}) = V(u_{\rho}) V(m_{ij}^{(p)}) \), and therefore the vector \( \sum_{i, j, \rho} c_{ij}^{(p)} V(m_{ij}^{(p)}) \cdot x \) belongs to the sum of the \( E_{\rho} \). This shows that the sum of the \( E_{\rho} \) is dense in \( E \).

(ii) That each \( E_{\rho} \) is stable under \( V \) follows from the fact that the \( u_{\rho} \) belong to the center of the algebra \( M_{c}(G) \). If \( V_{\rho} \) is the restriction of \( V \) to \( E_{\rho} \), then \( V_{\rho}(u_{\rho'}) = 0 \) for \( \rho' \neq \rho \), because \( u_{\rho} \ast u_{\rho} = 0 \). The restriction of \( (V_{\rho})_{ext} \) to the algebra \( L^1_{c}(G) \) may therefore be considered as a nondegenerate representation of the algebra \( a_{\rho} \) on \( E_{\rho} \); it follows therefore from (15.8.16) that this representation is the Hilbert sum, finite or infinite (according as the dimension of \( E_{\rho} \) is finite or not), of irreducible representations each equivalent to the representation \( U_{i_{1}} \), in the notation of (21.2.4). But it follows from the definition of \( U_{i_{1}} \) (15.8.1) and from (21.1.9) that \( U_{i_{1}} \) is the restriction of \( R_{ext} \) to \( a_{\rho} \). Now we have

\[
(e_{s} \ast m_{i_{1}})(t) = m_{i_{1}}(s^{-1} t) = \frac{1}{n_{\rho}} \sum_{j=1}^{n_{\rho}} m_{i_{j}}(s^{-1}) m_{j_{1}}(t)
\]

by (21.2.5); this shows that relative to the basis of \( I_{1} \) formed by the \( m_{i_{j}}^{-1} m_{i_{1}} \) \((1 \leq i \leq n_{\rho})\), the matrix of \( R(s) \) is \( 'M_{\rho}(s^{-1}) = M_{\rho}(s) = M_{\rho}(s) \) by (21.2.5).

(21.4.1.1) If \( G \) is a commutative compact group, every continuous unitary representation of \( G \) is therefore a Hilbert sum of one-dimensional representations (21.3.8).

(21.4.2) With the same notation, if \( E_{\rho} \neq \{0\} \), the irreducible representation \( M_{\rho} \) is said to be contained in the representation \( V \); if \( E_{\rho} \) is of finite dimension \( d_{\rho} n_{\rho} > 0 \) (resp. of infinite dimension), then \( M_{\rho} \) is said to be contained \( d_{\rho} \).
times (resp. infinitely many times) in $V$, and $d_\rho$ is called the multiplicity of $M_\rho$ in $V$. The $M_\rho$ such that $d_\rho > 0$ are also called the irreducible components of the representation $V$.

It follows from (21.4.1) that every irreducible continuous unitary representation of $G$ is equivalent to one of the representations $M_\rho$, and that $M_\rho$ is contained $n_\rho$ times in the regular representation (21.1.9) of $G$.

(21.4.3) A continuous linear representation $U$ of a compact group $G$ on a finite-dimensional complex vector space $E$ (21.1.1) may always be considered as a continuous unitary representation, because there exists a positive definite Hermitian form on $E$ (in other words, a scalar product (6.2)) that is invariant under the action $(s, x) \mapsto U(s) \cdot x$ of $G$ on $E$ (20.11.3.3). For compact groups there is therefore no loss of generality, where finite-dimensional continuous linear representations are concerned, in restricting consideration to unitary representations. If, for such a representation $U$, we identify $U(s)$ with its matrix relative to a fixed basis of $E$ that is orthonormal with respect to the scalar product referred to above, we have (21.1.2.1)

\[
U(s) = U'(s)^{-1} = U(s^{-1}).
\]

(21.4.4) Let $V$ be a continuous unitary representation of a compact group $G$ on a vector space $E$ of finite dimension $d$, and suppose that for each $\rho \in \mathbb{R}$ the irreducible representation $M_\rho$ is contained $d_\rho$ times in $V$, so that $d = \sum_{\rho \in \mathbb{R}} d_\rho n_\rho$.

Then, for all $s \in G$, we have

\[
\text{Tr}(V(s)) = \sum_{\rho \in \mathbb{R}} d_\rho \chi_\rho(s).
\]

This follows from (21.3.2.7) and the fact that $\text{Tr}(PUP^{-1}) = \text{Tr}(U)$ for any square matrix $U$ and invertible matrix $P$ of the same size.

(21.4.5) Two finite-dimensional continuous unitary representations $V_1, V_2$ of a compact group $G$ are equivalent if and only if $\text{Tr}(V_1(s)) = \text{Tr}(V_2(s))$ for all $s \in G$.

This follows immediately from the formula (21.4.4.1) and the linear independence of characters (21.3.2).

(21.4.6) Let $V', V''$ be continuous linear representations of a topological group $G$ on spaces $E'$, $E''$ of finite dimensions $d'$, $d''$, respectively. Then it is clear that the mapping

\[
V' \otimes V'': s \mapsto V'(s) \otimes V''(s)
\]
is a continuous linear representation of $G$ on the vector space $E' \otimes E''$ of dimension $d'd''$. This representation is called the tensor product of $V'$ and $V''$, and we have ((A.10.5) and (A.11.3))

\[(21.4.6.2) \quad \text{Tr}(V'(s) \otimes V''(s)) = \text{Tr}(V'(s)) \text{Tr}(V''(s)).\]

In particular, if $G$ is compact we may form the tensor product $M_{\rho'} \otimes M_{\rho''}$ for any two elements $\rho', \rho''$ of $\mathbb{R}$, and then by (21.4.4.1) we have

\[(21.4.6.3) \quad \chi_{\rho'} \chi_{\rho''} = \sum_{\rho} c_{\rho\rho'}^{\rho''} \chi_{\rho},\]

where $c_{\rho\rho'}^{\rho''}$ is the number of times the representation $M_{\rho}$ is contained in $M_{\rho'} \otimes M_{\rho''}$, and is therefore a nonnegative integer. Since the $\chi_{\rho}$ are linearly independent over $\mathbb{C}$ and a fortiori over $\mathbb{Z}$, we see that the subring of $\mathcal{C}_{c}(G)$ generated by the characters of $G$ is a $\mathbb{Z}$-algebra; its identity element is the trivial character, the characters $\chi_{\rho}$ form a basis over $\mathbb{Z}$, and the multiplication table is given by (21.4.6.3).

\[(21.4.6.4) \quad \text{For each } \rho \in \mathbb{R}, \text{ the trivial representation (21.2.7) is contained in } M_{\rho} \otimes M_{\rho} = M_{\rho} \otimes M_{\rho}; \text{ for if it were not so, then by (21.3.2.6) and (21.4.6.3) we should have}\]

\[\int \chi_{\rho}(s) \chi_{\rho}(s) \, d\beta(s) = \int |\chi_{\rho}(s)|^2 \, d\beta(s) = 0,\]

which is absurd.

\[(21.4.7) \quad \text{Since any irreducible representation } V \text{ of } G \text{ is equivalent to a representation } M_{\rho} \text{ for a unique index } \rho, \text{ we shall say (by abuse of language) that } \rho \text{ is the class of the representation } V \text{ and we write } \rho = \text{cl}(V). \text{ The class } \rho_0 \text{ of the trivial representation is called the trivial class. The class } \rho \text{ is called the conjugate of the class } \rho.\]

If $V$ is a finite-dimensional continuous unitary representation of $G$, and if for each $\rho \in \mathbb{R}$ the representation $M_{\rho}$ is contained $d_{\rho}$ times in $V$, then the element $\sum_{\rho \in \mathbb{R}} d_{\rho} \cdot \rho$ of the $\mathbb{Z}$-module $Z^{(\mathbb{R})}$ of formal linear combinations of elements of $\mathbb{R}$ with integer coefficients is called the class of the representation $V$, and is written $\text{cl}(V)$. The relation $\text{cl}(V_1) = \text{cl}(V_2)$ therefore signifies that the representations $V_1$ and $V_2$ are equivalent, which justifies this terminology. We say also that the class $\rho$ is contained $d_{\rho}$ times in $\text{cl}(V)$, or that $d_{\rho}$ is the multiplicity of $\rho$ in $\text{cl}(V)$.

Conversely, every element $\sum_{\rho \in \mathbb{R}} d_{\rho} \cdot \rho$ of $Z^{(\mathbb{R})}$ in which the coefficients $d_{\rho}$
are positive or zero is the class of a linear representation of $G$, namely the Hilbert sum of a family of $m = \sum_{\rho \in \mathbb{R}} d_\rho$ irreducible representations, containing $d_\rho$ representations equal to $M_\rho$ for each $\rho \in \mathbb{R}$. It is clear that the bijection $\rho \mapsto \chi_\rho$ extends by linearity to an isomorphism of the $\mathbb{Z}$-module $\mathbb{Z}(\mathbb{R})$ onto the subring of $\mathcal{C}(G)$ generated by the characters of $G$. Transporting the ring structure back to $\mathbb{Z}(\mathbb{R})$ by means of the inverse of this isomorphism, we define on $\mathbb{Z}(\mathbb{R})$ a structure of a commutative ring, for which $\rho_0$ is the identity element and the multiplication is given by

$$\rho' \rho'' = \sum_{\rho} c_{\rho' \rho''}^\rho \cdot \rho.$$ 

For this ring structure we have

$$\text{cl}(V_1 \otimes V_2) = \text{cl}(V_1) \cdot \text{cl}(V_2)$$

for any two finite-dimensional continuous linear representations $V_1, V_2$ of $G$.

By abuse of language, the ring $\mathbb{Z}(\mathbb{R})$ just defined is called the ring of classes of continuous linear representations of $G$. (The abuse of language lies in the fact that a linear combination of the elements of $\mathbb{R}$ with integer coefficients is the class of a representation only if all the coefficients are $\geq 0$.) Also we shall sometimes write $\mathbb{R}(G)$ in place of $\mathbb{R}$.

For example, if $G = U^n$ (isomorphic to $\mathbb{T}^n$), it follows from (21.3.9) that the ring of classes of linear representations of $G$ is isomorphic to the subring $\mathbb{Z}[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}]$ of the field of rational functions $\mathbb{Q}(X_1, \ldots, X_n)$ in $n$ indeterminates over the field $\mathbb{Q}$ of rational numbers.

With the notation of (21.2.4), the formula (21.2.3.1) may be written as

$$\tilde{f} = \sum_{\rho \in \mathbb{R}} \left( \sum_{j=1}^{n_\rho} (f \ast m_{jj}^{(\rho)})^{-1} \right).$$

Now we have, by definition,

$$(f \ast m_{jj}^{(\rho)})(s) = \int f(t)m_{jj}^{(\rho)}(t^{-1}s) \, d\beta(t),$$

and therefore

$$\sum_{j=1}^{n_\rho} (f \ast m_{jj}^{(\rho)})(s) = n_\rho \cdot \text{Tr} \left( \int f(t)M_\rho(t^{-1}s) \, d\beta(t) \right).$$
Also we have \( M_\rho(t^{-1}s) = M_\rho(t^{-1})M_\rho(s) \), and
\[
\int f(t)M_\rho(t) \, d\beta(t) = M_\rho(\tilde{f})
\]
by virtue of (21.1.4.2) and the fact that \( G \), being compact, is unimodular. Hence, for all \( f \in \mathcal{L}^2(G) \), we obtain the formula
\[
\tilde{f} = \sum_{\rho \in \mathcal{R}} n_\rho \cdot \text{Tr}(M_\rho(\tilde{f})M_\rho(\cdot))
\]
where the series on the right converges in \( \mathcal{L}^2(G) \), no matter how the elements of \( \mathcal{R} \) are arranged in a sequence. The function \( \rho \mapsto M_\rho(\tilde{f}) \), defined on \( \mathcal{R} \) and taking its values in the space of all complex square matrices, is sometimes called the "Fourier transform" of \( f \), and the formula (21.4.8.1) is the "Fourier inversion formula for compact groups" (cf. Chapter XXII).

### PROBLEMS

1. Let \( G, H \) be two compact groups. Show that the ring \( \mathcal{Z}^{(G \times H)} \) of classes of continuous linear representations of \( G \times H \) is isomorphic to the tensor product \( \mathcal{Z}^{(G)} \otimes \mathcal{Z}^{(H)} \) (cf. Section 21.1, Problem 12).

2. Let \( P_k(\sigma_1, \sigma_2, \ldots, \sigma_m) \) be the polynomial with rational integer coefficients that expresses the sum \( X_1^k + \cdots + X_m^k \) of the \( k \)th powers of \( m \) indeterminates in terms of the elementary symmetric functions \( \sigma_k = \sum_{(j)} X_{j_1} \cdots X_{j_k} \) of these indeterminates (the summation is over all strictly increasing sequences \( j_1 < j_2 < \cdots < j_k \) of \( h \leq m \) indices). Let \( U \) be a finite-dimensional linear representation of a compact group \( G \) and consider the element of \( \mathcal{Z}^{(G)} \) given by
\[
P_k\left( \text{cl}(U), \text{cl}\left( \bigwedge^2 U \right), \ldots, \text{cl}\left( \bigwedge^n U \right) \right)
\]
(Section 21.1, Problem 11). Consider also the canonical homomorphism \( \chi \) of \( \mathcal{Z}^{(G)} \) into \( \mathfrak{g}(G) \), which maps \( \rho \in \mathcal{R}(G) \) to \( \chi_\rho \). Show that the image under \( \chi \) of the element (\( *) \) above is equal to the function \( s \mapsto \text{Tr}(U(s^k)) \).

3. Let \( G \) be a locally compact group and let \( U \) be a continuous unitary representation of \( G \) on a separable Hilbert space \( E \). Let \( \mathcal{H}(U) \) denote the algebra of intertwining operators of \( U \) with itself (Section 21.1, Problem 6), i.e., the algebra of continuous operators \( T \in \mathcal{L}(E) \) such that \( TU(s) = U(s)T \) for all \( s \in G \).

The representation \( U \) is said to be primary if the center of \( \mathcal{H}(U) \) consists only of the homotheties of \( E \), and isotypic if it is primary and if there exists a nontrivial irreducible subrepresentation of \( U \).
4. Let \( G \) be a unimodular locally compact group. A continuous unitary representation of \( G \) on a separable Hilbert space \( E \) is said to admit a **discrete decomposition** if it is a Hilbert sum of irreducible representations.

(a) Let \( R(G) \) be the set of equivalence classes of irreducible continuous unitary representations of \( G \). Let \( U \) be a continuous unitary representation of \( G \) on \( E \), and suppose that \( E \) is a Hilbert sum of subspaces \( E_\alpha \) such that the restriction \( U_\alpha \) of \( U \) to \( E_\alpha \) is irreducible. For each \( \rho \in R(G) \), let \( M_\rho \) be the Hilbert sum of the \( E_\alpha \) such that \( U_\alpha \) is in the class \( \rho \). The nonzero \( M_\rho \) are called the **isotypic components** of \( E \). Show that for every irreducible subrepresentation \( V \) of \( U \), the space of \( V \) is necessarily contained in one of the \( M_\rho \), and that \( V \) is then of class \( \rho \), so that \( M_\rho \) may be defined as the smallest closed subspace of \( E \) that contains the spaces of all the irreducible subrepresentations of \( U \) of class \( \rho \) (and is therefore defined independently of the decomposition \( (E_\alpha) \) chosen). (Use Problem 3(c) above and Section 21.1, Problem 6.) If the restriction of \( U \) to \( M_\rho \) is the Hilbert sum of \( n_\rho \) representations of class \( \rho \), where \( n_\rho \) is finite or \(+\infty\), this number \( n_\rho \) is called the **multiplicity** of \( \rho \) in \( U \) (or in the class of \( \rho \)).

(b) Let \( U \) be a continuous unitary representation of \( G \) on \( E \) that has the following property: for every closed subspace \( F \) of \( E \) stable under \( U \), there exists a closed subspace \( L \) of \( F \) that is minimal among those that are stable under \( U \). Show that \( U \) admits a discrete decomposition. (Argue by induction, as in (15.8.10).)

(c) Let \( f_\alpha \) be a sequence of continuous functions on \( G \) satisfying the conditions of (14.11.2). Let \( U \) be a continuous unitary representation of \( G \) such that, for each \( \alpha \), the operator \( U(f_\alpha) \) is compact. Show that \( U \) admits a discrete decomposition into irreducible representations and that, for each \( \rho \in R(G) \), the multiplicity of \( \rho \) in \( U \) is finite. (Show that
5. Let $G$ be a unimodular locally compact group, and let $U$ be a continuous unitary representation of $G$ on a separable Hilbert space $E$. For each pair $(x, y)$ of points of $E$, the function $s \mapsto (U(s) \cdot x | y)$, which is continuous and bounded on $G$, is called the coefficient of $U$ relative to $(x, y)$, and is denoted by $c_U(x, y)$. For each bounded measure $\mu$ on $G$, we have $c_U(\mu \cdot x, y) = c_U(x, y) \ast \mu$ and $c_U(x, \mu \cdot y) = \mu \ast c_U(x, y)$. If $J$ is a semilinear bijection of $E$ into itself such that $(u \cdot x | y) = (x | y')$ (we may take $J(e_u) = e_{y'}$, where $e_u$ is a Hilbert basis of $E$), let $U$ denote the continuous unitary representation $s \mapsto JU(s)J^{-1}$ of $G$ on $E$, which is well-defined up to equivalence. Show that $c_U(x, y) = c_{U'}(x, y)$.

(a) Suppose that $U$ is irreducible and that there exist two nonzero vectors $x, y$ in $E$ such that the function $c_U(x, y)$ belongs to $L^2(G)$. Then $c_U(x, u(\mu) \cdot y)$ belongs to $L^2(G)$ for every bounded measure $\mu$ on $G$. Deduce that the set of $z \in E$ such that $c_U(x, z) \in L^2(G)$ is a dense vector subspace $F$ of $E$, and that the linear mapping $z \mapsto c_U(x, z)$ of $F$ into $L^2(G)$ is closed (Section 15.12, Problem 1). Use Section 21.1, Problem 6, to show that $F = E$ and that $U$ is equivalent to a subrepresentation of the regular representation $R$ of $G$ on $L^2(G)$; also that $c_U(x, y)$ belongs to $L^2(G)$ for all pairs $x, y$ in $E$.

(b) Show that for each function $f \in \mathcal{H}(G)$, the coefficient $c_R(\hat{f}, \hat{g})$ of the regular representation $R$ belongs to $L^2(G)$ for each $\hat{g} \in L^2(G)$. Deduce that all the coefficients of an irreducible subrepresentation of $R$ belong to $L^2(G)$. An irreducible unitary representation of $G$ is said to be square-integrable if it is equivalent to a subrepresentation of the regular representation of $G$.

(c) Show that if at least one irreducible unitary representation $U$ of $G$ is square-integrable, then the center $Z$ of $G$ is necessarily compact. (Observe that the function $|c_U(x, y)|$ on $G \times G$ is invariant under left and right translations by elements of $Z$.)

6. Let $G$ be a unimodular locally compact group, $U$ an irreducible unitary representation of $G$ on a Hilbert space $E$, and assume that $U$ is square-integrable (Problem 5).

(a) For all $x, y, x', y'$ in $E$ we have

$$
(c_U(x, y) | c_U(x', y')) = d_{x'}^{-1/2}(x | x')(y' | y')
$$

in $L^2(G)$, where $d_{x'}$ is a number $> 0$ that depends only on the equivalence class of $U$. (Observe that, as a result of Problem 5, the mapping $S_{x'}: z \mapsto c_U(x, z)$ is an intertwining operator between $U$ and the regular representation $R$, and consequently $S_{x'}^* S_{x'}$ is a homomorphism in $E$, by virtue of Schur's lemma; in other words, there exists a constant $a(x, x')$ such that

$$
(c_U(x, y) | c_U(x', y')) = a(x, x')(y' | y').
$$

Show on the other hand that

$$
(c_U(x, y) | c_{U'}(x', y')) = (c_U(y, x') | c_U(y, x))
$$

by using the fact that $G$ is unimodular.)
The number $d_U$ is multiplied by $a^{-1}$ when the Haar measure $\beta$ on $G$ is replaced by $a\beta$.

When $G$ is compact and $\beta$ is the Haar measure with total mass 1, the number $d_U$ is equal to the dimension of the representation $U$.

(b) Deduce from the Banach–Steinhaus theorem that there exists a constant $b > 0$ such that $N_G(c_0(x, y)) \leq b \cdot \|x\| \cdot \|y\|$ for all $x, y$ in $E$.

(c) Let $A, B$ be two nuclear operators on $E$ (Section 15.11, Problem 7). Show that

$$
\int_G \text{Tr}(U(s)AU(s)^{-1}B) \, d\beta(s) = d_U^{-1} \text{Tr}(AB),
$$

(Observe that there exists a Hilbert basis $(e_n)$ of $E$ and a sequence $(f_n)$ of vectors of norm 1 in $E$ such that, for all $x \in E$, we have $A \cdot x = \sum_n \lambda_n(x \cdot e_n)f_n$, where $\sum_n |\lambda_n| < \infty$, and use (a) and (b) above.)

7. Let $U, U'$ be two square-integrable irreducible unitary representations of $G$ on separable Hilbert spaces $E, E'$ respectively. Show that if $U$ and $U'$ are inequivalent, then every coefficient of $U$ is orthogonal in $L_2(G)$ to every coefficient of $U'$. (Consider on $E' \times E$ the sesquilinear form $(x', x) \mapsto \langle c_0(x', a') | c_0(x, a) \rangle$; show that it is continuous (Problem 6(b)) and that it can be written in the form $(x', x) \mapsto (x' \cdot A \cdot x)$, where $A$ is a continuous operator from $E$ to $E'$; finally prove that $A$ is an intertwining operator of $U$ with $U'$.)

8. Given two Hilbert spaces $E_1$ and $E_2$, a continuous operator $T : E_1 \to E_2$ is said to be a Hilbert–Schmidt operator if the operator on $E_1 \oplus E_2$ that is equal to $T$ on $E_1$ and 0 on $E_2$ is Hilbert–Schmidt (15.4.8). The space $L_2^2(E_1, E_2) \subset L_2^2(E_1 \oplus E_2)$ of Hilbert–Schmidt operators from $E_1$ to $E_2$ is a Hilbert space.

For each $x_1 \in E_1$ and $x_2 \in E_2$, let $u_{x_1, x_2}$ denote the linear mapping $z \mapsto \{z \cdot x_1, x_2\}$ of $E_1$ into $E_2$. This mapping belongs to $L_2^2(E_1, E_2)$, and we have $\|u_{x_1, x_2}\|_2 = \|x_1\| \cdot \|x_2\|$. If $(a_n)$ (resp. $(b_n)$) is a Hilbert basis of $E_1$ (resp. $E_2$), then the $u_{a_n, b_n}$ form a Hilbert basis of $L_2^2(E_1, E_2)$.

(a) Let $G_1, G_2$ be two locally compact groups and let $U_1$ (resp. $U_2$) be a continuous unitary representation of $G_1$ (resp. $G_2$) on a separable Hilbert space $E_1$ (resp. $E_2$). For $s_1 \in G_1, s_2 \in G_2$, and $T \in L_2^2(E_1, E_2)$, show that the mapping $U_2(s_2)TU_1(s_1)^{-1}$, which we denote by $U(s_1, s_2) \cdot T$, belongs to $L_2^2(E_1, E_2)$, and that $U(s_1, s_2)$ is a continuous unitary representation of $G_1 \times G_2$ on the Hilbert space $L_2^2(E_1, E_2)$.

(b) Suppose that $U_1$ and $U_2$ are irreducible. Show that $U$ is irreducible. (Remark that the closed subspace of $L_2^2(E_1, E_2)$ generated by the transforms $U_2(s_2)u_{a, b}$, where $a \neq 0$ in $E_1$ and $b \neq 0$ in $E_2$, contains all the elements $u_{a, b}$ for $y \in E_2$; likewise for the transforms $u_{a, b}U_1(s_1)$.) The restriction of $U$ to the subgroup $G_1 \times \{e_2\}$ of $G_1 \times G_2$ is then an isotypic unitary representation (Problem 3), a Hilbert sum of representations equivalent to $U_1$, the multiplicity of the class of $U_1$ in this restriction being equal to the dimension of $E_2$. Likewise for the restriction of $U$ to the subgroup $\{e_1\} \times G_2$.

9. Let $G$ be a unimodular locally compact group, and let $U$ be a square-integrable irreducible continuous unitary representation of $G$ on a Hilbert space $E$ (Problem 5). Let $M_U$ be the
closed vector subspace of $L^2_c(G)$ spanned by the coefficients (Problem 5) of $U$. It is stable
under the operators $\gamma(s)$ and $\delta(s)$ for each $s \in G$.

(a) Let $U'$ be another square-integrable irreducible representation of $G$. Show that if
$U'$ is equivalent to $U$, then $M_U = M_{U'}$, so that $M_U$ depends only on the class $\rho$ of $U$, and is
therefore also denoted by $M_\rho$. If on the other hand $U'$ is not equivalent to $U$, then the
subspaces $M_U$ and $M_{U'}$ are orthogonal. If $(e_j)$ is a Hilbert basis of $E$, the elements
$f_{\mu} = d_{\mu}^{1/2}c_{\mu}(e_j, e_j)$ form a Hilbert basis of $M_U$.

(b) Define a continuous unitary representation $(s, t) \mapsto V(s, t)$ of $G \times G$ on $M_U$ by
$V(s, t) \cdot c_{\mu}(x, y) = \gamma(s)\delta(t)c_{\mu}(x, y)$. Show that this representation is equivalent to the con-
tinuous unitary representation $(s, t) \mapsto W(s, t)$ of $G \times G$ on the Hilbert space $L^2(E)$ of
Hilbert–Schmidt operators on $E$, defined by $W(s, t) \cdot T = U(s)TU(t)^{-1}$ (Problem 8).
Deduce that $V$ is irreducible, and that the restriction to $M_\rho$ of the regular representation $R$
is a Hilbert sum of irreducible representations equivalent to $U$, the multiplicity of $U$ in this
decomposition (Problem 4) being the dimension of $E$.

(c) Let $f$ be a function in $L^2_c(G)$, with compact support, and let $P$ be the orthogonal
projection of $L^2_c(G)$ onto the subspace $M_U$. Show that $U(f)$ is a Hilbert–Schmidt operator
on $E$ and that $\|U(f)\|_2 \leq d_{\rho}^{1/2}N_\rho(P \cdot f)$. (Use the basis $(f_{\mu})$ of $M_\rho$ to calculate $N_\rho(P \cdot f)$)

(d) Let $L^2_c(G)_\rho$ be the closed subspace of $L^2_c(G)$ that is the Hilbert sum of the
subspaces $M_\rho$, as $\rho$ runs through the set of equivalence classes of square-integrable irreducible
representations of $G$. Show that $L^2_c(G)_\rho$ contains every closed subspace $F$ of $L^2_c(G)$
that is stable under $\gamma(s)$ (resp. $\delta(s)$) for all $s \in G$ and is minimal with respect to this
property among nonzero subspaces. (Let $P$ be the orthogonal projection of $L^2_c(G)$ onto $F$.
If $V$ is the irreducible representation that is the restriction of $(G)$ to $F$, calculate the
coefficients $c_{\rho}(f, P \cdot g)$ for $f \in F$ and $g \in \pi(G)$)

10. Let $G$ be a locally compact group and let $U$ be a continuous linear representation of $G$ on
a finite-dimensional complex vector space. Assume that the coefficients $c_U(x, x^*)$ (Section
21.2, Problem 1) belong to $L^2_c(G)$.

(a) Show that there exists on $E$ a (nondegenerate) Hermitian scalar product $\Phi$ that is
invariant under $U$ (same method as in (20.11.3.1)).

(b) Deduce from (a) that the group $G$ is necessarily compact. (Observe that the
coefficients of the matrix of $\Phi$, relative to a basis of $E$, belong to $L^2_c(G)$)

11. (a) Let $G$ be a topological group, let $U$ be a continuous linear representation of $G$ on
a complex vector space $E$ of dimension $d$, and let $V_0$ be the trivial representation of $G$ on
a vector space $F$ of dimension $n$. Let $W$ be the representation $s \mapsto U(s) \otimes V_0(s)$ of $G$
on $E \otimes F$. Show that if $n > d$, there exists no vector $z \in E \otimes F$ such that the vectors $W(s) \cdot z$
$(s \in G)$ generate $E \otimes F$. (Write $z$ in the form $\sum_{j=1}^d x_j \otimes y_j$, where the $x_j$ form a basis of $E$, and
the $y_j$ belong to $F$.)

(b) Let $G$ be a compact group. With the notation of (21.4.1), if $V$ is the Hilbert sum
of $q \leq n_\rho$ representations equal to $M_\rho$, then there exists a totalizing vector $x_0$ in the space
$E$ of the representation $V$ (in other words the vectors $V(s) \cdot x_0$ for $s \in G$ span $E$). (Reduce
to the case where $E$ is the sum $I_1 + I_2 + \cdots + I_\rho$ in $a_\rho$ and $V$ is the restriction to $E$ of the
regular representation. Show that we may take $x_0 = m_1 + m_2 + \cdots + m_\rho$, by showing
that no nonzero vector in $E$ is orthogonal to all the $V(s) \cdot x_0$.)

(c) Let $G$ be a compact group. Show that a continuous unitary representation $V$ of
$G$ on a separable Hilbert space $E$ is topologically cyclic if and only if, for each $\rho \in R$, the
multiplicity of $M_\rho$ in $V$ is $\leq n_\rho$. (To show that the condition is sufficient, we may assume
that $E$ is the Hilbert sum of left ideals $b_\rho = a_\rho$, where $\rho$ runs through a subset $R'$ of $R$, and
$V$ is the restriction to $E$ of the regular representation. If $x_{\rho} \in \mathfrak{b}_{\rho}$ is a totalizer for the restriction of $V$ to $\mathfrak{b}_{\rho}$, consider a vector $x_{\rho} = \sum_{\rho \in \mathfrak{R}} x_{\rho}$, where $\sum_{\rho \in \mathfrak{R}} \xi_{\rho}^{2} \|x_{\rho}\|^2 < \infty$ and $\xi_{\rho} > 0$.

5. INVARIANT BILINEAR FORMS; THE KILLING FORM

(21.5.1) From now on in this chapter we shall consider only (real or complex) Lie groups. By a linear representation of a real Lie group $G$ on a finite-dimensional real or complex vector space $E$ we shall mean (as in (16.9.7)), unless the contrary is expressly stated, a Lie group homomorphism (hence of class $C^{\infty}$) $s \mapsto U(s)$ of $G$ into $\text{GL}(E)$. (If $E$ is a complex vector space, we consider $\text{GL}(E)$ as equipped with its underlying structure of a real Lie group.) By virtue of (19.10.2), this notion in fact coincides with the notion of continuous linear representation (on a finite-dimensional complex vector space) introduced in (21.1).

If $G$ is a complex Lie group, a linear representation of $G$ on a finite-dimensional complex vector space $E$ is by definition a homomorphism of complex Lie groups $s \mapsto U(s)$ (hence a holomorphic mapping) of $G$ into $\text{GL}(E)$. One must be careful to distinguish these representations from linear representations of the underlying real Lie group $G_{\mathbb{R}}$ on $E$; every linear representation of $G$ on $E$ is also a linear representation of $G_{\mathbb{R}}$, but the converse is false.

Let $E$ be a finite-dimensional real vector space, and let $E_{(C)} = E \otimes \mathbb{R} \mathbb{C}$ be its complexification. Every endomorphism $P$ of $E$ has a unique extension to an endomorphism $P \otimes 1_{C}$ of $E_{(C)}$, such that $(P \otimes 1_{C}) \cdot (x \otimes \zeta) = (P \cdot x) \otimes \zeta$ for all $x \in E$ and all $\zeta \in \mathbb{C}$ (A.10.6). The matrix of $P$ relative to a basis $(e_{j})$ of $E$ is the same as the matrix of $P \otimes 1_{C}$ relative to the basis $(e_{j} \otimes 1)$ of $E_{(C)}$. It follows immediately that every linear representation $s \mapsto U(s)$ of a real Lie group $G$ on $E$ extends uniquely to a linear representation $s \mapsto U(s) \otimes 1_{C}$ of $G$ on $E_{(C)}$.

(21.5.2) Given any linear representation $s \mapsto U(s)$ of a real (resp. complex) Lie group $G$ on a finite-dimensional real or complex (resp. complex) vector space $E$, we have a derived homomorphism $u \mapsto U_{\ast}(u)$ of the Lie algebra $\mathfrak{g}_{e}$ of $G$ into the Lie algebra $\mathfrak{gl}(E)$. For each $w \in \mathfrak{g}_{e}$, we have (19.8.9)

(21.5.2.1) $U(\exp(w)) = \exp(U_{\ast}(w))$.

If $G$ is a real Lie group and $E$ a real vector space, the derived homomorphism of the representation $U \otimes 1_{C}$ of $G$ on $E_{(C)}$ (21.5.1) is the homomorphism $u \mapsto U_{\ast}(u) \otimes 1_{C}$ of $\mathfrak{g}_{e}$ into $\mathfrak{g}(E_{(C)}) = \mathfrak{g}(E) \otimes \mathbb{R} \mathbb{C}$. 
5. INVARIANT BILINEAR FORMS; THE KILLING FORM

We remark also that if $F$ is a finite-dimensional complex vector space, $a$ a real Lie algebra (of finite or infinite dimension) and $\rho: a \to \mathfrak{gl}(F)$ a homomorphism of real Lie algebras, then the mapping $\rho_C: u \otimes \zeta \mapsto \rho(u)\zeta$ is a (C-linear) homomorphism of the complexification $a_C = a \otimes_{\mathbb{R}} \mathbb{C}$ of $a$ into $\mathfrak{gl}(F)$ that extends $\rho$.

(21.5.3) Let $s \mapsto U(s)$ be a linear representation of a real (resp. complex) Lie group $G$ on a finite-dimensional real or complex (resp. complex) vector space $E$. Canonically associated with $U$ is the following bilinear form on the real (resp. complex) vector space $g_e \times g_e$:

\[(21.5.3.1) \quad B_U: (u, v) \mapsto \text{Tr}(U_*(u) \circ U_*(v)).\]

From the symmetry $\text{Tr}(PQ) = \text{Tr}(QP)$ of the trace it follows that the form $B_U$ is symmetric, but it can be degenerate. Furthermore, it is invariant under the action $(s, u) \mapsto \text{Ad}(s) \cdot u$ of $G$ on $g_e$: for by (16.5.4) and (19.2.1.1) we have

\[
U_*(\text{Ad}(s) \cdot u) = \text{Ad}(U(s)) \cdot U_*(u) = U(s)U_*(u)U(s)^{-1},
\]

and the relation

\[(21.5.3.2) \quad B_U(\text{Ad}(s) \cdot u, \text{Ad}(s) \cdot v) = B_U(u, v)\]

therefore follows from the symmetry of the trace.

(21.5.4) In general, let $\Phi$ be any $\mathbb{R}$-bilinear mapping of $g_e \times g_e$ into a real vector space $E$ that is invariant under the action $(s, u) \mapsto \text{Ad}(s) \cdot u$ of $G$ on $g_e$; then, for all $u, v, w$ in $g_e$, we have

\[(21.5.4.1) \quad \Phi([w, u], v) + \Phi(u, [w, v]) = 0.\]

For by hypothesis we have, for all $t \in \mathbb{R}$,

\[
\Phi(\text{Ad}(\exp(tw)) \cdot u, \text{Ad}(\exp(tw)) \cdot v) = \Phi(u, v);
\]

if we now differentiate both sides of this relation with respect to $t$ at $t = 0$, we obtain (21.5.4.1) by use of (8.1.4) and (19.11.2.2).

(21.5.5) More generally, if $a$ is a Lie algebra over $\mathbb{R}$ (resp. $\mathbb{C}$) and $F$ is a finite-dimensional vector space over $\mathbb{R}$ (resp. $\mathbb{C}$), then to each Lie algebra homomorphism $\rho: a \to \mathfrak{gl}(F)$ we may associate a symmetric bilinear $\mathbb{R}$-form (resp. $\mathbb{C}$-form) on $a \times a$ by the formula

\[(21.5.5.1) \quad B_\rho(u, v) = \text{Tr}(\rho(u) \circ \rho(v)).\]
Since $\rho([u, v]) = \rho(u) \circ \rho(v) - \rho(v) \circ \rho(u)$, the symmetry property of the trace shows again that we have

\[(21.5.5.2) \quad B_\rho(ad(w) \cdot u, v) + B_\rho(u, ad(w) \cdot v) = 0\]

for all $u, v, w \in \mathfrak{a}$.

(21.5.6) Consider a finite-dimensional real or complex Lie algebra $\mathfrak{a}$, and its adjoint representation $u \mapsto ad(u)$, which is a homomorphism of $\mathfrak{a}$ into $\mathfrak{gl}(\mathfrak{a})$. We denote by $B_\mathfrak{a}$ or simply $B$ the symmetric bilinear form corresponding to this homomorphism according to (21.5.5); it is called the Killing form of the Lie algebra $\mathfrak{a}$. By (21.5.5.2) we have

\[(21.5.6.1) \quad B([w, u], v) + B(u, [w, v]) = 0.\]

If $\sigma$ is any automorphism of the Lie algebra $\mathfrak{a}$, we have $\sigma([u, v]) = [\sigma(u), \sigma(v)]$, or equivalently $\sigma \circ ad(u) = ad(\sigma(u)) \circ \sigma$ in $\text{End}(\mathfrak{a})$. From this and the symmetry of the trace we deduce immediately that

\[(21.5.6.2) \quad B(\sigma(u), \sigma(v)) = B(u, v).\]

(21.5.7) If $b$ is an ideal in a Lie algebra $\mathfrak{a}$, the restriction to $b \times b$ of the Killing form $B_\mathfrak{a}$ is the Killing form $B_b$.

By hypothesis, for each $x \in b$, we have $ad(x) \cdot b \subset b$; hence, for $x$ and $y \in b$, if we put $U = ad(x) \cdot ad(y)$, we have $U(a) \subset b$. If we now calculate the trace of $U$ by means of a basis of $\mathfrak{a}$ consisting of a basis of $b$ and a basis of a subspace of $\mathfrak{a}$ supplementary to $b$, we see that this trace is equal to that of the restriction of $U$ to $b$.

It should be remarked, however, that there is no simple relation between the Killing form of an arbitrary Lie subalgebra of $\mathfrak{a}$, and the restriction to this subalgebra of the Killing form of $\mathfrak{a}$.

(21.5.8) If $G$ is a (real or complex) Lie group, $\mathfrak{g}_e$ its Lie algebra, the Killing form of $\mathfrak{g}_e$ is called the Killing form of $G$.

(21.5.9) Let $G$ be a connected Lie group with center $\{e\}$, and let $U$ be a linear representation of $G$ on a finite-dimensional vector space, such that the bilinear form $B_U$ is nondegenerate. Then there exists a pseudo-Riemannian structure on $G$ whose metric tensor $g$ satisfies $g(e) = B_U$, and which is invariant under left and right translations by elements of $G$ (20.11.8).
6. SEMISIMPLE LIE GROUPS. CRITERION OF SEMISIMPLICITY FOR A COMPACT LIE GROUP

(21.6.1) A finite-dimensional real or complex Lie algebra \( a \) is said to be \emph{semisimple} if its Killing form (21.5.6) is \emph{nondegenerate}. A real or complex Lie group is said to be \emph{semisimple} if its Lie algebra is semisimple.

If \( a \) is a finite-dimensional real Lie algebra, any basis of \( a \) over \( \mathbb{R} \) can be canonically identified with a basis of its complexification \( a_{\mathbb{C}} \) over \( \mathbb{C} \). Consequently, the Killing form \( B_{a_{\mathbb{C}}} \) of \( a_{\mathbb{C}} \) has the same matrix relative to this basis as does the Killing form \( B_a \). It follows immediately that if \( a \) is semisimple, so also is its complexification, and conversely.

On the other hand, if \( a \) is a complex Lie algebra and \( a_{\mathbb{R}} \) the real Lie algebra obtained from \( a \) by restriction of scalars, then we have \( B_{a_{\mathbb{R}}} = 2 \mathcal{R}(B_a) \). For if \( u \) is an endomorphism of a finite-dimensional complex vector space \( E \), and if \( u_0 \) is the same mapping \( u \) considered as an \( \mathbb{R} \)-linear mapping, then it is easy to verify that \( \text{Tr}(u_0) = 2 \mathcal{R}(\text{Tr}(u)) \) (16.21.13.1). Hence it follows that if \( a \) is semisimple, so also is \( a_{\mathbb{R}} \); for by taking a basis of \( a \) that is orthogonal relative to \( B_a \), we see from the remarks above that \( B_{a_{\mathbb{R}}} \) has signature \( (n, n) \) if \( n = \dim_{\mathbb{C}}(a) \), and therefore is nondegenerate.

(21.6.2) Let \( a \) be a real or complex semisimple Lie algebra.

(i) The only commutative ideal in \( a \) is the zero ideal.

(ii) For each ideal \( b \) in \( a \), the subspace \( b^\perp \) of \( a \) orthogonal to \( b \) with respect to the Killing form \( B_a \) is an ideal of \( a \), supplementary to \( b \), and the Lie algebras \( b \) and \( b^\perp \) are semisimple.

(i) Let \( c \) be a commutative ideal in \( a \). For each \( y \in a \), we have \( \text{ad}(y) \cdot c = c \) and therefore \( \text{ad}(x) \cdot (\text{ad}(y) \cdot c) = 0 \) for all \( x \in c \). On the other hand, \( \text{ad}(x) \cdot (\text{ad}(y) \cdot a) \subseteq c \), because \( x \in c \). If we compute the trace of \( U = \text{ad}(x) \circ \text{ad}(y) \) with the help of a basis of \( a \) consisting of a basis of \( c \) and a basis of a subspace supplementary to \( c \), it follows that we obtain 0: in other words, \( B_a(x, y) = 0 \) for all \( x \in c \) and \( y \in a \). Since \( B_a \) is nondegenerate, this forces \( x = 0 \).

(ii) It follows immediately from (21.5.6.1) that if \( b \) is an ideal in \( a \), then so also is \( b^\perp \). Hence \( b \cap b^\perp \) is an ideal in \( a \), and we shall show that it is \emph{commutative}. Indeed, if \( u, v \) are any two elements of \( b \cap b^\perp \), then by (21.5.6.1) we have \( B_a([w, [u, v]]) = B_a([w, u], v) = 0 \) for all \( w \in a \), because \( [w, u] \in b \) and \( v \in b^\perp \). Since \( B_a \) is nondegenerate, it follows that \( [u, v] = 0 \), which proves our assertion. Hence, by virtue of (i) above, we have \( b \cap b^\perp = \{0\} \) and therefore \( b + b^\perp = a \), so that \( b \) and \( b^\perp \) are supplementary ideals. The restrictions of \( B_a \) to the nonisotropic subspaces \( b \) and \( b^\perp \) are
therefore nondegenerate, so that \( b \) and \( b^\perp \) are semisimple Lie algebras, by virtue of (21.5.7).

We shall show later that, conversely, a finite-dimensional real or complex Lie algebra that has no nonzero commutative ideals is semisimple (21.22.4).

From (21.6.2) it follows immediately that:

(21.6.3) The center of a semisimple Lie algebra is \( \{0\} \).

In particular (19.11.9), every semisimple Lie algebra over \( \mathbb{R} \) (resp. \( \mathbb{C} \)) is the Lie algebra of a real (resp. complex) semisimple Lie group, and there is a one-to-one correspondence between semisimple Lie algebras and simply connected semisimple Lie groups (up to isomorphism).

A finite-dimensional real or complex Lie algebra is said to be simple if it is noncommutative and if it contains no ideals other than itself and \( \{0\} \).

It can be shown that if \( a \) is a simple Lie algebra over \( \mathbb{C} \), then the Lie algebra \( a_{\mathbb{R}} \) obtained by restriction of scalars is also simple (Problem 1). On the other hand, if \( g \) is a simple Lie algebra over \( \mathbb{R} \), then the Lie algebra \( g_{\mathbb{C}} \) over \( \mathbb{C} \) obtained by extension of scalars is semisimple, but not necessarily simple (Problem 1).

(21.6.4) Every semisimple Lie algebra \( g \) is the direct sum of a finite number of ideals \( g_i \) (1 \( \leq \) i \( \leq \) r), each of which is a simple Lie algebra, and which are mutually orthogonal with respect to \( B_\mathfrak{a} \). Every ideal of \( g \) is the direct sum of a subfamily of \( (g_i)_{1 \leq i \leq r} \).

The proof is by induction on the dimension of \( g \). Let \( a \) be a nonzero ideal of \( g \) of smallest possible dimension; by virtue of (21.6.2), \( g \) is the direct sum of \( a \) and the ideal \( a^\perp \), which implies that \( [a, a^\perp] = \{0\} \). Every ideal in the Lie algebra \( a \) is therefore also an ideal in \( g \), and therefore by hypothesis the Lie algebra \( a \) contains no ideals other than itself and \( \{0\} \). Since moreover \( a \) is not commutative (21.6.2), it is a simple Lie algebra. By applying the inductive hypothesis to the semisimple Lie algebra \( a^\perp \), the first assertion is established.

If now \( b \) is any ideal in \( g \), then \( b \cap g_i \) is an ideal in \( g_i \), hence is either \( g_i \) or \( \{0\} \). If \( a \) is the sum of the \( g_i \) contained in \( b \), then \( a^\perp \) is the sum of the remaining \( g_i \), and we have \( b = a \oplus c \), where \( c = b \cap a^\perp \). Since \( b \cap g_i = \{0\} \) for each \( g_i \subset a^\perp \), we have also \( [b, g_i] = \{0\} \) for these \( g_i \), hence \( [b, a^\perp] = \{0\} \) and so a fortiori \( [c, c] = \{0\} \). But since the Lie algebra \( a^\perp \) is semisimple, it has no nonzero commutative ideals (21.6.2), so that \( c = 0 \) and therefore \( b = a \).

(21.6.5) Every semisimple Lie algebra \( g \) is equal to its derived algebra \( \mathfrak{D}(g) \).
This is obvious if \( g \) is simple, because by definition \( \mathfrak{D}(g) \) cannot be zero. The general case now follows from (21.6.4).

(21.6.5.1) With the notation of the proof of (21.6.4), the ideals \( a \) and \( a^\perp \) are orthogonal relative to any invariant symmetric \( \mathbb{R} \)-bilinear form \( \Phi \) on \( g \) (21.5.4). For, by virtue of (21.6.5), it is enough to show that for \( a \neq 0 \), \( x, y \in a \) and \( z \in a^\perp \) we have \( \Phi([x, y], z) = 0 \); but by (21.5.4.1) this is equivalent to \( \Phi(x, [y, z]) = 0 \), and since \( y \in a \) and \( z \in a^\perp \) we have \([y, z] \in a \cap a^\perp = \{0\}\).

(21.6.6) A Lie group is said to be almost simple if its Lie algebra is simple. It follows from (21.6.4) that a simply connected semisimple Lie group \( G \) is isomorphic to a product of simply connected almost simple Lie groups \( G_j \). The only connected Lie groups immersed in \( G \) that are normal in \( G \) and of positive dimension are the products of subfamilies of the \( G_j \); they are closed in \( G \). It follows from (21.6.3) that the center of a semisimple Lie group is discrete, and from (21.6.5) that the commutator subgroup of a semisimple Lie group is an open subgroup (19.7.1).

This last result shows in particular that a connected semisimple Lie group \( G \) is unimodular, since the kernel of the modulus function \( s \mapsto \Delta_G(s) \) contains the commutator subgroup of \( G \).

(21.6.7) Every derivation (A.18.2) of a semisimple Lie algebra \( g \) is inner (A.19.4).

Let \( \mathcal{D} = \text{Der}(g) \) be the Lie algebra of derivations of \( g \) (A.19). Since the center of \( g \) is \( \{0\} \) (21.6.3), the image \( \text{ad}(g) \) of \( g \) under the adjoint representation \( x \mapsto \text{ad}(x) \) is a Lie subalgebra isomorphic to \( g \), and therefore semisimple; moreover, since \( \text{ad}(D)u = [D, \text{ad}(u)] \) for \( u \in g \) and \( D \in \mathcal{D} \) (A.19.4), \( \text{ad}(g) \) is an ideal of \( \mathcal{D} \). Consider the subspace \( a \) of \( \mathcal{D} \) that is orthogonal to \( \text{ad}(g) \) relative to the Killing form \( B_\mathcal{D} \) (which a priori might be degenerate). Since the restriction of \( B_\mathcal{D} \) to the ideal \( \text{ad}(g) \) is the Killing form \( B_{\text{ad}(g)} \) (21.5.6), and since this form is nondegenerate, it follows that the intersection \( a \cap \text{ad}(g) \), which is the subspace of \( \text{ad}(g) \) orthogonal to \( \text{ad}(g) \) relative to \( B_{\text{ad}(g)} \), is zero. Also, by (21.5.6.1), \( a \) is an ideal of \( \mathcal{D} \), and therefore \( [a, \text{ad}(g)] \subseteq a \cap \text{ad}(g) = \{0\} \). Consequently, for \( D \in a \) and \( u \in g \), we have \( \text{ad}(Du) = [D, \text{ad}(u)] = 0 \), and since the mapping \( x \mapsto \text{ad}(x) \) is injective, it follows that \( Du = 0 \), hence \( D = 0 \) and so \( a = \{0\} \). This proves that \( B_\mathcal{D} \) is nondegenerate and that \( \mathcal{D} = \text{ad}(g) \).

(21.6.8) Let \( G \) be a connected semisimple (real or complex) Lie group. Then the image \( \text{Ad}(G) \) of \( G \) under the homomorphism \( s \mapsto \text{Ad}(s) \) is an open subgroup of the group \( \text{Aut}(g) \) of automorphisms of the Lie algebra of \( G \).
For this image is a connected Lie group immersed in Aut(\(g_\omega\)), whose Lie algebra is ad(\(g_\omega\)) (19.13.9); but the latter is equal to the Lie algebra Der(\(g_\omega\)) of Aut(\(g_\omega\)) by virtue of (21.6.7) and (19.3.8). Hence the result, by (19.7.1).

(21.6.9) Let \(G\) be a connected (real) Lie group, \(C\) its center and \(g\) its Lie algebra. The following conditions are equivalent:

(a) The quotient group \(G/C\) is compact.
(b) \(G\) is isomorphic to a product \(\mathbb{R}^n \times G_1\), where \(G_1\) is compact.
(c) The Lie group \(\tilde{G}\), the universal covering of \(G\), is isomorphic to a product \(\mathbb{R}^n \times K\), where \(K\) is a simply connected semisimple compact group.
(d) The Lie algebra \(g\) is the direct sum \(c \oplus \mathcal{D}(g)\) of its center \(c\) and its derived algebra \(\mathcal{D}(g)\), and the restriction to \(\mathcal{D}(g)\) of the Killing form \(B_\eta\) is negative definite.

When these equivalent conditions are satisfied, \(\mathcal{D}(g)\) is isomorphic to the Lie algebra of \(K\); the center \(Z\) of \(K\) is finite; \(G\) is isomorphic to \(\tilde{G}/D\), where \(D\) is a discrete subgroup of \(\mathbb{R}^n \times Z\); the center \(C\) of \(G\) is isomorphic to \((\mathbb{R}^n \times Z)/D\); and the center of \(G/C\) consists only of the identity element. The subgroups Ad(\(\tilde{G}\)), Ad(\(G\)), and Ad(\(K\)) of \(Aut(g)\) may be identified with the same (compact) open subgroup of \(Aut(\mathcal{D}(g))\) (itself a direct factor of \(Aut(g)\)), and are isomorphic to \(G/C\) and to \(K/Z\).

The commutator subgroup \(\mathcal{D}(K)\) of \(K\) is equal to \(K\), and the commutator subgroup \(\mathcal{D}(G)\) of \(G\) may be identified with the group \(K/(D \cap Z)\) (and is therefore compact).

Clearly (b) implies (a). We shall first prove that (a) implies (d).

The homomorphism \(s \mapsto Ad(s)\) of \(G\) into \(Aut(g) \subset GL(g)\) has kernel \(C\) (19.11.6) and therefore factorizes as \(G \rightarrow G/C \rightarrow Aut(g)\), where \(v\) is an injective homomorphism of Lie groups (16.10.9). If \(G/C\) is compact, then so also is its image Ad(\(G\)) under \(v\), and \(v\) is therefore an isomorphism of \(G/C\) onto the compact Lie subgroup Ad(\(G\)) of \(Aut(g)\) ((19.10.1) and (16.9.9)). Hence, by (20.11.3.1), there exists a positive definite symmetric bilinear form \(\Phi\) on the vector space \(g\) that is invariant under the canonical action of Ad(\(G\)) on \(g\). It is clear that \(Ad(s) \cdot c = \{0\}\) for all \(s \in G\) (19.11.6); the subspace \(c^\perp\) of \(g\), which is the orthogonal supplement of \(c\) relative to \(\Phi\), is therefore also stable under every automorphism Ad(\(s\)) of \(g\), hence is an ideal in \(g\) (19.11.3). But since Ad(\(G\)) may be canonically identified with a closed subgroup of the orthogonal group \(O(\Phi)\), its Lie algebra ad(\(g\)) is identified with a Lie subalgebra of the Lie algebra \(o(\Phi)\) of \(O(\Phi)\). Relative to a basis of \(g\) that is orthonormal with respect to \(\Phi\), the matrix \((\alpha_{jk})\) of the endomorphism ad(\(u\))
of \( g \), where \( u \) is any element of \( g \), satisfies \( \alpha_{kj} = -\alpha_{jk} \) (19.4.4.3). It follows that

\[
B_g(u, u) = \text{Tr}((\text{ad}(u))^2) = \sum_{j,k} \alpha_{jk} \alpha_{kj} = -\sum_{j,k} \alpha_{jk}^2 \leq 0;
\]

and, moreover, that we have \( B_g(u, u) = 0 \) only if \( \text{ad}(u) = 0 \), hence if \( u \in c \).

The restriction of \( B_g \) to the ideal \( c' \) is therefore negative definite. By virtue of (21.5.7), this shows that the Lie algebra \( c' \) is semisimple, hence equal to its derived algebra (21.6.5); and since \([c, g] = \{0\}\) by definition, we have also \( \mathcal{D}(g) = [g, g] = c' \).

Next we shall prove that (d) implies (c). Clearly it is enough to show that if \( \mathfrak{l} \) is a semisimple real Lie algebra, such that the Killing form \( B_\mathfrak{l} \) is negative definite, then a simply connected Lie group \( K \) whose Lie algebra is isomorphic to \( \mathfrak{l} \) (21.6.3) is necessarily compact. Now, since \( B_\mathfrak{l} \) is invariant under the adjoint action of \( K \) on \( \mathfrak{l} \), the subgroup \( \text{Ad}(K) \) of \( \text{Aut}(\mathfrak{l}) \), which is closed (21.6.8), may be identified with a closed subgroup of the orthogonal group \( O(B_\mathfrak{l}) \), hence is compact (16.11.2). On the other hand, the Lie algebra \( \text{ad}(\mathfrak{l}) \) of \( \text{Ad}(K) \) is isomorphic to \( \mathfrak{l} \) and therefore has center \( \{0\} \) (21.6.3). Hence the center of \( \text{Ad}(K) \) is discrete, and it follows from Weyl's theorem (20.22.5) that the Lie group \( K \), which is the universal covering of \( \text{Ad}(K) \), is also compact.

We go on to prove the assertions in the second and third paragraphs of (21.6.9). From (16.30.2.1) we have \( G = \tilde{G}/D \), where \( D \) is a discrete subgroup of the center \( \mathbb{R}^n \times Z \) of \( \tilde{G} = \mathbb{R}^n \times K \). In view of (21.6.8) and the fact that every automorphism of \( g \) leaves \( c \) and \( \mathcal{D}(g) \) stable, these assertions (except for those relating to the derived groups) follow from (20.22.5.1). The derived group \( \mathcal{D}(K) \) has Lie algebra \( \mathcal{D}(\mathfrak{l}) = \mathfrak{l} \) (19.12.1), and because \( K \) is connected it follows that \( \mathcal{D}(K) = K \). We deduce that \( \mathcal{D}((\tilde{G})) = K \), and since \( \mathcal{D}(G) \) is evidently the canonical image of \( \mathcal{D}(\tilde{G}) \), it is therefore equal to the canonical image of \( K \), which is isomorphic to \( K/(D \cap K) = K/(D \cap Z) \) (12.12.5).

Finally, we shall prove that (c) implies (b). Let \( p \) be the order of the center \( Z \) of \( K \). The projection of the group \( D \) on \( \mathbb{R}^n \) is a discrete group, because the inverse image in \( \mathbb{R}^n \times Z \) of a compact neighborhood of \( 0 \) in \( \mathbb{R}^n \) is a compact set, and therefore intersects \( D \) in a finite set. It follows (19.7.9.1) that \( D \) is finitely-generated, and hence the set of \( z^n \) as \( z \) runs through \( D \) is a subgroup \( D' \) of \( D \cap \mathbb{R}^n \), of finite index in \( D \) (and \textit{a fortiori} in \( D \cap \mathbb{R}^n \)). By (19.7.9.1), the group \( \mathbb{R}^n/D' \) is therefore isomorphic to a product \( \mathbb{R}^m \times \mathbb{T}^{n-m} \), and hence \( \tilde{G}/D' \) is isomorphic to \( \mathbb{R}^m \times G' \), where \( G' = \mathbb{T}^{n-m} \times K \) is compact. Furthermore, \( D/D' \) is a finite subgroup of the center of \( \tilde{G}/D' \), and since \( \mathbb{R}^n \) has no finite subgroup other than \( \{0\} \), it follows that \( D/D' \) may be identified with a finite subgroup \( C' \) of the center of \( G' \). Hence \( \tilde{G}/D \), being isomorphic to \( (\tilde{G}/D')/(D/D') \), is isomorphic to \( \mathbb{R}^m \times G_1 \), where \( G_1 = G'/C' \) is compact.
Remarks

(21.6.10) (i) Since \( \{0\} \) is the only compact subgroup of \( \mathbb{R}^n \), the subgroup \( G_1 \) of \( G = \mathbb{R}^n \times G_1 \) is a maximal compact subgroup of \( G \).

(ii) If a real Lie algebra \( g \) satisfies condition (d) of (21.6.9), it is isomorphic to the Lie algebra of a compact connected Lie group, namely the group \( T^n \times K \) (in the notation of (21.6.9)). It follows that this condition characterizes the Lie algebras of compact connected Lie groups. Since the Lie algebra \( \mathcal{D}(g) \) is semisimple, it is equal to its derived algebra. The same argument as in (21.6.5.1) then shows that \( c \) and \( \mathcal{D}(g) \) are orthogonal with respect to any invariant \( \mathbb{R} \)-bilinear form on \( g \).

(iii) The discrete subgroups of the group \( \mathbb{R}^n \times \mathbb{Z} \) are easily determined (Problem 7), and therefore the structure of compact connected Lie groups is essentially reduced to that of simply connected semisimple compact Lie groups.

(iv) It can be shown (Section 21.11, Problem 12(b)) that, under the conditions of (21.6.9), the group \( \text{Ad}(K) \) is of finite index in \( \text{Aut}(K) \), and the latter is therefore compact.

(v) In view of (19.16.4.3), a connected Lie group \( G \) is unimodular if and only if \( \text{Ad}(G) \) is unimodular. Since every compact group is unimodular (14.3.3), it follows from (21.6.9) that every connected Lie group \( G \), such that the quotient of \( G \) by its center is compact, is unimodular.

PROBLEMS

1. (a) Let \( a \) be a simple Lie algebra over \( \mathbb{C} \). Show that the Lie algebra \( a_{\mathbb{R}} \) over \( \mathbb{R} \) is simple. (Observe that if \( b \) is an ideal in the semisimple Lie algebra \( a_{\mathbb{R}} \), then \( [a, b] = b \).

(b) Let \( a \) be a simple Lie algebra over \( \mathbb{R} \). Show that the Lie algebra \( a_{\mathbb{C}} \) over \( \mathbb{C} \) is either simple or the direct sum of two isomorphic simple algebras. (Let \( c \) be the semilinear bijection of \( a_{\mathbb{C}} = a \oplus ia \) onto itself such that \( c(x + iy) = x - iy \) for all \( x, y \in a \). Show first that if \( V \) is a complex vector subspace of \( a_{\mathbb{C}} \) such that \( c(V) = V \), and if \( W = a \cap V \), then \( V = W \oplus iW \). Deduce that if \( b \) is an ideal of \( a_{\mathbb{C}} \) other than \( a \), then we have

\[
b \cap c(b) = \{0\}, \quad b \cap a = \{0\}, \quad a_{\mathbb{C}} = b \oplus c(b),
\]

and that \( b \) is a simple Lie algebra over \( \mathbb{C} \).

(c) Let \( a \) be a simple Lie algebra over \( \mathbb{C} \). Show that the Lie algebra \( (a_{\mathbb{R}})_{\mathbb{C}} \) over \( \mathbb{C} \) is the direct sum of two simple Lie algebras, each isomorphic to \( a \). (For each \( x \in a \), consider the element \( \frac{1}{2}(x \otimes 1 + (ix) \otimes i) \in (a_{\mathbb{R}})_{\mathbb{C}} \).)

2. (a) In order that a finite-dimensional real Lie algebra \( g \) should be the Lie algebra of a compact Lie group, it is necessary and sufficient that for each \( u \in g \) the endomorphism \( \text{ad}(u) \otimes 1 \) of \( g_{\mathbb{C}} \) be diagonalizable and that its eigenvalues be pure imaginary. (Argue as in (21.6.9).)
6. SEMISIMPLE LIE GROUPS

(b) Deduce from (a) that if \( g \) is the Lie algebra of a compact group, then every Lie subalgebra \( \mathfrak{h} \) of \( g \) is also the Lie algebra of a compact group; in particular, \( \mathfrak{h} \) cannot be solvable unless \( \mathfrak{h} \) is commutative.

3. Show that the Killing form of a real Lie algebra \( g \) of positive finite dimension cannot be positive definite. (Use Problem 2, by noting that \( \text{ad}(u) \otimes i \) is a self-adjoint endomorphism relative to the form \( B_{ac} \).)

4. (a) Let \( g \) be a real or complex Lie algebra, \( \mathfrak{h} \) a semisimple ideal of \( g \). Show that \( g \) is the direct sum of \( \mathfrak{h} \) and the centralizer \( Z(h) \) of \( h \). (Use (21.6.7).)
   (b) Let \( g \) be the Lie algebra of a compact Lie group and let \( n \) be an ideal in \( g \). If \( c \) is the center of \( g \), show that
   \[
   n = (n \cap c) \oplus (n \cap Z_g)
   \]
   (consider the Killing form of \( n \)), and deduce that there exists an ideal \( n' \) in \( g \) such that \( g = n \oplus n' \).
   (c) Let \( g \) be a real Lie algebra and \( n \) an ideal in \( g \); suppose that \( n \) and \( g/n \) are the Lie algebras of compact Lie groups. Show that \( g \) is the Lie algebra of a compact group if and only if \( g \) is the direct sum of \( n \) and another ideal. (Use (b).)

5. (a) Let \( G \) be a connected Lie group, \( g \) its Lie algebra, \( \mathfrak{h} \) a semisimple subalgebra of \( g \), and \( H \) the connected Lie group immersed in \( G \) corresponding to \( \mathfrak{h} \). Show that if the center of \( H \) is finite, then \( H \) is closed in \( G \). (Use Section 19.11, Problem 4.) (Cf. Section 21.18, Problem 18.)
   (b) Let \( G \) be a connected, almost simple, noncompact Lie group with finite center. Show that there exists no nontrivial continuous unitary linear representation of \( G \) on a finite-dimensional complex vector space.

6. (a) Let \( g \) be a finite-dimensional (real or complex) Lie algebra. Show that the sum \( a \) of all the semisimple ideals of \( g \) is a semisimple ideal of \( g \) (and hence is the unique largest semisimple ideal of \( g \)), and deduce that the number of semisimple ideals of \( g \) is finite.
   (b) Use (a) and Section 21.2, Problem 7, to show that in a compact Lie group \( G \) the number of conjugacy classes of connected semisimple Lie subgroups of \( G \) is finite.

7. Let \( A \) be a finite commutative group. Then every discrete subgroup of \( \mathbb{R}^n \times A \) is of the form \( EB \) (isomorphic to \( E \times B \)), where \( B \) is a subgroup of \( A \), and \( E \) is a subgroup of \( \mathbb{R}^n \times A \) such that the restriction to \( E \) of the projection \( \mathbb{R}^n \times A \to \mathbb{R}^n \) is an isomorphism of \( E \) onto a discrete subgroup of \( \mathbb{R}^n \) (hence isomorphic to \( \mathbb{Z}^p \) for some \( p \leq n \)).

8. Let \( G \) be a Lie group for which the number of connected components is finite, and let \( G_0 \) be the identity component of \( G \). Suppose that \( \text{Lie}(G) = \text{Lie}(G_0) = g \) is the Lie algebra of a compact group. Show that \( G \) is the semidirect product of a maximal compact subgroup \( K \) and a normal subgroup \( V \) isomorphic to \( \mathbb{R}^m \) for some \( m \); also that \( K \cap G_0 \) is the identity component of \( K \), and that \( G_0 \) is the direct product of \( K \cap G_0 \) and \( V \). (Use (21.6.9) and the fact that the group \( \text{Ad}(G) \) is compact. By considering a scalar product on \( g \) that is invariant under \( \text{Ad}(G) \), we may assume that in the decomposition \( G_0 = V \times K_0 \) of \( G_0 \) as the direct product of a subgroup \( V \) isomorphic to \( \mathbb{R}^m \) and a compact connected group \( K_0 \), the Lie algebra of \( V \) is orthogonal to that of \( K_0 \) for the scalar product in question, and hence that \( V \) is a normal subgroup of \( G_0 \). Then use Section 19.14, Problem 3.) Under what conditions is the subgroup \( K \) (resp. \( V \)) above unique?
9. Let $N$ be the nilpotent Lie group consisting of all $3 \times 3$ matrices $(x_{ij})$ such that $x_{ij} = 0$ if $i < j$ and $x_{ii} = 1$ for $i = 1, 2, 3$. Let $G_1$ be the closed subgroup of $N$ consisting of the matrices $(x_{ij})$ for which $x_{12}$ and $x_{23}$ are rational integers, and let $H_1$ be the subgroup of $G_1$ consisting of the $(x_{ij})$ for which $x_{12} = x_{23} = 0$ and $x_{13}$ is a rational integer. Show that the Lie group $G_1/H_1$ has infinitely many connected components; its center $Z$, which is also its commutator subgroup, is compact and connected, and is also the identity component of $G$, and is the largest compact subgroup of $G$; but $G$ is not the semidirect product of $Z$ with any other subgroup.

10. Let $G$ be a connected Lie group. Define inductively $\mathcal{D}^0(G) = G$, and $\mathcal{D}^p(G)$ to be the closure of the commutator subgroup of $\mathcal{D}^{p-1}(G)$ for $p \geq 1$. Show that if $\mathcal{D}^p(G)$ is compact, then $\mathcal{D}^{p+1}(G)$ is compact and semisimple, and that $G = \mathcal{D}^{p+1}(G) \cdot H$, where $H$ is the identity component of the centralizer of $\mathcal{D}^{p+1}(G)$ in $G$. The group $\mathcal{D}^{p+1}(G) \cap H$ is finite and commutative, and $\mathcal{D}^p[H]$ is contained in the identity component of the center of $H$. Show that the connected Lie group $N/H_1 = G_2$ (in the notation of Problem 9) is such that $\mathcal{D}(G_2)$ is compact, but that the Lie algebra of $G_2$ is not the Lie algebra of a compact group.

11. (a) Let $G$ be a connected Lie group, $\mathfrak{g}$ its Lie algebra. Show that if the closure of $\text{Ad}(G)$ in $\text{Aut}(\mathfrak{g})$ is compact, then the quotient of $G$ by its center is compact, and consequently $\text{Ad}(G)$ is compact. (Observe that there exists an $\text{Ad}(G)$-invariant scalar product on $\mathfrak{g}$.)

(b) In order that a connected Lie group $G$ should be such that the quotient of $G$ by its center is compact, it is necessary and sufficient that for each neighborhood $U$ of $e$ in $G$ there should exist a neighborhood $V \subset U$ of $e$ such that $xVx^{-1} = V$ for all $x \in G$. (The condition is necessary by (21.3.4.1). To show that it is sufficient, use (a) above, by proving that the closure of $\text{Ad}(G)$ in $\text{End}(\mathfrak{g})$ is contained in $\text{Aut}(\mathfrak{g})$.)

12. Let $G$ be a nondiscrete, almost simple Lie group, and $G_0$ its identity component. Show that each normal subgroup $N$ of $G$ either contains $G_0$ or is contained in the centralizer $\mathcal{Z}(G_0)$ of $G_0$, which is the largest discrete normal subgroup of $G$. In particular, if $G$ is compact, then $\mathcal{Z}(G_0)$ is finite, and there are only finitely many elements $s \in G$ such that $\text{Ad}(s)$ is the identity mapping.

13. Let $G$ be an almost simple compact Lie group of dimension $n \geq 1$. For each $s \in G$, each integer $m \geq 1$ and each neighborhood $V$ of $e$ in $G$, let $M(s, m, V)$ denote the set of elements of $G$ of the form

$$(x_1(y_1, s)x_1^{-1})(x_2(y_2, s)x_2^{-1}) \cdots (x_n(y_n, s)x_n^{-1})$$

where $x_1, \ldots, x_m, y_1, \ldots, y_m$ belong to $V$.

(a) Show that if $s \in G$ is such that $\text{Ad}(s)$ is not the identity mapping of the Lie algebra $\mathfrak{g}$ of $G$, and if $m \geq n$, then for each neighborhood $V$ of $e$ the set $M(s, m, V)$ is a neighborhood of $e$. (There exists a vector $a \in \mathfrak{g}$ such that $b = \text{Ad}(s) \cdot a - a \neq 0$. Show that there exist elements $x_1, \ldots, x_m$ in $V$ such that the sequence $(\text{Ad}(x_1) \cdot b)_{1 \leq j \leq m}$ contains a basis of $\mathfrak{g}$. Then consider the mapping

$$(z_1, \ldots, z_m, y_1, \ldots, y_m) \mapsto (z_1(y_1, s)z_1^{-1}) \cdots (z_m(y_m, s)z_m^{-1})$$

of $G^{2m}$ into $G$, and its tangent linear mapping at the point $(x_1, \ldots, x_m, e, \ldots, e)$.)

(b) Let $U$ be a neighborhood of $e$ in $G$ and let $m$ be an integer $\geq 1$. Show that there exists an element $s \in G$ such that $\text{Ad}(s)$ is not the identity mapping and such that
Let $G$ be a compact connected Lie group of dimension $n$, and let $(u, v)$ be a scalar product on the Lie algebra $\mathfrak{g}_e$, invariant under the operators $\text{Ad}(s)$ for all $s \in G$ (20.11.3.1); also let $||u||^2 = (u, u)$. This scalar product induces canonically a Riemannian metric tensor $g$ on $G$, invariant under left and right translations (20.11.8), and for which the geodesic trajectories are the left-translates of the one-parameter subgroups.

(a) Let $t \mapsto x(t) = \exp(tu)$ be a geodesic passing through $e$, and let $y \in G$. Put $z(t) = x(t)yx(-t)$. Show that

$$z'(t) = -x(t)y \cdot ((1_{\mathfrak{g}_e} - \text{Ad}(y^{-1})) \cdot u) \cdot x(-t)$$

(Use (16.9.9) and the relations $x'(t) = x(t)u = u \cdot x(t)$ (19.11.2.2)). Deduce that

$$||z'(t)||_g = ||(1_{\mathfrak{g}_e} - \text{Ad}(y^{-1})) \cdot u||.$$

(b) By means of the scalar product $(u, v)$, the group $\text{Ad}(G)$ may be identified with a subgroup of $O(n) \subset U(n)$. Consider on $U(n)$ the function $s \mapsto \theta(s)$ defined in Section 16.11, Problem 1. For each $x \in G$ put $\delta(x) = \theta(\text{Ad}(x))$; then we have $0 \leq \delta(x) \leq \pi$, and

$$\delta(x^{-1}) = \delta(x), \quad \delta(yxy^{-1}) = \delta(x), \quad \delta(xy) \leq \delta(x) + \delta(y)$$

for all $x, y \in G$, and $\delta(xz) = \delta(x)$ for all $z$ in the center of $G$.

Let $d(x, y)$ be the Riemannian distance on $G$ defined by the metric tensor $g$ (20.16.3). Show that for any two points $x, y \in G$ we have

$$d(e, (x, y)) \leq (2 \sin \frac{1}{2} \delta(y)) \cdot d(e, x).$$

(Join $e$ to $x$ by a geodesic arc of length $d(e, x)$ (20.18.5), and then use (a) above and the definition of $\theta(s)$ in Section 16.11, Problem 1.)

15. Let $G$ be an almost simple connected Lie group, $N$ an arbitrary normal subgroup of $G$.

(a) Consider the Lie subalgebra $\mathfrak{n}_e = \text{Lie}(G)$ associated with $N$ by the procedure of Section 19.11, Problem 7(b). Show that if $N \neq G$, we have $\mathfrak{n}_e = \{0\}$.

(b) Show that if $N \neq G$, then $N$ must be contained in the center $C$ of $G$ (and consequently $G/C$ is a simple group). (If $x \in N$, apply Section 19.11, Problem 7(c) to the mapping $y \mapsto yxy^{-1}x^{-1}$ of $G$ into $N$.)

**7. MAXIMAL TORI IN COMPACT CONNECTED LIE GROUPS**

(21.7.1) A compact, connected, commutative Lie group is necessarily isomorphic to a group $T^n$ (19.7.9.2). For brevity’s sake, such a group will be called an $n$-dimensional torus.

In a compact Lie group $G$, a connected closed commutative subgroup $T$ is a Lie subgroup of $G$ (19.10.1), hence is a torus. We say that $T$ is a maximal torus in $G$ if there exists no torus in $G$ that properly contains $T$. 

A connected Lie group \( H \) immersed in a compact Lie group \( G \) is a maximal torus of \( G \) if and only if its Lie algebra \( h_e \) is a maximal commutative subalgebra of the Lie algebra \( g_e \) of \( G \).

In view of the canonical one-to-one correspondence between Lie subalgebras of \( g_e \) and connected Lie groups immersed in \( G \) (19.7.4), it is enough to show that if \( h_e \) is a maximal commutative Lie subalgebra of \( g_e \), then the corresponding subgroup \( H \) is necessarily closed in \( G \). If this were not the case, its closure \( H = H' \) in \( G \) would be a compact group (hence a Lie subgroup (19.10.1)), connected (3.19.2) and commutative (12.8.5); consequently its Lie algebra \( h'_e \) would be commutative and would contain \( h_e \) properly: contradiction.

The condition in (21.7.2) may also be put in the following equivalent form: the commutative subalgebra \( h_e \) is equal to its centralizer \( \mathfrak{Z}(h_e) \) in \( g_e \). For it is clear that \( h_e \) is maximal if this condition is satisfied; and, conversely, if \( h_e \) is commutative and \( u \in \mathfrak{Z}(h_e) \), the vector subspace \( h_e + Ru \) of \( g_e \) is a commutative Lie subalgebra, and therefore if \( h_e \) is maximal we must have \( u \in h_e \), and hence \( \mathfrak{Z}(h_e) = h_e \).

Every connected commutative Lie group \( H \) immersed in a compact Lie group \( G \) is contained in a maximal torus of \( G \).

The Lie algebra \( h_e \) of \( H \) is commutative, hence is contained in a maximal commutative Lie subalgebra of \( g_e \) (for example, a commutative subalgebra whose dimension is maximal among those which contain \( h_e \)). The result now follows from (21.7.2) and (19.7.4).

Every compact connected Lie group \( G \) is the union of its maximal tori.

Since (21.7.3) may be applied to the one-parameter subgroups of \( G \), the result to be proved is equivalent to the assertion that the exponential mapping \( \exp \) is surjective. Now, there exists on \( G \) a Riemannian structure for which the one-parameter subgroups are the geodesic trajectories passing through \( e \) (20.11.8). Since \( G \) is compact and connected, the proposition is therefore a consequence of the Hopf–Rinow theorem (20.18.5).

The importance of the tori in a compact Lie group is that one knows explicitly all their linear representations (21.3.8). By virtue of (19.7.2) and (19.8.7.2), the Lie algebra of the commutative real Lie group \( (\mathbb{C}^*)^n \) may
be canonically identified with the real vector space $\mathbb{C}^n$, and the exponential mapping is

\begin{equation} \tag{21.7.5.1}
(z_1, \ldots, z_n) \mapsto (e^{z_1}, \ldots, e^{z_n}).
\end{equation}

The Lie algebra of the subgroup $U^n$ of $(\mathbb{C}^*)^n$ is therefore the subspace $i\mathbb{R}^n$ of $\mathbb{C}^n$, and the exponential mapping of $i\mathbb{R}^n$ into $U^n$ is the restriction of (21.7.5.1) to $i\mathbb{R}^n$; its kernel is therefore the discrete subgroup $2\pi i\mathbb{Z}^n$ of $i\mathbb{R}^n$. Every character $\chi$ of $U^n$, being a homomorphism of $U^n$ into $U$, has therefore a derived homomorphism, which is an $\mathbb{R}$-linear mapping $\alpha: i\mathbb{R}^n \to i\mathbb{R}$ such that, by virtue of (21.5.2.1),

\begin{equation} \tag{21.7.5.2}
\chi(e^{i\xi_1}, \ldots, e^{i\xi_n}) = e^{\alpha(i\xi_1, \ldots, i\xi_n)}
\end{equation}

for all $(\xi_1, \ldots, \xi_n) \in \mathbb{R}^n$. This implies that we must have

$$\alpha(2\pi im_1, \ldots, 2\pi im_n) \in 2\pi i\mathbb{Z}$$

for all $(m_1, \ldots, m_n) \in \mathbb{Z}^n$. Conversely, if this condition is satisfied, the mapping $(i\xi_1, \ldots, i\xi_n) \mapsto e^{\alpha(i\xi_1, \ldots, i\xi_n)}$ factorizes as

$$(i\xi_1, \ldots, i\xi_n) \mapsto (e^{i\xi_1}, \ldots, e^{i\xi_n}) \mapsto e^{\alpha(i\xi_1, \ldots, i\xi_n)}$$

where $\chi$ is a character of $U^n$.

By transport of structure, it therefore follows that if $T$ is an $n$-dimensional torus and $t$ its Lie algebra, the exponential mapping $\exp_T$ is a homomorphism of Lie groups from $t$ (regarded as an additive group) to $T$, the kernel $\Gamma_T$ of which is a lattice in $t$, that is to say, a free $\mathbb{Z}$-module that spans the real vector space $t$. The characters of $T$ are the continuous mappings $\chi$ of $T$ into $U$ such that

\begin{equation} \tag{21.7.5.3}
\chi(\exp(u)) = e^{2\pi i\varphi(u)}
\end{equation}

for all $u \in t$, where $\varphi \in t^*$ is an $\mathbb{R}$-linear form on the vector space $t$ such that $\varphi(u)$ is an integer for all $u \in \Gamma_T$. These linear forms constitute a lattice $\Gamma_T^\vee$ in the real vector space $t^*$, called the dual of the lattice $\Gamma_T$ (22.14.6). The elements of the lattice $2\pi i\Gamma_T^\vee$ in the complexification $t^*_t$ of $t^*$ are called the weights of $T$; they are therefore $\mathbb{R}$-linear mappings of $t$ into $i\mathbb{R} \subset \mathbb{C}$, namely the derived homomorphisms of the characters of $T$.

If now $V: T \to \text{GL}(E)$ is a linear representation of $T$ on a complex vector space $E$ of finite dimension $m$, it leaves invariant a scalar product (6.2) on $E$ (21.4.3); and $E$ is the Hilbert sum, relative to this scalar product, of subspaces $E_k$ ($1 \leq k \leq m$) of complex dimension 1, such that for all $x \in E_k$ we have

\begin{equation} \tag{21.7.5.4}
V(s) \cdot x = \chi_k(s)x
\end{equation}
where \( \chi_k \) is a character of \( T \) (21.4.4). Bearing in mind (21.7.5.3) and (21.5.2.1), we see therefore that the derived homomorphism \( V_\ast : \mathfrak{t} \rightarrow \mathfrak{gl}(E) = \text{End}(E) \) is such that

\[
(21.7.5.5) \quad V_\ast(u) \cdot x = \alpha_k(u)x
\]

for all \( u \in \mathfrak{t} \) and \( x \in E_k \) (1 \( \leq k \leq m \)), where \( \alpha_k \) is a weight of \( T \). We remark that the \( \alpha_k \) are not \textit{a priori} necessarily distinct, for distinct values of the index \( k \).

\[
(21.7.5.6) \quad \text{There exists } u_0 \in \mathfrak{t} \text{ such that } \ker(V_\ast(u_0)) \text{ is the intersection of all the kernels } \ker(V_\ast(u)) \text{ in } \mathfrak{t}, \text{ as } u \text{ runs through } \mathfrak{t}.
\]

Since \( \mathfrak{t} \) is not the union of any finite number of hyperplanes (12.16.1), there exists an element \( u_0 \in \mathfrak{t} \) such that \( \alpha_k(u_0) \neq 0 \) for all the indices \( k \) such that the linear form \( \alpha_k \) is not identically zero. This clearly proves the proposition (A.4.17).

\[
(21.7.6) \quad \text{The study of the structure of a compact connected Lie group } G \text{ and of its linear representations rests entirely on the consideration of the restrictions to the tori in } G \text{ (and especially to the maximal tori) of the linear representations of } G \text{ (on complex vector spaces). Let } \mathfrak{g} \text{ be the Lie algebra of } G. \text{ Up to the end of Section 21.12, we shall study from this point of view the extension of the adjoint representation of } G \text{ to the complex vector space } \mathfrak{g}(\mathbb{C}) = \mathfrak{g} \otimes \mathbb{C}, \text{ that is to say (21.5.1) the homomorphism}
\]

\[
(21.7.6.1) \quad s \mapsto \text{Ad}(s) \otimes 1_{\mathbb{C}}
\]

of \( G \) into \( \text{GL}(\mathfrak{g}(\mathbb{C})) \). If we consider the restriction of this homomorphism to a torus \( T \) in \( G \), its derived homomorphism is the restriction, to the Lie algebra \( \mathfrak{t} \) of \( T \), of the homomorphism

\[
(21.7.6.2) \quad u \mapsto \text{ad}(u) \otimes 1_{\mathbb{C}}
\]

of \( \mathfrak{g} \) into \( \mathfrak{gl}(\mathfrak{g}(\mathbb{C})) \) (19.11.2). Applying (21.7.5.6) to this restriction, we obtain:

\[
(21.7.6.3) \quad \text{If } \mathfrak{t} \text{ is the Lie algebra of a torus } T \text{ in the compact Lie group } G, \text{ there exists a vector } u_0 \in \mathfrak{t} \text{ such that } \mathfrak{z}(\mathfrak{t}) = \mathfrak{z}(u_0) \text{ in } \mathfrak{g}.
\]

We shall use this result to prove the fundamental theorem on the conjugacy of maximal tori:
(21.7.7) Let $G$ be a compact connected Lie group, $T$ a maximal torus in $G$, and $A$ a torus in $G$. Then there exists an element $s \in G$ such that $sAs^{-1} \subset T$ (which implies that $sAs^{-1} = T$ if $A$ is a maximal torus).

Let $\mathfrak{g}$, $\mathfrak{t}$, $\mathfrak{a}$ be the Lie algebras of $G$, $T$, $A$, respectively. Since all three groups are connected, it follows from (19.7.4) and (19.2.1.1) that it is enough to prove the following proposition:

(21.7.7.1) There exists $s \in G$ such that $\text{Ad}(s) \cdot \mathfrak{a} \subset \mathfrak{t}$.

By virtue of (21.7.6.3), there exists a vector $u \in \mathfrak{a}$ and a vector $v \in \mathfrak{t}$ such that $\mathfrak{a}(a) = \mathfrak{a}(u)$ and $\mathfrak{a}(t) = \mathfrak{a}(v)$. Consider a scalar product $(x | y)$ on $\mathfrak{g}$ that is invariant under the action $(s, x) \mapsto \text{Ad}(s) \cdot x$ of $G$ on $\mathfrak{g}$ (20.11.3.2); for this scalar product and the corresponding norm $\|x\| = (x | x)^{1/2}$, the function $s \mapsto \|\text{Ad}(s) \cdot u - v\|^2$ is continuous on the compact group $G$, hence attains its minimum at some $s_0 \in G$ (3.17.10). We shall show that $\text{Ad}(s_0) \cdot u \in \mathfrak{t}$; this will imply, by virtue of the commutativity of $\mathfrak{t}$ and by transport of structure, that

$$\mathfrak{t} \subset \mathfrak{a}(\text{Ad}(s_0) \cdot u) = \text{Ad}(s_0) \cdot \mathfrak{a}(u) = \text{Ad}(s_0) \cdot \mathfrak{a}(a) = \mathfrak{a}(\text{Ad}(s_0) \cdot a)$$

and consequently that the vector subspace $\mathfrak{t} + \text{Ad}(s_0) \cdot \mathfrak{a}$ of $\mathfrak{g}$ is a commutative Lie subalgebra. But since $\mathfrak{t}$ is maximal among such subalgebras, it follows that $\text{Ad}(s_0) \cdot \mathfrak{a} \subset \mathfrak{t}$, which will establish (21.7.7.1).

By replacing $u$ by $\text{Ad}(s_0) \cdot u$, and $a$ by $\text{Ad}(s_0) \cdot a$, we may assume (because of the invariance of the scalar product) that $s_0 = e$. Let us express that, for each $x \in \mathfrak{g}$, the derivative of the function of a real variable

$$t \mapsto \|\text{Ad}(\exp(tx)) \cdot u - v\|^2$$

vanishes at $t = 0$. Since the derivative of $t \mapsto \text{Ad}(\exp(tx)) \cdot u$ at $t = 0$ is $[x, u]$ (19.11.2), we obtain by use of (21.5.4.1)

$$0 = 2([x, u] | u - v) = 2(x | [u, u - v])$$

for all $x \in \mathfrak{g}$; in other words, $[u, v] = 0$ and therefore $u \in \mathfrak{a}(v) = \mathfrak{a}(t)$. Q.E.D.

(21.7.7.2) In particular, any two maximal tori of $G$ have the same dimension; this dimension is called the rank of the compact connected Lie group $G$ or of its Lie algebra $\mathfrak{g}$. If $G$ is a compact semisimple Lie group, $\mathfrak{g} = \bigoplus_j \mathfrak{g}_j$ the decomposition of its Lie algebra as a direct sum of simple algebras (21.6.4), and $\mathfrak{t}_j$ a maximal commutative subalgebra of $\mathfrak{g}_j$, then it is immediately verified that $\mathfrak{t} = \bigoplus_j \mathfrak{t}_j$ is equal to its centralizer in $\mathfrak{g}$, so that the rank of $\mathfrak{g}$ is the sum of the ranks of the $\mathfrak{g}_j$. 


(21.7.8) Let $G$ be a compact connected Lie group and $T$ a maximal torus in $G$. For each $x \in G$, there exists $s \in G$ such that $sx{s}^{-1} \in T$.

For $x$ lies in some torus in $G$ (21.7.4).

(21.7.9) Let $G$ be a compact connected Lie group. For each torus $A$ in $G$, the centralizer $\mathcal{Z}(A)$ of $A$ in $G$ is connected. Moreover, for each $s \in \mathcal{Z}(A)$, $A \cup \{s\}$ is contained in a maximal torus of $G$.

Let $s \in \mathcal{Z}(A)$; the centralizer $\mathcal{Z}(s)$ of $s$ is a Lie subgroup of $G$, and its identity component $H$ is a compact connected subgroup of $G$. There exists a maximal torus $T$ of $G$ containing $s$ (21.7.8), and by definition we have $T \subset H$ and $A \subset H$; moreover, $T$ is clearly a maximal torus of $H$. By (21.7.7), therefore, there exists an element $h \in H$ such that $A \subset T' = hTh^{-1}$, and therefore $T'$ is contained in the identity component of $\mathcal{Z}(A)$. But we have $hsh^{-1} = s$ by definition of $H$, hence $s$ lies in the identity component of $\mathcal{Z}(A)$; and $T'$ is a maximal torus of $G$ containing $A$ and $s$. Q.E.D.

In particular:

(21.7.10) In a compact connected Lie group $G$, every maximal torus is equal to its centralizer, and is therefore maximal in the set of all commutative subgroups of $G$.

It should be noted, however, that the set of commutative subgroups of $G$ in general contains maximal elements that are not tori (Problem 1).

(21.7.11) The center of a compact connected Lie group $G$ is the intersection of the maximal tori of $G$.

Since $G$ is the union of its maximal tori (21.7.4), their intersection is contained in the center $C$ of $G$. Conversely, if $T$ is any maximal torus of $G$, then $CT$ is a commutative subgroup of $G$ containing $T$, hence is equal to $T$ by (21.7.10), so that $C \subset T$.

(21.7.12) For each element $s$ of a compact connected Lie group $G$, the identity component of $\mathcal{Z}(s)$ is the union of the maximal tori of $G$ that contain $s$.

Clearly this identity component $(\mathcal{Z}(s))_0$ contains every maximal torus that contains $s$. Conversely, if $x \in (\mathcal{Z}(s))_0$, then $x$ belongs to some maximal torus $A$ of the compact connected Lie group $(\mathcal{Z}(s))_0$ (21.7.4); but since $A$ is a torus in $G$, there exists a maximal torus $T$ of $G$ containing both $A$ and $s$, because by definition $s \in \mathcal{Z}(A)$ (21.7.9).
7. MAXIMAL TORI IN COMPACT CONNECTED LIE GROUPS

We remark that the centralizer of an arbitrary element \( s \in G \) is not necessarily connected (Problem 1).

(21.7.13) An element \( s \) in a compact connected Lie group \( G \) is said to be \textit{regular} if it belongs to \textit{only one} maximal torus of \( G \), and \textit{singular} if it belongs to more than one. Likewise, an element \( u \) of the Lie algebra \( g_e \) of \( G \) is said to be \textit{regular} if it belongs to only one maximal commutative Lie subalgebra, and \textit{singular} if it belongs to more than one (see (21.8.4.2)).

It follows from (21.7.12) that an element \( s \in G \) is regular if and only if the identity component of \( \mathcal{Z}(s) \) is a maximal torus. An equivalent condition is that the dimension of \( \mathcal{Z}(s) \) is equal to the rank of \( G \); for \( \mathcal{Z}(s) \) contains at least one maximal torus \( T \), and if the dimension of \( \mathcal{Z}(s) \) is equal to that of \( T \), then \( T \) must be open in \( \mathcal{Z}(s) \) (16.8.3.3), hence is the identity component of \( \mathcal{Z}(s) \). Likewise, in order that \( u \in g_e \) should be regular, it is necessary and sufficient that the centralizer \( \mathcal{Z}(u) \) should be a maximal commutative subalgebra. For this condition is clearly sufficient; and conversely if \( u \) is regular and \( t \) is a maximal commutative subalgebra that contains \( u \), then \( \mathcal{Z}(u) \) cannot contain any element \( v \notin t \), otherwise the commutative subalgebra generated by \( u \) and \( v \) would be contained in a maximal commutative subalgebra distinct from \( t \).

(21.7.14) Let \( G \) be a compact connected Lie group. If \( u \) is a regular element of the Lie algebra of \( G \), then the centralizer \( \mathcal{Z}(Ru) \) in \( G \) (19.11.3) is a maximal torus of \( G \).

For if \( A \) is the torus in \( G \) that is the closure of the one-parameter subgroup corresponding to \( Ru \), we have \( \mathcal{Z}(A) = \mathcal{Z}(Ru) \) ((19.11.6) and (12.8.6)). Since \( \mathcal{Z}(A) \) is connected (21.7.9), its Lie algebra is the centralizer of \( Ru \) (19.11.6), and the proposition follows.

(21.7.15) Let \( G \) be a compact connected Lie group. Every maximal torus \( T \) of \( G \) is open (hence of finite index) in its normalizer \( \mathcal{N}(T) \) in \( G \).

Let \( H \) be the identity component of the Lie group \( \mathcal{N}(T) \), and for each \( s \in H \) let \( \sigma_s \) denote the automorphism \( x \mapsto sx^{-1} \) of \( T \). The argument of (19.14.4) shows that the mapping \( s \mapsto \sigma_s \) is a Lie group homomorphism of \( H \) into the group \( \text{Aut}(T) \). But \( \text{Aut}(T) \) is discrete (19.13.6) and \( H \) is connected, hence \( \sigma_s \) is the identity mapping for each \( s \in H \) (3.19.7). In other words, \( H \) is contained in the centralizer of \( T \), hence \( H = T \) (21.7.10).

(21.7.16) With the notation of (21.7.15), the finite quotient group \( W(G, T) = \mathcal{N}(T)/T \) is called the \textit{Weyl group} of the compact connected Lie
group $G$, relative to the maximal torus $T$. For each $s \in G$, we have $N(sTs^{-1}) = sN(T)s^{-1}$ by transport of structure, hence $W(G, sTs^{-1})$ is isomorphic to $W(G, T)$. By virtue of the conjugacy theorem (21.7.7), the Weyl groups corresponding to the various maximal tori of $G$ are all isomorphic; any one of these Weyl groups $W(G, T)$ is called the Weyl group of $G$, and denoted by $W(G)$, or simply $W$. The group $W(G, T)$ acts differentiably on $T$ in a canonical way: every element $w \in W(G, T)$ is the coset of an element $s \in W(T)$, and we define $w \cdot t = stsl$, which is independent of the choice of representative $s \in w$, because $T$ is commutative. Since $\mathcal{Z}(T) = T$ (21.7.10), it follows that $W(G, T)$ acts faithfully on $T$.

(21.7.17) Let $G$ be a compact connected Lie group and $T$ a maximal torus in $G$. If two elements $t_1, t_2$ of $T$ are conjugate in $G$, there exists an element $w \in W(G, T)$ such that $t_2 = w \cdot t_1$.

We have $t_2 = st_1s^{-1}$ for some $s \in G$, and we have to show that $t_2 = nt_1n^{-1}$ for some $n \in N(T)$. The torus $T$ is contained in $\mathcal{Z}(t_1)$ and $\mathcal{Z}(t_2)$, hence $\mathcal{Z}(t_2)$ also contains the torus $sTs^{-1}$. Hence, if $H$ is the identity component of $\mathcal{Z}(t_2)$, both $T$ and $sTs^{-1}$ are maximal tori in the compact connected Lie group $H$, and therefore there exists an element $h \in H$ such that $sTs^{-1} = hTh^{-1}$ (21.7.7). It follows that $h^{-1}sT(h^{-1}s)^{-1} = T$, so that $n = h^{-1}s \in N(T)$; and since $h \in \mathcal{Z}(t_2)$, we have $h^{-1}(st_1s^{-1})h = t_2$, that is to say, $nt_1n^{-1} = t_2$.

(21.7.18) Let $G$ be a compact connected Lie group and $C'$ a closed subgroup of the center $C$ of $G$. Then, if $T$ is a maximal torus of $G$, the quotient group $T/C'$ is a maximal torus of $G/C'$; also $N(T/C') = N(T)/C'$, and the Weyl group $W(G/C', T/C')$ is isomorphic to $W(G, T)$.

Recall that $C$ is contained in $T$ (21.7.11). If $\pi: G \to G/C'$ is the canonical homomorphism, and if $\pi(s)$ belongs to the normalizer of $\pi(T) = T/C'$, we have $\pi(sts^{-1}) \in \pi(T)$ for all $t \in T$, and therefore $sts^{-1} \in C'T = T$, whence $s \in N(T)$ and thus $\mathcal{N}(T/C') = \mathcal{N}(T)/C'$. It is clear that $\pi(T)$ is a compact connected commutative subgroup of $G/C'$, hence is a torus. Let $U$ be a compact connected commutative subgroup of $G/C'$ containing $\pi(T) = T/C'$; then $U \subset \mathcal{N}(T/C') = \mathcal{N}(T)/C'$, hence $\pi^{-1}(U)$ is a compact subgroup of $G$ such that $T \subset \pi^{-1}(U) \subset N(T)$. By (21.7.15), $T$ is open in $\pi^{-1}(U)$, hence $T/C'$ is the identity component of $U = \pi^{-1}(U)/C'$. Since $U$ is connected, we have $T/C' = U$, and hence $T/C'$ is a maximal torus in $G/C'$. Finally,

$$W(G/C', T/C') = \mathcal{N}(T/C')/(T/C') = (\mathcal{N}(T)/C')/(T/C') = \mathcal{N}(T)/T$$

$$= W(G, T)$$

up to canonical isomorphism ((12.12.2) and (19.10.2)).
7. MAXIMAL TORI IN COMPACT CONNECTED LIE GROUPS

PROBLEMS

1. Let $G$ be the rotation group $\text{SO}(4k, \mathbb{R})$, where $k \geq 1$. Let $V$ be a vector subspace of dimension $2k$ in $\mathbb{R}^{4k}$, $V^\perp$ its orthogonal supplement, and let $s$ be the automorphism of $\mathbb{R}^{4k}$ such that $s(x) = x$ for $x \in V$ and $s(x) = -x$ for $x \in V^\perp$; then $s \in G$. Let $H$ (resp. $H'$) be a hyperplane in $V$ (resp. $V^\perp$), and let $t$ be the automorphism of $\mathbb{R}^{4k}$ whose restriction to $V$ (resp. $V^\perp$) is the orthogonal reflection with respect to $H$ (resp. $H'$). We have $t \in G$ and $ts = st$. Let $S$ be the centralizer of $s$ in $G$, and $S_0$ the identity component of $S$. Show that $\det(u|V) > 0$ for all $u \in S_0$ and hence that $r \notin S_0$. Deduce that $S$ is not connected, and that the commutative subgroup generated by $s$ and $t$ is not contained in any maximal torus of $G$.

2. Let $G$ be a Lie group, $\mathfrak{g}$ its Lie algebra, and $\Phi$ a $G$-invariant symmetric $\mathbb{R}$-bilinear form on $\mathfrak{g} \times \mathfrak{g}$ (21.5.4). Let $K$ be a compact subgroup of $G$. Let $x$, $y$ be elements of $\mathfrak{g}$; show that there exists an element $t \in K$ such that $\Phi(u, [\text{Ad}(t) \cdot x, y]) = 0$ for all $u \in \mathfrak{t} = \text{Lie}(K)$. (Argue as in (21.7.7.1).)

3. Let $G$ be a compact Lie group, $\mathfrak{g}$ its Lie algebra, and $m$ a vector subspace of $\mathfrak{g}$ such that $[[u, v], w] \in m$ for all $u, v, w$ in $m$. Let $G'$ be the identity component of the normalizer $\mathcal{N}(m)$ of $m$ in $G$ (19.11.3), and let $t$ be a maximal element of the set of commutative subalgebras of $\mathfrak{g}$ contained in $m$. Show that for each commutative subalgebra $\mathfrak{a}$ of $\mathfrak{g}$ contained in $m$, there exists an element $s \in G'$ such that $\text{Ad}(s) \cdot \mathfrak{a} = t$. (Argue as in (21.7.7).)

4. Let $G$ be a Lie group, $s$ an element of $G$, and $\mathfrak{g}$ the Lie algebra of $G$. Let $\pi$ be the union of the kernels of the endomorphisms $(\text{Ad}(s) - I)^k$ of the vector space $\mathfrak{g}$, for all integers $k \geq 1$. Show that $\pi$ is a Lie subalgebra of $\mathfrak{g}$. Let $N$ be the connected Lie group immersed in $G$ corresponding to the Lie algebra $\pi$. Show that the mapping $(s, t) \mapsto sxts^{-1}$ of $G \times N$ into $G$ is a submersion (16.7.1) at the point $(e, e)$. (The vector space $\mathfrak{g}$ is the direct sum of $\pi$ and a subspace $\mathfrak{m}$ such that the restriction of $\text{Ad}(s) - I$ to $\mathfrak{m}$ is an automorphism of this subspace (11.4.1). Calculate the tangent linear mapping at the point $\xi = 0$ of the mapping $\zeta \mapsto \exp(\xi u)x \exp(\xi v) \exp(-\xi u)$ of $\mathbb{R}$ into $G$, for $u \in \pi$ and $v \in \mathfrak{m}$.)

5. Give a proof of (21.7.4) without using the Riemannian structure of $G$, but using instead (21.7.7) and proceeding by induction on $n = \dim(G)$. (Given a maximal torus $T$ of $G$, show that the union $E$ of the conjugates of $T$ is open in $G$. For this it is enough to show that $E$ is a neighborhood of any point $s \in T$; distinguish two cases, according as $s$ belongs or does not belong to the center of $G$. In the second case consider the identity component of the centralizer of $s$ in $G$, and use the inductive hypothesis and Problem 4.)

6. Let $G$ be a compact connected Lie group, $T$ and $T'$ two maximal tori in $G$. Let $A$ (resp. $A'$) be a subset of $T$ (resp. $T'$) and let $\sigma$ be an automorphism of $G$ such that $\sigma(A) = A'$. Show that there exists $s \in G$ such that $\sigma(a)s^{-1} = \sigma(a)$ for all $a \in A$ and such that $\sigma(T)s^{-1} = T'$. (Consider the maximal torus $T'' = \sigma(T)$ and the identity component of the centralizer of $A'$ in $G$.)

In particular, there exists an inner automorphism of $G$ that transforms $T$ into $T'$ and fixes the elements of $T \cap T'$. 


7. Let $G$ be a compact connected Lie group and $N$ a closed normal subgroup of $G$. Show that if there exists a maximal torus $T$ of $G$ such that $T \cap N = \{e\}$, then $N = \{e\}$. (Consider a maximal torus $S$ of $N$, and use (16.30.2.2).)

8. Let $G$ be a compact connected Lie group.

(a) If $H$ is a connected closed subgroup of $G$, every maximal torus of $H$ is of the form $T_n^H$, where $T$ is a maximal torus of $G$.

The Weyl group $W(H, T \cap H)$ is isomorphic to the quotient $F/F$, where $F$ is the subgroup of $W(G, T)$ that leaves $T \cap H$ stable as a whole, and $F'$ is the normal subgroup of $F$ that fixes $T \cap H$ elementwise.

(b) If $N$ is a closed normal subgroup of $G$, every maximal torus of $G/N$ is of the form $T_n^G/N$, where $T$ is a maximal torus of $G$ (use Section 21.6, Problem 4). If in addition $N$ is discrete, every maximal torus of $G$ is the inverse image of a maximal torus of $G/N$ under the canonical homomorphism (use (16.30.2.2)).

9. Let $G$ be a compact connected Lie group, $T$ a maximal torus in $G$, and $N$ its normalizer in $G$. Then $G$ (resp. $N$) acts differentiably on $G$ (resp. $T$) by inner automorphisms; let $E$ and $F$ be the respective orbit spaces (12.10) and $A: G \rightarrow E$, $n': T \rightarrow F$ the canonical mappings. If $j: T \rightarrow G$ is the canonical injection, there exists one and only one continuous mapping $f: F \rightarrow E$ such that $A_0 j = f \circ A'$. Show that $f$ is a homeomorphism of $F$ onto $E$.

10. Let $G$ be a compact connected Lie group and $T$ a maximal torus of $G$. Show that the manifold $G/T$ is simply connected, and that if $G'$ is a compact connected Lie group, locally isomorphic to $G$, and if $T'$ is a maximal torus of $G'$, then $G/T$ and $G'/T'$ are diffeomorphic. (Reduce to the case where $G$ and $G'$ are semisimple, and use Section 16.30, Problem 11.)

8. ROOTS AND ALMOST SIMPLE SUBGROUPS OF RANK ONE

Throughout this section, $G$ denotes a compact connected Lie group, $T$ a maximal torus of $G$, $g$ (resp. $t$) the Lie algebra of $G$ (resp. $T$), and $W = W(G, T)$ the Weyl group of $G$ relative to $T$. Since $W$ may be identified with a group of automorphisms of $T$, it acts linearly and faithfully on $t$ via the derived automorphisms. To be precise, if $s$ is a representative of $w \in W$ in $N(T)$, we have $w \cdot u = \text{Ad}(s) \cdot u$ for all $u \in t$. Since $w$ is now an automorphism of the real vector space $t$, its contragredient $w^{-1}$ is an automorphism of the dual $t^*$ of $t$; we shall write $w \cdot \lambda$ in place of $(w^{-1})(\lambda)$ for $\lambda \in t^*$, so that we have $\langle w \cdot u, w \cdot \lambda \rangle = \langle u, \lambda \rangle$ for all $u \in t$ and $\lambda \in t^*$, and $W$ acts linearly on the vector space $t^*$ by the rule $(w, \lambda) \mapsto w \cdot \lambda$.

Consider again the linear representation $s \mapsto \text{Ad}(s) \otimes 1_C$ of $T$ on the complex vector space $g(C) = g \otimes_R C = g \oplus ig$, and the derived homomorphism $u \mapsto \text{Ad}(u) \otimes 1_C$ of $t$ into $\text{gl}(g(C))$. It follows from (21.7.5) that there is a finite set $S \subset 2\pi i \Gamma_+^*$ of nonzero weights of $T$ (also denoted by $S(G, T)$ or $S(G)$) such that the complex vector space $g(C)$ is the direct sum of a vector
subspace \( g_0 \supset t_{(C)} \) and vector subspaces \( g_\alpha \), each of the latter being nonzero and corresponding to a weight \( \alpha \in S \). Furthermore, for each \( u \in t \) we have

\[(21.8.1.1) \quad [u, x] = 0 \]

for all \( x \in g_0 \), and

\[(21.8.1.2) \quad [u, x] = \alpha(u)x \]

for all \( \alpha \in S \) and all \( x \in g_\alpha \).

In fact, \( g_0 = t \oplus it = t_{(C)} \), the complexification of \( t \), because if \( x = y + iz \) with \( y, z \in g \), the relation \([u, x] = 0 \) for \( u \in t \) implies that \([u, y] = 0 \) and \([u, z] = 0 \) for all \( u \in t \), and therefore \( y \in t \) and \( z \in t \), since \( t \) is its own centralizer in \( g \) (21.7.2.1).

The weights \( \alpha \in S \) are called the roots of \( G \) relative to \( T \), or of \( g \) relative to \( t \).

\[(21.8.1.3) \quad \text{The roots } \alpha \in S \text{ are the only } R\text{-linear mappings } \lambda \text{ of } t \text{ into } C \text{ that are not identically zero and are such that for some } x_0 \neq 0 \text{ in } g_{(C)}, \text{ we have } [u, x_0] = \lambda(u)x_0 \text{ for all } u \in t \text{ (A.24.4).} \]

\[(21.8.2) \quad \text{Let } c \text{ be the semilinear bijection of the complex vector space } g_{(C)} \text{ onto itself defined by } c(y + iz) = y - iz \text{ for } y, z \in g. \text{ The real subspace } g \text{ (resp. } ig) \text{ is therefore the set of all } x \in g_{(C)} \text{ such that } c(x) = x \text{ (resp. } c(x) = -x). \text{ It is clear that } [u, c(x)] = c([u, x]) \text{ for all } x \in g_{(C)} \text{ and all } u \in t; \text{ hence it follows from } (21.8.1.2) \text{ that, for all } x \in g_\alpha \text{ and all } u \in t, \text{ we have } [u, c(x)] = \alpha(u)c(x) = -\alpha(u)c(x), \text{ since } \alpha(u) \text{ is pure imaginary. Consequently, if } \alpha \text{ is a root, so also is } -\alpha, \text{ and we have } g_{-\alpha} = c(g_\alpha). \]

\[(21.8.3) \quad \text{Consider a root } \alpha = 2\pi i\varphi, \text{ where } \varphi \text{ is an } R\text{-linear form on } t. \text{ For each } x_\alpha \in g_\alpha, \text{ the two elements} \]

\[y_\alpha = x_\alpha + c(x_\alpha), \quad z_\alpha = i(x_\alpha - c(x_\alpha)) \]

belong to \( g \), and as \( x_\alpha \) runs through a \( C \)-basis of \( g_\alpha \), the \( y_\alpha \) and \( z_\alpha \) form an \( R \)-basis of \( (g_\alpha \oplus g_{-\alpha}) \cap g \). For each \( u \in t \), we have

\[(21.8.3.2) \quad [u, y_\alpha] = 2\pi \varphi(u)z_\alpha, \quad [u, z_\alpha] = -2\pi \varphi(u)y_\alpha. \]

Since the center \( c \) of \( g \) is contained in \( t \), it follows from these formulas that \( c \) is the set of vectors \( u \in t \) such that \( \alpha(u) = 0 \) for all \( \alpha \in S \).
Moreover, since \((\text{Ad}(\exp(u)) \otimes 1_c) \cdot x_a = e^{2\pi i \phi(u)} x_a\) (21.7.5.1), we deduce from (21.8.3.1) that

\[
\text{(21.8.3.3)}
\]

\[
\begin{align*}
\text{Ad}(\exp(u)) \cdot y_a &= \cos(2\pi \phi(u)) y_a + \sin(2\pi \phi(u)) z_a, \\
\text{Ad}(\exp(u)) \cdot z_a &= -\sin(2\pi \phi(u)) y_a + \cos(2\pi \phi(u)) z_a.
\end{align*}
\]

From these formulas we obtain a characterization of the regular elements of \(G\) (resp. \(g\)) (21.7.13) that are contained in \(T\) (resp. \(t\)).

\[
\text{(21.8.4)}
\]

In order that an element \(u \in t\) be regular, it is necessary and sufficient that it belong to none of the hyperplanes \(u_a = u_{-a} = \alpha^{-1}(0)\) in \(t\), where \(\alpha \in S\).

In order that an element \(s \in T\) be regular, it is necessary and sufficient that it belong to none of the subgroups \(U_a = U_{-a} = \chi_a^{-1}(1)\) in \(T\), where \(\chi_a\) is the character of \(T\) defined by \(\chi_a(\exp(u)) = e^{\alpha(u)}\) for \(u \in t\) and \(\alpha \in S\).

If \(u\) belongs to none of the \(u_a\), it follows from (21.8.3.2) that the image of \(g\) under \(\text{ad}(u)\) is the sum of the subspaces \(\mathfrak{g} \cap (\mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha})\), where \(\alpha \in S\); hence its kernel has the same dimension as \(t\) (A.4.17), and since this kernel contains \(t\) it coincides with \(t\), and therefore \(u\) is regular (21.7.13). Conversely, if \(u \in u_a\), the kernel of \(\text{ad}(u)\) contains \(t \oplus ((\mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}) \cap \mathfrak{g})\), hence \(u\) is singular (21.7.13).

Likewise, if \(s\) lies in none of the subgroups \(U_a\), then the set of vectors in \(\mathfrak{g}_{(\alpha)}\) that are fixed by \(\text{Ad}(s) \otimes 1_c\) is precisely \(t_{(\alpha)}\), because in each of the \(\mathfrak{g}_\alpha\) the restriction of \(\text{Ad}(s) \otimes 1_c\) is multiplication by \(\chi_a(s)\). Since \(\text{Ad}(s)\) fixes all the elements of the Lie algebra of \(\mathfrak{z}(s)\), this Lie algebra is equal to \(t\), and therefore \(s\) is regular (21.7.13). Conversely, if \(s \in U_a\), then \(\text{Ad}(s)\) fixes the vectors belonging to \((\mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}) \cap \mathfrak{g}\), and therefore (19.11.2.3) the Lie algebra of \(\mathfrak{z}(s)\) has dimension strictly larger than the rank of \(G\), and \(s\) is singular.

More precisely, this proof shows that the Lie algebra of \(\mathfrak{z}(s)\) is the direct sum of \(t\) and the subspaces \((\mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}) \cap \mathfrak{g}\) for all roots \(\alpha\) such that \(s \in U_a\). If the number of these roots is \(2k\) (it is an even number because \(U_{-a} = U_a\)), we have therefore

\[
\text{(21.8.4.1)}
\]

\[\dim(\mathfrak{z}(s)) \geq l + 2k\]

where \(l\) is the rank of \(G\). (We shall see later (21.10.3) that in fact the two sides of (21.8.4.1) are equal.)
For each $\alpha \in S$, the group $U_\alpha$ is a compact subgroup of $T$, of dimension $l - 1$, and $u_\alpha$ is its Lie algebra. It should be remarked that $U_\alpha$ need not be connected (Problem 2).

(21.8.4.2) In order that $u \in t$ should be such that $\exp(u)$ is a singular element of $G$, it is necessary and sufficient that $\alpha(u)$ should be an integer multiple of $2\pi i$ for some root $\alpha \in S$. In order that $u$ should be such that $\exp(u)$ lies in the center of $G$, it is necessary and sufficient that $\alpha(u)$ should be an integer multiple of $2\pi i$ for all roots $\alpha \in S$.

This follows from (21.8.3.3).

(21.8.4.3) For each $u \in t$, the set consisting of 0 and the $\alpha(u), \alpha \in S$, is the set of eigenvalues of the endomorphism $\text{ad}(u)$ of $g(\mathbb{C})$. It follows therefore from (19.16.6) that the set of elements $u \in t$ such that the tangent linear mapping $T_u(\exp_G)$ is not bijective is the set of $u \in t$ such that at least one of the numbers $\alpha(u), \alpha \in S$, is a nonzero integer multiple of $2\pi i$.

(21.8.5) For each root $\alpha \in S$ and each element $x_\alpha \neq 0$ in $g_\alpha$, the two elements $y_z, z_z$ of $g$ defined in (21.8.3.1), and the element $h^0 = [y_z, z_z]$ (which belongs to $t$), form a basis of the Lie algebra of a connected closed subgroup $K_\alpha$ of $G$, locally isomorphic to $SU(2, \mathbb{C})$. Furthermore, $-i\alpha(h^0) > 0$.

The Jacobi identity shows that, for each $u \in t$,

$$[u, h^0_z] = [u, [y_z, z_z]] = [y_z, [u, z_z]] - [z_z, [u, y_z]] = 0$$

by virtue of (21.8.3.2). Since $t$ is its own centralizer in $g$, it follows that $h^0_z \in t$.

Now let $(u | v)$ be a $G$-invariant scalar product on $g$ (21.4.3). Bearing in mind (21.5.4.1) and (21.8.3.2), we have

(21.8.5.1) \((u | h^0_z) = (u | [y_z, z_z]) = ([u, y_z] | z_z) = 2\pi \varphi(u)(z_z | z_z)\).

Since $z_z \neq 0$, we have $(z_z | z_z) \neq 0$; since the linear form $\varphi = (2\pi i)^{-1}x$ is not identically zero on $t$, we have $h^0_z \neq 0$; and therefore from (21.8.5.1) we obtain

(21.8.5.2) \(i(h^0_z | h^0_z) = \alpha(h^0_z)(z_z | z_z),\)

so that $\alpha(h^0_z) \neq 0$, and $-i\alpha(h^0_z) > 0$. 
We have therefore shown that the three vectors $h_z^0, y_z, z_z$ form a basis of a Lie subalgebra $t_z$ of $g$, for which the multiplication table is as follows:

\[
[h_z^0, y_z] = -i\alpha(h_z^0)z_z, \\
[h_z^0, z_z] = i\alpha(h_z^0)y_z, \\
[y_z, z_z] = h_z^0.
\]

(21.8.5.3)

We now recall that the compact connected Lie group $\text{SU}(2, \mathbb{C}) = \text{SU}(2)$ (16.11.3) has as Lie algebra the Lie subalgebra $\text{su}(2)$ (over $\mathbb{R}$) of $\text{gl}(2, \mathbb{C}) = \mathbb{M}_2(\mathbb{C})$ consisting of the antihermitian matrices $S$ (i.e., matrices $S$ such that $\overline{S} + S = 0$) with trace 0 ((19.4.3.2) and (19.7.1.1)). It is immediately seen that the three matrices

\[
I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
\]

form an $\mathbb{R}$-basis of this Lie algebra, and that the multiplication table is

\[
[iH, Y] = 2Z, \\
[iH, Z] = -2Y, \\
[Y, Z] = 2iH.
\]

(21.8.5.4)

If we now observe that by (21.8.5.2) the number

\[
a_z = -i\alpha(h_z^0)
\]

is strictly positive, it is clear that we may define an isomorphism $\sigma$ of $\text{su}(2)$ onto $t_z$ by the formulas

\[
\sigma(iH) = \frac{2}{a_z} h_z^0, \quad \sigma(Y) = \frac{2}{a_z^{1/2}} y_z, \quad \sigma(Z) = \frac{2}{a_z^{1/2}} z_z.
\]

It is immediately verified that no matrix $\not= \lambda I$ in $\mathbb{M}_2(\mathbb{C})$ commutes with each of $H, Y$, and $Z$, and therefore the center of $\text{su}(2)$ is $\{0\}$, so that the compact group $\text{SU}(2)$ is semisimple, with discrete and therefore finite center (in fact, it is easily shown that the center consists of $\pm I$). Moreover, $\text{SU}(2)$ is simply connected (16.30.6), hence the groups locally isomorphic to $\text{SU}(2)$ are compact (in fact, there are up to isomorphism only two of them, namely $\text{SU}(2)$ itself and its quotient by its center, which is isomorphic to $\text{SO}(3)$). The connected Lie group $K_z$ immersed in $G$ that has $t_z$ as its Lie algebra is therefore compact with respect to its proper topology, hence is closed in $G$ (3.17.2).
It follows immediately from (21.8.5.5) that $R_i H$ is a maximal commutative subalgebra of $\mathfrak{su}(2)$, and consequently (21.7.7.2) $SU(2)$ and the $K_2$ are almost simple groups of rank 1.

(21.8.6) If $\nu$ is any automorphism of $G$, it is clear by transport of structure that $\nu(T)$ is a maximal torus of $G$. The derived automorphism $\nu_*$ of $\mathfrak{g}$ transforms $t$ into the Lie algebra of $\nu(T)$, and the contragredient $\nu_*^{-1}$ of this automorphism therefore transforms the lattice of weights of $T$ into that of $\nu(T)$, and the set $S$ of roots of $G$ relative to $T$ into the set of roots of $G$ relative to $\nu(T)$.

In particular, taking $\nu = Int(s)$, where $s \in \mathbb{M}(T)$, these remarks show that the Weyl group $W = W(G, T)$ leaves invariant (globally) the lattice of weights of $T$ and the set $S$ of roots of $G$ relative to $T$. For each $w \in W$ we have, evidently,

$$(w \otimes 1_c)(g_u) = g_{w \cdot u}.$$ 

Furthermore:

(21.8.7) There exists an element $r_s \in K_2$ belonging to the normalizer $\mathbb{N}(T)$, whose coset $s_s$ modulo $T$ in the Weyl group $W$ acts on $t$ as the orthogonal reflection in the hyperplane $u_s$ (relative to any $G$-invariant scalar product on $\mathfrak{g}$), mapping $h_s^0$ to $-h_s^0$.

We shall show that we may take $r_s = \exp(\xi y_s)$ for a suitably chosen real number $\xi$. We have (19.11.2.2)

$$\text{Ad}(r_s) = \exp(\xi \text{ ad}(y_s)) = \sum_{n=0}^{\infty} \frac{\xi^n}{n!} (\text{ad}(y_s))^n$$

in the algebra $\text{End}(\mathfrak{g})$. Now, for each $u \in u_s$, we have

$$\text{ad}(y_s) \cdot u = -[u, y_s] = -i\alpha(u)z_s = 0$$

by definition, hence $\text{Ad}(r_s) \cdot u = 0$; also, if we put $a_s = -i\alpha(h_s^0) > 0$ as above, it follows from the formulas (21.8.5.3) that

$$\text{Ad}(r_s) \cdot h_s^0 = \cos(-a_s \xi)h_s^0 + \sin(-a_s \xi)z_s,$$

and therefore, if we put $\xi = \pi/a_s$, we obtain $\text{Ad}(r_s) \cdot h_s^0 = -h_s^0$. Hence, for this value of $\xi$, the automorphism $\text{Ad}(r_s)$ leaves invariant $t = u_s \oplus R h_s^0$ so that $r_s \in \mathbb{N}(T)$ (19.11.4); and since $h_s^0$ is orthogonal to $u_s$, relative to any $G$-invariant scalar product on $\mathfrak{g}$ by virtue of (21.8.5.1), it follows that the restriction of $\text{Ad}(r_s)$ to $t$ is the orthogonal reflection in the hyperplane $u_s$. 

The definition of the roots involves only the Lie algebra \( g \) and a maximal commutative subalgebra \( t \) of \( g \) (21.8.1). Since any one of these subalgebras can be transformed into any other by an automorphism of \( g \) (21.7.7), it follows that the set of roots, up to automorphisms of \( g \), depends only on \( g \) and is therefore the same for any two locally isomorphic compact connected Lie groups. Moreover, if we canonically decompose \( g \) as the direct sum \( c \oplus D(g) \) of its center \( c \) and its derived algebra \( D(g) \) (21.6.9), we have \( t = c \oplus t' \), where \( t' \) is a maximal commutative subalgebra of \( D(g) \). Also \( g(c) = c \oplus (D(g))(c) \), and it is immediate that \( c(c) \) is the center and \( (D(g))(c) \) the derived algebra of \( g(c) \); and by decomposing an element \( x \in g_a \) relative to this direct sum, it follows from (21.8.1.2) that the component of \( x \) in \( c(c) \) is zero, so that the \( g_a \) are contained in \( (D(g))(c) \). Finally, for each root \( \alpha \in \mathfrak{s} \), we have \( \alpha(u) = 0 \) for all \( u \in c \), so that \( \alpha \) may be identified with its restriction to \( t' \). The result of these considerations is that the set of roots of \( g \) relative to \( t \) may be identified with the set of roots of \( D(g) \) relative to \( t' \), so that in the study of the roots of a compact connected Lie group \( G \) we may assume without loss of generality that \( G \) is semisimple (or even semisimple and simply connected).

PROBLEMS

1. Every quaternion of norm 1 can be written uniquely as \( x + yj \), where \( x \) and \( y \) are complex numbers such that \( |x|^2 + |y|^2 = 1 \). Show that the mapping

\[
    x + yj \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}
\]

defines an isomorphism of the Lie group \( U(1, H) \) onto the Lie group \( SU(2, C) \).

2. With the notation of (21.8.4) and (21.8.5), show that the group \( U_\alpha \) has two connected components if \( K_\alpha \) is isomorphic to \( SU(2, C) \), and is connected if \( K_\alpha \) is isomorphic to \( SO(3, R) \).

3. With the notation of (21.8.1), show that for every symmetric \( C \)-bilinear form \( \Phi \) on \( g_{(c)} \times g_{(c)} \), the spaces \( g_\alpha \) and \( g_\beta \) are orthogonal relative to \( \Phi \) if \( \alpha + \beta \neq 0 \), and \( g_0 = t_{(c)} \) is orthogonal to \( g_\alpha \) for each \( \alpha \in \mathfrak{s} \).

4. Show that a singular element of a compact connected Lie group lies in infinitely many maximal tori.
9. LINEAR REPRESENTATIONS OF SU(2)

The study of the roots of a compact connected Lie group \( G \) is based on the existence of the subgroups \( K_s \) of \( G \), locally isomorphic to \( SU(2) \) (21.8.5). In this section we shall show that it is possible to describe explicitly all the linear representations of \( SU(2) \). This result, applied to the restrictions to the subgroups \( K_s \) of the linear representation \( s \mapsto \text{Ad}(s) \otimes 1_c \) of \( G \) on \( \mathfrak{g}(C) \), will enable us in Section 20.10 to derive certain properties of the set \( S \) of roots of \( G \), on the basis of which it is possible to describe explicitly all possible sets of roots.

(21.9.1) We recall that if \( G \) is a connected, simply connected, real Lie group and \( E \) is a finite-dimensional complex vector space, the mapping \( V \mapsto V_* \) is a bijection of the set of linear representations of \( G \) on \( E \), onto the set of \((\mathbb{R}\text{-linear})\) homomorphisms of the Lie algebra \( \mathfrak{g}_e \) of \( G \) into the Lie algebra \( \mathfrak{gl}(E) = \text{End}(E) \) (19.7.6). By virtue of (21.5.2.1) and the connectedness of \( G \), a complex vector subspace \( F \) of \( E \) is stable under \( V \) if and only if it is stable under \( V_* \).

Furthermore, from any \( \mathbb{R}\text{-linear} \) homomorphism of Lie algebras

\[
\rho : \mathfrak{g}_e \to \mathfrak{gl}(E),
\]

we obtain a \( \mathbb{C} \text{-linear} \) homomorphism \( \rho \otimes 1_c : \mathfrak{g}_e \otimes_{\mathbb{R}} \mathbb{C} \to \mathfrak{gl}(E) \) of the complexification of \( \mathfrak{g}_e \) into \( \mathfrak{gl}(E) \), and we obtain in this way a bijection of the set of \( \mathbb{R}\text{-homomorphisms} \) of \( \mathfrak{g}_e \) into \( \mathfrak{gl}(E) \) onto the set of \( \mathbb{C}\text{-homomorphisms} \) of \( \mathfrak{g}_e \otimes_{\mathbb{R}} \mathbb{C} \) into \( \mathfrak{gl}(E) \), the inverse bijection being the restriction \( \rho' \mapsto \rho' |_{\mathfrak{g}_e} \) (21.5.2); equivalently, a complex vector subspace \( F \) of \( E \) is stable under \( \rho \) if and only if it is stable under \( \rho \otimes 1_c \).

Finally, if \( \mathfrak{g} \) is the Lie algebra of a (real or complex) Lie group, and \( \rho \) is a Lie algebra homomorphism of \( \mathfrak{g} \) into \( \mathfrak{gl}(E) = \text{End}(E) \), then (19.6.4) \( \rho \) extends uniquely to a homomorphism of associative algebras \( U(\rho) : U(\mathfrak{g}) \to \text{End}(E) \), which makes \( E \) into a left module over the enveloping algebra \( U(\mathfrak{g}) \) of \( \mathfrak{g} \); to say that a complex vector subspace \( F \) of \( E \) is stable under \( \rho \) therefore signifies that it is a \( U(\mathfrak{g})\text{-submodule} \) of \( E \).

From these remarks it follows that a linear representation \( V \) of a compact Lie group \( G \) on a finite-dimensional complex vector space \( E \) is irreducible if and only if \( E \) is a simple \( U(\mathfrak{g}_e \otimes_{\mathbb{R}} \mathbb{C})\text{-module} \), where the module structure on \( E \) is defined by \( U(V_* \otimes 1_c) \).

Moreover, for every linear representation \( V \) of the compact group \( G \) on a finite-dimensional complex vector space \( E \), the module \( E \) is a direct sum of simple \( U(\mathfrak{g}_e \otimes_{\mathbb{R}} \mathbb{C})\text{-submodules} \). Among these simple submodules there may
appear trivial $U(g_e \otimes \mathbb{R}C)$-modules, corresponding to the trivial representation of $G$ (21.1.1): in such a submodule, the product of any element of the module by any element of $g_e \otimes \mathbb{R}C$ is zero.

(21.9.2) The three matrices $Y, Z, H$ (21.8.5.4) are clearly linearly independent over $\mathbb{C}$ in $M_2(\mathbb{C})$, and therefore form a basis of the complexification of $su(2)$. Another, more convenient basis consists of the three matrices

(21.9.2.1)

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$X^+ = -\frac{i}{2}(Z + iY) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$X^- = \frac{i}{2}(Z - iY) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

from which it is clear that the complexification of $su(2)$ is $sl(2, \mathbb{C})$ (19.7.1.1).

The multiplication table for this basis is

$$[H, X^+] = 2X^+,$$

$$[H, X^-] = -2X^-,$$

$$[X^+, X^-] = H.$$

If $\rho: sl(2, \mathbb{C}) \rightarrow gl(E)$ is a $\mathbb{C}$-homomorphism of $sl(2, \mathbb{C})$ into the Lie algebra $gl(E)$, where $E$ is a finite-dimensional complex vector space, we denote by $(P, x) \mapsto P \cdot x$ the corresponding $U(sl(2, \mathbb{C}))$-module structure on $E$ (21.9.1) (so that $P$ is a sum of noncommutative monomials in $H$, $X^+$, and $X^-$ with complex coefficients).

(21.9.3) For each integer $m \geq 0$ there exists an irreducible linear representation of $SU(2)$ on a complex vector space $L_m$ of dimension $m + 1$, which has a basis $(e_j)_{0 \leq j \leq m}$ for which the $U(sl(2, \mathbb{C}))$-module structure of $L_m$ is defined by the formulas

(21.9.3.1)

$$H \cdot e_j = (m - 2j)e_j,$$

$$X^+ \cdot e_j = (m - j + 1)e_{j-1},$$

$$X^- \cdot e_j = (j + 1)e_{j+1}$$

(with the convention that $e_{-1} = e_{m+1} = 0$). Every irreducible linear representation of $SU(2)$ is equivalent to one of these representations.
Consider a linear representation \( V \), not necessarily irreducible, of \( \text{SU}(2) \) on a nonzero finite-dimensional complex vector space \( E \). For each \( \lambda \in \mathbb{C} \), let \( E_\lambda \) denote the subspace of all vectors \( x \) in \( E \) such that \( H \cdot x = \lambda x \).

The set \( P \) of complex numbers \( \lambda \) such that \( E_\lambda \neq \{0\} \) is the finite set of eigenvalues of the endomorphism \( V_*(H) \) of \( E \). It follows from (21.7.5), applied to the maximal torus of \( \text{SU}(2) \) for which \( R_iH \) is the Lie algebra, that \( E \) is the direct sum of the \( E_\lambda \) for \( \lambda \in P \).

(21.9.3.2) If \( x \in E_\lambda \), then \( X^+ \cdot x \in E_{\lambda + 2} \) and \( X^- \cdot x \in E_{\lambda - 2} \).

For by virtue of (21.9.2.2) we have
\[
H \cdot (X^+ \cdot x) = [H, X^+] \cdot x + X^+ \cdot (H \cdot x) = (\lambda + 2)X^+ \cdot x,
\]
\[
H \cdot (X^- \cdot x) = [H, X^-] \cdot x + X^- \cdot (H \cdot x) = (\lambda - 2)X^- \cdot x.
\]

An element \( x \in E \) is said to be primitive for the eigenvalue \( \lambda \in P \) if \( x \neq 0 \) and if

(21.9.3.3) \( H \cdot x = \lambda x, \quad X^+ \cdot x = 0. \)

We then have:

(21.9.3.4) There exists a primitive element in \( E \).

Let \( z \) be a nonzero element of some \( E_\lambda \). Not all of the vectors \( (X^+)^n \cdot z \) \( (n \geq 0) \) can be different from 0, otherwise by virtue of (21.9.3.2) they would all belong to distinct eigenspaces \( E_\mu \), which is absurd. If \( k \geq 0 \) is the smallest integer such that \( (X^+)^{k+1} \cdot z = 0 \), the vector \( x = (X^+)^k \cdot z \) is primitive for the eigenvalue \( \lambda + 2k \).

(21.9.3.5) Let \( M \) be a (not necessarily finite-dimensional) complex vector space, \( (P, z) \to P \cdot z \) a \( \text{U}(\text{sl}(2, \mathbb{C})) \)-module structure on \( M \), and let \( x \neq 0 \) be an element of \( M \) satisfying (21.9.3.3). For each integer \( j \geq 0 \), put \( x_j = (X^-)^j \cdot x/j! \)

(i) For each integer \( j \geq 0 \), we have

(21.9.3.6) \( H \cdot x_j = (\lambda - 2j)x_j, \)
\( X^- \cdot x_j = (j + 1)x_{j+1}, \)
\( X^+ \cdot x_j = (\lambda - j + 1)x_{j-1} \)

with the convention that \( x_{-1} = 0. \)
(ii) If $M$ is finite-dimensional, then $\lambda$ is an integer $m \geq 0$, the subspace $F$ of $M$ spanned by the $x_j$ is a simple $U(sl(2, \mathbb{C}))$-submodule, and the corresponding irreducible linear representation of $SU(2)$ is equivalent to that defined by (21.9.3.1).

The first of the formulas (21.9.3.6) follows from the calculation in (21.9.3.2), and the second follows from the definition of the $x_j$. As to the third, it is true by hypothesis when $j = 0$, and we proceed by induction on $j \geq 1$. By use of (21.9.2.2) and the first of the formulas (21.9.3.6), we obtain

$$jX^+ \cdot x_j = (X^+ X^-) \cdot x_{j-1} = [X^+, X^-] \cdot x_{j-1} + X^- \cdot (X^+ \cdot x_{j-1}) = H \cdot x_{j-1} + (\lambda - j + 2)X^- \cdot x_{j-2} = (\lambda - 2j + 2 + (j - 1)(\lambda - j + 2))x_{j-1} = j(\lambda - j + 1)x_{j-1}.$$

The $x_j$ belong to eigenspaces of $H$ corresponding to distinct eigenvalues of $H$ in $M$, hence the nonzero $x_j$ are linearly independent. Consequently, if $M$ is finite-dimensional, there exists a smallest integer $m \geq 0$ such that $x_{m+1} = 0$; by (21.9.3.6), we then have $0 = X^+ \cdot x_{m+1} = (\lambda - m)x_m$, whence $\lambda = m$. The subspace $F$ spanned by the $m + 1$ vectors $x_j$ ($0 \leq j \leq m$) then has these vectors as a basis, because they are all nonzero and hence linearly independent. The formulas (21.9.3.6) show that $F$ is a $U(sl(2, \mathbb{C}))$-submodule of $M$. To show that $F$ is simple, we remark that if $F'$ is a nonzero submodule of $F$, it is a vector subspace of $F$ that is stable under the endomorphism $z \mapsto H \cdot z$, hence is a direct sum of a certain number of 1-dimensional eigenspaces $\mathbb{C} x_j$ of this endomorphism (A.24.3); in other words, there exists at least one index $j \in [0, m]$ such that $x_j \in F'$. But then, since $m - j + 1 \neq 0$ for all $j$ such that $0 \leq j \leq m$, the third of the formulas (21.9.3.6) shows that $x_0 \in F'$, and the second that $x_k \in F'$ for $0 \leq k \leq m$, so that finally $F' = F$.

It remains to show that for each integer $m \geq 0$, the formulas (21.9.3.1) effectively define a homomorphism of $sl(2, \mathbb{C})$ into $gl(L_m)$ for which $L_m$ is a simple $U(sl(2, \mathbb{C}))$-module. The first point amounts to the verification that

$$H \cdot (X^+ \cdot e_j) - X^+ \cdot (H \cdot e_j) = 2X^+ \cdot e_j,$$
$$H \cdot (X^- \cdot e_j) - X^- \cdot (H \cdot e_j) = -2X^- \cdot e_j,$$
$$X^+ \cdot (X^- \cdot e_j) - X^- \cdot (X^+ \cdot e_j) = H \cdot e_j,$$

which is a simple calculation. Finally, the proof above that $F$ is simple shows that $L_m$ is simple, and the proof of (21.9.3) is therefore complete.
(21.9.4) Let $V$ be an arbitrary continuous linear representation of $\text{SU}(2)$ on a finite-dimensional complex vector space $E$, and let $\rho = V_\ast$ be the derived homomorphism. Then $E$ is the direct sum of $r$ simple $\text{U}(\text{sl}(2, \mathbb{C}))$-submodules $E_1, \ldots, E_r$, with $E_k$ isomorphic to $L_{m_k}$, say. From (21.9.3) we deduce immediately the following simple rule for determining the integer $r$ and the integers $m_k$: $r$ is the dimension of the kernel $N$ of the endomorphism $\rho(X^+)$ of $E$; this kernel $N$ is stable under the endomorphism $\rho(H)$, and the eigenvalues (each counted according to its multiplicity) of this endomorphism of $N$ are precisely the numbers $m_k$.

Another characterization of the number $r$, which follows from the first of the formulas (21.9.3.1), is that it is the sum of the multiplicities of the eigenvalues 0 and 1 of $\rho(H)$.

**PROBLEMS**

1. In the almost simple compact Lie group $\text{SU}(2) = G$, the matrices $r(t) = \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix}$, where $t \in I = [-\pi, \pi] \subset \mathbb{R}$, form a maximal torus $T$ of $G$. For each central function $f$ on $G$, put $f^0(t) = f(r(t))$. For $f$ to belong to $\mathcal{L}^1(G)$ it is necessary and sufficient that $f^0(t) \sin^2 t$ belong to $\mathcal{L}^1(1)$, and we have

$$\int_G f(s) \, dm_G(s) = \frac{1}{\pi} \int_{-\pi}^{\pi} f^0(t) \sin^2 t \, dt$$

(21.15.4.2).

(a) Let $\chi_m$ denote the character of the irreducible representation of $G$ on $L_m$. Then

$$\chi_m^0(t) = \frac{\sin(m + 1)t}{\sin t} = \sum_{j=0}^{m} e^{i(m-2j)t}.$$ 

For each $f \in \mathcal{L}^1(G)$ we have $(f \mid \chi_m) = 2 \sum_{j=0}^{m} c_{m-2j}$, where $c_k$ is the coefficient of $e^{ikt}$ in the Fourier series of the function $f^0(t) \sin^2 t$.

(b) Let $p$ be a real number such that $0 < p < 1$, and let $a_n = (n+1)^p - (n-1)^p$ for each integer $n \geq 1$. Then the series

$$g_p(t) = 2 + \sum_{n=1}^{\infty} a_n \cos nt$$

converges for each $t$ that is not an integer multiple of $2\pi$, and its sum belongs to $\mathcal{L}^1(1)$ (Section 22.19, Problem 10(c)). Hence there exists a central function $f_p \in \mathcal{L}^1(G)$ such that $f_p^0(t) \sin^2 t = g_p(t)$. Deduce (by taking $p$ close to 1) that the majorations of Section 21.2, Problem 3(e) cannot be improved by replacing the exponents of by smaller exponents.

(c) There exists a continuous central function $h$ on $G$ such that $h^0(t) = \sum_{n=2}^{\infty} n^{-2} \cos n^3 t$. 

With the notation of Section 21.2, Problem 3, show that the family of numbers $N_\alpha(h \cdot u_\mu)$ is unbounded.

2. With the notation of Problem 1, show that

$$x_m x_n = x_{m+n} + x_{m+n-2} + \cdots + x_{|m-n|}.$$  

10. PROPERTIES OF THE ROOFS OF A COMPACT SEMISIMPLE GROUP

(21.10.1) Let $K$ be a compact, connected, semisimple Lie group, $\mathfrak{t}$ its Lie algebra, and $t$ a maximal commutative subalgebra of $\mathfrak{t}$. Let $\mathfrak{g}$ denote the complexified Lie algebra $\mathfrak{t}(\mathbb{C})$, $\mathfrak{h}$ its commutative subalgebra $\mathfrak{t}(\mathbb{C})_0$, and $S$ the set of roots of $\mathfrak{t}$ relative to $t$. By abuse of notation, for each root $\alpha \in S$ we shall denote again by $\alpha$ its extension $\alpha \otimes 1_\mathbb{C}$ to a $\mathbb{C}$-linear form on $\mathfrak{h}$; these linear forms are called the roots of $\mathfrak{g}$ relative to $h$. The complex Lie algebra $\mathfrak{g}$, its commutative subalgebra $\mathfrak{h}$, and the finite set $S \subset h^* - \{0\}$ of linear forms have the following properties:

(A) There exists a decomposition of $\mathfrak{g}$ as a direct sum of nonzero complex vector subspaces:

$$\mathfrak{g} = \mathfrak{h} \oplus \left( \bigoplus_{\alpha \in S} \mathfrak{g}_\alpha \right)$$

such that for each $h \in \mathfrak{h}$ and each $x \in \mathfrak{g}_\alpha$, we have

$$[h, x] = \alpha(h)x.$$  

(B) There exists a nondegenerate symmetric $\mathbb{C}$-bilinear form $\Phi$ on the vector space $\mathfrak{g}$ such that

$$\Phi([x, y], z) + \Phi(y, [x, z]) = 0$$

for all $x, y, z \in \mathfrak{g}$; also, for each root $\alpha \in S$, there exists $h^0_\alpha \in \mathfrak{h}$ such that

$$\alpha(h) = \Phi(h, h^0_\alpha)$$

for all $h \in \mathfrak{h}$, and

$$\alpha(h^0_\alpha) \neq 0.$$
10. PROPERTIES OF THE ROOTS OF A COMPACT SEMISIMPLE GROUP

(C) The center of \( g \) is \( \{0\} \).

Property (A) has in effect been established in (21.8.1); property (C) follows from the hypothesis that \( K \) is semisimple (21.6.3). As to (B), take any \( K \)-invariant \( \mathbb{R} \)-bilinear scalar product on \( t \) (21.4.3), and extend it to a symmetric \( \mathbb{C} \)-bilinear form \( \Phi \) on \( \mathfrak{f}(c) = g \); this is always possible, and in one way only (note that \( \Phi \) is not a hermitian scalar product). The existence of the element \( h^0 \) satisfying (21.10.1.4) and (21.10.1.5) then follows from (21.8.5) and (21.8.5.1).

In view of later applications (Section 21.20), in this and the following section we shall not make use (unless otherwise stated) of the fact that \( g \) and \( \mathfrak{h} \) arise by complexification of the Lie algebras of a compact semisimple group and one of its maximal tori; we shall use only the properties (A), (B), (C) listed above.

(21.10.2) (i) If \( \alpha, \beta \) are two roots in \( S \) such that \( \alpha + \beta \neq 0 \), then \( g_\alpha \) and \( g_\beta \) are orthogonal relative to \( \Phi \). In particular, \( g_\alpha \) is totally isotropic, for each \( \alpha \in S \).

(ii) For each \( \alpha \in S \), we have \( -\alpha \in S \), and \( g_\alpha \) and \( g_{-\alpha} \) are totally isotropic subspaces of the same dimension. Each of the subspaces \( \mathfrak{h} \), \( g_\alpha \oplus g_{-\alpha} \) is nonisotropic.

(iii) For each \( \alpha \in S \), and each \( x \in g_\alpha \), \( y \in g_{-\alpha} \), we have

\[
[x, y] = \Phi(x, y)h^0.
\]

(i) If \( x \in g_\alpha \), \( y \in g_\beta \), \( h \in \mathfrak{h} \), then by (21.10.1.3) and (21.10.1.2) we have \( \Phi([h, x], y) + \Phi(x, [h, y]) = 0 \), and hence \( (\alpha(h) + \beta(h))\Phi(x, y) = 0 \). Since \( \alpha + \beta \neq 0 \), there exists \( h \in \mathfrak{h} \) such that \( \alpha(h) + \beta(h) \neq 0 \), and therefore \( \Phi(x, y) = 0 \).

(ii) The same proof shows that \( \mathfrak{h} \) is orthogonal to \( g_\alpha \) for each \( \alpha \in S \); furthermore, if the roots \( \alpha, \beta \) are such that \( \beta \neq \alpha \) and \( \beta \neq -\alpha \), then \( g_\beta \) and \( g_{-\beta} \) are orthogonal to \( g_\alpha \oplus g_{-\alpha} \). In other words, \( g \) is the direct sum of \( \mathfrak{h} \) and the distinct subspaces \( g_\alpha \oplus g_{-\alpha} (\alpha \in S) \), which are mutually orthogonal; each of these subspaces is therefore nonisotropic, and since each \( g_\alpha \) is totally isotropic by (i), the assertions in (ii) are consequences of the elementary properties of nondegenerate symmetric \( \mathbb{C} \)-bilinear forms.

(iii) Since the restriction of \( \Phi \) to \( \mathfrak{h} \times \mathfrak{h} \) is nondegenerate, by (ii), the element \( h^0 \) satisfying (21.10.1.4) for all \( h \in \mathfrak{h} \) is unique. If \( x \in g_\alpha \) and \( y \in g_{-\alpha} \), then by (21.10.1.2) and (21.10.1.3) we have, for all \( h \in \mathfrak{h} \),

\[
\Phi(h, [x, y]) = \Phi([h, x], y) = \alpha(h)\Phi(x, y) = \Phi(h, \Phi(x, y)h^0) = \Phi(h, \Phi(x, y)h^0)
\]

and (21.10.2.1) follows from this, since the restriction of \( \Phi \) to \( \mathfrak{h} \times \mathfrak{h} \) is nondegenerate.
(21.10.2.2) With the convention that \( g_{\lambda} = \{0\} \) for \( \lambda \in \mathfrak{h}^* \) whenever \( \lambda \) is not a root, we have \([g_{\alpha}, g_{\beta}] \subseteq g_{\alpha + \beta}\) for any two roots \( \alpha, \beta \) (cf. (21.10.5)). For it follows from the Jacobi identity that

\[
[h, [x, y]] = [[h, x], y] + [x, [h, y]] = (\alpha(h) + \beta(h))[x, y]
\]

for all \( h \in \mathfrak{h}, x \in g_{\alpha}, y \in g_{\beta} \), and the result therefore follows from (21.8.1.3).

(21.10.3) (i) For each \( \alpha \in \mathfrak{s} \) there exists one and only one element \( h_{\alpha} \in \mathfrak{h} \) belonging to \([g_{\alpha}, g_{-\alpha}]\) and such that

\[
(21.10.3.1) \quad \alpha(h_{\alpha}) = 2.
\]

The spaces \( g_{\alpha} \) and \( h_{\alpha} = [g_{\alpha}, g_{-\alpha}] \subseteq \mathfrak{h} \) are one-dimensional. For each non-zero \( x_{\alpha} \in g_{\alpha} \) there exists one and only one element \( x_{-\alpha} \in g_{-\alpha} \) such that

\[
(21.10.3.2) \quad [x_{\alpha}, x_{-\alpha}] = h_{\alpha}
\]

and we have

\[
(21.10.3.3) \quad [h_{\alpha}, x_{\alpha}] = 2x_{\alpha}, \quad [h_{\alpha}, x_{-\alpha}] = -2x_{-\alpha},
\]

so that the subspace \( s_{\alpha} = Ch_{\alpha} \oplus Cx_{\alpha} \oplus Cx_{-\alpha} \) of \( g \) is a Lie subalgebra of \( g \) isomorphic to \( \text{sl}(2, \mathbb{C}) \).

(ii) The set \( \mathfrak{s} \) of roots has the following properties:

(S_1) \( \mathfrak{s} \) spans the vector space \( \mathfrak{h}^* \).

(S_2) For each \( \alpha \in \mathfrak{s} \), the linear mapping \( \sigma_{\alpha} : \lambda \mapsto \lambda - \lambda(h_{\alpha})\alpha \) is an involutory bijection of \( \mathfrak{h}^* \) onto itself, not equal to the identity mapping, and \( \mathfrak{s} \) is stable under \( \sigma_{\alpha} \).

(S_3) For each pair \( \alpha, \beta \) in \( \mathfrak{s} \), the number \( \beta(h_{\alpha}) \) is an integer (positive, negative, or zero).

(S_4) For each \( \alpha \in \mathfrak{s} \), the only element of the form \( t\alpha \) (where \( t \in \mathbb{C} \) and \( t \neq 1 \)) belonging to \( \mathfrak{s} \) is \(-\alpha \).

(i) Since the restriction of \( \Phi \) to \( g_{\alpha} \oplus g_{-\alpha} \) is nondegenerate (21.10.2(ii)), it follows from (21.10.2.1) that the vector space \([g_{\alpha}, g_{-\alpha}]\) is one-dimensional. It is clear that the only element \( h_{\alpha} \) in this space that satisfies (21.10.3.1) is \( h_{\alpha} = 2(\alpha(h_{\alpha}^0))^{-1}h_{\alpha}^0 \). For each \( x_{\alpha} \neq 0 \) in \( g_{\alpha} \), by virtue of (21.10.2.3(iii)) and the elementary properties of nondegenerate symmetric bilinear forms, there exists an element \( y \in g_{-\alpha} \) such that \( \Phi(x_{\alpha}, y) \neq 0 \). By multiplying \( y \) by a suitable nonzero scalar and using (21.10.2.1), we obtain an element
10. PROPERTIES OF THE ROOTS OF A COMPACT SEMISIMPLE GROUP

$x_-, \in g_-$ satisfying (21.10.3.2), and then the relations (21.10.3.3) follow from (21.10.3.1). For each $x_+ \neq 0$ in $g_+$ and each $x_- \in g_-$ satisfying (21.10.3.2), the subspace $s_x = Ch_x \oplus Cx_+ \oplus Cx_- \oplus Cx_-$ of $g$ is therefore a Lie subalgebra isomorphic to $sl(2, \mathbb{C})$ (21.9.2). Next, suppose that $\text{dim}(g_+) > 1$, and hence also $\text{dim}(g_-) > 1$. Then the hyperplane in $g$ with equation $\Phi(x_+, y) = 0$ would have nonzero intersection with $g_-$; in other words, there would exist a vector $y \neq 0$ in $g_-$ such that $[x_+, y] = 0$ and $[h_-, y] = -2y$, by virtue of (21.10.2.1). But this would mean that, for the homomorphism $u \mapsto \text{ad}(u)$ of $s_x$ into $gl(g)$, $y$ was a primitive element (21.9.3) for the eigenvalue $-2$ of $\text{ad}(h_-)$, contrary to (21.9.3.5). The uniqueness of $x_- \in g_-$ satisfying (21.10.3.2) is now evident.

We shall henceforth identify the Lie algebra $s_x$ with $sI(2, \mathbb{C})$ by identifying $h_-$, $x_+$, and $x_-$ with $H$, $X'$, and $X_-$, respectively (21.9.2.1).

(ii) If the vector subspace of $\mathfrak{g}^*$ spanned by $\mathfrak{S}$ were not the whole of $\mathfrak{h}^*$, there would exist $h \neq 0$ in $\mathfrak{h}$ such that $\alpha(h) = 0$ for all roots $\alpha \in \mathfrak{S}$; hence $h$ would belong to the center of $g$, contrary to hypothesis. This establishes (S_1).

Let $\alpha, \beta \in \mathfrak{S}$ and let $y$ be a nonzero element of $g_\beta$. Then $[h_-, y] = \beta(h_+)y$, so that $\beta(h_+)$ is an eigenvalue of $\text{ad}(h_+)$ in $g$. By virtue of the identification of $s_x$ with $sI(2, \mathbb{C})$, it follows from (21.9.3) that $\beta(h_+)$ is an integer $p$, which proves (S_3).

It follows from the relation $\alpha(h_+) = 2$ that the linear mapping $\alpha_\mathfrak{H}: \lambda \mapsto \lambda - \lambda(h_+)\alpha$ of $\mathfrak{h}^*$ into itself is such that $\alpha_\mathfrak{H}^2 = 1$. With the identification of $s_x$ with $sl(2, \mathbb{C})$, the $U(sl(2, \mathbb{C}))-submodule of g$ generated by the element $y$ above may be identified with one of the modules $L_m$ (21.9.3.1), the element $y$ being identified with $e_1$, where $p = m - 2j$ (A.24.4). Now define $z = (\text{ad}(x_-))y$ if $p \geq 0$, and $z = (\text{ad}(x_+))^p - y$ if $p \leq 0$. By virtue of the formulas (21.9.3.1), in all cases $z$ is a nonzero multiple of $e_{j+p} = e_{m-j}$, and we have $z \in g_{\beta - px}$ by (21.10.2.2). This shows that $\beta - px \in \mathfrak{S}$, and proves (S_2).

If $\alpha$ and $\beta = t\alpha$ both belong to $\mathfrak{S}$, it follows from (S_3) and (21.10.3.1) that $2t \in \mathbb{Z}$. Since $\alpha = t^{-1}\beta$, we may assume that $0 < |t| \leq 1$, and then the only possible values of $t$ are $\pm \frac{1}{2}, \pm 1$. Suppose that $\beta \in \mathfrak{S}$ is such that $2\beta \in \mathfrak{S}$, and let $y$ be a nonzero element of $g_{2\beta}$; then $[h_\beta, y] = 2\beta(h_+)y = 4y \neq 0$. Now $3\beta = 2\beta + \beta$ is not a root, hence from (21.10.2.2) $\text{ad}(x_\beta) \cdot y = 0$. But since $h_\beta = [x_\beta, x_\beta]$, we have

$$\text{ad}(h_\beta) \cdot y = \text{ad}(x_\beta)(\text{ad}(x_\beta) \cdot y) - \text{ad}(x_\beta) \cdot (\text{ad}(x_\beta) \cdot y)$$

$$= \text{ad}(x_\beta)(\text{ad}(x_\beta) \cdot y).$$

By (21.10.2.2) again, $\text{ad}(x_\beta) \cdot y \in g_\beta$; since $g_\beta$ is one-dimensional, it follows that $\text{ad}(x_\beta) \cdot y$ is a scalar multiple of $x_\beta$, so that $\text{ad}(x_\beta) \cdot (\text{ad}(x_\beta) \cdot y) = 0$. This contradicts the previous calculation that $\text{ad}(h_\beta) \cdot y = 4y \neq 0$, and thereby proves (S_4).
(21.10.4) With the notation of (21.10.3), let \( \alpha, \beta \) be two roots that are not proportional to each other, and let \( p \) (resp. \( q \)) be the largest integer \( \geq 0 \) such that \( \beta - p\alpha \) (resp. \( \beta + q\alpha \)) is a root. Then \( \beta + k\alpha \) is a root for all integers \( k \) such that \( -p \leq k \leq q \); also \( \beta(h_a) = p - q \), and \( \text{ad}(x_a) \) is a bijection of \( g_{\beta + k\alpha} \) onto \( g_{\beta + (k + 1)\alpha} \) for \( -p \leq k \leq q - 1 \).

Let \( E \) denote the vector subspace of \( g \) that is the direct sum of the \( g_{\beta + k\alpha} \) for all integers \( k \in \mathbb{Z} \) such that \( \beta + k\alpha \) is a root. With the identification (21.10.3) of the subalgebra \( s_a \) of \( g \) with \( \mathfrak{sl}(2, \mathbb{C}) \), it follows from (21.10.2.2) that \( E \) is an \( U(e_\mathfrak{sl}(2, \mathbb{C})) \)-module. Since the \( g_{\beta + k\alpha} \) such that \( \beta + k\alpha \) is a root are one-dimensional, and since all the numbers \( \beta(h_a) + k\alpha(h_a) = \beta(h_a) + 2k \) are all distinct and of the same parity, it follows immediately from (21.9.4) that \( E \) is simple, hence isomorphic to \( L_m \) for some integer \( m \geq 0 \). Hence \( E \) is the direct sum of \( m + 1 \) subspaces \( g_{\beta + k\alpha} \), with \( a \leq k \leq b \), where \( a \) and \( b \) are rational integers such that \( b - a = m \), \( \beta + k\alpha \in S \) for \( a \leq k \leq b \), and \( \beta(h_a) + 2a = -m \), \( \beta(h_b) + 2b = m \). Since the interval \([a, b]\) of \( \mathbb{Z} \) contains \( 0 \), we have \( a = -p \leq 0 \), \( b = q \geq 0 \), and \( \beta(h_a) = p - q \). Finally, the last assertion of the proposition follows from the second of the formulas (21.9.3.1).

(21.10.5) If \( \alpha, \beta \) are two roots, then

\[
\begin{align*}
\text{if } \alpha + \beta \text{ is not a root,} \\
\text{if } \alpha + \beta \text{ is a root.}
\end{align*}
\]

The first assertion has already been proved (21.10.2.2). If \( \alpha + \beta \) is a root, then with the notation of (21.10.4) we have \( q \geq 1 \), and \( \text{ad}(x_a) \) is a bijection of \( g_{\beta} \) onto \( g_{\alpha + \beta} \), by (21.10.4).

(21.10.6) When \( g, \mathfrak{h} \) and \( S \) arise from a compact connected semisimple group \( K \) and a maximal torus of \( K \), as at the beginning of this section, we can say more about the properties of the elements \( h_a, x_a, \) and \( x_{-a} \) of (21.10.3). Starting with an element \( x'_a \neq 0 \in g_a \), we have \( c(x'_a) \in g_{-a} \) (21.8.2); writing \( y_a = x'_a + c(x'_a) \), \( z_a = i(x'_a - c(x'_a)) \) as in (21.8.3), we obtain the formulas (21.8.5.3), with \( -i\alpha(h_a^0) = a_a > 0 \), from which we deduce

\[
(21.10.6.1) \quad [2x'_a, -2c(x'_a)] = a_a h_a
\]

where \( h_a = -2ia_a^{-1}h_a^0 \in \mathfrak{h} \) it satisfies (21.10.3.1). It follows that the vectors
\[ x_\alpha = 2a_\alpha^{-1/2}x_\alpha, \quad x_{-\alpha} = -2a_\alpha^{-1/2}c(x_\alpha) \] satisfy the relation (21.10.3.2), and are such that

\[(21.10.6.2) \quad x_{-\alpha} = -c(x_\alpha).\]

By virtue of (21.10.5), we may write

\[(21.10.6.3) \quad [x_\alpha, x_\beta] = N_{\alpha, \beta} x_\alpha + \beta\]

for all pairs of roots \(\alpha, \beta\) such that \(\alpha + \beta\) is a root. Since \([c(x_\alpha), c(x_\beta)] = c([x_\alpha, x_\beta])\), it follows from (21.10.6.2) that

\[(21.10.6.4) \quad N_{-\alpha, -\beta} = -N_{\alpha, \beta}\]

if \(\alpha + \beta \in \mathfrak{S}\). It may be shown (21.20.7) that it is possible to choose the \(h_\alpha, x_\alpha, x_{-\alpha}\) such that the numbers \(N_{\alpha, \beta}\) are real.

A basis (over \(\mathbb{C}\)) of \(\mathfrak{g} = \mathfrak{t}_{\mathfrak{c}0}\) consisting of elements \(x_\alpha\) satisfying the conditions of (21.10.3) and also (21.10.6.4) for which the \(N_{\alpha, \beta}\) are real, together with an \(\mathbb{R}\)-basis of it, is called a Weyl basis of \(\mathfrak{g}\) (cf. Section 21.20).

We remark also that the linear mapping \(\lambda \mapsto s_\alpha \cdot \lambda\) of \(\mathfrak{h}^*\) onto itself, defined by the element \(s_\alpha\) of the Weyl group constructed in (21.8.7), is the same as the mapping \(\sigma_\alpha: \lambda \mapsto \lambda - \lambda(h_\alpha)\alpha\), which features in (S2) of (21.10.3): for it follows immediately from (21.8.7) that \((s_\alpha \cdot \lambda)(u) = \lambda(u)\) for \(u \in u_\alpha\), and \((s_\alpha \cdot \lambda)(h_\alpha) = -\lambda(h_\alpha)\).

**PROBLEMS**

1. Let \(G\) be a compact connected Lie group and \(G'\) a connected closed subgroup of \(G\); let \(\mathfrak{g}, \mathfrak{g}'\) be the Lie algebras of \(G, G'\); let \(T\) be a maximal torus of \(G\) such that \(T' = T \cap G'\) is a maximal torus of \(G'\) (Section 21.7, Problem 8), and let \(t, t'\) be the Lie algebras of \(T, T'\).

Show that every root of \(G'\) relative to \(T'\) is the restriction to \(t'\) of at least one root of \(G\) relative to \(T\). (Observe that \(\mathfrak{g}(t)\) is stable under \(\text{Ad}(t)\) for all \(t \in T'\), and that \(\mathfrak{g}_{\mathfrak{c}0}\) is the direct sum of \(t_{\mathfrak{c}0}\) and the \(\mathfrak{g}_{\alpha}, \) where \(\alpha\) runs through the set of restrictions to \(t'\) of the roots of \(G\) relative to \(T\), and \(\mathfrak{g}_{\alpha}\) denotes the sum of the \(\mathfrak{g}_{\alpha}\) for the roots \(\alpha\) whose restriction to \(t'\) is \(\alpha'\).)

2. With the notation of Problem 1, assume that \(T' = T\), so that \(G'\) has the same rank as \(G\). Then every root of \(G'\) relative to \(T\) is also a root of \(G\) relative to \(T\), i.e., \(\mathfrak{S}(G') \subset \mathfrak{S}(G)\).

(a) Suppose that \(G\) is the product of almost simple compact groups \(G_i (1 \leq i \leq r)\), \(T\) being
the product of maximal tori $T_i \subset G_i$. Show that $G'$ is necessarily a product of connected closed subgroups $G_i' \supset T_i$ of $G_i$. (If $G_i'$ is the projection of $G'$ in $G_i$, use the fact that every $x \in G'$ is of the form $yty^{-1}$, where $t \in T$ and $y \in G'$, and deduce that the projection $x_i$ of $x$ in $G_i'$ belongs to $G_i'$.)

(b) The Lie algebra $g_{G'}$ is the direct sum of $g_{G_i'}$ and the $a_\alpha$ for the roots $\alpha \in S(G) - S(G')$. Show that the subgroup of $G$ consisting of the elements $s \in G$ such that the restriction of $\text{Ad}(s)$ to $a_\alpha$ is the identity mapping, for each $\alpha \in S(G) - S(G')$, is the largest normal subgroup of $G$ contained in $G'$. (Consider the homogeneous space $G/G'$.)

(c) Let $D(G)$ denote the union of the hyperplanes in $\mathfrak{t}$ described by the equations $\alpha(u) = 2\pi in$, where $\alpha \in S(G)$ and $n \in \mathbb{Z}$; $D(G)$ is also the inverse image under $\exp_G$ of the set of singular elements of $T$ (21.8.4.2). Define $D(G')$ in the same way. In general, if $\Delta$ is the union of a family of hyperplanes in $\mathfrak{t}$ consisting of a finite number of families of parallel hyperplanes, a point of $\Delta$ is called special if it lies in a hyperplane of each of the parallel families. The special points of $D(G)$ form the inverse image under $\exp_G$ of the center of $G$. Deduce from (b) that if $G$ is almost simple and if $\Delta$ is the union of the hyperplanes contained in $D(G)$ but not in $D(G')$, then every special point of $\Delta$ is also a special point of $D(G)$ (i.e., its image under $\exp_G$ lies in the center of $G$). Deduce that if $G' \neq G$, then $\dim(G') \leq \dim(G) - 2 \text{rank}(G)$ (where $\text{rank}(G) = \dim(T)$).

3. With the notation of (21.8.4), show that the union of the conjugates of a subgroup $U_\alpha$ in $G$ is the continuous image of a compact manifold of dimension $\dim(G) - 3$. (Use the fact that $\dim(\mathfrak{z}(U_\alpha)) = \dim(T) + 2$.) Deduce that the set of regular points of $G$ (21.7.13) is a dense open subset of $G$ (cf. (16.23.2)).

11. BASES OF A ROOT SYSTEM

(21.11.1) Let $F$ be a complex vector space of finite dimension $n$. A finite subset $\mathfrak{S}$ of $F$ that does not contain 0 is called a reduced root system in $F$ if it satisfies the conditions $(S_1)$, $(S_2)$, $(S_3)$, and $(S_4)$ of (21.10.3), with $\mathfrak{h}^*$ replaced by $F$ and the $C$-linear forms $\lambda \mapsto \lambda(h_\alpha)$ replaced by $C$-linear forms $v_\alpha$ on $F$, so that $\sigma_\alpha(\lambda) = \lambda - v_\alpha(\lambda)x$.

In this terminology, we have proved in (21.10.3) that the set $\mathfrak{S}$ of roots of $\mathfrak{g}$ relative to $\mathfrak{h}$ (or of $K$ relative to $T$, if we had started with a compact connected semisimple group $K$ and a maximal torus $T$ of $K$) is a reduced root system in $\mathfrak{h}^*$. Conversely, it can be shown that every reduced root system is (up to isomorphisms of complex vector spaces) the set of roots of a compact connected semisimple Lie group $K$, whose Lie algebra is determined up to isomorphism by the root system. Moreover, it is possible to describe explicitly all reduced root systems (and hence all compact connected Lie groups). We shall not give the proofs of these facts, for which we refer to [79] and [85]; our purpose in this section is to deduce from the definition some properties of reduced root systems that are useful in the theory of compact connected Lie groups.
(21.11.2) Let $\mathbf{S}$ be a reduced root system in a vector space $\mathbf{F}$ of dimension $n$ over $\mathbb{C}$ (21.11.1).

(i) The vector subspace $\mathbf{F}_0$ over $\mathbb{R}$ spanned by $\mathbf{S}$ has dimension $n$, and the real vector subspace of the dual $\mathbf{F}^*$ of $\mathbf{F}$ spanned by the forms $v_\alpha$ is of dimension $n$, and may be identified with the dual $\mathbf{F}^*_0$ of $\mathbf{F}_0$.

(ii) There exists a scalar product $(\lambda | \mu)$ on $\mathbf{F}_0$, with respect to which the $\mathbb{R}$-linear mappings $\sigma_\alpha : \lambda \mapsto \lambda - v_\alpha(\lambda)\alpha$ of $\mathbf{F}_0$ into itself are orthogonal reflections in hyperplanes, such that $\sigma_\alpha(\alpha) = -\alpha$, and the group $\mathbf{W}_\mathbf{S}$ of orthogonal transformations of $\mathbf{F}_0$ generated by the $\sigma_\alpha$ is finite.

The restrictions $v_\alpha^0$ of the linear forms $v_\alpha$ to $\mathbf{F}_0$ are real-valued, because by hypothesis the numbers $v_\alpha(\beta) (\alpha, \beta \in \mathbf{S})$ are integers, hence $\mathbf{F}_0$ is stable under the mappings $\lambda \mapsto \lambda - v_\alpha(\lambda)\alpha$. Since $\mathbf{S}$ spans $\mathbf{F}_0$, any endomorphism of $\mathbf{F}_0$ that fixes each element of $\mathbf{S}$ is the identity mapping; consequently the restriction mapping $w \mapsto w | \mathbf{S}$ of $\mathbf{W}_\mathbf{S}$ into the group of all permutations of $\mathbf{S}$ is injective, and therefore $\mathbf{W}_\mathbf{S}$ is finite. Hence there exists a scalar product $(\lambda | \mu)$ on $\mathbf{F}_0$ that is invariant under $\mathbf{W}_\mathbf{S}$ (20.11.3.1); each element of $\mathbf{W}_\mathbf{S}$ is therefore an orthogonal transformation relative to this scalar product. In particular, since $\sigma_\alpha$ is an orthogonal transformation that is not the identity and that fixes the points of the hyperplane $\mathbf{M}_\alpha$ in $\mathbf{F}_0$ given by the equation $v_\alpha^0(\lambda) = 0$, it is necessarily the orthogonal reflection in this hyperplane $\mathbf{M}_\alpha$. Next, by expressing $\sigma_\alpha^2$ as the identity, we obtain $v_\alpha^0(\lambda)(v_\alpha^0(\alpha) - 2)\alpha = 0$, and since $v_\alpha^0$ is not identically zero on $\mathbf{F}_0$ (because $\mathbf{F}_0$ spans $\mathbf{F}$), we have $v_\alpha^0(\alpha) = 2$ and $\sigma_\alpha(\alpha) = -\alpha$; this implies that $\alpha$ is orthogonal to $\mathbf{M}_\alpha$, and consequently $\sigma_\alpha$ is the reflection

$$\sigma_\alpha : \lambda \mapsto \lambda - \frac{2(\alpha | \lambda)}{(\alpha | \alpha)} \alpha,$$

which shows that $v_\alpha^0(\lambda) = 2(\alpha | \lambda)/(\alpha | \alpha)$. If $j : \mathbf{F}_0 \rightarrow \mathbf{F}_0^*$ is the bijective linear mapping canonically associated with the scalar product, so that the image of $\mu \in \mathbf{F}_0$ under $j$ is the linear form $\lambda \mapsto (\mu | \lambda)$ on $\mathbf{F}_0$, then we have $j(2\alpha(\alpha | \alpha)) = v_\alpha^0$. Since $\mathbf{S}$ spans $\mathbf{F}_0$, the linear forms $v_\alpha^0 (\alpha \in \mathbf{S})$ span $\mathbf{F}_0^*$. It remains to be shown that the dimension of $\mathbf{F}_0$ over $\mathbb{R}$ cannot exceed $n$; if we had $n + 1$ elements $\alpha_k$ $(1 \leq k \leq n + 1)$ of $\mathbf{S}$ linearly independent over $\mathbb{R}$, there would exist $n + 1$ complex numbers $c_k$, not all zero, such that

$$\sum_{k=1}^{n+1} c_k \alpha_k = 0,$$

and therefore

$$\sum_{k=1}^{n+1} c_k v_\beta(\alpha_k) = 0$$

for all $\beta \in \mathbf{S}$. Now, the numbers $v_\beta(\alpha_k)$ are real, and therefore this system of linear equations in the unknowns $c_k$ has a nontrivial solution $(c_k^0)$ consisting of real numbers, because it has a nontrivial solution consisting of complex numbers. Since the $v_\alpha$ span $\mathbf{F}_0^*$, we should therefore have

$$\sum_{k=1}^{n+1} c_k^0 \alpha_k = 0,$$

contrary to hypothesis.
(21.11.3) With the notation of (21.11.2), the numbers

\[(21.11.3.1) \quad n(\beta, \alpha) = \frac{2(\beta \mid \alpha)}{\langle \alpha \mid \alpha \rangle} = v_\alpha(\beta) \quad (\alpha, \beta \in \mathbf{S})\]

are integers such that

\[(21.11.3.2) \quad 0 \leq n(\beta, \alpha)n(\alpha, \beta) \leq 4,\]

and we have \(n(\beta, \alpha)n(\alpha, \beta) = 4\) only when \(\beta = \pm \alpha\). If \(\alpha, \beta\) are distinct and \(n(\beta, \alpha) > 0\), then \(\alpha - \beta\) is a root.

With the notation of (21.11.1), we have seen in the proof of (21.11.2) that

\[v_\alpha(\beta) = \frac{2(\beta \mid \alpha)}{\langle \alpha \mid \alpha \rangle} = n(\beta, \alpha),\]

and therefore \(n(\beta, \alpha)\) is an integer, by virtue of \((S_3)\). The inequality (21.11.3.2) is a direct consequence of the Cauchy–Schwarz inequality, which also shows that the equality \((\beta \mid \alpha)^2 = (\alpha \mid \alpha)(\beta \mid \beta)\) holds only when \(\beta = t\alpha\) with \(t \in \mathbb{R}\), and by virtue of \((S_4)\) this implies that \(\beta = \pm \alpha\). If \(n(\beta, \alpha) > 0\), we cannot have \(\beta = -\alpha\) and therefore, if \(\alpha\) and \(\beta\) are distinct, the product \(n(\beta, \alpha)n(\alpha, \beta)\) can take only the values 1, 2, 3; consequently one of the numbers \(n(\beta, \alpha), n(\alpha, \beta)\) is equal to 1. Interchanging \(\alpha\) and \(\beta\) if necessary (which replaces \(\alpha - \beta\) by its negative \(\beta - \alpha\)), we may assume that \(n(\alpha, \beta) = 1\), and then \(\sigma_\beta(\alpha) = \alpha - \beta\) is a root, by virtue of \((S_2)\).

(21.11.3.3) Since we have

\[(21.11.3.4) \quad \sigma_\alpha(\beta) = \beta - n(\beta, \alpha)\alpha\]

for each pair of roots \(\alpha, \beta\), and since \(\mathbf{S}\) spans \(F\), it follows that the reflections \(\sigma_\alpha\) are uniquely determined by the integers \(n(\beta, \alpha)\). Hence the same is true of the linear forms \(v_\alpha\), which are therefore independent of the choice of invariant scalar product \((\lambda \mid \mu)\).

(21.11.4) We shall now change notation, and henceforth denote by \(E\) the real vector space \(F_0^*\), so that its dual \(E^*\) (the space of \(\mathbb{R}\)-linear forms on \(E\)) is canonically identified with the real vector space spanned by \(\mathbf{S}\).
Let $S$ be a reduced root system and $E^*$ the real vector space spanned by $S$. There exists a subset $B$ of $S$ that is a basis of $E^*$ over $R$ and is such that for each root $\beta \in S$, the coefficients $m_{\beta\alpha}$ in the expression

$$\beta = \sum_{\alpha \in B} m_{\beta\alpha} \alpha$$

are integers, all of the same sign.

Such a subset $B$ of $S$ is called a basis of the reduced root system $S$.

Since $E$ is not the union of any finite set of hyperplanes, there exists $x \in E$ such that $\alpha(x) \neq 0$ for all $\alpha \in S$. Let $S_+^*$ denote the set of roots $\alpha \in S$ such that $\alpha(x) > 0$, so that $S = S_+^* \cup (-S_+^*)$, and $S_+^* \cap (-S_+^*) = \emptyset$. A root $\alpha \in S_+^*$ will be called decomposable if there exist two roots $\beta, \gamma$ in $S_+^*$ such that $\alpha = \beta + \gamma$, and indecomposable otherwise. We shall prove (21.11.5) in the following more precise form:

For each $x \in E$ such that $\alpha(x) \neq 0$ for each root $\alpha \in S$, the set $B_x$ of indecomposable elements of $S_+^*$ is a basis of $S$. Conversely, if $B$ is a basis of $S$, then $B = B_x$ for each $x \in E$ such that $\alpha(x) > 0$ for all roots $\alpha \in B$.

We shall first show that each root belonging to $S_+^*$ is a linear combination of elements of $B_x$ with coefficients that are integers $\geq 0$. Suppose then that this is not the case, and let $I \subset S_+^*$ be the nonempty set of roots that do not have this property. Then there exists a root $\alpha \in I$ for which $\alpha(x) > 0$ takes the smallest possible value; since $B_x \cap I = \emptyset$ by definition, we have $\alpha \notin B_x$, hence there exist $\beta, \gamma \in S_+^*$ such that $\alpha = \beta + \gamma$. It follows that $\alpha(x) = \beta(x) + \gamma(x)$ and $\beta(x) > 0, \gamma(x) > 0$, so that

$$\beta(x) < \alpha(x) \quad \text{and} \quad \gamma(x) < \alpha(x),$$

and therefore $\beta \notin I$ and $\gamma \notin I$. But then $\alpha = \beta + \gamma \notin I$, by the definition of $I$, and we have arrived at a contradiction.

Next, we shall prove that

If $\alpha, \beta$ are distinct elements of $B_x$, then $(\alpha | \beta) \leq 0$.

For otherwise it would follow from (21.11.3) that $\gamma = \alpha - \beta$ was a root, and therefore either $\gamma \in S_+^*$ and $\alpha = \beta + \gamma$ would be decomposable, or else $-\gamma \in S_+^*$ and $\beta = \alpha + (-\gamma)$ would be decomposable.
Now suppose that a subset \( A \) of \( E^* \) and an element \( x \) of \( E \) are such that \( A(x) > 0 \) for all \( I \in A \), and \( (A I p) \neq 0 \) for any two distinct elements \( I, p \) of \( A \). Then the elements of \( A \) are linearly independent over \( \mathbb{R} \). For otherwise we should have two disjoint nonempty subsets \( A', A'' \) of \( A \) and a relation

\[
(21.1.1.5.4) \quad (v | v) = \sum_{(A I p) \in A' \times A''} a_{A I} b_{p I} (\lambda | I) \leq 0
\]

and therefore \( v = 0 \). Consequently \( 0 = v(x) = \sum_{\lambda \in A} a_{\lambda I} \lambda(x) \), and since \( a_{\lambda I} \geq 0 \) and \( \lambda(x) > 0 \) for all \( \lambda \in A' \), we must have \( a_{\lambda I} = 0 \) for all \( \lambda \in A' \); similarly \( b_{p I} = 0 \) for all \( p \in A'' \), and we have a contradiction.

We have therefore now proved by these considerations that \( B_x \) is a basis of \( S \). Conversely, if \( B \) is any basis of \( S \), then \( B \) is a basis of the vector space \( E^* \), hence there exists in the dual space \( E \) an element \( x \) such that \( x(x) > 0 \) for all \( x \in B \). Consider any one of the elements \( x \in E \) having this property. Let \( S^+ \) be the set of roots that are linear combinations of elements of \( B \) with coefficients that are all integers \( \geq 0 \); clearly \( S^+ \subset S^+_x \), \( -S^+ \subset -S^+_x \), and since by hypothesis \( S = S^+ \cup (-S^+) = S^+_x \cup (-S^+_x) \), it follows that \( S^+ = S_x^+ \). If for some root \( \alpha \in B \) we had \( \alpha = \beta + \gamma \) with \( \beta, \gamma \in S^+_x \), it would follow that \( \alpha = \sum_{\lambda \in B} (m_{\beta I} + m_{\gamma I}) \lambda, \) where the coefficients \( m_{\beta I} \) and \( m_{\gamma I} \) are integers \( \geq 0 \) and at least one of the \( m_{\beta I} \) (resp. \( m_{\gamma I} \)) is \( > 0 \); consequently \( \sum_{\lambda \in B} (m_{\beta I} + m_{\gamma I}) \geq 2 \), whereas this sum must be equal to 1, because \( B \) is a basis of \( E^* \). Hence \( B \subset B_x \), and since both \( B \) and \( B_x \) are bases of \( E^* \), we have \( B = B_x \).

If \( B = B_x \), the set \( S^+ = S_x^+ \) (resp. \( -S^+ \)) is called the set of positive (resp. negative) roots, relative to \( B \); it is the set of roots \( \beta \in S \) such that in (21.1.1.5.1) all the integers \( m_{\beta I} \) are \( \geq 0 \) (resp. \( \leq 0 \)).

(21.1.1.5.5) With the notation of (21.1.1), if \( S \) is a reduced root system in \( F \), the set \( S^* \) of linear forms \( \nu_x \) is a reduced root system in the dual space \( F^* \), and is called the dual of \( S \). For \( S^* \) does not contain 0, because \( \sigma_x \neq 1 \) for all \( x \in S \), and it spans \( F^* \), by (21.1.2). The transpose \( ' \sigma_x \) is the linear mapping \( u \mapsto u - u(x) \nu_x \) of \( F^* \) into itself, which is an involutory bijection. Furthermore, if \( \sigma_x(\beta) = \gamma \in S \), where \( x \) and \( \beta \) are roots, then we have \( \sigma_\gamma = \sigma_x \sigma_\beta \sigma_x^{-1} \).
writing this relation in the form $\sigma_x \sigma_\beta = \sigma_\gamma \sigma_x$, we obtain $v_\beta = v_\gamma - v_\beta(a)v_\alpha$, that is to say, $V(a) = v_\beta(a)v_\alpha$. Thus the set $S'$ satisfies $(S_2)$. The verification of $(S_2)$ is immediate, and $(S_4)$ follows from the fact that if $\alpha$ and $t\alpha$ are roots, where $t \in \mathbb{R}$, then $\sigma_\alpha = \sigma_{t\alpha}$, and conversely. It is clear that, if we identify $F^{**}$ with $F$, we have $(S')^* = S$.

If now $B$ is a basis of $S$, the set $B'$ of elements $v_\alpha$, where $\alpha \in B$, is a basis of $S'$. For, using the bijection $j$ defined in (21.11.2), we may identify $S'$ with the set $S'$ of elements $\alpha' = 2\alpha/(\alpha|\alpha)$ of $F$, where $\alpha \in S$, and $B$ with the set $B'$ of elements $\alpha' = \alpha \in B$. We have $B = B'_x$ for some $x \in F^*$, by (21.11.5.2), and since the relations $\alpha(x) > 0$ and $\alpha'(x) > 0$ are equivalent, it follows that $S'_x$ is the set of $\alpha'$ for which $\alpha \in S'_x$. Now if three roots $\alpha, \beta, \gamma \in S'_x$ are such that $\alpha' = \beta' + \gamma'$, then we have $\alpha = t_1 \beta + t_2 \gamma$ with $t_1 > 0$ and $t_2 > 0$, and therefore (since $\beta'$ and $\gamma'$ are not proportional to each other) there are at least two nonzero components of $\alpha$ with respect to the basis $B$, in other words $\alpha \notin B$. This shows also that $B'$ is contained in the set $B'_x$ of indecomposable elements of $S'_x$: these two sets have the same number of elements, hence $B' = B'_x$ and therefore $B'$ is a basis of $S'$ (21.11.5.2).

(21.11.6) Let $B$ be a basis of the reduced root system $S$. For each root $\alpha \in B$, the reflection $\sigma_\alpha$ (21.11.2.1) leaves invariant the set $S^+ - \{\alpha\}$ of positive roots (relative to $B$) other than $\alpha$, and transforms $\alpha$ into $-\alpha$.

Let $\beta$ be an element of $S^+$, other than $\alpha$; we have $\beta = \sum_{\lambda \in B} m_{\beta, \lambda} \lambda$, with coefficients $m_{\beta, \lambda}$ that are integers $\geq 0$. There exists $\gamma \neq \alpha \in B$ such that $m_{\beta, \gamma} > 0$, otherwise we should have $\beta = m_{\beta, \alpha} \alpha$ and therefore $\beta = \alpha$ by virtue of $(S_4)$. This being so, if $\beta' = \sigma_\alpha(\beta) = \beta - n(\beta, \alpha)\alpha$, the coefficients $m_{\beta, \lambda}$ in the decomposition $\beta' = \sum_{\lambda \in B} m_{\beta, \lambda} \lambda$ are all integers of the same sign, and by definition we have $m_{\beta, \gamma} = m_{\beta, \gamma} > 0$; hence $\beta' \in S^+$.

(21.11.7) Let $B$ be a basis of $S$, and let

\[ \delta = \frac{1}{2} \sum_{\lambda \in S^+} \lambda \]

be half the sum of the positive roots (relative to $B$). Then we have

\[ \sigma_\alpha(\delta) = \delta - \alpha \]

for all roots $\alpha \in B$. (In other words, $\nu_\alpha(\delta) = 1$ for all $\alpha \in B$.)
For if $\delta$ is half the sum of the roots $\mu \in S^+ - \{\alpha\}$, then it follows from (21.11.6) that $\sigma_\alpha(\delta) = \delta$, and therefore, since $\delta = \delta - \frac{1}{2}\alpha$, that $\sigma_\alpha(\delta) = \delta - \frac{1}{2}\alpha = \delta - \alpha$.

(21.11.8) Let $S$ be a reduced root system, $B$ a basis of $S$, and $W_S$ the finite group generated by the orthogonal reflections $\sigma_\alpha$ (21.11.2.1) for all $\alpha \in S$.

(i) For each $x \in E$, there exists $w \in W_S$ such that $\alpha(w \cdot x) \geq 0$ for all $\alpha \in B$.

(ii) For each basis $B'$ of $S$, there exists $w \in W_S$ such that $w(B') = B$.

(iii) For each root $\beta \in S$, there exists $w \in W_S$ such that $w(\beta) \in B$.

(iv) The group $W_S$ is generated by the reflections $\sigma_\alpha$ for $\alpha \in B$.

(Here $w \cdot x$ is by definition equal to $\langle w, x \rangle$.)

Let $W_B$ denote the subgroup of $W_S$ generated by the $\sigma_\alpha$, $\alpha \in B$. We shall prove (i) by showing, more precisely, that there exists an element $w \in W_B$ such that $\alpha(w \cdot x) \geq 0$ for all $\alpha \in B$. If $\delta$ denotes half the sum of the positive roots relative to $B$, choose $w \in W_B$ so that the number $\delta(w \cdot x)$ is as large as possible. For $\alpha \in B$ we have then $\delta(w \cdot x) \geq \delta((\sigma_\alpha w) \cdot x)$. But since $\sigma^{-1}_\alpha = \sigma_\alpha$, we have $\delta((\sigma_\alpha w) \cdot x) = (\sigma_\alpha(\delta))(w \cdot x) = \delta(w \cdot x) - \alpha(w \cdot x)$ by virtue of (21.11.7.2), whence $\alpha(w \cdot x) \geq 0$.

Likewise, we shall prove (ii) by showing, more precisely, that there exists an element $w \in W_B$ such that $w(B') = B$. Since $B'$ is a basis of $E^*$, there exists $x' \in E$ such that $\alpha'(x') > 0$ for all $\alpha' \in B'$; from the definition of a basis of $S$, it follows (21.11.5) that $\lambda(x') \neq 0$ for all $\lambda \in S$. By virtue of (i), there exists $w \in W_B$ such that $\alpha(w \cdot x') \geq 0$ for all $\alpha \in B$, that is to say, such that

$$
(w^{-1}(x') \geq 0;
$$

and since $\lambda(x') \neq 0$ for all $\lambda \in S$, we have $(w^{-1}(x') \geq 0$ or equivalently $\alpha(w \cdot x') > 0$ for all $\alpha \in B$, which as above implies that $\lambda(w \cdot x') \neq 0$ for all $\lambda \in S$. Hence, with the notation of (21.11.5), we have $B = B_{w \cdot x'}$ and $B' = B_{x'}$, by (21.11.5.2); by transport of structure, it follows that $B = w(B')$.

We shall now prove (iii), again by showing that there exists an element $w \in W_B$ such that $w(\beta) \in B$. Let $L$ be the hyperplane in $E$ given by the equation $\beta(x) = 0$. Since $L$ is not the union of any finite number of subspaces of codimension 2, it follows from (21.11.2) that there exists $x_0 \in L$ such that $\gamma(x_0) \neq 0$ for all roots $\gamma \neq \pm \beta$. Hence there exists a number $\varepsilon > 0$ and a point $x \in E$ sufficiently close to $x_0$ so that $\beta(x) = \varepsilon$ and $|\gamma(x)| > \varepsilon$ for all roots $\gamma$ other than $\pm \beta$. With the notation of (21.11.5), we have therefore $\beta \in B_{x}$, by the definition of $B_{x}$; hence, by virtue of (ii), there exists an element $w \in W_B$ such that $w(B_{x}) = B$, and therefore $w(\beta) \in B$. 
Finally, to establish (iv), it is enough to show that $\sigma_\beta \in W_\mathcal{B}$ for each root $\beta \in \mathcal{S}$. But by virtue of (iii) there exists $w \in W_\mathcal{B}$ such that $w(\beta) \in \mathcal{B}$, and since $\sigma_{w(\beta)} = w^{-1} \sigma_\beta w^{-1}$, we have $\sigma_\beta = w^{-1} \sigma_{w(\beta)} w \in W_\mathcal{B}$.

Q.E.D.

(21.11.9) When $\mathfrak{g}$, $\mathfrak{h}$ and $\mathcal{S}$ arise from a compact connected semisimple Lie group $K$ and a maximal torus $T$ of $K$, as in (21.10.1), the complex vector spaces $F$, $F^*$ defined in (21.11.2) are, respectively, $\mathfrak{h}^* = \mathfrak{t}^* \oplus i\mathfrak{t}^*$ and $\mathfrak{h} = \mathfrak{t} \oplus i\mathfrak{t}$, and the real vector spaces $E^* = F_0$ and $F_0^*$ are, respectively, $i\mathfrak{t}^*$ and $i\mathfrak{t}$.

If we choose a $K$-invariant scalar product $(x \mid y)$ on $\mathfrak{t}$ (20.11.3.1), we obtain from it canonically an $\mathbb{R}$-isomorphism $j$ of $\mathfrak{t}$ onto $\mathfrak{t}^*$, for which $j(x)$ (where $x \in \mathfrak{t}$) is the linear form $y \mapsto (x \mid y)$; and then by transport of structure a scalar product $(\lambda \mid \mu)$ on $E^*$, by defining $(\lambda \mid \mu) = (j^{-1}(i\lambda) \mid j^{-1}(i\mu))$. It is clear that this scalar product is invariant under the Weyl group $W$ of $K$ with respect to $T$, acting faithfully on $E^*$ (21.8.6). We have already remarked (21.10.6) that the reflections $\sigma_\alpha$ corresponding to the roots $\alpha \in \mathcal{S}$ (21.11.2.1) are precisely the elements $s_\alpha$ of the Weyl group defined in (21.8.7). In other words, with the notation of (21.11.8), we have $W_{\mathcal{S}} \subseteq W$. In fact:

(21.11.10) Under the conditions of (21.11.9), we have $W_{\mathcal{S}} = W$.

Let $x$ be an element of the normalizer $N(T)$ of $T$ in $K$, and let $w \in W = N(T)/T$ be the corresponding element of the Weyl group. Clearly, if $\mathcal{B}$ is a basis of $\mathcal{S}$, so also is $w(\mathcal{B})$, by transport of structure; since $W_\mathcal{S}$ acts transitively on the set of bases of $\mathcal{S}$ (21.11.8(ii)), it follows that by multiplying $w$ by a suitable element of $W_\mathcal{S}$ we may assume that $w(\mathcal{B}) = \mathcal{B}$. Let $u \in E = i\mathfrak{t}$ be an element such that $\alpha(u) > 0$ for each root $\alpha \in \mathcal{B}$ (21.11.5.2). Since $w$ permutes the roots in $\mathcal{B}$, it follows that $(w^{-1} \cdot \alpha)(u) > 0$ for all $\alpha \in \mathcal{B}$, in other words $\alpha(w \cdot u) > 0$. Let $m$ be the order of $w$ in $W$, and let $z = m^{-1} \sum_{k=0}^{m-1} w^k \cdot u \in E$; then we have $w \cdot z = z$, and $\alpha(z) > 0$ for all $\alpha \in \mathcal{B}$; this implies, as we have seen (21.11.5), that $\beta(z) \neq 0$ for all roots $\beta \in \mathcal{S}$. Hence $iz \in \mathfrak{t}$ is regular (21.8.4); and since $\text{Ad}(x) \cdot iz = iz$, it follows from (21.7.14) that $x \in T$ and therefore that $w$ is the identity. Q.E.D.

The proof just given also shows that the relation $w(\mathcal{B}) = \mathcal{B}$ implies that $w = 1$; in other words:

(21.11.10.1) The Weyl group of $K$ relative to $T$ acts simply transitively on the set of bases of the root system of $K$ relative to $T$. 
Remarks

(21.11.11) (i) Under the conditions of (21.11.9), the reflections $\sigma_\pm$ defined in (21.11.2.1) are the same as the reflections $\lambda \mapsto s_\pm \cdot \lambda$ (21.10.6) and therefore may be expressed in the form

$$\lambda \mapsto \lambda - \lambda(h_\pm)$$

where $h_\pm$ is as defined in (21.10.3.2). We have therefore

$$\lambda(h_\pm) = \frac{2(\alpha \lambda)}{\langle \alpha, \alpha \rangle}$$

for all $\lambda \in i\mathfrak{t}^*$, and consequently

$$n(\beta, \alpha) = \beta(h_\pm)$$

for all $\alpha, \beta \in \mathfrak{s}$.

The integers $n(\alpha, \beta)$, for the elements $\alpha, \beta$ of a basis of $\mathfrak{s}$, are called the Cartan integers of $\mathfrak{s}$ (or of the Lie algebra $\mathfrak{t}$ or $\mathfrak{g}$, or of the group $K$). They are independent of the basis chosen, because any basis can be transformed into any other basis by the action of the Weyl group.

The vectors $h_\pm \in i\mathfrak{t}$ form a reduced root system $\mathfrak{s}^\vee$, the dual of $\mathfrak{s}$ (21.11.5.5); the Weyl group of $\mathfrak{s}^\vee$ may be canonically identified with $W$.

(ii) Under the conditions of (21.11.9), if $\alpha$ and $\beta$ are roots such that $\beta \neq \pm \alpha$, and if $k$ is an integer such that $\beta + j\alpha$ is a root for $j = 0, 1, \ldots, k$, then we have $k \leq 3$. For by replacing $\beta$ by $\beta - p\alpha$ for some $p > 0$ if necessary, we may assume that $\beta - \alpha$ is not a root; it follows then from (21.10.4) that $k \leq -\beta(h_\pm)$, and the assertion is a consequence of (21.11.3).

(iii) Under the conditions of (21.11.9), if $\mathfrak{b}$ is a basis of $\mathfrak{s}$ and if $\alpha, \beta$ are two roots belonging to $\mathfrak{b}$, such that $\langle \alpha, \beta \rangle = 0$, then $\alpha + \beta$ is not a root. For we have $\beta(h_\pm) = 0$, which, in the notation of (21.10.4), implies that $p = q$; hence if $q \geq 1$ we should have also $p \geq 1$, and then $\beta - \alpha$ would be a root, contrary to the definition (21.11.5) of a basis of a root system.

(iv) Again under the conditions of (21.11.9), let $\mathfrak{t} = \bigoplus j \mathfrak{t}_j$ be the decomposition of $\mathfrak{t}$ as a direct sum of simple algebras (21.6.4). From (21.7.7.2), if $\mathfrak{t}_j$ is a maximal commutative subalgebra of $\mathfrak{t}_j$, then $\mathfrak{t} = \bigoplus j \mathfrak{t}_j$ is a maximal
commutative subalgebra of \( t \). It then follows directly from the definitions (21.8.1) and from the fact that \([t_j, t_h] = 0\) for \( j \neq h\), that if \( S_j \) is the root system of \( t_j \) relative to \( t_h \), then the union \( S \) of the \( S_j \) is the root system of \( t \) relative to \( t \). Note that if \( \alpha \in S_j \) and \( \beta \in S_h \), where \( j \neq h \), then \( n(\alpha, \beta) = 0 \). Finally, it is clear from the definition (21.11.5) that if \( B_j \) is a basis of the root system \( S_j \), then the union \( B \) of the \( B_j \) is a basis of \( S \).

**PROBLEMS**

1. (a) With the notation of (21.11.3), let \( \alpha \) and \( \beta \) be two roots in \( S \) such that \( \alpha \neq \pm \beta \), and let \( \theta \) be the angle (between 0 and \( \pi \)) between the two vectors \( \alpha, \beta \) (relative to the scalar product \((\alpha | \beta)\)). Show that if we write \( \| \lambda \| = (\lambda | \lambda)^{1/2} \), the following cases exhaust all the possibilities, for \( \| \beta \| \geq \| \alpha \| \):

   (i) \( n(\alpha, \beta) = 0, \quad n(\beta, \alpha) = 0, \quad \theta = \frac{1}{2} \pi \).

   (ii) \( n(\alpha, \beta) = 1, \quad n(\beta, \alpha) = 1, \quad \theta = \frac{3}{4} \pi, \quad \| \beta \| = \| \alpha \| \).

   (iii) \( n(\alpha, \beta) = -1, \quad n(\beta, \alpha) = -1, \quad \theta = \frac{5}{4} \pi, \quad \| \beta \| = \sqrt{2} \| \alpha \| \).

   (iv) \( n(\alpha, \beta) = 1, \quad n(\beta, \alpha) = 2, \quad \theta = \frac{3}{4} \pi, \quad \| \beta \| = \frac{\sqrt{2}}{2} \| \alpha \| \).

   (v) \( n(\alpha, \beta) = -1, \quad n(\beta, \alpha) = -2, \quad \theta = \frac{3}{4} \pi, \quad \| \beta \| = \frac{\sqrt{2}}{2} \| \alpha \| \).

   (vi) \( n(\alpha, \beta) = 1, \quad n(\beta, \alpha) = 3, \quad \theta = \frac{3}{4} \pi, \quad \| \beta \| = \sqrt{3/2} \| \alpha \| \).

   (vii) \( n(\alpha, \beta) = -1, \quad n(\beta, \alpha) = -3, \quad \theta = \frac{3}{4} \pi, \quad \| \beta \| = \sqrt{3/2} \| \alpha \| \).

(b) If \( p, q \) are the integers defined in (21.10.4) and if \( \alpha + \beta \) is a root, show that

\[
\frac{(\beta + \alpha | \beta + \alpha)}{(\beta | \beta)} = \frac{p + 1}{q}.
\]

(Consider the various possibilities.)

(c) Show that if \( \| \alpha \| = \| \beta \| \) and if \( S \) is irreducible (Problem 10), there exists \( w \in W_s \) such that \( w(\alpha) = \beta \). (Observe that by replacing \( \alpha \) by one of its transforms under \( W_s \), we may assume that \( (\alpha | \beta) \neq 0 \), and then \( n(\alpha, \beta) = n(\beta, \alpha) \), and we may also assume that \( n(\alpha, \beta) > 0 \). Consider the subgroup of \( W_s \) generated by \( \sigma_\alpha \) and \( \sigma_\beta \), and use (a) above.)

2. Show that the only reduced root systems in a two-dimensional vector space over \( \mathbb{R} \) are the following:

- For \( A_1 \times A_1 \):
  \[
  \begin{array}{c}
  \beta \\
  -\alpha \\
  0 \\
  \pi/2 \\
  \alpha \\
  -\beta \\
  \end{array}
  \]

- For \( A_2 \):
  \[
  \begin{array}{c}
  \beta + \alpha \\
  -\beta - \alpha \\
  0 \\
  \pi/3 \\
  \alpha \\
  -\beta \\
  \end{array}
  \]
3. Let \( \alpha_1, \alpha_2, \ldots, \alpha \) be linearly independent roots in a reduced root system \( S \).

(a) Suppose that a root \( \alpha \in S \) is of the form

\[
\alpha = c_1 \alpha_1 + c_2 \alpha_2 + \cdots + c_p \alpha_p - c_{p+1} \alpha_{p+1} - \cdots - c_r \alpha_r
\]

where the \( c_i \) are real numbers \( \geq 0 \). Show that there exists at least one integer \( j \in [1, r] \) such that \( \alpha - \alpha_j \) is a root if \( j \leq p \), and such that \( \alpha + \alpha_j \) is a root if \( j > p \). (Assume the contrary, and show that it leads to \( \alpha | \alpha \leq 0 \).)

(b) Suppose now that the \( c_i \) are integers \( \geq 0 \). Show that there exists a sequence of indices \( (j_k)_{1 \leq k \leq r} \) between 1 and \( r \), and a sequence \( (c_k)_{1 \leq k \leq r} \) of numbers equal to \( \pm 1 \), such that the linear combinations

\[
e_1 \alpha_{j_1} + e_2 \alpha_{j_2} + \cdots + e_p \alpha_{j_p} + \cdots + e_r \alpha_{j_r},
\]

are roots, the last one being equal to \( \alpha \).

(c) In particular, if \( B \) is a basis of \( S \) and \( \alpha \) is a positive root of \( S \) (relative to \( B \)), then there exists a sequence \( (\alpha_1, \alpha_2, \ldots, \alpha) \) of roots belonging to \( B \) such that \( \alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + \alpha_3, \ldots, \alpha_1 + \alpha_2 + \cdots + \alpha \) are roots, the last one being equal to \( \alpha \).

4. Let \( G \) be a compact connected Lie group and \( T \) a maximal torus of \( G \); let \( S(G) \) be the corresponding root system and \( S' \) a subset of \( S(G) \). Show that for there to exist a connected closed subgroup \( G' \) of \( G \) containing \( T \), such that \( S' \) is the root system \( S(G') \) of \( G' \) relative to \( T \), it is necessary and sufficient that the following conditions should be satisfied:

(i) There exists a subset \( B' \) of \( S' \), consisting of linearly independent roots, and such that every element of \( S' \) is a linear combination of elements of \( B' \) with rational integer coefficients.

(ii) Every linear combination of elements of \( S' \) with rational integer coefficients that belongs to \( S(G) \) belongs to \( S' \).

(To show that condition (ii) is necessary, use Problem 3(b) together with (21.10.5.2). To show that the conditions are sufficient, consider in the Lie algebra \( t \) of \( T \) the union \( \Delta \) of the hyperplanes given by the equations \( \alpha(u) = 2\pi n \), where \( \alpha \in S' \) and \( n \in \mathbb{Z} \), and the set \( P \) of special points of \( \Delta \) (Section 21.10, Problem 2). Show that the identity component \( G' \) of the centralizer of \( P \) in \( G \) (i.e., the subgroup of elements \( s \in G \) such that \( \text{Ad}(s) \cdot \alpha = \alpha \) for all \( \alpha \in P \) has the required properties, by showing that there exists no root \( \alpha \in S(G') \) that does not belong to \( S' \) and is such that \( (2\pi)^{-1} \alpha(x) \) is an integer for all \( x \in P \); consider in turn the cases where \( \alpha \) is linearly independent of \( B' \), and where it is linearly dependent on \( B' \).)
A connected closed subgroup \( G' \neq G \), with rank equal to that of \( G \), is necessarily the identity component of the centralizer in \( G \) of its center. If there exists no connected closed subgroup \( G'' \) of \( G \) such that \( G' \subset G'' \subset G \), with \( G'' \) distinct from \( G' \) and \( G \), then \( G' \) is also the identity component of the centralizer in \( G \) of any element of its center that does not belong to the center of \( G \).

Show that \( G' \) is also the identity component of the normalizer of its center in \( G \). (Note that the group of automorphisms of a compact commutative Lie group is discrete.) In order that \( G' \) should be the identity component of the centralizer of an element of its center, it is necessary and sufficient that there should exist a special point of \( D(G') \) that is not contained in \( D(G) \).

5. Let \( S, S' \) be reduced root systems in real vector spaces \( E^*, E'^* \), respectively, and let \( B, B' \) be bases of \( S, S' \), respectively. Suppose that there exists a bijection \( \varphi \) of \( B \) onto \( B' \) such that \( n(\varphi(\alpha), \varphi(\beta)) = n(\alpha, \beta) \) for all pairs \( \alpha, \beta \in B \). Show that there then exists a unique linear bijection \( f \) of \( E^* \) onto \( E'^* \) that extends \( \varphi \) and maps \( S \) onto \( S' \). (Consider the reflections \( \sigma_\alpha \) and \( \sigma_{\varphi(\alpha)} \).)

6. Show that if \( B \) is a basis of a reduced root system \( S \), then \( B \) is the only basis of \( S \) that consists of positive roots relative to \( B \).

7. Let \( G \) be a compact connected group, \( G_1 \) a connected closed subgroup of \( G \), and \( T \) a maximal torus of \( G \) such that \( T_1 = T \cap G_1 \) is a maximal torus of \( G_1 \); let \( g, g_1, t, t_1 \) be the Lie algebras of \( G, G_1, T, T_1 \), respectively. For each root \( \lambda \) of \( G_1 \) relative to \( T_1 \), let \( R(\lambda) \) denote the set of roots \( \alpha \in S(G) \) whose restriction to \( t_1 \) is equal to \( \lambda \) (Section 21.10, Problem 1).

(a) If \( \mu \) is a root of \( G_1 \) that is the transform of \( \lambda \) under an element of the Weyl group of \( G_1 \), show that \( R(\mu) \) is the transform of \( R(\lambda) \) under an element of the Weyl group of \( G \) (Section 21.7, Problem 8).

(b) For each root \( \lambda \in S(G_1) \), let \( K_\lambda \) be the corresponding almost simple subgroup of \( G_1 \) of rank 1 (21.8.5). Show that there exists a connected closed subgroup \( G_\lambda \) of \( G \) containing \( T \), whose root system \( S(G_\lambda) \) consists of the integral linear combinations of the roots belonging to \( R(\lambda) \) that are roots of \( G \) (Problem 4), and that \( K_\lambda \) is contained in \( G_\lambda \).

(c) The subgroup \( G_\lambda \) is said to be nice if it is contained in no connected closed subgroup \( G' \neq G \) of rank equal to the rank of \( G \). Show that the center of \( G_\lambda \) is then the intersection of \( G_1 \) with the center of \( G \). (Consider the identity component of the centralizer in \( G \) of an element of the center of \( G_\lambda \).) In particular, if \( G \) is semisimple, every nice subgroup of \( G \) is semisimple.

(d) If \( G_1 \) is a nice subgroup of \( G \), and if \( G_2 \) is a connected closed subgroup of \( G \) containing \( G_1 \) and distinct from \( G \) or \( G_1 \), show that the ranks of \( G_1 \) and \( G_2 \) are all distinct. (Show that if the ranks of \( G_1 \) and \( G_2 \) were equal, then \( G_1 \) and \( G_2 \) would have the same center; then use Problem 4 to obtain a contradiction.)

(e) Let \( B(G_1) \) be a basis of the root system \( S(G_1) \), and let \( L \) be the union of the sets \( R(\rho) \) for \( \rho \in B(G_1) \). Show that for each root \( \lambda \in S(G_1) \), the roots \( \alpha \in R(\lambda) \) are integral linear combinations of the roots belonging to \( L \). (Observe that there exists an element \( w \in W(G_1) \) such that \( w \cdot \lambda = \rho \) belongs to \( B(G_1) \), and that \( w \) is a product of reflections \( s_\gamma \) with \( \gamma \in B(G_1) \); on the other hand, \( s_\gamma \) is the restriction to \( t_1 \) of a product of reflections \( s_\gamma \in W(G_1) \subset W(G) \) (see (b) above), and for each root \( \beta \in S(G) \), the vector \( s_\gamma(\beta) = \beta \) is an integral linear combination of roots belonging to \( R(\gamma) \).) In particular, if \( G_1 \) is nice, every root in \( S(G) \) is an integral linear combination of roots belonging to \( L \). (Consider the
Let \( G \) be a compact connected semisimple Lie group, \( B = \mathcal{B}(G) \) a basis of the root system \( \mathcal{S}(G) \) of \( G \) relative to a maximal torus \( T \), with Lie algebra \( \mathfrak{g} \). A diagonal of \( G \) (relative to \( B \)) is by definition a line in \( \mathfrak{g} \) defined by a system of linear equations of the form

\[
\beta_1(x) = \beta_2(x) = \cdots = \beta_k(x) = 0, \quad \beta_{k+1}(x) = \cdots = \beta_l(x),
\]

where \( B = \{\beta_1, \beta_2, \ldots, \beta_l\} \). A diagonal is principal if \( k = 0 \) (or, equivalently, if it contains a regular element of \( T \)). A diagonal always contains a special point of \( D(G) \), other than the origin (Section 21.10, Problem 2).

Under the general hypotheses of Problem 7, let \( R_1 \) be a principal diagonal of \( G_1 \), containing points \( u \in \mathfrak{g} \) such that, for each of the roots \( \beta_j \) (\( 1 \leq j \leq l \)) of \( \mathcal{B}(G) \), we have \(-i \beta_j(u) \geq 0\). Let \( \mathcal{B}(G_1) = \{\rho_1, \ldots, \rho_n\} \) be a basis of \( \mathcal{S}(G_1) \) such that \( \rho_j(x) = \cdots = \rho_k(x) \) are the equations defining \( R_1 \). Show that if \( G \) is a nice subgroup of \( G_1 \), every root belonging to the union of the \( R(\rho_j) \) (\( 1 \leq j \leq h \)) is of the form \( \beta_{k+1} + m_1 \beta_1 + \cdots + m_r \beta_r \), where \( \beta_1, \ldots, \beta_r \) are the roots of the basis \( \mathcal{B}(G) \) that vanish on \( R_1 \), the index \( j \) satisfies \( 1 \leq j \leq l - k \), and the \( m_r \) (\( 1 \leq r \leq k \)) are integers \( \geq 0 \). (Observe that the point \( z \in R_1 \) at which all the roots \( \rho_j \) take the value \( 2 \pi i \) is a special point of \( D(G) \), and use Problem 7(c).)

Deduce that \( R_1 \) is a diagonal of \( G \).

If \( R_1 \) is a principal diagonal of \( G \), then \( k = 0 \) and the \( R(\rho_j) \) form a partition of \( \mathcal{B}(G) \). When this is so, the restriction to \( t_1 \) of a root \( \alpha \) of \( G \) is never identically zero, and there exists a root \( \rho \) of \( G_1 \) such that \( \alpha \) is a positive integral linear combination of the roots belonging to \( R(\rho) \). (Observe that the trace on \( t_1 \) of the hyperplane given by the equation \( \alpha(x) = 0 \) must be one of the hyperplanes \( \rho_j(x) = 0 \) (\( 1 \leq j \leq h \)), by expressing \( \alpha \) (resp. its restriction to \( t_1 \)) as a linear combination of the \( \beta_j \) (resp. the \( \rho_j \)).) Deduce that the restriction of \( \alpha \) to \( t_1 \) is a scalar multiple of a root belonging to \( \mathcal{S}(G_1) \). If \( G_1 \) is a nice subgroup of \( G \) and \( R_1 \) is a principal diagonal of \( G_1 \), then \( G_1 \) is said to be a principal nice subgroup of \( G \).

Let \( G_1 \) be a principal nice subgroup of \( G \). With the notation of Problem 8, let \( (\lambda | \mu) \) be the scalar product on \( \mathfrak{g}^\ast \) induced by that on \( \mathfrak{g} \).

(a) Show that if \( (\rho_1 | \rho_2) = 0 \), then \((\beta' | \beta'') = 0 \) for all \( \beta' \in R(\rho_1) \) and \( \beta'' \in R(\rho_2) \). (Observe that, by virtue of Problem 8, the restriction of \( \beta' + \beta'' \) to \( t_1 \) cannot belong to \( \mathcal{S}(G_1) \), and therefore \( \beta' + \beta'' \) is not a root of \( G \).)

Deduce that if \( G \) is almost simple then so also is \( G_1 \).

(b) Let \( \rho_1, \rho_2 \) be two roots belonging to \( \mathcal{B}(G_1) \) such that \( (\rho_1 | \rho_2) \neq 0 \) (and hence \( (\rho_1 | \rho_2) < 0 \)), so that \( \rho = \rho_1 + \rho_2 \) is a root of \( G_1 \). We may assume (Problem 2) that the reflection \( s_{\rho_1} \) interchanges \( \rho_1 \) and \( \rho_1; \ s_{\rho_2} \) is the restriction to \( t_1 \) of an element \( w \in \mathcal{W}(G_{\rho_1}) \) (Problem 7(b)), and \( w \) interchanges \( R(\rho) \) and \( R(\rho_1) \). If \( R(\rho_1) = \{\alpha_1, \ldots, \alpha_n\} \), show that for each \( j = 1, 2, \ldots, n \) there exists a root \( \gamma_j \in R(\rho_2) \) such that \( w \cdot \alpha_j = \alpha_j + \gamma_j \), and that if \( j \neq h \) the vector \( w \cdot \alpha_j - \alpha_j \) does not belong to \( R(\rho_2) \). (Consider the restrictions of \( \alpha_j \) and \( \alpha_j \) to \( t_1 \).) Deduce that \( (\alpha_j | \gamma_j) = 0 \) for all \( \gamma \neq \gamma_j \) in \( R(\rho_2) \).

(c) With the hypotheses and notation of (b), show that for each root \( \gamma \in R(\rho_2) \) there exists at least one root \( \alpha_j \in R(\rho_1) \) such that \( \gamma = \gamma_j \), so that the number of elements of \( R(\rho_2) \) is \( \leq n \). (Use (b) above.) Furthermore, if \( \gamma \) and \( \gamma' \) are distinct elements of \( R(\rho_2) \), then \((\gamma | \gamma') = 0 \). (Express that \( (w \cdot \alpha_j | w \cdot \alpha_j) = (\alpha_j | \alpha_j) \).

In particular, if \( \|\rho_1\| = \|\rho_2\| \), then \( R(\rho_1) \) and \( R(\rho_2) \) have the same number of elements, and we have \( (\alpha_j | \gamma_j) < 0 \), and \( (\alpha_j | \alpha_k) = (\gamma_j | \gamma_k) = (\alpha_j | \gamma_k) = 0 \) for \( j \neq h \).
11. BASES OF A ROOT SYSTEM

10. (a) Let $S$ be a reduced root system and $B$ a basis of $S$. Suppose that there exists a partition $(B_1, B_2)$ of $B$ such that $(\lambda | \mu) = 0$ for each $\lambda \in B_1$ and $\mu \in B_2$. Show that every positive root (relative to $B$) is a linear combination (with integral coefficients $\geq 0$) of roots that all belong either to $B_1$ or to $B_2$. (Use Problem 3(c) to argue by induction, proceeding as in (21.11.11(iii)).) Deduce that $S$ admits a partition $(S_1, S_2)$, where $S_1$ (resp. $S_2$) is a reduced root system with basis $B_1$ (resp. $B_2$).

(b) A reduced root system $S$ is said to be irreducible if the action of the Weyl group $W_S$ on the vector space spanned by $S$ is irreducible. If $G$ is a compact semisimple Lie group, show that the root system $S(G)$ is irreducible if and only if $G$ is almost simple. (Use (a) above.)

(c) Let $S$ be an irreducible reduced root system spanning a real vector space $E^*$, and let $(\lambda | \mu)$ be a scalar product on $E^*$ that is invariant under the Weyl group $W_S$. Show that every $W_S$-invariant bilinear form on $E^* \times E^*$ is a scalar multiple of $(\lambda | \mu)$. (Any bilinear form $\Phi$ on $E^* \times E^*$ can be written uniquely as $(\lambda, \mu) \mapsto (\Phi(\lambda) | \mu)$, where $\Phi$ is an endomorphism of $E^*$. If $\Phi$ is $W_S$-invariant, then $\Phi$ commutes with all elements of $W_S$, and in particular with the reflections $s_\alpha$. Deduce that $\Phi$ leaves fixed the lines $\mathbb{R} \alpha$, and hence that there exists a scalar $c \in \mathbb{R}$ such that the kernel of $\Phi - c$ is nonzero, hence is equal to $E^*$ by virtue of the hypothesis of irreducibility.)

11. Let $S$ be a reduced root system.

(a) Show that there exists, on the real vector space $E^*$ spanned by $S$, a unique scalar product—called the canonical scalar product—satisfying the relation

$$(\lambda | \mu) = \sum_{\alpha \in S} (\alpha | \lambda)(\alpha | \mu)$$

for all $\lambda, \mu \in E^*$. (Use Problem 10 to reduce to the case where $S$ is irreducible, and consider the bilinear form

$$(\lambda, \mu) \mapsto \sum_{\alpha \in S} (\alpha | \lambda)(\alpha | \mu)$$

where $(\lambda | \mu)$ is any $W_S$-invariant scalar product on $E^*$.)

(b) Show that for the canonical scalar product we have

$$\sum_{\alpha \in S} (\alpha | \alpha) = \dim(E^*).$$

(Observe that if $M$ is the matrix with entries $(\lambda | \mu)$ where $\lambda, \mu \in S$, then $M^2 = M$, and the rank of $M$ is equal to $\dim(E^*)$.)

(c) If $S$ is irreducible, show that there exists a constant $\gamma(S)$ such that

$$\sum_{\alpha \in S} (\alpha | \lambda)(\alpha | \mu) = \gamma(S)(\lambda | \mu).$$

(Consider the bilinear form $(\lambda, \mu) \mapsto \sum_{\alpha \in S} (\lambda(h_\alpha) | \mu(h_\alpha))$)

12. (a) Let $G$ be a compact connected semisimple Lie group $\neq \{e\}$, and let $T$ be a maximal torus of $G$. If $v$ is an automorphism of $G$ such that $v(T) = T$, and such that $v^{-1}$ fixes each of the roots of $G$ relative to $T$, show that the automorphism $u = v_* \otimes 1$ of $\mathfrak{g} \oplus \mathfrak{e}$ is such that, with the notation of (21.10.3),

$$u(x) = v_\alpha x_\alpha.$$
for all roots \( \alpha \in \mathcal{S}(G) \), where the \( v_\alpha \) are complex numbers of absolute value 1 and satisfy the relations

\[
(*) \quad v_\alpha v_{-\alpha} = 1, \quad v_\alpha v_{\beta} = v_{\alpha + \beta} \quad \text{if} \quad \alpha + \beta \in \mathcal{S}(G).
\]

Show that there exists an element \( u \in \mathfrak{t} \) such that \( e^{i\theta} = v_\alpha \) for each \( \alpha \in \mathcal{S}(G) \). (Observe that, in view of the relations \((*)\), it is enough that \( e^{i\theta} = v_\alpha \) for each root \( \alpha \) in a basis of \( \mathcal{S}(G) \).)

(b) Deduce from (a) that the Lie group \( \text{Aut}(G) / \text{Int}(G) \) is finite. (Use the conjugacy theorem.)

(c) Deduce from (b) that for any compact connected Lie group \( G \), the Lie group \( \text{Aut}(G) / \text{Int}(G) \) is discrete. (Use (19.13.3)).

(d) Show that if \( G \) is semisimple and if \( \tau \in \text{Aut}(G) \) is such that \( \tau(T) = T \), then there exists \( x \in G \) such that \( \text{Int}(x) \) fixes each point of some one-parameter subgroup of \( G \). (Argue as in (21.11.10)).

13. Let \( \mathcal{S} \) be a reduced root system.

(a) Let \( \mathcal{B} \) be a basis of \( \mathcal{S} \). Two roots \( \alpha, \beta \in \mathcal{B} \) are said to be linked if \( (\alpha | \beta) \neq 0 \), or equivalently if the Cartan integers \( n(\alpha, \beta) \) and \( n(\beta, \alpha) \) are \( \leq -1 \). Show that there exists no sequence \( (\alpha_1, \ldots, \alpha_r) \) of distinct elements of \( \mathcal{B} \) such that \( \alpha_i \) and \( \alpha_{i+1} \) are linked for \( 1 \leq i \leq r - 1 \), and such that \( \alpha_r \) and \( \alpha_1 \) are also linked. (If \( \lambda = \alpha_1 + \alpha_2 + \cdots + \alpha_r \), show that the hypothesis would imply that \( (\lambda | \lambda) \leq 0 \), by using (21.11.5.3)).

(b) Deduce from (a) that there exists a root \( \alpha \in \mathcal{B} \) that is linked to at most one other root in \( \mathcal{B} \). (Consider a sequence of maximum length \( (\alpha_1, \ldots, \alpha_r) \) of roots in \( \mathcal{B} \) such that \( \alpha_i \) is linked to \( \alpha_{i+1} \) for \( 1 \leq i \leq r - 1 \).)

(c) Suppose that \( \mathcal{B} \) has at least two elements. Show that there exists a partition of \( \mathcal{B} \) into two nonempty subsets \( \mathcal{B}', \mathcal{B}'' \) such that no two roots of \( \mathcal{B}' \) or of \( \mathcal{B}'' \) are linked. (Prove that this result is true not only for \( \mathcal{B} \) but more generally for any subset \( F \) of \( \mathcal{B} \) containing at least two elements, by induction on the number of elements \( m \) of \( F \) and by observing that \( F \) also has the property (b) above.)

(d) Let \( \alpha_1, \ldots, \alpha_r \) be distinct elements of \( \mathcal{B} \). Show that in the Weyl group \( \mathcal{W}_\mathcal{S} \) all the products \( \sigma_{\alpha_{r-1}} \sigma_{\alpha_{r-2}} \cdots \sigma_{\alpha_{1}} \), where \( \pi \) is any permutation of \( \{1, 2, \ldots, r\} \), are conjugate. (Observe that if \( \alpha_i \) and \( \alpha_j \) are not linked, then \( \sigma_{\alpha_i} \) and \( \sigma_{\alpha_j} \) commute. Then show more generally that if \( \alpha \mapsto u(\alpha) \) is a mapping into any group \( \Gamma \) such that \( u(\alpha) \) and \( u(\alpha_j) \) commute whenever \( \alpha \) and \( \alpha_j \) are not linked, all the products \( u(\alpha_{r-1}) \cdots u(\alpha_{1}) \) are conjugate in \( \Gamma \). Prove this result by induction on \( r \), by using (b) above and reducing to the case where \( \alpha_{r-1} \) is linked to at most one other \( \alpha_j \), and then to the case where this \( \alpha_j \) (if it exists) is \( \alpha_{r-2} \); in this case, observe that the inductive hypothesis may be applied to the elements \( \alpha_{r-1}, \ldots, \alpha_{r-2} \) and the mapping \( u' \) that coincides with \( u \) on \( \alpha_{r-1}, \ldots, \alpha_{r-2} \) and is such that \( u'(\alpha_{r-1}) = u(\alpha_{r-1})u(\alpha_{r-2}) \).

14. Let \( \mathcal{S} \) be a reduced root system spanning a vector space \( \mathbf{E}^* \), and let \( \mathcal{B} = \{\beta_1, \ldots, \beta_l\} \) be a basis of \( \mathcal{S} \). For every permutation \( \pi \) of \( \{1, 2, \ldots, l\} \), the product \( \sigma_{\beta_{\pi(l)}} \cdots \sigma_{\beta_{\pi(1)}} \) is called a Coxeter element of the Weyl group \( \mathcal{W}_\mathcal{S} \).

(a) The conjugacy class in \( \mathcal{W}_\mathcal{S} \) of a Coxeter element depends neither on the permutation \( \pi \) nor on the choice of basis \( \mathcal{B} \) (cf. Problem 13(d)).

(b) Suppose that \( \mathcal{B} \) is numbered in such a way that \( \beta_1, \ldots, \beta_r \) are pairwise orthogonal
and $\beta_{r_{-1}}, \ldots, \beta_i$ are pairwise orthogonal (Problem 13(c)). Put $\sigma' = \sigma_{\beta_1} \sigma_{\beta_2} \cdots \sigma_{\beta_i}$ and $\sigma'' = \sigma_{\beta_{r_{-1}}} \cdots \sigma_{\beta_{r_i}}$, so that $\sigma \equiv \sigma' \sigma''$ is a Coxeter element: $\sigma'$ is the orthogonal symmetry with respect to the subspace $V'$ of $E^*$ orthogonal to $\beta_1, \beta_2, \ldots, \beta_i$, and $\sigma''$ is the orthogonal symmetry with respect to the subspace $V''$ of $E^*$ orthogonal to $\beta_{r_{-1}}, \ldots, \beta_i$, so that $E^* = V' \oplus V''$. Deduce that no eigenvalue of $\sigma$ is equal to 1. (Observe that if $\sigma' (\lambda) = \sigma'' (\lambda)$, then $\lambda - \sigma '(\lambda) = \lambda - \sigma'' (\lambda)$ is orthogonal to both $V'$ and $V''$.)

(c) The order $h$ of $\sigma$ in $W_\mathbb{R}$ is called the Coxeter number of $\mathcal{S}$. The characteristic polynomial $P(T)$ of $\sigma$ may be written as

$$P(T) = \prod_{j=1}^l \left( T - \exp \frac{2\pi im_j}{h} \right),$$

where $m_1, \ldots, m_l$ are integers such that $0 \leq m_1 \leq m_2 \leq \cdots \leq m_l < h$. Show that $m_j + m_{j+1} - j = h$ for $1 \leq j \leq l$, and that $m_l > 0$. (Use the fact that the coefficients of $P(T)$ are real.)

15. Let $F$ be a real vector space of dimension $l$ and let $U', U''$ be two supplementary subspaces of respective dimensions $r$ and $l - r$. Suppose that $F$ is equipped with a scalar product $(.,.)$. Let $e_1, \ldots, e_l$ be an orthonormal basis of $U'$, and $e_{l+1}, \ldots, e_l$ an orthonormal basis of $U''$. Relative to the basis $(e_1, \ldots, e_l)$ of $F$, the matrix of the bilinear form $(.,.)$ is $A = ([e_j | e_k])_{1 \leq j, k \leq l}$; it is positive definite.

(a) Suppose that $e_j \neq e_k$ for each pair of indices $j, k$ such that $1 \leq j \leq r$ and $1 \leq k \leq l - r$. If $z' \in U'$ and $z'' \in U''$ are two nonzero vectors and if $\theta$ is the angle between them, show that the smallest value of $1 + \cos \theta$ is the smallest eigenvalue $\lambda_0$ of the matrix $A$ (15.11.7).

(b) Suppose in addition that there exists no partition of $\{1, 2, \ldots, l\}$ into two subsets $I, I'$ such that $(e_i | e_j) = 0$ for all $i \in I$ and $j \in I'$. Show that the eigenspace $N(\lambda_0)$ of the self-adjoint operator $u$ on $F$ defined by the matrix $A$ is one-dimensional, spanned by a vector all of whose components are positive. (If $(\xi_j)_{j=1}^l$ is a vector in $N(\lambda_0)$, i.e., a vector orthogonal to $R^l$ relative to the positive semidefinite quadratic form with matrix $A - \lambda_0 I = (a_{ij})$ on $R^l$, observe that the vector $(|\xi_j|)$ also belongs to $N(\lambda_0)$, by showing that $\sum_{i,j} a_{ij} |\xi_i| |\xi_j| \leq \sum_{i,j} a_{ij} \xi_i \xi_j$, and then that if $I$ is the set of indices $i$ such that $\xi_i \neq 0$, we have $a_{ii} |\xi_i| \leq 0$ for $i \in I$ and $j \notin I$, and $\sum_i |a_{ij}| |\xi_i| = 0$ for $j \notin I$. Conclude that either $I = \emptyset$ or $I = \{1, 2, \ldots, l\}$.)

Under the hypotheses of (b), deduce that there exists a unique vector

$$z' = \xi_1 e_1 + \cdots + \xi_l e_l$$

in $U'$ and a unique vector $z'' = \xi_{r+1} e_{r+1} + \cdots + \xi_l e_l$ in $U''$ such that $\|z'\| = \|z''\| = 1$, the $\xi_j$ are all positive, and the angle $\theta$ between $z'$ and $z''$ satisfies $1 + \cos \theta = \lambda_0$. Show that the line $R z'$ (resp. $R z''$) is the orthogonal projection of $R z'$ (resp. $R z''$) on $U'$ (resp. $U''$). (Use the minimal property of $\cos \theta$.)

(d) Let $V'$ (resp. $V''$) be the orthogonal supplement of $U'$ (resp. $U''$) in $F$. If $(f_j)_{1 \leq j \leq s}$ is the basis of $F$ such that $(e_j | f_j) = \delta_{j,k}$ (Kronecker delta), then $f_1, \ldots, f_s$ form a basis of $V'$ and $f_{r+1}, \ldots, f_l$ a basis of $V''$; also $e_j$ is the orthogonal projection of $f_j$ on $U'$ (if $1 \leq j \leq r$), and $e_{r+j}$ the orthogonal projection of $f_{r+j}$ on $U''$ (if $1 \leq j \leq l - r$). Let $x'$ (resp. $x''$) be the vector in $V'$ (resp. $V''$) whose projection on $U'$ (resp. $U''$) is $z$ (resp. $z''$). The plane $P = R x' + R x''$ is also equal to $R x' + R x''$. If $s'$ (resp. $s''$) is the reflection in $V'$ (resp. $V''$), then $P$ is stable under $s'$ and $s''$, and $s' | P, s'' | P$ are the reflections in the lines $R x', R x''$, respectively. If $C$ is the set of the vectors $y \in F$ such that $(e_j | y) > 0$ for $1 \leq j \leq l$, then we have $x' \in C, x'' \in C$, and $P \cap C$ is the set of linear combinations $ax' + bx''$ with $a > 0$ and $b > 0$. 

11. BASES OF A ROOT SYSTEM
16. With the hypotheses and notation of Problem 14, suppose in addition that $S$ is irreducible (Problem 10). Let $C$ be the set of $I \in E^*$ such that $(\beta_j|I) > 0$ for $1 \leq j \leq l$ (21.14.4). For each element $w \in W_s$, either $w(C) = C$ or $w(C) \cap C = \emptyset$ (21.11.10.1).

(a) By using (21.11.5.3) and Problem 15, show that there exist $y', y'' \in V$ such that $u'$ and $u''$ leave invariant the plane $P = R_{y'} + R_{y''}$, and that $\sigma'|P$, $\sigma''|P$ are the reflections in the lines $R_{y'}$, $R_{y''}$, respectively; also $P \cap C$ is the set of linear combinations of $\gamma'$ and $\gamma''$ with positive coefficients. Show that the restrictions to $P$ of the transformations belonging to the subgroup $W'$ of $W$, generated by $\sigma'$ and $\sigma''$ form a group of order $2h$; deduce that $u|P$ is a rotation through $2\pi/h$, and that $m_i = 1$.

(b) Show that the only roots in $S$ that are orthogonal to $\gamma'$ (resp. $\gamma''$) are $\beta_1, \ldots, \beta_r$ (resp. $\beta_{r+1}, \ldots, \beta_s$). (Observe that if $\alpha$ is orthogonal to $\gamma'$, then $\alpha$ is a linear combination of $\beta_1, \ldots, \beta_r$, by using (21.11.5); observe also that $\sigma_\alpha(\beta)$ is a linear combination of $\beta_1, \ldots, \beta_r$, for $1 \leq j \leq r$.) Deduce that the intersection of $P$ with a hyperplane orthogonal to a root of $S$ is necessarily the transform of $R_{y'}$ or $R_{y''}$ by an element of $W'$, and that the number of roots in $S$ is $hl$.

(c) Let $\xi$ be an eigenvector of $\sigma \otimes 1$ in $P \otimes \delta C$ corresponding to the eigenvalue $\exp(2\pi i/h)$. Show that $\langle \xi|\alpha \rangle \neq 0$ for each $\alpha \in S$. (Use (b) above and observe that $\xi$ cannot be of the form $c\eta$ with $\eta \in P$ and $\delta \in C$.)

(d) A root $\theta \in S$ is said to be pivotal (with respect to $u$) if $\theta > 0$ and $\sigma(\theta) < 0$. Show that the pivotal roots are $\theta_k = \sigma_{\beta_k}\sigma_{\beta_{k-1}} \cdots \sigma_{\beta_1}(\beta_0)$ (1 \leq k \leq l) (use 21.11.6) and deduce that the $\theta_k$ form a basis of $E^*$ (use 21.11.2.1). If $m_k (1 \leq k \leq l)$ are the elements of $C$ such that $(m_k|\beta_k) = \delta_{m_k}$, then $(1 - \sigma^{-1}) \cdot m_k = \theta_k$. Deduce that two distinct pivotal roots $\theta_j$, $\theta_k$ cannot be in the same orbit in $S$ under the action of the cyclic subgroup of $W_s$ generated by $\sigma$ (use 21.14.7.1)). Show that every orbit in $S$ under this subgroup contains a pivotal root (consider the sum of the elements of the orbit), and deduce that there are exactly $l$ orbits, each with $h$ elements.

(e) Show that, for each root $\alpha \in S$, we have

$$\sum_{\beta \in S} \frac{(\alpha|\beta)^2}{(\beta|\beta)} = h \cdot (\alpha|\alpha).$$

(Use Problem 10.)

(f) Show that for each positive integer $m$ less than $h$ and prime to $h$, the complex number $\exp(2\pi im/h)$ is an eigenvalue of $\sigma$. (Observe that the matrix of $\sigma$ relative to the basis $\{\beta_1, \beta_2, \ldots, \beta_l\}$ has integer entries, and use that fact that cyclotomic polynomials are irreducible over $\mathbb{Q}$.)

17. Let $G$ be a compact Lie group, not necessarily connected, and let $G_0$ be its identity component. Suppose that there exists an element $a \in G$ whose centralizer is discrete.

(a) Show that the connected component of $a$ in $G$ consists of conjugates of $a$. (Show that the mapping $x \mapsto xax^{-1}$ of $G_0$ into $G$ is a local diffeomorphism.)

(b) Deduce from (a) that $G_0$ is commutative. (If not, there would exist $z \in G_0$ such that $\text{Int}(za)$ leaves invariant a maximal torus of $G_0$ and the corresponding root system; now use Problem 12(d).)

18. (a) Let $G$ be a compact connected semisimple Lie group $\neq \{e\}$. Show that for each automorphism $\nu$ of $G$, the subgroup of fixed points of $\nu$ is not discrete. (Apply Problem 17 to the compact Lie group $\text{Aut}(G)$, using Problem 12 and the fact that the center of $G$ is discrete.)
12. EXAMPLES: THE CLASSICAL COMPACT GROUPS

(b) Let $G$ be a noncommutative compact connected Lie group, and let $\nu$ be an automorphism of $G$. Show that the identity component $U$ of the subgroup of fixed points of $\nu$ is such that every maximal torus of $U$ is contained in a unique maximal torus of $G$, and therefore contains regular elements of $G$. (Let $V$ be a maximal torus of $U$, and let $Z$ be the identity component of the centralizer of $V$ in $G$. Show that $U \cap Z$ is discrete, and use (a) to deduce that $Z = \{e\}$.) Hence show that there exists a maximal torus $T$ of $G$ that is globally invariant under $\nu$, and a basis of the root system of $G$ relative to $T$ that is globally invariant under $\nu$. (Consider a regular element of $G$ that belongs to $U$ and is arbitrarily close to $e$.)

19. Let $G$ be a compact connected semisimple Lie group $\neq \{e\}$, let $\nu$ be an automorphism of $G$, let $F$ be the closed subgroup of fixed points of $\nu$, and let $F_0$ be the identity component of $F$ (so that $F_0 \neq \{e\}$, by virtue of Problem 18(a)). Then every connected component of $F$ contains regular elements of $G$ (21.7.13). The proof is as follows:

(a) Let $x \in F$ be a singular element of $G$. Then the identity component $Z(x)$ of the centralizer of $x$ is not commutative (21.8.4). Show that a maximal torus $S$ of the identity component of $F \cap Z(x)$ has dimension $\leq 1$. Let $U$ be the identity component of the intersection $Z(S) \cap Z(x)$ of the centralizers of $S$ and $x$, which is globally invariant under $\nu$, and has rank equal to the rank of $G$ (21.7.9).

(b) Show that $U$ is a maximal torus, by proving that its derived group $Z(U) = \{e\}$. For otherwise $Z(U) \cap F$ would contain a torus $S'$ of dimension $\geq 1$, and $SS'$ would be a torus in $Z(x) \cap F$ containing $S$ properly.

(c) Show that it is not possible that all the elements of $xS = Sx$ should be singular in $G$ (cf. (21.8.4.1)).

12. EXAMPLES: THE CLASSICAL COMPACT GROUPS

(21.12.1) The groups $U(n) (= U(n, C))$ and $SU(n) (n \geq 2)$.

We shall show that the group $T$ of diagonal matrices $\operatorname{diag}(\zeta_1, \ldots, \zeta_n)$, where each $\zeta_j \in U$, the unit circle in $C$ (so that $T$ is isomorphic to $U^n$) is a maximal torus in $U(n)$. The Lie algebra $u(n)$ of $U(n)$ is the Lie subalgebra of $\operatorname{gl}(n, C) = M_n(C)$ consisting of the antihermitian matrices, i.e., the matrices $X$ such that $\bar{X} = -X$ (19.4.3.3); it has an $R$-basis consisting of the $n$ matrices $iE_{rr} (1 \leq r \leq n)$ and the $n^2 - n$ matrices $E_{rs} - E_{sr}$ and $i(E_{rs} + E_{sr})$

$$
(1 \leq r < s \leq n),
$$

so that the complexification of $u(n)$ is $\operatorname{gl}(n, C)$. The $n$ matrices $iE_{rr}$ $(1 \leq r \leq n)$ form a basis of the Lie algebra $t$ of $T$. Since $[iE_{rr}, E_{rs}] = iE_{rs}$, $[iE_{rr}, E_{sr}] = -iE_{sr}$, and $[iE_{rr}, E_{pq}] = 0$ when $p \neq r$ and $q \neq r$ (19.4.2.2), we may write, for any $h \in t$,

$$(21.12.1.1) \quad [h, E_{rs}] = (\varepsilon_r(h) - \varepsilon_s(h))E_{rs}$$
for \(1 \leq r, s \leq n\) and \(r \neq s\), where \(\delta_r^s = i\delta_{rs}\) (Kronecker delta). This shows immediately that \(t\) is a maximal commutative subalgebra of \(u(n)\), and the center \(c\) of \(u(n)\) is the subalgebra \(\mathbb{R}iI\) consisting of the pure imaginary multiples of the unit matrix; \(u(n)\) is the direct sum of \(c\) and the Lie algebra \(su(n)\) of the group \(SU(n)\), consisting of the matrices in \(u(n)\) with zero trace, and \(t\) is the direct sum of \(c\) and the maximal commutative subalgebra \(t'\) of \(su(n)\) generated by the matrices \(i(E_{rr} - E_{ss})\). It follows from (21.12.1.1) that the roots of \(u(n)\) relative to \(t\) are the \(\mathbb{R}\)-linear mappings of \(t\) into \(i\mathbb{R}\)

\[
(21.12.1.2) \quad \alpha_{rs} = \varepsilon_r - \varepsilon_s \quad (1 \leq r, s \leq n, r \neq s).
\]

The roots of \(su(n)\) relative to \(t'\) are obtained by identifying the \(\alpha_{rs}\) with their restrictions to \(t'\) (21.8.8). If we write \(g = sl(n, \mathbb{C})\), the complexification of \(su(n)\), and \(h = t_{\mathbb{C}}\), then with the notation of (21.8.1) we have \(g_{rs} = CE_{rs}\), and the element \(h_{rs} \in h\) is \(E_{rr} - E_{ss}\). It is immediately verified from the definition (21.11.5) that the set of roots

\[
(21.12.1.3) \quad \beta_r = \alpha_{r, r+1} = \varepsilon_r - \varepsilon_{r+1} \quad (1 \leq r \leq n - 1)
\]

is a basis of the root system, for which the positive roots are

\[
(21.12.1.4) \quad \varepsilon_r - \varepsilon_s = \beta_r + \beta_{r+1} + \cdots + \beta_{s-1} \quad (1 \leq r < s \leq n).
\]

It follows also from these facts and from (21.11.11.3) that the Cartan integers are given by

\[
(21.12.1.5) \quad n(\beta_r, \beta_s) = 0 \quad \text{if} \quad |r - s| \geq 2,
\]

\[
\quad n(\beta_r, \beta_s) = n(\beta_r, \beta_{r+1}) = -1 \quad (1 \leq r \leq n - 2).
\]

It follows that the group \(SU(n)\) is almost simple (21.6.6). Indeed, from (21.12.1.5) it is clear that the interval \([1, n - 1]\) of \(\mathbb{N}\) cannot be partitioned into two nonempty subsets \(A, B\) such that \(n(\beta_r, \beta_s) = 0\) whenever \(r \in A\) and \(s \in B\); for if \(r \in A\), then we must also have \(r + 1 \in A\) if \(r \leq n - 2\), and \(r - 1 \in A\) if \(r \geq 2\). The assertion therefore follows from (21.11.11).

Finally, it follows from (21.12.1.5) that the reflection \(\sigma_{\beta_r}\) (21.11.11), where \(1 \leq r \leq n - 1\), interchanges \(\varepsilon_r\) and \(\varepsilon_{r+1}\) and fixes the other \(\varepsilon_s\); hence the Weyl group may be identified with the symmetric group \(S_n\) of all permutations of \([1, n]\).

\[
(21.12.2) \quad \text{The group } U(n, H) \quad (n \geq 2).
\]
We shall identify the division ring of quaternions

\[ H = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k \]

with \( \mathbb{C} \oplus \mathbb{C}j \), so that \( jz = \bar{z}j \) for \( z \in \mathbb{C} \), and the conjugate of the quaternion \( x + yj \) (\( x, y \in \mathbb{C} \)) is \( \bar{x} - yj \). The group \( U(n, \mathbb{C}) \) is then identified with the subgroup of \( U(n, H) \) consisting of the unitary matrices with entries in the subfield \( \mathbb{C} \) of \( H \). We shall show that the maximal torus \( T \) of \( U(n, \mathbb{C}) \) defined in (21.12.1) is also a maximal torus of \( U(n, H) \). The Lie algebra \( u(n, H) \) of \( U(n, H) \) consists of the antihermitian matrices \( X \in M_n(H) \), i.e., the matrices \( X \) satisfying \( \bar{X} = -X \) (19.4.3.2). Observe now that any matrix \( X \in M_n(H) \) can be written uniquely in the form \( U + Vj \), where

\[ U, V \in M_n(\mathbb{C}); \]

the relation \( \bar{X} = -X \) is equivalent to the two relations

\[ \bar{U} = -U, \quad \bar{V} = V. \tag{21.12.2.1} \]

Next, it is easily verified that the mapping \( \varphi: M_n(H) \to M_{2n}(\mathbb{C}) \) defined by

\[ \varphi(U + Vj) = \begin{pmatrix} U & V \\ -\bar{V} & \bar{U} \end{pmatrix} \tag{21.12.2.2} \]

is an injective homomorphism of \( \mathbb{R} \)-algebras. Since \( \mathfrak{gl}(n, H) \) (resp. \( \mathfrak{gl}(2n, \mathbb{C}) \)) is just \( M_n(H) \) (resp. \( M_{2n}(\mathbb{C}) \)) with Lie algebra multiplication \( [X, Y] = XY - YX \), it follows that \( \varphi \) is also an injective homomorphism of the real Lie algebra \( \mathfrak{gl}(n, H) \) into the real Lie algebra \( \mathfrak{gl}(2n, \mathbb{C}) \).

We shall from now on identify \( u(n, H) \) with its image under \( \varphi \). Then the Lie algebra \( \mathfrak{t} \) of \( T \) has an \( \mathbb{R} \)-basis consisting of the matrices \( i(E_{rr} - E_{n+r,n+r}) \) for \( 1 \leq r \leq n \), and the Lie algebra \( u(n, H) \) has an \( \mathbb{R} \)-basis consisting of this basis of \( \mathfrak{t} \) and the matrices

\[
\begin{align*}
E_{rs} - E_{sr} - E_{n+s,n+r} + E_{n+r,n+s} & \quad (1 \leq r < s \leq n), \\
i(E_{rs} + E_{sr} - E_{n+s,n+r} - E_{n+r,n+s}) & \quad (1 \leq r < s \leq n), \\
E_{n+r,s} + E_{n+s,r} - E_{r,n+s} - E_{s,n+r} & \quad (1 \leq r \leq s \leq n), \\
i(E_{n+r,s} + E_{n+s,r} + E_{r,n+s} + E_{s,n+r}) & \quad (1 \leq r \leq s \leq n).
\end{align*}
\]

It follows as in (21.12.1) that the complexification of \( u(n, H) \) may be identified with the Lie subalgebra of \( \mathfrak{gl}(2n, \mathbb{C}) \) consisting of the matrices

\[ Y = \begin{pmatrix} U & W \\ V & -\bar{U} \end{pmatrix} \tag{21.12.2.3} \]
such that \( Y = V \) and \( Y = W \), the matrix \( U \in M_n(C) \) being arbitrary. It is immediately verified that these matrices \( Y \) are those which satisfy the relation \( Y \cdot J + J \cdot Y = 0 \), where

\[
J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}
\]

and consequently the complexification of \( u(n, H) \) may be identified, by virtue of (19.4.3.3), with the Lie algebra \( \mathfrak{sp}(2n, C) \) of the complex symplectic group \( \text{Sp}(2n, C) \), consisting of the matrices \( Z \in M_{2n}(C) \) that satisfy the relation

\[
'Z \cdot J \cdot Z = J.
\]

A basis of \( \mathfrak{sp}(2n, C) \) over \( C \) is therefore formed by the \( n \) matrices \( E_r - E_{n+r,n+r} \) \((1 \leq r \leq n)\), which form a basis of the complexification \( \mathfrak{h} = t(C) \) of \( t \), and the \( 2n^2 \) matrices

\[
E_{r+s} + E_{n+r,s}, \quad E_{r,n+s} + E_{s,n+r} \quad (1 \leq r \leq s \leq n),
\]

\[
E_{rs} - E_{n+s,n+r} \quad (1 \leq r, s \leq n, r \neq s).
\]

Let \( \varepsilon_r \) \((1 \leq r \leq n)\) be the \( C \)-linear forms on \( \mathfrak{h} \) defined by the equations

\[
\varepsilon_r(E_s - E_{n+s,n+s}) = \delta_{rs} \quad (1 \leq s \leq n).
\]

Then we have

\[
[h, E_{n+r,s} + E_{n+s,r}] = - (\varepsilon_r(h) + \varepsilon_s(h))(E_{n+r,s} + E_{n+s,r}) \quad (1 \leq r \leq s \leq n)
\]

\[
[h, E_{r,n+s} + E_{s,n+r}] = (\varepsilon_r(h) + \varepsilon_s(h))(E_{r,n+s} + E_{s,n+r})
\]

\[
[h, E_{rs} - E_{n+s,n+r}] = (\varepsilon_r(h) - \varepsilon_s(h))(E_{rs} - E_{n+s,n+r}) \quad (1 \leq r, s \leq n, r \neq s)
\]

for all \( h \in \mathfrak{h} \). This shows on the one hand that \( \mathfrak{h} \) is a maximal commutative subalgebra of \( \mathfrak{sp}(2n, C) \) (and hence that \( t \) is a maximal commutative subalgebra of \( u(n, H) \)), and on the other hand that the roots of \( \mathfrak{sp}(2n, C) \) relative to \( \mathfrak{h} \) (or of \( u(n, H) \) relative to \( t \)) are the \( 2n^2 \) linear forms

\[
\pm 2\varepsilon_r \quad (1 \leq r \leq n), \quad \pm \varepsilon_r \pm \varepsilon_s \quad (1 \leq r < s \leq n).
\]

If we put

\[
\beta_r = \varepsilon_r - \varepsilon_{r+1} \quad (1 \leq r \leq n - 1), \quad \beta_n = 2\varepsilon_n
\]
then we have the formulas

\[
\begin{align*}
\varepsilon_r - \varepsilon_s &= \beta_r + \beta_{r+1} + \cdots + \beta_{s-1} \quad (r < s), \\
\varepsilon_r + \varepsilon_s &= \beta_r + \cdots + \beta_{s-1} + 2\beta_s + 2\beta_{s+1} + \cdots + 2\beta_{n-1} + \beta_n \quad (r < s \leq n - 1), \\
\varepsilon_r + \varepsilon_s &= \beta_r + \cdots + \beta_{n-1} + \beta_n \quad (r \leq n - 1), \\
2\varepsilon_r &= 2\beta_r + 2\beta_{r+1} + \cdots + 2\beta_{n-1} + \beta_n \quad (r \leq n - 1),
\end{align*}
\]

which show that the \(n\) roots \((21.12.2.8)\) form a basis of the root system; the positive roots corresponding to this basis are

\[(21.12.2.9) \quad 2\varepsilon_r \quad (1 \leq r \leq n), \quad \varepsilon_r \pm \varepsilon_s \quad (1 \leq r < s \leq n).\]

Also we have

\[
\begin{align*}
h_{\beta_r} &= E_{rr} - E_{n+r,n+r} - E_{r+1,r+1} + E_{n+r+1,n+r+1} \quad (1 \leq r \leq n - 1), \\
h_{\beta_n} &= E_{nn} - E_{2n,2n}
\end{align*}
\]

and therefore the Cartan integers are

\[(21.12.2.10) \quad n(\beta_r, \beta_s) = 0 \quad \text{if} \quad |r - s| \geq 2 \quad (1 \leq r \leq n - 1),
\]

\[n(\beta_r, \beta_{r+1}) = n(\beta_{r+1}, \beta_r) = -1 \quad (1 \leq r \leq n - 2),
\]

\[n(\beta_{n-1}, \beta_n) = -1, \quad n(\beta_n, \beta_{n-1}) = -2,
\]

\[n(\beta_n, \beta_r) = 0 \quad (1 \leq r \leq n - 2).
\]

The same proof as in \((21.12.1)\) shows that \(U(n, H)\) is almost simple. Moreover, it is easily checked with the help of \((21.12.2.10)\) that the reflection \(\sigma_{\beta_r}\) \((21.11.11)\) interchanges \(\varepsilon_r\) and \(\varepsilon_{r+1}\), and fixes the other \(\varepsilon_s\), for

\[1 \leq r \leq n - 1,
\]

together with \(\sigma_{\beta_n}\) transforms \(\varepsilon_n\) into \(-\varepsilon_n\) and fixes the other \(\varepsilon_s\). It follows that the Weyl group is the semidirect product \((19.14)\) of the commutative group \(\{-1, 1\}^n\) and the symmetric group \(S_n\), for the action \((\pi, u)\rightarrow \pi \cdot u\) of \(S_n\) on \(\{-1, 1\}^n\) defined by \(\pi \cdot u = \pi \cdot (u_1, \ldots, u_n) = (u_{\pi^{-1}(1)}, \ldots, u_{\pi^{-1}(n)})\). Its order is therefore \(2^n \cdot n!\).

When \(n = 1\), the formulas above show that \(sp(2, C)\) is isomorphic to \(sl(2, C)\), hence \(U(1, H)\) is isomorphic to \(SU(2)\). This can also be proved directly (Section 21.8, Problem 1).

\[(21.12.3) \quad \text{The group } SO(2n) \quad (n \geq 2).\]
The mapping that takes each endomorphism $u$ of $\mathbb{C}^n$ to the same $u$, considered as an endomorphism of $\mathbb{R}^{2n}$ (16.21.13.1), is an injective homomorphism of the $\mathbb{R}$-algebra $M_n(\mathbb{C})$ into the $\mathbb{R}$-algebra $M_{2n}(\mathbb{R})$, under which the image of a matrix $(z_{jk}) \in M_n(\mathbb{C})$, with $z_{jk} = x_{jk} + iy_{jk}$, is the matrix $(Z_{jk}) \in M_{2n}(\mathbb{R})$, where

$$Z_{jk} = \begin{pmatrix} x_{jk} & -y_{jk} \\ y_{jk} & x_{jk} \end{pmatrix}.$$ 

The image of the group $U(n)$ under this homomorphism is a subgroup of $SO(2n)$, which we shall identify with $U(n)$. We shall show that the maximal torus $T$ of $U(n)$ defined in (21.12.1) is a maximal torus of $SO(2n)$. The Lie algebra $\mathfrak{so}(2n)$ of $SO(2n)$ consists of all real skew-symmetric matrices $X$ (19.4.3.2), and its complexification is therefore the Lie algebra of all complex $2n \times 2n$ skew-symmetric matrices. By virtue of (19.4.3.3), this is the Lie algebra $\mathfrak{so}(2n, \mathbb{C})$ of the complex special orthogonal group $SO(2n, \mathbb{C})$, consisting of the complex matrices $Z \in M_{2n}(\mathbb{C})$ of determinant 1, such that $'Z \cdot Z = I_{2n}$. A basis over $\mathbb{C}$ of $\mathfrak{so}(2n, \mathbb{C})$ is formed by the $n$ matrices

$$H_r = i(E_{2r-1, 2r} - E_{2r, 2r-1}) \quad (1 \leq r \leq n),$$

which form a basis of the complexification $\mathfrak{h} = t(\mathbb{C})$ of the Lie algebra $t$ of $T$, and by the following $2n(n-1)$ matrices:

$$\tilde{M}_{rs} - M_{sr}, \quad \tilde{N}_{rs} - N_{sr}$$

where $1 \leq r, s \leq n$, $r \neq s$, and

$$M_{rs} = E_{2r-1, 2s-1} + E_{2r, 2s} + i(E_{2r, 2s-1} - E_{2s, 2r-1}) = '\tilde{M}_{sr},$$

$$N_{rs} = E_{2r-1, 2s-1} - E_{2r, 2s} - i(E_{2r, 2s-1} + E_{2s, 2r-1}) = 'N_{sr}. \quad (21.12.3.1)$$

Let $\varepsilon_r$ $(1 \leq r \leq n)$ be the $\mathbb{C}$-linear forms on $\mathfrak{h}$ defined by the equations $\varepsilon_r(H_s) = \delta_{rs}$ $(1 \leq s \leq n)$. Then we have

$$[h, \tilde{M}_{rs} - M_{sr}] = (\varepsilon_r(h) - \varepsilon_s(h))(\tilde{M}_{rs} - M_{sr}),$$

$$[h, \tilde{N}_{rs} - N_{sr}] = (\varepsilon_r(h) + \varepsilon_s(h))(\tilde{N}_{rs} - N_{sr}), \quad (21.12.3.2)$$

for $1 \leq r, s \leq n$, $r \neq s$, and all $h \in \mathfrak{h}$. To verify these formulas it is enough to observe that $[H_r, \tilde{M}_{rs}] = \tilde{M}_{rs}$, $[H_r, \tilde{N}_{rs}] = N_{rs}$, and to use the relations (21.12.3.1) together with $\tilde{H}_r = -H_r = 'H_r$. This shows firstly that $\mathfrak{h}$ is a maximal commutative subalgebra of $\mathfrak{so}(2n, \mathbb{C})$ (and hence that $t$ is a maximal commutative subalgebra of $\mathfrak{so}(2n, \mathbb{R})$), and secondly that the roots of $\mathfrak{so}(2n, \mathbb{C})$ relative to $\mathfrak{h}$ (or of $\mathfrak{so}(2n, \mathbb{R})$ relative to $t$) are the $2n(n-1)$ linear forms

$$\pm \varepsilon_r \pm \varepsilon_s \quad (1 \leq r < s \leq n). \quad (21.12.3.3)$$
If we put

\[(21.12.3.4) \quad \beta_r = \varepsilon_r - \varepsilon_{r+1} \quad (1 \leq r \leq n - 1), \quad \beta_n = \varepsilon_{n-1} + \varepsilon_n,\]

then we have the formulas (for \(n \geq 4\))

\[\varepsilon_r - \varepsilon_s = \beta_r + \beta_{r+1} + \cdots + \beta_{s-1} \quad (r < s),\]

\[\varepsilon_r + \varepsilon_s = \beta_r + \beta_{r+1} + 2\beta_s + 2\beta_{s+1} + \cdots + 2\beta_{n-2} + \beta_{n-1} + \beta_n \quad (r < s \leq n - 2),\]

\[\varepsilon_r + \varepsilon_{n-1} = \beta_r + \beta_{r+1} + \cdots + \beta_n \quad (r \leq n - 2),\]

\[\varepsilon_r + \varepsilon_n = \beta_r + \beta_{r+1} + \cdots + \beta_{n-2} + \beta_n \quad (r \leq n - 2).\]

which show that the \(n\) roots \((21.12.3.4)\) form a basis of the root system; the positive roots corresponding to this basis are

\[(21.12.3.5) \quad \varepsilon_r \pm \varepsilon_s \quad (1 \leq r < s \leq n).\]

Also we have

\[h_{\beta_r} = H_r - H_{r+1} \quad (1 \leq r \leq n - 1),\]

\[h_{\beta_n} = H_{n-1} + H_n,\]

from which we obtain the values of the Cartan integers for the basis \((21.12.3.4)\):

\[n(\beta_r, \beta_s) = n(\beta_s, \beta_r) \quad \text{for all} \quad r, s,\]

\[n(\beta_r, \beta_s) = 0 \quad (1 \leq r \leq n - 3, s \geq r + 2),\]

\[(21.12.3.6) \quad n(\beta_r, \beta_{r+1}) = -1 \quad (1 \leq r \leq n - 2),\]

\[n(\beta_{n-2}, \beta_n) = -1,\]

\[n(\beta_{n-1}, \beta_n) = 0.\]

From these formulas, a proof analogous to that of \((21.12.1)\) shows that \(\text{SO}(2n)\) is almost simple if \(n \geq 4\). Furthermore, the reflection \(\sigma_{\beta_r}\), interchanges \(\varepsilon_r\) and \(\varepsilon_{r+1}\) and fixes the remaining \(\varepsilon_s\), for \(1 \leq r \leq n - 1\), while \(\sigma_{\beta_n}\) transforms \(\varepsilon_{n-1}\) into \(-\varepsilon_{n-1}\), \(\varepsilon_n\) into \(-\varepsilon_n\), and fixes the other \(\varepsilon_s\). From this it follows that if \(E\) is the subgroup of the multiplicative group \(
\{ -1, 1 \}^n
\) consisting of the elements \((u_1, \ldots, u_n)\) such that \(u_1 u_2 \cdots u_n = 1\) (a subgroup that is isomorphic to \(
\{ -1, 1 \}^{n-1}\)), the Weyl group is isomorphic to the semidirect product of \(E\) with the symmetric group \(\mathfrak{S}_n\), the action being the same as in \((21.12.2)\). The order of the Weyl group is therefore \(2^{n-1} \cdot n!\).
For \( n = 3 \), it may be shown that \( \mathfrak{so}(6) \) is isomorphic to \( \mathfrak{su}(4) \); for \( n = 2 \), that \( \mathfrak{so}(4) \) is isomorphic to the direct sum \( \mathfrak{su}(2) \oplus \mathfrak{su}(2) \) (Problems 1 and 2).

**The group \( \mathbf{SO}(2n + 1) \) \((n \geq 2)\).**

The mapping \( \mathbf{M}_{2n}(\mathbb{R}) \to \mathbf{M}_{2n+1}(\mathbb{R}) \) defined by

\[
U \mapsto \begin{pmatrix} U & 0 \\ 0 & 1 \end{pmatrix}
\]

is injective and maps \( \mathbf{SO}(2n) \) onto a subgroup of \( \mathbf{SO}(2n + 1) \); we shall identify \( \mathbf{SO}(2n) \) with this subgroup. Then the maximal torus \( T \) of \( \mathbf{SO}(2n) \) defined in (21.12.3) is also a maximal torus of \( \mathbf{SO}(2n + 1) \). For the complexification of the Lie algebra \( \mathfrak{so}(2n + 1) \) of \( \mathbf{SO}(2n + 1) \) is again the Lie algebra \( \mathfrak{so}(2n + 1, \mathbb{C}) \) of complex skew-symmetric matrices (and is the Lie algebra of the complex special orthogonal group \( \mathbf{SO}(2n + 1, \mathbb{C}) \), defined as in (21.12.3)). With the notation of (21.12.3), a basis of \( \mathfrak{so}(2n + 1, \mathbb{C}) \) may be obtained from the basis of \( \mathfrak{so}(2n, \mathbb{C}) \) defined in (21.12.3) by adjoining the \( 2n \) matrices

\[
P_r^\pm = E_{2r-1,2n+1} - E_{2n+1,2r} \pm i(E_{2r,2n+1} - E_{2n+1,2r})
\]

for which we have

\[
[h, P_r^\pm] = \mp \varepsilon_r(h)P_r^\pm
\]

for all \( h \in \mathfrak{h} \). This proves our assertion and shows that the roots of the \( \mathfrak{so}(2n + 1, \mathbb{C}) \)

relative to \( \mathfrak{h} \) (or of \( \mathfrak{so}(2n + 1) \) relative to \( t \)) are the \( 2n^2 \) linear forms

\[
\pm \varepsilon_r \quad (1 \leq r \leq n), \quad \pm \varepsilon_r \pm \varepsilon_s \quad (1 \leq r < s \leq n).
\]

If we put

\[
\beta_r = \varepsilon_r - \varepsilon_{r+1} \quad (1 \leq r \leq n - 1), \quad \beta_n = \varepsilon_n,
\]

then we have

\[
\varepsilon_r = \beta_r + \beta_{r+1} + \cdots + \beta_n \quad (1 \leq r \leq n),
\]

\[
\varepsilon_r - \varepsilon_s = \beta_r + \beta_{r+1} + \cdots + \beta_{s-1} \quad (1 \leq r < s \leq n),
\]

\[
\varepsilon_r + \varepsilon_s = \beta_r + \cdots + \beta_{s-1} + 2\beta_s + 2\beta_{s+1} + \cdots + 2\beta_n \quad (1 \leq r < s \leq n),
\]
12. EXAMPLES: THE CLASSICAL COMPACT GROUPS 103

showing that the \( n \) roots (21.12.4.3) form a basis of the root system, the positive roots for this basis being

\[
(21.12.4.4) \quad \varepsilon_r \quad (1 \leq r \leq n), \quad \varepsilon_r \pm \varepsilon_s \quad (1 \leq r < s \leq n).
\]

Furthermore, we have

\[
\begin{align*}
\mathbf{h}_{\beta_r} &= H_r - H_{r+1} \quad (1 \leq r \leq n - 1), \\
\mathbf{h}_{\beta_n} &= 2H_n,
\end{align*}
\]

and therefore the Cartan integers are

\[
(21.12.4.5) \quad n(\beta_r, \beta_s) = 0 \quad \text{if} \quad |r - s| \geq 2 \quad (1 \leq r \leq n - 1),
\]

\[
\begin{align*}
n(\beta_r, \beta_{r+1}) &= n(\beta_{r+1}, \beta_r) = -1 \quad (1 \leq r \leq n - 2), \\
n(\beta_{n-1}, \beta_n) &= -2, \quad n(\beta_n, \beta_{n-1}) = -1, \\
n(\beta_n, \beta_r) &= 0 \quad (1 \leq r \leq n - 2).
\end{align*}
\]

One shows as in (21.12.2) that \( \text{SO}(2n + 1) \) is almost simple and that the Weyl group is isomorphic to the semidirect product of \( \{-1, 1\}^n \) and \( \varpi_n \).

For \( n = 1 \), the formulas above and in (21.12.1) show that \( \text{so}(3) \) is isomorphic to \( \text{su}(2) \); also, using (21.12.2), that \( \text{so}(5) \) is isomorphic to \( \text{u}(2, \mathbb{H}) \) (Problem 1).

(21.12.5) In the four cases studied above, the scalar product on \( \mathfrak{t}^* \) defined by \( (\varepsilon_j | \varepsilon_k) = \delta_{jk} \) (Kronecker delta) is invariant under the action of the Weyl group.

(21.12.6) The complex Lie algebras \( \text{sl}(n, \mathbb{C}), \text{so}(2n + 1, \mathbb{C}), \text{sp}(2n, \mathbb{C}) \), and \( \text{so}(2n, \mathbb{C}) \) are denoted, respectively, by \( A_{n-1}, B_n, C_n, D_n \) \((n \geq 2)\). We have seen that, with the exception of \( \text{so}(4, \mathbb{C}) \), they are simple. It can be shown that, apart from these Lie algebras, there are (up to isomorphism) only five other complex simple Lie algebras, of dimensions 14, 52, 78, 133, and 248 [85]. They are known as the exceptional complex simple Lie algebras.

An almost simple compact Lie group that is locally isomorphic to one of the groups of the four types studied in this section is often called a classical almost simple compact group.

PROBLEMS

1. (a) Identify the exterior square \( \bigwedge^2 (\mathbb{C}^4) \) with the vector space \( \mathbb{C}^6 \), by identifying the basis

\[
\begin{align*}
e_1 \wedge e_2, & \quad e_2 \wedge e_3, \quad e_3 \wedge e_4, \quad e_4 \wedge e_1, \quad e_1 \wedge e_4, \quad e_2 \wedge e_4
\end{align*}
\]
of $\bigwedge^2 (C^4)$ (where $(e_1, e_2, e_3, e_4)$ is the canonical basis of $C^4$) with the canonical basis $e'_1, e'_2, e'_3, e'_4, e'_5, e'_6$ of $C^6$. If two bivectors $x, y \in \bigwedge^2 (C^4)$ are identified in this way with the vectors $\sum_{j=1}^6 \xi^j e'_j, \sum_{j=1}^6 \eta^j e'_j$, then the 4-vector $x \wedge y$ is equal to $B(x, y)e'_1 \wedge e'_2 \wedge e'_3 \wedge e'_4$, where

$$B(x, y) = \xi^1 \eta^4 + \eta^1 \xi^4 + \xi^2 \eta^5 + \eta^2 \xi^5 + \xi^3 \eta^6 + \eta^3 \xi^6.$$ 

Consider the mapping that transforms each $u \in SL(4, C)$ into $A'u$. Show that $u \mapsto A'u$ is a surjective homomorphism of the Lie group $SL(4, C)$ onto a group isomorphic to the orthogonal group $SO(6, C)$, with kernel $(I, -I)$, so that $SL(4, C)$ is a two-sheeted covering of $SO(6, C)$. (To show that the homomorphism is surjective, consider the dimensions of the two groups.)

(b) Show that the restriction of $u \mapsto A'u$ to $SU(4)$ is a surjective homomorphism onto a group isomorphic to $SO(6) \subset SO(5, C)$. By restricting to $U(2, H) \subset Sp(4, C)$, we obtain a homomorphism $U(2, H) \rightarrow SO(5)$, which makes $U(2, H)$ a double covering of $SO(5)$. For each pair of matrices $(U_1, U_2)$ in $SL(2, C)$, let $\varphi(U_1, U_2)$ denote the automorphism $X \mapsto U_1 \cdot X \cdot U_2$ of the vector space $M_2(C)$, identified with $C^4$ by identifying the matrix $(-: i:)$ with the vector $(t_2, t_1, \xi^3, \xi^4)$. Show that $\varphi$ is a surjective homomorphism of $SL(2, C) \times SL(2, C)$ onto a group isomorphic to $SO(4, C)$, with kernel consisting of $(I, I)$ and $(-I, -I)$, so that $SL(2, C) \times SL(2, C)$ is a double covering of $SO(4, C)$. Show also that the restriction of $\varphi$ to $SU(2) \times SU(2)$ is a surjective homomorphism of this group onto a group isomorphic to $SO(4)$. (Same method as in Problem 1.)

3. Show that apart from the isomorphisms

$$B_2 \cong C_2, \quad D_2 \cong A_1 \oplus A_1, \quad D_3 \cong A_3,$$

which follow from Problems 1 and 2 (or which may be obtained directly from the explicit descriptions of these Lie algebras), there exist no other isomorphisms among the algebras $A_{n-1}, B_n, C_n, D_n$ for $n \geq 2$. (Consider the systems of Cartan integers of these Lie algebras.)

4. Let $G$ be an almost simple compact connected Lie group. Show that if $G_1$ is a principal nice subgroup of $G$ (Section 21.11, Problem 9), the Lie algebra of $G_1$ cannot be isomorphic to $su(n+1)$ or $so(2n)$ for $n \geq 2$. (Observe that for these Lie algebras, all the roots have the same length.)

5. Let $G$ be a classical compact group. Suppose that $G$ has a principal nice subgroup $G_1$ (Section 21.11, Problem 9) that is also a classical group, of rank $\geq 3$. The complexified Lie
algebra of $G_1$ is necessarily of type $B_n$ or $C_n$ (Problem 4), hence there exists a basis 
\{\rho_1, \ldots, \rho_h\} of $\mathfrak{S}(G_1)$ such that $h \geq 3, \|\rho_1\| = \|\rho_2\| = \cdots = \|\rho_{h-1}\|, (\rho_j|\rho_j) < 0, and 
(\rho_j|\rho_k) = 0 \text{ if } |k-j| > 1. Then the sets $R(\rho_1), \ldots, R(\rho_{h-1})$ all have the same number $n$ of 
elements (Section 21.11, Problem 9).

(a) Show that $n \leq 2$ (use Section 21.11, Problem 9(a) and (c)).

(b) Show that if $n = 2$, the inclusion $G_1 \subset G$ is one of the two canonical inclusions 
$SO(2h + 1) \subset SU(2h + 1), U(h, H) \subset SU(2h)$. (Use Section 21.11, Problem 9(b).)

(c) Show that if $n = 1$ the inclusion $G_1 \subset G$ is the canonical inclusion 
$SO(2h + 1) \subset SO(2h + 2)$.

(Same method.)

6. In the Lie algebra $\mathfrak{so}(7)$, the three roots

$$\gamma_1 = \varepsilon_1, \quad \gamma_2 = \varepsilon_2 - \varepsilon_1, \quad \gamma_3 = -\varepsilon_2 - \varepsilon_3,$$

form a basis of the root system. Let $t_1$ be the plane in $t$ on which the linear form $\gamma_1 - \gamma_3 = 
\varepsilon_1 + \varepsilon_2 + \varepsilon_3$ vanishes. Show that the restrictions to $t_1$ of the roots of $\mathfrak{so}(7)$ form a reduced 
root system of type $G_2$ (Section 21.11, Problem 2). Show that there exists a principal nice 
subgroup of $SO(7)$ whose root system relative to $t_1$ consists of these restrictions.

13. LINEAR REPRESENTATIONS OF COMPACT CONNECTED LIE GROUPS

We recall that, until the end of this chapter, by a linear representation of a 
compact Lie group is meant a continuous (or, equivalently, $C^\infty$ (19.10.12)) 
linear representation on a finite-dimensional complex vector space.

(21.13.1) Every compact Lie group $G$ has a faithful linear representation.

In other words, bearing in mind (20.11.3.1), there exists an integer $N > 0$ 
such that $G$ is isomorphic to a Lie subgroup of $U(N)$.

Consider the set of irreducible representations $s \mapsto M_\rho(s)$ of $G$ ($\rho \in R$) 
(21.2.5). It is enough to show that there exists a finite subset $J$ of $R$ such that 
the kernels $N_\rho$ of the homomorphisms $s \mapsto M_\rho(s)$ for $\rho \in J$ intersect only in $e,$ 
for the Hilbert sum of the representations $s \mapsto M_\rho(s)$ for $\rho \in J$ will then be 
faithful. Now there exists an open neighborhood $V$ of $e$ in $G$ that contains no 
subgroup of $G$ other than $\{e\}. To see that this is so, let $W$ be an open 
neighborhood of $0$ in the Lie algebra $\mathfrak{g}_e$ of $G$, such that $\exp_G$ is a diffeomorphism of $W$ onto an open neighborhood of $e$ in $G$ (19.8.6). We may assume 
that, relative to some norm that defines the topology of $\mathfrak{g}_e$, the open neigh-
borhood $W$ is defined by $\|x\| < a.$ Then the neighborhood $V = \exp(\frac{1}{2}W)$ of $e$ 
in $G$ has the required property: for if $x \neq 0$ belongs to $\frac{1}{2}W$, there exists 
a smallest integer $p > 0$ such that $(p + 1)\|x\| > \frac{1}{2}a$, and necessarily
(p + 1)x ∈ W; if now there were a subgroup H ≠ \{e\} of G contained in V and such that s = \exp(x) ∈ H, then we should have
\[ s^{p+1} = \exp((p + 1)x) ∈ H, \]
contradicting the fact that (p + 1)x ∈ W and (p + 1)x ∉ \frac{1}{2}W.

Now the intersection of the kernels N_\rho, for all \rho ∈ R, consists only of e (21.3.5), and hence the intersection of the closed sets N_\rho ∩ (G - V) (\rho ∈ R) is empty. Since G is compact, it follows from the Borel–Lebesgue axiom that there exists a finite subset J of R such that the intersection of the sets N_\rho ∩ (G - V) for \rho ∈ J is empty. The set \bigcap_{\rho ∈ J} N_\rho is then a subgroup of G contained in V, hence consists only of e by the construction of V, and the proof is complete.

(21.13.1.1) We remark that this proof shows in fact that every compact metrizable group G, in which there exists a neighborhood of e containing no subgroup other than \{e\}, is isomorphic to a subgroup of a unitary group \overline{U}(\mathbb{N}), hence is a Lie group (cf. Section 19.8, Problem 9).

(21.13.2) Let G be a compact Lie group and U a faithful linear representation. Then every irreducible linear representation of G is contained (21.4.2) in a tensor product of a certain number of linear representations equal to U and a certain number of linear representations equal to its conjugate (21.4.3).

Put \( \text{cl}(U) = \sum_{\rho ∈ J} d_\rho \cdot \rho \) (21.4.7), where \( d_\rho > 0 \) for all \( \rho \) belonging to a finite subset J of R. Then \( \text{cl}(\overline{U}) = \sum_{\rho ∈ J} d_\rho \cdot \rho \).

Suppose that there exists \( \rho' \in R \) such that the proposition is false for the representation \( M_{\rho'} \). This means that the subring of \( Z^{(R)} \) generated by the classes \( \rho \in J \) and their conjugates \( \bar{\rho} \) is contained in a \( \mathbb{Z} \)-module of the form \( Z^{(R')} \), where \( R' < R \) and \( \rho' \notin R' \). It follows from the Peter–Weyl theorem (21.2.3) that \( \chi_{\rho'} \) is orthogonal to all the functions \( m_j^{(n)}(s) \), \( s ∈ R' \). Consequently, if we put \( U(s) ^{⊗m} \otimes \overline{U}(s) ^{⊗n} = (p^{(m,n)}_{kk}(s)) \) for each pair of integers \( m \geq 0, n \geq 0, \) such that \( m + n \geq 1 \), the function \( \chi_{\rho'} \) is orthogonal to all the functions \( p^{(m,n)}_{kk} \). Moreover, since the trivial representation is contained in \( U \otimes \overline{U} \) (21.4.6.4), the class \( \rho' \) cannot be the class of the trivial representation, and therefore \( \chi_{\rho'} \) is orthogonal also to the constant functions (21.3.2.6). But by the definition of the tensor product of matrices, among the functions \( p^{(m,n)}_{kk} \) there appear all the monomials with respect to continuous functions that are elements of the matrix \( U \) or of \( \overline{U} \). By hypothesis, these functions separate the points of G, hence the complex vector subspace of \( \mathcal{C}_c(G) \) spanned by the constants and the \( p^{(m,n)}_{kk} \) is dense, by the Stone–Weierstrass theorem (7.3.1). Since the con-
tinuous function $\chi_{p'}$ is not identically zero, we arrive at a contradiction (13.14.4), which proves (21.13.2).

(21.13.3) Let $G$ be a compact Lie group and $H$ a closed subgroup of $G$. Then every irreducible linear representation of $H$ is contained in the restriction to $H$ of a linear representation of $G$.

Let $U$ be a faithful linear representation of $G$ (21.13.1). Clearly its restriction $V$ to $H$ is faithful, hence every irreducible linear representation of $H$ is contained in some representation of the form $V^{\otimes m} \otimes \bar{V}^{\otimes n}$ (21.13.2); since this representation is obviously the restriction to $H$ of $U^{\otimes m} \otimes \bar{U}^{\otimes n}$, the proposition is proved.

(21.13.4) Let $G$ be a compact connected Lie group and $T$ a maximal torus in $G$. (This notation will be in force up to the end of Section 21.15.)

As we have already remarked (21.7.6), the study of the linear representations of $G$ is based on the study of their restrictions to $T$. In the first place, a linear representation of $G$ is uniquely determined, up to equivalence, by its restriction to $T$. Clearly it is enough to consider irreducible representations, and since up to equivalence such a representation is entirely determined by its character (21.4.5), it is enough to show that if two characters $\chi'$, $\chi''$ have the same restriction to $T$, then they are equal. We shall in fact prove a more precise result: for this purpose, we remark that if $f$ is a continuous central function on $G$ (21.2.2), its restriction to $T$ is a continuous function which, by definition (21.2.2.1), is invariant under the Weyl group $W$ of $G$ relative to $T$.

(21.13.5) The mapping that sends each continuous central function on $G$ to its restriction to $T$ is an isomorphism of the complex vector space of continuous central functions on $G$, onto the complex vector space $\mathcal{C}_c(T)^W$ of continuous complex functions on $T$ that are invariant under the Weyl group $W$.

The fact that the mapping $f \mapsto f|_T$ is injective is immediately obvious. For each $x \in G$ is of the form $sts^{-1}$ for some $s \in G$ and $t \in T$ (21.7.8), hence $f(x) = f(t)$ because $f$ is central. To show that $f \mapsto f|_T$ is surjective, suppose we are given a function $g \in \mathcal{C}_c(T)^W$; let us first show that we may define a function $f$ on $G$ by the condition $f(sts^{-1}) = g(t)$ for all $t \in T$ and $s \in G$. For this purpose, we must verify that if $t_1$, $t_2$ are two elements of $T$ that are conjugate in $G$, then $g(t_1) = g(t_2)$; but by virtue of (21.7.17), there exists $w \in W$ such that $t_2 = w \cdot t_1$, and the result follows from the $W$-invariance of $g$. It remains to be shown that the function $f$, so defined, is continuous (it is a central function by definition).

If $f$ were not continuous, there would exist a sequence $(x_n)$ of points of $G$,
converging to a limit \( x \in G \), and such that \( f(x_n) \) does not converge to \( f(x) \). We may write \( x_n = s_n t_n s_n^{-1} \), where \( t_n \in T \) and \( s_n \in G \), and because both \( G \) and \( T \) are compact, we may assume, by passing to a subsequence of \( (x_n) \), that \( (t_n) \) has a limit \( t \in T \), and \( (s_n) \) a limit \( s \in G \). But then \( x = st s^{-1} \); we have \( f(x_n) = g(t_n) \) and \( f(x) = g(t) \), and the hypothesis on \( (x_n) \) contradicts the continuity of \( g \).

(21.13.6) We recall (21.7.5) that the characters of the maximal torus \( T \) are the functions \( \xi \) with values in \( U \), such that \( \xi(\exp(u)) = e^{p(u)} \) for all \( u \in t \), where \( p \) is a weight of \( T \). The weights of \( T \) are \( \mathbb{R} \)-linear functions on \( T \), with values in \( i\mathbb{R} \), which take values belonging to \( 2\pi i\mathbb{Z} \) at the points of the lattice \( \Gamma_T \), the kernel of \( \exp_T = (\exp_G)|_T \). These functions form a lattice \( 2\pi i\mathbb{Z}^\ast \), which we denote by \( P(G, T) \) or \( P(G) \) (or simply \( P \)) and call the weight lattice of \( G \) (with respect to \( T \)). If \( u_1, u_2 \) are two points of \( T \) such that \( \exp(u_1) = \exp(u_2) \), we have therefore \( e^{p(u_1)} = e^{p(u_2)} \); this leads us to write \( e^p \) (or \( e^{p(s)} \)) by abuse of notation, for the character \( \xi \) corresponding to the weight \( p \), whenever there is no risk of confusion.

Consider a character \( \chi \) of \( G \). If \( U \) is an irreducible representation of \( G \) with character \( \chi \), the restriction of \( U \) to \( T \) is a Hilbert sum of one-dimensional representations, and the restriction of \( \chi \) to \( T \) may therefore be written uniquely in the form

\[
\sum_{p \in P} n(p) e^p
\]

where each \( n(p) \) is an integer \( \geq 0 \), and is zero for all but a finite number of values of \( p \in P \); it is the multiplicity (21.4.2) of the representation \( s \mapsto e^{p(s)} \cdot 1 \) in the representation \( U|_T \). This number \( n(p) \) is called the multiplicity of the weight \( p \) in the character \( \chi \) (or the representation \( U \)), and we shall say that \( p \) is contained in \( \chi \) (or is a weight of \( U \)) if \( n(p) > 0 \).

For each element \( w \) of the Weyl group \( W \), we have \( n(w \cdot p) = n(p) \) (21.13.5). This leads us to consider functions of the form (21.13.6.1) in which the integers \( n(p) \) are of arbitrary sign and satisfy the relations \( n(w \cdot p) = n(p) \) for all \( w \in W \). It is clear that these functions form a \( \mathbb{Z} \)-module, having as a basis the sums

\[
S(\Pi) = \sum_{p \in \Pi} e^p
\]

where \( \Pi \) runs through the set \( P/W \) of orbits of \( W \) in \( P \).

Since the characters \( e^p \) of \( T \) are linearly independent (21.3.2) and since, for any two weights \( p', p'' \in P \), we have \( e^p' \cdot e^p'' = e^{p'+p''} \), the set of all linear
13. LINEAR REPRESENTATIONS OF COMPACT LIE GROUPS

combinations $\sum_{p \in P} n(p)e^p$, with arbitrary integers $n(p) \in \mathbb{Z}$, may be identified with the algebra $\mathbb{Z}[P]$ of the additive group $P$ over $\mathbb{Z}$. The $\mathbb{Z}$-module having as basis the $S(\Pi)$, for all $\Pi \in P/W$, is therefore the subalgebra $\mathbb{Z}[P]^W$ of $W$-invariant elements of $\mathbb{Z}[P]$.

It follows therefore from (21.13.5) that the $\mathbb{Z}$-algebra generated by the characters of $G$, which may be canonically identified (21.4.7) with the ring $\mathbb{Z}(R(G))$ of classes of linear representations of $G$, is canonically isomorphic to a subalgebra of $\mathbb{Z}[P]^W$. In general, the basis elements $S(\Pi)$ of $\mathbb{Z}[P]^W$ are not the restrictions of characters of $G$, as can be seen already from the example of the group $SU(2)$, for which we know explicitly all the irreducible representations (21.9.3) and the Weyl group, consisting of two elements (21.12.1). We shall nevertheless show that the canonical homomorphism of $\mathbb{Z}(R(G))$ into $\mathbb{Z}[P]^W$ is always bijective (21.15.5).

(21.13.7) Let $V$ be a linear representation of $G$, and suppose that the restriction to $T$ of the function $s \mapsto \text{Tr}(V(s))$ is of the form $S(\Pi)$ for some orbit $\Pi \in P/W$. Then it follows immediately from (21.4.4) and (21.13.6) that the representation $V$ is irreducible and that $S(\Pi)$ is the restriction to $T$ of its character.

PROBLEMS

1. Let $G$ be a compact subgroup of $\text{GL}(n, \mathbb{R})$. Show that if $A$ and $B$ are two compact $G$-stable subsets of $\mathbb{R}^n$ with no common point, there exists a polynomial $P \in \mathbb{R}[T_1, \ldots, T_n]$ such that $|P(x)| \leq \frac{1}{2}$ for all $x \in A$, $|P(x) - 1| \leq \frac{1}{2}$ for all $x \in B$, and $P(s \cdot x) = P(x)$ for all $s \in G$. (Apply the Weierstrass–Stone theorem and integration with respect to a Haar measure on $G$.)

2. Deduce from Problem 1 that if $G$ is a compact subgroup of $\text{GL}(n, \mathbb{R})$ there exists a family of polynomials $P_x \in \mathbb{R}[T_1, \ldots, T_n]$ in $n^2$ indeterminates, such that $G$ is the set of matrices $s \in \text{GL}(n, \mathbb{R}) \subset \mathbb{R}^{n^2}$ such that $P_x(s) = 0$ for all $x$.

3. Let $G$ be a compact Lie group and $H$ a closed subgroup of $G$. Show that there exists a neighborhood $U$ of $H$ such that there is no subgroup $K$ of $G$ contained in $U$ that contains $H$ properly. (Use (16.14.2) and argue as in (21.13.1) for the case $H = \{e\}$.)

4. Let $G$ be a compact Lie group and $H$ a closed subgroup of $G$. Show that if $H \neq G$ there exists at least one irreducible representation of $G$, other than the trivial representation, whose restriction to $H$ contains the trivial representation. (Assume that the result is false and show, by use of (21.3.4) and (21.2.5), that for all continuous functions $f$ on $G$ we should have $\int_G f \, dm_G = \int_H f \, dm_H$, where $m_G$ and $m_H$ are the normalized Haar measures on $G$, $H$, respectively; use this to obtain a contradiction.)
5. Let $G$ be a compact Lie group and $H$ a closed subgroup of $G$. Show that there exists a continuous linear representation $U$ of $G$ on a finite-dimensional complex vector space $E$ such that $H$ is the stabilizer of some point of $E$ (for the action of $G$ on $E$ defined by $U$). (We may assume that $H \neq G$. For each closed subgroup $F$ that properly contains $H$, let $V_F$ be an irreducible representation of $F$, other than the trivial representation, whose restriction to $H$ contains the trivial representation (Problem 4), and let $U_F$ be a linear representation of $G$ whose restriction to $F$ contains $V_F$. Let $H_F \supset H$ be the stabilizer of a point $\neq 0$ in the space of $V_F$. Show that the intersection of the subgroups $H_F$ is equal to $H$, and observe that this intersection is also the intersection of a finite number of the $H_F$, by using Problem 3.)

14. ANTI-INARIANT ELEMENTS

We shall first study in more detail the structure of the algebras $Z[P]$ and $Z[P]^w$, by using the properties of root systems. We shall require the following lemma:

(21.14.1) Let $u, v$ be two linearly independent elements of $P$. If an element $\Phi \in Z[P]$ is divisible by $1 - e^u$ and by $1 - e^v$, then it is divisible by the product $(1 - e^u)(1 - e^v)$.

The $Z$-module $P$ is isomorphic to $Z^r$ for some $r > 0$. If $(j_1, \ldots, j_r)$ are the coordinates of $u$ with respect to a $Z$-basis of $P$, and if $d > 0$ is the highest common factor of the $j_k$ ($1 \leq k \leq r$), we may write $u = du_1$, where the coordinates of $u_1$ are relatively coprime. The elementary theory of free $Z$-modules (A.26.6) shows that there exists a basis $(u_1, \ldots, u_r)$ of $P$ containing $u_1$. The projection of $v$ on $Zu_2 \oplus Zu_3 \oplus \cdots \oplus Zu_r$ is nonzero, by hypothesis; by applying the same argument to this projection, we may assume that $u_2, \ldots, u_r$ have been chosen so that $v = mu_2 - nu_1$, where $m, n \in Z$ and $m \neq 0$. Since the ring $Z[P]$ is isomorphic to the ring

$$A = Z[X_1, \ldots, X_r, X_1^{-1}, \ldots, X_r^{-1}]$$

(21.4.7), it follows that we are reduced to showing that if an element $\Phi$ of this ring is divisible by $X_2^m - 1$ and by $X_2^n - X_1^n$, then it is divisible by their product. Furthermore, since the $X_k$ are invertible in $A$, we may assume that $m > 0$, and since we have $\Phi = (X_2^m - 1)\Phi_1 + \Phi_1$, with $\Phi_1 \in A$, we may also assume that $\Phi_1$ is a polynomial in $X_2$ with coefficients in the ring

$$B = Z[X_1, X_3, \ldots, X_r, X_1^{-1}, X_3^{-1}, \ldots, X_r^{-1}]$$

The Euclidean algorithm then enables us to write

$$\Phi_1 = (X_2^m - X_1^n)\Phi_2 + (\Psi_1 X_2^{m-1} + \cdots + \Psi_{m-1}),$$
where $\Phi_2 \in A$ and the $\Psi_j$ belong to $B$. By hypothesis, the product

\[(21.14.1.1) \quad (X_1^d - 1)(\Psi_1 X_2^{m-1} + \cdots + \Psi_{n-1})\]

is divisible by $X_2^m - X_1^n$. If the $\Psi_j$ were not all zero, we should be able to substitute for $X_1, X_3, \ldots, X_r$ nonzero complex numbers $z_1, z_3, \ldots, z_r$ such that $z_1^d \neq 1$ and such that the value of at least one of the coefficients $\Psi_j(z_1, z_3, \ldots, z_r)$ were $\neq 0$. Under this substitution, $(21.14.1.1)$ would become a nonzero polynomial of degree $\leq m - 1$ in $X_2$ with complex coefficients, divisible by $X_2^m - z_1^n$; and this is absurd.

We remark that the lemma $(21.14.1)$ applies equally to the ring $\mathbb{Z}[cP]$, where $c$ is any nonzero real number.

$(21.14.2)$ If $g = c \oplus \mathfrak{D}(g)$ is the canonical decomposition of the Lie algebra $g$ of $G$ as the direct sum of its center and its derived algebra $(21.6.9)$, the Lie algebra $t$ of $T$ takes the form $t = c \oplus t'$, where $t'$ is a maximal commutative subalgebra of $\mathfrak{D}(g)$. We have seen $(21.8.8)$ that the root system $S \subset it^*$ of $\mathfrak{D}(g)$ relative to $t'$ may be identified with a finite subset of the lattice of weights $P(G)$ ($t^*$ being identified with the annihilator of $c$ in $t^*$). We shall suppose that a basis $B = \{\beta_1, \ldots, \beta_l\}$ of $S$ $(21.11.5)$ has been chosen. The elements $h_a$ of $it'$, for $a \in S$, form a reduced root system $S'$, the dual of $S$ $(21.11.11)$. For simplicity we shall put $h_a = h_{\beta_a}$; we recall $(21.11.5.5)$ that the $h_a$ form a basis $B'$ of the root system $S'$, and also a basis of the real vector space $it'$.

$(21.14.3)$ The weight lattice $P = P(G)$ is contained in the set $P(g)$ of $\mathbb{C}$-linear forms $\lambda$ on $t_{\mathbb{C}}$ such that $\lambda(h_a) \in \mathbb{Z}$ for $1 \leq j \leq l$. (Since each $h_a \in S'$ is a linear combination of the $h_a$ with integer coefficients, this condition is equivalent to requiring that $\lambda(h_a)$ should be an integer for all roots $a \in S$.)

For each $p \in P(G)$, $e^p$ is a character of $T$. By virtue of $(21.13.3)$, there exists a linear representation $U$ of $G$ on a vector space $E$ such that for each $h \in t_{\mathbb{C}}$ the complex number $p(h)$ is an eigenvalue of the endomorphism $U_*(h)$ of $E$ (we identify $U_*$ with its extension $U_* \otimes 1_c$ to $g_{(\mathbb{C})}$). With the notation of $(21.10.3)$, we may apply $(21.9.3)$ to the restriction of $U_*$ to each subalgebra $s_a \subset g_{(\mathbb{C})}$ isomorphic to $\text{sl}(2, \mathbb{C})$, and conclude that $p(h_a)$ is an integer for each $a \in S$.

Since the dual $t_{\mathbb{C}}^*$ of $t_{\mathbb{C}}$ may be identified with $c_{\mathbb{C}}^* \oplus t_{\mathbb{C}}^*$ ($c^*$ being identified with the annihilator of $t'$ in $t^*$), $P(g)$ may be identified with $c_{\mathbb{C}}^* \oplus P(\mathfrak{D}(g))$, where $P(\mathfrak{D}(g)) \subset it^*$ is the lattice dual $(21.7.5)$ to the lattice in $it'$ generated by the $h_a$.
(21.14.4) In the real vector space $it^* = i\mathfrak{c}^* \oplus it^*$, the set $C$ (or $C(g)$) of linear forms $\lambda$ such that $\lambda(h_j) > 0$ ($1 \leq j \leq l$) is called the Weyl chamber relative to the basis $\mathcal{B}$ of $\mathfrak{S}$. Since the $h_j$ form a basis of the real vector space $it'$, the closure $\overline{C}$ of $C$ in $it^*$ is the set of linear forms $I$ such that $I(h_j) > 0$ for $1 \leq j \leq l$. We have $C(g) = i\mathfrak{c}^* + C(\mathfrak{d}(g))$ and $\overline{C}(g) = i\mathfrak{c}^* + \overline{C}(\mathfrak{d}(g))$.

(21.14.5) Let $L$ be the set of linear forms $\lambda \in it^*$ that can be written

$$\lambda = \gamma + \sum_{j=1}^{l} c_j \beta_j,$$

where $\gamma \in i\mathfrak{c}^*$ and the $c_j$ are real numbers $\geq 0$, not all zero. If we put $L_0 = L \cup \{0\}$, it is clear that $L_0 + L_0 \subset L_0$, $aL_0 \subset L_0$ for all real $a > 0$, and $L_0 \cap (-L_0) = \{0\}$. The relation $\mu - \lambda \in L_0$ is therefore a (partial) ordering on $it^*$, which we denote by $\lambda \leq \mu$. The relation $\lambda \leq \mu$ is equivalent to $\lambda + v \leq \mu + v$ for all $v \in it^*$, and to $\lambda a \leq a\mu$ for all real $a > 0$; and the relation $\lambda > 0$ is equivalent to $\lambda \in L$.

The positive roots (relative to the basis $\mathcal{B}$) in the sense of (21.11.5) are therefore exactly those which are $> 0$ in the ordering just defined. This justifies the terminology.

(21.14.6) (i) The Weyl chamber $C$ is contained in the set $L$ of forms $> 0$. For any $W$-invariant scalar product $\langle \lambda | \mu \rangle$ on $it^*$, we have $\langle \lambda | \mu \rangle > 0$ for all pairs of forms $\lambda$, $\mu$ such that $\lambda \in C$ and $\mu > 0$.

(ii) The Weyl chamber $C$ (resp. its closure $\overline{C}$) is the set of linear forms $\lambda \in it^*$ such that $w \cdot \lambda < \lambda$ (resp. $w \cdot \lambda \leq \lambda$) for all $w \neq 1$ in the Weyl group $W$.

(i) By virtue of (21.11.11.2), the Weyl chamber $C$ may also be defined as the set of $\lambda \in it^*$ such that $\langle \lambda | \beta_j \rangle > 0$ for $1 \leq j \leq l$. In view of (21.11.5.3), the relation $C \subset L$ is a consequence of the following lemma:

(21.14.6.1) In a real Hilbert space $E$, let $(\beta_j)_{1 \leq j \leq n}$ be a finite free family such that $\langle \beta_j | \beta_k \rangle \leq 0$ whenever $j \neq k$. Then, if $\lambda = \sum_{j=1}^{n} c_j \beta_j$ is such that $\langle \lambda | \beta_j \rangle \geq 0$ for $1 \leq j \leq n$, we must have $c_j \geq 0$ for $1 \leq j \leq n$.

The result is obvious if $n = 1$, and we proceed by induction on $n$. It is not possible that $c_j < 0$ for all $j$, because it would then follow that $\langle \lambda | c_j \beta_j \rangle \leq 0$ for all $j$, and therefore

$$\langle \lambda | \lambda \rangle = \sum_{j=1}^{n} \langle \lambda | c_j \beta_j \rangle \leq 0,$$
so that \( \lambda = 0 \), contradicting the hypothesis that \( c_j \neq 0 \) for all \( j \). Suppose therefore, without loss of generality, that \( c_n \geq 0 \). Then, for \( 1 \leq j \leq n - 1 \), we have

\[
c_1(\beta_1 | \beta_j) + \cdots + c_{n-1}(\beta_{n-1} | \beta_j) \geq -c_n(\beta_n | \beta_j) \geq 0,
\]

and by applying the inductive hypothesis to \( c_1 \beta_1 + \cdots + c_{n-1} \beta_{n-1} \), we deduce that \( c_j \geq 0 \) for \( 1 \leq j \leq n \).

If \( \mu > 0 \), it follows from the definition (21.14.4) that we may write

\[
\mu = \gamma + \sum_{j=1}^{l} t_j \beta_j,
\]

where \( \gamma \in i\mathfrak{t}^* \) and \( t_j \geq 0 \) for \( 1 \leq j \leq l \), and at least one of the \( t_j \) is \( > 0 \). If then \( \lambda \in C \), we have \( (\lambda | \mu) = \sum_{j=1}^{l} t_j(\lambda | \beta_j) > 0 \), because \( (\lambda | \beta_j) > 0 \) for \( 1 \leq j \leq l \).

(ii) If \( w \cdot \lambda < \lambda \) for all \( w \neq 1 \) in \( W \), then in particular (21.10.6) \( s_a \cdot \lambda = \lambda - \lambda(h_a) \alpha < \lambda \) for all positive roots \( \alpha \), which is possible only if \( \lambda(h_j) > 0 \) for \( 1 \leq j \leq l \), in other words if \( \lambda \in C \). To prove the converse, put \( s_j = s_{\beta_j} \) for \( 1 \leq j \leq l \); then \( W \) is generated by the reflections \( s_j \) (21.11.8), and we shall argue by induction on the smallest number \( p \) such that \( w \) can be written in the form \( w = s_{j_1} s_{j_2} \cdots s_{j_p} \). The result is clear if \( p = 1 \); suppose therefore that it is true for all products of at most \( p - 1 \) reflections \( s_j \), and put \( w = w's_{j_p} \), where \( w' = s_{j_1} s_{j_2} \cdots s_{j_{p-1}} \). Then we have \( w \cdot \lambda = w' \cdot \lambda - \lambda(h_{j_p}) w' \cdot \beta_{j_p} \). We distinguish two cases, according as the root \( w' \cdot \beta_{j_p} \) is positive or negative. In the first case, the hypothesis \( \lambda(h_{j_p}) > 0 \) implies that \( w \cdot \lambda < \lambda \). Consider therefore the second case, and let \( r \) be the least integer such that for all \( k \geq r \) the root \( \alpha_k = s_{j_k} s_{j_{k+1}} \cdots s_{j_{p-1}} \cdot \beta_{j_p} \) is positive. This number \( r \) always exists (if we agree to put \( r = p \) and \( \alpha_p = \beta_{j_p} \) when \( \alpha_k < 0 \) for \( 1 \leq k \leq p - 1 \), and we have \( r > 1 \) because \( w' \cdot \beta_{j_p} < 0 \). By definition, we have \( \alpha_r > 0 \) and \( \alpha_{r-1} = s_{j_{r-1}} \cdot \alpha_r < 0 \), and by virtue of (21.11.6), this is possible only if \( \alpha_r = \beta_{j_{r-1}} \). Now put \( w_1 = s_{j_1} s_{j_2} \cdots s_{j_{r-2}} \), \( w_2 = s_{j_k} \cdots s_{j_{p-1}} \), so that \( w' = w_1 s_{j_{r-1}} w_2 \), and \( w_2 \cdot \beta_{j_p} = \beta_{j_{r-1}} \). Since \( w_2 s_a w_2^{-1} = s_{w_2 a} \) for all roots \( \alpha \), we have \( w_2 s_{j_p} = s_{j_{r-1}} w_2 \) and therefore

\[
w = w's_{j_p} = w_1 s_{j_{r-1}}^2 w_2 = w_1 w_2;
\]

in other words, \( w \) can be written as a product of \( p - 2 \) reflections \( s_j \), and hence \( w \cdot \lambda < \lambda \) by virtue of the inductive hypothesis. For the relations \( w \cdot \lambda \leq \lambda \) and \( \lambda \in C \), the proof is the same.

(21.14.6.2) Let \( \lambda \in i\mathfrak{t}^* \) be such that \( \lambda(h_j) \) is an integer \( \geq 0 \) for \( 1 \leq j \leq l \)(or, equivalently, such that \( \lambda(h_a) \) is an integer \( \geq 0 \) for all positive roots \( \alpha \) (relative
to $B$, since the $h_j$ form a basis of the root system $S^\vee$ formed by the $h_x$ (21.11.5.5). Then for each $w \in W$ we have

$$w \cdot \lambda = \lambda - \sum_{j=1}^{l} n_j \beta_j \quad (21.14.6.3)$$

where the $n_j$ are integers $\geq 0$. We may proceed by induction as in the proof of (21.14.6(iii)), since the result is obvious when $w = s_j$. With the same notation, the case in which $w' \cdot \beta_j$ is a negative root can be eliminated, because $w$ is then a product of $p-2$ reflections $s_j$; and if $w' \cdot \beta_j$ is a positive root, we may write $w' \cdot \beta_j = \sum_{j=1}^{l} n'_j \beta_j$, where the $n'_j$ are integers $\geq 0$, and $w' \cdot \lambda = \lambda - \sum_{j=1}^{l} n''_j \beta_j$ where the $n''_j$ are integers $\geq 0$. From these two equations we obtain (21.14.6.3), with $n_j = n'_j \lambda(h_{j_p}) + n''_j$.

(21.14.6.4) It follows from (21.11.5.3) that if there are two roots $\beta_j, \beta_k \in B$ such that $(\beta_j | \beta_k) \neq 0$, then they cannot belong to $\bar{C}$. In all the examples considered in (21.12), with the exception of $SU(2)$, none of the basis roots therefore belong to $\bar{C}$.

(21.14.7) For each root $\alpha \in S$, let $H_\alpha$ be the hyperplane in $it^*$ defined by the equation $\lambda(h_\alpha) = 0$. A linear form $\lambda \in it^*$ is said to be singular if it belongs to at least one of the $H_\alpha$, and regular if it does not. Clearly the Weyl group transforms regular forms into regular forms, and singular forms into singular forms.

(21.14.7.1) For each regular linear form $\lambda \in it^*$, there exists one and only one element $w$ of the Weyl group $W$ such that $w \cdot \lambda \in C$. For each linear form $\lambda \in it^*$ there exists one and only one $w \cdot \lambda$ in the $W$-orbit of $\lambda$ that belongs to $C$.

Suppose first that $\lambda$ is regular. We may write $\lambda = \gamma + \mu$, where $\gamma \in it^*$ and $\mu \in it^*$, and since $\gamma(h_\alpha) = 0$ for all $\alpha \in S$ we have $\mu(h_\alpha) \neq 0$ for all $\alpha \in S$. It follows then from (21.11.5.2), applied to the dual root system $S^\vee$, that $\mu$ defines a basis $B^\vee_\mu$ of $S^\vee$. By virtue of (21.11.8), there exists $w \in W$ such that $w(B^\vee_\gamma) = B^\vee$; and since $w(B^\vee_\mu) = B^\vee_{-\mu}$ and $w \cdot \gamma = \gamma$, this implies that $w \cdot \lambda \in C$, by definition. The uniqueness of $w$ follows from the same argument, in conjunction with the fact that $W$ acts simply transitively on the set of bases of $S^\vee$ (21.11.10.1).
Now let \( \lambda \) be any element of \( \mathfrak{g}^* \), and let \( \lambda_0 \) be a regular linear form. Since the number of hyperplanes \( H_x \) is finite, the linear form \( \lambda + t(\lambda_0 - \lambda) \) is singular for only finitely many values of \( t \in \mathbb{R} \), and we may therefore assume that it is regular for \( 0 < t \leq 1 \). Let \( w \in W \) be such that \( w \cdot \lambda_0 \in C \); since \( w \cdot (\lambda + t(\lambda_0 - \lambda)) \) is regular for \( 0 < t \leq 1 \), all these linear forms belong to \( C \), and therefore \( w \cdot \lambda \) must belong to the closure \( \bar{C} \).

If \( \lambda \in \bar{C} \) and if there were an element \( w \in W \) such that \( w \cdot \lambda \not\in \bar{C} \) and \( w \cdot \lambda \neq \lambda \), we should have \( w \cdot \lambda \leq \lambda \) by (21.14.6), hence \( w \cdot \lambda < \lambda \). But since \( \lambda = w^{-1} \cdot (w \cdot \lambda) \), the same argument shows that \( w \cdot \lambda > \lambda \), which is absurd.

(21.14.8) (i) The half-sum \( \delta \) of the positive roots of \( \mathfrak{g} \) (21.11.7) is such that \( \delta(h_j) = 1 \) for \( 1 \leq j \leq l \), and hence belongs to \( C \cap P(g) \).

(ii) Every element of \( P(g) \cap C \) is of the form \( \delta + p \), where \( p \in P(g) \cap \bar{C} \).

(iii) For each \( p \in P \cap \bar{C} \), the set of linear forms \( q \in P \cap \bar{C} \) such that \( q \leq p \) is finite.

(i) We have seen in (21.11.7) that \( s_j \cdot \delta = \delta - \delta(h_j) \cdot \beta_j = \delta - \beta_j \), hence \( \delta(h_j) = 1 \) for \( 1 \leq j \leq l \).

(ii) If \( \lambda \in P(g) \cap C \), we have \( \lambda(h_j) > 0 \) for \( 1 \leq j \leq l \) and moreover \( \lambda(h_j) \) is an integer, hence \( \lambda(h_j) \geq 1 \) for \( 1 \leq j \leq l \). Consequently \( p = \lambda - \delta \) is such that \( p(h_j) \geq 0 \) for all \( j \), hence \( p \in P(g) \cap \bar{C} \). The converse is obvious.

(iii) Since \( p - q \geq 0 \) and \( p, q \) are in \( \bar{C} \), we have \( (p | p - q) \geq 0 \) and \( (q | p - q) \geq 0 \) (21.14.6), so that \( (q | q) \leq (p | q) \leq (p | p) \). But since \( P \) is a discrete subspace of \( \mathfrak{g}^* \), its intersection with the closed ball with center 0 and radius \( (p | p)^{1/2} \) is finite (3.16.3), whence the result.

(21.14.8.1) If the compact connected group \( G \) is semisimple, the set \( P(g) \) is also discrete, because \( c = \{0\} \). The proof of (iii) above then applies without any modification to show that, for each \( p \in P(g) \cap \bar{C} \), the set of \( q \in P(g) \cap \bar{C} \) such that \( q \leq p \) is finite.

(21.14.9) The elements of the Weyl group, considered as endomorphisms of \( \mathfrak{g}^* \), belong to the orthogonal group relative to the scalar product \( (\lambda | \mu) \), hence have determinant equal to \( \pm 1 \). An element \( \Phi \) of the free \( \mathbb{Z} \)-module \( \mathbb{Z}[\mathfrak{p}] \) (or of \( \mathbb{Z}[c\mathfrak{p}] \), where \( c \) is a nonzero real number) is said to be anti-invariant under \( W \) if \( w \cdot \Phi = \det(w)\Phi \) for all \( w \in W \). For each \( p \in P \), the element

\[
J(e^p) = \sum_{w \in W} \det(w)e^w \cdot p
\]
of $\mathbb{Z}[P]$ is anti-invariant, because for each $w' \in W$ we have

$$w' \cdot J(e^p) = \sum_{w \in W} \det(w)(w' \cdot e^w \cdot p)$$

$$= \sum_{w \in W} \det(w)e^{(w'w) \cdot p}$$

$$= \det(w') \sum_{w \in W} \det(w)e^{(w'w) \cdot p}$$

$$= \det(w')J(e^p).$$

(21.14.10) (i) If the weight $p \in P$ is a singular linear form (21.14.6.3), we have $J(e^p) = 0$.

(ii) As $p$ runs through $P \cap C$, the elements $J(e^p)$ form a basis of the $\mathbb{Z}$-module $\mathbb{Z}[P]^W$ of anti-invariant elements of $\mathbb{Z}[P]$.

(i) Suppose that $p(h_a) = 0$ for some root $a \in S$; then we have $s_a \cdot p = p$, where $s_a$ is the corresponding reflection. If $W'$ is a set of representatives of the left cosets of the subgroup $\{1, s_a\}$ in $W$, we have

$$J(e^p) = \sum_{w' \in W'} (\det(w')e^{w' \cdot p} + \det(w's_a)e^{(w's_a) \cdot p})$$

$$= 0$$

because $\det(w's_a) = -\det(w')$ and $(w's_a) \cdot p = w' \cdot p$.

(ii) To say that an element $\sum_{p \in P} z_p e^p$ of $\mathbb{Z}[P]$ (where $z_p \in \mathbb{Z}$ for all $p \in P$) is anti-invariant means that $z_w \cdot p = \det(w)z_p$ for all $w \in W$, and consequently the $J(e^p)$ generate the $\mathbb{Z}$-module $\mathbb{Z}[P]^W$. It follows from (21.14.7) that the group $W$ acts freely on the set $P_{\text{reg}}$ of weights that are regular linear forms, so that $J(e^p) \neq 0$ for all $p \in P_{\text{reg}}$; furthermore, each $W$-orbit in $P_{\text{reg}}$ intersects $C$ in exactly one point (21.14.7), hence the $J(e^p)$ with $p \in P \cap C = P_{\text{reg}} \cap C$ are linearly independent over $\mathbb{Z}$. In view of (i), this proves (ii).

The results of (21.14.10) apply unchanged to $\mathbb{Z}[cP]$ if $c > 0$.

(21.14.11) Given an element $\Phi = \sum_{p \in P} z_p e^p$ of $\mathbb{Z}[P]$, we shall say that $z_p e^p$ is the leading term of $\Phi$ if $z_p \neq 0$ and if $p' < p$ for all other $p' \in P$ such that $z_{p'} \neq 0$. It is clear that if $z_p e^p$ is the leading term of $\Phi$, and if $\Phi' = \sum_{p \in P} z_p e^p$ is another element of $\mathbb{Z}[P]$, with leading term $z'_q e^q$, then $z_p z'_q e^{p+q}$ is the leading term of $\Phi \Phi'$. This definition and this remark apply without change to $\mathbb{Z}[cP]$, $c > 0$.

It follows from (21.14.7) that each orbit $\Pi \in P/W$ intersects $C$ in exactly
14. ANTI-IN Variant ELEMENTS 117

one point \( p \). For \( p \in P \cap \mathbb{C} \) we therefore denote the sum \( S(\Pi) \) by \( S(p) \). Since \( w \cdot p \leq p \) for all \( w \in W \) (21.14.6), it follows that \( e^p \) is the leading term of \( S(p) \). Every element \( \Psi \) of \( Z[P]^w \) that has leading term \( z_p e^p \) may therefore be written uniquely in the form \( \Psi = z_p S(p) + \sum_{q \in P \cap \mathbb{C}, q < p} z_q S(q) \), where \( z_p \) and the \( z_q \) are integers.

(21.14.12) Since the roots \( \alpha \in S \) belong to \( P \) (21.14.2), the element

\[
\Delta = \prod_{\alpha \in S^+} (e^{\alpha/2} - e^{-\alpha/2})
\]

(where \( S^+ \) is the set of positive roots, relative to the basis \( B \)) belongs to \( Z[\frac{1}{2}P] \), but not necessarily to \( Z[P] \) (cf. (21.16.10)). We have

\[
\Delta = e^\delta \prod_{\alpha \in S^+} (1 - e^{-\alpha}) = e^{-\delta} \prod_{\alpha \in S^+} (e^{\alpha} - 1);
\]

by virtue of (21.14.8), this shows that \( \Delta \) belongs to \( Z[P(\delta)] \) in any case, and that \( e^{-\delta} \Delta \) belongs to \( Z[P] \); moreover the first of the formulas (21.14.12.2) shows immediately that \( e^\delta \) is the leading term of \( \Delta \) (21.14.11). By virtue of the formula (21.14.12.1), \( \Delta \) is anti-invariant. Indeed, it is enough to show that \( s_j \cdot \Delta = -\Delta \) for \( 1 \leq j \leq l \), because \( W \) is generated by the reflections \( s_j \), in the notation of (21.14.7); but by virtue of (21.14.7), \( s_j \) changes the sign of the factor \( e^{\beta_j/2} - e^{-\beta_j/2} \) and permutes the other factors of \( \Delta \), whence the result.

(21.14.13) (i) We have \( \Delta = J(e^\delta) \) in \( Z[\frac{1}{2}P] \).

(ii) For each weight \( p \in P \cap \mathbb{C} \), the element \( J(e^{p+\delta})/J(e^\delta) \) is an invariant element of \( Z[P] \), with leading term equal to \( e^p \).

(iii) For each \( p \in P \cap \mathbb{C} \), let \( \Psi_p \) be an element of \( Z[P]^w \) with leading term equal to \( e^p \); then the \( \Psi_p \) form a \( Z \)-basis of the \( Z \)-algebra \( Z[P]^w \). (In particular, this is so for the elements \( J(e^{p+\delta})/J(e^\delta) \).)

(i) Since \( \Delta \) is anti-invariant and belongs to \( Z[\frac{1}{2}P] \), it is a linear combination with integral coefficients of the \( J(e^q) \) with \( q \in \frac{1}{2}P \cap \mathbb{C} \) (21.14.10); but since \( e^{-\delta} \Delta \in Z[P] \), we must have \( q - \delta \in P \) for each of the \( J(e^q) \) appearing in \( \Delta \) with a nonzero coefficient; hence \( \Delta = \sum_{p \in P \cap \mathbb{C}} z_p J(e^{p+\delta}) \), with \( z_p \in Z \). The coefficient of \( e^{p+\delta} \) in \( \Delta \) is therefore \( z_p \). Now, for \( p \in P \cap \mathbb{C} \) and \( p \neq 0 \), \( p + \delta \) is not comparable with \( \delta \) with respect to the ordering if \( p \in i\mathbb{C}^* \), and is \( \geq \delta \) otherwise. Since all the terms of \( \Delta \) other than \( e^\delta \) are of the form \( z_q e^q \) with \( q < \delta \), we must have \( z_p = 0 \) for \( p \neq 0 \), and \( z_0 = 1 \).
(ii) Since \( w \cdot \delta - \delta \in \mathcal{P} \) for all \( w \in W \) (21.11.7), it follows that 
\[ e^{-\delta}J(e^{p+\delta}) \] 
belongs to \( \mathbb{Z}[\mathcal{P}] \). Hence, by virtue of (21.14.12.2) and (21.14.1), it is enough to show that 
\[ e^{-\delta}J(e^{p+\delta}) \] 
is divisible by each of the elements \( 1 - e^{-a} \) with \( a \in \mathbf{S}^+ \) (bearing in mind that no two distinct elements of \( \mathbf{S}^+ \) are proportional). If \( W' \) is a set of representatives of the right cosets of the subgroup \( \{1, s_a\} \) in \( W \), we have 
\[ e^{-\delta}J(e^{\vartheta}) = \sum_{w' \in W'} \det(w')(e^{w' \cdot q} - e^{w \cdot q})e^{-\delta} \]
where \( q = p + \delta \). But since \( q \in \mathcal{P}(g) \), we have \( w' \cdot q \in \mathcal{P}(g) \) and therefore \( s_a \cdot (w' \cdot q) = w' \cdot q - m(w')a \), where \( m(w') \) is an integer. We reduce therefore to showing that \( 1 - e^{-ma} \) is divisible by \( 1 - e^{-a} \) in \( \mathbb{Z}[\mathcal{P}] \) for all integers \( n \in \mathbb{Z} \).

This is clear if \( n \geq 0 \), and if \( n < 0 \) we have only to remark that 
\[ 1 - e^{-ma} = e^{-na}(e^{-a} - 1) \] 
and that \( e^{-a} \) is invertible in \( \mathbb{Z}[\mathcal{P}] \).

Now put 
\[ J(e^{p+\delta})/J(e^{\delta}) = \sum_{r \in \mathcal{P}} z_r e^r \] 
and let \( u \) be a maximal element of the finite set of \( r \in \mathcal{P} \) such that \( z_r \neq 0 \). We shall show that \( \delta + u \) is maximal among the elements \( v \in \frac{1}{2}\mathcal{P} \) such that the coefficient of \( e^v \) in \( J(e^{p+\delta}) \) is \( \neq 0 \). Indeed, if \( z_r e^r \) is a term of \( J(e^{\vartheta}) \) other than \( e^u \), then \( t < \delta \); if we had \( t + r > \delta + u \), it would follow that \( r > u + \delta - t > u \), contrary to the hypothesis that \( u \) is maximal. Since \( p + \delta \in \mathcal{C} \), we have \( p + \delta > w \cdot (p + \delta) \) for all \( w \neq 1 \) in \( W \) (21.14.6), and consequently \( e^{p+\delta} \) is the leading term of \( J(e^{p+\delta}) \); hence \( u = p \) and \( z_{p} = 1 \), and \( e^{p} \) is the leading term of \( J(e^{p+\delta})/J(e^{\delta}) \).

(iii) The hypothesis implies that for each \( p \in \mathcal{P} \cap \mathcal{C} \) we may write

\[ (21.14.13.1) \quad \Psi_p - S(p) = \sum_{q \in \mathcal{P} \cap \mathcal{C}, q < p} z_{pq} S(q). \]

We shall first show that the \( \Psi_p \) are linearly independent. If not, there would exist a finite nonempty subset \( I \) of \( \mathcal{P} \cap \mathcal{C} \), and for each \( p \in I \) an integer \( c_p \neq 0 \) such that \( \sum_{p \in I} c_p \Psi_p = 0 \), and therefore, by \( 21.14.13.1 \),

\[ (21.14.13.2) \quad \sum_{p \in I} c_p \left( S(p) + \sum_{q \in \mathcal{P} \cap \mathcal{C}, q < p} z_{pq} S(q) \right) = 0. \]

There exists in the finite set \( I \) a maximal element \( r \). For each \( p \in I \) distinct from \( r \) (resp. each \( q \in \mathcal{P} \cap \mathcal{C} \) such that \( q < r \) or \( q < p \) for \( p \in I \) and \( p \neq r \)) there cannot appear in \( S(p) \) (resp. \( S(q) \)) a term in \( e^r \) with a nonzero coefficient, because this would imply that \( r < p \) (resp. \( r \leq q < r \) or \( r \leq q < p \)) by virtue of \( 21.14.11 \), contradicting the definition of \( r \). Hence we cannot have \( c_r \neq 0 \), which proves our assertion.
Next we shall prove that each $S(p)$, for $p \in P \cap \tilde{C}$, is a linear combination of the $\Psi_q$ with $q \in P \cap \tilde{C}$. Suppose that this were not the case, and let $p_0 \in P \cap \tilde{C}$ be an element for which the assertion is not true. Since the set of weights $p \leq p_0$ in $P \cap \tilde{C}$ is finite (21.14.8), we may assume that $p_0$ is minimal, in other words, that for each $p \in P \cap \tilde{C}$ such that $p < p_0$, $S(p)$ is a linear combination of the $\Psi_q$. But then the relation (21.14.13.1), with $p = p_0$, would show that the difference $\Psi_{p_0} - S(p_0)$ was a linear combination of the $\Psi_q$ with $q \in P \cap \tilde{C}$, and we should arrive at a contradiction.

15. WEYL'S FORMULAS

(21.15.1) Let $G$ be a compact connected Lie group, $T$ a maximal torus of $G$. Then the $C^\infty$ mapping $(s, t) \mapsto sts^{-1}$ of $G \times T$ into $G$ is a submersion (16.7.1) at all points $(s, t)$ such that $t$ is regular (21.7.1).

For each $s_0 \in G$, we have $sts^{-1} = s_0((s_0^{-1}s)t(s_0^{-1}s)^{-1})s_0^{-1}$; therefore, since $x \mapsto s_0 x s_0^{-1}$ is an automorphism of $G$, it is enough to prove the proposition at the point $(e, t)$ of $G \times T$. Let $t$ be the Lie algebra of $T$ and let $m$ be the subspace of the Lie algebra $g$ of $G$ that is the direct sum of the $(g_0 + g_{-}) \cap g$ (in the notation of (21.8.1)) and supplementary to $t$. Since the exponential mapping is a diffeomorphism of a neighborhood of $0$ in $g$ onto a neighborhood of $e$ in $G$, it will be enough to show that the $C^\infty$ mapping $\varphi: (u, t) \mapsto \exp(u)t_0(\exp(u))^{-1}$ is a submersion of $\tilde{m} \times T$ into $G$ at the point $(0, t_0)$ when $t_0 \in T$ is regular. Since the dimensions of $\tilde{m} \times T$ and $G$ are equal, it comes to the same thing to show that the tangent linear mapping $T_{(0, t_0)}(\varphi)$ is injective (A.4.11). The tangent vectors in $T_{(0, t_0)}(\tilde{m} \times T)$ are of the form $(v, t_0 \cdot w)$ with $v \in \tilde{m}$ and $w \in t$. Let us apply (16.6.6) to the functions $\varphi(0, \cdot): t \mapsto t$ and $\varphi(\cdot, t_0): u \mapsto \exp(u)t_0(\exp(u))^{-1}$: the second of these is the composition of the left translation $z \mapsto t_0 z$, the mapping $(x, y) \mapsto xy$ of $G \times G$ into $G$ and the mapping $u \mapsto (t_0^{-1}\exp(u)t_0, \exp(u))^{-1}$ of $\tilde{m}$ into $G \times G$. Using the formulas of (16.9.9), we obtain

\[ (21.15.1.1) \quad T_{(0, t_0)}(\varphi) \cdot (v, t_0 \cdot w) = t_0 \cdot (\text{Ad}(t_0^{-1}) \cdot v - v + w). \]

If this tangent vector is zero, then $w = v - \text{Ad}(t_0^{-1}) \cdot v$ belongs to both $t$ and $\tilde{m}$, because the choice of $\tilde{m}$ ensures that it is stable under $\text{Ad}(t)$ for all $t \in T$; consequently $w = 0$ and $v = \text{Ad}(t_0^{-1}) \cdot v$. But the second of these relations implies that $v = 0$, by reason of the hypothesis that $t_0$ is regular (21.8.4), and the proof is complete.
For each \( t' \in T \), we have \((st')t(s't')^{-1} = sts^{-1}\) for all \( s \in G \) and \( t \in T \), because \( T \) is commutative. If \( \pi: G \to G/T \) is the canonical projection, it follows therefore that the mapping \((s, t) \mapsto sts^{-1}\) factorizes as

\[
(G \times T) \xrightarrow{T \times 1} (G/T) \times T \xrightarrow{\pi \times 1} G
\]

where \( f \) is of class \( C^\infty \) ((16.10.4) and (16.10.5)). Let \( T_{\text{reg}} \) be the set of regular points of \( T \); it is a dense open subset of \( T \), whose complement \( N \) is the union of the tori \( U_\alpha \) of dimension \( \dim(T) - 1 \), as \( \alpha \) runs through the set \( S^+ \) of positive roots of \( G \) relative to \( T \) (with respect to an arbitrary basis \( B \) of the root system \( S \)) (21.8.4). Hence \((G/T) \times N\) is negligible in \((G/T) \times T\) (16.22.2), and it follows from Sard's theorem that the compact set \( f((G/T) \times N)\) is negligible in \( G \) (16.23.2). Next, the restriction of \( f \) to \((G/T) \times T_{\text{reg}}\) is a submersion of this open set onto an open subset \( V \) in \( G \), by virtue of (21.15.1) and (16.7.5). Finally, the mapping \( f \) is surjective by (21.7.4), hence \( G \) is the union of \( V \) and \( f((G/T) \times N)\), from which it follows that the complement of \( V \) is negligible.

Let \( W \) be the Weyl group of \( G \) relative to \( T \). We shall show that \((G/T) \times T_{\text{reg}}\) is a covering of the open set \( V \), with \( \text{Card}(W) \) sheets, the projection being the restriction of \( f \). For this purpose, we shall show that \( W \) acts differentiably and freely on \((G/T) \times T_{\text{reg}}\), so that the orbits are precisely the intersections of this submanifold with the inverse images \( f^{-1}(x) \) for \( x \in V \). In the first place, since \( W \) permutes the roots (21.8.6), it leaves \( T_{\text{reg}} \) stable and acts differentiably on this manifold by virtue of (16.10.4) and the definition of \( W \) (21.7.16). Next, the normalizer \( N(T) \) of \( T \) in \( G \) acts on \( G/T \) on the right, by the rule \( n(s) \cdot x = \pi(sx) \) for \( s \in G \) and \( x \in N(T) \), because we have \( sTx = sxT \) since \( x \) normalizes \( T \). Furthermore, if \( x' = xt \), where \( t \in T \), then \( \pi(sx') = \pi(sx) \), and therefore for each coset \( w \in W = N(T)/T \) we may define \( \pi(s) \cdot w \) as the common value of \( \pi(sx) \) for all \( x \in w \). It is clear that this action of \( W \) on \( G/T \) is differentiable (16.10.4) and free, because the relation \( \pi(sx) = \pi(s) \) implies that \( x \in T \). We now define a left action of \( W \) on \((G/T) \times T_{\text{reg}}\) by the rule \( w \cdot (\pi(s), t) = (\pi(s) \cdot w^{-1}, w \cdot t) \) for \( w \in W \), \( s \in G \), and \( t \in T_{\text{reg}} \). Clearly this is a free action of \( W \). Moreover, if \( sts^{-1} = s't's'^{-1} \), where \( s, s' \in G \) and \( t, t' \in T \), there exists \( w \in W \) such that \( t' = w \cdot t \) (21.7.17), and it follows that \( \pi(s') = \pi(s) \cdot w^{-1} \). The restriction of \( f \) to \((G/T) \times T_{\text{reg}}\) therefore factorizes as

\[
(G/T) \times T_{\text{reg}} \xrightarrow{\pi} ((G/T) \times T_{\text{reg}})/W \xrightarrow{f_0} V,
\]

and since \( f \) maps each open set in \((G/T) \times T_{\text{reg}}\) to an open set in \( V \), the mapping \( f_0 \) is a homeomorphism of the orbit space \(((G/T) \times T_{\text{reg}})/W\) onto \( V \). But since the restriction of \( f \) to \((G/T) \times T_{\text{reg}}\) is a submersion, we deduce
from (16.10.3) that the orbit manifold exists, and that \( f_0 \) is a diffeomorphism. The result now follows from (16.14.1).

(21.15.3) With the notation of (21.15.1), let \( l = \dim(T) \) (the rank of \( G \)), and \( 2n = \dim(G/T) = \dim(m) \). Let \( \nu_G \) and \( \nu_T \) denote the translation-invariant volume forms on \( G \) and \( T \), respectively, corresponding (16.24.1) to the normalized Haar measures \( m_G \) and \( m_T \) on \( G \) and \( T \), respectively. We shall show that there is a canonically determined volume form \( \nu_{G/T} \) on \( G/T \), invariant under the action of \( G \). For this purpose, we observe that the tangent space \( T_{\pi(e)}(G/T) \) may be canonically identified with \( g/t \), and hence also with the supplement \( m \) of \( t \) in \( g \). The image of a 2n-vector \( \mathbf{z} \in \bigwedge^2 \mathfrak{t}(G/T) \) under the diffeomorphism \( x \mapsto s \cdot x \) is \( \bigwedge^2 \mathfrak{t}_s(\pi(e)) \cdot (s \cdot \mathbf{z}) \in \bigwedge^2 \mathfrak{t}_s \pi(e)(G/T) \); it depends only on the point \( s \cdot \pi(e) \in G/T \), not on \( s \in G \). For the relation \( s \cdot \pi(e) = s' \cdot \pi(e) \) is equivalent to \( s' = st \) for some \( t \in T \), and we therefore have to see that \( \bigwedge^2 \mathfrak{t}_s(\pi) \cdot (t \cdot \mathbf{z}) = \mathbf{z} \).

Now, for each vector \( \mathbf{u} \in \mathfrak{m} \), we have
\[
\bigwedge^2 \mathfrak{t}_t(\pi) \cdot (\mathbf{u} \cdot t^{-1}) = \mathbf{u},
\]
with the identification made above, and therefore
\[
\bigwedge^2 \mathfrak{t}_t(\pi) \cdot (t \cdot \mathbf{u}) = \text{Ad}(t) \cdot \mathbf{u} \in \mathfrak{m} \text{ (since } \mathfrak{m} \text{ is stable under } \text{Ad}(t)) ;
\]
but \( t \mapsto \text{Ad}(t) | \mathfrak{m} \) is a homomorphism of \( T \) into the orthogonal group of the restriction to \( \mathfrak{m} \) of an \( \text{Ad}(G) \)-invariant scalar product on \( g \); since \( T \) is connected, the determinant of \( \text{Ad}(t) | \mathfrak{m} \) is necessarily equal to 1, and therefore we have
\[
\bigwedge^2 \mathfrak{t}_t(\pi) \cdot (t \cdot \mathbf{z}) = \bigwedge^2 \text{Ad}(t) \cdot \mathbf{z} = \mathbf{z}.
\]

Let now \( \mathbf{e}^* \) be a 2n-covector on \( \mathfrak{m} \) such that \( \mathbf{e}^* \wedge \nu_T(e) = \nu_G(e) \) (we are identifying \( \mathbf{e}^* \) and \( \nu_T(e) \) with their canonical images in \( \bigwedge^2 \mathfrak{g}^* \) under \( \bigwedge^2 \text{pr}_1 \) and \( \bigwedge^2 \text{pr}_2 \); for each \( s \in G \) the 2n-covector \( s \cdot \mathbf{e}^* \) in \( \bigwedge^2 \mathfrak{t}_s \pi(e)(G/T) \) depends on \( x = s \cdot \pi(e) \) and not on \( s \), by the remarks above and (19.1.9.1). We may therefore define \( \nu_{G/T}(x) = s \cdot \mathbf{e}^* \). We denote by \( m_{G/T} \) the positive measure on \( G/T \) corresponding to \( \nu_{G/T} \) (16.24.1), which is therefore \( G \)-invariant.

By abuse of notation, we denote by \( \nu_{G/T} \wedge \nu_T \) the volume form on \( (G/T) \times T \) that is equal to \( \bigwedge^2 \text{pr}_1(\nu_{G/T}) \wedge \bigwedge^2 \text{pr}_2(\nu_T) \), to which corresponds the product measure \( m_{G/T} \otimes m_T \). For the \( C^\infty \) mapping \( f \) defined in (21.15.2.1), \( f(\nu_G) \) is a \( (2n + l) \)-form on \( (G/T) \times T \), and we may therefore write
\[
(21.15.3.1) \quad f(\nu_G) = \Theta \cdot (\nu_{G/T} \wedge \nu_T).
\]

+ The use of the letter \( T \) (with indices) to denote tangent spaces and tangent linear mappings should not be confused with the use of the same letter (without indices) to denote a maximal torus in \( G \).
We propose to calculate the numerical function \( \Theta \) on \((G/T) \times T\). For this purpose, we first remark that since \( f(\pi(s), t) = s f(\pi(e), t) s^{-1} \) by definition (i.e., \( f \circ \gamma(s) = \text{Int}(s) \circ f \), where \( \gamma(s) \) denotes the diffeomorphism \((x, t) \mapsto (s \cdot x, t)\) of \((G/T) \times T\) onto itself), by transport of structure we have also \( f(s \cdot v_G \cdot s^{-1}) = s \cdot f(v_G) \), and \( s \cdot v_G \cdot s^{-1} = v_G \) since \( G \) is unimodular. Also \( s \cdot v_{G/T} = v_{G/T} \), and therefore we see that for all \( s \in G \) we have

\[
(21.15.3.2) \quad \Theta(\pi(s), t) = \Theta(\pi(e), t).
\]

If as before we identify \( \mathfrak{m} \) and \( T_{\pi(e)}(G/T) \), the calculation in (21.15.1) shows that

\[
T_{(\pi(e), 0)}(f) \cdot (v, t \cdot w) = t \cdot (\text{Ad}(t^{-1}) \cdot v - v + w)
\]

for \( v \in \mathfrak{m} \) and \( w \in t \), since \( T_0(\exp_G) \) is the identity mapping. The definition of \( f'(v_G) \) (16.20.9.3) and the choice of \( e^* \) then show that

\[
(21.15.3.3) \quad \Theta(\pi(e), t) = \det((\text{Ad}(t^{-1})|\mathfrak{m}) - 1_\mathfrak{m}).
\]

Now take in \( \mathfrak{m} \) the basis consisting of the vectors \( y_\alpha \) and \( z_\alpha \) defined in (21.8.3), for \( \alpha \in S^+ \). Relative to this basis, \( \text{Ad}(t^{-1})|\mathfrak{m} \) is defined by the formulas (21.8.3.3), with \( \exp(u) \) replaced by \( t^{-1} \). Since

\[
\begin{vmatrix}
\cos \theta - 1 & \sin \theta \\
-\sin \theta & \cos \theta - 1
\end{vmatrix} = 2(1 - \cos \theta) = 4 \sin^2 \frac{\theta}{2} = |e^{i\theta/2} - e^{-i\theta/2}|^2,
\]

it follows from the formula (21.14.12.1) that we have

\[
(21.15.3.4) \quad \Theta(\pi(e), \exp(u)) = |\Lambda(-u)|^2 = |\Lambda(u)|^2.
\]

This shows in the first place that the restriction of \( f \) to \((G/T) \times T_{\text{reg}} \) is a local diffeomorphism onto \( V \) that preserves the orientation, when \((G/T) \times T \) and \( G \) are oriented by the forms \( v_{G/T} \wedge v_T \) and \( v_G \), respectively. Secondly, we deduce Weyl's integration formula:

\[
(21.15.4) \quad \text{Considering the function } |\Lambda|^2 = \prod_{\alpha \in S^+} |e^\alpha - 1|^2 \text{ as a function on } T
\]

(21.13.6), for each continuous complex-valued function \( g \) on \( G \) we have

\[
(21.15.4.1) \quad \int_G g(s) \, dm_G(s) = (\text{Card}(W))^{-1} \int_{G/T} \int_T g(f(x, t)) |\Lambda(t)|^2 \, dm_{G/T}(x) \, dm_T(t),
\]
and if g is a central function (21.2.2)

\[ \int_G g(s) \, dm_G(s) = (\text{Card}(W))^{-1} \int_T g(t) |\Delta(t)|^2 \, dm_T(t). \]  

Apply the formula of successive integrations (16.24.8.1) with \((G/T) \times T_{\text{reg}}\) in place of \(X\), \(V\) in place of \(Y\), the restriction to \(V\) of the \((2n+1)\)-form \(\nu_G\) in place of \(\zeta\), and the inverse image \((g \circ f) \cdot f'(v_G)\) of this restriction in place of \(\nu\). Each of the fibers \(f^{-1}(y)\) is a finite set of cardinality \(\text{Card}(W)\) (21.15.2), and at each point \((x, t)\) of this fiber, \(\nu/\zeta(y)\) is the number 1 by virtue of (16.21.9.2); hence we have

\[ \int_V g(s) \, dm_G(s) = (\text{Card}(W))^{-1} \int_{G/T} \int_{T_{\text{reg}}} g(f(x, t)) |\Delta(t)|^2 \, dm_G/T(x) \, dm_T(t). \]

But since the complement of \(V\) in \(G\) and the complement of \((G/T) \times T_{\text{reg}}\) in \((G/T) \times T\) are negligible (21.15.2), we may replace \(V\) by \(G\) and \(T_{\text{reg}}\) by \(T\) in this formula, which gives (21.15.4.1). In particular, putting \(g = 1\) and remembering that \(m,\) is normalized, we obtain

\[ 1 = (\text{Card}(W))^{-1} m_{G/T}(G/T) \int_{T_{\text{reg}}} |\Delta(t)|^2 \, dm_T(t). \]

Since \(\Delta = J(e^\delta) = e^\delta \sum_{w \in \mathcal{W}} \det(w) e^{w \cdot \delta - \delta} \) on \(t\), and since the \(w \cdot \delta - \delta\) are pairwise distinct weights in \(P = 2\pi i \Gamma_{\text{reg}}\), it follows from the orthogonality relations for characters (21.3.2.4) applied to \(T\) that

\[ \int_T |\Delta(t)|^2 \, dm_T(t) = \text{Card}(W) \]

and consequently that \(m_{G/T}(G/T) = 1\) (cf. (22.3.7.4)). If now \(g\) is a central function, we have \(g(f(x, t)) = g(t)\) for all \(x \in G/T\), and the formula (21.15.4.2) follows from (21.15.4.1) applied to \(g\), together with the above evaluation of \(m_{G/T}(G/T)\) and the Lebesgue–Fubini theorem.

We can now describe completely the characters of a compact connected Lie group \(G\) in terms of the weight lattice \(P = P(G)\) and the half-sum \(\delta\) of the positive roots:

(21.15.5) (Weyl's theorem) The mapping that sends each character \(\chi_p\) of \(G\) to its restriction \(\chi_p|T\) is a bijection onto the set of elements \(J(e^{p+\delta})/J(e^\delta)\) of \(\mathbb{Z}[P]^\mathcal{W}\), where \(p\) runs through the set \(P(G) \cap \mathcal{C}\), and each of the weights \(p \in P(G) \cap \mathcal{C}\) has multiplicity 1 in the character \(\chi_p\) to which it corresponds. The canonical mapping \(\mathbb{Z}[\mathbb{R}(G)] \rightarrow \mathbb{Z}[P]^\mathcal{W}\) is a ring isomorphism.
For each weight \( p \in \mathcal{P} \), let \( g_p \) denote the unique continuous central function on \( G \) whose restriction to \( T \) is \( J(e^{p+\delta})/J(e^\delta) \). Then the \( g_p \) form an orthonormal system in \( L^2(G, m_G) \). For since \( \Delta = J(e^\delta) \), it follows from Weyl's integration formula (21.15.4.2) that

\[
(21.15.5.1) \quad \int_G g_p \overline{g_q} \, dm_G = (\text{Card}(W))^{-1} \int_T \left( e^{-\delta} J(e^{p+\delta}) (e^{\delta} J(e^{p+\delta})) \right) dm_T.
\]

As \( w \) runs through \( W \), the weights \( w \cdot (p + \delta) - \delta \) are all distinct (21.14.5), and if \( p \neq q \) and \( q \in \mathcal{P} \), all the weights \( w \cdot (q + \delta) - \delta \) are distinct from the weights \( w \cdot (p + \delta) - \delta \) (21.14.7). By virtue of the orthogonality relations for the characters of \( T \) (21.3.2.4), the right-hand side of (21.15.5.1) therefore vanishes if \( p \neq q \). Furthermore, when \( q = p \), since \( e^{-\delta} J(e^{p+\delta}) \) is a linear combination of \( \text{Card}(W) \) characters of \( T \) with coefficients \( \pm 1 \), the right-hand side of (21.15.5.1) is equal to 1.

This being so, it follows from (21.14.13(iii)) and (21.13.6) that we may write

\[
\chi_p \big|_T = \sum_{p \in \mathcal{P} \cap \mathcal{C}} n(p) J(e^{p+\delta})/J(e^\delta),
\]

where the \( n(p) \) are integers \( \geq 0 \); by (21.13.5), this implies that \( \chi_p = \sum_{p \in \mathcal{P} \cap \mathcal{C}} n(p) g_p \). Since \( \int_G |\chi_p|^2 \, dm_G = 1 \) (21.3.2.4), it follows therefore from the orthonormality of the \( g_p \) that \( \sum_{p \in \mathcal{P} \cap \mathcal{C}} (n(p))^2 = 1 \), and hence we have \( n(p) = 0 \) except for one weight \( p_0 \in \mathcal{P} \cap \mathcal{C} \), for which \( n(p_0) = 1 \). Consequently \( \chi_p = g_{p_0} \), and the weight \( p_0 \) occurs with multiplicity 1 in the character \( \chi_p \), because \( e^{p_0} \) occurs with coefficient 1 in \( J(e^{p_0+\delta})/J(e^\delta) \) (21.14.13(iii)).

In view of (21.14.13(iii)), the proof will be complete if we show that each \( g_p \) is a character of \( G \). If it were not so, there would exist a weight \( p_0 \in \mathcal{P} \cap \mathcal{C} \) such that \( g_{p_0} \) were orthogonal to all the characters of \( G \), by the previous part of the proof. Since \( g_{p_0} \neq 0 \), this would contradict the fact that the characters of \( G \) form a Hilbert basis of the center of \( L^2(G, m_G) \) (21.3.2).

A class of irreducible representations \( \rho \in \mathcal{R}(G) \) is therefore determined by the highest weight \( p \in \mathcal{P}(G) \) contained in \( \chi_p \). This weight \( p \) is called the dominant weight of the class \( \rho \) (or of any representation in this class), relative to the chosen basis \( \mathcal{B} \) of \( \mathfrak{S} \). Every weight \( p \in \mathcal{P} \cap \mathcal{C} \) is therefore the dominant weight of a unique class \( \rho \in \mathcal{R}(G) \). Moreover, we have

\[
(21.15.5.2) \quad \text{If } p \text{ is the dominant weight of } \rho, \text{ the other weights contained in } \chi_p \text{ are all of the form } p - \sum_j n_j \beta_j, \text{ where the } n_j \text{ are integers } \geq 0.
\]
If \( \chi_\rho | T = \sum_{q \in P} n(q)e^q \), we have

\[
(21.15.5.3) \quad e^{-J(e^q)} \cdot \sum_{q \in P} n(q)e^{-q} = e^{-(p+\delta)}J(e^{p+\delta}).
\]

Since \( e^{-J(e^q)} \) is a polynomial in the \( e^{-\beta_j} \) (21.14.12.2), it is enough to show that \( e^{-(p+\delta)}J(e^{p+\delta}) \) is also a polynomial in the \( e^{-\beta_j} \), for it will then follow from (21.15.5.3) that if \( n(q) \neq 0 \) we must have \( q - p = \sum z_j\beta_j \) with coefficients \( z_j \in \mathbb{Z} \), and since we know that \( q \leq p \), the \( z_j \) must all be \( \leq 0 \). From the definition of \( J(e^{p+\delta}) \), it is enough to verify that for all \( r \in P \cap \mathbb{C} \) and all \( w \in W \), the weight \( r - w \cdot r \) is a linear combination of the \( \beta_j \) with coefficients that are integers \( \geq 0 \). But this result is precisely (21.14.6.2), since the numbers \( r(h_j) \) are integers \( \geq 0 \).

(21.15.5.4) For \( p \in \mathfrak{t}^* \) we have \( h \cdot p = p \) for all \( w \in W \), hence \( J(e^{p+\delta})/J(e^q) = e^n \). These are the only weights \( p \in P(G) \) such that the character \( e^p \) of \( T \) is the restriction of a character of \( G \). For if \( p \) is such that \( h \cdot p = p \) for all \( w \in W \), then \( p \) must be orthogonal to all elements \( w \cdot u - u \in \mathfrak{t} \), for all \( u \in \mathfrak{t} \) and all \( w \in W \); but these elements span \( \mathfrak{t}^* \) because \( s_a \cdot h_x = -h_x \), and therefore we must have \( p \in \mathfrak{t}^* \).

(21.15.5.5) Let \( \rho', \rho'' \) be two classes of irreducible representations in \( R(G) \), with dominant weights \( p', p'' \), respectively. Since \( e^{p'} \) (resp. \( e^{p''} \)) is the leading term in \( \chi_{\rho'} | T \) (resp. \( \chi_{\rho''} | T \)), it follows that \( e^{p'+\delta} \) is the leading term in the restriction to \( T \) of the product \( \chi_{\rho'} \chi_{\rho''} \). If \( \rho \) is the class of irreducible representations with dominant weight \( p' + p'' \), it follows therefore that \( \rho \) is contained in \( \rho' \rho'' \) with multiplicity 1, and that every other class \( \rho_1 \in R(G) \) contained in \( \rho' \rho'' \) corresponds to a dominant weight \( \prec p' + p'' \).

(21.15.6) The dimension of the representations in the class \( \rho \in R(G) \) with dominant weight \( p \in P \cap \mathbb{C} \) is given by the formula (Weyl's dimension formula)

\[
(21.15.6.1) \quad n_\rho = \prod_{\alpha \in \mathfrak{a}^+} (p + \delta | \alpha) / \prod_{\alpha \in \mathfrak{a}^+} (\delta | \alpha) = \prod_{\alpha \in \mathfrak{a}^+} \langle p + \delta, h_\alpha \rangle / \prod_{\alpha \in \mathfrak{a}^+} \langle \delta, h_\alpha \rangle
\]

(where \( \langle \lambda | \mu \rangle \) is a \( W \)-invariant scalar product on \( \mathfrak{t}^* \)).

The problem here is to calculate the value of the character \( \chi_\rho \) at the identity element of \( G \) (21.3.2.8), i.e., to calculate the value of \( J(e^{p+\delta})/J(e^q) \) at
the identity element of $T$ (21.15.5), or equivalently at the point $0 \in t$, by considering the elements of $Z[P]$ as functions defined on $t$. We shall calculate

$$
J(e^{P+\delta})/J(e^\delta)
$$

at a point of the form $t_{i\alpha}$, where $\alpha$ is the element of $i$ defined by the relation $\lambda(\alpha) = (\lambda | \delta)$ for all $\lambda \in \mathfrak{t}^*$, and $\xi$ is a nonzero real number; and then we shall take the limit of this as $\xi \to 0$. Now, for each linear form $q \in Z$, the value of $J(\xi)$ at the point $t_{i\alpha}$ is by definition

$$
\det(w)e^{i\xi(q|\alpha)/2},
$$

i.e., it is the value of $\Delta = J(e^\delta)$ at the point $\xi\mathfrak{h}_q \in t$, where $\mathfrak{h}_q$ is the element of $i$ defined by the relation $\lambda(\mathfrak{h}_q) = (\lambda | \delta)$ for all $\lambda \in \mathfrak{t}^*$. From the formula (21.14.12.1) for $A$, we therefore have

$$
\Delta(\xi\mathfrak{h}_q) = \prod_{\alpha \in \Phi^+} (e^{i\xi(q|\alpha)/2} - e^{-i\xi(q|\alpha)/2}),
$$

a function of $\xi$ whose principal part, as $\xi \to 0$, is

$$
(i\xi(q|\alpha)).
$$

The formula (21.15.6.1) now follows immediately.

PROBLEMS

1. Let $G$ be a compact connected group, and let $P$ be the weight lattice of $G$ (relative to a maximal torus $T$), $\Phi \subset P$ the root system of $G$ relative to $T$, and $W$ the Weyl group of $G$. Let $V$ be an irreducible representation of $G$, and let $\mathfrak{p}$ be a weight of $V$.

(a) Let $\alpha \in \Phi$, and let $I$ be the set of integers $t \in \mathbb{Z}$ such that $\mathfrak{p} + t\alpha$ is a weight of $V$; let $n(\mathfrak{p} + t\alpha)$ be the multiplicity of this weight in $V$. Let $b$ (resp. $-a$) be the largest (resp. smallest) element of $I$. Prove that $I = [-a, b]$ and that $a - b = \mathfrak{p}(\mathfrak{h},)$. (Consider the restriction of $V$ to the subgroup $K$ of $G$ (21.8.5) and use (21.9.3))

(b) Show that for each integer $u \in [0, a + b]$ we have

$$
\mathfrak{p}(\mathfrak{p} + (b - u)\alpha) = \mathfrak{p} - (a - u)\alpha,
$$

and hence that the weights $\mathfrak{p} + (b - u)\alpha, \mathfrak{p} - (a - u)\alpha$ have the same multiplicity in $V$.

(c) Show that the function $t \mapsto n(\mathfrak{p} + t\alpha)$ is increasing in the interval $[-a, b]$ and decreasing in the interval $[b - a, b]$. (Use (21.9.3).)

(d) A subset $X$ of $P$ is said to be $\Phi$-saturated if, for each $\mathfrak{p} \in X$ and each root $\alpha \in \Phi$, we have $\mathfrak{p} + t\alpha \in X$ for all integers $t$ lying between $0$ and $\mathfrak{p}(\mathfrak{h},)$ inclusive. Show that every $\Phi$-saturated subset of $P$ is stable under the Weyl group. For each integer $d \geq 1$, the set of weights $\mathfrak{p}$ of $V$ with multiplicity $n(\mathfrak{p}) \geq d$ is $\Phi$-saturated. (Use (c).)

2. With the notation of Problem 1, let $E$ be the complex vector space of the representation $V$. Then $E$ is a simple $U(g_{(\mathfrak{c})})$-module (21.9.1), hence is generated by any $v \neq 0 \in V$.

(a) For each weight $\mathfrak{p}$ of $V$, let $E_\mathfrak{p}$ be the set of vectors $v \in E$ such that $h \cdot v = \mathfrak{p}(h)v$ for all $h \in i$; then $E$ is the direct sum of the $E_\mathfrak{p}$ as $\mathfrak{p}$ runs through the set of weights of $V$. Show that for each root $\alpha \in \Phi$, either $\mathfrak{p} + \alpha$ is not a weight of $V$, in which case $x_\alpha \cdot E_\mathfrak{p} = \{0\}$, or else $x_\alpha \cdot E_\mathfrak{p} \subset E_{\mathfrak{p} + \alpha}$.

(b) Let $B$ be a basis of $\Phi$, and let $\alpha_1, \ldots, \alpha_n$ be the positive roots in $\Phi$ relative to this basis. Let $\mathfrak{p}$ be a weight of $V$ such that none of the weights $\mathfrak{p} + \alpha_j (1 \leq j \leq n)$ is a weight of $V$. Then every weight of $V$ is of the form $\mathfrak{p} = p - m_1\alpha_1 - \cdots - m_n\alpha_n$, where the $m_j$ are integers $\geq 0$, and $\mathfrak{p}$ is the dominant weight of $V$. (If $v \neq 0$ is a vector in $E_\mathfrak{p}$, remark that $v$ generates $E$ as $U(g_{(\mathfrak{c})})$-module, and use the basis (21.16.3.4) of $U(g_{(\mathfrak{c})})$.)
3. The notation is the same as in Problems 1 and 2. Let \( Y \) be a subset of \( P \); an element \( p \in Y \)
is said to be \( S \)-extremal in \( Y \) if, for each root \( \alpha \in S \), we have either \( p + \alpha \notin Y \) or \( p - \alpha \notin Y \).

(a) Let \( p \) be the dominant weight of \( V \), and let \( X \) be the set of weights of \( V \). Show that the
\( S \)-extremal elements of \( X \) are the transforms \( w \cdot p \) of \( p \) under the Weyl group. (Let \( q \) be an
\( S \)-extremal element of \( X \); without loss of generality, we may assume that \( q \in P \cap \mathbb{C} \). If \( \alpha \) is
a positive root, show that in the notation of Problem 1 we must have \( b = 0 \), and then use
Problem 2.)

(b) Show that \( X \) is the smallest \( S \)-saturated subset of \( P \) that contains \( p \). (If \( X' \) is this set,
we have \( X' \subseteq X \) by virtue of Problem 1(d). Assume that \( X \neq X' \), and choose in \( X - X' \) a
maximal element \( q \) (relative to the ordering defined by \( B \)). Then there exists a positive root
\( \alpha \) such that \( q + \alpha \in X \); deduce that, in the notation of Problem 1, we have \( q + b\alpha \in X' \), and
hence (by using the definition of a saturated subset and Problem 1) that \( q \in X' \), which is a
contradiction.)

4. With the same notation, show that for each weight \( q \) of \( V \) other than the dominant weight
\( p \), we have \( (q | q) \leq (p | p) \) and \( (q + \delta | q + \delta) < (p + \delta | p + \delta) \). (Reduce to the case where
\( q \in P \cap \mathbb{C} \), and use (21.14.6).)

5. With the same notation, show that there exists a weight in \( X \) that is the smallest element of
\( X \) relative to the ordering defined by \( B \), and that this smallest weight has multiplicity 1.
(Observe that there exists an element \( w_0 \) in the Weyl group that transforms \( B \) into \(-B \).)

6. With the same notation, show that for each finite nonempty \( S \)-saturated subset \( X \) of \( P \),
there exists a linear representation \( V \) of \( G \) such that \( X \) is the union of the sets of weights of
the irreducible components of \( V \). (For each \( p \in X \) consider the weight \( w \cdot p \) that lies in
\( P \cap \mathbb{C} \) (21.14.7) and the irreducible representation with dominant weight \( w \cdot p \).)

7. (a) With the same notation, let \( p \in P \) and let \( X \) be the smallest \( S \)-saturated subset of \( P \)
containing \( p \). Prove that the following conditions are equivalent:

\begin{align*}
(\alpha) & \quad X = W \cdot p. \\
(\beta) & \quad (q | q) = (p | p) \quad \text{for all} \quad q \in X. \\
(\gamma) & \quad \text{For all roots} \quad \alpha \in S \quad \text{and all integers} \quad t \quad \text{between 0 and} \quad p(h_\alpha) \quad \text{inclusive, we have} \\
& \quad (p - t\alpha | p - t\alpha) \geq (p | p). \\
(\delta) & \quad \text{For all roots} \quad \alpha \in S \quad \text{and} \quad p(h_\alpha) \quad \text{is equal to} \quad 0, \quad 1, \quad \text{or} \quad -1.
\end{align*}

(To show that \( (\gamma) \) implies \( (\delta) \), observe that \( (p - p(h_\alpha)\alpha | p - p(h_\alpha)\alpha) = (p | p) \) and that the
Euclidean ball is strictly convex. To show that \( (\delta) \) implies \( (\alpha) \), observe that for each \( w \in W \),
\( (w \cdot p)(h_\alpha) \) is also equal to \( 0, \quad 1, \quad \text{or} \quad -1, \) and deduce that for each integer \( t \) lying between 0
and \( (w \cdot p)(h_\alpha) \) inclusive, \( w \cdot p - t\alpha \) is equal to either \( w \cdot p \) or \((s_\alpha w) \cdot p \).
Deduce that every nonempty \( S \)-saturated subset \( Y \) of \( P \) contains an element \( p \) satisfying
these conditions.

(b) Let \( U \) be an irreducible representation of \( G \), let \( E \) be the representation space of \( U \),
and let \( p \) be the dominant weight of \( U \). Show that the following conditions are equivalent:

\begin{align*}
(\alpha) & \quad p \quad \text{satisfies the equivalent conditions of} \quad (\alpha) \quad \text{above.} \\
(\beta) & \quad \text{All the weights of} \quad U \quad \text{are of the form} \quad w \cdot p \quad \text{for some} \quad w \in W. \\
(\gamma) & \quad \text{For each root} \quad \alpha \in S \quad \text{and each} \quad v \in E, \quad \text{we have} \quad (x_\alpha)^2 \cdot v = 0.
\end{align*}

(To show that \( (\alpha) \) and \( (\beta) \) are equivalent, use Problem 3(b). To show that \( (\alpha) \) implies \( (\gamma) \),
use Problem 2(a). To show that if there exists \( \alpha \in S \) such that \( p(h_\alpha) \geq 2 \) we cannot have
(x_j^2) \cdot v = 0 \text{ for all } v \in \mathfrak{e}, \text{ consider the restriction of } U \text{ to the subgroup } K_\lambda \text{ of } G \text{ (21.8.5) and use (21.9.3).}

8. (a) On the model of the algebra of formal power series (A.21), show that it is possible to define a $\mathbb{Z}$-algebra $\mathbb{Z}[[P^-]]$ whose elements are "formal sums" $\sum_{\mu \in \mathfrak{t}^*} c_\lambda e^\lambda$ (where $\lambda \in \mathfrak{t}^*$), the multiplication being defined by

$$\left( \sum_{p \in \lambda} c_p e^p \right) \left( \sum_{p \in \mu} c_p' e^p \right) = \sum_{p + r = p} \left( \sum_{q + r = p} c_q c'_r \right) e^p.$$  

With the notation of Problem 2(b), for each weight $\rho \in P$ let $v(\rho)$ denote the number of systems of integers $(m_1, \ldots, m_n) \in \mathbb{N}^n$ such that $\rho = m_1 \alpha_1 + \cdots + m_n \alpha_n$ (so that $v(\rho)$ is the "number of partitions of $\rho$ into positive roots"). To say that $v(\rho) > 0$ means that $\rho$ is a linear combination of positive roots with coefficients that are integers $\geq 0$. Then we have

$$\frac{1}{\prod_{\rho \in P} (1 - e^{-\rho})} = \sum_{\rho \in P} v(\rho) e^{-\rho}$$  

in the ring $\mathbb{Z}[[P^-]]$.

(b) For each weight $\rho \in P \cap \mathcal{C}$, show that the multiplicity $n_\rho(q)$ of a weight $q$ in the irreducible representation with dominant weight $\rho$ is given by the formula

$$(1) \quad n_\rho(q) = \sum_{w \in W} \det(w) \cdot v(w \cdot (\rho + \delta) - (q + \delta)).$$

(Use (a) above and Weyl's theorem.)

(c) Deduce from (b) that for each weight $q \neq \rho$ of the representation with dominant weight $\rho$ we have

$$n_\rho(q) = - \sum_{w \in W, w \neq 1} \det(w) \cdot n_\rho(q + \delta - w \cdot \delta).$$

(Use the formula (1) with $\rho = 0$.)

(d) Let $\rho_p$ be the class of irreducible representations of $G$ with dominant weight $\rho \in P \cap \mathcal{C}$. Show that the formula (21.4.7.1) can be written explicitly as

$$(2) \quad c(p, q, r) = \sum_{w \in W, w' \in W} \det(ww') \cdot v(w \cdot (\rho + \delta) + w' \cdot (q + \delta) - (r + 2\delta)).$$

(Observe that by virtue of (21.4.6.2) we have

$$(3) \quad \sum_{r \in P \cap \mathcal{C}} c(p, q, r) e^{r+\delta} = \left( \sum_{s \in P} n_s(s) e^s \right) e^{(r+\delta)}$$

and note that for $r \in P \cap \mathcal{C}$, $w \cdot (r + \delta)$ does not belong to $P \cap \mathcal{C}$; consequently $c(p, q, r)$ is equal to the coefficient of $e^{r+\delta}$ in the right-hand side of (3).)
9. With the notation of Section 21.15, take as scalar product \((\lambda, \mu)\) on \(iR^*\) the canonical scalar product (Section 21.11, Problem 11). Show that if the representations of the class \(\rho \in R(G)\) have dominant weight \(\rho \in P \cap C\) and dimension \(n_\rho\) (given by (21.15.6.1)), then

\[
\sum_q (q, \delta)^2 = \frac{1}{2} n_\rho (p + \delta | p + \delta) - (\delta | \delta)
\]

where the sum on the left-hand side is over all the weights \(q\) of \(\rho\), counted according to their multiplicities. (Expand the right-hand side of (21.15.6.2) and \(\chi_\rho(z|\mathbf{h}_\rho)\) as far as terms in \(z^3\).

10. Let \(G\) be an almost simple compact connected Lie group.

(a) With the notation of Section 21.14, let \(B\) be a basis of \(S\). Show that for the ordering defined by \(B\) there exists a highest root \(\mu = n_1 \beta_1 + \cdots + n_k \beta_k\), such that for each other root \(\alpha = p_1 \beta_1 + \cdots + p_k \beta_k\) in \(S\), we have \(p_1 \leq n_1 \leq 1 \leq p_2 \leq n_2 \leq \cdots \leq l \leq n_l\). (Observe that the adjoint representation of \(G\) on \(\mathfrak{g}_{C_1}\) is irreducible, and consider its dominant weight.) The root \(\mu\) lies in \(C\), the Weyl chamber relative to \(B\), and we have \(\langle a | \alpha \rangle \leq \langle \mu | \mu \rangle\) for all roots \(a \in S\). Also, for each root \(\alpha > 0\) other than \(\mu\), the Cartan integer \(n(a, \mu)\) is equal to 0 or 1 (use Section 21.11, Problem 1).

(b) Let \(h_0\) be the half-sum of the \(h_\alpha\) in \(S\) for all positive roots \(\alpha\). For each root \(\alpha = p_1 \beta_1 + \cdots + p_k \beta_k\), we have \(\alpha(h_0) = p_1 + p_2 + \cdots + p_l\). (Use (21.15.5.5) and (21.15.7).)

(c) If \(\mu = n_1 \beta_1 + \cdots + n_k \beta_k\) is the highest root (relative to \(B\)), show that

\[
n_1 + \cdots + n_l = h - 1,
\]

where \(h\) is the Coxeter number. (Use Section 21.11, Problem 16(e), and observe that \(n(a, \mu)^2 = n(a, \mu)\) for all roots \(a > 0\).

11. Let \(G\) be an almost simple compact connected Lie group, and retain the notation of Problem 10. For each \(a \in S\) and \(k \in Z\), let \(u_{a,k}\) denote the affine hyperplane \(a^{-1}(2\pi k)\) in it. Also let \(p_1, \ldots, p_l\) be the basis of it dual to the basis \(B = \{ \beta_1, \ldots, \beta_k \}\) of \(R^*\), so that \(\beta_j(p_i) = \delta_{ij}\) (Kronecker delta). Then the element \(h_0 \in S\) (Problem 10) is equal to \(p_1 + \cdots + p_l\) (cf. (21.16.5.2)).

The Weyl group \(W\), considered as a group of automorphisms of the vector space \(iR^*\), is generated by the reflections \(s_x : u \mapsto u - x(u)h_\alpha\) (21.8.7), where \(\alpha \in S\).

(a) The group \(W_\alpha\) generated by the orthogonal reflections in the affine hyperplanes \(u_{a,k}\) is called the affine Weyl group. Show that \(W_\alpha\) is the semidirect product of \(W\) by the group \(P_0\), generated by the translations \(u \mapsto u + 2\pi h_\alpha\), \(\alpha \in S\) (or, equivalently, by the translations \(u \mapsto u + 2\pi h_{j} , 1 \leq j \leq l\)). (Observe that the translation \(u \mapsto u + 2\pi h_\alpha\) is the product of the reflections in the hyperplanes \(u_{a,0}\) and \(u_{a,1}\), and that \(W\) leaves invariant the root system \(S^*\) formed by the \(h_\alpha\).) The group \(W_\alpha\) leaves globally invariant the union of the hyperplanes \(u_{a,k}\).

(b) The set \(C^*\) of vectors \(u \in S^*\) such that \(\beta_j(u) > 0\) for \(1 \leq j \leq l\) is called the Weyl chamber of \(S^*\) (relative to the basis \(B\)), and the set \(A^*\) of vectors \(u \in C^*\) such that \(\mu(u) < 2\pi\), where \(\mu\) is the highest root of \(S\) relative to \(B\) (Problem 10) is called the principal alcove of \(C^*\). Show that \(A^*\) intersects none of the hyperplanes \(u_{a,k}\). The set \(A^*\) is the interior of the simplex constructed on the vectors \(2\pi p_i/n_i\) (1 \(\leq j \leq l\) (14.3.10).

(c) Show that if an element of \(W_\alpha\) fixes a vector \(x\) not lying in any of the hyperplanes \(u_{a,k}\), then it is the identity element of \(W_\alpha\). (The element of \(W_\alpha\) in question is the product of an element \(w \in W\) by a translation \(u \mapsto u + h\) of \(P_0\), and must satisfy \(w \cdot x = x + h\); deduce that \(\exp(iw \cdot x) = \exp(ix)\) and use (21.7.14).)
(d) Deduce from (c) that the only element of $W_\epsilon$ that leaves $A^*$ globally invariant is the identity. (Remark that the subgroup $W_\epsilon$ of $W_\epsilon$ leaving $A^*$ globally invariant is finite, and consider the barycenter of the transforms under $W_\epsilon$ of a vector in $A^*$.)

(e) The connected components of the complement in it of the union $iD(G)$ (Section 21.10, Problem 2) of the hyperplanes $u_{\lambda, k}$ are called the alcoves of $S$. Show that each alcove is of the form $v(A^*)$ for a unique element $v \in W_\epsilon$. (The uniqueness follows from (d) above. To prove the existence of $v$, take a point $x$ in an alcove and a point $a \in A^*$; consider the point $y$ of the $W_\epsilon$-orbit of $x$ that is nearest to $a$, and show that $y \in A^*$. To do this, show that $y$ and $a$ lie on the same side of each of the "walls" of $A^*$, i.e., the $l + 1$ hyperplanes $u_{\beta_j, 0}$ and $u_{\beta_i, 1}$.)

(f) Show that each point of $G$ is conjugate to a point of the form $\exp_i(u)$, where $u \in A^*$. (Observe that $\exp(2\pi i\alpha)$ is $e$ for all roots $\alpha$, and use (e) above and (21.8.7).)

(g) Show that, for $1 \leq j \leq l$, the points of the form $2\pi i\mathbf{p}_j$ with $0 \leq t \leq 1$ that belong to $iD(G)$ are the points $2\pi i\mathbf{p}_j/m$, where $1 \leq m \leq n_j$. (Use Section 21.11, Problem 3(c).)

12. We retain the hypotheses and notation of Problem 11, and the notation of (21.10.6). Suppose that the vectors $x_\gamma$, together with a basis of it, from a Weyl basis of $g_{(C)}$ (21.10.6). Consider the vector $h_\gamma \in it$, and take an element in $g$ of the form

$$z = \sum_{j=1}^{l}(z_j x_{\beta_j} - z_j x_{-\beta_j})$$

with $z_j \in \mathbb{C}$ ($1 \leq j \leq l$).

(a) Show that if we put

$$z' = \sum_{j=1}^{l}(i(z_j x_{\beta_j} + z_j x_{-\beta_j}),$$

which belongs to $g$, then we have

$$[ih_\gamma, z] = z', \quad [ih_\gamma, z'] = -z,$$

and

$$[z, z'] = 2i \sum_{j=1}^{l} z_j x_{\beta_j} h_{\beta_j}.$$

(Use the fact that $\beta_j - \beta_i$ is not a root.) Show that we may choose the coefficients $z_j \neq 0$ so that $[z, z'] = 2ih_\gamma$. The vectors $ih_\gamma$, $z$, and $z'$ then generate a three-dimensional Lie subalgebra $t_0$ of $g$, which is the Lie algebra of an almost simple compact subgroup $K_0$ of $G$.

(b) Show that $K_0$ is a principal nice subgroup of $G$, of rank 1. (If $G'$ is a connected closed subgroup of $G$ that contains $K_0$ and $T$, and if $g'$ is its Lie algebra, observe that $g_{(C)}$ must be the direct sum of $h = t_{(C)}$ and a certain number of subspaces $g_\alpha$, and that the sum of these $g_\alpha$ must contain $z$ and $z'$; note also that the $g_{\beta_j}$ and $g_{-\beta_i}$ must occur among these $g_\alpha$, because the $x_j$ are $\neq 0$.)

(c) Show that a nice subgroup of $G$ of rank 1 that contains a regular element of $G$ is necessarily conjugate to the group $K_0$ (use Problems 8 and 12 of Section 21.11). Such a subgroup is called miniprincipal.

(d) Let $G_1$ be a connected closed subgroup of $G$. Show that for $G_1$ to be a principal nice subgroup of $G$, it is necessary and sufficient that $G_1$ contain a miniprincipal subgroup $K_0$ of $G$ (To show that the condition is necessary, consider a miniprincipal subgroup $K_0$ of $G_1$, and use Section 21.11, Problem 8 to show that a principal diagonal of $K_0$ is a principal
13. Let $G$ be an almost simple compact connected Lie group. With the notation of Problem 11, if $\sigma$ is a Coxeter element in the Weyl group $W$ (Section 21.11, Problem 14), there exists an element $s \in \mathcal{A}(T)$ such that the restriction of $\text{Ad}(s) \otimes 1_G$ to $t_G$ is equal to that of the contragradient $\tau^{-1}$ of $\sigma$. For each root $\alpha \in S$, $\text{Ad}(s) \otimes 1_G$ transforms $g_\alpha$ into $g_{\alpha^*}$. Deduce that the eigenvalues of this transformation on the stable subspace $\sum g_\alpha$ are $h$th roots of unity, each occurring with multiplicity $l$ (Section 21.11, Problem 16(d)); the eigenvalues of $\text{Ad}(s) \otimes 1_G$ on $t_G$ are the complex numbers $\exp(2\pi i j/h)$ (Section 21.11, Problem 14(c)).

The element $s$ is called a Coxeter element of $G$ (relative to $T$). Show that any two such elements are conjugate in $G$. (Use the fact that $1$ is not an eigenvalue of $\sigma$)

14. Let $G$ be an almost simple compact connected Lie group, and retain the notation of Problem 11. Each Coxeter element of $G$ (Problem 13) is regular in $G$ and of finite order, equal to $h$. Show that each element $s \in G$ that is regular and of order $h$ is conjugate to a Coxeter element, and that no regular element $s \neq e$ in $G$ has finite order $\leq h - 1$. (We may assume that $s = \exp(iu)$, where $u$ lies in the principal alcove $A^*$ (Problem 11) in it. Use the fact that $s^h = e$ to show that $\beta_j(u) = 2\pi p_j/h$ with $p_j$ a positive integer, and $\mu(u) = 2\pi(\sum p_j n_j)/h$; then express that $\mu(u) < 2\pi$ and use Problem 10(c) to deduce that $p_j = 1$ for $1 \leq j \leq l$ and hence that $u = (2\pi/h)h_0$ (Problem 10(b)).

15. With the same hypotheses and notation as in Problem 13, let $s \in \mathcal{A}(T)$ be the Coxeter element considered there. Since $s$ is regular in $G$, it is contained in a unique maximal torus $T'$ of $G$. Let $t'$ be the Lie algebra of $T'$, let $S'$ be the corresponding root system, and let $\{\beta'_1, \ldots, \beta'_l\}$ be a basis of $S'$. If $h_0 \in S'$ is such that $\beta'_j(h_0) = 1$ for $1 \leq j \leq l$, we may assume that $s = \exp(iu')$ with $u' = (2\pi/h)h_0$ (Problem 14). For each integer $j \neq 0$, let $a_j$ denote the direct sum of the $g_{\alpha'}$ for all $\alpha' \in S'$ such that $\alpha' = p_1 \beta'_1 + \cdots + p_l \beta'_l$ with $p_1 + \cdots + p_l = j$, so that we have $a_j = \{0\}$ if $|j| \geq h$. Also put $a_0' = t_{(e)}$, so that $a_0'$ is the direct sum of the $a_j$. For all $x \in a_j$, we have $[h_0, x] = jx$.

(a) Show that

$$\dim a_j + \dim a_{j-1} = \dim a_j + \dim a_{j-1} = l + \phi(j)$$

for $0 \leq j \leq h - 1$, where $\phi(j)$ is the multiplicity of $\exp(2\pi ij/h)$ as an eigenvalue of $\sigma$ (and therefore $\phi(j) = 0$ if $j$ is not one of the $m_k$ (Section 21.11, Problem 14)). (Use Problem 13.)

(b) Let $b_j = t_{(e)} \cap (a_j + a_{j-1})$, so that $b_j$ is the eigenspace of $\sigma$ for the eigenvalue $\exp(2\pi ij/h)$, and $\dim b_j = \phi(j)$. We have $b_0 = \{0\}$, and $b_1$ contains a regular element $x$ (Section 21.11, Problems 14(b) and 16(c)). Let $g'_x$ (resp. $g'_x$) denote the direct sum of the $a_j$ with $j > 0$ (resp. $j < 0$), so that $g'_x$ is the direct sum of $g'_x$, $g'_x$, and $a_0'$. Let $\pi_+$ and $\pi_-$ denote the projections of $g'_x$ onto $g'_x$ and $g'_x$ defined by this direct sum decomposition. Then by definition we have $x = \pi_+(x) + \pi_-(x)$, $\pi_+(x) = \sum_{j \geq 0} r_j x_{j'}$ and $\pi_-(x) = r x_{-\mu}$.
where \( \{x^*_i \} \) is a basis of \( g_{+} \), and \( \mu' \) is the highest root of the system \( S' \), and \( r_{i}, r \) are complex numbers. Show that the \( r_{i} \) are all \( \neq 0 \). (Note that the centralizer of \( x \) in \( g_{+} \) is \( t_{G_{0}} \) and that \( [x_{k}], x_{-k} \] = 0 for \( k \neq 0 \), and \( [x_{-k}], x_{-k} \] = 0.) Putting \( \epsilon = \pi_{+}(x) \), deduce that there exists an element \( f \in g'_{-} \) such that \( [\epsilon, f] = h_{0}^{*}, [h_{0}^{*}, \epsilon] = \epsilon, \) and \( [h_{0}^{*}, f] = -f \).

(c) The vector subspace \( s \) of \( g_{+} \) spanned by \( \epsilon, f, \) and \( h_{0}^{*} \) is a Lie subalgebra isomorphic to \( sl(2, \mathbb{C}) \). Show that \( g_{+} \), considered as \( U(s) \)-module corresponding to the adjoint representation restricted to \( s \), is the direct sum of \( l \) simple \( U(s) \)-modules that are odd-dimensional as complex vector spaces. (Observe that all the eigenvalues of \( ad(h_{0}^{*}) \) are integers, and use (21.9.3).)

(d) Show that the mapping \( \pi_{+} \), restricted to \( t_{G_{0}} \), is injective. (Observe that \( b_{0} = 0 \) and that \( ad(x) \) is nilpotent for each \( x \in g_{+} \), whereas \( ad(u) \) is not nilpotent for \( u \neq 0 \) in \( t_{G_{0}} \)). Show that \( \pi_{+}(t_{G_{0}}) \) is contained in the kernel of \( ad(\epsilon) \). (We have \([x, u] = 0 \) for \( u \in t_{G_{0}} \); deduce that \( [\pi_{+}(x), \pi_{+}(u)] = 0 \), by writing \( x = \pi_{+}(x) + \pi_{-}(x) \) and \( u = \pi_{+}(u) + \pi_{-}(u) \).) Deduce that \( \pi_{+}(t_{G_{0}}) \) is equal to the kernel of \( ad(\epsilon) \) (use (c) above).

(e) Deduce from (d) that the image of \( g_{+}^{'}, a_{0}' \) under \( ad(\epsilon) \) is \( g_{+}^{'}, \) and hence that the image of \( a_{j}' \) under \( ad(\epsilon) \) is \( a_{j'+1}' \). Hence, by using (b) above, obtain Kostant’s formula

\[
\varphi(j) = \dim a_{j}' - \dim a_{j'+1}'
\]

for \( 0 \leq j \leq h - 1 \).

(f) Show that the \( l \) simple \( U(s) \)-modules into which \( g_{+} \) splits have dimensions \( 2m_{j} + 1 \) \((1 \leq j \leq l)\), where the \( m_{j} \) are the integers defined in Section 21.11, Problem 14(c). (Note that the kernel of \( ad(\epsilon) \) is the direct sum of the \( \pi_{+}(t_{G_{0}}) \cap a_{j}' \), and that in \( a_{j}' \) the restriction of \( ad(h_{0}^{*}) \) is multiplication by \( j \); then use (21.9.4).)

16. Let \( G \) be an almost simple compact connected Lie group, and let \( T \) be a maximal torus of \( G \). We retain the notation of Problem 11.

(a) The identity component of the centralizer \( Z(s) \) in \( G \) of an arbitrary element \( s \in G \) is conjugate to that of the centralizer of an element of the form \( exp(iu) \), where \( u \) lies in the closure of the principal alcove \( A^* \).

(b) Let \( \mathcal{F} \) be the set of connected closed proper subgroups of \( G \). The identity components of the centralizers \( Z(s) \) that are maximal elements of \( \mathcal{F} \) are the conjugates of certain of the identity components \( (Z(exp(2\pi irp)))_{0} \), where \( 1 \leq j \leq l \) and \( 0 < t < 1/n_{j} \). (Use Section 21.11, Problem 4.)

(c) If \( n_{j} = 1 \), the identity component \( G' = (Z(exp(2\pi irp)))_{0} \) is the same for all \( t \) such that \( 0 < t < 1 \), and is maximal in \( \mathcal{F} \). (Observe that if \( G' = G' \) is a connected Lie subgroup, distinct from \( G \) or \( G' \), then \( \mathcal{S}(G') \) must be equal to \( \mathcal{S}(G') \), by using Problem 10(a).) The center of \( G' \) is 1-dimensional.

(d) If \( n_{j} > 1 \) and is not a prime number, the group \( G' = (Z(exp(2\pi irp)))_{0} \) is not a maximal element of \( \mathcal{F} \), for any value of \( t \) such that \( 0 < t < 1/n_{j} \). (It is sufficient to consider the case \( t = 1/n_{j} \); the roots in \( \mathcal{S}(G') \) are the roots in \( \mathcal{S}(G) \) that are of the form \( \sum_{k=1}^{l} m_{k} \beta_{k} \), where \( m_{j} = n_{j} \) or \( m_{j} = 0 \). If \( n_{j} = ab \) where \( a, b \) are integers \( > 1 \), and if \( G'' = (Z(exp(2\pi irp)/b))_{0} \), show that \( \mathcal{S}(G'') \supset \mathcal{S}(G') \) and that \( \mathcal{S}(G'') \) contains at least one root that does not belong to \( \mathcal{S}(G') \), by using Problem 11(g).)

(e) If \( n_{j} > 1 \) and is prime, then \( G' \) is maximal in \( \mathcal{F} \). (Argue by contradiction, by supposing that \( G' \subset G' = (Z(exp(2\pi iv)))_{0} \) with \( G'' \) distinct from \( G' \) and \( G \). We should then have \( v = \sum_{k=1}^{l} a_{k} p_{k} \), where the \( a_{k} \) are integers except for \( a_{j} = q/n_{j} \), where \( q \) is not a multiple of \( n_{j} \). If \( r \) is an integer such that \( qr \equiv 1 \pmod{n_{j}} \), consider the centralizer of \( exp(2\pi irv) \) and thus obtain a contradiction.) The group \( G' \) is semisimple.

(f) Describe the maximal elements of \( \mathcal{F} \) that have rank equal to the rank of \( G \), when \( G \) is an almost simple classical group.
16. CENTER, FUNDAMENTAL GROUP, AND IRREDUCIBLE REPRESENTATIONS OF SEMISIMPLE COMPACT CONNECTED GROUPS

Throughout this section, $G$ denotes a compact connected semisimple Lie group, so that its center $Z$ is finite and is contained in all the maximal tori of $G$ (21.7.11). All other notation is the same as in Sections 21.13-21.15.

(21.16.1) The lattice $P(G/Z)$ of weights of $G/Z$ relative to $T/Z$ is the lattice $Q(g)$ generated by the roots $\alpha \in S$ (and is therefore a free $\mathbb{Z}$-module with basis any basis $B$ of $S$), and $Z$ is isomorphic to the quotient $P(G)/P(G/Z) = P(G)/Q(g)$.

Since the center of $G/Z$ consists only of the identity element (21.6.9), the adjoint representation of $G/Z$ is faithful; hence (21.13.2) every irreducible representation of $G/Z$ is contained in the tensor product of a certain number of linear representations equal to $\text{Ad} \otimes I_c$ and a certain number of linear representations equal to its conjugate. By definition, the restriction to $T$ of the character of an irreducible representation contained in $\text{Ad} \otimes I_c$ is a linear combination of characters of $T$ of the form $e^a$, where $a$ is a root (21.8.1). These remarks, coupled with (21.15.5), show that $P(G/Z) = Q(g)$.

Next, the groups $T$ and $T/Z$ have the same Lie algebra $t$, and the exponential mapping $\exp_{T/Z}$ is the composition of the canonical homomorphism $T \rightarrow T/Z$ with $\exp_T$; consequently the lattice $\Gamma_{T/Z}$ (21.7.5) is the inverse image $\exp_{T/Z}^{-1}(Z)$, and $Z$ is isomorphic to $\Gamma_{T/Z}/\Gamma_T$. The elementary theory of free $\mathbb{Z}$-modules (A.26.5) then shows that $Z$ is also isomorphic to $\Gamma_T/\Gamma_{T/Z}$, i.e. to $P(G)/P(G/Z)$.

(21.16.2) The result just proved may be applied to the universal covering group $\tilde{G}$ of $G$; if $D$ is the center of $\tilde{G}$, then $\tilde{G}/D$ is isomorphic to $G/Z$, and $\tilde{G}$ is isomorphic to $\tilde{G}/Z_G$, where $Z_G$ is a subgroup of the center $D$ of $\tilde{G}$ (16.30.4); also $Z$ is isomorphic to $D/Z_G$ (20.22.5.1). It follows that the fundamental group $\pi_1(G)$ is isomorphic to $P(\tilde{G})/P(G)$, hence to $\Gamma_T/\Gamma_{T_1}$, where $T_1$ is the maximal torus of $\tilde{G}$ that is the inverse image of $T$.

Since $\tilde{G}$ has the same Lie algebra as $G$, it follows that $P(\tilde{G})$ is contained in the lattice $P(g)$ (21.14.3). But from the fact that $\tilde{G}$ is semisimple and simply connected, it follows that $P(\tilde{G}) = P(g)$. In other words:

(21.16.3) Let $G$ be a simply connected compact semisimple group and $g$ its Lie algebra. Let $P(g)$ be the lattice of linear forms $\lambda \in \text{it}^*$ such that $\lambda(h_\alpha)$ is an integer for all $\alpha \in S$ (i.e., the lattice dual to the lattice in it having as basis the $h_j$ (21.14.2) for $1 \leq j \leq l$). Then $P(G) = P(g)$.
Let $p \neq 0$ be a linear form belonging to $P(g)$. It is enough to construct a linear representation $V$ of $G$ on a finite-dimensional complex vector space $E$, such that there exists a vector $x \neq 0$ in $E$ with the property that $V(\exp(u)) \cdot x = e^{\rho(u)x}$ for all $u \in \mathfrak{t}$ (21.13.6). Since $G$ is simply connected, it comes to the same thing (19.7.6) to define a $C$-homomorphism of Lie algebras $\rho: g(C) \to gl(E)$ such that, for all $u \in \mathfrak{h} = \mathfrak{t} \oplus \mathfrak{i}t$, we have

$$\rho(u) \cdot x = p(u)x.$$  

(21.16.3.1)

If $U$ denotes the enveloping algebra $U(g(C))$ (19.6.3), it again comes to the same thing (21.9.1) to construct a left $U$-module $E$ of finite dimension over $C$, and an element $x \neq 0$ in $E$ such that

$$\begin{equation}
(\mathfrak{u} - p(u) \cdot 1) \cdot x = 0
\end{equation}$$

(21.16.3.2) for all $u \in \mathfrak{h}$.

Since $P(G)$ and $P(g)$ are both invariant under the action of the Weyl group, we may, by replacing $p$ by $w \cdot p$ for a suitably chosen $w \in W$, assume that $p \in \mathbb{C}$, or in other words that

$$m_j = p(h_j) \geq 0 \quad (1 \leq j \leq l).$$

(21.16.3.3)

The construction of $E$ is in several steps.

(A) Arrange the positive roots (relative to $B$) in a sequence $(a_k)_{1 \leq k \leq n}$. With the notation of (21.10.3), the algebra $U$ has a basis over $C$ consisting of the elements

$$x_{a_1} \cdots x_{a_k} \cdots x_{a_n}, h_1, \cdots h_l, x_j, x_{j+1}, \cdots x_{h_n}$$

(21.16.3.4)

where the $a_k, b_k, c_j$ $(1 \leq k \leq n, 1 \leq j \leq l)$ are arbitrary integers $\geq 0$ (19.6.2). Let $U_-$ denote the vector subspace of $U$ generated by the basis elements (21.16.3.4) for which $b_k = 0$ for $1 \leq k \leq n$ and $c_j = 0$ for $1 \leq j \leq l$, and let $U_0$ denote the vector subspace generated by the basis elements (21.16.3.4) for which $a_k = 0$ for $1 \leq k \leq n$. Then the vector space $U$ may be identified with $U_- \otimes_C U_0$ (A.20.2). We remark that the elements $x_{\alpha}$ for $\alpha \in S^+$ and the $h_j$ for $1 \leq j \leq l$ form a basis of a Lie subalgebra $b$ of the complex Lie algebra $g(C)$, because if $\alpha$ and $\beta$ are any two positive roots, we have $[x_{\alpha}, x_{\beta}] = 0$ if $\alpha + \beta$ is not a root, and $[x_{\alpha}, x_{\beta}] \in g_{\alpha + \beta} \subset b$ if $\alpha + \beta$ is a root (21.10.5). The vector subspace $U_0$ of $U$ may therefore be identified with the enveloping algebra $U(b)$ (19.6.2).
Let \( \mathfrak{u} \) denote the left ideal of \( U \) generated by the elements

\[(21.16.3.5) \quad x_{-k} \quad (1 \leq k \leq n), \quad u - p(u) \cdot 1 \quad (u \in \mathfrak{h}).\]

Let \( M \) be the quotient \( U \)-module \( U/\mathfrak{u} \). We shall first show that

\[(21.16.3.6) \quad \text{The } U\text{-module } M \text{ is nonzero, and if } v \text{ is the canonical image in } M \text{ of the identity element } 1 \text{ of } U, \text{ then } M \text{ has a } C\text{-basis consisting of the elements}\]

\[(21.16.3.7) \quad x_{a_1} \cdots x_{a_n} \cdot v\]

where the exponents \( a_k \ (1 \leq k \leq n) \) are arbitrary integers \( \geq 0 \).

The elements (21.16.3.5) belong to \( U_0 \); let \( \mathfrak{u}_0 \) be the left ideal of \( U_0 \) that they generate. Clearly we have

\[(21.16.3.8) \quad \mathfrak{u} = U_\mathfrak{c} \otimes_C \mathfrak{u}_0, \quad U/\mathfrak{u} = U_\mathfrak{c} \otimes_C (U_0/\mathfrak{u}_0).\]

To prove (21.16.3.6), it is enough to show that \( U_0/\mathfrak{u}_0 \) is 1-dimensional over \( C \). Now, we may define a \( C \)-homomorphism of Lie algebras \( \theta: \mathfrak{b} \to C \) by setting \( \theta(u) = p(u) \) for \( u \in \mathfrak{h} \), and \( \theta(x_\alpha) = 0 \) for \( \alpha \in S^+ \); we have only to verify that \( \theta([u, x_\alpha]) = 0 \) for \( u \in \mathfrak{h} \) and \( \alpha \in S^+ \), and this follows from the fact that \([u, x_\alpha]\) is a scalar multiple of \( x_\alpha \). Since \( p \neq 0 \), the homomorphism \( \theta \) extends to a surjective homomorphism \( \theta: U(\mathfrak{b}) \to C \) (19.6.4), the kernel of which evidently contains \( \mathfrak{u}_0 \); but since the \( h_i \) commute with each other, every element \( h_1^{b_1} \cdots h_l^{b_l} x_{k_1}^{a_1} \cdots x_{k_l}^{a_l} \) is congruent modulo \( \mathfrak{u}_0 \) to \( p(h_1)^{b_1} \cdots p(h_l)^{b_l} x_{k_1}^{a_1} \cdots x_{k_l}^{a_l} \) (and hence to 0 unless all the integers \( b_k \) are zero), and therefore the kernel of \( \theta \) is equal to \( \mathfrak{u}_0 \), which proves our assertion.

(B) For each \( u \in \mathfrak{h} \) we have \( u x_{-a_k} - x_{-a_k} u = -\alpha_k(u) x_{-a_k} \) in the algebra \( U \), from which it follows immediately by induction on \( a_1 + \cdots + a_n \) that

\[(21.16.3.9) \quad u \cdot (x_{-a_1}^{a_1} \cdots x_{-a_n}^{a_n} \cdot v) = (p(u) - a_1 \alpha_1(u) - \cdots - a_n \alpha_n(u))(x_{-a_1}^{a_1} \cdots x_{-a_n}^{a_n} \cdot v)\]

in the module \( M \); and since we have (21.11.5)

\[(21.16.3.10) \quad \alpha_k = \sum_{j=1}^{l} d_{kj} \beta_j\]
where the $d_{kj}$ are integers $\geq 0$, we may write

\begin{equation}
\mathbf{u} \cdot (x_{-a_1}^{\alpha_1} \cdots x_{-a_n}^{\alpha_n} \cdot \mathbf{v}) = (\mathbf{p}(\mathbf{u}) - n_1 \beta_1(\mathbf{u}) - \cdots - n_l \beta_l(\mathbf{u})) (x_{-a_1}^{\alpha_1} \cdots x_{-a_n}^{\alpha_n} \cdot \mathbf{v})
\end{equation}

where

\begin{equation}
n_j = \sum_{k=1}^{n} d_{kj} a_k.
\end{equation}

For each multi-index $\mathbf{n} = (n_j) \in \mathbb{N}^l$, put

\begin{equation}
p_n = p - n_1 \beta_1 - \cdots - n_l \beta_l,
\end{equation}

so that $p_0 = p$ and $p_n < p$ (for the ordering defined in (21.14.6)) for all $\mathbf{n} \neq 0$.

Next, for each $q \in P(g)$, let $M(q)$ be the vector subspace of $M$ consisting of the vectors $\mathbf{z}$ satisfying

\begin{equation}
\mathbf{u} \cdot \mathbf{z} = q(\mathbf{u}) \mathbf{z}
\end{equation}

for all $\mathbf{u} \in \mathfrak{h}$. Then:

\begin{equation}
The vector space $M$ is the direct sum of the $M(q)$ for all $q \in P(g)$ such that $q \leq p$; the subspaces $M(q)$ are finite-dimensional, and $M(p)$ is 1-dimensional. For each root $\alpha \in \mathfrak{S}$, we have $\mathbf{x}_\alpha \cdot M(q) \subset M(q + \alpha)$.
\end{equation}

The first assertion is a consequence of what has already been established; by virtue of (21.16.3.6), $M$ is the direct sum of the $M(p_n)$ for $\mathbf{n} \in \mathbb{N}^l$, and $M(q) = \{0\}$ if $q$ is not one of the forms $p_n$ (A.24.4). For each given $\mathbf{n} = (n_j) \in \mathbb{N}^l$, there is only a finite number of systems of integers $a_k \geq 0$ ($1 \leq k \leq n$) satisfying the equations (21.16.3.12), hence the subspaces $M(p_n)$ are finite-dimensional; also it is clear that the only element of the basis (21.16.3.7) that belongs to $M(p)$ is $\mathbf{v}$, and hence $M(p)$ is one-dimensional. Since $[\mathbf{u}, \mathbf{x}_\alpha] = \alpha(\mathbf{u}) \mathbf{x}_\alpha$, (21.16.3.14) implies that

\begin{equation}
\mathbf{u} \cdot (\mathbf{x}_\alpha \cdot \mathbf{z}) = \mathbf{x}_\alpha \cdot (\mathbf{u} \cdot \mathbf{z}) + [\mathbf{u}, \mathbf{x}_\alpha] \cdot \mathbf{z} = (q(\mathbf{u}) + \alpha(\mathbf{u})) (\mathbf{x}_\alpha \cdot \mathbf{z}),
\end{equation}

which completes the proof.

(C) The integers $m_j$ being those defined in (21.16.3.3), we shall now show that:
16. REPRESENTATIONS OF SEMISIMPLE COMPACT CONNECTED GROUPS

The U-submodule $N$ of $M$ generated by the $l$ elements

\[ x_{\beta_j}^{m_j} \cdot v \quad (1 \leq j \leq l) \]

does not contain $v$; moreover, for each $z \in M$ and each index $j \in [1, l]$, there exists an integer $s \geq 0$ such that $x_{-\beta_j}^s \cdot z \in N$.

We first remark that in the algebra $U$, every element $x_\alpha$ (resp. $x_{-\alpha}$) for $\alpha \in S^+$ is a linear combination of products $x_{\gamma_1}, x_{\gamma_2}, \ldots, x_{\gamma_r}$ (resp. $x_{-\gamma_1}, x_{-\gamma_2}, \ldots, x_{-\gamma_r}$), where $(\gamma_1, \ldots, \gamma_r)$ is a sequence of roots all belonging to the basis $B = \{\beta_1, \ldots, \beta_l\}$. Indeed, this is obvious if $\alpha \in B$; if not, $\alpha$ is of the form $\sum d_j \beta_j$ with each $d_j$ an integer $\geq 0$ (21.11.5), and we can proceed by induction on $\sum d_j$. By hypothesis, we have $\alpha = \lambda + \mu$, where $\lambda = \sum d_j \beta_j$ and $\mu = \sum d''_j \beta_j$ are two roots in $S^+$ with $\sum d'_j < \sum d_j$ and $\sum d''_j < \sum d_j$ (21.11.5); hence $x_\mu$, a scalar multiple of $[x_{\gamma_1}, x_{\gamma_2}, \ldots] = x_\alpha - x_\lambda x_\beta$ (21.10.5), and our assertion follows from the inductive hypothesis.

To prove the first assertion of (21.16.3.17), it will be enough to show that $N$ is contained in the sum of the subalgebras $M(q)$ with $q < p$. In view of what has already been established, and the form of the elements of the basis (21.16.3.4) of $U$, this will result from the following properties:

1. For $u \in h$ and $\alpha \in S^+$ we have

\[ u \cdot (x_\alpha^r \cdot v) = (p(u) + r\alpha(u))(x_\alpha^r \cdot v) \]

by induction on $r$, starting from (21.16.3.16).

2. For $1 \leq k \leq l$, we have $x_{\beta_k} \cdot (x_{\beta_j}^{m_j} \cdot v) = 0$. Indeed, if $k \neq j$, $\beta_k - \beta_j$ is not a root (21.11.5), hence $[x_{\beta_k}, x_{-\beta_j}] = 0$ (21.10.5): in other words, $x_{\beta_k}$ and $x_{-\beta_j}$ commute in $U$, and the assertion follows from the fact that $x_{\beta_k} \cdot v = 0$ for all $k$, by the definition of $M$. If $k = j$, we observe that (in the notation of (21.10.3)) the algebra $U(s_{\beta_j})$ is a subalgebra of $U$, and that if we apply the formulas (21.9.3.6) to the $U(s_{\beta_j})$ module generated by the element $v \in M$, we have

\[ x_{\beta_j} \cdot (x_{-\beta_j}^r \cdot v) = r(p(h_j) - r + 1)(x_{-\beta_j}^r \cdot v) \]

for all $r \geq 1$, and therefore when $r = m_j + 1 = p(h_j) + 1$ we obtain $x_{\beta_j} \cdot (x_{\beta_j}^{m_j} \cdot v) = 0$. 

(3) For $1 \leq k \leq l$ we have, by definition,
\[ x_{-\beta_k} \cdot (x_{-\beta_j}^{m_j+1} \cdot v) \in M(q) \]
where $q = p - (m_j + 1)\beta_j - \beta_k$, by virtue of (21.16.3.15).

To prove the second assertion of (21.16.3.17), we need only consider the case where
\[ z = x_{-\gamma_1} x_{-\gamma_2} \cdots x_{-\gamma_r} \cdot v \]
in which the $\gamma_k$ belong to $B$; when $r = 0$, the assertion follows from the definition of $N$, and we proceed by induction on $r$. The only positive integral values of $k$ for which $k\beta_j + \gamma_i$ can be a root are 0, 1, 2, 3 at most (21.11.11). In view of (21.10.5) we may therefore write
\[
\begin{align*}
    x_{-\beta_j}^{s+3} x_{-\gamma_1} &\quad= t_s x_{-\gamma_1} x_{-\beta_j}^{s+3} + t_s' x_{-\gamma_1 - \beta_j} x_{-\beta_j}^{s+2} \\
    &\quad+ t_s'' x_{-\gamma_1 - 2\beta_j} x_{-\beta_j}^{s+1} + t_s''' x_{-\gamma_1 - 3\beta_j} x_{-\beta_j}^{s-1}
\end{align*}
\]
for all integers $s > 0$, with scalar coefficients $t_s, t_s', t_s''$ and $x_s$ replaced by 0 if $\lambda$ is not a root. The result now follows from the inductive hypothesis.

(D) Now consider the $U$-module $E = M/N$. By virtue of (21.16.3.17), the image $\bar{v}$ of $v$ in $E$ is not zero, and satisfies the relation $u \cdot \bar{v} = p(u)\bar{v}$ for all $u \in \mathfrak{h}$. It is therefore enough to show that $E$ is finite-dimensional over $C$. Let $E_q$ denote the canonical image of $M(q)$ in $E$, for all $q \in P(g)$ such that $q \leq p$; then $E_q$ is finite-dimensional, and for each $y \in E_q$ and $u \in \mathfrak{h}$ we have $u \cdot y = q(u)y$; furthermore, $E$ is the sum of the subspaces $E_q$ (hence in fact the direct sum, cf. (A.24.4)). Hence we have to prove that $E_q = \{0\}$ for all but a finite number of values of $q \in P(g)$. This is a consequence of the following proposition:

**Proposition 21.16.3.21** If $E_q \neq \{0\}$, then also $E_{w \cdot q} \neq \{0\}$ for all elements $w$ of the Weyl group $W$.

Assume this result for a moment. For each $q \in P(g)$ such that $E_q \neq \{0\}$, there exists $w \in W$ such that $w \cdot q \in \hat{C}$ (21.14.5.1). Since $E_{w \cdot q} \neq \{0\}$, we must have $w \cdot q \leq p$ (in fact, $w \cdot q$ must be one of the $p_n$, cf. (A.24.4)). But the set of $p_n$ such that $p_n \in \hat{C}$ is finite, because they satisfy $p_n \leq p$ (21.14.8.1). Since $W$ is a finite group, it follows that the set of $q \in P(g)$ such that $E_q \neq \{0\}$ is finite, as required.

It remains therefore to prove (21.16.3.21). Let $y \neq 0$ be an element of $E_q$. It is enough to show that $E_{w \cdot q} \neq \{0\}$ for $w = s_j$ ($1 \leq j \leq l$), because $W$ is generated by the $s_j$ (21.11.8). Consider the $U(s_{\beta_j})$-submodule $F$ of $E$ gen-
erated by \( y \); we claim that it is finite-dimensional over \( \mathbb{C} \). Indeed, it is clear that the vector space \( F \) is spanned by the elements \( x_{\beta_j}^a \cdot y \), where \( a, b \) are integers \( \geq 0 \). But \( x_{\beta_j}^a \cdot y \in \mathbb{E}_{a+b\beta_j} \) by virtue of (21.16.3.15), and since by definition and the fact that \( \beta_j(h_{\beta_j}) = 2 \) we cannot have \( q + b\beta_j \leq p \) for more than a finite number of integers \( b \geq 0 \), it follows that \( x_{\beta_j}^a \cdot y = 0 \) for all but finitely many values of \( b \). It then follows from (21.16.3.17) that for each of these values of \( b \) we have \( x_{\beta_j}^a \cdot y = 0 \) for all sufficiently large \( a \), and therefore \( F \) is indeed finite-dimensional. The \( \mathbb{U}(s_{\beta_j}) \)-module \( F \) is thus a direct sum of submodules isomorphic to the modules \( L_{\nu m} \) (21.9.3) (if we identify \( s_{\beta_j} \) with \( \text{su}(2) \)). By hypothesis, there is an element \( y' \neq 0 \) in one of these submodules such that \( h_j : y' = q(h_j)y' \), and therefore it follows from the first of the formulas (21.9.3.1) that there is also an element \( y'' \neq 0 \) in this submodule that belongs to an \( \mathbb{E}_q \) with \( q' = q + k\beta_j \) for some integer \( k \in \mathbb{Z} \) and \( q'(h_j) = -q(h_j) \). This last relation may also be written as \( (q + q'|\beta_j) = 0 \); now \( \frac{1}{2}(q + q') \) cannot be orthogonal to \( \beta_j \), for \( q' \) of the form \( q + k\beta_j \), unless \( q \) and \( q' \) are images of each other under the orthogonal reflection \( \sigma_{\beta_j} \) (21.11.2.1); hence we have \( q' = s_j \cdot q \). This completes the proof of (21.16.3.21) and hence also of (21.16.3).

With the same notation, the results of (21.16.2) and (21.16.3) can be stated as follows:

(21.16.4) Let \( G \) be a simply connected semisimple compact Lie group, \( Z \) its center, \( \mathfrak{g} \) its Lie algebra, \( P(\mathbb{G}) = P(\mathfrak{g}) \) the lattice of weights of \( G \) relative to a maximal torus \( T \) of \( G \), and \( Q(\mathfrak{g}) \) the sublattice of \( P(\mathfrak{g}) \) generated by the roots of \( \mathfrak{g} \) (relative to \( T \)).

(i) The lattice \( P(\mathfrak{g}) \) is the dual in \( \mathbb{G}^* \) of the lattice in it generated by the \( \mathbf{h}_j \), which is the lattice \( (2\pi i)^{-1} \Gamma_T = (2\pi i)^{-1} \exp_T^{-1}(e) \) (21.7.5). The lattice \( Q(\mathfrak{g}) \) is the dual of the lattice \( (2\pi i)^{-1} \exp_T^{-1}(Z) \).

(ii) There is a canonical one-to-one correspondence between the quotients \( G_0 = G/D \) of \( G \) by a subgroup \( D \) of the center \( Z \), and the lattices \( \Gamma^* \) in it* such that \( Q(\mathfrak{g}) \subset \Gamma^* \subset P(\mathfrak{g}) \). If \( T_0 = T/D \), a maximal torus of \( G_0 \), then \( \Gamma^* \) is the dual of the lattice \( (2\pi i)^{-1} \Gamma_{T_0} \), the quotient \( P(\mathfrak{g})/\Gamma^* \) is isomorphic to the fundamental group \( \pi_1(G_0) \), and \( \Gamma^*/Q(\mathfrak{g}) \) is isomorphic to the center \( Z_0 = Z/D \) of \( G_0 \).

(21.16.5) Since the \( \mathbf{h}_j \) (1 \( \leq j \leq l \)) form a basis of the lattice \( (2\pi i)^{-1} \Gamma_T \) generated by the \( \mathbf{h}_j \) (21.11.5.5), the lattice \( P(\mathfrak{g}) \) admits as \( \mathbb{Z} \)-basis the basis of the vector space \( \mathbb{G}^* \) dual to the basis \( \{ \mathbf{h}_j \} \), i.e., the basis consisting of the linear forms \( \varpi_j \) (1 \( \leq j \leq l \)) such that

\[
\varpi_j(\mathbf{h}_k) = \delta_{jk} \quad (1 \leq j, k \leq l).
\]
The $m_j$ (1 \leq j \leq l) are called the fundamental weights of $g$ (or of the corresponding simply connected group $G$) relative to the basis $B$ of the root system $S$. From the definition of $P(g)$, all the elements of $P(g) \cap C$ are linear combinations $\sum_{j=1}^{i} n_j m_j$ in which the $n_j$ are integers $\geq 0$. By virtue of (21.11.7), the half-sum of the positive roots is given by the formula

$$\delta = m_1 + m_2 + \cdots + m_l.$$  

This is the smallest element of $P(g) \cap C$ (21.14.8).

It should be noted, however, that the $m_j$ are not necessarily minimal elements of $(P(g) - \{0\}) \cap C$.

If $p_j \in R(G)$ is the class of irreducible representations of $G$ with dominant weight $m_j$ (1 \leq j \leq l), the classes $p_j$ (or the representations belonging to these classes) are called fundamental.

(21.16.6) Let $G$ be a simply connected semisimple compact Lie group of rank $l$. Then the $Z$-algebra homomorphism

$$Z[X_1, X_2, \ldots, X_l] \rightarrow Z(R(G))$$

which maps identity element to identity element, and each indeterminate $X_j$ to the fundamental class $p_j$ (1 \leq j \leq l), is bijective.

We know from (21.15.5) that there is a canonical isomorphism $Z(R(G)) \rightarrow Z[P(g)]^W$, because $G$ is simply connected (21.16.3), and that the elements $v_p = J(e^p + \delta)/J(e^\delta)$ form a basis of $Z[P(g)]^W$ as $p$ runs through $P(g) \cap C$ (21.14.13). Composing this isomorphism with (21.16.6.1), we obtain a homomorphism of $Z[X_1, X_2, \ldots, X_l]$ into $Z[P(g)]^W$ that, for each multi-index $n = (n_1, \ldots, n_l) \in N^l$, maps $X_n = X_1^{n_1} \cdots X_l^{n_l}$ to the element $u_n = v_{n_1} \cdots v_{n_l}$. Since in the expression of $v_p$ as a linear combination of the $e^q$ with $q \in P(g)$, the term $e^p$ is the leading term (21.14.13), it is clear that $u_n$ has a leading term equal to $e^{\omega(n)}$, where $\omega(n) = n_1 m_1 + \cdots + n_l m_l$. As $n$ runs through $N^l$, $\omega(n)$ runs through the set $P(g) \cap C$, by virtue of (21.16.5.1) and the definition of $C$. It follows therefore from (21.14.13) that the $u_n$ form a basis of $Z[P(g)]^W$, and the proof is complete.

Remarks

(21.16.7) (i) It should be observed that the restrictions $\chi_{p_j}|T = v_{m_j} = J(e^{m_j} + \delta)/J(e^\delta)$ of the characters of the fundamental representations are not necessarily equal to the elements $S(m_j)$ (21.16.10).
(ii) Once the linear representations of a simply-connected semisimple compact Lie group $G$ are known, the linear representations of any quotient $G/D$ of $G$ by a discrete subgroup of its center (i.e., of a Lie group locally isomorphic to $G$) can be deduced: they are the representations obtained on passing to the quotient from a representation $U: G \to \text{GL}(E)$ such that the image of $D$ under $U$ is the identity element of $\text{GL}(E)$.

**Examples: The Fundamental Representations of the Classical Groups**

(21.16.8) 1. **Representations of $\text{SU}(n)$**. With the notation of (21.12.1), the elements $h_j$ of the basis $B$ of $S$ are the matrices

$$E_{jj} - E_{j+1,j+1} \quad (1 \leq j \leq n-1);$$

the $ih_j$ $(1 \leq j \leq n-1)$ form a basis of the Lie algebra $t'$ of the maximal torus $T' = T \cap \text{SU}(n)$, the intersection of $\text{SU}(n)$ with the maximal torus $T$ of $U(n)$ defined in (21.12.1); the lattice $\Gamma_{r'}$, the kernel of the exponential mapping $\exp_{r'}$, has as a $\mathbb{Z}$-basis the elements $2\pi i h_j (1 \leq j \leq n-1)$; the lattice $2\pi i \Gamma_{r'} = P(\text{SU}(n))$ therefore has as a basis the fundamental weights $\omega_j (1 \leq j \leq n-1)$, and we regain the fact that $P(\text{SU}(n)) = P(\text{su}(n))$ (21.16.3).

The restrictions $\varepsilon'_j$ to $it'$ of the $n$ linear forms $\varepsilon_j (1 \leq j \leq n)$ generate the dual $it'^*$ of the real vector space $it'$, and satisfy the relation

$$\varepsilon'_1 + \varepsilon'_2 + \cdots + \varepsilon'_n = 0;$$

the $\varepsilon'_j$ for $1 \leq j \leq n-1$ form a basis of $it'^*$ over $\mathbb{R}$. A simple calculation then shows that the linear form $\omega_j$ on $it'$ $(1 \leq j \leq n-1)$ is given by the formula

(21.16.8.1) $\omega_j = \varepsilon'_1 + \varepsilon'_2 + \cdots + \varepsilon'_j \quad (1 \leq j \leq n-1).$

The vector space $it$ is the direct sum of $it'$ and $ic = \mathbb{R} \sum_{j=1}^{n} E_{jj}$; hence the dual $it'^*$ may be canonically identified with the annihilator of $ic$ in $it^*$, and with this identification it is easily verified that

(21.16.8.2) $\varepsilon'_j = \varepsilon_j - \frac{1}{n} \sum_{h=1}^{n} \varepsilon_h \quad (1 \leq j \leq n).$
We shall now determine explicitly the irreducible representations of SU\(n\) with dominant weights \(m_j \ (1 \leq j \leq n - 1)\). Since the functions \(e^{i_j}\) take values belonging to \(2\pi i\mathbb{Z}\) at the points of the lattice \(\Gamma_T\), generated by the \(2\pi i\mathbf{h}_j\), we may identify \(e^{i_j}\) with a function on \(T'\) \((21.13.6)\). Let \(U_1\) be the canonical injection \(s \mapsto s\) of SU\(n\) into GL\((n, \mathbb{C})\); it is clearly a linear representation of SU\(n\), and its restriction to \(T'\) is the Hilbert sum of \(n\) one-dimensional representations on spaces \(\mathbb{C}a_j\), where \((a_j)_{1 \leq j \leq n}\) is the canonical basis of \(\mathbb{C}^n\). The representation on \(\mathbb{C}a_j\) maps \(s \in T\) to the homothety with ratio \(e^{i_j}\), hence we have \(\text{Tr}(U_1(s)) = \sum_{j=1}^{n} e^{i_j(s)}\) for \(s \in T'\); as a function on \(T'\) this is just the sum \(S(m_1)\), because the Weyl group is equal to \(\mathfrak{S}_n\). It follows \((21.13.7)\) that \(U_1\) is irreducible; and from the expressions for the roots forming the basis \((21.12.1.3)\), that \(m_1\) is indeed the dominant weight of \(U_1\) relative to this basis.

For \(2 \leq j \leq n - 1\), we now define \(U_j(s) = \bigwedge_j U_1(s)\), so that \(U_j\) is a linear representation of SU\(n\) on the space \(\bigwedge_j \mathbb{C}^n\) of dimension \(\binom{n}{j}\). The canonical basis of this space consists of the \(j\)-vectors

\[a_H = a_{k_1} \wedge a_{k_2} \wedge \cdots \wedge a_{k_j}\]

where \(H\) is the set of elements of the strictly increasing sequence of integers \(k_1 < k_2 < \cdots < k_j\) in the interval \([1, n]\), and \(H\) runs through all \(j\)-element subsets of \([1, n]\). It is clear that the restriction of \(U_j\) to \(T'\) is the Hilbert sum of \(\binom{n}{j}\) one-dimensional representations on spaces \(\mathbb{C}a_H\), and that the representation on \(\mathbb{C}a_H\) maps \(s \in T'\) to the homothety with ratio \(e^{i_H(s)}\), where \(i_H = i_{k_1} + i_{k_2} + \cdots + i_{k_j}\); from this it follows that \(\text{Tr}(U_j(s)) = S(m_j)\). We deduce as above that \(U_j\) is irreducible and that \(m_j\) is its dominant weight.

It is easily verified (for example with the help of \((21.8.4.2)\)) that the center of SU\(n\) is the subgroup of \(T'\) formed by the scalar matrices \(\omega I_n\), where \(\omega\) runs through the set of \(n\)th roots of unity. We may also calculate directly \(P(\mathfrak{su}(n))/Q(\mathfrak{su}(n))\) by using the preceding results \((21.16.4)\).

\(21.16.9\) II. Representations of \(U(n, H)\). In view of the description of the maximal torus \(T\) considered in \((21.12.2)\), the elements \(2\pi i\mathbf{h}_j \ (1 \leq j \leq n)\) form a basis of the lattice \(\Gamma_T\); as in \((21.16.8)\) we recover the fact that \(P(U(n, H)) = P(\mathfrak{u}(n, H))\) \((21.16.3)\), and verify that

\(21.16.9.1\)

\[m_j = e_1 + e_2 + \cdots + e_j \quad (1 \leq j \leq n).\]
Since $U(n, H)$ is simply connected, the canonical injection
\[ u(n, H) \to \text{sp}(2n, \mathbb{C}) \]
described in (21.12.2) corresponds to a linear representation $U_1$ of $U(n, H)$ on $\mathbb{C}^{2n}$. If $(a_j)_{1 \leq j \leq 2n}$ is the canonical basis of $\mathbb{C}^{2n}$, the restriction of $U_1$ to $T$ is the Hilbert sum of $2n$ one-dimensional representations on the spaces $\mathbb{C}a_j$ ($1 \leq j \leq n$); for $1 \leq j \leq n$, the representation on $\mathbb{C}a_j$ maps $s \in T$ to the homothety with ratio $e^{i\theta_j s}$, and the representation on $\mathbb{C}a_{n+j}$ maps $s \in T$ to the homothety with ratio $e^{-i\theta_j s}$. From the description of the Weyl group (21.12.2), it follows that the function $s \mapsto \text{Tr}(U_1(s))$ on $T$ is equal to the sum $S(m,)$; hence $U_1$ is irreducible (21.13.7) with dominant weight $\varpi_1$.

Likewise, if we define $U_j(s) = \bigwedge^j U_1(s)$ for $2 \leq j \leq n$, then $U_j$ is a linear representation of $U(n, H)$ on the space $\bigwedge^j (\mathbb{C}^{2n})$ of dimension $\binom{2n}{j}$, whose canonical basis consists of the $j$-vectors $a_{1,2,...,j}$. The restriction of $U_j$ to $T$ is the Hilbert sum of $\binom{2n}{j}$ one-dimensional representations of $T$ on the spaces $\mathbb{C}a_{1,2,...,j}$: the representation on $\mathbb{C}a_{1,2,...,j}$ maps each $s \in T$ to the homothety with ratio $e^{i\theta_{1,2,...,j}}$, where $\theta_{1,2,...,j}$ is defined as follows: if the elements of $H$ are $j_1 < j_2 < \cdots < j_k$, then $\theta_{1,2,...,j} = \theta_{j_1} + \theta_{j_2} + \cdots + \theta_{j_k}$, where $\theta_{j_h} = \theta_{k_h}$ if $1 \leq k_h \leq n$, and $\theta_{k_h} = -\theta_{k_h-n}$ if $n + 1 \leq k_h \leq 2n$.

However, when $j \geq 2$, the representation $U_j$ so defined is not irreducible. For example, since $U(n, H)$ may be identified with a subgroup of the symplectic group $\text{Sp}(2n, \mathbb{C})$, it follows from (A.16.4) that $U_2$ leaves invariant the bivector $a_1 \wedge a_{n+1} + \cdots + a_n \wedge a_{2n}$ in $\bigwedge^2 (\mathbb{C}^{2n})$. Nevertheless, we shall show that the representation $U_j$ decomposes into a Hilbert sum of irreducible representations, of which exactly one has $\varpi_j$ as dominant weight (cf. Problem 3). Indeed, the dominant weights of the irreducible representations into which $U_j$ splits must be certain of the $\theta_{1,2,...,j}$; if we observe that $\theta_r > \theta_r'$ for all $r, r'$ (21.12.2.8), we see that the set of weights $\theta_{1,2,...,j}$ contains a greatest element, corresponding to the subset $H_0 = \{1, 2, \ldots, j\}$, and that $\theta_{H_0} = \varpi_j$. Hence, among the irreducible components of the representation $U_j$, there is a unique $V_j$ whose dominant weight is $\varpi_j$. The space $E_j$ of this representation is the subspace of $\bigwedge^j (\mathbb{C}^{2n})$ generated by the transforms $S \cdot a_{1,2,...,j}$ of $a_{1,2,...,j}$ by all symplectic matrices $S \in \text{Sp}(2n, \mathbb{C})$. By construction, $a_{1,2,...,j}$ is a decomposable $j$-vector corresponding to a totally isotropic $j$-dimensional subspace of $\mathbb{C}^{2n}$; since the symplectic group acts transi-
tively on the set of totally isotropic subspaces of dimension \( j \leq n \), it follows that \( E_j \) is the subspace of \( \bigwedge^j (C^{2n}) \) spanned by all the decomposable \( j \)-vectors (called totally isotropic \( j \)-vectors), which correspond to the totally isotropic subspaces of dimension \( j \).

(21.16.10) III. Representations of \( \text{SO}(m) \). With the notation of (21.12.3) and (21.12.4), in both cases the lattice \( \Gamma_T \) has as a basis the \( 2\pi n_i H_j \) for \( 1 \leq j \leq n \). For \( \text{SO}(2n) \) we have

\[
H_j = h_j + h_{j+1} + \cdots + h_{n-2} + \frac{1}{2}(h_{n-1} + h_n) \\
(1 \leq j \leq n - 2),
\]

(21.16.10.1)

\[
H_{n-1} = \frac{1}{2}(h_{n-1} + h_n), \\
H_n = \frac{1}{2}(h_n - h_{n-1}),
\]

and for \( \text{SO}(2n + 1) \)

\[
H_j = h_j + h_{j+1} + \cdots + h_{n-1} + \frac{3}{2}h_n \quad (1 \leq j \leq n - 1),
\]

(21.16.10.2)

\[
H_n = \frac{3}{2}h_n.
\]

In both cases, we see therefore that \( \text{SO}(m) \), for \( m \geq 3 \), is not simply connected (21.16.4). We denote by \( \text{Spin}(m) \) the Lie group that is the universal covering of \( \text{SO}(m) \). If \( T_1 \) is the inverse image of the torus \( T \) in \( \text{Spin}(m) \), the formulas above show that the lattice \( (2\pi i)^{-1} \Gamma_T \) is generated by \( (2\pi i)^{-1} \Gamma_{T_1} \) and the element \( \frac{1}{2}(h_n - h_{n-1}) \) in the case of \( \text{SO}(2n) \), and by \( (2\pi i)^{-1} \Gamma_{T_1} \) and \( \frac{3}{2}h_n \) in the case of \( \text{SO}(2n + 1) \); in both cases, it follows that the fundamental group \( \pi_1(\text{SO}(m)) \) is a group with two elements (cf. (16.30.6)).

The fundamental weights are given by the following formulas, for \( \text{Spin}(2n) \):

\[
\omega_j = \varepsilon_1 + \cdots + \varepsilon_j \quad (1 \leq j \leq n - 2),
\]

(21.16.10.3)

\[
\omega_{n-1} = \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_{n-2} + \varepsilon_{n-1} - \varepsilon_n), \\
\omega_n = \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_{n-2} + \varepsilon_{n-1} + \varepsilon_n),
\]

and for \( \text{Spin}(2n + 1) \):

\[
\omega_j = \varepsilon_1 + \cdots + \varepsilon_j \quad (1 \leq j \leq n - 1),
\]

(21.16.10.4)

\[
\omega_n = \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_{n-1} + \varepsilon_n).
Consider the canonical injection $SO(m) \to SO(m, \mathbb{C})$, which defines a linear representation $V_1$ of $SO(m)$ on $\mathbb{C}^m$. For $j \leq m$ we obtain as in (21.16.8) a linear representation $V_j = \bigwedge^j V_1$; by composing these with the canonical homomorphism $Spin(m) \to SO(m)$, we obtain linear representations $U_j$ ($1 \leq j \leq m$) of $Spin(m)$. We shall now study these representations directly, and show that for $m = 2n$ and $j \leq n - 1$, or $m = 2n + 1$ and $j \leq n$, the representation $V_j$ (and hence also $U_j$) is irreducible. Let $(a_k)_{1 \leq k \leq m}$ be the canonical basis of $\mathbb{R}^m$, identified with the canonical basis of $\mathbb{C}^m$; then the canonical basis of $\bigwedge^j (\mathbb{C}^m)$ consists of the $j$-vectors

$$a_H = a_{k_1} \wedge a_{k_2} \wedge \cdots \wedge a_{k_j},$$

where $H$ is the set of elements $k_1 < k_2 < \cdots < k_j$ in the interval $[1, m]$, and $H$ runs through the set of all $j$-element subsets of $[1, m]$. We shall show (under the above restrictions on $j$) that the subspace $F(z)$ of $\bigwedge^j (\mathbb{C}^m)$ stable under $V_j$, generated by an arbitrary $j$-vector $z \neq 0$, is the whole space $\bigwedge^j (\mathbb{C}^m)$. Put $z = \sum_H c_H a_H$, where $c_H \in \mathbb{C}$; we shall argue by induction on the number $r$ of coefficients $c_H$ that are $\neq 0$. The assertion is obvious when $r = 1$: indeed, for each permutation $\pi \in S_m$, the automorphism of $\mathbb{C}^m$ that transforms $a_k$ into $\pm a_{\pi(k)}$ for $1 \leq k \leq m$ belongs to the image of $SO(m)$ under $V_1$, provided that the product of the minus signs is equal to the signature of $\pi$. Since $F(z)$ contains the element $a_h$ of the canonical basis of $\bigwedge^j (\mathbb{C}^m)$, it therefore contains also all elements $a_{\pi(h)}$, and hence is the whole of $\bigwedge^j (\mathbb{C}^m)$. Suppose now that the assertion has been proved for some value of $r \geq 1$, and for all values $< r$, and suppose that the number of nonzero coefficients $c_H$ in $z$ is $r + 1$. Then there exist two distinct $j$-element subsets $H, L$ of $[1, m]$ such that $c_H c_L \neq 0$. Let $p$ be an element of $L \cap H$. Next, since $2j < m$, there exists $q \in [1, m]$ that does not belong to $H \cup L$. The automorphism $T$ of $\mathbb{C}^m$ that leaves $a_k$ fixed for $k$ not equal to $p$ or $q$, and transforms $a_p$ into $-a_p$ and $a_q$ into $-a_q$, is in the image of $SO(m)$ under $V_1$ and transforms $a_H$ into itself, $a_L$ into $-a_L$, and each other $a_M$ into $\pm a_M$. It follows immediately that in the $j$-vector $z + T \cdot z$, which belongs to $F(z)$, the number of coefficients $\neq 0$ is $\geq 1$ and $\leq r$; we may therefore apply the inductive hypothesis to complete the proof.

Put $b_{2r-1} = a_{2r-1} - ia_{2r}$, $b_{2r} = a_{2r-1} + ia_{2r}$, for $2r \leq m$. When $m = 2n$, the $b_k$ for $1 \leq k \leq 2n$ form a basis of $\mathbb{C}^{2n}$; the restriction of $V_1$ to $T$ is the Hilbert sum of $2n$ one-dimensional representations on subspaces $Cb_k$ ($1 \leq k \leq 2n$), and the representation on $Cb_{2r-1}$ (resp. $Cb_{2r}$) is the homo-
they with ratio $e^\nu$ (resp. $e^{-\nu}$). For $j \leq 2n$, a basis of $\bigwedge^j (\mathbb{C}^{2n})$ is formed by the
\(j\)-vectors $b_H = b_{k_1} \wedge b_{k_2} \wedge \cdots \wedge b_{k_j}$, where $H$ is the set of elements
$k_1 < k_2 < \cdots < k_j$ in the interval $[1, 2n]$, and $H$ runs through all $j$-element
subsets of $[1, 2n]$. Then the restriction of $V_j(s)$ to $T$ transforms $b_H$ into
$e^{\epsilon_H(s)} b_H$, where $\epsilon_H = \epsilon_{k_1} + \epsilon_{k_2} + \cdots + \epsilon_{k_j}$, the $\epsilon_k$ being defined by
$\epsilon_{2r-1} = \epsilon_r$ and $\epsilon_{2r} = -\epsilon_r$. Since, for the ordering on it* (21.14.5), we have $\epsilon_r > \epsilon_{r'}$ if
$r < r'$, and $\epsilon_r > -\epsilon_{r'}$ for all $r, r' \in [1, n]$ by virtue of (21.12.3.5), it follows
that, for $j \leq n - 2$, the representation $V_j$ has dominant weight $\omega_j$.

When $m = 2n + 1$, a basis of $\bigwedge^j (\mathbb{C}^{2n+1})$ is formed by the $b_H$ defined
above and the $b_{H'} \wedge a_{2n+1}$, where $H'$ is a subset of $j - 1$ elements of $[1, 2n]$;
it follows as above that $V_j$ has dominant weight $\omega_j$ for $j \leq n - 1$.

For the irreducible representations of $\text{Spin}(2n)$ with dominant weights
$\omega_{n-1}$ and $\omega_n$, and the irreducible representation of $\text{Spin}(2n + 1)$ with dominant
weight $\omega_n$, see Problem 7.

PROBLEMS

1. With the notation of (21.16.8), show that the complex conjugate of the irreducible
representation $U_j$ is equivalent to $U_{n-j}$ ($1 \leq j \leq n - 1$). If $n = 2m$ is even, the representation
$U_m^{(n)}$ (Section 21.1, Problem 9) is defined when $m$ is even, and the representation $U_m^{(m)}$ is
defined when $m$ is odd.

2. With the notation of (21.16.9), show that each of the representations $U_j$ (or $V_j$) is equiva-
lent to its complex conjugate, $U_j^{(n)}$ is defined for even $j$, and $U_j^{(m)}$ for odd $j$.

3. (a) Let $B$ be a nondegenerate alternating bilinear form on $\mathbb{C}^{2n}$; let $(e_j)_{1 \leq j \leq 2n}$
be a symplectic basis of $\mathbb{C}^{2n}$, and let $(e_j^*)_{1 \leq j \leq 2n}$ be the dual basis, so that
$B = e_1^* \wedge e_2^* + \cdots + e_{2n-1}^* \wedge e_{2n}$
in the vector space $\bigwedge^2 (\mathbb{C}^{2n})$. Put
$B^* = e_1 \wedge e_2 + \cdots + e_{2n-1} \wedge e_{2n}$
in the vector space $\bigwedge^2 (\mathbb{C}^{2n})$; the bivector $B^*$ is independent of the symplectic basis $(e_j)$
chosen.

For each subset $H$ of $[1, 2n]$, we have

$$(e_{2j-1} \wedge e_{2j}) \wedge e_H = 0 \quad \text{if} \quad \{2j-1, 2j\} \cap H = \emptyset,$$

$$(e_{2j-1} \wedge e_{2j}) \wedge e_H = e_H \wedge (e_{2j-1} \wedge e_{2j}) = e_H \cup \{2j-1, 2j\}$$
if \([2j - 1, 2j] \cap H = \emptyset\). If we consider \(C^{2n}\) as the dual of \((C^{2n})^*\), we have likewise
\[
(e_j^+ \wedge e_j^+) \cdot e_H = \begin{cases} 0 & \text{if } [2j - 1, 2j] \cap H = \emptyset, \\ e_{H - 2j - 1, 2j} & \text{if } [2j - 1, 2j] \subseteq H. \end{cases}
\]

(b) In the endomorphism ring of the vector space \(\bigwedge (C^{2n})\), let \(Y^+\) denote the mapping \(z \mapsto B \cup z\), and \(Y^-\) the mapping \(z \mapsto B^* \wedge z\); also put \(Z = [Y^+, Y^-]\). For each subset \(H\) of \([1, 2n]\), let \(c^n_H\) (resp. \(c^H_H\)) denote the number of subsets \([2j - 1, 2j]\) contained in \([H\) (resp. \(H\)). Show that
\[
Z \cdot e_H = (c^n_H - c^H_H) e_H
\]
(\text{use (a) above}). Deduce that
\[
[Z, Y^+] = 2Y^+, \quad [Z, Y^-] = -2Y^-\]
and hence that the Lie subalgebra of \(\mathfrak{gl}(\bigwedge (C^{2n}))\) spanned by \(Y^+, Y^-\), and \(Z\) is isomorphic to \(\mathfrak{o}(2, C)\).

(c) With the notation of (21.16.9), show that for each \(p \in [1, n]\) the restrictions of \(Y^+\) and \(Y^-\) to \(\bigwedge (C^{2n})\) commute with all the automorphisms \(U_p\). Use (21.9.3) to deduce that the subspace \(E_p = \bigwedge (C^{2n})\) spanned by the totally isotropic decomposable \(p\)-vectors consists of the \(p\)-vectors \(z\) such that \(Y^+ \cdot z = 0\) and \(Z \cdot z = (n - p)z\). Deduce that if \(p < n\), the mapping \(z \mapsto (Y^-)^{n-p} \cdot z = (B^*)^{n-p} \wedge z\) (where \((B^*)^h\) denotes the \(2h\)-vector that is the product of \(h\) factors equal to \(B^*\) in the exterior algebra \(\bigwedge (C^{2n}))\) is injective on \(\bigwedge (C^{2n})\).

(d) Hence show that, for \(p \leq n\), \(\bigwedge (C^{2n})\) is the direct sum of the subspaces
\[
E_p, \quad (B^*) \wedge E_{p-2}, \quad (B^*)^2 \wedge E_{p-4}, \ldots
\]
each stable under the representation \(U_p\), and that the restriction of \(U_p\) to \((B^*)^h \wedge E_{p-2h}\) is irreducible and similar to \(V_{p-2h}\) (Lepage's decomposition). The dimension of \(E_p\) is
\[
\binom{2n}{p} - \binom{2n}{p-2}.
\]

4. There exists a \(C\)-algebra \(C_m\) (the Clifford algebra) of dimension \(2^n\), having a basis consisting of the identity and all products \(a_{i_1} a_{i_2} \cdots a_{i_p}\) for \(1 \leq i_1 < i_2 < \cdots < i_p \leq m\), where the \(a_j\) (\(1 \leq j \leq m\)) are \(n\) elements such that \(a_j^2 = 1\) and \(a_j a_k = -a_k a_j\) whenever \(j \neq k\) (cf. Section 16.15, Problem 2). The algebra \(C_m\) is the direct sum of the vector subspace \(C_m^+\) spanned by the products \(a_{i_1} a_{i_2} \cdots a_{i_p}\) with \(p\) even, and the subspace \(C_m^-\) spanned by the analogous products with \(p\) odd; also \(C_m^+\) is a subalgebra of \(C_m^-\).

(a) If \(m\) is even, the center of \(C_m\) is \(C \cdot 1\), and the center of \(C_m^+\) is spanned by \(1\) and \(a_1 a_2 \cdots a_m\). If \(m\) is odd, the center of \(C_m\) is spanned by \(1\) and \(a_1 a_2 \cdots a_m\), and the center of \(C_m^-\) is \(C \cdot 1\).

(b) Let \(E\) be the \(C\)-vector subspace of \(C_m\) spanned by \(a_1, \ldots, a_m\) and let \(\Phi\) be the symmetric bilinear form on \(E\) such that \(\Phi(a_j, a_k) = \delta_{jk}\) (Kronecker delta). For each \(x \in E\), we have \(x^2 = \Phi(x, x) \cdot 1\) and \(xy + yx = 2\Phi(x, y) \cdot 1\) in the algebra \(C_m\). Show that if \(A\) is a \(C\)-algebra and \(f\) a \(C\)-linear mapping of \(E\) into \(A\) such that \(f(x)^2 = \Phi(x, x) \cdot 1\) for all \(x \in E\), then \(f\) has a unique extension to a homomorphism of \(C_m\) into \(A\).

(c) Show that there exists an isomorphism \(\beta\) of \(C_m\) onto the algebra opposite to \(C_m\) (i.e., \(\beta\) is an anti-automorphism of \(C_m\)) such that \(\beta(x) = x\) for all \(x \in E\).
(d) Let $G$ be the group of invertible elements $s \in C_m$ such that $sEs^{-1} = E$, and let $G^+ = G \cap C_m^+$. For each $s \in G$, let $\varphi(s)$ denote the linear mapping $x \mapsto sx^*s^{-1}$ of $E$ into itself. Show that $E \cap G$ is the set of vectors in $E$ that are nonisotropic for $\Phi$, and that for each $x \in E \cap G$, $-\varphi(x)$ is the reflection in the hyperplane in $E$ orthogonal to $x$ (relative to $\Phi$). Deduce that $\varphi$ is a homomorphism of $G$ into the orthogonal group $O(\Phi)$, whose kernel is the set of invertible elements of the center $Z$ of $C_m$. We have $\varphi(G) = O(\Phi)$ if $m$ is even, $\varphi(G) = SO(\Phi)$ if $m$ is odd, and $\varphi(G^+) = SO(\Phi)$ in either case.

(e) For each $s \in G^+$, show that $N(s) = \beta(s)s$ is a scalar, and that $s \mapsto N(s)$ is a homomorphism of $G^+$ into $C^*$.  

5. With the notation of Problem 4, suppose that $m = 2n$ is even, and put $m_j = a_{2j-1} - ia_{2j}$, $p_j = a_{2j-1} + ia_{2j}$ for $1 \leq j \leq n$. The $m_j$ (resp. the $p_j$) form a basis of a totally isotropic subspace $M$ (resp. $P$) (relative to $\Phi$), and $E$ is the direct sum of $M$ and $P$. We may identify $M$ with the dual of $P$ by identifying each subset $H$ with an even number and an odd number of elements. The subalgebra of $C_{2n}$ generated by $M$ has as a basis the elements $m_{i_1} \cdots m_{i_j}$, and for each pair of subsets $H, K$ of $I$, put $m_{H, K} = m_{i_1} \cdots m_{i_j}$, $m_{K, i_1} = m_{i_1} \cdots m_{i_j}$ if each subset of $I$ of the form $\{i_1, i_2, \ldots, i_j\}$, the $i_j$ being the elements of $H$ arranged in ascending order; this subalgebra may be identified with the exterior algebra $S = \wedge M$ on the vector space $M$.

Show that there exists a unique homomorphism $\rho$ of $C_{2n}$ into the algebra $\text{End}(S)$ of endomorphisms of the vector space $S$, such that for each $m \in M$ the image $\rho(m)$ is the linear mapping $z \mapsto mz$ of $S$ into itself, and that for each $p \in P$, $\rho(p)$ is the interior product $i(p)$ (A.15.3). $M$ being identified with the subalgebra of $C_{2n}$ generated by $M$, $S$ restricted to $S$. Then $\rho(M)$ is isomorphic to $\text{End}(S)$, which is isomorphic to the matrix algebra $M_{2n}(C)$. The vector space $S$ is the direct sum of $S^+ = S \cap C_{2n}^+$ and $S^- = S \cap C_{2n}^-$, having as respective bases the set of $m_{i_1}$ for subsets $H$ with an even number and an odd number of elements. The subalgebra $\rho(C_{2n}^\pm)$ of $\text{End}(S)$ leaves invariant the subspaces $S^+$ and $S^-$, and is isomorphic to $\text{End}(S^+) \times \text{End}(S^-)$.

6. With the notation of Problem 4, suppose that $m = 2n + 1$ is odd; the algebra $C_{2n}$ may be canonically identified with the subalgebra of $C_{2n+1}$ generated by the $a_j$ with $j \leq 2n$. Show that the mapping $p \mapsto iya_{2n+1}$ of the vector space $F \subset E$ spanned by the $a_j$ with $j \leq 2n$, into the algebra $C_{2n+1}^+$, extends to an isomorphism $\theta$ of $C_{2n}$ onto $C_{2n+1}^+$ (use Problem 4(b)). Deducet that $C_{2n+1}^+$ is isomorphic to the product of two algebras isomorphic to $M_{2n}(C)$.

7. With the notation of Problem 4, let $E_0$ be the real vector space spanned by $a_1, \ldots, a_m$. Then $E_0 \cap G$ is the set of vectors $0 \neq 0$ in $E_0$. Let $G_0$ be the subgroup of $G^+$ generated by the products of an even number of vectors $x \in E_0$ such that $N(x) = \Phi(x, x) = 1$.

(a) Show that $G_0$ is connected. (If $x, y$ are two distinct vectors in $E_0$ such that $\Phi(x, x) = \Phi(y, y) = 1$, consider the plane in $E_0$ spanned by $x$ and $y$, and a vector $x'$ in that plane orthogonal to $x$ and such that $\Phi(x', x') = 1$, and the vectors $z = x \cos t + x' \sin t$ for $t \in \mathbb{R}$.) Deduce that $G_0$ is isomorphic to $\text{Spin}(m)$, by observing that $\varphi(G_0)$ is isomorphic to $\text{SO}(m)$ and that $\varphi$ makes $G_0$ a double covering of $\text{SO}(m)$.

(b) Deduce from Problems 5 and 6 that for $m = 2n$ the representations $s \mapsto \rho(s)$ of $S^+$ and $s \mapsto \rho(s)|S^-$ are irreducible representations of $\text{Spin}(2n)$ (identifed with $G_0$) of dimension $2^{n-1}$; for $m = 2n + 1$, the representation $s \mapsto \rho(\theta^{-1}(s))$ is an irreducible representation of $\text{Spin}(2n+1)$ of dimension $2^n$.  

xxi compact lie groups and semisimple lie groups
8. Let \((a_j)_{1 \leq j \leq 2n}\) be the canonical basis of \(C^{2n}\), and let \(\Phi\) be the symmetric bilinear form on \(C^{2n}\) such that \(\Phi(a_j, a_k) = \delta_{jk}\), so that \(\text{O}(\Phi) = \text{O}(2n; \mathbb{C})\).

(a) Consider the basis \((a_j)_{1 \leq j \leq 2n}\) also as an orthonormal basis of \(\mathbb{R}^{2n}\), relative to the restriction of \(\Phi\) to \(\mathbb{R}^{2n}\). Define a mapping \(T\) of \((\mathbb{R}^{2n})^*\) into \(\bigwedge^\tau (\mathbb{R}^{2n})\) as follows: if \(x_1, \ldots, x_s\) are linearly dependent in \(\mathbb{R}^{2n}\), then \(T(x_1, \ldots, x_s) = 0\); if they are linearly independent, then we may write \(x_1 \wedge \cdots \wedge x_s = \lambda y_1 \wedge \cdots \wedge y_s\), where the vectors \(y_j\) (\(1 \leq j \leq n\)) form an orthonormal basis of the subspace of dimension \(n\) in \(\mathbb{R}^{2n}\) spanned by the \(x_j\), and \(\lambda \in \mathbb{R}\); then there exists an element \(u \in \text{SO}(2n)\) such that \(u(a_{j-1}) = y_j\) for \(1 \leq j \leq n\), and we define \(T(x_1, \ldots, x_s) = \lambda u(a_s) \wedge \cdots \wedge u(a_s)\). Show that this value depends neither on the choice of the \(y_j\) nor on the choice of \(u\), and that \(T\) is an alternating \(n\)-linear mapping, which therefore factorizes uniquely into \((\mathbb{R}^{2n})^* \to \bigwedge^n (\mathbb{R}^{2n}) \to \bigwedge^n (\mathbb{R}^{2n})\), where \(\tau\) is a linear bijection. This bijection extends uniquely to a \(n\)-linear bijection on \((\mathbb{C}^{2n})^*\) onto itself, also denoted by \(\tau\). We have \(\tau^2 = (-1)^{n+1} \cdot 1\). For each \(u \in \text{SO}(2n; \mathbb{C})\), we have \(\tau \circ \bigwedge^n (u) = \bigwedge^n (u) \circ \tau\); but if \(u \in \text{O}(2n; \mathbb{C})\), its determinant is equal to \(-1\), so \(\tau \circ \bigwedge^n (u) = -\bigwedge^n (u) \circ \tau\).

Deduce that \(\bigwedge^n (\mathbb{C}^{2n})\) is the direct sum of two subspaces \(F^+\), \(F^-\) of the same dimension, such that the restriction of \(\tau\) to \(F^+\) (resp. \(F^-\)) is the homothety with ratio 1 (resp. \(-1\)) if \(n\) is even, the homothety of ratio \(i\) (resp. \(-i\)) if \(n\) is odd.

(b) Put
\[
m_j = a_{2j-1} - ia_{2j}, \quad p_j = a_{2j-1} + ia_{2j}, \quad m_j = m_1 \wedge m_2 \wedge \cdots \wedge m_n, \quad m'_j = m_1 \wedge m_2 \wedge \cdots \wedge m_{n-1} \wedge p_n.
\]
Show that \(\tau(m_i) = i^m m_i\), \(\tau(m'_i) = -i^m m'_i\).

If we define a **totally isotropic** \(n\)-vector \(z\) corresponding to a totally isotropic subspace \(V_z\) of \(C^{2n}\), deduce from these results that every totally isotropic \(n\)-vector belongs either to \(F^+\) or to \(F^-\). Let \(N^+\) (resp. \(N^-\)) denote the set of those \(z\) which belong to \(F^+\) (resp. \(F^-\)) (cf. Section 16.14, Problem 18). If \(z\) and \(z'\) belong to \(N^+\) or both to \(N^-\), show that \(V_z \cap V_{z'}\) has even codimension in \(V_z\) (and in \(V_{z'}\)); if on the other hand one of \(z\), \(z'\) belongs to \(N^+\) and the other to \(N^-\), then \(V_z \cap V_{z'}\) has odd codimension in \(V_z\) (and in \(V_{z'}\)).

(c) Show that the \(n\)-vectors belonging to \(N^+\) (resp. \(N^-\)) span the \(C\)-vector space \(F^+\).
(resp. \( F^- \)), and deduce that the representation \( V_\alpha \) of \( SO(2n) \) on \( \bigwedge^n (C^{2n}) \) (in the notation of (21.16.10)) splits into two inequivalent irreducible representations on the subspaces \( F^+ \) and \( F^- \), respectively. The dominant weights of these two representations are \( 2m_\alpha \) and \( 2m_\alpha \) (To show that \( N^+ \) spans \( F^+ \) and \( N^- \) spans \( F^- \), prove that \( N^+ \cup N^- \) spans the whole space \( \bigwedge^n (C^{2n}) \), by using the irreducibility of the representation \( V_{n-1} \) of \( SO(2n - 1) \).)

9. (a) For the group \( SO(2n + 1) \), the weight lattice \( P \) is generated by \( m_1, \ldots, m_{n-1} \) and \( 2m_n \), and another basis of \( P \) is \( \varepsilon_1, \ldots, \varepsilon_n \). The elements of \( \mathbb{Z}[P]^W \) (21.13.6) are of the form

\[ G(e^{\varepsilon_1}, e^{-\varepsilon_1}, \ldots, e^{\varepsilon_n}, e^{-\varepsilon_n}) \]

where \( G(T_1, T_2, \ldots, T_{2n}) \) is a symmetric polynomial with integer coefficients. In particular, let \( \sigma_j (0 \leq j \leq 2n) \) be the elementary symmetric functions of \( T_1, \ldots, T_{2n} \), i.e., the coefficients of the polynomial \( (X + T_1)(X + T_2) \cdots (X + T_{2n}) \) in \( X \). Then the character of the representation \( V_j (1 \leq j \leq n) \) is

\[ \sigma_j (e^{\varepsilon_1}, e^{-\varepsilon_1}, \ldots, e^{\varepsilon_n}, e^{-\varepsilon_n}) + \sigma_{j-1} (e^{\varepsilon_1}, e^{-\varepsilon_1}, \ldots, e^{\varepsilon_n}, e^{-\varepsilon_n}). \]

Deduce that if \( \rho_j \) is the class of the representation \( V_j \), the ring \( \mathbb{Z}^{RG} \) for the group \( G = SO(2n + 1) \) is isomorphic to \( \mathbb{Z}[\rho_1, \ldots, \rho_n] \), the \( \rho_i \) being algebraically independent over \( \mathbb{Z} \).

(b) For the group \( SO(2n) \), the weight lattice \( P \) is generated by \( m_1, \ldots, m_{n-2}, 2m_{n-1} \), and \( 2m_n \), and has as a basis \( \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \). Let \( H \) be the vector space of polynomials \( G(T_1, T_2, \ldots, T_{2n}) \) with rational coefficients that are invariant (i) under the product of transpositions that interchange \( T_{2i-1} \) and \( T_{2j-1} \), and \( T_{2i} \) and \( T_{2j} \), where \( i \neq j \); (ii) under the product of an even number of transpositions that interchange \( T_{2i-1} \) and \( T_{2i} \). The space \( H \) is the direct sum of the space \( H^+ \) of symmetric polynomials in \( T_1, \ldots, T_{2n} \) and the space \( H^- \) of polynomials in \( H \) that change sign under interchange of \( T_{2n-1} \) and \( T_{2n} \) (observe that \( H \) remains globally invariant when this interchange is made on every polynomial in \( H \)). Every polynomial in \( H^- \) is of the form \( \left(T_1 - T_2\right)\left(T_3 - T_4\right) \cdots \left(T_{2n-1} - T_{2n}\right)F \), where \( F \in H^+ \). Show that \( \mathbb{Z}[P]^W \) is the set of elements \( G(e^{\varepsilon_1}, e^{-\varepsilon_1}, \ldots, e^{\varepsilon_n}, e^{-\varepsilon_n}) \) where \( G \) runs through the set of polynomials \( G(T_1, T_2, \ldots, T_{2n}) \) with integer coefficients that belong to \( H \). Deduce that the ring \( \mathbb{Z}^{RG} \) for the group \( G = SO(2n) \) is a free module over the ring \( \mathbb{Z}[\rho_1, \ldots, \rho_n] \) (where \( \rho_j \) is the class of the representation \( V_j \), the \( \rho_j \) being algebraically independent); a basis of this module is formed by 1 and the class \( \rho_\alpha \) of the restriction of \( V_\alpha \) to \( F^+ \) (in the notation of Problem 8). This implies the existence of a relation \( (\rho_\alpha)^2 = \alpha + \beta \rho_\alpha \), where \( \alpha \) and \( \beta \) lie in the ring \( \mathbb{Z}[\rho_1, \ldots, \rho_n] \).

10. Let \( G \) be a simply connected almost simple compact group. We retain the notation of Section 21.15, Problem 11.

(a) Consider the composite mapping

\[ g: (G/T) \times I \rightarrow (G/T) \times T \rightarrow G \]

where \( f \) is the mapping defined in (21.15.2.1). Show that the affine Weyl group \( W_\alpha \) acts differentiably and freely on \( (G/T) \times (t - D(G)) \), and that \( g \) makes this space into a covering of the open subset \( V \) of \( G \) that is the image of \( (G/T) \times T_{\alpha} \) under \( g \). Use Section 21.15, Problem 11(e) to show that \( (G/T) \times (t - D(G)) \) is the disjoint union of the open sets \( (G/T) \times iv(A^\ast) \), where \( v \in W_\alpha \), and that the restriction of \( g \) to \( (G/T) \times iv(A^\ast) \) is a diffeomorphism onto \( V \) for each \( v \in W_\alpha \). (Note that the lattice \( (2\pi i)^{-1}T_\alpha \) is generated by the \( h_\alpha \).)

(b) Show that none of the vertices of the simplex \( A^\ast \), other than 0, can belong to the
16. REPRESENTATIONS OF SEMISIMPLE COMPACT CONNECTED GROUPS

lattice \( i \Gamma_T \). (Suppose if possible that there exists a vertex \( a_j = \frac{2 \pi p_j}{n_j} \) of \( A^* \) in \( i \Gamma_T \). Then \( A^* - a_j = w(A^*) \) for some \( w \in W \); show that if \( u \in A^* \) is sufficiently close to 0, we have \( u \neq a_j + w(u) \), and obtain a contradiction by observing that there exist \( s_1 \) and \( s_2 \) in \( G/T \) such that \( g(s_1, iu) = g(s_2, i(a_j + w(u))) \). Deduce that each orbit of \( W_\mathfrak{a} \) in \( A^* \) meets the closure of \( A^* \) in exactly one point.

(c) If \( Z \) is the center of \( G \), show that \( \text{Card}(Z) - 1 \) is the number of integers \( n_j \) that are equal to 1 in the expression \( \mu = \sum_{j=1}^{l} n_j \beta_j \), where \( \mu \) is the highest root (Section 21.15, Problem 10). (Observe that the vectors \( p_j \) form a basis of the lattice \( (2\pi)^{-1} \exp i(Z) \).)

11. (a) The hypotheses on \( G \) and the notation are the same as in Problem 10. Show that for each automorphism \( v \) of \( G \), the group \( F \) of fixed points of \( v \) is connected. (Use Section 21.11, Problem 19 to reduce to showing that each \( x \in F \) that is regular in \( G \) is contained in the identity component of \( F \). Having chosen a maximal torus \( T \) in \( G \), we may write \( x = \exp_i(u) \), where \( u \in A^* \); we then have \( v_\mathfrak{a}(u) = u = x \), where \( i \alpha \in \exp^{-1}(Z) \). Use Problem 10 to show that \( z = 0 \), and deduce that the one-parameter subgroup consisting of the \( \exp_i(\xi \mu) \) with \( \xi \in R \) is contained in \( F \).

(b) Give an example of an involutory automorphism of the group \( SO(3) \) whose set of fixed points is not connected.

12. With the notation of the proof of (21.16.3), let \( \mathfrak{u}_+ \) and \( \mathfrak{u}_- \) be the Lie subalgebras of \( \mathfrak{g}(\mathfrak{c}) \) spanned respectively by the elements \( \mathfrak{x}_a \) (1 \( \leq k \leq n \)) and \( \mathfrak{x}_-a \) (1 \( \leq k \leq n \)). Let \( e_{a, b, c} \) denote the element (21.16.3.4), where \( a = (a_1, ..., a_n) \), \( b = (b_1, ..., b_n) \), \( c = (c_1, ..., c_l) \).

(a) Let \( \mathfrak{u}^0 \) be the commutator of \( \mathfrak{h} \) in \( \mathfrak{u} \), or equivalently the commutator of the subalgebra \( \mathfrak{u}(\mathfrak{h}) \) in \( \mathfrak{u} = \mathfrak{u}(\mathfrak{g}(\mathfrak{c})) \). Show that \( \mathfrak{u}^0 \) has a basis consisting of the \( e_{a, b, c} \) such that \( \sum_k a_k s_k = \sum_k b_k a_k \).

(b) Show that \( \mathfrak{l} = (\mathfrak{u}_+ \cap \mathfrak{u}_-) \cap \mathfrak{u}^0 \cap (\mathfrak{u}_+ \cap \mathfrak{u}_-) \) is a two-sided ideal in \( \mathfrak{u}^0 \), and that \( \mathfrak{u}^0 = \mathfrak{u}(\mathfrak{h}) \oplus \mathfrak{l} \).

13. With the same notation as in Problem 12, for each integer \( r > 0 \) let \( \mathfrak{u}^{(r)} \) be the vector subspace of \( \mathfrak{u} \) spanned by the \( e_{a, b, c} \) such that

\[ a_1 + \cdots + a_n + b_1 + \cdots + b_n + c_1 + \cdots + c_l \leq r. \]

For each \( s \in G \) the automorphism \( Ad(s) \) of \( \mathfrak{g} \) has a unique extension to an automorphism, also written \( Ad(s) \), of the algebra \( \mathfrak{u} \), which leaves invariant each \( \mathfrak{u}^{(r)} \), and \( s \mapsto Ad(s) \upharpoonright \mathfrak{u}^{(r)} \) is a continuous linear representation of \( G \) on \( \mathfrak{u}^{(r)} \). The derived homomorphism is \( u \mapsto ad(u) \), where \( ad(u) \) denotes the mapping \( z \mapsto uz - zu \) of \( \mathfrak{u}^{(r)} \) into itself (cf. Section 19.11, Problem 1).

(a) Let \( [\mathfrak{u}, \mathfrak{u}] \) denote the subspace of \( \mathfrak{u} \) spanned by the elements \( [x, x'] = xx' - x'x \) for all \( x, x' \) in \( \mathfrak{u} \). Likewise let \( [\mathfrak{g}, \mathfrak{u}] \) denote the subspace of \( [\mathfrak{u}, \mathfrak{u}] \) spanned by all \( [u, x] \) with \( u \in \mathfrak{g} \) and \( x \in \mathfrak{u} \). Show that \( [\mathfrak{u}, \mathfrak{u}] = [\mathfrak{g}, \mathfrak{u}] \).

(b) If \( Z \) is the center of the algebra \( \mathfrak{u} \), show that \( \mathfrak{u} = Z \oplus [\mathfrak{u}, \mathfrak{u}] \). (Using (a) and the complete reducibility of the linear representation \( s \mapsto Ad(s) \upharpoonright \mathfrak{u}^{(r)} \) of \( G \), show that

\[ \mathfrak{u}^{(r)} = (Z \cap \mathfrak{u}^{(r)}) \oplus ([\mathfrak{u}, \mathfrak{u}] \cap \mathfrak{u}^{(r)}). \]

If the component of \( x \in \mathfrak{u} \) in \( Z \) is denoted by \( x^r \), show that \( (xy)^r = (yx)^r \) and that \( (xz)^r = z(x^r) \) if \( z \in Z \).
(c) Each element \( x = \sum \xi_c \mathbf{h}^c \) (where \( \mathbf{h}^c = \mathbf{h}_1^c \cdots \mathbf{h}_n^c \)) in \( U(\mathfrak{h}) \) may be canonically identified with the polynomial function
\[
\lambda \mapsto H_\lambda(\lambda) = \sum \xi_c \lambda(\lambda, \mathbf{h}_1^c) \cdots \lambda(\lambda, \mathbf{h}_n^c)
\]
on the dual \( \mathfrak{h}^* \) of \( \mathfrak{h} \), with values in \( C \). For each irreducible representation \( V_\rho \) of \( G \) on a vector space \( E_\rho \), with dominant weight \( p \in \mathfrak{p}(\mathfrak{g}) \), the homomorphism \( (V_\rho) \otimes 1: \mathfrak{g}(\mathfrak{C}) \to \mathfrak{gl}(E_\rho) \) extends to a homomorphism \( \mathfrak{R}_\rho: U(\mathfrak{g}(\mathfrak{C})) \to \text{End}(E_\rho) \) of \( C \)-algebras. For each \( x \in U \), put \( \Xi_d(x) = (\dim E_\rho)^{-1} \text{Tr}(\mathfrak{R}_\rho(x)) \). Show that \( \Xi_d(x) = \Xi_d(x^*). \) If \( \Phi \) is the canonical homomorphism of \( U^0 \) onto \( U(\mathfrak{h}) \) with kernel \( \mathfrak{z} \) (Problem 12(b)), show that \( Z_d(x) = \Xi_d(p) \) for all \( x \in U \). (Observe that if \( y \in E_\rho \) is such that \( \mathfrak{R}_\rho(x) \cdot y = p(x)y \) for all \( x \in \mathfrak{h} \), then we have \( \mathfrak{R}_\rho(z) \cdot y \neq 0 \) for all \( z \in Z \), and \( \mathfrak{R}_\rho(x) \cdot y = 0 \) for all \( x \in \mathfrak{z} \).)

14. (a) With the same notation, put \( D(\lambda) = \prod \langle \lambda, \mathbf{h}_u \rangle \) for all \( \lambda \in \mathfrak{h}^* \). Show that for each \( \mathbf{u} \in \mathfrak{h} \) and each \( \lambda \in \mathfrak{h}^* \), the series \( \sum_{n=0}^{\infty} (1/n!) \mathfrak{H}_\mathbf{u}(\lambda) \) is absolutely convergent in \( C \), and that
\[
D(\lambda + \delta) \left( \sum_{n=0}^{\infty} \frac{1}{n!} \mathfrak{H}_\mathbf{u}(\lambda) \left( \sum_{w \in \mathfrak{w}} \text{det}(w)e^{w \cdot (\lambda + \delta), \mathbf{u}} \right) \right) = D(\delta) \sum_{w \in \mathfrak{w}} \text{det}(w)e^{w \cdot (\lambda, \mathbf{u})}.
\]
(Use Weyl's formulas to show that the formula is true for all \( \lambda = p \in \mathfrak{p}(\mathfrak{g}) \), by using (21.13.6.1) and the power-series expansion of \( e^{(\mathbf{w}, \mathbf{u})} \).)

(b) Deduce from this formula that, for each integer \( n \geq 0 \) and each \( \mathbf{u} \in \mathfrak{h} \), the rational function on \( \mathfrak{h}^* \) is in fact a polynomial function, and is a linear combination of the polynomial functions \( \mathfrak{H}_\mathbf{u}(\mathbf{v} - \mathbf{w}) \) for \( 0 \leq \mathbf{v} \leq \mathbf{w} \). Deduce from the same formula that each of the polynomial functions \( \mathfrak{H}_\mathbf{u}(\mathbf{v} - \mathbf{w}) \) is invariant under the action of \( W \) on \( \mathfrak{h}^* \).

(c) Show that \( U(\mathfrak{h}) + [U, U] = U \). (Consider as in Problem 13 the representation \( \mathfrak{s} \to \mathfrak{ad}(\mathfrak{s}) \) of \( U^0 \) and show, by considering the derived homomorphism, that the image of \( U(\mathfrak{h}) \cap U^0 \) under \( \mathfrak{ad}(\mathfrak{s}) \) is contained in \( [U, U] \cap U^0 \).) Next, using the conjugacy of the maximal commutative subalgebras of \( \mathfrak{g} \), show that for each \( \mathbf{v} \in \mathfrak{g} \) there exists \( \mathbf{s} \in \mathfrak{g} \) such that \( \mathfrak{ad}(\mathfrak{s}) \cdot \mathbf{w} = \mathbf{w} \in U(\mathfrak{h}) \) for all \( \mathbf{w} \), and deduce that \( U(\mathfrak{h}) + [U, U] \) contains the vector subspace \( V \) of \( U \) spanned by the \( \mathbf{v}^m \) for \( \mathbf{v} \in \mathfrak{g} \) and \( m \geq 0 \). Finally, prove that this vector subspace is the whole of \( U \), by showing by induction on \( r \) that it contains all products \( \mathbf{v}_1 \mathbf{v}_2 \cdots \mathbf{v}_r \) of \( r \) elements \( \mathbf{v}_j \in \mathfrak{g} \). For this purpose, observe that for each \( \mathbf{v} \in \mathfrak{g} \), the difference \( \mathbf{v}_{n+1} \mathbf{v}_{n+2} \cdots \mathbf{v}_{n+\rho} - \mathbf{v}_1 \mathbf{v}_2 \cdots \mathbf{v}_r \) belongs to \( U^0 \), and that \( \{\xi_1, \mathbf{v}_1, \cdots, \xi_r, \mathbf{v}_r, \cdots\} \in V \cap U^0 \) for all systems of scalars \( \xi_1, \cdots, \xi_r \).

(d) Deduce from (c) that if we put \( H_{\mathbf{u}}(\lambda) = H_\lambda(\lambda - \delta) \) for all \( x \in U(\mathfrak{h}) \), the mapping \( z \mapsto \mathfrak{H}_\mathbf{u}(\lambda) \) is a surjective homomorphism of the center \( Z \) of \( U(\mathfrak{g}) \) onto the algebra \( \mathfrak{I}^{(\mathfrak{h}, \mathfrak{W})} \) of polynomial functions on \( \mathfrak{h}^* \) that are invariant under the action of \( W \). (Use the fact that each function in \( \mathfrak{I}^{(\mathfrak{h}, \mathfrak{W})} \) is a linear combination of polynomial functions of the form \( (1) \).)

15. (a) With the same notation, there exists a canonical homomorphism
\[
\psi: \mathfrak{t}(\mathfrak{g}(\mathfrak{C})) \to U(\mathfrak{g}(\mathfrak{C})) = U.
\]
of the tensor algebra of \( g_\mathcal{C} \) onto the algebra \( U \), which is the identity on \( g_\mathcal{C} \) and maps \( x \otimes y - y \otimes x \) to \([x, y]\) for all \( x, y \in g_\mathcal{C} \). Show that the restriction of \( \psi \) to the space \( S_i(g_\mathcal{C}) \) of symmetric tensors of order \( r \) on \( g_\mathcal{C} \) is an isomorphism of this vector space onto a supplement of \( U^r \) in \( U^m \), and deduce that the restriction of \( \psi \) to the symmetric algebra \( S(g_\mathcal{C}) \) is an isomorphism of vector spaces (but not of algebras) of \( S(g_\mathcal{C}) \) onto \( U \). For each \( x \in G \), the automorphism \( Ad(x) \) extends to an algebra automorphism, also denoted by \( Ad(x) \). If \( x \in G \), we have \( \psi(Ad(x) \cdot y) = Ad(x) \cdot \psi(y) \). Let \( (g_\mathcal{C}, G) \) denote the set of elements of \( S(g_\mathcal{C}) \) that are invariant under \( Ad(s) \) for all \( s \in G \). Show that the restriction of \( \psi \) to \( I(g_\mathcal{C}, G) \) is a vector space isomorphism of \( I(g_\mathcal{C}), G \) onto the center \( Z \) of \( U \), but is not necessarily an isomorphism of algebras (take \( G = SU(2) \)).

(b) For each linear form \( \beta \) on the vector space \( g_\mathcal{C} \), let \( \beta(u^*) \) be the element of \( g_\mathcal{C} \) such that \( B_{\mathcal{C}}(\beta(u^*), v) = \langle u^*, v \rangle \) for all \( v \in g_\mathcal{C} \), so that \( \beta \) is an isomorphism of the vector space \( g_\mathcal{C} \) (the dual of \( g_\mathcal{C} \) onto \( g_\mathcal{C} \)). Show that the annihilator in \( g_\mathcal{C} \) of the subspace \( \mathcal{C}_+ + \mathcal{C}_- \) of \( g_\mathcal{C} \) is mapped onto \( h \) by \( \beta \), and may therefore be identified with the dual \( h^* \) of \( h \). The isomorphism \( \beta \) extends uniquely to an isomorphism (also denoted by \( \beta \)) of the symmetric algebra \( S(g_\mathcal{C}) \) onto \( S(g_\mathcal{C}) \), which transforms \( S^r(h) \) into \( S^r(h) \). If \( I \) is the ideal of \( S(g_\mathcal{C}) \) generated by \( \mathcal{C}_+ + \mathcal{C}_- \), we have \( S(g_\mathcal{C}) = U(h) \oplus I \). If \( j \) is the homomorphism \( S(g_\mathcal{C}) \rightarrow U(h) \) defined by this decomposition, then \( j^{-1}(I) \) is the kernel of the restriction homomorphism \( i : S(h^*) \rightarrow S(h^*) \); obtained by considering \( S(g_\mathcal{C}) \) (resp. \( S(h^*) \)) as the algebra of polynomial functions on \( g_\mathcal{C} \) (resp. \( h \)), and we have \( j^{-1}(I) = S(g_\mathcal{C}) \rightarrow S(h^*) \).

For each \( x \in G \), \( Ad(x) \) acts on \( S(g_\mathcal{C}) \), and extends to an algebra automorphism of \( S(g_\mathcal{C}) \), again denoted by \( Ad(x) \). If \( I(g_\mathcal{C}, G) \) is the subalgebra of \( S(g_\mathcal{C}) \) consisting of the elements that are invariant under \( Ad(s) \) for all \( s \in G \), then the image of \( I(g_\mathcal{C}, G) \) under \( j \) is \( I(h, G) \). Likewise, if \( I(h^*, W) \) is the subalgebra of \( S(h^*) \) consisting of the elements that are invariant under the action of \( W \) on \( h^* \), then the image of \( I(h^*, W) \) under \( j \) is \( I(h, W) \subset U(h) \).

(c) For each linear representation \( V \) of \( G \) on a complex vector space, the polynomial functions \( u \rightarrow \text{Tr}((V(u))^r) \) on \( g_\mathcal{C} \) belong to \( I(g_\mathcal{C}, G) \), and their restrictions to \( h \) belong to \( I(h^*, W) \). Show conversely that every polynomial function in \( I(h^*, W) \) is a linear combination of these restrictions. (Use the fact that the weights \( p \in P(g) \) span the vector space \( h^* \), and the isomorphism \( Z^\prime(\mathfrak{g}) \rightarrow Z[P]^m \) of (21.15.5.).)

(d) Show that the restriction to \( I(g_\mathcal{C}, G) \) of the homomorphism \( i \) in (b) above is an isomorphism of this algebra onto \( I(h^*, W) \). (To show that \( i \) is injective, note that if \( j(f) = 0 \) for \( f \in I(g_\mathcal{C}, G) \), then \( f = 0 \) on \( h \) and also on \( Ad(s) \cdot h \) for each \( s \in G \), and use the conjugacy theorem. To show that \( i \) is surjective, note that if \( L \) is the set of all linear combinations of the polynomial functions \( u \rightarrow \text{Tr}((V(u))^r) \) for all linear representations \( V \) of \( G \), then \( i(L) = I(h^*, W) \) by virtue of (c) above.) Deduce that the homomorphism

\[
j : I(g_\mathcal{C}, G) \rightarrow I(h, W)
\]

defined in (b) above is bijective.

(e) Show that the composite isomorphism

\[
Z \xrightarrow{\psi^{-1}} I(g_\mathcal{C}, G) \xrightarrow{i} I(h, W)
\]

is the same as the isomorphism \( z \rightarrow H_0^\mathfrak{g}\mathfrak{h}_0^\mathfrak{g} \) defined in Problem 14(d). (Show that for each \( r \) these two homomorphisms define the same mapping of \( (Z \cap U^r)/(Z \cap U^{r-1}) \) onto \( I(h, W) \cap S_i(h) \cap S_{i-1}(h) \), and that this mapping is bijective; for this purpose, use the basis \( \{e_a, b_a\} \) of \( U \) defined in (21.16.3.4).)

16. Let \( E \) be a complex vector space of dimension \( n \). If we identify the symmetric algebra \( S(E^*) \) with the algebra of polynomial functions on \( E \), the group \( \text{GL}(E) \) acts on \( S(E^*) \) by
the rule \((s \cdot P)(x) = P(s^{-1} \cdot x)\) for all \(P \in \mathfrak{S}(E^*)\), \(s \in \text{GL}(E)\), and \(x \in E\). If \(G\) is a subgroup of \(\text{GL}(E)\), denote by \(I(E, G)\) the subalgebra of \(\mathfrak{S}(E^*)\) consisting of the \(G\)-invariant polynomial functions \(P\), i.e., those for which \(s \cdot P = P\) for all \(s \in G\). If \(G\) is finite, with order \(N\), then for each \(P \in \mathfrak{S}(E^*)\) the polynomial function \(\mu(P) = N^{-1} \sum_{s \in G} s \cdot P\) is \(G\)-invariant. We have \(\mu(P) = P\) if \(P \in I(E, G)\).

(a) Let \(P = P_0 + P_1 + \cdots + P_n\) be a polynomial function on \(E\) that is invariant under a subgroup \(G\) of \(\text{GL}(E)\), where \(P_j\) is the homogeneous component of degree \(j\) in \(P\). Show that each \(P_j\) is \(G\)-invariant (consider \(P(tx)\) for \(t \in C\)).

(b) Suppose that \(G\) is finite. A rational function \(R\) on \(E\) is said to be \(G\)-invariant if \(R(s^{-1} \cdot x) = R(x)\) whenever both sides are defined. Show that \(R\) is then of the form \(P/Q\), where \(P\) and \(Q\) are \(G\)-invariant polynomial functions.

(c) The ring \(I(E, G) = \mathbb{C} \oplus J_1 \oplus \cdots \oplus J_n \oplus \cdots\) is graded, \(J_n\) being the vector space spanned by the \(P \in I(E, G)\), which are homogeneous of degree \(h\) (by virtue of (a) above); we define \(I_0\) to be \(C\). Let \(J_+ = J_1 \oplus \cdots \oplus J_n \oplus \cdots\), which is an ideal of \(I(E, G)\), and let \(\mathfrak{N}\) be the graded ideal of \(\mathfrak{S}(E^*)\) generated by \(J_+\).

Suppose from now on that \(G \subseteq \text{GL}(E)\) is a finite group, generated by orthogonal reflections \(r_1, \ldots, r_m\) in hyperplanes in \(E\) (relative to a scalar product on \(E\)). In order that a homogeneous polynomial function \(P\) of degree \(h > 0\) should belong to \(\mathfrak{N}\), it is necessary and sufficient that \(r_j \cdot P = P\) for \(1 \leq j \leq m\). (Observe that this condition implies that \(s \cdot P = P\) for all \(s \in G\), and that \(\mu(P) \in \mathfrak{N}\).)

(d) Let \(U_1, U_2, \ldots, U_n\) be elements of \(J_n\) such that \(U_1\) does not belong to the ideal in \(I(E, G)\) generated by \(U_2, \ldots, U_n\). Let \(P_1, P_2, \ldots, P_n\) be homogeneous elements of \(\mathfrak{S}(E^*)\) such that \(P_1U_1 + P_2U_2 + \cdots + P_nU_n = 0\). Show that \(P_1 \in \mathfrak{N}\). (Proceed by induction on the degree of \(P_1\). If \(P_1\) is a constant, observe that \(\sum \mu(P_j)U_j = 0\), and deduce that \(P_1 = 0\).

In general, show that \(r_j \cdot P_1 - P_1 \in \mathfrak{N}\) for \(1 \leq j \leq m\), by observing that there is a linear form \(L_j \neq 0\) such that \(r_j \cdot P - P\) is divisible by \(L_j\), for all \(P \in \mathfrak{S}(E^*)\).

(e) Let \((I_1, I_2, \ldots, I_q)\) be a minimal system of generators of the ideal \(\mathfrak{N}\), consisting of homogeneous invariant polynomial functions. Let \(d_k > 0\) be the degree of \(I_k\). Show that \(I_1, \ldots, I_q\) are algebraically independent over the field \(C\). (Suppose not, and let \(H(Y_1, \ldots, Y_q) \in \mathbb{C}[Y_1, \ldots, Y_q]\) be a nonzero polynomial of smallest degree such that \(H(I_1, \ldots, I_q) = 0\); we may also assume that all the monomials \(Y_{i_1}^{d_1} \cdots Y_{i_q}^{d_q}\) appearing in \(H\) are such that \(v_i d_1 + \cdots + v_q d_q\) has the same value. Then the invariants \(H_k = (\partial H/\partial Y_k)(I_1, \ldots, I_q)\) are not all zero. If \(U\) is the ideal that they generate in \(I(E, G)\), we may assume that \(I_1, \ldots, I_q\) is a minimal set of generators of \(U\), so that we have equations \(H_{i+j} = \sum_{k=1}^q V_{jk} H_k\), where the \(V_{jk}\) are homogeneous \((1 \leq j \leq q - s)\) and belong to \(I(E, G)\). Identifying the functions in \(\mathfrak{S}(E^*)\) with polynomials in the coordinates \(x_j \ (1 \leq h \leq n)\) of a point \(x \in E\), show that we have

\[
\frac{\partial l_k}{\partial x_h} + \sum_{j=1}^q V_{jk} \frac{\partial l_{s+j}}{\partial x_h} \in \mathfrak{N}
\]

for \(1 \leq h \leq n\) and \(1 \leq k \leq s\) (use (d) above). Use Euler's identity to deduce that for \(1 \leq k \leq s\) we have

\[
d_k I_k + \sum_{j=1}^{q-s} d_{s+j} V_{jk} I_{s+j} = \sum_{i=1}^q W_{ji} I_i
\]

where the \(W_{ji}\) are homogeneous of degree \(> 0\), and all the polynomials \(I_k, V_{jk} I_{s+j}\), and \(W_{ji} I_i\) are homogeneous of the same degree; this implies in particular that \(W_{ji} = 0\) and leads to a contradiction.)
16. REPRESENTATIONS OF SEMISIMPLE COMPACT CONNECTED GROUPS

17. Let $V$ be a finite-dimensional complex vector space, $s$ an endomorphism of $V$, and $s_m$ the canonical extension of $s$ to the $m$th symmetric power $S_m(V)$. Show that we have

$$\sum_{m=0}^\infty \text{Tr}(s_m)T^m = (\text{det}(1-sT))^{-1}$$

in the formal power series ring $\mathbb{C}[[T]]$. (Choose a basis of $V$ with respect to which the matrix of $s$ is triangular.)

18. With the notation of Problem 16, suppose that $G$ is a finite group of order $N$.

(a) Show that the endomorphism $f = N^{-1} \sum_{s \in G} s$ is a projection of $V$ onto the subspace $F$ of $V$ consisting of $G$-invariant elements. Hence we have $\dim(F) = \text{Tr}(f)$.

(b) Show that

$$\sum_{m=0}^n (\dim(J_m))T^m = N^{-1} \sum_{s \in G} (\text{det}(1-sT))^{-1}$$

in the formal power series ring $\mathbb{C}[[T]]$. (Apply (a) to each of the spaces $S_m(V^*)$, and use Problem 17.)

(c) Suppose from now on that $G$ is generated by orthogonal reflections, and let $R$ be the set of orthogonal reflections belonging to $G$. We have $s \in R$ if and only if $\text{det}(1-sT)$ is divisible by $(1-T)^r$ but not by $(1-T)^{r+1}$. Use Problem 16(f) to show that

$$\prod_{k=1}^r d_k = N, \quad \sum_{k=1}^r (d_k - 1) = r.$$
respectively, which generate the algebra \(I(h, W)\) (Problem 16(f)). Take a basis of \(h\) consisting of eigenvectors \(e_j (1 \leq j \leq l)\) of a Coxeter element \(\sigma\) (which is diagonalizable), so that 
\[
\sigma \cdot e_j = \exp(2\pi i m_j/h)e_j
\]
in the notation of Section 21.11, Problem 14. Use Problem 18(e) and Section 21.11, Problem 16(e) to show that, for the chosen basis of \(h\), there exists a permutation \(\alpha \in S\), such that \((\partial I\partial x_{\alpha(i)j})_j(1, 0, \ldots, 0) \neq 0\), and hence that in \(\sigma\), the monomial 
\[
x_{\alpha(i)j}^{m_j} x_{\alpha(i)j}\text{ }_h\text{ appears with nonzero coefficient. By expressing that \(I_j\) is invariant under}
\]
generating eigenvectors of \(\sigma\), deduce that we have \(d_r - 1 + m_{n(j)} \equiv 0 \mod h\). Using the relation \(m_j + m_{n(j)} = h\), deduce that by renumbering the \(I\), we may assume that we have \(d_r - 1 \equiv m_j \mod h\); and since \(d_r - 1 \geq 0\) and \(m_j < h\), we have \(d_r - 1 = m_j + \frac{1}{2}h\) with \(\mu_j\) an integer \(\geq 0\). Finally, use the relation \(m_1 + m_2 + \cdots + m_l = \frac{1}{2}h\), the fact that the number of roots is \(lh\) (Section 21.11, Problem 16(b)), and Problem 18(d) to show that \(d_r = m_j + 1\) for \(1 \leq j \leq l\).

20. (a) When \(G = SU(n)\), show that for the basis of \(u(n)\) defined in (21.12.1) the polynomial functions \(I_1, \ldots, I_n\) generating the algebra \(I(h, W)\) may be taken to be the restrictions to \(h \in \mathfrak{t}(\mathbb{C})\) of the elementary symmetric functions 
\[
s_j(x_1, \ldots, x_n) = \sum_{x \in \mathfrak{a}_h} x_{\alpha(1)} x_{\alpha(2)} \cdots x_{\alpha(j)}
\]
for \(2 \leq j \leq n\), so that the \(m_j\) are the numbers \(1, 2, \ldots, n - 1\).

(b) When \(G = U(n, H)\) or \(G = SO(2n + 1)\), the rings \(I(h, W)\) corresponding to these two groups are isomorphic. For the bases of \(h\) given in (21.12.2) and (21.12.4), the polynomial functions \(I_1, \ldots, I_n\) that generate \(I(h, W)\) may be taken to be the elementary symmetric functions 
\[
s_j(x_1, \ldots, x_n) = \sum_{x \in \mathfrak{a}_h} x_{\alpha(1)}^2 x_{\alpha(2)}^2 \cdots x_{\alpha(j)}^2
\]
for \(1 \leq j \leq n\), so that the \(m_j\) are the numbers \(1, 3, 5, \ldots, 2n - 1\).

(c) When \(G = SO(2n)\), for the basis of \(h\) defined in (21.12.3), the polynomial functions \(I_1, \ldots, I_n\) that generate \(I(h, W)\) may be taken to be the elementary symmetric functions 
\[
s_j(x_1^2, \ldots, x_n^2) = \sum_{x \in \mathfrak{a}_h} x_{\alpha(1)}^2 x_{\alpha(2)}^2 \cdots x_{\alpha(j)}^2
\]
for \(1 \leq j \leq n - 1\), and the function \(x_1 x_2 \cdots x_n\). The \(m_j\) are the numbers \(1, 3, 5, \ldots, 2n - 3, n - 1\).

21. Let \(G\) be a denumerable group of displacements in a real vector space \(E\) endowed with a scalar product, and let \(\mu\) be a positive \(G\)-invariant measure on \(E\) (for example, Lebesgue measure if \(E\) is identified with \(\mathbb{R}^n\), with the usual scalar product).

(a) Let \(U\), \(U'\) be two open subsets of \(E\), of finite measure. Suppose that the sets \(s \cdot U\) (resp. \(s \cdot U'\)) are pairwise disjoint for all \(s \in G\), and that the complement of their union is \(\mu\)-negligible. Show that \(\mu(U) = \mu(U')\). (If \(V\) (resp. \(V'\)) is the union of the sets \(s \cdot U\) (resp. \(s \cdot U'\)) for \(s \in G\), then \(V \cap V'\) is \(G\)-stable and has a negligible complement, and \(U \cap V'\) and \(U' \cap V\) are two \(G\)-tessellations of \(V \cap V'\) (Section 14.1, Problem 6).)

(b) Let \(G_0\) be a subgroup of \(G\), and suppose that there exists an open subset \(U_0\) of \(E\), of finite measure, such that the \(t \cdot U_0\) for \(t \in G_0\) are pairwise disjoint and the complement of their union is negligible. Then the index \((G : G_0)\) is finite and equal to \(\mu(U_0)/\mu(U)\) (Section 14.1, Problem 6(d)).

22. The hypotheses are as in Section 21.15, Problem 11. Apply the results of Problem 21 to the group \(W_0\) and the open set \(A^*\), to the group \(P_0\) and the open parallelotope constructed on the vectors \(2h, (1 \leq j \leq l)\), and finally to the subgroup \(Q_0\) of \(P_0\) generated by the translations \(u \rightarrow u + 2\pi n_jp_j\) and the parallelopetope constructed on the vectors \(2\pi p_j\) \((1 \leq j \leq l)\). Deduce that the order of the Weyl group \(W\) is \(l! n_1 n_2 \cdots n_l f\), where \(f - 1\) is the number of indices \(j\) such that \(n_j = 1\).
17. COMPLEXIFICATIONS OF COMPACT CONNECTED SEMISIMPLE GROUPS

(21.17.1) Let $\bar{K}$ be a simply connected compact semisimple Lie group, $K = \text{Ad}(\bar{K})$ its adjoint group, the quotient $\bar{K}/C$ of $\bar{K}$ by its (finite) center, and $\mathfrak{t}$ the Lie algebra of $\bar{K}$ and $K$. The group $K$ is the identity component of the closed subgroup $\text{Aut}(\mathfrak{t})$ of $GL(\mathfrak{t})$ (21.6.9). The complexification $\mathfrak{g} = \mathfrak{t}(C) = \mathfrak{t} \oplus i\mathfrak{t}$ if of $\mathfrak{t}$ is a complex semisimple Lie algebra (21.6.1). We shall denote by $c$ the semilinear bijection of $\mathfrak{g}$ onto itself defined by $c(y + iz) = y - iz$ for $y, z \in \mathfrak{t}$, so that $c^2 = 1_{\mathfrak{g}}$. It is immediately verified that

$$c([u, v]) = [c(u), c(v)]$$

for all $u, v \in \mathfrak{g}$. The Lie subalgebra $\mathfrak{t}$ of $g_{\mathbb{R}}$ is the set of all $u \in \mathfrak{g}$ such that $c(u) = u$.

We propose to describe (up to isomorphism) the complex connected semisimple Lie groups having $\mathfrak{g}$ as Lie algebra. If $\mathcal{G}$ is the simply connected complex group with $\mathfrak{g}$ as Lie algebra (19.11.9), then the adjoint group $G = \text{Ad}(\mathcal{G})$, the quotient of $\mathcal{G}$ by its (discrete) center, may be identified with the identity component of the closed subgroup $\text{Aut}(\mathfrak{g})$ of $GL(\mathfrak{g})$ (21.6.8), and its center consists only of $e$ (20.22.5.1). We shall first study the group $\text{Aut}(\mathfrak{g})$, whose Lie algebra is the image $\text{ad}(\mathfrak{g})$ of $\mathfrak{g}$ under the homomorphism $u \mapsto \text{ad}(u)$, a Lie subalgebra of $gl(\mathfrak{g}) = \text{End}_{\mathbb{C}}(\mathfrak{g})$, isomorphic to $\mathfrak{g}$ (21.6.3). Since every automorphism $u$ of $\mathfrak{t}$ extends uniquely to an automorphism $u \otimes 1_{\mathfrak{C}}$ of $\mathfrak{g}$, the group $\text{Aut}(\mathfrak{t})$ may be identified with the subgroup of $\text{Aut}(\mathfrak{g})$ consisting of the automorphisms that leave $\mathfrak{t}$ globally invariant.

(21.17.2) The Killing form $B_\mathfrak{t}$ of $\mathfrak{t}$ is the restriction to $\mathfrak{t} \times \mathfrak{t}$ of the Killing form $B_\mathfrak{g}$ of $\mathfrak{g}$ (21.6.1), and $B_\mathfrak{t}$ is negative definite. It follows that the mapping

$$B_\mathfrak{g}(u, c(v))$$

is a scalar product, which gives $\mathfrak{g}$ the structure of a finite-dimensional Hilbert space. For if $u = y + iz$ and $u' = y' + iz'$ with $y, z, y', z' \in \mathfrak{t}$, we have

$$B_\mathfrak{g}(u, c(u')) = B_\mathfrak{t}(y, y') + B_\mathfrak{t}(z, z') + i(B_\mathfrak{t}(y', z) - B_\mathfrak{t}(y, z'))$$

and $B_\mathfrak{g}(u, c(u)) = B_\mathfrak{t}(y, y) + B_\mathfrak{t}(z, z)$, which vanishes only if $y = z = 0$, i.e., $u = 0$. For each endomorphism $V$ of the complex vector space $\mathfrak{g}$, let $V^*$ denote the endomorphism adjoint to $V$, relative to this Hilbert space struc-
ture on \( \mathfrak{g} \) (11.5.1). Relative to any orthonormal basis of \( \mathfrak{g} \), the matrix of \( V^* \) is the conjugate transpose of the matrix of \( V \).

(21.17.3) (i) For each automorphism \( U \in \text{Aut}(\mathfrak{g}) \), we have

\[
U^* = c \circ U^{-1} \circ c.
\]

(ii) For each \( u \in \mathfrak{g} \) we have

\[
(\text{ad}(u))^* = -\text{ad}(c(u)).
\]

(i) For \( x, y \in \mathfrak{g} \) we have

\[
B_\mathfrak{g}(U \cdot x, c(y)) = B_\mathfrak{g}(x, U^{-1} \cdot c(y)) = B_\mathfrak{g}(x, c((c \circ U^{-1} \circ c) \cdot y))
\]
since \( B_\mathfrak{g} \) is invariant under \( U \) (21.5.6.2). This proves (21.17.3.1).

(ii) By virtue of (21.5.6.1), we have

\[
B_\mathfrak{g}(\text{ad}(u) \cdot x, c(y)) + B_\mathfrak{g}(x, c((c \circ \text{ad}(u) \circ c) \cdot y)) = 0.
\]

But it follows from (21.17.1.1) and the fact that \( c^2 = 1 \), that \( c \circ \text{ad}(u) \circ c = \text{ad}(c(u)) \). This proves (21.17.3.2)

(21.17.4) An automorphism \( U \in \text{Aut}(\mathfrak{g}) \) is unitary (relative to the Hilbert space structure of \( \mathfrak{g} \)) if and only if \( U \in \text{Aut}(\mathfrak{t}) \).

By virtue of (21.17.3.1), to say that \( U \) is unitary signifies that \( U^{-1} \) commutes with \( c \), or again that \( U \) commutes with \( c \); this implies that \( U \) leaves invariant the subspace \( \mathfrak{t} \) of fixed points of \( c \). The converse is obvious.

(21.17.5) We shall now characterize those automorphisms of \( \mathfrak{g} \) that are positive and self-adjoint relative to the Hilbert space structure on \( \mathfrak{g} \). For that purpose we shall first examine, from the viewpoint of the theory of Lie groups, the decomposition of an endomorphism of a complex vector space as the product of a self-adjoint operator and a unitary operator (cf. Section 11.5, Problem 15). Let \( E \) be a complex Hilbert space of finite dimension \( n \), and let \( \mathfrak{a}(E) \subset \mathfrak{gl}(E) = \text{End}_c(E) \) be the set of self-adjoint endomorphisms of \( E \); it is a real vector space, which may be identified (Section 11.5) with the space \( \mathscr{H}(E) \) of Hermitian forms on \( E \times E \), under the mapping that replaces each \( H \in \mathfrak{a}(E) \) by the Hermitian form \( (x, y) \mapsto (H \cdot x | y) \). Under this mapping, the set \( \mathfrak{a}_+(E) \) of positive self-adjoint endomorphisms, characterized by the relation \( (H \cdot x | x) > 0 \) for all \( x \neq 0 \) (or, equivalently, by the condition that their spectra should contain only numbers \( > 0 \) (11.5.7)), is identified
with the subset \( \mathcal{H}_{n,0}(E) \) of Hermitian forms of signature \((n,0)\) on \( E \times E \), which is an open subset of the vector space \( \mathcal{H}(E) \) (16.11.3). Also, let \( U(E) \) denote the unitary group (isomorphic to \( U(n, \mathbb{C}) \)) of the form \( \Phi(x, y) = (x \mid y) \), the scalar product on \( E \). Then:

\[
(21.17.6)
\]

(i) The mapping \( H \mapsto \exp(H) \) is a diffeomorphism of \( a(E) \) onto the submanifold \( a_+(E) \) of \( GL(E) \subset \text{End}(E) \).

(ii) The mapping \( (H, U) \mapsto \exp(H) \cdot U \) is a diffeomorphism of \( a(E) \times U(E) \) onto the Lie group \( GL(E) \).

(Here \( \exp \) is the exponential mapping \( H \mapsto \sum_{n=0}^{\infty} \frac{1}{n!} H^n \) of the group \( GL(E) \) (19.8.7.2).)

(i) The fact that \( H \mapsto \exp(H) \) is a bijection of \( a(E) \) onto \( a_+(E) \) is a particular case of (15.11.11), applied to the function \( x \mapsto e^x \), which is a homeomorphism of \( \mathbb{R} \) onto \( \mathbb{R}^*_+ = ]0, +\infty[ \). To show that \( H \mapsto \exp(H) \) is a diffeomorphism of \( a(E) \) onto \( a_+(E) \), it is enough to prove that the tangent linear mapping \( T_H(\exp) \) is bijective for all \( H \in a(E) \) (16.8.8(iv)); by virtue of (19.16.6), this reduces to showing that no nonzero eigenvalue of the endomorphism \( \text{ad}(H) \) of \( \text{gl}(E) \) is of the form \( 2\pi i k \) with \( k \in \mathbb{Z} \). Now, relative to a suitably chosen orthonormal basis of \( E \), the matrix of \( H \) is a diagonal matrix \( (\lambda_1, \lambda_2, \ldots, \lambda_n) \), with \( \lambda_j \) real (11.5.7), and therefore by (19.4.2.2) we have

\[
(21.17.6.1) \quad \text{ad}(H) \cdot E_{jk} = (\lambda_j - \lambda_k)E_{jk} \]

for all the matrix units \( E_{jk} \) (\( 1 \leq j, k \leq n \)). This shows that the eigenvalues of \( \text{ad}(H) \) are the real numbers \( \lambda_j - \lambda_k \), and completes the proof of (i).

(ii) The relation \( X = \exp(H) \cdot U \), where \( H \in a(E) \) and \( U \in U(E) \), implies that \( X^* = U^* \cdot \exp(H) = U^{-1} \cdot \exp(H) \), and therefore

\[
XX^* = \exp(2H). \]

Now, for each automorphism \( X \in GL(E) \), \( XX^* \) is a positive self-adjoint automorphism of \( E \) (11.5.3). Hence, by virtue of (i) above, there exists a unique \( H \in a(E) \) satisfying the equation \( \exp(2H) = XX^* \), which we write as \( H = \frac{1}{2} \log(XX^*) \). If we put \( U = (\exp(H))^{-1} \cdot X \), it is immediately verified that we have \( UU^* = I \), that is to say, \( U \in U(E) \). Since \( H \mapsto \exp(H) \) is a diffeomorphism of \( a(E) \) onto \( a_+(E) \), and \( A \mapsto \log(A) \) is the inverse diffeomorphism, (ii) is established.
We now return to the determination of the positive self-adjoint automorphisms of \( g \). By virtue of (21.17.6), such an automorphism is uniquely expressible as \( \exp(H) \), where \( H \in \mathfrak{a}(g) \).

(21.17.7) For a self-adjoint endomorphism \( H \) of the vector space \( g \) (relative to the Hilbert space structure defined in (21.17.2)) to be such that \( \exp(H) \) is an automorphism of the Lie algebra \( g \), it is necessary and sufficient that \( H = \text{ad}(i\mathbf{u}) \) with \( \mathbf{u} \in \mathfrak{t} \).

To say that \( \exp(H) \in \text{Aut}(g) \) signifies that \( \left[ \exp(H) \cdot \mathbf{u}, \exp(H) \cdot \mathbf{v} \right] = \exp(H) \cdot [\mathbf{u}, \mathbf{v}] \) for all \( \mathbf{u}, \mathbf{v} \in g \), or equivalently

\[
\exp(H) \circ \text{ad}(\mathbf{u}) \circ \exp(H)^{-1} = \text{ad}(\exp(H) \cdot \mathbf{u})
\]

in \( \text{End}(g) \). If we put \( \mathfrak{m} = \mathfrak{ad}(g) \), this therefore implies (19.11.2.5) that

\[
(21.17.7.1) \quad \text{Ad}(\exp(H)) \cdot \mathfrak{m} \subseteq \mathfrak{m}
\]

in \( \mathfrak{gl}(g) = \text{End}(g) \), which can also be written (19.11.2.2) as

\[
(21.17.7.2) \quad \exp(\text{ad}(H)) \cdot \mathfrak{m} \subseteq \mathfrak{m},
\]

the exponential here being that of the group \( \text{GL}(\text{End}(g)) \). Relative to a suitably chosen orthonormal basis of \( g \), \( \text{ad}(H) \) acts on \( \text{End}(g) \) according to the formulas (21.17.6.1); hence, relative to the basis \( (E_k) \), its matrix is the diagonal matrix formed by the \( \lambda_j - \lambda_k \), and the matrix of \( \exp(\text{ad}(H)) \) is therefore the diagonal matrix formed by the \( e^{\lambda_j - \lambda_k} \). From this it follows that the subspaces of the vector space \( \text{End}(g) \) that are stable under \( \exp(\text{ad}(H)) \) are the same as those which are stable under \( \text{ad}(H) \) (A.24.3), and hence

\[
(21.17.7.3) \quad \text{ad}(H) \cdot \mathfrak{m} \subseteq \mathfrak{m}.
\]

This signifies also that \( X \mapsto [H, X] \) is a derivation of the Lie algebra \( \mathfrak{m} = \mathfrak{ad}(g) \); but \( \mathfrak{ad}(g) \) is isomorphic to \( g \), hence semisimple, and therefore every derivation of \( \mathfrak{ad}(g) \) is inner (21.6.7). In other words, there exists a unique \( \mathbf{u}_0 \in g \) such that, putting \( H_0 = \text{ad}(\mathbf{u}_0) \), we have \( [H - H_0, X] = 0 \) for all \( X \in \mathfrak{ad}(g) \). Since \( \mathfrak{ad}(g) \) is stable under the mapping \( X \mapsto X^* \) (21.17.3.2), we have also \( [H - H_0^*, X] = 0 \) for all \( X \in \mathfrak{ad}(g) \), because \( H \) is self-adjoint. From this we conclude that \( H_0^* = H_0 \) and therefore (21.17.3.2) \( c(\mathbf{u}_0) = -\mathbf{u}_0 \), that is to say, \( \mathbf{u}_0 \in \mathfrak{t} \). Since \( H_0 \in \mathfrak{ad}(g) \), we have \( [H, H_0] = 0 \), so that \( H \) and \( H_0 \) commute, and consequently

\[
\exp(H) = \exp(H - H_0) \exp(H_0);
\]

and clearly

\[
\exp(H_0) = \exp(\text{ad}(\mathbf{u}_0)) = \text{Ad}(\exp(\mathbf{u}_0)) \in \text{Aut}(g),
\]

so that the hypothesis \( \exp(H) \in \text{Aut}(g) \) implies that \( \exp(H - H_0) \in \text{Aut}(g) \).
Let \( \alpha_1, \ldots, \alpha_m \) be the distinct eigenvalues of the selfadjoint endomorphism \( Z = H - H_0 \) of the Hilbert space \( \mathfrak{g} \), and let \( \mathfrak{g}_1, \ldots, \mathfrak{g}_m \) be the corresponding eigenspaces, so that \( \mathfrak{g} \) is the Hilbert sum of the \( \mathfrak{g}_j \) (1 \( \leq j \leq m \)) (11.5.7). Since, for each \( u \in \mathfrak{g} \), \( \text{ad}(u) \) commutes with \( Z \) in \( \text{End}(\mathfrak{g}) \), we must have \( \text{ad}(u) \cdot \mathfrak{g}_j \subset \mathfrak{g}_j \) for 1 \( \leq j \leq m \); in other words, the \( \mathfrak{g}_j \) are ideals of the algebra \( \mathfrak{g} \). Moreover, for each \( x \in \mathfrak{g}_j \), we have \( \exp(Z) \cdot x = e^{2\alpha_j}x \); but since \( \exp(Z) \in \text{Aut}(\mathfrak{g}) \), we have \( e^{2\alpha_j}[x, y] = e^{2\alpha_j}[x, y] \). This is possible only if either \( \alpha_j = 0 \) or else \([x, y] = 0 \) for all \( x, y \in \mathfrak{g} \). The second alternative is ruled out by virtue of (21.6.2(i)), hence we have \( \alpha_j = 0 \) for all \( j \), which means that \( Z = 0 \); in other words, \( H = H_0 = \text{ad}(iu) \) with \( u \in \mathfrak{f} \). The converse follows immediately from (21.17.3.2) and (21.17.6(i)).

(21.17.8) The mapping \( (u, U) \mapsto \exp(\text{ad}(iu)) \cdot U \) is a diffeomorphism of \( \mathfrak{f} \times \text{Aut}(\mathfrak{f}) \) onto \( \text{Aut}(\mathfrak{g}) \).

Since \( \text{Aut}(\mathfrak{f}) \) consists of unitary endomorphisms of the Hilbert space \( \mathfrak{g} \) (21.17.4), and since \( u \mapsto \exp(\text{ad}(iu)) \) is a diffeomorphism of \( \mathfrak{f} \) onto a submanifold of the vector space of Hermitian endomorphisms of the Hilbert space \( \mathfrak{g} \) (21.17.6(i)), it follows from (21.17.6(ii)) that is enough to show that the image of the mapping \( (u, U) \mapsto \exp(\text{ad}(iu)) \cdot U \) of \( \mathfrak{f} \times \text{Aut}(\mathfrak{f}) \) into \( \text{GL}(\mathfrak{g}) \) is exactly equal to \( \text{Aut}(\mathfrak{g}) \). Now, if \( X \in \text{Aut}(\mathfrak{g}) \), then also \( X^* \in \text{Aut}(\mathfrak{g}) \) by virtue of (21.17.3.1) and (21.17.1.1); hence \( XX^* \in \text{Aut}(\mathfrak{g}) \). We have seen in (21.17.6(i)) that there exists a unique self-adjoint endomorphism \( H \) of the Hilbert space \( \mathfrak{g} \) such that \( \exp(2H) = XX^* \); it follows from (21.17.7) that \( H = \text{ad}(iu) \) with \( u \in \mathfrak{f} \), and the calculation made in the course of the proof of (21.17.6(ii)) then shows that \( U = (\exp(H))^{-1}X \) is unitary; but since \( U \in \text{Aut}(\mathfrak{g}) \), it follows from (21.17.4) that \( U \in \text{Aut}(\mathfrak{f}) \) and therefore \( X = \exp(\text{ad}(iu)) \cdot U \). The converse inclusion is obvious from the identification of \( \text{Aut}(\mathfrak{f}) \) with a subgroup of \( \text{Aut}(\mathfrak{g}) \).

(21.17.9) The mapping \( (u, U) \mapsto \exp(\text{ad}(iu)) \cdot U \) is a diffeomorphism of \( \mathfrak{f} \times \text{Ad}(\mathfrak{K}) \) onto \( \text{Ad} (\mathfrak{G}) \).

This follows from the fact that \( \mathfrak{f} \) is connected and therefore \( \mathfrak{f} \times \text{Ad}(\mathfrak{K}) \) is the identity component of \( \mathfrak{f} \times \text{Aut}(\mathfrak{f}) \).

(21.17.10) Let \( \pi : \mathfrak{G} \rightarrow \mathfrak{G} = \text{Ad}(\mathfrak{G}) \) denote the canonical projection (so that \( \pi(s) = \text{Ad}(s) \)).

(i) The inverse image \( \pi^{-1}(K) \) (where \( K = \text{Ad}(\mathfrak{K}) \)) may be identified with the simply connected compact group \( \mathfrak{K} \), and with the Lie subgroup of \( \mathfrak{G}_{\mathfrak{K}} \) corresponding to the Lie subalgebra \( \mathfrak{f}_{\mathfrak{K}} \) \( \mathfrak{G} \) (19.7.4); in particular, the center \( C \) of \( \mathfrak{K} \) may be identified with the center of \( \mathfrak{G} \).
(ii) The mapping $i u \mapsto \exp_G(i u)$ is a diffeomorphism of the vector subspace $i \mathfrak{g}$ onto a submanifold $\tilde{P}$ of $\tilde{G}$, such that $\tilde{P} \cap \tilde{K} = \{ \tilde{e} \}$ (the identity element of $\tilde{G}$).

(iii) The mapping $(y, z) \mapsto yz$ of $P \times K$ into $G$ is a diffeomorphism of $P \times K$ onto $G$.

Let $P$ be the image of $i \mathfrak{g}$ in $G$ under the mapping $i u \mapsto \exp_G(i u)$, which is the same as the mapping $i u \mapsto \exp(\mathrm{ad}(i u))$ by definition of $G = \mathrm{Ad}(\tilde{G})$; $P$ is therefore a submanifold of $G$ diffeomorphic to it. If $\tilde{P}$ is the connected component of $\tilde{e}$ in $\pi^{-1}(P)$, then $\tilde{P}$ is a covering of $P$ ((16.12.9) and (16.28.6)); but since $P$, being homeomorphic to a vector space, is simply connected, the restriction of $\pi$ to $\tilde{P}$ is a diffeomorphism of $\tilde{P}$ onto $P$ (16.28.6), and the intersection $\tilde{P} \cap \pi^{-1}(e)$ of $\tilde{P}$ and the center of $\tilde{G}$ consists only of the identity element. Furthermore, for each $u \in \mathfrak{g}$ we have $\pi(e^{[i u]}(e)) = e^{\exp_G(i u)}$; since the one-parameter subgroup of $G$ that is the image of $\mathfrak{g}$ under the mapping $t \mapsto e^{\exp_G(i u)}$ is connected, we have $\exp_G(i u) \in \tilde{P}$, and consequently $\tilde{P}$ is the image of $i \mathfrak{g}$ under the restriction to $\mathfrak{g}$ of the mapping $\exp_G$, which is a diffeomorphism.

Consider now the Lie subgroup $K' = \pi^{-1}(K)$, which is a covering of $K$ and contains the center $\pi^{-1}(e)$ of $\tilde{G}$. We shall show that every $x \in \tilde{G}$ can be written uniquely in the form $yz$ with $y \in \tilde{P}$ and $z \in K'$. We have $\pi(x) = y_0 z_0$ with $y_0 \in P$ and $z_0 \in K$, and this decomposition is unique (21.17.9); we may write $y_0 = \pi(y)$ and $z_0 = \pi(z')$, with $y \in \tilde{P}$ and $z' \in K'$; hence $x = yz'w$, where $w \in \pi^{-1}(e)$; but since $\pi^{-1}(e) \subset K'$, it follows that $z = z'w \in K'$ and we have $x = yz$ as required. As to the uniqueness of this factorization, if $x = y_1 z_1$ with $y_1 \in \tilde{P}$ and $z_1 \in K'$, then $\pi(y_1)\pi(z) = \pi(y_1)\pi(z_1)$, whence $\pi(y) = \pi(y_1)$ (21.17.9), which as above implies that $y_1 = y$ and therefore $z_1 = z$.

Next we shall show that the bijection $(y, z) \mapsto yz$ of $\tilde{P} \times K'$ onto $\tilde{G}$ is a diffeomorphism. If $(a, b) \in \tilde{P} \times K'$ and $c = ab$, there exist open neighborhoods $U$, $V$, $W$ of $a$ in $\tilde{P}$, $b$ in $K'$, and $c$ in $\tilde{G}$, respectively, such that the restrictions of $\pi$ to $U$, $V$, $W$ are diffeomorphisms onto the open sets $\pi(U)$, $\pi(V)$, $\pi(W)$ in $P$, $K$, and $G$, respectively. Since we may assume that $U$ and $V$ are so small that the mapping $(y_0, z_0) \mapsto y_0 z_0$ of $\pi(U) \times \pi(V)$ into $\pi(W)$ is a diffeomorphism onto an open subset of $\pi(W)$ (21.17.9), the result now follows immediately.

We see therefore that $\tilde{P} \times K'$ is diffeomorphic to $\tilde{G}$. This implies that $K'$ is simply connected (16.27.10), hence isomorphic to $\tilde{K}$. If we identify $\tilde{K}$ with $K'$, the center of $\tilde{K}$ contains $\pi^{-1}(e)$, and since $K = \tilde{K} / \pi^{-1}(e)$ has center $\{ e \}$, it follows that $\pi^{-1}(e)$ is in fact the center $C$ of $\tilde{K}$ (20.22.5.1).

(21.17.11) It is now easy to deduce from (21.17.10) the determination of all the complex connected Lie groups that have $\mathfrak{g}$ as Lie algebra. Indeed, such a
group is isomorphic to a quotient $G_1 = \tilde{G}/D$ of $\tilde{G}$ by a subgroup $D$ of its (finite) center $C$ (16.30.4); the center $C_1$ of $G_1$ is $C/D$. If $\pi_1 : G_1 \to G = G_1/C_1$ is the canonical projection, then $\pi_1^{-1}(K)$ may be identified with the compact group $K_1 = \tilde{K}/D$ with center $C_1$, and $K$ with $K_1/C_1$. We may therefore repeat without any changes the argument of (21.17.10); if $P_1$ is the connected component of the identity element $e_1$ of $G_1$ in $\pi^{-1}(P)$, the restriction of $\pi_1$ to $P_1$ is a diffeomorphism of $P_1$ onto $P$, and $iu \mapsto \exp_G(iu)$ is a diffeomorphism of $it$ onto $P_1$. We have $P_1 \cap K_1 = \{e_1\}$, and the mapping $(y, z) \mapsto yz$ is a diffeomorphism of $P_1 \times K_1$ onto $G_1$.

There is therefore a canonical one-to-one correspondence between the compact connected semisimple Lie groups with Lie algebra $\mathfrak{t}$, and the complex connected semisimple Lie groups with Lie algebra $\mathfrak{g}_0 = \mathfrak{g}$.

(21.17.12) (i) The exponential mapping of $G$ maps $\mathfrak{t}$ onto $\tilde{K}$ (21.7.4) and $it$ onto $\tilde{P}$; nevertheless, it is not necessarily a surjection of $\mathfrak{g} = \mathfrak{t} \oplus it$ onto $\tilde{G}$ (Section 19.8, Problem 2).

(ii) With the notation of (21.17.11), the subgroup $K_1$ is maximal among the compact subgroups of $G_1$. For if an element $yz$, with $y \in P_1$ and $z \in K_1$, belongs to a compact subgroup $K_1 \supset K_1$, then $y \in K_1'$; but if $y = \exp(iu)$ with $u \in \mathfrak{t}$, the subgroup of $G_1$ generated by $y$ is the image under the exponential mapping of the subgroup $Z_iu$ of $\mathfrak{t}$; this subgroup is closed and not compact in $it$ if $u \neq 0$, and therefore the subgroup generated by $y$ would also be closed and noncompact in $K_1'$, which is impossible. Hence we must have $u = 0$ and therefore $K_1' = K_1$.

PROBLEMS

1. Let $G_o$ be a connected (real) Lie group, $\mathfrak{g}_0$ its Lie algebra, $\mathfrak{g} = \mathfrak{g}_0 \otimes \mathbb{C}$ the complexification of $\mathfrak{g}_0$, and $G$ the simply connected complex Lie group with Lie algebra $\mathfrak{g}$ (21.23.4). If $\tilde{G}_o$ is the simply connected universal covering Lie group of $G_o$, then the canonical injection $\mathfrak{g}_0 \to \mathfrak{g}_\mathbb{C}$ is the derived homomorphism of a unique homomorphism $h: \tilde{G}_o \to H_{\mathbb{C}}$. For each Lie group homomorphism $u: G_o \to H_{\mathbb{C}}$ of complex Lie groups, there exists a unique homomorphism $u^*: G \to H$ of complex Lie groups such that $u^* \circ h = u \circ p$, where $p: \tilde{G}_o \to G_o$ is the canonical homomorphism. Let $G^+$ be the quotient of $G$ by the intersection $N$ of the kernels of the homomorphisms $u^*$ corresponding to all homomorphisms $u: G_o \to H_{\mathbb{C}}$. Show that if $D$ is the kernel of $p$, then $h(D) \subset N$. (Consider the composite homomorphism $G_o \xrightarrow{\alpha} \text{Aut}(\mathfrak{g}_0) \to \text{Aut}(\mathfrak{g}_\mathbb{C})$.) Deduce that there exists a canonical homomorphism $\varphi: G_o \to G_+^*$ such that every homomorphism $u: G_o \to H_{\mathbb{C}}$ (where $H$ is a complex Lie group) factorizes uniquely as $G_o \xrightarrow{\varphi} G_+^* \xrightarrow{u^*} H_{\mathbb{C}}$, where $u^*: G^+ \to H$ is a homomorphism of complex Lie groups.
Show that if there exists an injective homomorphism \( u: G_0 \to H_{\mathbb{R}} \), where \( H \) is a complex Lie group, then the homomorphism \( \varphi: G_0 \to G_{\mathbb{R}}^+ \) is injective and \( g \) is the Lie algebra of \( G^+ \); the group \( G^+ \) is said to be the complexification of \( G_0 \). If we identify \( G_0 \) with a subgroup of \( G_{\mathbb{R}}^+ \), there exists no complex Lie subgroup of \( G^+ \) containing \( G_0 \), other than \( G^+ \) itself.

2. Let \( K \) be a compact connected Lie group of dimension \( n \), which we may assume to be a subgroup of \( O(N, \mathbb{R}) \) (21.13.1); \( K \) is then the set of real matrices whose components are the zeros of some family of polynomials in \( \mathbb{R}[T_{11}, T_{12}, \ldots, T_{nn}] \) (Section 21.13, Problem 2). Let \( a \) denote the ideal of \( \mathbb{R}[T_{11}, \ldots, T_{nn}] \) formed by the polynomials that vanish at all points of \( K \).

(a) Let \( G \) be the set of complex matrices in \( \text{GL}(N, \mathbb{C}) \) for which all the polynomials in \( a \) vanish; \( G \) is also the set of complex matrices for which the polynomials in the ideal \( a^+ = a + ia \) in \( \mathbb{C}[T_{11}, \ldots, T_{nn}] \) vanish. Show that \( G \) is a closed subgroup of \( \text{GL}(N, \mathbb{C}) \).

(First prove that if \( s \in K \) and \( t \in G \), then \( st \in G \).) We have \( K = G \cap \text{GL}(N, \mathbb{R}) = G \cap \text{O}(N, \mathbb{R}) = G \cap U(N, \mathbb{C}) = \text{O}(N, \mathbb{R}) \).

(b) If \( X \) is a matrix belonging to \( G \), then \( \overline{X} \) also belongs to \( G \). If we write \( X = HU \), where \( U \) is unitary and \( H \) is hermitian and positive definite (21.17.6), then the matrices \( H, U \) also belong to \( G \). (Note that \( H^2 = XX^* \in G \) and therefore \( H^{2k} \in G \) for all integers \( k \in \mathbb{Z} \).)

If we write \( H = A \cdot \exp(D) \cdot A^{-1} \) where \( D = \text{diag}(a_1, \ldots, a_n) \), the \( a_j \) being real, then for each polynomial \( P \in a^+ \) and each \( z \in \mathbb{C} \), \( P(A \cdot \exp(zD) \cdot A^{-1}) \) is a linear combination of exponentials \( e^{cz} \) with \( c \in \mathbb{R} \). By observing that this function of \( z \) vanishes for all \( z \in 2\mathbb{Z} \), show that it vanishes identically, and hence in particular is zero for \( z = 1 \). If \( S = ADA^{-1} \), so that \( H = \exp(S) \), then \( \exp(zS) \in G \) for all \( z \in \mathbb{C} \).

(c) Let \( S \) be a hermitian matrix. Show that \( \exp(S) \in G \) if and only if \( iS \in \mathfrak{l} \), the Lie algebra of \( K \). (Observe that if \( \exp(itS) \) is a zero of all the polynomials in \( a \), where \( t \in \mathbb{R} \), then the same is true of \( \exp(zS) \) for \( z \in \mathbb{C} \).) Deduce from (b) above and from (21.17.6) that \( G \) is diffeomorphic to \( K \times \mathbb{R}^n \) and that its Lie algebra is \( \mathfrak{l} \oplus \mathbb{R}^n \). The group \( G \) may therefore be identified with the complexification of the compact group \( K \); its Lie algebra \( \mathfrak{g} \) is the direct sum of its center \( \mathfrak{c} \) and its derived algebra \( \mathfrak{d}(\mathfrak{g}) \), which is semisimple, and the universal covering \( \hat{G} \) of \( G \) is therefore isomorphic to the product of \( \mathbb{C}^m \) (for some positive integer \( m \)) and a complex semisimple Lie group, which is the complexification of a compact semisimple Lie group.

18. REAL FORMS OF THE COMPLEXIFICATIONS OF COMPACT CONNECTED SEMISIMPLE GROUPS AND SYMMETRIC SPACES

(21.18.1) We have already observed in two contexts ((21.8.2) and (21.17.1)) that if \( a \) is a real Lie algebra and \( b = a(\mathbb{C}) \) is its complexification, then the bijection \( c: y + iz \mapsto y - iz \) of \( b \) onto itself (where \( y, z \in a \)) is a semilinear involution that satisfies the relation \( c([u, v]) = [c(u), c(v)] \) for all \( u, v \in b \) (i.e., it is an automorphism of the real Lie algebra \( b_{\mathbb{R}} \)). For the sake of brevity, a bijection of a complex Lie algebra \( b \) onto itself that has these properties will be called a conjugation. Conversely, a conjugation \( c \) in a complex Lie algebra \( b \) determines uniquely a real Lie subalgebra \( a \) of \( b_{\mathbb{R}} \) such that \( b \) is isomorphic to the complexification of \( a \). For since \( c \) is \( \mathbb{R} \)-linear
and \( c^2 = 1_b \), the vector space \( b_{\mathbb{R}} \) is the direct sum \( \alpha \oplus \alpha' \) of two real vector subspaces \( \alpha, \alpha' \), such that \( c(u) = u \) for \( u \in \alpha \), and \( c(u) = -u \) for \( u \in \alpha' \). Since also \( c(iu) = -ic(u) \) for all \( u \in b \), we have \( ia \subset \alpha' \) and \( ia \subset \alpha \), from which it follows that \( \alpha' = ia \). Finally, since \( c \) is an automorphism of \( b_{\mathbb{R}} \), the subspace \( \alpha \) is a Lie subalgebra of \( b_{\mathbb{R}} \), and it is immediately seen that \( b \) is the complexification of \( \alpha \). There is therefore a canonical one-to-one correspondence between conjugations of \( b \) and real forms of \( b \). Further, if \( \varphi \) is an automorphism of the complex Lie algebra \( b \), and \( c \) is a conjugation of \( b \), it is clear that \( \varphi \circ c \circ \varphi^{-1} = c_1 \) is also a conjugation of \( b \), and that if \( \alpha \) and \( \alpha_1 \) are the real forms of \( b \) corresponding to \( c \) and \( c_1 \), respectively, then \( \alpha_1 = \varphi(\alpha) \).

(21.18.2) Changing the notation of (21.17), let \( \tilde{G}_u \) be a simply connected compact semisimple Lie group, \( g_u \) its Lie algebra, \( g = (g_u)_{c_u} \) the complexification of \( g_u \), and \( c_u \) the conjugation of \( g \) corresponding to \( g_u \). We propose to determine, up to isomorphism, all the real forms of the complex semisimple algebra \( g \), and we shall show that this is equivalent to the following problem relative to the algebra \( g_u \): to determine the involutory automorphisms of this Lie algebra.

This will result from the following proposition:

(21.18.3) With the notation of (21.18.2), let \( c \) be a conjugation of \( g \). Then there exists an automorphism \( \varphi \) of \( g \) such that \( c \) commutes with \( \varphi \circ c \circ \varphi^{-1} \).

We have seen (21.17.2.1) that \( (x | y) = -B_g(x, c_u(y)) \) is a scalar product that makes \( g \) a finite-dimensional Hilbert space. The mapping \( H = cc_u \) is an automorphism of the complex Lie algebra \( g \); it is also a self-adjoint endomorphism of the Hilbert space \( g \), because we have

\[
B_g(H \cdot x, c_u \cdot y) = B_g(x, H^{-1} c_u \cdot y) = B_g(x, c_u H \cdot y)
\]

since \( H \) leaves invariant the Killing form of \( g_u \), and \( c, c_u \) are involutions. Hence there exists an orthonormal basis \( (e_j)_{1 \leq j \leq n} \) of \( g \) with respect to which the matrix of \( H \) is diagonal and invertible. Consequently the matrix of \( H^2 = A \) with respect to this basis is of the form \( \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) \), where the \( \lambda_j \) are real and \( > 0 \). For each real number \( t > 0 \), let \( A^t \) be the automorphism of the vector space \( g \) defined by the matrix \( \text{diag}(\lambda_1^t, \lambda_2^t, \ldots, \lambda_n^t) \) (cf. (15.11.11)); these automorphisms commute with \( H \), and moreover they are automorphisms of the complex Lie algebra \( g \). For if the multiplication table of \( g \), relative to the basis \( (e_j) \), is

\[
[e_j, e_k] = \sum_l a_{jkl} e_l
\]
then the fact that \( A \) is an automorphism of \( g \) is expressed by the relations
\[
\lambda_j \lambda_k a_{jkl} = a_{jkl} \lambda_i \quad (1 \leq j, k, l \leq n),
\]
which evidently imply, for all \( t > 0 \), that
\[
\lambda_j \lambda_k a_{jkl} = a_{jkl} \lambda_i,
\]
thereby proving our assertion. Now consider the conjugation \( c' = A'c_u A^{-t} \) of \( g \), and note that by definition we have \( c_u H c_u^{-1} = c_u c = H^{-1} \), so that \( c_u A c_u^{-1} = A^{-1} \). But if we put \( L = \text{diag}(\log \lambda_1, \log \lambda_2, \ldots, \log \lambda_n) \), then \( A = e^L \), so that \( A' = e^{tL} \) and therefore \( c_u A c_u^{-1} = A^{-1} \). Consequently
\[
cc' = cA'c_u A^{-2t} = HA^{-2t},
\]
\[
c'c = (cc')^{-1} = A^{2t}H^{-1} = H^{-1}A^{2t},
\]
and therefore when \( t = \frac{1}{4} \) we have \( cc' = c'c = H^{-1}A^{1/2} \), because \( HA^{-1} = H^{-1} \). Hence \( \varphi = A^{-1/4} \) satisfies the conditions of the proposition.

(21.18.4) In the determination of all conjugations of \( g \), we may therefore limit our search to conjugations \( c_0 \) that commute with \( c_u \), and therefore leave \( g_u \) and \( ig_u \) globally invariant. The restriction of \( c_0 \) to \( g_u \) is then an involutory automorphism of this real Lie algebra. Consequently, \( g_u \) is the direct sum of a real Lie subalgebra \( f_0 \), consisting of the \( x \in g_u \) such that \( c_0(x) = x \), and a real vector subspace, denoted by \( p_0 \), consisting of the \( x \in g_u \) such that \( c_0(x) = -x \). It follows that \( ig_u \) is the direct sum of \( if_0 \) and \( p_0 \), and because \( c_0 \) is a conjugation of \( g \) we have \( c_0(x) = x \) for \( x \in p_0 \) and \( c_0(x) = -x \) for \( x \in if_0 \). The real form \( g_0 \) of \( g \) corresponding to \( c_0 \) is therefore
\[
(21.18.4.1) \quad g_0 = f_0 \oplus p_0.
\]

Since the Killing form \( B_{g_u} \) is the restriction of \( B_g \) to \( g_u \times g_u \), it follows from the definition of the scalar product \( \langle x, y \rangle \) on \( g \) that \( \langle x, y \rangle = -B_{g_u}(x, y) \) for \( x, y \in g_u \). Since the restriction of \( c_0 \) to \( g_u \) is an automorphism of this Lie algebra, it leaves invariant its Killing form \((21.5.6)\); for \( x \in f_0 \) and \( y \in p_0 \), we have therefore \( \langle x, y \rangle = (c_0(x) | c_0(y)) = -\langle x, y \rangle \), whence \( \langle x, y \rangle = 0 \). It follows that \( B_{g_u}(x, y) = 0 \) and hence also \( B_0(x, iy) = 0 \). Since the Killing form \( B_{g_0} \) is the restriction of \( B_g \), it follows that in the decomposition \((21.18.4.1)\), \( f_0 \) and \( p_0 \) are orthogonal subspaces relative to the Killing form of \( g_0 \) (hence are nonisotropic). Further, the restriction of \( B_{g_0} \) to \( f_0 \times f_0 \) is negative definite, because it is also the restriction of \( B_{g_u} \) \((21.6.9)\); by contrast, its restriction to \( p_0 \times p_0 \) is positive definite, because for \( x \in ip_0 \) we have \( B_{g_0}(ix, ix) = B_0(ix, ix) = -B_0(x, x) = -B_{g_u}(x, x) \). Finally, we have
\[
(21.18.4.2) \quad [f_0, p_0] \subset p_0, \quad [p_0, p_0] \subset f_0.
\]
For if \( x \in t_0 \) and \( y \in ip_0 \), then \( c_0([x, y]) = [c_0(x), c_0(y)] = -[x, y] \), and since \([x, y] \in g_u\) we have \([x, y] \in ip_o\); this shows that \([t_0, ip_o] \subset ip_o\) and therefore also that \([t_0, p_o] \subset p_o\). Likewise, if \( x, y \in ip_o \), then \( c_0([x, y]) = [x, y] \) and hence \([x, y] \in t_0 \), because \([x, y] \in g_u\); this proves the relation \([ip_o, ip_o] \subset t_0 \), whence \([p_o, p_o] \subset t_o \).

(21.18.5) Let \( \tilde{G} \) be the simply connected complex (semisimple) Lie group of which \( g \) is the Lie algebra (19.11.9), and let \( \tilde{P} \) be the closed submanifold of \( \tilde{G} \) that is the image of \( ig_u \) under the mapping \( iu \mapsto \exp \tilde{G}(iu) \). From (21.17.10), the mapping \( (y, z) \mapsto yz \) of \( \tilde{P} \times \tilde{G}_u \) into \( \tilde{G} \) is a diffeomorphism.

To the automorphism \( c_0 \) of the real Lie algebra \( g_{\mathbb{R}} \) there corresponds a unique involutory automorphism \( \sigma \) of \( \tilde{G}_{\mathbb{R}} \) such that the derived automorphism \( \sigma_* = c_0 \) (19.7.6); \( \sigma \) therefore leaves \( \tilde{G}_u \) and \( \tilde{P} \) stable, because \( c_0 \) leaves \( g_u \) and \( ig_u \) stable. Let \( G_0 \) be the Lie subgroup of \( \tilde{G}_{\mathbb{R}} \) consisting of the points fixed by \( \sigma \) (19.10.1); its Lie algebra is \( g_0 \) (20.4.3), hence is semisimple, and it evidently contains the compact subgroup \( K_0 = G_0 \cap \tilde{G}_u \) consisting of the fixed points of the restriction of \( \sigma \) to \( G_u \), because \( \tilde{G}_u \) is stable under \( \sigma \). Likewise, \( G_0 \) contains the image \( P_0 \) under the exponential mapping \( u \mapsto \exp \tilde{G}(u) = \exp_{G_0}(u) \) of the vector subspace \( p_0 \) of \( ig_u \), and since \( \exp(c_0(u)) = \sigma(\exp(u)) \), \( P \) is the set of points of \( \tilde{P} \) fixed by \( \sigma \). Furthermore:

(21.18.5.1) \( P_0 \) is a closed submanifold of \( G_0 \); the mapping \( u \mapsto \exp_{G_0}(u) \) is a diffeomorphism of \( p_0 \) onto \( P_0 \), and the mapping \( (y, z) \mapsto yz \) of \( P_0 \times K_0 \) into \( G_0 \) is a diffeomorphism of \( P_0 \times K_0 \) onto \( G_0 \).

The first two assertions are obvious, since \( p_0 \) is a vector subspace (and hence a closed submanifold) of \( ig_u \). Again, it is clear that the restriction to \( P_0 \times K_0 \) of the diffeomorphism \( (y, z) \mapsto yz \) of \( \tilde{P} \times \tilde{G}_u \) onto \( \tilde{G} \) is a diffeomorphism onto its image in \( \tilde{G} \), and it remains to show that this image is the whole of \( G_0 \). Each element \( x \in G_0 \) is uniquely expressible in the form \( yz \) with \( y \in \tilde{P} \) and \( z \in \tilde{G}_u \); since \( \sigma(x) = x \), we have \( \sigma(y) \sigma(z) = yz \), and since \( \sigma(y) \in \tilde{P} \) and \( \sigma(z) \in \tilde{G}_u \), we must have \( y = \sigma(y) \) and \( z = \sigma(z) \), whence \( y \in P_0 \) and \( z \in K_0 \).

(21.18.5.2) If \( C \) is the center of \( \tilde{G} \) (identified with the center of \( \tilde{G}_u \) (21.17.10)), the center of \( G_0 \) is \( C \cap G_0 \).

For if \( s \in G_0 \), the restriction of \( \text{Ad}(s) \) to \( g_0 \) is the identity if and only if the restriction of \( \text{Ad}(s) \) to \( g \) is the identity, because \( g \) is the complexification of \( g_0 \); the result therefore follows from (19.11.6).
(21.18.6) It can be proved that the compact group $K_0$ is connected (Section 21.16, Problem 11); we shall assume this result in the rest of this section. On the other hand, $K_0$ is not necessarily semisimple or simply connected. The group $G_0$ is therefore connected, and the same reasoning as in (21.17.10), with $G$ replaced by $G_0$, and $\hat{G}$ by $\hat{G}_0$, the universal covering group of $G_0$, shows that:

(21.18.7) The inverse image $\pi^{-1}(K_0)$ of $K_0$ under the canonical projection $\pi$ of $\hat{G}_0$ onto $G_0$ is isomorphic to the simply connected group $K_0$, the universal covering of the compact group $K_0$. The mapping $u \mapsto \exp_{G_0}(u)$ is a diffeomorphism of $\mathfrak{p}_0$ onto a closed submanifold $\mathfrak{p}$ of $\mathfrak{g}_0$, such that $\mathfrak{p} \cap K_0$ consists only of the identity element of $\hat{G}_0$. The mapping $(y, z) \mapsto yz$ is a diffeomorphism of $\mathfrak{p} \times K_0$ onto $G_0$.

The center $Z$ of $\hat{G}_0$ is $\pi^{-1}(C_0)$, a discrete subgroup contained in the center of $\hat{K}_0$, but distinct from the latter if $K_0$ is not semisimple (in which case $\hat{K}_0$ is not compact (21.6.9)).

(21.18.8) Finally, the reasoning of (21.17.11) gives the determination (up to isomorphism) of all the connected real Lie groups that have $\mathfrak{g}_0$ as their Lie algebra: such a group is isomorphic to a quotient $G_1 = \hat{G}_0 / D$, where $D$ is a (discrete) subgroup of the center $Z$ of $\hat{G}_0$, and the center $C_1$ of $G_1$ is $Z / D$. If $\pi_1 : G_1 \to \text{Ad}(G_0) = G_1 / C_1$ is the canonical projection, $\pi_1^{-1}(\text{Ad}(K_0))$ may be identified with the group $K_1 = \hat{K}_0 / D$, the connected Lie subgroup of $G_1$ with Lie algebra $\mathfrak{l}_0$; it contains $C_1$ (which is not in general the center of $K_1$), and is compact if and only if $C_1$ is finite. If $P_1$ is the connected component of the identity element $e_1 \in G_1$ in $\pi_1^{-1}(\text{Ad}(P_0))$, the restriction of $\pi_1$ to $P_1$ is a diffeomorphism of $P_1$ onto $\text{Ad}(P_0)$, and $u \mapsto \exp_{G_1}(u)$ is a diffeomorphism of $\mathfrak{p}_0$ onto $P_1$; we have $P_1 \cap K_1 = \{e_1\}$, and the mapping $(y, z) \mapsto yz$ is a diffeomorphism of $P_1 \times K_1$ onto $G_1$.

The decomposition (21.18.4.1) is called the Cartan decomposition of the semisimple real Lie algebra $\mathfrak{g}_0$. The corresponding decomposition as a product $P_1 \times K_1$, for a connected Lie group $G_1$ having $\mathfrak{g}_0$ as its Lie algebra, is called a Cartan decomposition of $G_1$. Since $\text{Ad}(K_0) = \text{Ad}(K_1)$ is compact, $K_1$ is in any case isomorphic to the product of a compact group and a vector group $R^m$ (21.6.9), hence $G_1$ is diffeomorphic to the product of a compact group and a vector group $R^N$; and the same argument as in (21.17.12) proves that the compact subgroup in this product decomposition is maximal in $G_1$.

† We shall not make use of this result anywhere except in this section.
18. REAL FORMS 169

Examples

(21.18.9) Consider a Weyl basis of $\mathfrak{g}$ (21.10.6), consisting of a basis of a maximal commutative subalgebra $t$ of $\mathfrak{g}_u$, together with elements $x_\alpha (\alpha \in S)$ satisfying (21.10.6.4). Since the numbers $N_{\alpha, \beta}$ are real, it is clear that the real vector subspace $\mathfrak{g}_0$ of $\mathfrak{g}$ spanned by this Weyl basis is a real Lie algebra having $\mathfrak{g}$ as its complexification; this real Lie algebra is called a normal real form of $\mathfrak{g}$. One sees immediately that in the corresponding Cartan decomposition $\mathfrak{g}_0 = t_0 + p_0$, the elements $x_\alpha - x_{-\alpha}$ form a basis of $t_0$, the subspace $p_0$ contains $t$ and is spanned by $t$ and the elements $x_\alpha + x_{-\alpha}$.

(21.18.10) Consider the complex Lie group $H = \hat{G} \times \hat{G}$, whose Lie algebra is $\mathfrak{g} \oplus \mathfrak{g}$, the complexification of the Lie algebra $\mathfrak{g}_u \oplus \mathfrak{g}_u$ of $G_u \times G_u$. Let $c_0$ be the conjugation of $\mathfrak{g} \oplus \mathfrak{g}$ defined by

$$c_0(\mathbf{x} + i\mathbf{y}, \mathbf{x}' + i\mathbf{y}') = (\mathbf{x}' - i\mathbf{y}', \mathbf{x} - i\mathbf{y})$$

for $\mathbf{x}, \mathbf{y}, \mathbf{x}', \mathbf{y}' \in \mathfrak{g}_u$. It is clear that the set of $(\mathbf{v}, \mathbf{w}) \in \mathfrak{g} \oplus \mathfrak{g}$ fixed by $c_0$ is the set of elements $(\mathbf{z}, c_u(\mathbf{z}))$ for $\mathbf{z} \in \mathfrak{g}$, and hence is isomorphic to $\mathfrak{g}_{\mathbb{R}}$. In this way the Lie algebra $\mathfrak{g}_{\mathbb{R}}$ appears as a real form of $\mathfrak{g} \oplus \mathfrak{g}$; the corresponding Cartan decomposition $t_0 \oplus p_0$ is such that $t_0 = \mathfrak{g}_u$ and $p_0 = i\mathfrak{g}_u$.

(21.18.11) Let us take $\hat{G}_u$ to be the almost simple compact group $SU(n)$ (21.12.1), which is simply connected (16.30.6). We have seen in (21.12.1) that the complexification $\mathfrak{g}$ of $\mathfrak{g}_u = \mathfrak{su}(n)$ may be identified with $\mathfrak{sl}(n, \mathbb{C})$. We shall show that the corresponding group $SL(n, \mathbb{C})$ is simply connected. By virtue of (21.17.6), $SL(n, \mathbb{C})$ is diffeomorphic to the submanifold of $a(\mathbb{C}^n) \times U(n)$ consisting of pairs of matrices $(H, U)$ such that det(exp$(H)) \cdot$ det$(U) = 1$, or equivalently $e^{\text{Tr}(H)} \cdot$ det$(U) = 1$; since $\text{Tr}(H)$ is a real number, and the only unitary matrices with a positive real determinant are those with determinant 1, it follows that $SL(n, \mathbb{C})$ is diffeomorphic to $V \times SU(n)$, where $V$ is the hyperplane in $a(\mathbb{C}^n)$ defined by the equation $\text{Tr}(H) = 0$. This proves our assertion (16.27.10); the group denoted by $\hat{G}$ in (21.18.5) is here $SL(n, \mathbb{C})$.

The conjugation $c_u$ corresponding to the real form $\mathfrak{g}_u$ is the involutory bijection $X \mapsto -\mathbf{X}$ of $\mathfrak{sl}(n, \mathbb{C})$ onto itself. Among the conjugations of $\mathfrak{g}$ that commute with $c_u$, there are the following three types:

(I) $c_0: X \mapsto \mathbf{X};$ $\mathfrak{g}_0$ is therefore the set of real matrices in $\mathfrak{sl}(n, \mathbb{C})$, hence is the Lie algebra $\mathfrak{sl}(n, \mathbb{R})$ (the normal real form of $\mathfrak{sl}(n, \mathbb{C})$ (21.18.9)); the subalgebra $t_0$ of $\mathfrak{g}_u$ is the set of real matrices in $\mathfrak{su}(n)$, so that $\mathfrak{g}_u = \mathfrak{so}(n)$ and therefore is semisimple if $n \geq 3$ ((21.12.3) and (21.12.4)); $p_0$ is the space of
real symmetric $n \times n$ matrices with trace 0, and $P_0$ is the set of positive definite real symmetric matrices with determinant 1. The automorphism $\sigma$ of $\mathcal{G}_G$ is again the mapping $X \mapsto X$ on $SL(n, C)$, and therefore we have $G_0 = SL(n, R)$ and $K_0 = SO(n)$. When $n = 2$, $K_0$ is isomorphic to $T$, and $K_0$ to $R$, so that $G_0$, the universal covering of $SL(2, R)$, is diffeomorphic to $R^3$; when $n \geq 3$, the group $K_0$ is not simply connected, and $K_0$ is isomorphic to $Spin(n)$ (21.16.10); hence $G_0$ has finite center, but it can be shown that $G_0$ is not isomorphic to any Lie subgroup of a linear group $GL(N, R)$ (Problem 1).

(II) Suppose that $n = 2m$ is even, and consider the mapping $c_0$: $X \mapsto JXJ^{-1}$, where

$$J = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix};$$

Since $J = J$ and $J^{-1} = -J = 'J$, it is immediately verified that $c_0$ is a conjugation that commutes with $c_u$. The corresponding automorphism $\sigma$ of $\mathcal{G}_G = SL(2m, C)$ is the same mapping $X \mapsto JXJ^{-1}$, and it is easily verified that the matrices fixed by $\sigma$ are the matrices in $SL(2m, C)$ of the form (21.12.2.2), in other words, the matrices of the form $\begin{pmatrix} U & V \\ -V & U \end{pmatrix}$ of determinant 1, with $U$ and $V$ in $GL(m, C)$. It follows therefore from (21.12.2) that $K_0$ is semisimple and simply connected, and is isomorphic to $U(m, H)$; the group $G_0$ is therefore simply connected and may be identified with the intersection of $GL(m, H)$ and $SL(2m, C)$; its center consists of $\pm I$.

(III) Let $p, q$ be two integers such that $p \geq q \geq 1$ and $p + q = n$. Consider the $n \times n$ matrix

$$I_{p, q} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix};$$

the mapping $c_0$: $X \mapsto -I_{p, q} \cdot X \cdot I_{p, q}$ is a conjugation that commutes with $c_u$, by reason of the relations $I_{p, q} = I_{p, q}$ and $I_{p, q}^{-1} = 'I_{p, q} = I_{p, q}$. The restriction of $c_0$ to $g_u$ is the automorphism $X \mapsto I_{p, q} X I_{p, q}$ of this real Lie algebra; the restriction to $\mathcal{G}_u = SU(n)$ of the corresponding automorphism $\sigma$ of $\mathcal{G}_G$ is the same mapping $X \mapsto I_{p, q} X I_{p, q}$, and it follows that the group $K_0$ is the set of matrices $\begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix}$, where $U \in U(p)$, $V \in U(q)$, and det$(U)$ det$(V) = 1$. One sees immediately that such a matrix can be uniquely expressed as a product

$$\begin{pmatrix} U & 0 \\ 0 & I_q \end{pmatrix} D \begin{pmatrix} I_p & 0 \\ 0 & V \end{pmatrix}$$

where $U \in SU(p)$, $V \in SU(q)$, and $D$ is a diagonal matrix of the form

$$D = \text{diag}(\delta, 1, \ldots, 1, \delta^{-1}, 1, \ldots, 1)$$
with $\delta^{-1}$ in the $(p+1)$th place, and $|\delta| = 1$. Consequently $K_0$ is diffeomorphic to $SU(p) \times T \times SU(q)$, hence is not simply connected. Its Lie algebra $t_0$ consists of the matrices of the form \[
abla \left( \begin{array}{c} X \\ 0 \\ Y \end{array} \right) \] with $X \in u(p)$, $Y \in u(q)$, and $\text{Tr}(X) + \text{Tr}(Y) = 0$; such a matrix can be written uniquely in the form \[
abla \left( \begin{array}{ccc} X_1 & 0 & 0 \\ 0 & p^{-1} & 0 \\ 0 & 0 & q^{-1} \end{array} \right) \]
where $\alpha \in \mathbb{R}$, $X_1 \in su(p)$, and $Y_1 \in su(q)$; and it is immediately verified that this decomposition $t_0 = su(p) \oplus \mathbb{R} \oplus su(q)$ is a decomposition into ideals. The simply connected group $\hat{K}_0$, the universal covering of $K_0$, is therefore isomorphic to $SU(p) \times \mathbb{R} \times SU(q)$. The group $G_0$ is the set of matrices $X \in SL(n, \mathbb{C})$ such that $t^n X \cdot I_{p,q} \cdot X = I_{p,q}$, i.e., it is the subgroup $SU(p, q)$ of matrices with determinant 1 in the unitary group $U(p, q)$ of a sesquilinear Hermitian form of signature $(p, q)$ on $\mathbb{C}^n$ (16.11.3); the foregoing remarks show that $G_0$ is not simply connected.

It can be shown (Problem 3; also [62], [85]) that every conjugation of $sl(n, \mathbb{C})$ that commutes with $c_u$ is of the form $\varphi \circ c_0 \circ \varphi^{-1}$, where $\varphi$ is an automorphism of $sl(n, \mathbb{C})$ and $c_0$ is one of the three types of conjugation just described.

(21.18.12) We retain the notation of (21.18.8). If $\tau$ is the involutory automorphism of the simply connected Lie group $\check{G}_0$ that corresponds to the automorphism $c_u|g_0$ of $g_0$, then $\tau$ fixes each element of $\check{K}_0$ and transforms each element of $\check{P}_0$ into its inverse. Since the center $Z$ of $\check{G}_0$ is contained in $\check{K}_0$, it follows that, on passing to the quotient in $G_1 = \check{G}_0/D$, $\tau$ gives rise to an involutory automorphism $\tau_1$ of $G_1$ which fixes the elements of $K_1 = \check{K}_0/D$ and transforms each element of $P_1$ into its inverse. We conclude that $K_1$ is exactly the subgroup of $G_1$ consisting of the fixed points of $\tau_1$, by virtue of the relation $G_1 = P_1 K_1$ and the fact that no element of $P_1$ has order 2, because of the existence of the diffeomorphism $u \mapsto \exp_{G_1}(u)$ of $p_0$ onto $P_1$.

Suppose now that the algebra $g$ is simple; this implies that every real form of $g$, and in particular $g_0$, is simple, and consequently the only normal Lie subgroups of $G_1$ are the subgroups of the center $C_1$. In order that the group $K_1$ should contain no normal subgroup of $G_1$ other than $\{e\}$, we must therefore take $D = Z$, i.e., $G_1 = \text{Ad}(G_0)$ and $K_1 = \text{Ad}(K_0)$. The composite canonical mapping

(21.18.12.1) \[ p_0 \to P_1 = \exp_{G_1}(p_0) \to G_1/K_1, \]
in which the left-hand arrow is the exponential mapping and the right-hand arrow is the restriction to $P_1$ of the canonical projection $G_1 \to G_1/K_1$, is a diffeomorphism. Identifying all the spaces $G_1/K_1$ with $\text{Ad}(G_1)/\text{Ad}(K_1)$, we see that, since the conditions of (20.11.1) are satisfied for the latter space, we may define a structure of a Riemannian symmetric space on the spaces $P_1$, or $G_1/K_1$, for which the Levi-Civita connection is entirely determined by the conjugation $c_0$. But in fact we can define canonically a $G_1$-invariant Riemannian metric on $G_1/K_1$; since the restriction to $p_0$ of the Killing form $B_0$ (or $B_g$) is positive definite and invariant under $\text{Ad}(t)$ for all $t \in K_1$, we may take this restriction as the value of the Riemannian metric tensor on $G_1/K_1$ at the point $x_0$ that is the image of the identity element (20.11.1).

With this choice of metric, the sectional curvature $A(u, v)$ is easily calculated, where $u, v$ are any two vectors in $p_0 = T_{x_0}(G_1/K_1)$: for by virtue of (20.21.2.1) and the invariance of $B_0$, we have

$$A(u, v) = -B_0([u, v], [u, v])/\|u \wedge v\|^2$$

Hence $G_1/K_1$ is a Riemannian manifold with sectional curvature everywhere $\leq 0$.

(21.18.13) The existence of the involutory automorphism $\sigma$ of $G_u$ corresponding to the conjugation $c_0$ (21.18.5) gives rise to other Riemannian symmetric spaces. Supposing always that $g$ is simple, the largest normal subgroup of $G_u$ contained in $K_0$ is $C \cap G_0$ (21.18.5.2). Let $G_2 = G_u/(C \cap G_0)$ and $K_2 = K_0/(C \cap G_0)$. On passing to the quotients, $\sigma$ defines an involutory automorphism $\sigma_2$ of $G_2$ that fixes the points of $K_2$; but here $K_2$ is only the identity component of the subgroup $K_2'$ of fixed points of $\sigma_2$, and may well be distinct from $K_2'$, as the example $G_2 = \text{SO}(n + 1)$, $K_2 = \text{SO}(n)$ ($n$ even) shows (20.11.4). For each subgroup $K''_2$ such that $K_2 \subset K''_2 \subset K_2'$, the symmetric pair $(G_2, K''_2)$ therefore fulfills the conditions of (20.11.1) and defines a compact Riemannian symmetric space $G_2/K''_2$. The tangent space to this manifold at the point $x_0$, the image of the identity element of $G_2$, may be identified with the subspace $ip_0$ of $g_u$. The restriction of $B_g$ to $ip_0$ is negative definite (21.18.4); on the other hand, for each $t \in K_2'$, the space $ip_0$ is stable under $\text{Ad}(t)$, and $B_0$ is invariant under $\text{Ad}(t)$, so that we may again define canonically a $G_2$-invariant Riemannian metric on $G_2/K''_2$, by taking the restriction of $-B_g$ to $ip_0$ as the value of the metric tensor at the point $x_0$ (so that the spaces $G_2/K''_2$, for all the different possible choices of $K''_2$, are locally isometric). The same calculation as in (21.18.2.2) now gives the sectional curvature $A(u, v)$, for $u, v \in ip_0$:

$$A(u, v) = \|[[u, v]]/\|u \wedge v\|^2$$
so that the Riemannian manifolds $G_2/K_2'$ have sectional curvature everywhere $\geq 0$. It can be shown that $G_2/K_2$ is simply connected (Problem 5), so that it is a finite covering of each of the spaces $G_2/K_2'$.

The direct sum decomposition of the Lie algebra $\mathfrak{g}_u$,\\

\[
(21.18.13.2) \quad \mathfrak{g}_u = \mathfrak{t}_0 \oplus \mathfrak{i} \mathfrak{p}_0,\\
\]

is again called the Cartan decomposition of $\mathfrak{g}_u$ corresponding to $c_0$. The image of $\mathfrak{t}_0$ under the exponential mapping $\exp_{\mathfrak{g}_2}$ is equal to $K_2$ (21.7.4). The image $\mathfrak{P}_2$ of $\mathfrak{i} \mathfrak{p}_0$ under the mapping $\exp_{\mathfrak{g}_2}$, however, has properties that are rather different from those of the set $\mathfrak{P}_1$ studied in (21.18.8):

\[
(21.18.13.3) \quad \text{For each } s \in G_2, \text{ let } s^* = \sigma_2(s^{-1}). \text{ Then the group } G_2 \text{ acts differentiably on itself by the action } (s, t) \mapsto sts^*. \text{ For this action, } \mathfrak{P}_2 \text{ is the orbit of } e, \text{ and } K_2' \text{ is the stabilizer of } e, \text{ so that } \mathfrak{P}_2 \text{ is a compact submanifold of } G_2, \text{ canonically diffeomorphic to } G_2/K_2'; \text{ also we have } K_2 \mathfrak{P}_2 = \mathfrak{P}_2 K_2 = G_2.\\
\]

We know from (20.7.10.4) that the geodesic trajectories on the compact Riemannian manifold $G_2/K_2$ that pass through $x_0$ are the images under $\pi: G_2 \to G_2/K_2$ of the 1-parameter subgroups corresponding to the tangent vectors belonging to $\mathfrak{i} \mathfrak{p}_0$. Since $G_2/K_2$ is compact and therefore complete, the union of these geodesic trajectories is the whole of $G_2/K_2$ (20.18.5); in other words, $\pi(\mathfrak{P}_2) = G_2/K_2$, or equivalently $G_2 = \mathfrak{P}_2 K_2$. Since the relation $x \in \mathfrak{P}_2$ implies $x^{-1} \in \mathfrak{P}_2$, it follows that also $G_2 = K_2 \mathfrak{P}_2$.

The mapping $x \mapsto x^*$ clearly has the following properties:

\[
x x^* = x, \quad (xy)^* = y^* x^*, \quad e^* = e;\\
\]

the relation $xx^* = e$ is equivalent to $x \in K_2'$; and for each $x \in \mathfrak{P}_2$ we have $x^* = x$, because $c_0(\mathfrak{u}) = -\mathfrak{u}$ for $\mathfrak{u} \in \mathfrak{i} \mathfrak{p}_0$. Observe now that $\exp(\mathfrak{u}) = (\exp(\frac{1}{2}\mathfrak{u}))^2$; from this it follows that each $x \in \mathfrak{P}_2$ may be written as $x = y^2$ with $y \in \mathfrak{P}_2$, or equivalently $x = yy^*$. Conversely, for each $s \in G_2$ we may write $s = xz$ with $x \in \mathfrak{P}_2$ and $z \in K_2$, so that $ss^* = xzz^{-1}x = x^2 \in \mathfrak{P}_2$. This shows that $\mathfrak{P}_2$ is the orbit of $e$ for the action $(s, t) \mapsto sts^*$ of $G_2$ on itself. Since $G_2$ is compact, $\mathfrak{P}_2$ is a compact submanifold of $G_2$ (16.10.7); moreover, we have seen above that the stabilizer of $e$ is $K_2'$, and therefore the corresponding canonical mapping $G_2/K_2' \to \mathfrak{P}_2$ is a diffeomorphism (16.10.7).

It should be carefully noted that in general the restriction to $\mathfrak{P}_2$ of the canonical mapping $\pi: G_2 \to G_2/K_2$ is not a diffeomorphism (Problem 6 and Section 21.21, Problem 2).

\[
(21.18.14) \quad \text{To summarize, we have shown that to each involutory automorphism of the Lie algebra } \mathfrak{g}_u \text{ (when } \mathfrak{g} \text{ is simple) there correspond:}\n\]
A real form $g_0$ of $g$, and the almost simple real Lie groups having $g_0$ as Lie algebra.

(2) A noncompact Riemannian symmetric space $G_1/K_1$, diffeomorphic to $\mathbb{R}^n$ for some $n$.

(3) A finite family of compact Riemannian symmetric spaces $G_2/K_2^*$.

It can be shown that, together with the Euclidean spaces (20.11.2) and the almost simple compact groups, the Riemannian symmetric spaces of types (2) and (3) enable us to describe all Riemannian symmetric spaces (Problem 13). On the other hand, we shall see in (21.20.7) that every complex semisimple Lie algebra is isomorphic to the complexification of the Lie algebra of a compact semisimple group. It follows therefore that the determination of the almost simple compact groups and their involutory automorphisms implies *ipso facto* the determination of the real or complex semisimple groups and Riemannian symmetric spaces.

(21.18.15) *Let the symbols $\tilde{G}_u$, $\tilde{G}$, and $\tilde{G}_0$, have the same meanings as before. Then the linear representations of these three groups on the same finite-dimensional complex vector space $E$ are in canonical one-to-one correspondence with each other, and are completely reducible (H. Weyl's "unitary trick").*

This is now obvious, because the linear representations of $\tilde{G}_u$ on $E$ correspond one-to-one to the $\mathbb{R}$-homomorphisms of $g_u$ into $\text{gl}(E)_\mathbb{R}$, which in turn are in canonical one-to-one correspondence with the $\mathbb{C}$-homomorphisms of $g = g_u \otimes \mathbb{C}$ into $\text{gl}(E)$, by virtue of the fact that $\text{gl}(E)$ is a complex Lie algebra (21.9.1); and the same argument applies when we replace $g_u$ by any real form $g_0$ of $g$.

It can be shown that for $\tilde{G}$ and $\tilde{G}_0$ (when $g_0$ is not the Lie algebra of a compact group), no finite-dimensional linear representation can be equivalent to a unitary representation (Section 21.6, Problem 5). On the other hand, these groups admit many irreducible unitary representations of infinite dimension (cf. Chapter XXII).

**PROBLEMS**

1. With the notation of (21.18.6), let $Q$ be the kernel of the canonical homomorphism $\tilde{G}_0 \to G_0$. For each quotient $G_1 = \tilde{G}_0/D$, where $D$ is a subgroup of the center $Z$ of $\tilde{G}_0$, and each linear representation $\rho_1: G_1 \to \text{GL}(E)$ of $G_1$ on a finite-dimensional complex vector space $E$, show that the kernel of $\rho_1$ contains $p_1(Q)$, where $p_1: \tilde{G}_0 \to G_1$ is the canonical homomorphism. (If $\sigma: \tilde{G}_0 \to G_0 \to \tilde{G}$ is the canonical homomorphism (with kernel $Q$), show that there exists a linear representation $\rho: \tilde{G} \to \text{GL}(E)$ such that $\rho \circ \sigma = \rho_1$.)
\( \rho_1 : p_1. \) The only groups \( G_1 \) that admit a faithful linear representation on a finite-dimensional space are those for which \( Q \subset D \) (use Section 21.17, Problem 2); their centers are therefore finite.

2. With the notation of (21.18.8), show that the compact group \( K_1 \) is its own normalizer in \( G_1. \) (Reduce to showing that if an element \( u \in p_0 \) is such that \( \rho_1 = \exp_{\alpha_1}(u) \) normalizes \( K_1 \), then \( u = 0. \) Using the unique decomposition of an element of \( G_1 \), as a product \( yz \), where \( y \in P_1 \) and \( z \in K_1 \), and the relation \([f_y, p_0] \subset p_0 \), show first that \([u, x] = 0 \) for all \( x \in t_0 \); then use the invariance of \( B_\alpha (21.5.6.1) \) to deduce that \([u, v] \in p_0 \) for all \( v \in p_0 \); this implies that \([u, v] = 0 \) and hence that \( u \) is in the center of \( g. \)

3. (a) With the notation of (21.8.2), suppose that the compact group \( \mathcal{G}_\alpha \) is almost simple. If \( f \) is an involutory automorphism of \( g_\alpha \), there exists a regular element of \( g_\alpha \) invariant under \( f \), and hence a maximal commutative subalgebra \( t \) of \( g_\alpha \) stable under \( f \), and a basis \( B \) of the system of roots of \( g_\alpha \) relative to \( t \) that is stable under \( f \) (Section 21.11, Problem 19).

(b) Suppose that the transpose \('(f \otimes 1)' \) leaves invariant each of the roots of \( B \) in \((t_\alpha)^* \); this is the only possibility when \( g \) is of type \( B_n \) or \( C_n \) (consider the Cartan integers for the basis \( B \)). Then we have \( f = \text{Ad}(\exp(u)) \) with \( u \in t \) (cf. Section 21.11, Problem 12); we may replace \( \exp(u) \) by \( z \cdot \exp(u) \), where \( z \) is in the center of \( \mathcal{G}_\alpha \), without changing \( f \), and if we replace \( u \) by \( w \cdot u \), where \( w \) is in the Weyl group \( W \), then \( f \) is replaced by \( \varphi \circ f \circ \varphi^{-1} \), where \( \varphi \) is an automorphism of \( g_\alpha \); we may therefore suppose that \( u \) is in the closure of the principal alcove \( \mathcal{A}^* \) corresponding to \( B \) (Section 21.15, Problem 11). By using the fact that \( f^2 = 1 \), show that either \( iu = \pi p_j \) for some index \( j \) such that \( n_j = 1 \), or \( iu = \pi p_j + \pi q \) for some index \( j \) such that \( n_j = 2 \), and \( iu = \pi (p_j + p_k) \) for two indices \( j, k \) such that \( n_j = n_k = 1 \) (cf. Section 21.16, Problem 10). Show that this last case may be reduced to the first (observe that \( 2\pi (p_j - p_k) \) is a vertex of an alcove \( w(\mathcal{A}^*) \) for some \( w \in W \).

(c) If \( g \) is of type \( A_n \) or \( D_n \), there exists an involutory automorphism \( f_0 \) of \( g_\alpha \) such that \'(f_0 \otimes 1)(B) = B \), but such that \'(f_0 \otimes 1) does not fix every element of \( B \). (For type \( A_n \), consider the automorphism \( X \mapsto X \) of \( u(n, C) \), and for \( D_n \), the automorphism defined in (20.11.4).) Furthermore, except for type \( D_n \), if \( f \) is another involutory automorphism of \( g_\alpha \) with the same property, then we must have \( f = \text{Ad}(\exp(u)) \circ f_0 \) for some \( u \in t \), and we must again suppose that \( u \) lies in the closure of \( \mathcal{A}^* \); use the fact that \( f^2 = 1 \) to show that \( \text{Ad}(\exp(u + f_0(u))) \) is the identity mapping. By observing that the indices \( j \) such that \( f_0(p_j) \neq p_j \) are such that \( n_j = 1 \) in both cases \( A_n \) and \( D_n \), show that \( iu = \pi p_j \) for some index \( j \) such that \( f_0(p_j) = p_j \) and \( n_j = 1 \). or \( 2 \).

(d) Deduce from (b) and (c) that for the classical groups of types \( B_n, C_n, \) and \( D_n \), the compact real forms (up to isomorphism) correspond to the conjugation \( c_\alpha : X \mapsto X \) in \( \mathfrak{so}(n, C) \) for types \( B_n \) and \( D_n \), and to the conjugation \( c_\alpha : X \mapsto JXJ^{-1} \) in \( \mathfrak{sp}(2n, C) \), where \( J \) is the matrix (21.12.2.4). The noncompact real forms (up to isomorphism) correspond to the following conjugations:

\[
\begin{align*}
c_0 : X & \mapsto I_{p,q}X I_{p,q} & \text{in } \mathfrak{so}(n, C) \ (p + q = n), \\
c_0 : X & \mapsto JXJ^{-1} & \text{in } \mathfrak{so}(2n, C), \\
c_0 : X & \mapsto X & \text{in } \mathfrak{sp}(2n, C), \\
c_0 : X & \mapsto -K_{p,q} : \mathfrak{X} : K_{p,q} & \text{in } \mathfrak{sp}(2n, C) \ (p + q = n).
\end{align*}
\]

\( \dagger \) It is necessary here to assume that \( l \neq 4 \) in order to apply (c), but it can be shown that the result remains true for \( D_n \).
where $K_{\eta^+}$ is the matrix
\[
\begin{pmatrix}
-I_p & 0 & 0 & 0 \\
0 & I_q & 0 & 0 \\
0 & 0 & -I_p & 0 \\
0 & 0 & 0 & I_q
\end{pmatrix}
\]

The compact symmetric spaces corresponding to the conjugations involving the matrices $I_{\eta^+} K_{\eta^+}$ include in particular the Grassmannians (16.11.9).

4. With the notation and hypotheses of Problem 3, show that if the conjugation $c_\eta$ has as its restriction to $g_\eta$ an automorphism of the type considered in Problem 3(b), then the group $K_\eta$ (in the notation of (21.18.13)) is connected. If on the other hand this restriction is of the type considered in Problem 3(c), then $(K_\eta : K_\eta) = 2$.

5. With the hypotheses and notation of (21.18.13), show that $G_2/K_2$ is simply connected. (Use (16.14.9) and Section 16.30, Problem 11(a)).

6. With the hypotheses and notation of (21.18.13), show that the mapping $(s, y) \mapsto y s t^\ast$ is a submersion of $G_2 \times K_2$ into $G_2$ at the point $(e, y_0)$, for each $y_0 \in K_2$ such that $-1$ is not an eigenvalue of $\text{Ad}(y_0)$. The set $P_2$ of points $t \in G_2$ such that $t^* = t$ contains the union of the orbits (for the action $(s, t) \mapsto t s t^\ast$) of the points $y \in K_2$ such that $y^2 = e$. Show that $P_2$ is the connected component of the point $e$ in $P_2^1$, and is open in $P_2$. For each $s \in G_2$, the mapping $z \mapsto z s t^\ast$ is an isometry of $P_2$ onto itself; deduce that the geodesics in $P_2$ are the curves $t \mapsto z t s t^\ast$ for $z \in G_2$ and $s \in G_2$.

(b) In the case where $G_2 = SO(\eta + 1)$ and $\sigma_2$ is the automorphism defined in (20.11.4), show that $P_2 \cap K_2$ is the set consisting of $e$ and a submanifold diffeomorphic to $S_{\eta - 1}$ that does not contain $e$, and that $P_2 \cap K_2 = \{e\}$. Determine the other connected components of $P_2^1$.

7. With the notation and hypotheses of (21.18.13), the mapping $s \mapsto s t^\ast$ of $G_2$ onto $P_2$ factorizes as $G_2 \xrightarrow{\pi} G_2/K_2 \xrightarrow{\mu} P_2$, where $\pi$ is the canonical mapping and $\mu$ is a diffeomorphism.

(a) Show that the composition $\mu \circ (\pi|P_2)$ is the mapping $y \mapsto y^2$ of $P_2$ onto itself. Let $\exp_{G_2} : g_\eta \mapsto G_2$ be the exponential mapping of the Lie group $G_2$ and $\exp_\omega$ the exponential mapping corresponding to the canonical connection on $G_2/K_2^1$; then we have $\pi(\exp_{G_2}(u)) = \exp_{G_2}(u)$ for $u \in ip_0$ (20.7.10.4) ($ip_0$ being canonically identified with the tangent space at $x_0$ to $G_2/K_2^1$). Show that $\mu(\exp_{G_2}(u)) = \exp_{G_2}(2u)$ for $u \in ip_0$.

(b) Let $u \in ip_0$ and let $y = \exp_{G_2}(u) \in P_2$. Show that for each vector $v \in ip_0$ we have
\[
T_{\tau}(\exp_\omega) \cdot \tau^{-1}(v) = T(\pi) \cdot \left(y \cdot \left(\sum_{k=0}^{\infty} \ad(u)^{2k} \left(\frac{1}{(2k + 1)!}\right) \cdot v\right)\right).
\]

(Use (19.16.5.1) and the relation $[p_0, p_0] \subset f_0$.)

8. With the notation and hypotheses of (21.18.12), let $s^\ast = \tau_s(s^{-1})$ for all $s \in G_2$. State and prove for $G_1$ and $K_1$ the analogues of (21.18.13.3) and Problems 6(a) and 7.

9. With the notation and hypotheses of (21.18.12), show that for a submanifold $S$ of $P_1$ to be totally geodesic (20.13.7), it is necessary and sufficient that the vector subspace $s = T_{x_0}(S)$
of $p_0$ should be such that the relations $u \in s, v \in s, w \in s$ imply $[u, [v, w]] \in s$; such an $s$ is called a Lie triple system, and $s$ is the image of $s$ under $\exp_{G_0}$. (Using the definitions of the second fundamental forms (20.12.4) and of the parallel transport of a vector (18.6.3), show first that if $S$ is totally geodesic, the parallel transport (relative to $P_1$) of a tangent vector to $S$ along a curve in $S$ is the same as the parallel transport of this vector relative to $S$, and therefore consists of tangent vectors to $S$. Then use (20.7.10.4) and Problem 8 to show that for all $u, v$ in $s$ we must have $(\text{ad}(u))^2 \cdot v \in s$, and deduce that $s$ is a Lie triple system. Conversely, show that if $s \subset p_0$ is a Lie triple system, then $g^* = s + [s, s]$ is a Lie subalgebra of $g_0$, stable under the conjugation $c_\gamma$; if $G'$ is the connected Lie group immersed in $G_1$ that corresponds to $g'$, and if $K' = G' \cap K$, then $K'$ is closed for the proper topology of $G'$; the image $S'$ of $s$ in $P_1$, under $\exp_{G_0}$, is a closed submanifold of $P_1$, and the canonical mapping $G'/K' \to S'$ is a diffeomorphism (for the proper topology of $G'$); consequently $S'$ is a geodesic submanifold at the point $x_0$, and $G'$ acts on $S'$ as a transitive group of isometries.)

Show that the unique geodesic trajectory in $P_1$ that passes through two distinct points of $S$ is contained in $S$.

10. In (21.18.12), take $G_1 = \text{SL}(n, \mathbb{R})$ and $\tau_1$ to be the automorphism $X \mapsto X^{-1}$; its derived automorphism, the restriction of $c_\tau$ to $\mathfrak{s}_\mathfrak{l}(n, \mathbb{R})$, is the automorphism $X \mapsto -X$. We have then $K_1 = \text{SO}(n)$, and $P_1$ is the set $S$ of positive definite symmetric matrices of determinant $1$, which can also be written as $e^t$, where $s = p_0$ is the space of symmetric matrices of trace $0$. The geodesics in the Riemannian symmetric space $S$ are the mappings $t \mapsto X(e^t, A), A \in \text{SL}(n, \mathbb{R})$ of $R$ into $S$, where $A \in \text{SL}(n, \mathbb{R})$ and $X \in s$ (Problem 8). Through any two points of $S$ there passes one and only one geodesic trajectory.

Let $Q(X, Y) = \text{Tr}(X^{-1}Y + Y^{-1}X)$ for any two matrices $X, Y \in S$.

(a) Show that $Q(A \cdot X \cdot e^A, A \cdot Y \cdot e^A) = Q(X, Y)$ for all $A \in \text{SL}(n, \mathbb{R})$ and that $Q(X, Y) > 0$ for all $X, Y \in s$. (Use the fact that $X$ can be written as $Z^2$, where $Z \in S$.)

(b) Show that $Q(i, X) = 2 \sum_{j=1}^n \text{ch}(\lambda_j)$, where $e^{\lambda_1}, \ldots, e^{\lambda_n}$ are the eigenvalues of the symmetric matrix $X \in S$ (use (a) above). Deduce that for each $X_0 \in S$ the mapping $t \mapsto Q(X_0, X)$ of $S$ into $R$ is proper (17.3.7).

(c) Let $t \mapsto G(t)$ be a geodesic in $S$. Show that for each $X_0 \in S$ the function $t \mapsto Q(X_0, G(t))$ is strictly convex on $R$. (Reduce to the case where $G(t) = e^t$, where $Y \in s$ is a diagonal matrix.)

11. (a) With the notation of Problem 10, let $P$ be a totally geodesic submanifold of $S$, and let $M$ be a compact subgroup of $\text{SL}(n, \mathbb{R})$ leaving $P$ globally invariant (for the action $(U, X) \mapsto U \cdot X \cdot U$ of $\text{SL}(n, \mathbb{R})$ on $S$). Show that there exists $X_0 \in P$ that is invariant under $M$. (By (20.11.3.1) there exists $Z_0 \in S$ invariant under $M$. By using Problem 10, show that as $X$ runs through $P$ the function $X \mapsto Q(Z_0, X)$ attains its lower bound at a unique point $X_0$: if the lower bound were attained at two distinct points, consider the unique geodesic trajectory joining them. Note also that $Q(Z_0, X_0) = Q(Z_0, U \cdot X_0 \cdot U)$ for all $U \in M$.)

(b) With the notation of (21.18.8), show that if $G_1 = \text{Ad}(G_0)$, then for each compact subgroup $M$ of $G_1$ there exists an inner automorphism of $G_1$ that transforms $M$ into a subgroup of $K_1$ (E. Cartan's conjugacy theorem). (Using Section 21.17, show that if we identify $\text{Aut}(g_0)$ with a subgroup of $\text{GL}(n, \mathbb{R})$ (where $n = \dim(g_0)$), so that $K_1$ is identified with a subgroup of $O(n)$ and $P_1$ with a submanifold of $S$, then there exists $y \in P$, such that $z \cdot y \cdot z = y$ for all $z \in M$, by using (a) above and Problem 10; then note that if $y = x^2$
with \( x \in P_1 \), the relation above takes the form \( \tau_1(x^{-1}zx) = x^{-1}zx \) for all \( z \in M \), in the notation of (21.18.12).)

12. (a) Let \( G/K \) be a symmetric Riemannian space (20.11.3), where \( G \) is a connected real Lie group and \( K \) is a compact subgroup of \( G \) that contains no normal subgroup of \( G \) other than \( \{e\} \). Let \( \sigma \) be the involutory automorphism of \( G \) for which \( K \) is contained in the subgroup of fixed points and contains the identity component of this subgroup. If \( g, t \) are the Lie algebras of \( G \) and \( K \), respectively, then \( f \) is the subspace of vectors in \( g \) fixed by \( s = \sigma \), and contains no nonzero ideal of \( g \). There exists a scalar product \( (x|y) \) on \( g \) such that \( (\text{ad}(x) \cdot x|y) + (x|\text{ad}(y) \cdot y) = 0 \) for all \( x \in f \). A pair \( (g, s) \) consisting of a finite-dimensional real Lie algebra \( g \) and an involutory automorphism \( s \) of \( g \) having the above properties is called a symmetrized Lie algebra, and \( s \) is called the symmetrization of \( g \).

(b) Let \( (g, s) \) be a symmetrized Lie algebra, \( f \) the subspace of vectors fixed by \( s \), and \( p \) the vector subspace of \( g \) consisting of all \( x \in g \) such that \( s(x) = -x \). Then \( g = f \oplus p \); we have \([f, f] \leq f, [f, p] \leq p, [p, p] \leq f \), and \( f, p \) are orthogonal to each other with respect to the Killing form \( B_g \). Show that \( f \) is the Lie algebra of a compact group and that there exists a scalar product \( Q(x, y) \) on \( p \) such that

\[
Q(\text{ad}(x) \cdot x|y) + Q(x|\text{ad}(y) \cdot y) = 0
\]

for all \( z \in f \) (cf. Section 21.6, Problem 2). Furthermore, the restriction of \( B_g \) to \( f \) is a negative definite symmetric bilinear form.

(c) With the hypotheses of (b), let \( A \) be the endomorphism of the vector space \( p \) such that \( Q(A \cdot x, y) = B_g(x, y) \) (Section 11.5, Problem 3), so that \( A \) is self-adjoint relative to the scalar product \( Q \). Let \( E_0 \) be the kernel of \( A \) (which may be zero) and \( E_i \) \((1 \leq i \leq r)\) the eigenspaces of \( A \) corresponding to the distinct nonzero eigenvalues \( c_i \) of \( A \), so that \( p \) is the direct sum of the \( E_i \) \((0 \leq i \leq r)\), which are pairwise orthogonal with respect to \( Q \); also \( B_g(x, y) = c_i Q(x, y) \) for \( x \) and \( y \) in \( E_i \), and \( E_0 \) is the subspace of \( p \) orthogonal to \( p \) with respect to \( B_g \).

(d) The endomorphism \( A \) commutes with \( \text{ad}(x) \) for all \( x \in f \), and therefore \([f, E_i] \subseteq E_i \) for \( 0 \leq i \leq r \). If \( K \) is a compact connected Lie group with \( f \) as Lie algebra, then the sum \( F \) of \( E_1, \ldots, E_r \), is the direct sum of subspaces \( p_j \) \((1 \leq j \leq m)\) stable under \( \text{Ad}(t) \) for all \( t \in K \), each of which is contained in some \( E_i \), and such that each representation \( t \mapsto \text{Ad}(t) \mid p_j \) of \( K \) is irreducible. The \( p_j \) are pairwise orthogonal with respect to both \( Q \) and \( B_g \); if we put \( p_0 = E_0 \), show that \([p_j, p_k] = 0 \) for \( 0 \leq j, h \leq m \) and \( j \neq h \). (If \( u \in p_j, v \in p_k \), then we have \( w = [u, v] \in f \); show that \( B_g(w, w) = 0 \) and use (b) above.)

(e) Put \( g_j = p_j + [p_j, p] \) for \( 1 \leq j \leq m \). Show that the \( g_j \) are ideals of \( g \) such that \([g_j, g_k] = 0 \) for \( j \neq k \), and that \( s(g_j) = g_j \). By considering the restrictions of \( B_g \) to \( g_j \times g_j \), show that the \( g_j \) are semisimple Lie algebras; \( g \) is the direct sum of the \( g_j \) \((1 \leq j \leq m)\) and the centralizer \( g_0 \) of the direct sum of the \( g_j \) \((1 \leq j \leq m)\) (Section 21.6, Problem 4); and we have \( s(g_0) = g_0, p_0 \subseteq g_0 \) and \([p_0, p_0] = 0 \).

13. With the notation of Problem 12, suppose that the decomposition of \( p \) as the direct sum of the \( p_j \) consists of only one term, and hence that \( g \) is equal to one of the algebras \( g_j \).

(a) If \([p, p] = 0 \), then \( g \) is the semidirect product of \( f \) and the ideal \( p \) (19.14.7). Hence there exists a connected Lie group \( G \) having \( g \) as Lie algebra, and a compact subgroup \( K \) of \( G \), such that \( G \) is the semidirect product \( f \times K \) and a commutative normal subgroup \( P \) (so that \( P \) is isomorphic to \( \mathbb{R}^r \times T^v \)), we may further suppose that \( K \) contains no normal subgroup of \( G \) other than \( \{e\} \). The corresponding Riemannian manifold \( G/K \) is the manifold \( P \) having as a Riemannian covering \( \mathbb{R}^{r+v} \) with its canonical metric; \( G \) acts on this
manifold as a transitive group of isometries, containing always the translations of the group $P$.

(b) If $[p, p] \neq 0$, then $g$ is semisimple; hence there exists a connected semisimple group $G$ having $g$ as Lie algebra, and a compact connected subgroup $K$ of $G$ having $l$ as Lie algebra, and containing no normal subgroup of $G$ other than $\{e\}$. We have $B_q(x, y) = cQ(x, y)$ for $x, y \in p$, with $c \neq 0$. If $c < 0$, then $G$ is compact semisimple; if $g$ is not simple, its simple ideals must be permuted by $s$. Show that the irreducibility of the representation $t \mapsto Ad(t)|p$ of $K$ implies that $g$ has in this case two isomorphic simple ideals $g_1, g_2$ such that $s(g_1) = g_2$, with $I$ isomorphic to $g_1$ and $g_2$. The Riemannian symmetric space $G/K$ is then isomorphic to a compact semisimple group with center $\{e\}$, endowed with a left- and right-invariant metric.

If $c < 0$ and $g$ is simple, we are in the situation described in (21.18.13).

If $c > 0$, then $G$ is semisimple and noncompact. Show that $g$ is necessarily simple, by showing that otherwise $g$ would be isomorphic to $I \times t$. In the complexified Lie algebra $g_0(x) = g_0 + itg_0$ is the Lie algebra of a compact group, and we are in the situation described in (21.18.12).

(c) Deduce from (a) and (b) and Problem 12 that every symmetrized Lie algebra arises from a simply connected Riemannian symmetric space by the procedure of Problem 12(a).

14. (a) Let $X$ be a $C^\infty$ vector field on a differential manifold $M$, and let $F_x$ be the flow of the field (18.2.1). Let $x_0$ be a point of $M$ at which $X(x_0) = 0$. For each $C^\infty$ vector field $Y$ on $M$, the vector $(\theta_x \cdot Y)(x_0)$ depends only on $Y(x_0)$ (cf. (17.14.11)). For each $u \in T_{x_0}(M)$, let $\theta_{X, x_0} : u$ denote the value of $(\theta_x \cdot Y)(x_0)$ for each vector field $Y$ such that $Y(x_0) = u$. If we put $g_t(x) = F_x(x, t)$, we have $g_t(x_0) = x_0$ for all $t \in \mathbb{R}$; for sufficiently small values of $t$, $g_t$ is a diffeomorphism of an open neighborhood $U_0$ of $x_0$ in $M$ onto another open neighborhood $U_t$ of $x_0$, and if $s, t \in \mathbb{R}$ are sufficiently small, then we have $g_{s+t} = g_s \circ g_t = g_t \circ g_s$. Hence if we put $V(t) = T_{x_0}(g_t) \in GL(T_{x_0}(M))$, we have $V(s+t) = V(s)V(t)$ for all sufficiently small $s$ and $t$. Show that for sufficiently small $t$ we have $V(t) = \exp(t\theta_{X, x_0})$, the exponential being that of the group $GL(T_{x_0}(M))$.

(b) Suppose that $M$ is endowed with a principal connection $P$ on $\mathbb{R}(M)$. If $X$ and $Y$ are infinitesimal automorphisms of the restrictions of $P$ to two neighborhoods $U, V$ of $x_0 \in M$ (Section 20.6, Problem 6), then $X$ and $Y$ are said to be equivalent if they coincide on a neighborhood of $x_0$ contained in $U \cap V$. The equivalence classes (or germs) of infinitesimal automorphisms of restrictions of $P$ to neighborhoods of $x_0$ form a Lie algebra $\mathfrak{g}_{x_0}$ of dimension $\leq n(n+1)$, where $n = \dim T_{x_0}(M)$. The classes of the $X$ such that $X(x_0) = 0$ form a Lie subalgebra $\mathfrak{t}_{x_0}$ of $\mathfrak{g}_{x_0}$. For each class $\xi \in \mathfrak{t}_{x_0}$, the mapping $\theta_{X, x_0} \in \mathfrak{End}(T_{x_0}(M))$ is independent of the choice of $X \in \xi$, and the mapping $\xi \mapsto \theta_{X, x_0}$ is an injective homomorphism of $\mathfrak{t}_{x_0}$ into the Lie algebra $\mathfrak{g}l(T_{x_0}(M)) = \mathfrak{End}(T_{x_0}(M))$.

15. Let $M$ be a connected differential manifold endowed with a linear connection that is invariant under parallelism (Section 20.6, Problem 18). Let $U$ be an open neighborhood of $x_0 \in M$, determined as in Section 20.6, Problem 15.

(a) For each vector $u \in T_{x_0}(M)$ and each $t \in \mathbb{R}$ such that $\exp(tu) \in U$, a transvection of the vector $tu$ is by definition an isomorphism $\tau_{tu}$ of a sufficiently small neighborhood of $x_0$ onto a sufficiently small neighborhood of $\exp(tu)$, such that $T_{x_0}(\tau_{tu})$ is the parallel transport of $T_{x_0}(M)$ onto $T_{\exp(tu)}(M)$ along the geodesic $\nu$ for which $\nu(0) = x_0$ and $\nu'(0) = u$ (18.6.3) (cf. Section 20.6, Problem 18). We have $\tau_{t+s} = \tau_s \circ \tau_{tu}$ if $s$ and $t$ are sufficiently small. For each $Y$ in a sufficiently small neighborhood of $x_0$, let $X(x_0) = u$; then $X_u$ is an infinitesimal automorphism of the connection restricted to the neighborhood of $x_0$ under consideration. This
field $X_\xi$ is called an infinitesimal transvection relative to $x_0$. Show that the mapping $u \mapsto \xi_u$ that sends each $u \in T_{\xi_0}(M)$ to the germ $\xi_u$ of the infinitesimal transvection $X_u$ (Problem 14(b)) is injective, and therefore identifies $T_{\xi_0}(M)$ with a vector subspace $p_{\xi_0}$ of the Lie algebra $\mathfrak{g}_{x_0}$. An isomorphism (for the induced connections) of a neighborhood of $x_0$ onto a neighborhood of $x \in M$ that transforms $x_0$ into $x$ also transforms $p_{\xi_0}$ into $p_x$, by transport of structure.

For simplicity of notation, we shall henceforth write $g, f, p$ in place of $g_{x_0}, f_{x_0}, p_{x_0}$.

(b) Show that for all sufficiently small $t$ and all $C^\infty$ vector fields $Y$ on $M$, we have $(\theta_{\xi_t} \cdot Y)(\exp(tu)) = (\nabla_{\xi_t} \cdot Y)(\exp(tu))$ (cf. Section 18.6, Problem 6).

(c) Let $Z$ be an infinitesimal automorphism defined in a neighborhood of $x_0$ and such that $Z(x_0) = 0$, so that its germ $\xi$ belongs to $T$; if we put $g_t(x) = F_\xi(x, t)$, then $g_t$ leaves $p$ globally invariant, by transport of structure, and transforms a germ $\xi_u \in p$ into $\xi_{g(t)u}$ (in the notation of Problem 14(a)). Consequently, we have $[I, p] \subset p$, and for each infinitesimal transvection $X_u$ relative to $x_0$ we have $[Z, X_u](x_0) = \theta_{X_u(x_0)} \cdot u$.

(d) Show that $g = f \oplus p$. (For an infinitesimal automorphism $Z$ defined in a neighborhood of $x_0$, consider the infinitesimal transvection $X_u$ for $u = Z(x_0)$.)

(e) Identify $T_{\xi_0}(M)$ with $p$ under the bijection $u \mapsto X_u$; the bracket $[u, v]$ of two vectors $u, v \in T_{\xi_0}(M)$ is then defined by the requirement that $X_u(\xi_v) = [u, v]$ (Problem 14(b)) to $[X_u, X_v]$. For all $u \in g$, let $u_t$ and $u_p$ denote the components of $u$ in $f$ and $p$, respectively. Show that, for $u, v, w \in p = T_{\xi_0}(M)$, we have

$$t \cdot (u \wedge v) = [u, v],$$
$$r \cdot (u \wedge v) \cdot w = -[[u, v], w],$$

where $t, r$ are the torsion and curvature morphisms of $M$ (Section 17.20). (Use (b) and (c) above to calculate $t \cdot (X_u \wedge X_v)$ and $(r \cdot (X_u \wedge X_v)) \cdot X_w$ by the formulas (17.20.1.1) and (17.20.6.1).)

(f) Let $M'$ be another connected differential manifold endowed with a linear connection invariant under parallelism, $x_0'$ a point of $M'$, and $g', f', p'$ the Lie algebras and the vector space corresponding to $g, f, p$. Suppose that there exists an isomorphism of $g$ onto $g'$ that maps $f$ onto $f'$ and $p$ onto $p'$. Then there exists an isomorphism $f$ of a neighborhood of $x_0$ onto a neighborhood of $x_0'$ (for the connections of $M$ and $M'$) such that $T_{\xi_0}(f) = F$ is the restriction to $p$ (identified with $T_{\xi_0}(M)$) of the given isomorphism of $g$ onto $g'$. (Use (e) above, together with Section 20.6, Problem 17.) When this is so, for every star-shaped neighborhood $U$ of $0_{\mathfrak{g}_{x_0}}$ in $T_{\xi_0}(M)$, on which the exponential mapping is a diffeomorphism, and such that $F(U)$ has the same property in $M'$, there exists an isomorphism $f$ of $\exp(U)$ onto $\exp(F(U))$ that extends the restriction of $f$ to a sufficiently small neighborhood of $x_0$. (Use the fact that in the linear differential equations of Section 20.6, Problem 15, the coefficients $\theta_{\xi_0}(ru)$ and $R_{\xi_0}(ru)$ are constants.)

16. (a) Let $M$ be a connected differential manifold endowed with a linear connection $\mathbf{C}$. Show that for $\mathbf{C}$ to be locally symmetric (Section 20.11, Problem 7) it is necessary and sufficient that $\mathbf{C}$ be torsion-free and that the parallel transport along a geodesic arc joining two points $x, y$ be the tangent linear mapping of an isomorphism (for $\mathbf{C}$) of a neighborhood of $x$ onto a neighborhood of $y$. If $s_x$ denotes the symmetry with center $x$ (Section 20.11, Problem 7), then $s_{x_0}$ defines by transport of structure an involutory automorphism $\sigma$ of the Lie algebra $\mathfrak{g}$ (in the notation of Problem 15) such that $\sigma(u) = u$ for $u \in f$ and $\sigma(u) = -u$ for $u \in p$, which implies the condition $[p, p] \subset f$. Show that $f$ contains no nonzero ideal of $\mathfrak{g}$ (use Problem 14(b)).

(b) Let $a \in M$ be a point in the neighborhood of $x_0$ on which $s_{x_0}$ is defined, and let
17. (a) Let $M$ and $M'$ be two connected, simply connected, complete Riemannian manifolds (20.18.5) satisfying the following condition: there exists a continuous function $\nu: M \times M' \to \mathbb{R}$ with values $> 0$ such that for each $(x, x') \in M \times M'$ the balls $B(x; \nu(x, x'))$ and $B(x'; \nu(x, x'))$ are strictly geodesically convex (20.17.2) and such that each isometry of a neighborhood $\nu = B(x; \nu(x, x'))$ of $x$ onto a neighborhood of $x'$, which maps $x$ to $x'$, extends to an isometry of $B(x; \nu(x, x'))$ onto $B(x'; \nu(x, x'))$.

Show that each isometry of an open subset of $M$ onto an open subset of $M$ extends to an isometry of $M$ onto $M'$. (Let $x_0 \in M$, and suppose that there exists an isometry $f_0$ of a neighborhood of $x_0$ onto a neighborhood of a point $x_0 \in M'$ such that $f_0(x_0) = x_0$. Given any point $x \in M$ and a piecewise-C$^1$ path $\gamma$ from $x_0$ to $x$, define an isometry of a neighborhood of $x$ onto an open set in $M'$ as follows: if $r$ is the length of $\gamma$ and $c$ the infimum of $\nu(y, y')$ in the relatively compact set $B(x_0; 2r) \times B(x_0'; 2r)$, consider a sequence $(x_0)_{0 \leq j \leq p}$ of points of $\gamma$ such that $x = x_p$ and the arc of $\gamma$ with endpoints $x_j$ and $x_{j+1}$ has length $< c$ for $0 \leq j \leq p - 1$. Show that for each $j$ we can define an isometry $f_j$ of $B(x_j; c)$ onto an open ball in $M'$, such that $f_j$ coincides with $f_0$ on the geodesically convex set $B(x_{j-1}; c) \cap B(x_j; c)$; for this purpose, use Problem 15(f) above and Section 20.6, Problem 9(a). Then show that the isometry $f_p$, defined on $B(x, c)$, does not depend on the choice of sequence $(x_j)$ satisfying the conditions above, and consequently that $f_p(x)$ may be written as $f(x)$, depending only on $\gamma$. Finally prove that if $\gamma'$ is another piecewise-C$^1$ path
18. Let $G$ be the universal covering group of $SL(2, \mathbb{R})$, and identify with $\mathbb{Z}$ the kernel of the canonical homomorphism $G \to SL(2, \mathbb{R})$ (21.18.11). Let $a \in T^*$ be an element whose powers form a dense set in $T^*$ (Section 19.7, Problem 6). Let $D$ be the discrete subgroup of $G \times T^*$ generated by $(1, a)$, and let $H = (G \times T^*)/D$. We have $\text{Lie}(H) = sl(2, \mathbb{R}) \times \mathbb{R}^*$. Show that the connected Lie group $H'$ immersed in $H$, with Lie algebra $sl(2, \mathbb{R}) \times \{0\}$, is dense in $H$. (Cf. Section 21.6, Problem 5.)

19. ROOTS OF A COMPLEX SEMISIMPLE LIE ALGEBRA

(21.19.1) Our aim now is to show that a complex semisimple Lie algebra $\mathfrak{g}$ of dimension $n$ is always isomorphic to the complexification of the Lie algebra of some compact semisimple Lie group. The method we shall follow consists, as a first step, in constructing a commutative Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ and a direct sum decomposition of the type (21.10.1.1) possessing the properties (A), (B), and (C) of Section 21.10; from this it will follow that all the results of Sections 21.10 and 21.11 that rest only on these properties are applicable, and the second step is to show that by use of these results it is possible to construct a Lie algebra of a compact Lie group, having $\mathfrak{g}$ as complexification.

(21.19.2) Let $\mathfrak{g}$ be an arbitrary complex Lie algebra of finite dimension $n$. For each element $u \in \mathfrak{g}$, the eigenvalues of the endomorphism $\text{ad}(u)$ of the complex vector space $\mathfrak{g}$ are given by the characteristic equation

$$\det(\text{ad}(u) - \xi \cdot 1_{\mathfrak{g}}) = 0,$$

the left-hand side of which is a polynomial in $\xi$ of degree $n$, with $(-1)^n$ as coefficient of $\xi^n$. Let $u_0$ be an element of $\mathfrak{g}$ for which the number of distinct roots of (21.19.2.1) is as large as possible. Since $[u_0, u_0] = 0$, $\text{ad}(u_0)$ will always have 0 as an eigenvalue; let then $\lambda_0 = 0, \lambda_1, \ldots, \lambda_m$ denote the distinct eigenvalues of $\text{ad}(u_0)$, and let $\mathfrak{g}_k (0 \leq k \leq m)$ denote the vector subspace $N(\lambda_k)$ of $\mathfrak{g}$ on which $\text{ad}(u_0) - \lambda_k \cdot 1_{\mathfrak{g}}$ is nilpotent. From (11.4.1), $\mathfrak{g}$ is the direct sum of the $\mathfrak{g}_k$. 

from $x_0 \to x$, then we have $f_y(x) = f_x(x)$, by reasoning as in (9.6.3) and using Section 20.6, Problem 9(a). We have thus defined a local isometry $f(20.8.1)$ of $\mathbb{M}$ into $\mathbb{M}'$; proceeding in the same way but starting with $f_0^{-1}$, use Section 20.6, Problem 9(a) once again to complete the proof.)

(b) Deduce from (a) that a locally symmetric, simply connected, complete Riemannian manifold is isometric to a simply connected Riemannian symmetric space. (Use Section 20.18, Problem 9, together with Problem 13(c) above.)
For all indices $h, k$ in $[0, m]$, we have $[g_h, g_k] = 0$ if $\lambda_h + \lambda_k$ is not an eigenvalue of $\text{ad}(u_0)$, and $[g_h, g_k] \subset g_l$ if $\lambda_h + \lambda_k = \lambda_l$ for some index $l$. In particular, $g_0$ is a Lie subalgebra of $g$, and we have $[g_0, g_k] \subset g_k$ for $1 \leq k \leq m$.

For all $x, y \in g$ we have

$$\left(\text{ad}(u_0) - (\lambda_h + \lambda_k) \cdot 1\right)[x, y] = \left(\text{ad}(u_0) - \lambda_h \cdot 1\right) \cdot x, y + [x, (\text{ad}(u_0) - \lambda_k \cdot 1) \cdot y]$$

from which it follows immediately by induction on $p$ that the element $(\text{ad}(u_0) - (\lambda_h + \lambda_k) \cdot 1)^p[x, y]$ is a linear combination of brackets of the form

$$\left(\text{ad}(u_0) - \lambda_h \cdot 1\right)^r \cdot x, (\text{ad}(u_0) - \lambda_k \cdot 1)^p \cdot y$$

for $0 \leq r \leq p$. The restriction of $\text{ad}(u_0) - (\lambda_h + \lambda_k) \cdot 1$ to $[g_h, g_k]$ is therefore nilpotent, and the proposition is proved.

Since $[g_0, g_k] \subset g_k$ for $0 \leq k \leq m$, it follows that for each element $u \in g_0$ the endomorphism $\text{ad}(u)$ leaves stable each of the subspaces $g_k$. Let $\alpha_k$ denote the linear form

$$u \mapsto \frac{1}{\dim g_k} \text{Tr}(\text{ad}(u) | g_k)$$

on the vector space $g_0$. Also let $P_k(u)$ denote the characteristic polynomial of the restriction of $\text{ad}(u)$ to $g_k$: the coefficients of this polynomial (in $\xi$) are therefore polynomials in the coordinates of $u$ with respect to any given basis of $g$. Hence the resultant† $R_{hk}(u)$ of the polynomials $P_h(u)$ and $P_k(u)$, where $h \neq k$, is a polynomial in the coordinates of $u$ that is not identically zero, because $P_h(u_0)(\xi) = (\lambda_h - \xi)^{\dim g_h}$ and $P_k(u_0)(\xi) = (\lambda_k - \xi)^{\dim g_k}$ have no root in common. It follows that, for each pair of distinct indices $h, k$, the set of elements $u \in g_0$ such that $R_{hk}(u) = 0$ is nowhere dense in $g_0$ (for otherwise $R_{hk}$ would be identically zero, by virtue of the principle of analytic continuation (9.4.1)). Let $E$ be the dense open subset of $g_0$ in which $R_{hk}(u) \neq 0$ for all pairs $(h, k)$ of distinct indices.

For each $u \in g_0$, the restriction of $\text{ad}(u) - \alpha_k(u) \cdot 1$ to $g_k$ is a nilpotent endomorphism. Furthermore, $\alpha_k(u) = 0$ for all $u \in g_0$.

Suppose first that $u \in E$. Since $\text{ad}(u) \cdot u = 0$, it is enough to show that the restriction of $\text{ad}(u)$ to each $g_k$ cannot have two or more distinct eigenvalues. Since, by the definition of $E$, these eigenvalues would be distinct.

† See, for example, my book *Infinitesimal Calculus*, Paris (Hermann), 1968, p. 61.
from all the eigenvalues of the restrictions of \( \text{ad}(u) \) to the other \( g_h \), and since there are at least \( m \) of these that are all distinct, it follows that the endomorphism \( \text{ad}(u) \) of \( g \) would have at least \( m + 2 \) distinct eigenvalues, contrary to the choice of \( u \). Hence for \( u \in E \) we have \( P_k(u)(\xi) = (\alpha_k(u) - \xi)^{\dim g_h} \) and \( P_0(u)(\xi) = (-\xi)^{\dim g_0} \); by continuity, these relations hold for all \( u \in g_0 \), because \( E \) is dense in \( g_0 \).

(21.19.6) We shall now change our notation and denote by \( h \) the Lie subalgebra \( g_0 \) of \( g \), and by \( S \) the set of linear forms \( \alpha_1, \alpha_2, \ldots, \alpha_m \) on \( h \), which are all \( \neq 0 \) and pairwise distinct, because they take distinct nonzero values at the point \( u_0 \); also we shall write \( g(\alpha_k) \) in place of \( g_h \), and put \( g(\beta) = \{0\} \) for every linear form \( \beta \) on \( h \) distinct from 0 and the \( \alpha \in S \). Then \( g(\alpha) \) may also be defined as the largest vector subspace of \( g \) such that for each \( u \in h \) the restriction of \( \text{ad}(u) - \alpha(u) \cdot 1 \) to this subspace is nilpotent. The proof of (21.19.3) shows that

\[
[g(\alpha), g(\beta)] = g(\alpha + \beta)
\]

for any two linear forms \( \alpha, \beta \) on \( h \).

(21.19.7) For all \( u, v \in h \) and all \( \alpha \in S \) we have \( \alpha([u, v]) = 0 \).

For the trace of the restriction of \( \text{ad}([u, v]) \) to \( g(\alpha) \) is \( \dim(g(\alpha)) \cdot \alpha([u, v]) \). On the other hand, we have

\[
\text{ad}([u, v]) = \text{ad}(u) \text{ad}(v) - \text{ad}(v) \text{ad}(u),
\]

and therefore the trace of the restriction of \( \text{ad}([u, v]) \) to \( g(\alpha) \) is zero.

((21.19.8) For all elements \( u, v \in h \), we have

\[
B_g(u, v) = \sum_{\alpha \in S} (\dim g(\alpha)) \cdot \alpha(u)\alpha(v).
\]

Since \( B_g \) is bilinear and symmetric, it is sufficient to calculate \( B_g(u + v, u + v) \); in other words, we need only prove (21.19.8.1) when \( u = v \). But then the restriction of \( \text{ad}(u)^2 \) to \( g(\alpha) \) has the single eigenvalue \( \alpha(u)^2 \); since the restriction of \( \text{ad}(u) \) to \( h \) is nilpotent, the result follows.

(21.19.9) If \( \alpha + \beta \neq 0 \), the subspaces \( g(\alpha) \) and \( g(\beta) \) are orthogonal relative to the Killing form \( B_g \).

Let \( u \in g(\alpha) \) and \( v \in g(\beta) \). Then it follows from (21.19.6.1) that the image of \( g(\gamma) \) under \( \text{ad}(u) \text{ad}(v) \) is contained in \( g(\alpha + \beta + \gamma) \). If we take a basis of \( g \)
consisting of a basis of $\mathfrak{h} = \mathfrak{g}(0)$ and bases of each of the subspaces $\mathfrak{g}(\alpha)$, $\alpha \in \mathfrak{S}$, it is clear that the diagonal elements of the matrix of $\text{ad}(u)\, \text{ad}(v)$ relative to this basis are all zero, and the result follows.

(21.19.10) Let $\alpha, \beta$ be two linear forms belonging to $\mathfrak{S}$. Let $p$ (resp. $q$) be the smallest (resp. largest) rational integer such that $\beta + p\alpha$ (resp. $\beta + q\alpha$) belongs to $\mathfrak{S}$. Then, for all $u \in [\mathfrak{g}(\alpha), \mathfrak{g}(-\alpha)] \subseteq \mathfrak{h}$, we have

$$\sum_{k=p}^{q} (\dim \mathfrak{g}(\beta + k\alpha))(\beta(u) + k\alpha(u)) = 0$$

and consequently $\beta(u) = r_{\alpha\beta} \alpha(u)$, where $r_{\alpha\beta}$ is a rational number.

Consider the subspace $V$ of $\mathfrak{g}$ that is the direct sum of the $\mathfrak{g}(\beta + k\alpha)$ for $p \leq k \leq q$. It will suffice to prove the formula (21.19.10.1) for $u = [x, y]$, where $x \in \mathfrak{g}(\alpha)$ and $y \in \mathfrak{g}(-\alpha)$. Since the image of $\mathfrak{g}(\gamma)$ under $\text{ad}(x)$ is contained in $\mathfrak{g}(\gamma + \alpha)$, by (21.19.6.1), and since $\mathfrak{g}(\beta + q\alpha + \alpha) = \{0\}$, it follows that $V$ is stable under $\text{ad}(x)$. Likewise, the image of $\mathfrak{g}(\gamma)$ under $\text{ad}(y)$ is contained in $\mathfrak{g}(\gamma - \alpha)$, and we have $\mathfrak{g}(\beta + p\alpha - \alpha) = \{0\}$, so that $V$ is stable under $\text{ad}(y)$ and hence also under $\text{ad}([x, y]) = \text{ad}(x)\, \text{ad}(y) - \text{ad}(y)\, \text{ad}(x)$. This being so, the trace of the restriction to $V$ of $\text{ad}(x)\, \text{ad}(y) - \text{ad}(y)\, \text{ad}(x)$ is zero. If we now observe that the restriction of $\text{ad}([x, y])$ to $\mathfrak{g}(\beta + k\alpha)$ has only one eigenvalue, namely $\beta([x, y]) + k\alpha([x, y])$, the formula (21.19.10.1) follows immediately.

(21.19.11) Suppose that the Lie algebra $\mathfrak{g}$ is semisimple. Then (with the same notation as above):

(i) The restriction to $\mathfrak{h}$ of the Killing form $B_{\mathfrak{g}}$ is nondegenerate.

(ii) If $\alpha \in \mathfrak{S}$, then also $-\alpha \in \mathfrak{S}$.

(iii) If $l$ is the dimension of $\mathfrak{h}$, there exist $l$ linearly independent forms belonging to $\mathfrak{S}$.

(iv) $\mathfrak{h}$ is a maximal commutative subalgebra of $\mathfrak{g}$.

(v) For each $u \in \mathfrak{h}$, the restriction of $\text{ad}(u)$ to $\mathfrak{g}(\alpha)$, for each $\alpha \in \mathfrak{S}$, is a homothety of ratio $\alpha(u)$: in other words

$$[u, x] = \alpha(u)x$$

for all $x \in \mathfrak{g}(\alpha)$.

(i) If $u \in \mathfrak{h}$ is orthogonal to $\mathfrak{h}$ (relative to $B_{\mathfrak{g}}$), then $u$ is orthogonal to all of $\mathfrak{g}$, because by virtue of (21.19.9) it is orthogonal to each $\mathfrak{g}(\alpha)$, $\alpha \in \mathfrak{S}$. Since $\mathfrak{g}$ is semisimple, it follows that $u = 0$. 

(ii) If we had $-\alpha \notin S$, then we should have $\alpha + \beta \neq 0$ for each $\beta \in S$, and therefore by virtue of (21.19.9) all the elements of $g(\alpha)$ would be orthogonal to each $g(\beta)$, $\beta \in S$; since they are also orthogonal to $h$, they would be orthogonal to the whole of $g$, and this is impossible since $g$ is semisimple.

(iii) If the rank of $S$, in the dual space of $h$, were strictly less than $l$, then there would exist an element $u \neq 0$ in $h$ such that $\alpha(u) = 0$ for all $\alpha \in S$; hence $B_u(u, v) = 0$ for all $v \in h$ by virtue of the formula (21.19.8.1), and this would contradict (i).

(iv) Since $\alpha([u, v]) = 0$ for all $\alpha \in S$ and all $u, v \in h$ (21.19.7), it follows from (iii) that $[u, v] = 0$, in other words, that $h$ is commutative. Hence $h$ is the kernel of $\text{ad}(u_0)$ and is therefore a maximal commutative subalgebra.

(v) The endomorphism $\text{ad}(u)$ decomposes uniquely as a sum $S + N$, where $S$ and $N$ are endomorphisms of the vector space $g$, which are polynomials in $\text{ad}(u)$ with complex coefficients, such that $N$ is nilpotent, $S$ diagonalizable and $SN = NS$ (A.25.3). Because $S$ is a polynomial in $\text{ad}(u)$, it stabilizes $h$ and the $g(\alpha)$, and the triangular form (A.6.10) of the restriction of $\text{ad}(u)$ to each $g(\alpha)$ shows that we have $S \cdot x = \alpha(u)x$ for all $x \in g(\alpha)$. Bearing in mind (21.19.6.1), we deduce that $S \cdot [x, y] = [S \cdot x, y] + [x, S \cdot y]$ for all $x \in g(\alpha)$ and $y \in g(\beta)$; and it then follows by linearity that $S$ is a derivation of the Lie algebra $g$. But $g$ is semisimple, hence every derivation of $g$ is inner (21.19.7): that is to say, there exists $v \in g$ such that $S = \text{ad}(v) \in \text{ad}(g)$. Now $x \mapsto \text{ad}(x)$ is an isomorphism of $g$ onto $\text{ad}(g)$ (21.6.3), and therefore $\text{ad}(u)$ commutes with $\text{ad}(w)$ for all $w \in h$; hence $S$, being a polynomial in $\text{ad}(u)$, also commutes with $\text{ad}(w)$ for all $w \in h$. Since $\text{ad}(h)$ is a maximal commutative subalgebra of $\text{ad}(g)$, by (iv) above, it follows that $v \in h$. Since $\text{Tr}(\text{ad}(v))|g(\alpha)| = \dim(g(\alpha)) \cdot \alpha(v)$ and $S \cdot x = \alpha(u)x$ for all $x \in g(\alpha)$, we see that $\alpha(u) = \alpha(v)$ for all $\alpha \in S$. By virtue of (iii), this implies that $u = v$ and shows that $\text{ad}(u) = S$ is diagonalizable.

Because of (21.19.11.1), for a semisimple complex Lie algebra $g$ the linear forms $\alpha \in S$ will henceforth be called the roots of $g$ relative to $h$.

(21.19.12) Since the restriction of $B_u$ to $h$ is nondegenerate, for each root $\alpha \in S$ there exists a unique element $h^\circ_\alpha \in h$ such that

\[
(21.19.12.1) \quad \alpha(u) = B_u(u, h^\circ_\alpha)
\]

for all $u \in h$.

(21.19.13) Suppose that the Lie algebra $g$ is semisimple. Then, for each root $\alpha \in S$:
For each \( x \in \mathfrak{g}(\alpha) \) and \( y \in \mathfrak{g}(-\alpha) \), we have

\[(21.19.13.1) \quad [x, y] = B_\alpha(x, y) \cdot h^0_\alpha.\]

(ii) \( \alpha(h^0_\alpha) \neq 0. \)

(i) We have \([x, y] \in \mathfrak{h} \), and from the invariance of the Killing form \((21.5.6.1)\)

\[B_\alpha([x, y], u) = B_\alpha([u, x], y) = \alpha(u)B_\alpha(x, y).\]

The formula \((21.19.13.1)\) now follows from \((21.19.12.1)\), since \(B_\alpha\) is nondegenerate.

(ii) Let \( x \) be an element \( \neq 0 \) in \( \mathfrak{g}(\alpha) \). Then \( x \) cannot be orthogonal to \( \mathfrak{g}(-\alpha) \) relative to \( B_\alpha \), for otherwise it would follow from \((21.19.9)\) that \( x \) was orthogonal to all of \( \mathfrak{g} \), contrary to the fact that \( \mathfrak{g} \) is semisimple. Hence there exists an element \( y \) in \( \mathfrak{g}(-\alpha) \) such that \([x, y] = h_\beta\) by virtue of \((21.19.13.1)\). This being so, it follows from \((21.19.10)\) that \( \beta([x, y]) = r_\alpha \alpha(h^0_\alpha) \) for each root \( \beta \in \mathfrak{S} \). If we had \( \alpha(h^0_\alpha) = 0 \), then we should have \( \beta(h^0_\alpha) = 0 \) for all roots \( \beta \in \mathfrak{S} \); since \( h^0_\alpha \neq 0 \) by virtue of \((21.19.12.1)\), this would contradict the existence of \( l \) linearly independent roots \((21.19.11(iii))\).

\[\text{PROBLEMS}\]

1. (a) Let \( \mathfrak{g} \) be a finite-dimensional complex Lie algebra and \( u \) any element of \( \mathfrak{g} \); let \( \lambda_0 = 0, \lambda_1, \ldots, \lambda_m \) be the distinct eigenvalues of \( \text{ad}(u) \), and \( \mathfrak{g}_k \) (\( 0 \leq k \leq m \)) the subspace \( \mathfrak{N}(\lambda_k) \) defined in \((11.4.1)\), so that \( \mathfrak{g} \) is the direct sum of the \( \mathfrak{g}_k \). If \( S \) and \( N \) are the diagonalizable and nilpotent endomorphisms of the vector space \( \mathfrak{g} \), such that \( S + N = \text{ad}(u) \) and \( SN = NS \) \((A.25.2)\), show that \( S \) and \( N \) are derivations of the Lie algebra \( \mathfrak{g} \). (Argue as in \((21.19.11(iv))\).)

(b) Suppose that \( \mathfrak{g} \) is semisimple. Then there exist uniquely determined elements \( v, w \in \mathfrak{g} \) such that \( \text{ad}(v) = S \) and \( \text{ad}(w) = N \). By abuse of language, \( v \) and \( w \) are called respectively the \textit{semisimple} and \textit{nilpotent components} of \( u \); they satisfy \([v, w] = 0\).

(c) Suppose that \( \mathfrak{g} \) is semisimple, and let \( \mathfrak{b} \) be a Lie subalgebra of \( \mathfrak{g} \) that is equal to its normalizer in \( \mathfrak{g} \). Show that for each \( u \in \mathfrak{b} \), the semisimple and nilpotent components of \( u \) belong to \( \mathfrak{b} \).

2. Let \( \mathfrak{g} \) be a complex semisimple Lie algebra. Suppose that there exist \( m + 1 \) distinct complex numbers \( \lambda_0 = 0, \lambda_1, \ldots, \lambda_m \) and a decomposition \( \mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_m \) of \( \mathfrak{g} \) as a direct sum of vector subspaces such that \([\mathfrak{g}_k, \mathfrak{g}_j] = 0 \) if \( \lambda_k + \lambda_j \) is not one of the \( \lambda_i \), and \([\mathfrak{g}_k, \mathfrak{g}_j] \subset \mathfrak{g}_j \) if \( \lambda_k + \lambda_j = \lambda_i \). Show that there exists an element \( u \in \mathfrak{g}_0 \) such that \( \text{ad}(u) \) leaves stable each of the \( \mathfrak{g}_j \), and such that the restriction of \( \text{ad}(u) \) to \( \mathfrak{g}_j \) is multiplication by \( \lambda_j \) (\( 0 \leq j \leq m \)). Extend this result to real semisimple Lie algebras when the \( \lambda_j \) (\( 1 \leq j \leq m \)) are real numbers.
20. Weyl Bases

(21.20.1) It follows from (21.19.11) and (21.19.13) that for a complex semisimple Lie algebra $\mathfrak{g}$ there exists a commutative subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ and a finite set $\mathfrak{s} \subset \mathfrak{h}^* - \{0\}$ of linear forms, such that the direct sum decomposition

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \mathfrak{s}} \mathfrak{g}(\alpha)$$

and the Killing form $B_{\mathfrak{g}}$ satisfy conditions (A), (B), and (C) of (21.10.1). For brevity we shall call (21.20.1.1) a root decomposition of $\mathfrak{g}$, $\mathfrak{h}$ being the maximal commutative subalgebra and $\mathfrak{s}$ the root system corresponding to this decomposition. We may then apply all the results of (21.10) and (21.11), with the (provisional) exception of those of (21.11.9), (21.11.10), and (21.11.11). The linear forms $v_{\alpha}$ that feature in (21.11.1) are here given by

$$v_{\alpha}(\lambda) = 2\lambda(\mathfrak{h}_{\alpha}^0)/\alpha(\mathfrak{h}_{\alpha}^0).$$

In particular, each subspace $\mathfrak{g}(\alpha)$ $(\alpha \in \mathfrak{s})$ is one-dimensional over $\mathbb{C}$ (21.10.3), $\mathfrak{g}(\alpha) \oplus \mathfrak{g}(-\alpha)$ is nonisotropic relative to $B_{\mathfrak{g}}$ (21.10.2), and we may therefore choose in each $\mathfrak{g}(\alpha)$ a vector $e_{\alpha}$ such that for all $\alpha \in \mathfrak{s}$ we have

$$B_{\mathfrak{g}}(e_{\alpha}, e_{-\alpha}) = 1$$

and hence, by (21.19.13.1),

$$[e_{\alpha}, e_{-\alpha}] = \mathfrak{h}_{\alpha}^0.$$

By virtue of (21.19.6.1), we may therefore write, for any two roots $\alpha, \beta$ in $\mathfrak{s}$,

$$[e_{\alpha}, e_{\beta}] = N(\alpha, \beta)e_{\alpha + \beta}$$

if $\alpha + \beta \in \mathfrak{s}$, with $N(\alpha, \beta) \in \mathbb{C}$, and

$$[e_{\alpha}, e_{\beta}] = 0$$

if $\alpha + \beta \notin \mathfrak{s}$ and $\alpha + \beta \neq 0$. We therefore define $N(\alpha, \beta)$ to be 0 when $\alpha + \beta \notin \mathfrak{s}$ and $\alpha + \beta \neq 0$.

These formulas, together with (21.19.11.1), show that the assignment of the numbers $N(\alpha, \beta)$ determines completely (once the roots are known) the mapping $(x, y) \mapsto [x, y]$ of $\mathfrak{g} \times \mathfrak{g}$ into $\mathfrak{g}$. By expressing that this mapping defines a Lie algebra structure, we shall obtain necessary conditions relating the $N(\alpha, \beta)$. 
In the first place, since the mapping \((x, y)\rightarrow [x, y]\) is skew-symmetric, we must have

\[(21.20.1.6) \quad N(\beta, \alpha) = -N(\alpha, \beta).\]

The following three lemmas follow from the Jacobi identity and properties of root systems.

\[(21.20.2) \quad \text{Let } \alpha, \beta, \gamma \in \mathbf{S} \text{ be such that } \alpha + \beta + \gamma = 0. \text{ Then}\]

\[(21.20.2.1) \quad N(\alpha, \beta) = N(\beta, \gamma) = N(\gamma, \alpha).\]

We have \([e_x, [e_\beta, e_y]] = N(\beta, \gamma)[e_x, e_{-\beta}] = N(\beta, \gamma)h_\beta^0\), so that the Jacobi identity

\[(21.20.2.2) \quad [e_x, [e_\beta, e_y]] + [e_\beta, [e_y, e_x]] + [e_y, [e_x, e_\beta]] = 0\]
gives the relation \(N(\beta, \gamma)h_\beta^0 + N(\gamma, \alpha)h_\gamma^0 + N(\alpha, \beta)h_\beta^0 = 0\); consequently, by virtue of \((21.19.12.1)\), we have

\[(21.20.2.3) \quad N(\beta, \gamma)\alpha + N(\gamma, \alpha)\beta + N(\alpha, \beta)\gamma = 0.\]

But the subspace of \(h^*\) spanned by \(\alpha, \beta,\) and \(\gamma,\) which is at most two-dimensional, cannot have dimension 1. For if these were so, the three roots \(\alpha, \beta,\) and \(\gamma\) would all be scalar multiples of one of them, say \(\alpha;\) but then \(\beta\) and \(\gamma\) would have to be equal to \(\pm \alpha (21.10.3)\), and since \(3\alpha \neq 0\) we should have either \(\beta = -\alpha\) or \(\gamma = -\alpha,\) whence either \(\gamma = 0\) or \(\beta = 0,\) both of which are impossible. Hence, replacing \(\gamma\) by \(-\alpha - \beta\) in \((21.20.2.3)\), we obtain \((21.20.2.1).\)

\[(21.20.3) \quad \text{Let } \alpha, \beta, \gamma, \delta \text{ be four roots (distinct or not) such that the sum of each pair is nonzero and such that } \alpha + \beta + \gamma + \delta = 0. \text{ Then}\]

\[(21.20.3.1) \quad N(\alpha, \beta)N(\gamma, \delta) + N(\beta, \gamma)N(\alpha, \delta) + N(\gamma, \alpha)N(\beta, \delta) = 0.\]

(Observe that each term in this sum is defined, by virtue of the conditions of the lemma.)

If \(\beta + \gamma \in \mathbf{S},\) then we have \([e_x, [e_\beta, e_y]] = N(\beta, \gamma)[e_x, e_{\beta + \gamma}] = N(\beta, \gamma)N(\alpha, \beta + \gamma)e_{-\delta},\) because \(\alpha + (\beta + \gamma) = -\delta \in \mathbf{S}.\) By virtue of \((21.20.2.1)\) applied to \(\alpha, \beta + \gamma,\) and \(\delta,\) we have \(N(\alpha, \beta + \gamma) = N(\delta, \alpha) = -N(\alpha, \delta),\) so that \([e_x, [e_\beta, e_y]] = -N(\beta, \gamma)N(\alpha, \delta)e_{-\delta}.\) If \(\beta + \gamma \not\in \mathbf{S},\) this relation still holds,
because both sides are zero. By applying the Jacobi identity (21.20.2.2), we obtain (21.20.3.1).

(21.20.4) Let \( \alpha, \beta \in S \) be two nonproportional roots, and let \( a \) (resp. \( b \)) be the smallest (resp. largest) rational integer such that \( \beta + a\alpha \) (resp. \( \beta + b\alpha \)) is a root. Then we have

\[
N(\alpha, \beta)N(-\alpha, -\beta) = -\frac{b(1 - a)}{2} \alpha(h^0_\beta).
\]

Suppose first that \( \alpha + \beta \in S \), so that \( b > 0 \). In the notation of the proof of (21.10.4), we have \( m = b - a \), and for \( 0 \leq j \leq m \) the element \( z_j = (j!)^{-1} \text{ad}(x_{-a})^j \cdot x_{\beta + ba} \) spans \( g(\beta + (b - j)a) \), by virtue of (21.9.3). In particular, \( z_0 \) spans \( g(\beta) \), and by (21.9.3.1) we have

\[
\text{ad}(x_{-a}) \cdot z_0 = (1 - a)z_{b - 1}, \quad \text{ad}(x_{-a}) \cdot z_{b - 1} = bz_b
\]

so that \([x_{-a}, [x_a, e_\beta]] = b(1 - a)e_\beta\). Since we may write \( e_a = \lambda x_a \), \( e_{-a} = \mu x_{-a} \), it follows from (21.20.1.3) and (21.10.3.2) that \( \lambda \mu h_a = h^0_\beta \), so that \( 2\lambda\mu = \alpha(h^0_\beta) \) and hence

\[
[x_{-a}, [x_a, e_\beta]] = \frac{1}{2} b(1 - a)\alpha(h^0_\beta)e_\beta.
\]

But since \( -\alpha + (\alpha + \beta) \neq 0 \), it follows that \([x_{-a}, [x_a, e_\beta]] = N(\alpha, \beta)N(-\alpha, \alpha + \beta)e_\beta \); and by virtue of (21.20.2) applied to the three roots \( -\alpha, \alpha + \beta, -\beta \), we have \( N(-\alpha, \alpha + \beta) = N(-\beta, -\alpha) = -N(-\alpha, -\beta) \). The relation (21.20.4.1) therefore results from (21.20.4.2). Finally, if \( b = 0 \), both sides of (21.20.4.1) are zero, so the relation is still true.

(21.20.5) (Weyl's theorem) Let \( g, g' \) be two complex semisimple Lie algebras, \( g = h \oplus \bigoplus S(\alpha) \), \( g' = h' \oplus \bigoplus S'(\alpha') \) root decompositions of \( g \) and \( g' \).

(21.20.1), \( S \subset h^* \) and \( S' \subset h'^* \) the corresponding root systems, \( E \) (resp. \( E' \)) the real vector space generated by \( S \) (resp. \( S' \)) (21.11.2); we may consider \( E \) (resp. \( E' \)) as the dual of the real vector space \( h_0 \) (resp. \( h'_0 \)) spanned by the elements \( h^0_\alpha \), \( \alpha \in S \) (resp. \( h^0_{\alpha'} \), \( \alpha' \in S' \)) (21.11.2). Let \( \varphi \) be an \( R \)-linear bijection of \( h_0 \) onto \( h'_0 \) such that \( \varphi(S') = S \). Then \( \varphi \) can be extended to a \( C \)-isomorphism of the Lie algebra \( g \) onto the Lie algebra \( g' \).

(In this statement, the elements \( h^0_{\alpha}, \alpha \in S \), are defined by the relations \( \alpha'(u') = B_g(u', h^0_\alpha) \) for \( u' \in h', \alpha' \in S' \), analogous to (21.19.12.1).)

Let us first show that for \( u, v \in h_0 \) we have

\[
B_g(u, v) = B_{g'}(\varphi(u), \varphi(v)).
\]
This will follow from the relations

\[ B_g(h^0_\alpha, h^0_\beta) = B_{g'}(h^0_\alpha, h^0_{\beta'}) \]

for \( \alpha', \beta' \) in \( S' \), and \( \alpha = '\varphi(\alpha') \), \( \beta = '\varphi(\beta') \).

For by definition we have

\[ \beta'(\varphi(u)) = \beta(u) = B_{g'}(u, h^0_\beta) = B_{g'}(\varphi(u), h^0_{\beta'}) \]

so that the relation (21.20.5.2) will imply that \( B_{g'}(\varphi(h^0_\alpha), h^0_{\beta'}) = B_{g'}(h^0_\alpha, h^0_{\beta'}) \) for all roots \( \alpha' \in S' \). But since the \( h^0_\beta \) span the complex vector space \( h' \), and since the restriction of \( B_{g'} \) to \( h' \) is nondegenerate, it follows that the relation \( \alpha = '\varphi(\alpha') \) implies that \( h^0_\beta = \varphi(h^0_\alpha) \) for all \( \alpha' \in S' \). Since the set of vectors \( h^0_\alpha \) contains a basis of \( h^0_\alpha \), the relation (21.20.5.1) indeed follows from (21.20.5.2).

To establish (21.20.5.2), we observe that the hypothesis on \( \varphi \) implies that if \( \alpha', \beta' \) are two nonproportional roots in \( S' \), then \( \alpha = '\varphi(\alpha') \) and \( \beta = '\varphi(\beta') \) are nonproportional, and the rational integers \( k \) for which \( \beta' + k\alpha' \in S' \) are exactly those for which \( \beta + k\alpha \in S \). By virtue of (21.10.4), we have therefore

\[ \frac{\beta'(\alpha^0)'(h^0_{\beta'})}{\alpha'(\alpha^0)'(h^0_{\beta'})} = \frac{\beta(\alpha^0)}{\alpha(\alpha^0)} \]

or, by virtue of the definition of the \( h^0_\alpha \) and the \( h^0_{\beta'} \),

\[ \frac{B_{g'}(h^0_\alpha, h^0_{\beta})}{B_g(h^0_\alpha, h^0_{\beta})} = \frac{B_{g'}(h^0_\alpha, h^0_{\beta})}{B_g(h^0_\alpha, h^0_{\beta})} \cdot \frac{B_g(h^0_\alpha, h^0_{\beta})}{B_{g'}(h^0_\alpha, h^0_{\beta})} \]

Since the Killing form is symmetric, this proves already that the ratio \( c_{\varphi} = \alpha'(h^0_\alpha)/\alpha(h^0_\alpha) \) is the same for all the roots \( \alpha' \in S' \), and that if we denote this ratio by \( c \), then we have \( \beta'(h^0_\alpha) = c \cdot \beta(h^0_\alpha) \) for all roots \( \alpha', \beta' \in S' \) (with \( \alpha = '\varphi(\alpha') \), \( \beta = '\varphi(\beta') \)). This relation may also be written as \( B_{g'}(h^0_\alpha, h^0_{\beta'}) = c \cdot B_g(h^0_\alpha, h^0_{\beta'}) \). On the other hand, the formula (21.19.8.1) applied to \( g \) and to \( g' \) gives, because of the hypothesis \( '\varphi(S') = S \),

\[ B_g(h^0_\alpha, h^0_{\beta'}) = \sum_{\gamma' \in S'} \gamma'(h^0_\gamma') \gamma(h^0_{\beta'}) = c^2 \sum_{\gamma \in S} \gamma(h^0_\gamma) \gamma(h^0_{\beta'}) \]

\[ = c^2 B_{g'}(h^0_\alpha, h^0_{\beta'}). \]

By comparison with the previous result, we obtain \( c = c^2 \), so that \( c = 1 \) (because \( c \neq 0 \)); this proves (21.20.5.1) and also establishes the relations

\[ (21.20.5.3) \quad \varphi(h^0_\alpha) = h^0_\alpha, \]

where \( \alpha = '\varphi(\alpha') \).
Suppose that we have chosen in each $g(a)$ a vector $e$, such that the relations (21.20.1.2)-(21.20.1.5) are satisfied. We shall show that it is possible to find in each $g'(a')$ an element $e_{a'}$ such that:

1. for each pair of roots $\alpha', \beta' \in S'$ such that $\alpha' + \beta' \neq 0$,

$$[e_{\alpha'}, e_{\beta'}] = N(\alpha, \beta)e_{\alpha' + \beta'}$$

where $\alpha = '\varphi(\alpha')$, $\beta = '\varphi(\beta')$ (which implies $\alpha + \beta = '\varphi(\alpha' + \beta')$, and therefore $\alpha + \beta \neq 0$, and $\alpha + \beta \in S$ if and only if $\alpha' + \beta' \in S'$);

2. for each root $\alpha' \in S'$,

$$B_{\alpha'}(e_{\alpha'}, e_{-\alpha'}) = 1$$

which, by (21.19.13.1), implies

$$[e_{\alpha'}, e_{-\alpha'}] = h_{\alpha'}^0.$$

Once the existence of these vectors $e_{\alpha'}$ has been established, the theorem will be proved by taking the extension of $\varphi$ to be the $\mathbb{C}$-linear mapping $\tilde{\varphi}$ such that

$$\tilde{\varphi}(e_a) = e_{\alpha'}.$$

for $\alpha' \in S'$ and $\alpha = '\varphi(\alpha')$. For it will follow from (21.20.5.3), (21.20.5.5), and (21.20.5.7) that $\tilde{\varphi}([e_a, e_{\beta}]) = [\tilde{\varphi}(e_a), \tilde{\varphi}(e_{\beta})]$ for all $\alpha, \beta \in S$; also, by reason of (21.20.5.3) and (21.20.5.1), we shall have $\tilde{\varphi}([h_a^0, e_{\beta}]) = [\tilde{\varphi}(h_a^0), \tilde{\varphi}(e_{\beta})]$ for all $\alpha, \beta \in S$; and since the $h_a^0$ and the $e_a$ span $g$, it will follow that $\tilde{\varphi}$ is a Lie algebra isomorphism of $g$ onto $g'$.

In order to define the vectors $e_{\alpha'}$, we shall begin by defining a lexicographic ordering on the real vector space $E$ spanned by $S$: we consider a basis $(e_j)_{1 \leq j \leq l}$ of this space, and for any two elements $\xi = \sum_{j=1}^{l} x_j e_j$, $\eta = \sum_{j=1}^{l} y_j e_j$, we define the relation $\xi < \eta$ to mean:

"$\xi \neq \eta$, and if $k$ is the smallest index such that $x_k \neq y_k$, then $x_k < y_k$ in $\mathbb{R}$."

It is immediately verified that the relation "$\xi < \eta$ or $\xi = \eta$" on $E$ is a total ordering (called the lexicographic ordering), that the relation $\xi < \eta$ implies $\xi + \zeta < \eta + \zeta$ for all $\zeta \in E$ (which implies that $\xi > 0$ is equivalent to
- \xi < 0) and that the relations \xi > 0, \eta > 0 imply \xi + \eta > 0. (This order relation should not be confused with that defined in (21.14.5).)

We may therefore write the elements of \( S \) in the form of a strictly increasing sequence, relative to this lexicographic ordering:

\[-\rho_m < -\rho_{m-1} < \cdots < -\rho_1 < 0 < \rho_1 < \cdots < \rho_{m-1} < \rho_m.\]

We shall define the \( e'_\alpha \) by the following (finite) inductive procedure: for each integer \( k \) such that \( 1 \leq k \leq m \), assume that the \( e'_\alpha \) have been defined for the \( \alpha' \in S' \) such that \( \alpha = \varphi(\alpha') \) satisfies the relations \(-\rho_k < \alpha < \rho_k\), that the relations (21.20.5.4) are satisfied by these roots \( \alpha' \), and that the relations (21.20.5.5) are satisfied by all pairs of these roots that also satisfy the conditions \( \alpha' + \beta' \neq 0 \) and \(-\rho_k < \varphi(\alpha'+\beta') < \rho_k\). The inductive step then consists in defining \( e'_\alpha \) and \( e'_{-\alpha} \) (where \( \rho_k = \varphi(\rho_k) \)) in such a way that these conditions continue to be satisfied when we replace \( k \) by \( k + 1 \).

(21.20.5.10) With a change of notation, our problem is reduced to the following: given a root \( \rho > 0 \) in \( S \), let \( S_\rho \) denote the set of roots \( \alpha \in S \) such that \(-\rho < \alpha < \rho\). Suppose that the \( e'_\alpha \) have been determined for those \( \alpha' \) such that \( \varphi(\alpha') \in S'_\rho \), and that they satisfy (21.20.5.4) and (21.20.5.5) whenever \( \alpha' + \beta' \neq 0 \) and \( \varphi(\alpha'+\beta') \in S'_\rho \). Then the problem is to define \( e'_\rho \) and \( e'_{-\rho} \), where \( \varphi(\rho') = \rho \), in such a way that the same conditions are still satisfied when we replace \( S'_\rho \) by \( S'_\rho \cup \{-\rho, \rho\} \).

If there exists no decomposition \( \rho = \alpha + \beta \) with \( \alpha, \beta \in S'_\rho \), then we may take \( e'_\rho \) to be an arbitrary nonzero element of \( g'(-\rho') \), and \( e'_{-\rho} \), the unique element of \( g'(\rho') \) such that \( B_g(e'_\rho, e'_{-\rho}) = 1 \). If on the other hand there exist \( \alpha, \beta \in S'_\rho \) such that \( \rho = \alpha + \beta \), and if \( \alpha = \varphi(\alpha'), \beta = \varphi(\beta') \), then we have \( N(\alpha, \beta) \neq 0 \) (21.10.5), and we shall define \( e'_\rho \) by the equation

\[ N(\alpha, \beta)e'_\rho = [e'_\alpha, e'_\beta]. \]

We have then \( e'_\rho \neq 0 \) (21.10.5), and we define \( e'_{-\rho} \) to be the unique element of \( g'(\rho') \) such that \( B_g(e'_\rho, e'_{-\rho}) = 1 \). We then define \( e''_\gamma \) for all \( \gamma \in S' \) by taking \( e''_\gamma = e'_\gamma \) if \( \varphi(\gamma') \in S'_\rho \cup \{-\rho, \rho\} \); if not, then we take \( e''_\gamma \) to be a nonzero element of \( g'(\gamma') \), and \( e'''_{-\gamma} \), to be the unique element of \( g'(-\gamma') \) such that \( B_g(e''_\gamma, e'''_{-\gamma}) = 1 \). We may then write \([e''_\gamma, e''_\delta] = N(\gamma, \delta)e''_{\gamma+\delta} \) if \( \gamma + \delta \neq 0 \) (where \( \gamma = \varphi(\gamma'), \delta = \varphi(\delta') \), and we know already that \( N(\gamma, \delta) = N(\gamma', \delta') \) whenever \( \gamma, \delta \) and \( \gamma + \delta \) are in \( S'_\rho \). We have to prove that this relation remains true when \( \gamma, \delta \), and \( \gamma + \delta \) are in \( S'_\rho \cup \{-\rho, \rho\} \). There are various cases to consider:

(a) \( \gamma + \delta = \rho \), and we may assume that \( \gamma \) and \( \delta \) are both distinct from \( \alpha \) and \( \beta \). Then we have \( \alpha + \beta + (-\gamma) + (-\delta) = 0 \), and no two of the four roots
\(\alpha, \beta, -\gamma, -\delta\) sum to 0. We may therefore apply (21.20.3) to \(g\) and to \(g'\), thus obtaining

\[
N(\alpha, \beta)N(-\gamma, -\delta) = -N(\beta, -\gamma)N(\alpha, -\delta) - N(-\gamma, \alpha)N(\beta, -\delta),
\]

\[
N'(\alpha, \beta)N'(-\gamma, -\delta) = -N'(\beta, -\gamma)N'(\alpha, -\delta) - N'(-\gamma, \alpha)N'(\beta, -\delta).
\]

We remark now that we must have \(\alpha > 0, \beta > 0, \gamma > 0, \delta > 0\); for if, for example, \(\alpha < 0\), it would follow that \(\beta = \rho + (-\alpha) > \rho\), which is absurd. Hence \(\gamma, \delta, \beta - \gamma, \alpha - \delta, \alpha - \gamma, \beta - \delta\) all belong to \(S\), and therefore the inductive hypothesis implies that the right-hand sides of the two relations (21.20.5.12) are equal; since also \(N'(\alpha, \beta) = N(\alpha, \beta)\) by (21.20.5.11) and \(N(\alpha, \beta) \neq 0\) (21.10.5), it follows that \(N(-\gamma, -\delta) = N'(-\gamma, -\delta)\).

Now, by using the fact that the integers \(k\) such that \(y' + k\delta' \in S'\) are exactly those for which \(y + k\delta \in S\), together with the relations (21.20.5.2), we deduce from (21.20.4.1) applied to \(g\) and to \(g'\) that

\[
N(\gamma, \delta)N(-\gamma, -\delta) = N'(\gamma, \delta)N'(-\gamma, -\delta),
\]

whence finally \(N(\gamma, \delta) = N'(\gamma, \delta)\).

(a) \(\gamma + \delta = -\rho\); then \(-\gamma\) and \(-\delta\) belong to \(S_\rho\), and we have

\[
(-\gamma) + (-\delta) = \rho.
\]

The reasoning in (a) above proves that \(N(\gamma, \delta) = N'(\gamma, \delta)\).

(b) One of the roots \(\gamma, \delta\) is equal to \(\pm \rho\), for example, \(\gamma = -\rho\). Then \(\delta \neq \pm \rho\), otherwise we should have either \(\gamma + \delta = 0\) or else

\[
\gamma + \delta \notin S_\rho \cup \{-\rho, \rho\}.
\]

We have \(\rho = \delta + (\gamma - \delta)\), and by hypothesis

\[
-\gamma - \delta \in S_\rho \cup \{-\rho, \rho\};
\]

but we cannot have \(-\gamma - \delta = \pm \rho\), for this would imply that \(\delta = 0\) or \(\delta = 2\rho\), both of which are absurd; hence \(-\gamma - \delta \in S_\rho\) and \(\delta \in S_\rho\). Consequently, by (a) above, we have \(N'(\delta, -\gamma - \delta) = N(\delta, -\gamma - \delta)\). But since the sum of the roots \(\gamma, \delta, \) and \(-\gamma - \delta\) is zero, we can apply (21.20.2) to \(g\) and to \(g'\), and obtain \(N(\gamma, \delta) = N(\delta, -\gamma - \delta)\) and \(N'(\gamma, \delta) = N'(\delta, -\gamma - \delta)\). Hence again we have \(N(\gamma, \delta) = N'(\gamma, \delta)\), and the proof of the theorem (21.20.5) is now complete.

(21.20.6) Let \(g\) be a complex semisimple Lie algebra and let \(g = h \oplus \bigoplus_{\alpha \in S} g(\alpha)\) be a root decomposition of \(g\). Then there exists for each \(\alpha \in S\) an element
20. WEYL BASES 195

\[ \mathbf{e}_x \in \mathfrak{g}(\alpha) \text{ such that the conditions of (21.20.1) are satisfied, and moreover such that} \]

\[ (21.20.6.1) \quad N(\alpha, \beta) = -N(-\alpha, -\beta) \]

whenever \( \alpha + \beta \neq 0 \).

For each system of elements \((\mathbf{e}_x)_{x \in \mathfrak{s}}\) satisfying these conditions we have

\[ (21.20.6.2) \quad N(\alpha, \beta)^2 = \frac{b(1-a)}{2} \alpha(\mathbf{h}_\alpha^0) \]

whenever \( \alpha + \beta \neq 0 \), where \( a \) and \( b \) are the integers defined in (21.20.4), and \( N(\alpha, \beta) \) is real.

Let \( \varphi \) be the mapping \( \mathbf{u} \mapsto -\mathbf{u} \) of the real vector space \( \mathfrak{h}_0 \) onto itself. Clearly we have \( '\varphi(\lambda) = -\lambda \) for each linear form \( \lambda \in \mathfrak{E} \), so that \( '\varphi(\mathfrak{S}) = \mathfrak{S} \)

and we may apply (21.20.5) with \( \mathfrak{g}' = \mathfrak{g} \). Let us denote by \( \mathbf{z}_x \in \mathfrak{g}(\alpha) \) the elements constructed in the proof of (21.20.5) (and denoted there by \( \mathbf{e}_x' \)); for the automorphism \( \hat{\varphi} \) of \( \mathfrak{g} \) that extends \( \varphi \), they satisfy by virtue of (21.20.5.8) the condition \( \hat{\varphi}(\mathbf{z}_x) \in \mathfrak{g}(-\alpha) \), and also the relation \( B_g(\mathbf{z}_x, \mathbf{z}_{-x}) = 1 \). We may therefore write \( \hat{\varphi}(\mathbf{z}_x) = c_{-x} \mathbf{z}_{-x} \), with \( c_{-x} \in \mathbb{C} \), and since \( B_g \) is invariant under the automorphism \( \hat{\varphi} \), we have \( c_x c_{-x} = 1 \). Hence there exists for each \( \alpha \in \mathfrak{S} \) a complex number \( a_\alpha \) such that \( a_\alpha^2 = -c_x \), and \( a_\alpha a_{-x} = 1 \), whence \( a_x c_{-x} = -a_{-x} \). Now put \( \mathbf{e}_x = a_x \mathbf{z}_x \) for each \( \alpha \in \mathfrak{S} \). First of all, we have

\[ B_g(\mathbf{e}_x, \mathbf{e}_{-x}) = a_x a_{-x} B_g(\mathbf{z}_x, \mathbf{z}_{-x}) = 1. \]

Also \( \hat{\varphi}(\mathbf{e}_x) = a_x \hat{\varphi}(\mathbf{z}_x) = a_x c_{-x} \mathbf{z}_{-x} = -a_{-x} \mathbf{z}_{-x} = -\mathbf{e}_{-x} \). If \( \alpha, \beta \) are two roots such that \( \alpha + \beta \in \mathfrak{S} \), then we have \( \hat{\varphi}([\mathbf{e}_x, \mathbf{e}_\beta]) = [-\mathbf{e}_{-x}, -\mathbf{e}_{-\beta}] = N(-\alpha, -\beta) \mathbf{e}_{-x} \mathbf{e}_{-\beta} \), and on the other hand \( \hat{\varphi}([\mathbf{e}_x, \mathbf{e}_\beta]) = N(\alpha, \beta) \mathbf{e}_{\alpha + \beta} \), which proves the formula (21.20.6.1). The relation (21.20.6.2) then follows from (21.20.4.1). Finally, since \( a \leq 0 \) and \( b \geq 0 \), in order to show that \( N(\alpha, \beta) \) is real it is enough to prove that \( \alpha(\mathbf{h}_\alpha^0) > 0 \). Now by (21.19.8) we have

\[ \alpha(\mathbf{h}_\alpha^0) = B_h(\mathbf{h}_\alpha^0, \mathbf{h}_\alpha^0) = \sum_{\beta \in \mathfrak{S}} \beta(\mathbf{h}_\alpha^0)^2 \left( \alpha(\mathbf{h}_\alpha^0) \right)^2 \sum_{\beta \in \mathfrak{S}} \mathbf{r}_{\beta}^2 \]

by virtue of (21.19.10), since \( \mathbf{h}_\alpha^0 \in [\mathfrak{g}(\alpha), \mathfrak{g}(-\alpha)] \). Since \( \alpha(\mathbf{h}_\alpha^0) \neq 0 \), it follows that \( \alpha(\mathbf{h}_\alpha^0) > 0 \), and the proof is complete.

A \( \mathfrak{C}\)-basis of \( \mathfrak{g} \) which consists of an \( \mathfrak{R}\)-basis of \( \mathfrak{h}_0 \) and elements \( \mathbf{e}_x \in \mathfrak{g}(\alpha) \) satisfying the conditions (21.20.1.2) and (21.20.6.1), appears therefore as a generalization of the notion of a Weyl basis of the complexification of the Lie algebra of a compact semisimple Lie group (21.10.6). In fact, the two notions are identical: and it is precisely the existence of such a basis in any complex
Every complex semisimple Lie algebra $\mathfrak{g}$ is isomorphic to the complexification of the Lie algebra $\mathfrak{t}$ of some compact semisimple Lie group; and the Lie algebra $\mathfrak{t}$ having this property is unique up to isomorphism.

Consider elements $e_x (x \in S)$ having the properties of (21.20.6), and put $y_x = e_x - e_{-x}$, $z_x = i(e_x + e_{-x})$; it is clear that $i\mathfrak{h}_0$ and the element $y_x, z_x$ $(x \in S)$ span a real vector subspace $\mathfrak{t}$ of $\mathfrak{g}$, of dimension equal to $\dim \mathfrak{g}$ (21.11.2), and that $\mathfrak{g} = \mathfrak{t} \oplus i\mathfrak{t}$. Moreover, by use of (21.20.6.1), the following formulas are easily verified:

\begin{align*}
[\mathfrak{h}_0^0, y_\beta] &= \beta(h_0^0)z_\beta, \quad [\mathfrak{h}_0^0, z_\beta] = -\beta(h_0^0)y_\beta \\
[y_x, z_x] &= 2i\mathfrak{h}_0^0,
\end{align*}

\begin{align*}
[y_x, y_\beta] &= N(\alpha, \beta)y_{x+\beta} - N(\alpha, -\beta)y_{x-\beta}, \\
[z_x, z_\beta] &= -N(\alpha, \beta)y_{x+\beta} - N(\alpha, -\beta)y_{x-\beta}, \\
[y_x, z_\beta] &= N(\alpha, \beta)z_{x+\beta} + N(\alpha, -\beta)z_{x-\beta},
\end{align*}

if $\alpha + \beta \neq 0$. These formulas show that $\mathfrak{t}$ is a real Lie algebra, since the $N(\alpha, \beta)$ are real, and $\mathfrak{g}$ is isomorphic to the complexification of $\mathfrak{t}$. To see that $\mathfrak{t}$ is the Lie algebra of a compact semisimple Lie group, it is enough to show that the restriction to $\mathfrak{t}$ of the Killing form $B_\mathfrak{g}$ is negative definite ((21.6.1) and (21.6.9)). Now we know already that the restriction of $B_\mathfrak{g}$ to $\mathfrak{h}$ is nondegenerate; on the other hand, $\beta(h_0^0)$ is real for all $\alpha, \beta \in S$ (21.19.10); and therefore, since the $h_0^0$ span the real vector space $\mathfrak{h}_0$, $\beta(u)$ is real for all $u \in \mathfrak{h}_0$, and the formula $B_\mathfrak{g}(u, u) = \sum_{\beta \in S} \beta(u)^2$ (21.19.8.1) shows that the restriction of $B_\mathfrak{g}$ to $\mathfrak{h}_0 \times \mathfrak{h}_0$ is positive definite. Consequently its restriction to $i\mathfrak{h}_0 \times i\mathfrak{h}_0$ is negative definite. Since the $y_x$ and $z_x$ are orthogonal to $i\mathfrak{h}_0$ relative to $B_\mathfrak{g}$ (21.19.9), since $B_\mathfrak{g}(e_x, e_\beta) = 0$ for $\alpha + \beta \neq 0$, and since

\[ B_\mathfrak{g}(y_x, z_x) = iB_\mathfrak{g}(e_x, e_x) - iB_\mathfrak{g}(e_{-x}, e_{-x}) = 0 \]

by virtue of (21.19.9), it remains to show that $B_\mathfrak{g}(y_x, y_x) < 0$ and $B_\mathfrak{g}(z_x, z_x) < 0$; and this follows from the formulas

\begin{align*}
B_\mathfrak{g}(y_x, y_x) &= -2B_\mathfrak{g}(e_x, e_{-x}) = -2, \\
B_\mathfrak{g}(z_x, z_x) &= -2B_\mathfrak{g}(e_x, e_{-x}) = -2.
\end{align*}
The uniqueness (to within isomorphism) of the Lie algebra \( t \) is a consequence of the study of the real forms of \( g \) undertaken in Section 21.18. With the notation of that section, the Killing form \( B_{g_0} \) is negative definite only if \( p_0 = \{0\} \), that is to say, \( g_0 = g_u \); hence there is no real form of \( g \) that is the Lie algebra of a compact group, except for the subalgebras \( \phi(g_u) \), where \( \phi \) is an automorphism of \( g \) (21.18.3).

**PROBLEM**

Under the conditions of (21.20.6), show that there exists for each \( a \in S \) an element \( e_a \in g(a) \) such that if we put \([e_a, e_b] = N'(\alpha, \beta)e_a \cdot e_b \) when \( \alpha + \beta \in S \), then the \( N'(\alpha, \beta) \) are real and satisfy the condition \( N'(\alpha, \beta) = -N'(-\alpha, -\beta) \), and such that for each pair \( \alpha, \beta \in S \) satisfying \( \alpha + \beta \neq 0 \) we have \( |N'(\alpha, \beta)| = 1 - \alpha \). A basis of \( g \) consisting of the \( e_a \) and a basis of \( h_0 \) over \( \mathbb{R} \) is called a Chevalley basis of \( g \). (Reduce to the case where \( S \) is irreducible (Section 21.11, Problem 10) and observe that, in this case if \( (\lambda, \mu) \) is a scalar product on \( E \) which is invariant under the Weyl group \( W \), then \( \varphi(h_a^\lambda)/(\beta(h_a^\mu)) = (\alpha|\alpha)/(\beta|\beta) \) by using (21.11.5.5); then use Section 21.11, Problem 1(b).)

**21. THE IWASAWA DECOMPOSITION**

(21.21.1) Let \( g \) be a complex semisimple Lie algebra, which we may, by virtue of (21.20.7), consider as the complexification \( (g_u)_{c_0} = g_u \oplus i\bar{g_u} \) of the Lie algebra \( g_u \) of a simply connected compact semisimple Lie group \( \bar{G_u} \). With the notation of Section 21.18, let \( c_0 \) be a conjugation of \( g \) that commutes with the conjugation \( c_u \), and let \( g_0 \) be the real form of \( g \) consisting of the elements of \( g \) fixed by \( c_0 \); let \( g_0 = t_0 \oplus p_0 \) be the corresponding Cartan decomposition (21.18.4.1), with the relations (21.18.4.2), and recall that we have \( g_u = t_0 \oplus i\bar{p}_0 \) and \( t_0 = g_0 \cap g_u \).

(21.21.2) Let \( a_0 \) be a maximal commutative (real) Lie subalgebra contained in the real vector space \( p_0 \). (There exist nonzero commutative real subalgebras of \( p_0 \); for example, the one-dimensional subspaces; we may take \( e_0 \) to be such a subalgebra of largest possible dimension.) The subspace \( ia_0 \) of \( ip_0 \) is then also a maximal commutative subalgebra of \( ip_0 \).

(21.21.3) If \( t \) is a maximal commutative subalgebra of the real Lie algebra \( g_u \), containing \( ia_0 \), then \( t = ia_0 \oplus (t \cap t_0) \).

Let \( x = y + iz \) be an element of \( t \), with \( y \in t_0 \) and \( z \in p_0 \). For each \( u \in a_0 \) we must have \([y, iu] + [iz, iu] = 0 \); but \([y, iu] \in ip_0 \) and \([iz, iu] \in t_0 \).
so that \([y, iu] = 0\) and \([z, u] = 0\). Since \(a_0\) is a maximal commutative subalgebra of \(p_0\), it follows that \(z \in a_0\) and hence \(y \in t \cap f_0\).

For the rest of this section, let \(t\) be a maximal commutative subalgebra of \(g_u\) containing \(i a_0\), fixed once for all. Let

\[(21.21.3.1) \quad t \oplus it = h,\]

then it is clear that

\[(21.21.3.2) \quad c_0(h) = h.\]

(21.21.4) Let \(S\) be the root system of \(g_u\) relative to \(t\) (21.8.1); we recall that the roots \(\alpha \in S\) are \(\mathbb{R}\)-linear mappings of \(t\) into \(i\mathbb{R}\), which may be canonically identified with linear forms on the complex vector space \(h = t \oplus it\). They take real values on \(a_0\), and moreover \((21.21.4.2)\) we have

\[(21.21.4.1) \quad \alpha \circ c_u = -\alpha,\]

\[(21.21.4.2) \quad c_u(g_a) = g_{-\alpha}.\]

Let \(S'\) denote the set of roots that vanish on \(i a_0\) (or on \(a_0 \oplus i a_0\)); it is clear that \(- S' = S'\). Let \(\varphi\) denote the involutory automorphism \(c_0 c_u = c_u c_0\) of the complex Lie algebra \(g\). Clearly \(\varphi\) leaves \(g_0\) and \(g_u\) stable, and we have

\[(21.21.4.3) \quad c_u \mid g_0 = \varphi \mid g_0.\]

(21.21.5) (i) We have \(\varphi(t) = t\) (and hence \(\varphi(h) = h\)), and the mapping \(\alpha \mapsto \alpha \circ \varphi\) is a bijection of \(S\) onto itself.

(ii) We have \(\alpha \in S'\) if and only if \(\alpha \circ \varphi = \alpha\).

(iii) For each root \(\alpha \in S'\) we have \(g_{\alpha} \oplus g_{-\alpha} \subset t_0 + it_0\).

(i) For \(x \in t_0\) we have \(\varphi(x) = x\), and for \(x \in i p_0\) we have \(\varphi(x) = -x\). Hence \(\varphi(t) = t\) by virtue of (21.21.3), and the fact that \(\alpha \mapsto \alpha \circ \varphi\) is a bijection of \(S\) onto itself follows from (21.8.6).

(ii) If \(\alpha \circ \varphi = \alpha\), then \(\alpha(x) = \alpha(\varphi(x)) = -\alpha(x)\) for \(x \in i a_0\), and therefore \(\alpha(x) = 0\). Conversely, if \(\alpha \in S'\), then \(\alpha(x) = \alpha(\varphi(x))\) for \(x \in i a_0\) and for \(x \in f_0\), and therefore \(\alpha = \alpha \circ \varphi\) by virtue of (21.21.3).

(iii) If \(\alpha \in S'\), it is clear that \(\varphi(g_{\alpha}) = g_{\alpha}\). Since the complex vector space \(g_{\alpha}\) has dimension 1 (20.10.3) and since \(\varphi\) is an involutory bijection of \(g_u\) onto itself, we must have either \(\varphi(x) = x\) for all \(x \in g_{\alpha}\) or else \(\varphi(x) = -x\) for all \(x \in g_{\alpha}\). In the first case, we have \(x \in f_0 \oplus i f_0\); in the second case,
21. THE IWASAWA DECOMPOSITION

\[ x \in p_0 \oplus ip_0, \] and by definition \( [z, x] = \alpha(z)x = 0 \) for all \( z \in a_0; \) if \( x = v + iw, \) with \( v \) and \( w \) in \( p_0, \) we have therefore \( [z, v] + i[z, w] = 0, \) and since \( [z, v] \in t_0 \) and \( [z, w] \in it_0, \) we have \( [z, v] = [z, w] = 0. \) But since \( a_0 \) is a maximal commutative subalgebra in \( p_0, \) these relations imply that \( v \in a_0 \) and \( w \in a_0, \) whence \( x \in h; \) and since \( h \cap g_\alpha = \{0\} \) by virtue of (21.8.1), it follows that \( x = 0 \) in this case. Hence the assumption that \( \varphi(x) = -x \) for all \( x \in g_\alpha \) is untenable, and the proof is complete.

(21.21.6) Let \( S'' = S - S'. \) For each root \( \alpha \in S'' \), the set of vectors \( z \in a_0 \) such that \( \alpha(z) = 0 \) is a hyperplane in the real vector space \( a_\alpha. \) Since \( S'' \) is finite, there exists \( z_0 \in a_0 \) such that \( \alpha(z_0) \neq 0 \) for all roots \( \alpha \in S''. \) Let \( S'_+ \) denote the set of roots \( \alpha \in S'' \) such that \( \alpha(z_0) > 0. \) Since \( -S'' = S'', \) it is clear that \( S'' \) is the union of the two disjoint sets \( S''_+ \) and \( -S''_+. \) Since \( c_0(z_0) = z_0, \) the set \( S''_+ \) is stable under the mapping \( \alpha \mapsto \alpha \circ c_0, \) since \( \varphi(z_0) = -z_0, \) the image of \( S''_+ \) under the mapping \( \alpha \mapsto \alpha \circ \varphi \) is \( -S''_+. \)

(21.21.7) Let \( \eta = \bigoplus_{\alpha \in S''} a_\alpha \) and \( \eta_0 = \eta \cap g_0. \) Then we have a direct sum decomposition of the real semisimple Lie algebra \( g_0: \)

\[(21.21.7.1) g_0 = t_0 \oplus a_0 \oplus \eta_0 \]

(Iwasawa decomposition of \( g_0 \)).

Let us first show that the sum on the right-hand side of (21.21.7.1) is direct. Suppose then that \( x \in t_0, y \in a_0, \) and \( z \in \eta_0 \) are such that \( x + y + z = 0. \) By operating with \( \varphi \) we obtain \( x - y + \varphi(z) = 0, \) hence \( 2y + z - \varphi(z) = 0. \) But \( 2y \in h, z \in \bigoplus_{\alpha \in S''} a_\alpha \) and \( \varphi(z) \in \bigoplus_{\alpha \in S''} g_{-\alpha} \) (21.21.6); hence, by virtue of (21.8.1), \( y = z = 0 \) and consequently also \( x = 0. \)

It remains to prove the equality (21.21.7.1). Let \( x \in g_0, \) then by definition \( x = c_0(x) = \frac{1}{2}(x + c_0(x)). \) Since also \( x = h + \sum_{\alpha \in S} v_\alpha, \) where \( h \in h \) and \( v_\alpha \in g_\alpha \) for each \( \alpha \in S, \) we have \( x = \frac{1}{2}(h + c_0(h)) + \frac{1}{2} \sum_{\alpha \in S} (v_\alpha + c_0(v_\alpha)). \) Since \( c_0(h) = h \) and since the elements of \( h \) fixed by \( c_0 \) are those which belong to \( \{t \cap t_0\} \oplus a_0, \) we have \( h + c_0(h) \in t_0 \oplus a_0. \) If \( \alpha \in S', \) we have \( v_\alpha \in t_0 \oplus it_0 \) by virtue of (21.21.5), hence \( v_\alpha + c_0(v_\alpha) \in t_0. \) If \( \alpha \in S''_+, \) then
by definition $v_z \in \mathfrak{u}$, hence $v_z + c_0(v_z) \in \mathfrak{u} \cap \mathfrak{g}_0 = \mathfrak{u}_0$. Finally, if $\alpha \in -S^+_z$, the relation $v_z \in \mathfrak{g}_z$ implies $c_u(v_z) \in \mathfrak{g}_{-z}$ (21.21.4.2), hence

$$c_u(v_z) + c_0(c_u(v_z)) \in \mathfrak{u}_0$$

by the preceding result. On the other hand, the sum

$$v_z + c_0(v_z) + c_u(v_z) + c_0(c_u(v_z))$$

is fixed by $c_0$ and by $c_u$, and therefore belongs to $\mathfrak{t}_0$. It follows that $v_z + c_0(v_z) \in \mathfrak{t}_0 \oplus \mathfrak{u}_0$, and this completes the proof of (21.21.7.1).

(21.21.8) A finite-dimensional (real or complex) Lie algebra $\mathfrak{b}$ is said to be nilpotent if there exists an integer $r$ such that, for all sequences $x_1, x_2, \ldots, x_s$ of elements of $\mathfrak{b}$, we have

$$(21.21.8.1) \quad \text{ad}(x_1) \circ \text{ad}(x_2) \circ \cdots \circ \text{ad}(x_s) = 0$$

in the ring $\text{End}(\mathfrak{b})$ of endomorphisms of the vector space $\mathfrak{b}$. A connected Lie group is said to be nilpotent if its Lie algebra is nilpotent.

(21.21.9) (i) In the Iwasawa decomposition (21.21.7.1), $\mathfrak{u}$ (resp. $\mathfrak{u}_0$) is a nilpotent complex (resp. real) Lie algebra, and $\mathfrak{s}_0 = \mathfrak{a}_0 \oplus \mathfrak{u}_0$ is a solvable Lie algebra in which $\mathfrak{u}_0$ is an ideal.

(ii) Relative to the hermitian scalar product $-B_\mathfrak{g}(x, c_\mathfrak{g}(y))$ on $\mathfrak{g}$ (21.17.2), there exists an orthonormal basis for which the endomorphism $\text{ad}(x)$ of the vector space $\mathfrak{g}$ is represented by a matrix that is

(a) skew-hermitian if $x \in \mathfrak{g}_u$;
(b) lower triangular with zero diagonal if $x \in \mathfrak{u}$;
(c) real diagonal if $x \in \mathfrak{a}_0$.

We shall prove (ii) first. Recall that for each root $\alpha \in S$ we have $c_u(\mathfrak{g}_z) = \mathfrak{g}_{-z}$ (21.21.4.2) and therefore, in the decomposition $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in S} \mathfrak{g}_z$, the subspaces $\mathfrak{h}$ and $\mathfrak{g}_z$ ($\alpha \in S$) are pairwise orthogonal relative to the hermitian scalar product $-B_\mathfrak{g}(x, c_\mathfrak{g}(y))$ (21.19.9). Take in $\mathfrak{h}$ an orthonormal basis $h_1, \ldots, h_t$, and a unit vector $a_1$ in each $\mathfrak{g}_z$, with the notation of (21.21.6), range the roots belonging to $S' \cup S^+_z$ in a sequence $\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_{r+m}$, so that $\alpha_j \in S'$ for $1 \leq j \leq r$, $\alpha_{r+j} \in S^+_z$ for $1 \leq j \leq m$, and such that $\alpha_{r+j}(\mathfrak{z}_0) \leq \alpha_{r+j+1}(\mathfrak{z}_0)$ for $1 \leq j \leq m - 1$. Consider now the orthonormal basis of $\mathfrak{g}$ arranged in the following order:

$$a_{-s-m}, \ldots, a_{-s+1}, h_1, \ldots, h_t, a_1, \ldots, a_r, a_{s+1}, \ldots, a_{s+m}.$$

We shall show that this basis has the required properties. For $x \in \mathfrak{g}_u$ this is clear, because every orthonormal basis will satisfy the condition (a)
21. THE IWASAWA DECOMPOSITION

(21.17.3.2). It is equally clear for $x \in a_0$, because $\text{ad}(x) \cdot h_j = 0$ for $1 \leq j \leq l$ and $\text{ad}(x) \cdot a_\alpha = \alpha(x) a_\alpha$ for all $\alpha \in S$, and furthermore on it $\Rightarrow a_0$ the roots are real-valued (21.8.1). Finally, to verify that condition (b) is satisfied we may restrict attention to the case where $x = a_{r+j}$, $1 \leq j \leq m$. We have $\text{ad}(a_{r+j}) \cdot h_j = \alpha_{r+j}(h_j) a_{r+j}$, and $\text{ad}(a_{r+j}) \cdot a_{-z+h}$ is either zero or belongs to $g_\beta$ if $\beta = \alpha_{r+j} - \alpha_{r+h}$ is a root; but in this latter case we have $\beta(z_0) = \alpha_{r+j}(z_0) - \alpha_{r+h}(z_0)$, so that either $\beta \in S'$ or $\beta \in S''$, or $\beta = -\alpha_{r+k}$, but with $k < h$. Next, $\text{ad}(a_{r+j}) \cdot a_{r+1}$, where $1 \leq h \leq r$, is either zero or belongs to $g_\beta$ if $\beta = \alpha_{r+j} + \alpha_h$ is a root; but then $\beta(z_0) = \alpha_{r+j}(z_0) > 0$, so that $\beta \in S''$. Finally, $\text{ad}(a_{r+j}) \cdot a_{r+k}$ is zero or belongs to $g_\beta$ if $\beta = \alpha_{r+j} + \alpha_{r+k}$ is a root; but then $\beta(z_0) > \alpha_{r+k}(z_0) > 0$, so that $\beta$ is of the form $\alpha_{r+k}$ with $k > h$. This completes the proof of (ii).

For the proof of (i), we observe that $x \mapsto \text{ad}(x)$ is an isomorphism of $g$ onto $\text{ad}(g)$ (21.6.3), it is enough to show that $\text{ad}(g)$ is a complex Lie subalgebra of $\text{ad}(g)$ that is nilpotent, and that $\text{ad}(g_0)$ is a real Lie subalgebra of $\text{ad}(g_0)$ that is solvable (the fact that $\text{ad}(g_0)$ is an ideal in $\text{ad}(g)$ follows from the relation $[a_0, g_0] \subseteq g_0$). Since every subalgebra of a solvable (resp. nilpotent) Lie algebra is solvable (resp. nilpotent), it is enough by virtue of (ii) to consider the Lie algebra $\mathfrak{gl}(n) = M_n(C)$ (where $n = \text{dim}(g)$) and for each integer $k$ such that $0 \leq k \leq n$ the vector subspace $\mathfrak{I}_k$ consisting of the matrices $(x_{kj})$ such that $x_{kj} = 0$ for $j < k$. It is easily verified that

$$[\mathfrak{I}_j, \mathfrak{I}_k] \subseteq \mathfrak{I}_{j+k}$$

which shows that $\mathfrak{I}_0$ (the algebra of lower triangular matrices) is solvable (19.12.3) and that $\mathfrak{I}_1$ (the algebra of lower triangular matrices with zeros on the diagonal) is a nilpotent Lie algebra.

(21.21.10) Let $G_1$ be a connected semisimple Lie group with Lie algebra $g_0$, and let $K_1, A_1, N_1$ be the connected Lie groups immersed in $G_1$ whose respective Lie algebras are $k_0, a_0$ and $n_0$, in the notation of (21.21.7).

(i) The subgroups $K_1, A_1, N_1$ are closed in $G_1$, and $K_1$ contains the center $C_1$ of $G_1$ (21.17.11). The mapping $x \mapsto \exp_{G_1}(x)$ is an isomorphism of $a_0$ onto $A_1$ and a diffeomorphism of $n_0$ onto $N_1$, so that $A_1$ is a commutative group isomorphic to $R^n$ for some $n$, and $N_1$ is a nilpotent group diffeomorphic to $R^m$ for some $m$.

(ii) The mapping $(x, y, z) \mapsto xyz$ is a diffeomorphism of $K_1 \times A_1 \times N_1$ onto $G_1$ (Iwasawa decomposition of $G_1$). The image of $\{e_1\} \times A_1 \times N_1$ under this mapping is a closed solvable subgroup $S_1$ of $G_1$.

Furthermore, if $m_{G_1}$ is a Haar measure on $G_1$, there exists a Haar measure...
on $K_1$ and a left Haar measure $m_{S_1}$ on $S_1$ such that, for every continuous function $f$ on $G_1$ with compact support, we have

$$
(21.21.10.1) \int_{G_1} f(s) \, dm_{G_1}(s) = \int_{K_1 \times S_1} f(xy^{-1}) \, dm_{K_1}(x) \, dm_{S_1}(y).
$$

(Recall that $G_1$ and $K_1$ are unimodular ((21.6.6) and (21.6.10))).

I) Consider first the case where $C_1 = \{e_1\}$, so that $G_1$ may be identified with its adjoint group $\text{Ad}(G_1)$. If $G$ is the complex semisimple subgroup that is the identity component of $\text{Aut}(g) \subset \text{GL}(g)$ (21.17.1), whose Lie algebra $\text{ad}(g)$ is isomorphic to $g$, then $\text{Ad}(G_1)$ is the connected Lie subgroup of $G_1$ whose Lie algebra is $\text{ad}(g_0)$ (21.6.8). We may therefore likewise identify $K_1$, $A_1$, $N_1$ with the connected Lie groups immersed in $\text{GL}(g)$ corresponding to the images $\text{ad}(t_0)$, $\text{ad}(a_0)$, and $\text{ad}(u_0)$ of the real Lie subalgebras $t_0$, $a_0$, $u_0$ under the isomorphism $x \mapsto \text{ad}(x)$ of $g$ onto $\text{ad}(g)$. We shall assume that an orthonormal basis of $g$ has been chosen to satisfy the conditions of (21.21.9(ii)). Since the matrices of $\text{ad}(a_0)$ are real and diagonal, the group $A_1$ consists of real diagonal matrices with diagonal entries $> 0$, and it is clear that the exponential mapping of $\text{GL}(g)$ is an isomorphism of $\text{ad}(a_0)$ onto $A_1$, and that $A_1$ is closed in $\text{GL}(g)$.

As to the group $N_1$, we observe that in the notation of (21.21.9) we have $\text{ad}(u_0) \subset \mathfrak{t}_1$, so that $N_1$ is a connected Lie group immersed in the connected Lie group $T_1$, immersed in $\text{GL}(g)$ with Lie algebra $\mathfrak{t}_1$. Now we have the following proposition:

$(21.21.10.2)$ The group $T_1$ is the closed subgroup of all matrices $I + N$, where $N \in \mathfrak{t}_1$, and the mapping $N \mapsto \exp(N)$ (where exp is the exponential map of $\text{GL}(g)$) is a diffeomorphism of $\mathfrak{t}_1$ onto $T_1$.

It is immediate that $N^n = 0$ for all $N \in \mathfrak{t}_1$, where $n = \dim(g)$, and it is clear that the matrices $I + N$ form a closed subgroup of $\text{GL}(g)$. If we put

$$
P_1(N) = N - \frac{1}{2} N^2 + \frac{1}{3} N^3 - \cdots + (-1)^{n-2} \frac{1}{n-1} N^{n-1},
$$

$$
P_2(N) = I + \frac{1}{1!} N + \frac{1}{2!} N^2 + \cdots + \frac{1}{(n-1)!} N^{n-1},
$$

then we have $\exp(N) = P_2(N) \in T_1$, and $P_1(N) \in \mathfrak{t}_1$ for all $N \in \mathfrak{t}_1$. To prove the proposition it is enough to show that $P_2(P_1(N)) = I + N$ and $P_1(P_2(N) - I) = N$ for all $N \in \mathfrak{t}_1$. Now, for $x$ real and sufficiently small we have

$$
\log(1 + x) = \sum_{n=1}^{\infty} (-1)^{n-1} x^n/n \quad (9.3.7),
$$

and for all real $x$ we have
\[ e^x = \sum_{p=0}^{\infty} \frac{x^p}{p!} \]; the theorem of substitution of power series in a power series (9.2.1) shows that

\[
\sum_{n_1 + n_2 + \cdots + n_p = k, \ n_1 \geq 1, \ldots, n_p \geq 1} \frac{1}{p!} \frac{(-1)^n}{n_1 n_2 \cdots n_p} = \begin{cases} 1 & \text{if } k = 1, \\ 0 & \text{if } k > 1, \end{cases}
\]

\[
\sum_{p_1 + p_2 + \cdots + p_n = k, \ p_i \geq 1, \ldots, p_n \geq 1} \frac{(-1)^{p-1}}{p_1! p_2! \cdots p_n!} = \begin{cases} 1 & \text{if } k = 1, \\ 0 & \text{if } k > 1, \end{cases}
\]

and the coefficients of \(N^k\) in \(P_2(P_1(N))\) and \(P_1(P_2(N) - I)\), for \(k < n\), are precisely the left-hand sides of these two relations.

Since \(\text{ad}(\mathfrak{n}_0)\) is closed in \(\mathfrak{t}_1\), it follows from (21.21.10.2) that \(\mathfrak{n}_1\) is closed in \(\mathfrak{t}_1\), since \(\mathfrak{t}_1\) is closed in \(\text{GL}(\mathfrak{g})\), it follows that \(\mathfrak{n}_1\) is also closed in \(G\) (because the topology of \(G\) is induced by that of \(\text{GL}(\mathfrak{g})\)).

Since \(\mathfrak{u}_0\) is an ideal of \(\mathfrak{s}_0 = \mathfrak{a}_0 \oplus \mathfrak{u}_0\), the elements of \(A_1\) normalize \(\mathfrak{n}_1\) (19.11.4), so that \(A_1 \mathfrak{n}_1 = \mathfrak{n}_1 A_1\), which shows that \(S_1 = A_1 \mathfrak{n}_1\) is the connected group immersed in \(G\) with Lie algebra \(\mathfrak{s}_0\). Moreover, if \(D \in A_1\) and \(U \in \mathfrak{n}_1\), then \(D\) is the diagonal of the triangular matrix \(DU\). If \((D_n U_n)\) is a sequence of matrices in \(S_1\) converging to a limit in \(T_1\), then the sequence \((D_n)\) also converges, and therefore so also does the sequence \((U_n)\); since \(A_1\) and \(\mathfrak{n}_1\) are closed, it follows that \(S_1\) also is closed. Moreover, the mapping \((D, U) \mapsto DU\) of \(A_1 \times \mathfrak{n}_1\) onto \(S_1\) is a diffeomorphism, the inverse mapping being \(X \mapsto (D(X), D(X)^{-1} X)\), where \(D(X)\) is the diagonal of \(X\).

In the situation under consideration, we know that \(K_1\) is a subgroup of \(\text{GL}(\mathfrak{g})\) consisting of unitary matrices (21.17.4). It follows that \(K_1 \cap S_1 = \{ I \}\): for the inverse of a lower triangular matrix is again lower triangular, and therefore cannot be unitary unless it is a diagonal matrix, with diagonal entries that are complex numbers of absolute value 1; hence \(K_1 \cap S_1\) consists of diagonal matrices whose diagonal entries are simultaneously positive real numbers and complex numbers of absolute value 1, and the only such matrix is \(I\).

Since \(K_1\) is compact, \(S_1 K_1\) is closed in \(G\) (12.10.5); its image under the canonical mapping \(p: G_1 \to G_1/K_1\) is therefore closed (12.10.5). But if \(\{x_0\} = p(K_1)\), this image is just the orbit \(S_1 \cdot x_0\) for the action of \(S_1\) on the space \(G_1/K_1\). Now for this action the stabilizer of \(x_0\) is \(S_1 \cap K_1 = \{ I \}\), hence \(S_1 \cdot x_0\) is a submanifold of \(G_1/K_1\), of dimension equal to that of \(S_1\), hence to that of \(G_1/K_1\) (16.10.7). It follows that \(S_1 \cdot x_0\) is both open and closed in the connected space \(G_1/K_1\), so that \(S_1 \cdot x_0 = G_1/K_1\), or equivalently \(S_1 K_1 = G_1 = K_1 S_1\) (since \(K_1\) and \(S_1\) are subgroups of \(G_1\)).

The \(C^\infty\) mapping \((x, s) \mapsto xs\) of \(K_1 \times S_1\) into \(G_1\) is therefore bijective; we have to show that it is a diffeomorphism. At each point \((x_1, s_1) \in K_1 \times S_1\),
every tangent vector to $K_1$ (resp. $S_1$) can be written uniquely in the form $x_1 \cdot v$ (resp. $w \cdot s_1$), where $v \in \mathfrak{f}_0$ (resp. $w \in \mathfrak{s}_0$) (16.9.8). The tangent linear mapping to $(x, s) \mapsto xs$ at the point $(x_1, s_1)$ is therefore (16.9.9)

$$(x_1 \cdot v, w \cdot s_1) \mapsto x_1 \cdot (v + w) \cdot s_1$$

which is clearly bijective, because the sum $\mathfrak{f}_0 \oplus \mathfrak{s}_0$ is direct. The result now follows from (16.8.8).

(II) We now consider the general case. Let $p_1 : G_1 \to G_1/C_1$ be the canonical homomorphism of $G_1$ onto its adjoint group, so that $p_1(K_1)$, $p_1(A_1)$, and $p_1(N_1)$ are connected Lie groups immersed in $p_1(G_1)$, with Lie algebras respectively $\mathfrak{k}_0$, $\mathfrak{a}_0$, and $\mathfrak{n}_0$. Using the fact that $p_1(A_1)$ and $p_1(N_1)$ are simply connected, we may repeat without any substantial change the argument of (21.17.10), by showing first that $A_1$ and $N_1$ are the identity components of $p_1^{-1}(p_1(A_1))$ and $p_1^{-1}(p_1(N_1))$, respectively. Then, using as in (21.17.10) the fact that $C_1 \subset K_1$, we see that $(x, y, z) \mapsto xyz$ is a bijection of $K_1 \times A_1 \times N_1$ onto $G_1$, and finally, using the result of (I), that it is a diffeomorphism.

To prove (21.21.10.1), denote by $z \mapsto (p(z), q(z))$ the diffeomorphism of $G_1$ onto $K_1 \times S_1$ that is the inverse of $(x, s) \mapsto xs$. Let $u \in \mathcal{K}(K_1)$ be a function with values $\geq 0$. As $v$ runs through $(x, s) \mapsto xs$, the mapping

$$v \mapsto \int u(p(z))v(q(z)) \ dm_{G_1}(z)$$

is a positive linear form on $\mathcal{K}(S_1)$ which is \textit{right-invariant}, because $G_1$ is unimodular and $p(z) = p(z)$ for $s \in S_1$; it can therefore be written as

$$v \mapsto J(u) \int v(s^{-1}) \ dm_{S_1}(s),$$

where $J(u)$ is a constant $\geq 0$ (14.1). We next extend $J$ to a positive linear form on $\mathcal{K}(K_1)$ in the obvious way; since $p(xz) = p(z)$ for $x \in K_1$, this linear form is \textit{left-invariant} and hence, by a suitable choice of $m_{K_1}$, it can be taken to be equal to $m_{K_1}$ (14.1). The formula (21.21.10.1) is therefore established for all functions $f$ of the form $z \mapsto u(p(z))v(q(z))$. To complete the proof, we invoke (13.21.1) and the existence of the homeomorphism $(x, s) \mapsto xs$ of $K_1 \times S_1$ onto $G_1$.

The relations between the Iwasawa decomposition and the Cartan decomposition of $G_1$ (21.18.8) are described in the next proposition:

(21.21.11) \textit{With the notation of (21.21.10) and Section 21.18, let $\tau_1$ be the involutory automorphism of $G_1$ for which $K_1$ is the set of fixed points, and such that $\tau_1(z) = z^{-1}$ for $z \in P_1$ (21.18.10). Then the mapping $f_1 : s \mapsto \tau_1(s)s^{-1}$ is a diffeomorphism of $S_1$ onto $P_1$.}
Since each $x \in G_1$ can be written uniquely as $x = zy$ with $z \in P_1$ and $y \in K_1$, we have $\tau_1(x)x^{-1} = z^{-2} \in P_1$, so that in particular $f_1(S_1) \subset P_1$. The mapping $f_1$ is a bijection of $S_1$ onto $P_1$: for the relation $\tau_1(s')s''^{-1} = \tau_1(s''s')$ for $s', s'' \in S_1$ implies that $\tau_1(s''^{-1}s') = s''^{-1}s'$, so that $s''^{-1}s' \in K_1$ and therefore $s'' = s'$ since $K_1 \cap S_1 = \{e_1\}$. Moreover $f_1(S_1) = P_1$, for every $z \in P_1$ is uniquely of the form exp$_{G_1}(u)$ with $u \in p_0$; there exist two elements $x' \in K_1$ and $s' \in S_1$ such that $z' = x's'^{-1} = \exp_{G_1}(\frac{1}{2}u)$ (21.21.10); since $z' \in P_1$, we have

\[ z = z'^2 = \tau_1(x'^{-1})z' = \tau_1(s')\tau_1(x'^{-1})x's'^{-1} = \tau_1(s')s'^{-1} = f_1(s') \]

since $\tau_1(x') = x'$. Finally, this calculation shows that the inverse of the mapping $f_1 : S_1 \to P_1$ is the mapping $z \mapsto q(\exp_{G_1}(\frac{1}{2}l(z)))$, where $q : G_1 \to S_1$ is the mapping defined in the proof of (21.21.10), and $l : P_1 \to p_0$ is the inverse of the restriction to $p_0$ of the exponential map. This shows that $f_1$ is a diffeomorphism of $S_1$ onto $P_1$.

**Remarks**

(21.21.12) (i) With the notation of (21.21.10), $K_1$ is isomorphic to the product of a compact group $K_1'$ and a vector group $R^p$ (21.6.9), whence we recover the fact (21.18.8) that $G_1$ is diffeomorphic to the product of a compact group $K_1'$ and a vector space $R^N$. Moreover, the compact subgroup $K_1'$ of $K_1$ is maximal in $G_1$, for the components in $A_1$ and in $N_1$ of an element of $G_1$ will generate subgroups that are noncompact if they are $\neq \{e_1\}$; hence every compact subgroup of $G_1$ containing $K_1'$ must be contained in $K_1$, and hence in $K_1'$.

(ii) It can be proved that the Lie algebras $t_0$, $a_0$, $u_0$ that figure in the Iwasawa decomposition are determined up to isomorphism. The dimension of $a_0$ is called the rank of the symmetric space $G_1/K_1$.

(iii) If $g_0$ is a normal real form of $g$ (21.18.9), we have $a_0 = it$, and the rank of $g_0$ is equal to that of $g_w$. It can be shown that this condition characterizes the normal forms of $g$, which are all isomorphic. We have in this case $S' = \emptyset$, and $S''_+$ is the set $S_+$ of all positive roots, relative to the ordering defined in (21.14.5).

We have then

(21.21.12.1) \[ g_{|R} = g_w \oplus it \oplus u_{|R}. \]

For the argument of (21.21.7) shows that the sum on the right-hand side is direct. Also $g_w$ contains $t$, hence the right-hand side of (21.21.12.1) contains
\[ h = t \oplus it; \] also \( g_u \) contains the elements \( e_x - e_{-x} \) and \( i(e_x + e_{-x}) \) for \( x \in \mathbb{S}^+ \), and since \( n \) contains the elements \( e_x \) and \( i e_x \) for \( x \in \mathbb{S}^+ \), the sum on the right-hand side of (21.21.12.1) contains \( e_x \) and \( i e_x \) for all \( x \in \mathbb{S} \), and is therefore equal to \( g \). The same proof as in (21.21.10) then shows that if \( G \) is a complex connected Lie group with Lie algebra \( g \), and if \( G_u, A, \) and \( N \) are the connected real Lie groups immersed in \( G_{\mathbb{R}} \) that correspond respectively to the subalgebras \( g_u, \) \( i t \), and \( n_{\mathbb{R}} \), then \( G_u \) is compact, \( A \) and \( N \) are closed subgroups of \( G \), and the mapping \((x, y, z) \mapsto xyz \) is a diffeomorphism of \( G_u \times A \times N \) onto \( G_{\mathbb{R}} \).

**Example (I)** of (21.18.9), we may take \( a_0 \) to be the set of real diagonal \( n \times n \) matrices with zero trace; then the \( g_x \) corresponding to the positive roots \( x \) are the spaces \( CE_x \) for \( r = s \) (21.12.1), and \( n_0 \) is therefore the nilpotent Lie algebra of all upper triangular real matrices with zeros on the diagonal.

**Example (II)** (21.21.14) With the notation of (21.21.7) and (21.21.10), for each vector \( x \in p_0 \) there exists \( s \in K_1 \) such that \( Ad(s) \cdot x \in a_0 \).

Since we may replace \( K_1 \) by its adjoint group, we may assume that \( K_1 \) is compact. We have \( Ad(s) \cdot p_0 = p_0 \) for all \( s \in K_1 \) ((21.18.4.2) and (19.11.3)), and the restriction of the Killing form \( B_g \) to \( p_0 \times p_0 \) is positive definite and invariant under the action \((s, z) \mapsto Ad(s) \cdot z \) of \( K_1 \) on \( p_0 \). For brevity let \( ||z|| = (B_g(z, z))^{1/2} \) for \( z \in p_0 \), and consider as in (21.7.7.1) the continuous function \( s \mapsto ||Ad(s) \cdot x - z_0||^2 \) on \( K_1 \), where \( z_0 \) is the element defined in (21.21.6); this function attains its minimum at a point \( s_0 \), and by replacing \( x \) by \( Ad(s_0) \cdot x \) we may suppose that \( s_0 = e_1 \), the identity element of \( K_1 \). By expressing that for each \( y \in t_0 \) the derivative of the function \( t \mapsto ||Ad(exp(ty)) \cdot x - z_0||^2 \) vanishes at \( t = 0 \) we obtain, using the invariance of \( B_g \),

\[
0 = 2B_g([y, x], x - z_0) = 2B_g(y, [x, x - z_0])
\]

for all \( y \in t_0 \). Since the restriction of \( B_g \) to \( g_0 \times g_0 \) is nondegenerate, and since \( t_0 \) and \( p_0 \) are orthogonal supplements of each other relative to this form, the formula just written implies that \( [x, z_0] \in p_0 \). But now \( [p_0, p_0] \subset t_0 \), and hence \( [x, z_0] \in p_0 \cap t_0 = \{0\} \); since \( x(z_0) \neq 0 \) for each root \( x \in \mathbb{S}' \) (21.21.6), we conclude that \( x \) lies in the intersection of \( g_0 \) and \( h \), and \( g_x \subset t_0 \oplus it_0 \) for \( x \in \mathbb{S}' \) by virtue of (21.21.5), we have \( x \in t_0 \oplus a_0 \), and finally \( x \in a_0 \) because \( x \in p_0 \). This completes the proof.

(21.21.15) With the notation of (21.21.10), we have \( G_1 = K_1 A_1 K_1 \).
Since \( G_1 = P_1 K_1 \) (21.18.8), it is enough to remark that every element of \( P_1 \) is of the form \( \exp(z) \) with \( z \in p_0 \), and that \( z = \text{Ad}(s) \cdot x \) for some \( s \in K_1 \) and \( x \in a_0 \) (21.21.14); since \( \exp(\text{Ad}(s) \cdot x) = s(\exp(x))s^{-1} \) (19.11.2.3), we have \( P_1 \subset K_1 A_1 K_1 \).

**PROBLEMS**

1. (a) With the notation of Sections 21.18 and 21.21, let \( m_0 \) be the intersection of \( l_0 \) with the centralizer of \( a_0 \) in \( g_0 \), and let \( l_0 \) (resp. \( g_0 \)) be the subspace of \( l_0 \) orthogonal to \( m_0 \) (resp. the subspace of \( p_0 \) orthogonal to \( a_0 \)) relative to the form \(-B_2(x, c_2(y))\). Let \( l = l_0 + i l_0 \), \( a = a_0 + i a_0 \), \( m = m_0 + im_0 \), \( l = l_0 + il_0 \), \( q = g_0 + ig_0 \). Show that \( m \) is the direct sum of \( h \cap l \) and the subspaces \( g_0 + ig_0 \). If \( s \) is a basis element of \( g_0 \) over \( C \), then the elements \( x_s + \varphi(x_s) \) with \( x \in S^* \) form a basis of \( l \), and the elements \( x_s - \varphi(x_s) \) with \( x \in S^* \) form a basis of \( q \).

(b) Deduce from (a) that there exists an element \( x_0 \in s \) such that the centralizer of \( R x_0 \) in \( g_0 \) is \( a + m \). Hence show, with the help of (21.21.14), that for each commutative subalgebra \( b_0 \) of \( p_0 \) there exists \( s \in K_2 \) such that \( \text{Ad}(s) b_0 \subset a_0 \).

(c) Show that for each \( x \in S^* \) the intersection \( g_0'' = g_0 \cap g_0 = \text{one-dimensional over} \ R \). Show that there exists \( x' \in g_0'' \) such that, if we put \( x'' = c_s(x') \in g_0'' \) and \( h'' = [x''_s, x''_s] \), then we have \( [h'', x''] = 2x'' \) and \( [h'', x''_s] = -2x''_s \). Also \( y''_s = x''_s + x''_s \) in \( t_0 \), and \( x''_s = x''_s - x''_s \) in \( p_0 \).

(d) Let \( M \) and \( M' \) be, respectively, the centralizer and the normalizer of \( ia_0 \) in \( K_2 \) (i.e., the intersections of \( K_2 \) with the centralizer and normalizer of \( a_0 \) in \( G_2 \), cf. (19.11.13)). Show that \( M \) and \( M' \) have the same Lie algebra \( m_0 \). (Observe that if \( u \in l_0 \) is such that \( [u, x] \in ia_0 \) for all \( x \in ia_0 \), then \( B_2(\text{ad}(u) \cdot x, \text{ad}(u) \cdot x) = 0 \).) The finite group \( W(G_2/K_2) = M'M/M \) is called the *Weyl group* of the symmetric space \( G_2/K_2 \); it acts faithfully on \( ia_0 \) with the notation of (c), show that for each \( x \in S^* \) there exists a real number \( \xi \) such that \( r_x = \exp(\xi y''_s) \) belongs to \( M' \) and has as image in \( W(G_2/K_2) \) the orthogonal reflection \( s''_x \) with respect to the hyperplane with equation \( \alpha(u) = 0 \) in \( ia_0 \).

(e) In order that a linear form \( \lambda \) on \( ia_0 \) should be the restriction of a root \( x \in S^* \), it is necessary and sufficient that there exist \( x \neq 0 \) in \( ia_0 \) such that \( \text{ad}(u)\cdot x = (\lambda(u))^2 \cdot x \) for all \( u \in ia_0 \). Deduce that every element of the Weyl group \( W(G_2/K_2) \) permutes the restrictions to \( ia_0 \) of the roots \( x \in S^* \).

(f) A *Weyl chamber* in \( ia_0 \) is any connected component of the complement of the union of the hyperplanes \( \alpha(u) = 0 \) in \( ia_0 \) for all \( x \in S^* \). Show that \( W(G_2/K_2) \) acts simply transitively on the set of Weyl chambers in \( ia_0 \), and is generated by the orthogonal reflections \( s''_x \), \( x \in S^* \). (If \( C_1, C_2 \) are two Weyl chambers and if \( W \) is the subgroup of \( W(G_2/K_2) \) generated by the \( s''_x \), consider for \( u_1 \in C_1 \) and \( u_2 \in C_2 \) an element \( w \in W \) such that the distance from \( u_1 \) to \( w \cdot u_2 \) is as small as possible; show that this implies that \( w \cdot u_2 \in C_1 \). To show that the action of \( W(G_2/K_2) \) is simply transitive, follow the proof of (21.11.10).)

(g) The image \( A_2 \) of \( ia_0 \) under the exponential mapping \( \exp \), is a torus contained in \( P_2 \), and \( P_2 \) is the union of the tori \( sA_2 s^{-1} \) for \( s \in K_2 \).

2. With the same notation as in Problem 1, let \( \Sigma \) denote the set of restrictions to \( ia_0 \) of the roots \( x \in S^* \). For each \( \lambda \in \Sigma \), let \( \Sigma(\lambda) \) denote the set of \( \alpha \in S^* \) of which \( \lambda \) is the restriction, and \( m(\lambda) \) the number of elements of \( \Sigma(\lambda) \); \( m(\lambda) \) is called the *multiplicity* of the linear form \( \lambda \).
(a) The set $\Sigma$ satisfies the conditions $S_1$, $S_2$, and $S_3$ of (21.10.3) relative to the space $(a_0)^s$: in other words, $\Sigma$ is a root system, in general nonreduced, i.e., not necessarily satisfying $S_4$ (cf. Problem 3). The elements $\lambda \in \Sigma$ are called the roots of $G_2/K_2$ relative to the choice of the maximal commutative subalgebra $a_0$ of $p_0$.

(b) For each $\lambda \in \Sigma$ let $l_1$ (resp. $l_0$) be the intersection of $l_1$ (resp. $l_0$) with the sum of the spaces $a_x + a_{-x}$ for $x \in \Sigma(\lambda)$; they are real vector spaces of dimension $m(\lambda)$. For $\lambda, \mu \in \Sigma$ we have

$$[l_\lambda, l_\mu] = l_{\lambda + \mu} + l_{\lambda - \mu}, \quad [l_\lambda, l_0] = i p_{\lambda + \mu} + i p_{\lambda - \mu},$$

where, if $\lambda + \mu = 0$ (resp. $\lambda - \mu = 0$), $l_{\lambda + \mu}$ (resp. $l_{\lambda - \mu}$) is to be replaced by $l_0$, and $i p_{\lambda + \mu}$ (resp. $i p_{\lambda - \mu}$) by $i l_0$.

(c) For each $\lambda \in \Sigma$ and each integer $k \in \mathbb{Z}$, let $u_{\lambda, k}$ be the affine hyperplane in $a_0$ given by the equation $\lambda(u) = 2k\pi i$: it is the intersection of $a_0$ with the affine hyperplanes $u_{\lambda, k}$ for all roots $\alpha \in \Sigma(\lambda)$. The union of the hyperplanes $u_{\lambda, k}$ for all $\lambda \in \Sigma$ and $k \neq 0$ is the set of $u \in a_0$ at which the restriction to $a_0$ of the tangent linear mapping $T_u(\exp_{a_0})$ is not bijective. If we identify $i p_0$ with the tangent space at $x_0$ to $G_2/K_2$ (or $G_2/K_2'$), the points $u \in a_0$, for which the tangent mapping $T_u(\exp_{a_0})$ (Section 21.18, Problem 7) is not bijective are those for which $2u$ belongs to the union of the $u_{\lambda, k}$ with $k \neq 0$.

(d) Show that, for all the points $x = \exp_{a_0}(u)$ such that $u \in a_0$ belongs to none of the $u_{\lambda, k}$, but $2u$ does lie in their union, the tangent mapping $T_u(\pi')$, where $\pi' : P_2 \to G_2/K_2'$ is the canonical mapping, is not bijective (use Section 21.18, Problem 7(a)). Does this result remain true when $u$ belongs to one of the $u_{\lambda, k}$?

(e) A point $x \in P_2$ is said to be singular if the dimension of the orbit of $x$ under the action $(s, t) \to sts^{-1}$ of $K_2$ on $P_2$ is strictly less than $\dim(K_2/M)$. The singular points of $P_2$ that belong to $A$ are the points lying in the union of the $U_{\lambda, k}$, $\lambda \in \Sigma$: we have $U_{\lambda, k} = U^\ast_{\lambda, k}$ in $A$ that is the image under $\exp_{a_0}$ of any of the hyperplanes $u_{\lambda, k}$. We have $U^{\ast}_{\lambda, k} = U^\ast_{\lambda, k}$, but $U^{\ast}_{\lambda, k} \neq U^\ast_{\mu, k}$ if both $\lambda$ and $2\lambda$ are in $\Sigma$. A point $x$ is said to be regular if it is not singular. Let $A_{reg}$ denote the open set in $A$ consisting of the regular points of $A$.

(f) Show that the mapping $(s, t) \to sts^{-1}$ of $K_2 \times A$ into $P_2$ is a submersion at all points $(s, t)$ such that $t \in A_{reg}$ (argue as in (21.15.1)). Deduce that $(K_2/M) \times A_{reg}$ is a covering, with $\text{card}(W(G_2/K_2))$ sheets, of an open subset $V$ of $P_2$ consisting of regular points and such that the complement of $V$ is negligible. This complement is the union of the sets $P^\ast_\lambda$, where $P^\ast_\lambda$ is the image under $(s, t) \to sts^{-1}$ of the set $M^\ast_\lambda \times U^\ast_{\lambda, k}$, and $M^\ast_\lambda$ is the centralizer of $U^\ast_{\lambda, k}$ in $K_2$. Show that $P^\ast_\lambda$ is the image under a $C^\ast$ mapping of a manifold of dimension $\leq \dim(P_2) - (1 + r)$, where $r$ is the smallest value of the multiplicity $m(\lambda)$ for roots $\lambda \in \Sigma$ such that $2\lambda \notin \Sigma$.

3. Take $c_0$ as in example (III) of (21.18.11), so that $G_2$ is the quotient of $SU(p + q)$ by its center, and $K_2$ is the quotient of $K_2$ by the center of $SU(p + q)$; then $i p_0$ is the space of matrices of the form \[
\begin{pmatrix}
0_p & Z \\
-Z & 0_q
\end{pmatrix},
\]
where $Z$ is a $p \times q$ complex matrix.

Let $a_0$ denote the subspace of $i p_0$ spanned (over $R$) by the matrices $E_{j, p+j} - E_{-j, p+j} = H_j$ for $1 \leq j \leq q$. Let $\{e_j\}_{1 \leq j \leq q}$ be the basis dual to $\{H_j\}_{1 \leq j \leq q}$, so that $e_j(H_k) = \delta_{jk}$. Show that $a_0$ is a maximal commutative subalgebra of $i p_0$. The roots of the corresponding system $\Sigma$ are

$$\pm e_j \quad (1 \leq j \leq q), \quad \pm 2e_j \quad (1 \leq j \leq q), \quad \pm e_j \pm e_h \quad (1 \leq j < h \leq q).$$
21. THE IWASAWA DECOMPOSITION

with multiplicities

\[ m(e_j) = 2(p - q), \quad m(2e_j) = 1, \quad m(e_j \pm e_k) = 2. \]

Determine the subspaces \( I_1 \) and \( I_p \) corresponding to these roots.

4. With the notation of Problem 1, show that for the compact symmetric space \( G_2/K_2 \) the following properties are equivalent:

(a) For each system of four points \( p, q, r, s \) in \( G_2/K_2 \) such that \( d(p, q) = d(r, s) \), where \( d \) is the Riemannian distance, there exists \( x \in G_2 \) such that \( x \cdot p = r \) and \( x \cdot q = s \).

(b) The group \( K_2 \) acts transitively on the set of lines passing through the origin in the tangent space \( i_{e_0} \) at the point \( \pi(e) \) of \( G_2/K_2 \).

(\( \iota \)) For all \( u \in ip_0 \) we have \( ip_0 = Ru + [I_1, u] \).

(\( \delta \)) \( G_2/K_2 \) has rank 1, in other words, \( i_{e_0} \) has dimension 1.

(c) The sectional curvature \( A(P_x) \) along a tangent plane \( P_x \) to \( G_2/K_2 \) (20.21.1) is never zero.

(To prove that (a) and (b) are equivalent, use the Hopf-Rinow theorem (20.18.5). To prove the equivalence of (\( \iota \)) and (\( \delta \)), use Problem 1(e); to prove the equivalence of (\( \delta \)) and (\( \iota \)), consider an orthonormal basis of \( ip_0 \) consisting of eigenvectors of the endomorphism \( \nu \mapsto [\nu, \nu], u \) (cf. Section 20.20, Problem 2, and (21.21.2)).)

5. With the notation of Sections 21.18 and 21.21, show that the following conditions are equivalent:

(a) The rank of \( g_0 \) (or of \( G_2/K_2 \)) is equal to the rank of \( g \) (or of \( G_u \)).

(b) All the roots \( \lambda \in \Sigma \) have multiplicity 1 (Problem 2).

(\( \iota \)) The rank of \( g \) is equal to \( 2 \dim(ip_0) - \dim(q) \).

(\( \delta \)) The rank of \( g \) is equal to \( \dim(ip_0) - \dim(t_0) \).

6. (a) With the notation of Section 21.21, show that for a root \( \alpha \in S^+ \) the following conditions are equivalent:

(1) \( \alpha \cdot \varphi = -\alpha \), (2) \( c_0(q_\alpha) = q_\alpha \), (3) the restriction of \( \alpha \) to \( t_0 \cap t \) is zero. When these conditions are satisfied, the subalgebra \( t_0 \cap t \) of \( t_0 \) is not a maximal commutative subalgebra. (Observe that we also have \( c_0(q_{-\alpha}) = q_{-\alpha} \) and deduce, using Problem 1(c), that \( y^\alpha \) centralizes \( t_0 \cap t \).)

(b) Deduce from (a) that for each \( \lambda \in \Sigma \) there can exist only one root \( \alpha \in \Sigma(\lambda) \) such that \( \alpha \cdot \varphi = -\alpha \). For such a root to exist it is necessary and sufficient that the multiplicity \( m(\lambda) \) should be odd. (Observe that if \( \alpha \in \Sigma(\lambda) \), then also \( \alpha \cdot \varphi \in \Sigma(\lambda) \).

(c) Suppose that \( m(\lambda) \) is even for all \( \lambda \in \Sigma \). Show that \( t_0 \) is the direct sum of \( t_0 \cap t \) and the distinct subspaces \( I_0 \cap (q_{\alpha} + q_{-\alpha} + q_{\alpha \cdot \varphi} + q_{-\alpha \cdot \varphi}) \), and that \( I_0 \cap t \) is a maximal commutative subalgebra of \( t_0 \).

(d) If \( \alpha \in S^+ \) is such that \( \alpha \cdot \varphi = -\alpha \), show that if \( u^\alpha \) denotes the hyperplane in \( a_0 \) with equation \( \alpha(x) = 0 \), then the sum of \( u^\alpha \), \( t_0 \cap t \), and \( Ry^\alpha \) is a commutative subalgebra of \( g_0 \), whose complexification is also the complexification of a maximal commutative subalgebra of \( g_0 \) (a "Cartan subalgebra" of \( g_0 \), cf. Section 21.22, Problem 4). Deduce that if there exist \( r \) roots \( \alpha \in S^+ \) such that \( \alpha \cdot \varphi = -\alpha \) and \( [g_{\alpha}, g_{\beta}] = 0 \) for any two of these roots, then there exist \( r \) Cartan subalgebras in \( g_0 \) with the property that no two of them are transforms of one another by automorphisms of \( g_0 \). (Consider the commutative subgroups of \( Ad(G_1) \) having these \( r \) subalgebras as their Lie algebras.)
22. CARTAN'S CRITERION FOR SOLVABLE LIE ALGEBRAS

In this section and the next, the Lie algebras under consideration are Lie algebras over either \( \mathbb{R} \) or \( \mathbb{C} \), unless the contrary is expressly stated.

\[ (21.22.1) \quad \text{Every finite-dimensional nilpotent (21.21.8) Lie algebra } \mathfrak{g} \text{ is solvable.} \]

It is enough to prove that \( \mathfrak{g} \neq \mathfrak{g} \); for every Lie subalgebra of a nilpotent Lie algebra is evidently nilpotent, so that by induction we shall have \( \mathfrak{g}^{k+1} \neq \mathfrak{g}^k \), and if \( \dim(\mathfrak{g}) = n \) this will imply that \( \mathfrak{g}^n = 0 \). By hypothesis, there exists an integer \( r \) satisfying (21.21.8.1). If we had \( \mathfrak{g}(\mathfrak{g}) = \mathfrak{g} \), then for a basis \( (u_j)_{1 \leq j \leq n} \) of \( \mathfrak{g} \), the sum of the subspaces \( \text{ad}(u_j) \cdot \mathfrak{g} \) would be equal to \( \mathfrak{g} \). By induction, it would follow that the sum of the subspaces \( (\text{ad}(u_j) \circ \text{ad}(u_j) \circ \cdots \circ \text{ad}(u_j)) \cdot \mathfrak{g} \) (where \( (j_k)_{1 \leq k \leq r} \) runs through the set of all sequences of \( r \) elements of \( [1, n] \)) would be equal to \( \mathfrak{g} \), contrary to (21.21.8.1).

\[ (21.22.2) \quad \text{(Engel's theorem) Let } \mathfrak{g} \text{ be a finite-dimensional Lie algebra such that for each } x \in \mathfrak{g} \text{ the endomorphism } \text{ad}(x) \text{ of the vector space } \mathfrak{g} \text{ is nilpotent. Then } \mathfrak{g} \text{ is a nilpotent Lie algebra.} \]

This statement is equivalent to the following:

\[ (21.22.2.1) \quad \text{If } E \text{ is a finite-dimensional vector space and } \mathfrak{g} \text{ is a Lie subalgebra of } \mathfrak{gl}(E) \text{ consisting of nilpotent endomorphisms of } E, \text{ then there exists an integer } r \text{ such that } \mathfrak{g}^r = \{0\}. \]

(If \( A \) and \( B \) are two vector subspaces of \( \mathfrak{gl}(E) = \text{End}(E) \), we denote by \( AB \) the vector subspace of all linear combinations of products of elements of \( A \) with elements of \( B \) in the algebra \( \text{End}(E) \), and we define \( A^r \) inductively to be \( A^r \cdot A \) for all integers \( r \geq 2 \).)

The proof is by induction on \( n = \dim(\mathfrak{g}) \); for \( n = 1 \), the result is trivial. Let \( \mathfrak{h} \neq \mathfrak{g} \) be a Lie subalgebra of \( \mathfrak{g} \) whose dimension \( m \) is maximal among proper subalgebras of \( \mathfrak{g} \). The endomorphisms \( \text{ad}(X) \) of the vector space \( \mathfrak{g} \) (where \( \text{ad}(X) \cdot Y = XY - YX \)) as \( X \) runs through \( \mathfrak{h} \) form a Lie subalgebra \( \mathfrak{h}_1 \) of \( \mathfrak{gl}(\mathfrak{g}) \), of dimension \( m < n \). Furthermore, each of the endomorphisms \( \text{ad}(X) \) is nilpotent, for it is immediate by induction on \( r \) that \( \text{ad}(X)^r \cdot Y \) is a linear combination of the products \( X^p Y X^q \) such that \( p + q = r \), hence if \( X^m = 0 \) we have \( \text{ad}(X)^{2s} = 0 \). The inductive hypothesis implies that
\[ h'_t = \{0\} \] for some integer \( t > 0 \). Let \( Z \) be an element of \( g \) that does not belong to \( \mathfrak{h} \), and let \( s \leq t \) be the largest integer such that there exist \( s \) elements \( X_1, \ldots, X_s \in \mathfrak{h} \) for which \( Y = (\text{ad}(X_1) \text{ad}(X_2) \cdots \text{ad}(X_s)) \cdot Z \notin \mathfrak{h} \). Then, by definition, we have \( \text{ad}(X) \cdot Y = [X, Y] \in \mathfrak{h} \) for all \( X \in \mathfrak{h} \), and therefore the vector subspace of \( g \) spanned by \( \mathfrak{h} \) and \( Y \), of dimension \( m + 1 \), is a Lie subalgebra of \( g \), and hence by the definition of \( \mathfrak{h} \) is equal to \( g \). Also, we have by hypothesis \( Y^p = 0 \) for some integer \( p > 0 \), and \( \mathfrak{h}^q = \{0\} \) for some integer \( q > 0 \) by virtue of the inductive assumption. We shall deduce from this that, for each sequence \( (T_j)_{1 \leq j \leq pq} \) of elements of \( g \), we have \( T_1 T_2 \cdots T_{pq} = 0 \), in other words, that \( g^{pq} = \{0\} \). Clearly we may assume that each \( T_j \) is either equal to \( Y \) or else belongs to \( \mathfrak{h} \). Suppose first that the number \( r \) of indices \( j \in [1, pq] \) such that \( T_j \in \mathfrak{h} \) is less than \( p \). Then the set of \( pq - r \) indices \( j \in [1, pq] \) for which \( T_j = Y \) is the union of at most \( r + 1 \) intervals in \( \mathbb{N} \), and since \( (r + 1)(q - 1) \leq p(q - 1) < pq - r \), at least one of these intervals must contain at least \( q \) numbers, so that the product \( T_1 T_2 \cdots T_{pq} \) certainly vanishes in this case. Next, for each value of \( r \) and each \( k \geq r \), we have

\[ T_1 T_2 \cdots T_k \in h'_r + Yh'_r + \cdots + Y^{k-r}h'_r \]

if the number of indices \( j \) such that \( T_j \in \mathfrak{h} \) is equal to \( r \). For this is obviously true for arbitrary \( r \) and \( k = r \); and by induction on \( k - r \) (the number of factors \( T_j \) equal to \( Y \)) one sees immediately that (21.22.2.2) is true provided that \( T_k \in \mathfrak{h} \). Now for each \( r \) we have

\[ h'_r Y \subseteq Yh'_r + h'_r \]

Indeed, this is true when \( r = 1 \), because \( XY = YX + [X, Y] \) and \( [X, Y] \in \mathfrak{h} \) for all \( X \in \mathfrak{h} \); and from (21.22.2.3) we have

\[ h^{r+1} Y \subseteq hYh^r + h^{r+1} \subseteq (Yh + h)h^r + h^{r+1} \]

\[ = Yh^{r+1} + h^{r+1}, \]

which proves (21.22.2.3) by induction on \( r \). This being so, if we have \( T_k = Y \) in (21.22.2.2), then by hypothesis

\[ T_1 T_2 \cdots T_{k-1} \in h'_r + Yh'_r + \cdots + Y^{k-r-1}h'_r \]

from which it follows that

\[ T_1 T_2 \cdots T_k \in h'_r Y + Yh'_r Y + \cdots + Y^{k-r-1}h'_r Y, \]

which, together with (21.22.2.3), implies (21.22.2.2). If now \( r \geq p \), the right-hand side of (21.22.2.2) reduces to zero, and the proof is complete.
(21.22.3) (Cartan's criterion) Let $g$ be a finite-dimensional Lie algebra such that the Killing form $B_g$ is identically zero on $g \times g$; then $g$ is solvable.

By considering the complexification of $g$, if $g$ is a real Lie algebra, we may assume that $g$ is a complex Lie algebra (21.6.1). The proof is by induction on $\dim(g)$, the result being trivial when $\dim(g) = 1$. It will be enough to show that $\mathfrak{D}(g) \neq g$; for the Killing form $B_{\mathfrak{D}(g)}$, being the restriction of $B_g$ to the ideal $\mathfrak{D}(g)$ (21.5.7), is identically zero and therefore by the inductive hypothesis $\mathfrak{D}(g)$ will be solvable, and hence $g$ also will be solvable (19.12.3).

Suppose then that $\mathfrak{D}(g) = g$. We define an element $u_0 \in g$ as in (21.19.2) and consider the corresponding direct sum decomposition $g = \mathfrak{h} \oplus \oplus g(\alpha)$. It follows that $\mathfrak{D}(g) = [g, g]$ is the sum (not in general direct) of the subspaces $[h, h], [h, g(\alpha)],$ and $[g(\alpha), g(\beta)]$ for $\alpha, \beta$ in $\mathfrak{S}$. But

$$[g(\alpha), g(\beta)] \subseteq g(\alpha + \beta)$$

and $[h, g(\alpha)] \subseteq g(\alpha)$ (21.19.6.1), hence our assumption on $g$ implies that

$$(21.22.3.1) \quad \mathfrak{h} = [h, h] + \sum_{\alpha \in \mathfrak{S}} [g(\alpha), g(-\alpha)].$$

We shall deduce from this that $\mathfrak{S}$ must be empty. For every linear form $\beta \in \mathfrak{S}$, the restriction of $\beta$ to $[h, h]$ is zero (21.19.7); also, for each $\alpha \in \mathfrak{S}$ and each $u \in [g(\alpha), g(-\alpha)]$ we have $\beta(u) = r_{\beta \alpha} \alpha(u)$, where $r_{\beta \alpha}$ is a rational number (21.19.10). But since by hypothesis $B_g(u, u) = 0$, the relation (21.19.8.1) implies that

$$\dim(g(\alpha)) \cdot \alpha(u)^2 + \sum_{\beta \not\alpha} r_{\beta \alpha}^2 \dim(g(\beta)) \alpha(u)^2 = 0$$

and hence that $\alpha(u) = 0$. But then $\beta(u) = r_{\beta \alpha} \alpha(u) = 0$ for all $\beta \in \mathfrak{S}$. If we had $\mathfrak{S} \neq \emptyset$, every linear form $\beta \in \mathfrak{S}$ would be zero on all of $\mathfrak{h}$, by what has just been proved and (21.22.3.1); and this contradicts the definition of $\mathfrak{S}$.

Hence we have $\mathfrak{S} = \emptyset$ and consequently $g = \mathfrak{h}$; but then $\text{ad}(u)$ would be nilpotent for all $u \in g$ (21.19.5); by virtue of Engel's theorem (21.22.2), $g$ would be nilpotent and a fortiori solvable (21.22.1), contrary to our assumption.

Q.E.D.

(21.22.4) If a finite-dimensional Lie algebra $g$ contains no solvable ideal $\neq \{0\}$, then $g$ is semisimple.

Suppose the contrary, so that the Killing form $B_g$ is degenerate: in other words, if $\mathfrak{n}$ is the subspace of all $x \in g$ such that $B_g(x, y) = 0$ for all $y \in g$, then $\mathfrak{n} \neq \{0\}$. But $\mathfrak{n}$ is an ideal of $g$, because by virtue of (21.5.6.1), if $x \in \mathfrak{n}$
and \( z \in \mathfrak{g} \) we have \( B_{\mathfrak{g}}([x, z], y) = B_{\mathfrak{g}}(x, [z, y]) = 0 \) for all \( y \in \mathfrak{g} \). This being so, the restriction of \( B_{\mathfrak{g}} \) to \( \mathfrak{h} \times \mathfrak{h} \) is identically zero; since this restriction is equal to \( B_{\mathfrak{h}} \) (21.5.7), it follows that \( \mathfrak{h} \) is solvable by Cartan's criterion (21.22.3), contrary to hypothesis.

**PROBLEMS**

1. Let \( E \) be a real or complex vector space of finite dimension and \( G \) a connected Lie group immersed in \( \text{GL}(E) \). Let \( N \) be a normal subgroup of \( G \); suppose that the linear representation of \( G \) on \( E \) defined by the canonical injection \( G \rightarrow \text{GL}(E) \) is irreducible, and that there exists a vector \( x_0 \neq 0 \) in \( E \) such that \( t \cdot x_0 = \lambda(t)x_0 \) for all \( t \in N \). Then \( N \) is contained in the center of \( \text{CL}(E) \), consisting of the nonzero scalar multiples of the identity. (Observe that the mapping \( t \mapsto \lambda(t) \) is continuous on \( N \) and that \( \lambda(sts^{-1}) = \lambda(t) \) for all \( s \in G \), and deduce that the set of \( x \in E \) such that \( t \cdot x = \lambda(t)x \) for all \( t \in N \) is stable under \( G \).)

2. Let \( E \) be a finite-dimensional complex vector space. Show that if \( G \) is a solvable connected Lie group immersed in \( \text{GL}(E) \), then there exists a basis of \( E \) such that \( G \), identified by this choice of basis with a group of matrices, is contained in the group of lower triangular matrices (Lie’s theorem). (It is enough to prove that there exists \( x_0 \neq 0 \) in \( E \) such that \( s \cdot x_0 = \lambda(s)x_0 \) for all \( s \in G \). Do this first for \( G \) commutative, and then use Problem 1 and the definition of solvable groups.)

3. (a) Show that if \( \mathfrak{g} \) is a finite-dimensional solvable (real or complex) Lie algebra, then its derived algebra \( \mathfrak{d}(\mathfrak{g}) \) is nilpotent. (Use Engel’s theorem and Lie’s theorem.)

(b) In order that \( \mathfrak{g} \) should be solvable, it is necessary and sufficient that the restriction to \( \mathfrak{d}(\mathfrak{g}) \) of the Killing form of \( \mathfrak{g} \) should be identically zero (use (a) and Cartan’s criterion). Give an example of a solvable Lie algebra whose Killing form is not identically zero.

(c) If \( \mathfrak{g} \) is nilpotent, then the Killing form of \( \mathfrak{g} \) is identically zero. Give an example of a solvable but not nilpotent Lie algebra whose Killing form is identically zero. (Consider the solvable Lie group defined in Section 19.14, Problem 4, and note that for the Killing form of its Lie algebra to vanish identically, it is necessary and sufficient that \( \text{Tr}(U^2) = 0 \).)
(e) Let $a$ be a subalgebra of $g$ and let $x_0$ be an element of $a$ such that the endomorphism of the vector space $g/a$ induced by $ad(x_0)$ is bijective. Show that the mapping $(x, u) \mapsto \exp(ad(u)) \cdot x$ of $a \times g$ into $g$ is a submersion at the point $(x_0, 0)$, and deduce with the help of (c) that $a$ contains a regular element of $g$.

(f) A nilpotent subalgebra of $g$ that is equal to its own normalizer is called a Cartan subalgebra. For each regular element $u_0 \in g$, the subalgebra $g_{u_0}$ defined in (d) is a Cartan subalgebra; and conversely, every Cartan subalgebra of $g$ may be obtained in this way. (If $n$ is a Cartan subalgebra, show by using (e) that it contains a regular element $u_n$; then we have $n \subset g_{u_n}$, and if the inclusion were strict, $n$ would not be equal to its normalizer (Section 19.14, Problem 7).) The subalgebra $g_{u_0}$ defined in (21.19.2) is a Cartan subalgebra.

(g) Suppose that $g$ is a complex Lie algebra. Let $\Gamma$ be the connected Lie group immersed in $\text{Aut}(g)$ whose Lie algebra is $ad(g)$. Show that any Cartan subalgebra of $g$ can be transformed into any other by an automorphism $\sigma \in \Gamma$. (For each Cartan subalgebra $h$ of $g$, let $b_{\text{reg}}$ denote the (open) subset of regular elements belonging to $h$, and let $R_h$ be the image of $\Gamma \times b_{\text{reg}}$ under the mapping $(\sigma, x) \mapsto \sigma \cdot x$ of $\Gamma \times b_{\text{reg}}$ into $g$. Use (e) to show that $R_h$ is open in $g$, and then use (c).) Compare with Section 21.21, Problem 6.

5. (a) Let $g$ be a (real or complex) Lie algebra of finite dimension. If $h$ is a Cartan subalgebra of $g$, then $h$ is also a Cartan subalgebra of every Lie subalgebra $g_1$ of $g$ that contains $h$.

(b) If $f$ is a surjective homomorphism of $g$ onto a Lie algebra $g_1$, then the image under $f$ of any regular element of $g$ is a regular element of $g_1$ (use the fact that the set of regular elements of $g_1$ is dense). Deduce that the image under $f$ of any Cartan subalgebra of $g$ is a Cartan subalgebra of $g_1$. If $g$ and $g_1$ are complex Lie algebras, then every Cartan subalgebra of $g_1$ is the image under $f$ of a Cartan subalgebra of $g$. (Use Problem 4(g).)

(c) If $h$ is a Cartan subalgebra of $g$ and if $a$ is a Lie subalgebra of $g$ which contains $h$, then $a$ is its own normalizer in $g$. (Apply (b) to the quotient algebra $g/a$.)

6. Let $G$ be a connected Lie group (real or complex). A Cartan subgroup of $G$ is any connected Lie group immersed in $G$ whose Lie algebra is a Cartan subalgebra of the Lie algebra $g$ of $G$.

(a) Show that a Cartan subgroup is closed in $G$.

(b) Suppose that $G$ is a complex semisimple group, and is the complexification of a compact connected semisimple group $K$. Then all the Cartan subgroups of $G$ are conjugate in $G$. We obtain a Cartan subalgebra of $g$ by taking the complexification $t + it$ of a maximal commutative subalgebra $t$ of the Lie algebra $t$ of $K$; the corresponding Cartan subgroup is isomorphic to $(C^*)^l$, where $l$ is the rank of $G$.

(c) With the hypotheses of (b), show that every Cartan subgroup $A$ of $G$ is its own centralizer in $G$, and that the normalizer $N(A)$ of $A$ in $G$ is such that $N(A)/A$ may be identified with the Weyl group of $K$. (Consider the centralizer and the normalizer of $t + it$ in $G$, and argue as in Section 21.11, Problem 12(a).)

(d) With the same hypotheses, all elements of a Cartan subalgebra of $g$ are semisimple (Section 21.19, Problem 1).

7. Let $G$ be a complex connected Lie group and $g$ its Lie algebra. A Borel subalgebra of $g$ is any maximal solvable subalgebra of $g$, and a Borel subgroup of $G$ is a (complex) connected Lie group immersed in $G$ whose Lie algebra is a Borel subalgebra of $g$.

(a) Show that a Borel subgroup is closed in $G$. 


9. Let $G$ be a complex connected semisimple group, and keep to the notation of (21.21.12(iii)). Show that $\mathfrak{b} = \mathfrak{t} + \mathfrak{i} + \mathfrak{n}$ is a Borel subalgebra of $\mathfrak{g}$, and that $\mathfrak{b}$ is the semidirect product of the Cartan subalgebra $\mathfrak{h} = \mathfrak{t} + \mathfrak{i}$ and the nilpotent algebra $\mathfrak{n}$, which is also the derived algebra $\Delta(\mathfrak{b})$. (Observe that a Lie subalgebra of $\mathfrak{g}$, that contains $\mathfrak{t}$ strictly cannot be solvable.)

(c) For each element $\mathfrak{u} \in \mathfrak{b}$, the semisimple and nilpotent components of $\mathfrak{u}$ (Section 21.19, Problem 1) both belong to $\mathfrak{b}$ (cf. Problem 5(c)). Show that the nilpotent elements of $\mathfrak{b}$ are the elements of $\mathfrak{n}$.

(d) Let $\mathfrak{b}$ be the Borel subgroup with Lie algebra $\mathfrak{b}$. If $T$ is the maximal torus of $G_{\mathfrak{b}}$ with Lie algebra $\mathfrak{t}$, then $\mathfrak{G}_{\mathfrak{b}} \cap \mathfrak{B} = T$ (cf. (21.21.12)). The homogeneous space $G/B$ is a compact complex manifold, and the canonical mapping of $G/B$ onto $G/T$ is a diffeomorphism (Section 16.10, Problem 3). Show that the center of $\mathfrak{b}$ is equal to the center of $G$ (and of $G_{\mathfrak{b}}$).

(e) Show that $\mathfrak{b}$ is its own normalizer in $G$. (Let $H$ be the Cartan subgroup of $G$ with Lie algebra $\mathfrak{h}$. If $\mathfrak{s} \in \mathfrak{a} \subseteq \mathfrak{b}$, show that there exists $x \in \mathfrak{b}$ such that Int$(\mathfrak{s}x)$ leaves $H$ globally invariant, and hence also the corresponding root system $\mathfrak{R}$; furthermore, the fact that Int$(\mathfrak{s}x)$ leaves $\mathfrak{b}$ globally invariant implies that $\text{Ad}(\mathfrak{s}x)$ permutes the $\mathfrak{a}_i$ for $x \in \mathfrak{x}$. Deduce that $\text{Ad}(\mathfrak{s}x)$ leaves each $\mathfrak{g}_i$ globally invariant, and by arguing as in Section 21.11, Problem 12(a), show that there exists $y \in \mathfrak{h}$ such that Int$(\mathfrak{s}y)$ is the identity. Complete the proof by observing that the center of $\mathfrak{g}$ is contained in every Cartan subgroup.)

8. Let $G$ be a complex connected semisimple group and $\mathfrak{g}$ its Lie algebra. A Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is said to be splittable if for each $\mathfrak{u} \in \mathfrak{h}$ the semisimple and nilpotent components of $\mathfrak{u}$ belong to $\mathfrak{h}$. A subalgebra $\mathfrak{a}$ of $\mathfrak{g}$ is said to be diagonalizable if there exists a basis of $\mathfrak{g}$ relative to which all the endomorphisms $\text{ad}(\mathfrak{u})$, for $\mathfrak{u} \in \mathfrak{a}$, are represented by diagonal matrices (which implies that all the elements of $\mathfrak{a}$ are semisimple).

(a) Let $\mathfrak{h}$ be a splittable subalgebra of $\mathfrak{g}$, and let $\mathfrak{a}$ be a diagonalizable subalgebra of $\mathfrak{h}$. Then there exists a direct sum decomposition of the vector space $\mathfrak{h}$: $\mathfrak{h} = \mathfrak{h}_0 \oplus \bigoplus_{\lambda \in F} \mathfrak{h}_\lambda$, where $\mathfrak{h}_0$ is the centralizer of $\mathfrak{a}$ in $\mathfrak{h}$, $F$ is a set of nonzero linear forms on $\mathfrak{a}$, and for each $\lambda \in F$ we have $[\mathfrak{u}, \mathfrak{x}] = \lambda(\mathfrak{u})\mathfrak{x}$ for $\mathfrak{u} \in \mathfrak{a}$ and $\mathfrak{x} \in \mathfrak{h}$.

(b) With the same hypotheses, suppose in addition that $\mathfrak{a}$ is a maximal diagonalizable subalgebra of $\mathfrak{h}$. Show that $\mathfrak{h}_0$ is a Cartan subalgebra of $\mathfrak{h}$ and is splittable. (Observe that if two elements of $\mathfrak{g}$ commute, then so do their semisimple and nilpotent components.) Show also that $\mathfrak{a}$ is the set of semisimple elements of $\mathfrak{h}_0$, that the set $\mathfrak{n}$ of nilpotent elements of $\mathfrak{h}_0$ is an ideal in $\mathfrak{h}_0$, and that $\mathfrak{h}_0$ is the direct sum of $\mathfrak{a}$ and $\mathfrak{n}$. Consider in particular the cases where $\mathfrak{h}$ is nilpotent, and where $\mathfrak{h} = \mathfrak{g}$.

(c) Suppose now that $\mathfrak{h}$ is a solvable and splittable subalgebra of $\mathfrak{g}$. Show that the set $\mathfrak{n}$ of nilpotent elements of $\mathfrak{h}$ is an ideal in $\mathfrak{h}$. (Use Lie's theorem (Problem 2).) Show also that if $\mathfrak{a}$ is a maximal diagonalizable subalgebra of $\mathfrak{h}$, then $\mathfrak{h}$ is the semidirect product of $\mathfrak{n}$ and $\mathfrak{a}$ (19.14.7).

9. Let $\rho$ be a continuous linear representation of a Lie group $G$ on a finite-dimensional complex vector space $E$. By passing to the quotient, $\rho$ induces a differentiable action of $G$ on the associated projective space $P(E)$, which is compact. Hence there exist in $P(E)$ nonempty closed $G$-stable subsets that are minimal among the subsets of $P(E)$ having these properties (Section 12.10, Problem 6).

Show that if $G$ is connected and solvable, every minimal nonempty closed $G$-stable subset of $P(E)$ consists of a single point. (Argue by induction on $n = \dim(E)$. For $n = 2$, use Lie's theorem (Problem 2). For $n > 2$, Lie's theorem proves the existence of a point
10. With the notation of Problem 7, the group $G$ being assumed to be semisimple, let $r = \dim(b)$. The Grassmannian $G_r(\mathfrak{g})$ of $r$-dimensional complex vector subspaces of $\mathfrak{g}$ (16.11.9) may be identified with a closed submanifold of the projective space $P(\wedge^r \mathfrak{g})$. Show that the subset $\mathcal{B}$ of $G_r(\mathfrak{g})$ consisting of the transforms $\text{Ad}(s) \cdot b$ of $b$ by the elements of $G$ is closed in $G_r(\mathfrak{g})$. (Observe that $G$ acts differentiably on $G_r(\mathfrak{g})$ by the action $(s, m) \mapsto \text{Ad}(s) \cdot m$, and use Problem 7(d) and (16.10.12)).

Let $\mathfrak{s}$ be a solvable subalgebra of $\mathfrak{g}$. By applying the result of Problem 9 to $E = \wedge \mathfrak{g}$, show that there exists $t \in G$ such that $\text{Ad}(t) \cdot \mathfrak{s} \subset b$. In particular, any two Borel subalgebras of $\mathfrak{q}$ can be obtained one from the other by an automorphism of the form $\text{Ad}(t)$, where $t \in G$. Any two Borel subgroups of $G$ are conjugate (Borel's theorem).

11. With the notation of Problem 7, show that as $w$ runs through the Weyl group $W$ of $\mathfrak{g}_a$ with respect to $t$, the mapping $w \mapsto w(b)$ is a bijection of $W$ onto the set of Borel subalgebras of $\mathfrak{g}_a$ that contain $\mathfrak{h} = t + i t$. (Use Problem 10 and the fact that two Cartan subalgebras both contained in a Lie subalgebra $\mathfrak{a}$ of $\mathfrak{g}$ can be transformed one into the other by an automorphism of the form $\text{Ad}(t)$, where $t$ belongs to the connected Lie group immersed in $G$ with Lie algebra $\mathfrak{a}$; finally use Problem 6(c)).

12. In a complex semisimple Lie algebra $\mathfrak{g}$, a Lie subalgebra distinct from $\mathfrak{g}_a$ that contains a Borel subalgebra is called parabolic. If $G$ is a complex connected semisimple group, a connected Lie group immersed in $G$ is a parabolic subgroup of $G$ if its Lie algebra is parabolic.

(a) Show that a parabolic subgroup is closed in $G$ (cf. Problem 5(c)).

(b) With the notation of Problem 7, let $\mathfrak{p}$ be a parabolic subalgebra containing $b$. Then the vector space $\mathfrak{p}$ is the direct sum of $\mathfrak{h}$ and a certain number of the $\mathfrak{g}_\alpha$, for $\alpha \in \mathcal{P}$ say, where $\mathcal{S}_\alpha \subset \mathfrak{P} \subset \mathcal{S}$. For any two roots $\alpha, \beta \in \mathcal{P}$, if $\alpha + \beta$ is a root then $\alpha + \beta \in \mathcal{P}$. If $\mathfrak{B}$ is the basis of $\mathfrak{S}$ that determines the given ordering on $\mathfrak{S}$, show that $\mathfrak{P}$ is the union of $\mathfrak{S}_\alpha$ and $\mathfrak{Q}$, where $\mathfrak{Q}$ is the set of roots that are linear combinations with integral coefficients $\leq 0$ of the roots belonging to $\mathfrak{B} \cap (- \mathfrak{P})$. (To show that $\mathfrak{Q} \subset \mathfrak{P} \cap (- \mathfrak{S}_\alpha)$, show that if $-\alpha \in \mathfrak{Q}$, then $-\alpha \in \mathfrak{P}$, by noting that $\alpha$ is the sum of say $n$ elements of $\mathfrak{B}$, and arguing by induction on $n$, with the help of Section 21.11, Problem 3(c). To show that $\mathfrak{P} \cap (- \mathfrak{S}_\alpha) \subset \mathfrak{Q}$, show that if $-\alpha \in \mathfrak{P} \cap (- \mathfrak{S}_\alpha)$, then $-\alpha \in \mathfrak{Q}$, by noting that $\alpha$ is the sum of say $m$ elements of $\mathfrak{B}$, and again arguing by induction.)

(c) Conversely, for each subset $\mathfrak{B}_\alpha$ of $\mathfrak{B}$, if $\mathfrak{Q}$ is the set of roots $\alpha \in \mathfrak{S}$ that are linear combinations with integral coefficients $\leq 0$ of the roots in $\mathfrak{B}_\alpha$, and if $\mathfrak{P} = \mathfrak{S}_\alpha \cup \mathfrak{Q}$, then the direct sum of $\mathfrak{h}$ and the $\mathfrak{g}_\alpha$ for $\alpha \in \mathfrak{P}$ is a parabolic subalgebra of $\mathfrak{g}$.

13. (a) Let $G$ be a complex connected semisimple group, and $B_1, B_2$ two Borel subgroups of $G$. Show that $B_1 \cap B_2$ contains a Cartan subgroup. (Let $b_1, b_2$ be the Lie algebras of $B_1$, $B_2$, and apply Problem 8(c) to $b_1 \cap b_2$, so that we obtain $b_1 \cap b_2 = a \oplus \mathfrak{n}$, where $a$ is a maximal diagonalizable subalgebra of $b_1 \cap b_2$, and $\mathfrak{n}$ is the set of nilpotent elements of $b_1 \cap b_2$. Show that $\dim(b_1 + b_2) \leq \dim(g) - \dim(n)$ by noting that $\mathfrak{n}$ is orthogonal to $b_1$ and $b_2$, relative to the Killing form of $g$; by observing that $\dim(b_1) + \dim(b_2) = \dim(g) + \dim(h)$, where $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$, conclude that $\dim(a) \geq \dim(h)$ and hence, by virtue of Problem 8(b), that $a$ is a Cartan subalgebra of $\mathfrak{g}$.)
(b) With the notation of Problem 7, for each element \( w \) of the Weyl group \( W \) of \( g_u \) relative to \( t \), let \( BwB \) denote the double coset of any element of the normalizer \( ^s V(T) \) of \( T \) in \( G_u \) belonging to the class of \( w \) in \( ^s V(T)/T \). Show that, as \( w \) runs through \( W \), the double cosets \( BwB \) form a partition of \( G \) (Bruhat decomposition). (If \( s \in G \), deduce from (a) and Problem 4(g) that there exists \( x \in B \) such that \( xsBs^{-1}x^{-1} \supset H \), and then use Problem 11; finally, observe that \( ^s V(T) \cap B = T \).)

**23. E. E. LEVI'S THEOREM**

(21.23.1) Let \( g \) be a (real or complex) Lie algebra of finite dimension and let \( a, b \) be two solvable ideals in \( g \). Since \( (a + b)/a \) is isomorphic to \( b/(a \cap b) \), it follows that \( (a + b)/a \) is a solvable Lie algebra; since the canonical image of \( D_k(a + b) \) in \( (a + b)/a \) is contained in \( D_k((a + b)/a) \), we have \( D_k(a + b) \subset a \) for sufficiently large \( k \), and therefore \( D_h(a + b) = \{0\} \) for sufficiently large \( h \), because \( a \) is solvable; hence the algebra \( a + b \) is solvable. It follows that if \( r \) is a solvable ideal of \( g \) of maximum dimension, then every solvable ideal of \( g \) is contained in \( r \); for if a solvable ideal \( a \) of \( g \) were not contained in \( r \), we should have \( \dim(a + r) > \dim r \), and \( a + r \) is a solvable ideal, contrary to the definition of \( r \). This unique ideal \( r \) of \( g \), the union of all the solvable ideals in \( g \), is called the radical of the Lie algebra \( g \).

(21.23.2) If \( g \) is a finite-dimensional Lie algebra, the quotient \( g/r \) of \( g \) by its radical \( r \) is a semisimple Lie algebra.

By virtue of (21.22.4), it is enough to show that the only solvable ideal \( a \) of \( g/r \) is \( \{0\} \). Now such an ideal is of the form \( b/r \), where \( b \) is an ideal in \( g \); since \( r \) and \( b/r \) are solvable, one shows as in (21.23.1) that \( b \) is solvable. But then by definition \( b \subset r \), so that \( a = \{0\} \).

(21.23.3) (E. E. Levi's theorem) Let \( g \) be a finite-dimensional complex Lie algebra and \( r \) its radical. Then there exists a semisimple subalgebra \( s \) of \( g \) such that \( g \) is isomorphic to a semidirect product \( r \rtimes s \) (19.14.7).

From the definition of the semidirect product of Lie algebras (19.14.7), it is enough to show that there exists a semisimple Lie subalgebra \( s \) of \( g \) such that \( s \cap r = \{0\} \) and \( s + r = g \). It comes to the same thing to say that, if \( p: g \to g/r \) is the canonical homomorphism, the restriction of \( p \) to \( s \) is an isomorphism of \( s \) on \( g/r \); or, again, that there exists a homomorphism \( q \) of \( g/r \) into \( g \) such that \( p \circ q = 1_{g/r} \). The proposition is therefore a particular case of the following:
Let $\mathfrak{g}$ be a complex semisimple Lie algebra, $\mathfrak{e}$ a finite-dimensional complex Lie algebra. $p: \mathfrak{e} \to \mathfrak{g}$ a surjective homomorphism. Then there exists a homomorphism $q: \mathfrak{g} \to \mathfrak{e}$ such that $p \circ q = 1_{\mathfrak{g}}$.

Let $\mathfrak{n} = \text{Ker}(p)$, which is an ideal of $\mathfrak{e}$, and argue by induction on the dimension of $\mathfrak{n}$. If $\mathfrak{n} = \{0\}$, there is nothing to prove. If $\mathfrak{e}$ is semisimple, then $\mathfrak{e}$ is the direct sum of $\mathfrak{n}$ and an ideal $\mathfrak{n}'$ (21.6.4), and the restriction of $p$ to $\mathfrak{n}'$ is an isomorphism of this Lie algebra onto $\mathfrak{g}$; we may therefore take $q$ to be the inverse of this isomorphism. Suppose therefore that $\mathfrak{e}$ is not semisimple, and let $\mathfrak{r}$ be the radical of $\mathfrak{e}$. For each ideal $\mathfrak{a}$ of $\mathfrak{r}$, it is easily seen that $\mathfrak{D}(\mathfrak{a})$ is also an ideal of $\mathfrak{e}$, by virtue of the Jacobi identity; hence $\mathfrak{D}^k(\mathfrak{r})$ is an ideal of $\mathfrak{e}$ for all $k$, and if $m$ is the smallest integer such that $\mathfrak{D}^m(\mathfrak{r}) = \{0\}$, then $\mathfrak{D}^{m-1}(\mathfrak{r})$ is a commutative nonzero ideal of $\mathfrak{e}$. We may therefore assume that such ideals exist in $\mathfrak{e}$; choose one, say $\mathfrak{a}$, of smallest possible dimension. Then $(\mathfrak{a} + \mathfrak{n})/\mathfrak{n}$ is a commutative ideal of $\mathfrak{e}/\mathfrak{n}$, isomorphic to $\mathfrak{g}$; but since $\mathfrak{g}$ is semisimple, this implies that $\mathfrak{a} + \mathfrak{n} \subset \mathfrak{n}$ (21.6.2), so that $\mathfrak{a} \subset \mathfrak{n}$.

Suppose first that $\mathfrak{a} \neq \mathfrak{n}$. On passing to the quotient, $p$ gives rise to a surjective Lie algebra homomorphism $p_1: \mathfrak{e}/\mathfrak{n} \to \mathfrak{g}$, with kernel $\mathfrak{n}/\mathfrak{a}$, and the inductive hypothesis guarantees the existence of a homomorphism $q_1: \mathfrak{g} \to \mathfrak{e}/\mathfrak{n}$ such that $p_1 \circ q_1 = 1_{\mathfrak{g}}$. We may write $q_1(\mathfrak{g}) = \mathfrak{f}/\mathfrak{a}$, where $\mathfrak{f}$ is a Lie subalgebra of $\mathfrak{e}$ containing $\mathfrak{a}$. Since $\dim(\mathfrak{a}) < \dim(\mathfrak{n})$, we may apply the inductive hypothesis to the canonical homomorphism $p_2: \mathfrak{f} \to \mathfrak{f}/\mathfrak{a}$ with kernel $\mathfrak{a}$, and deduce that there exists a homomorphism $q_2: \mathfrak{f}/\mathfrak{a} \to \mathfrak{f}$ such that $p_2 \circ q_2 = 1_{\mathfrak{f}/\mathfrak{a}}$. It is now clear that the homomorphism $q = q_2 \circ q_1$ has the required property.

We have still to consider the case where $\mathfrak{a} = \mathfrak{n}$. We shall define canonically a Lie algebra homomorphism $\rho: \mathfrak{g} \to \mathfrak{gl}($a) as follows: each $x \in \mathfrak{g}$ is of the form $p(z)$ for some $z \in \mathfrak{e}$; the restriction to $\mathfrak{a}$ of the endomorphism $\text{ad}(z)$ of $\mathfrak{e}$ is an endomorphism of the vector space $\mathfrak{a}$, because $\mathfrak{a}$ is an ideal in $\mathfrak{e}$; but since $\mathfrak{a}$ is commutative and equal to $\mathfrak{n}$, if $p(z) = p(z')$ then $z' - z \in \mathfrak{a}$, and consequently the restrictions of $\text{ad}(z)$ and $\text{ad}(z')$ to $\mathfrak{a}$ are equal. The restriction of $\text{ad}(z)$ to $\mathfrak{a}$ therefore depends only on $x$; if we denote it by $\rho(x)$, then it is clear that $\rho$ is a homomorphism of $\mathfrak{g}$ into $\mathfrak{gl}(\mathfrak{a})$, because $[p(z_1), p(z_2)] = p([z_1, z_2])$.

The vector space $\mathfrak{a}$ may therefore be regarded as a $U(\mathfrak{g})$-module by means of $U(\rho)$, and it follows from (21.9.1) that $\mathfrak{a}$ is a direct sum of simple $U(\mathfrak{g})$-submodules. But by definition a $U(\mathfrak{g})$-submodule of $\mathfrak{a}$ is an ideal of $\mathfrak{e}$; by virtue of the choice of $\mathfrak{a}$, we see that $\mathfrak{a}$ is necessarily a simple $U(\mathfrak{g})$-module.

It may happen that $\rho(x) = 0$ for all $x \in \mathfrak{g}$; this is the case when $\mathfrak{a} = \mathfrak{n}$ is contained in the center of $\mathfrak{e}$, and in fact is equal to this center, because $\mathfrak{g} = \mathfrak{e}/\mathfrak{a}$ contains no nonzero commutative ideals (21.6.2) (by reason of the choice of $\mathfrak{a}$, it then follows that $\dim(\mathfrak{a}) = 1$). In this case, if $x = p(z)$, the
endomorphism \( \text{ad}(z) \) itself (and not merely its restriction to \( a \)) depends only on \( x \), and if we denote it by \( \rho'(x) \), we see as above that \( \rho' \) is a homomorphism of \( g \) into \( \mathfrak{gl}(e) = \text{End}(e) \). We may therefore in this case consider the space \( e \) itself as a \( U(g) \)-module, and \( a \) as a \( U(g) \)-submodule of \( e \). But then ((21.9.1) and (A.23.3)) there exists in \( e \) a \( U(g) \)-submodule supplementary to \( a \); by definition, \( b \) is an ideal of \( e \), and the restriction of \( \rho \) to \( b \) is an isomorphism of \( b \) onto \( g \); we then take \( q \) to be the inverse of this isomorphism.

It remains to consider the case where \( a = \mathfrak{n} \) is a simple \( U(g) \)-module and \( \rho(x) \) is not zero for all \( x \in g \). We shall show that there exists a finite-dimensional complex vector space \( M \), a Lie algebra homomorphism \( \sigma : e \to \mathfrak{gl}(M) = \text{End}(M) \), and an element \( w \in M \) having the following properties:

\begin{enumerate}
\item[(21.23.3.2)] The mapping \( t \mapsto \sigma(t) \cdot w \) of \( a \) into \( M \) is bijective.
\item[(21.23.3.3)] For each \( z \in e \), there exists \( t \in a \) such that \( \sigma(z) \cdot w = \sigma(t) \cdot w \).
\end{enumerate}

We then define \( s \) to be the set of all \( z \in e \) such that \( \sigma(z) \cdot w = 0 \). For since \( \sigma([z_1, z_2]) = \sigma(z_1)\sigma(z_2) - \sigma(z_2)\sigma(z_1) \), it is clear that \( s \) is a Lie subalgebra of \( e \); it follows from (21.23.3.2) that \( s \cap a = \{0\} \), and from (21.23.3.3) that \( e = s + a \), so that \( s \) has the required properties.

We shall take \( M \) to be the vector space \( \text{End}(e) \) and \( \sigma \) to be the Lie algebra homomorphism such that, for each \( f \in \text{End}(e) \) and each \( z \in e \),

\begin{equation}
(21.23.3.4) \quad \sigma(z) \cdot f = [\text{ad}(z), f] = \text{ad}(z) \cdot f - f \cdot \text{ad}(z),
\end{equation}

or, in other terms

\begin{equation}
(21.23.3.5) \quad (\sigma(z) \cdot f)(y) = [z, f(y)] - f([z, y])
\end{equation}

for all \( y \in e \).

We shall first show that the condition (21.23.3.2) is satisfied when we take \( w \) to be a projection of the vector space \( e \) onto the subspace \( a \) (so that \( w(y) \in a \) for all \( y \in e \), and \( w(t) = t \) for all \( t \in a \)). Indeed, it follows from (21.23.3.5) that for \( t \in a \) we have

\begin{equation}
(21.23.3.6) \quad (\sigma(t) \cdot w)(y) = -w([t, y]) = -[t, y]
\end{equation}

because \( w(y) \in a \), \( [a, a] = 0 \), and \( [e, a] \subset a \). Hence \( \sigma(t) \cdot w = 0 \) means that \( [t, y] = 0 \) for all \( y \in e \), or equivalently \( \rho(x) \cdot t = 0 \) for all \( x \in g \). But since \( a \) is a simple \( U(g) \)-module and the set of \( t \in a \) such that \( \rho(x) \cdot t = 0 \) for all \( x \in g \) is a \( U(g) \)-submodule of \( a \), this submodule can only be \( a \) or \( \{0\} \), and the first alternative has been ruled out.
The relation (21.23.3.6) likewise shows that for (21.23.3.3) to be satisfied, it is necessary and sufficient that for each $z \in e$ there should exist $t \in a$ such that $\sigma(z) \cdot w = -\text{ad}(t)$ in $M = \text{End}(e)$.

The conditions imposed on $w$ may be reformulated as follows. Let $P$ denote the vector subspace of $M$ that is the image of $a$ under the mapping $t \mapsto \text{ad}(t)$, and let $R$ denote the vector subspace of $M$ consisting of the $f \in \text{End}(e)$ such that (1) $f(e) \subseteq a$, and (2) the restriction of $f$ to $a$ is a scalar multiplication by $\lambda_f$. It is clear that $R$ is a vector space, that $P \subseteq R$, and that $f \mapsto \lambda_f$ is a $C$-linear form $\lambda$ on $R$; the set of projections of $e$ onto $a$ is the affine hyperplane $\lambda^{-1}(1)$ in $R$. Observe now that if $f \in R$ and $z \in e$, then also $\sigma(z) \cdot f \in R$; for the fact that $\sigma(z) \cdot f$ maps $e$ into $a$ follows from (21.23.3.5) and the fact that $a$ is an ideal of $e$, and it is immediately seen that $\lambda_{\sigma(z) \cdot f} = 0$.

It follows that $R$ is a $U(e)$-module and that $\lambda : f \mapsto \lambda_f$ is a $U(e)$-module homomorphism of $R$ into $C$, if $C$ is regarded as a trivial $U(e)$-module. On the other hand, the Jacobi identity shows that if $f = \text{ad}(t)$ with $t \in a$, then $\sigma(z) \cdot f = \lambda_{\sigma(z) \cdot t}$ in $R$; this shows that for each $x = p(t) \in g$ and each $f \in R$, the coset of $\sigma(z) \cdot f$ modulo $P$ depends only on $x$ and the coset $f$ modulo $P$. If we denote this coset by $a(x)$, it is immediately verified that $a : g \rightarrow \text{gl}(R/P)$ is a Lie algebra homomorphism. We have thus defined a $U(g)$-module structure on $R/P$, and the mapping $\lambda : R/P \rightarrow C$ induced by $\lambda$ on passing to the quotient is a surjective $U(g)$-module homomorphism, if $C$ is regarded as a trivial $U(g)$-module.

Next we remark that for $t \in a$ and $f \in R$, we have $\sigma(t) \cdot f = -\lambda_f \text{ad}(t)$, in other words $\sigma(t) \cdot R \subseteq P$. This shows that for each $x = p(z) \in g$ and each $f \in R$, the coset of $\sigma(z) \cdot f$ modulo $P$ depends only on $x$ and the coset $f$ modulo $P$. If we denote this coset by $\tilde{\sigma}(x) \cdot \tilde{f}$, it is immediately verified that $\tilde{\sigma} : g \rightarrow \text{gl}(R/P)$ is a Lie algebra homomorphism. We have thus defined a $U(g)$-module structure on $R/P$, and the mapping $\tilde{\lambda} : R/P \rightarrow C$ induced by $\lambda$ on passing to the quotient is a surjective $U(g)$-module homomorphism, if $C$ is regarded as a trivial $U(g)$-module.

This being so, the conditions imposed on $w$ are (1) $w \in R$, (2) $\lambda_w = 1$, (3) $\sigma(z) \cdot w \in P$ for all $z \in e$. If $\bar{w}$ is the image of $w$ in $R/P$, these conditions are equivalent to: (1) $\bar{w} \in R/P$, (2) $\tilde{\lambda}_{\bar{w}} = 1$, (3) $\tilde{\sigma}(x) \cdot \bar{w} = 0$ for all $x \in g$. This implies that the one-dimensional subspace $C\bar{w}$ in $R/P$ is a $U(g)$-module supplementary to the $U(g)$-submodule $\text{Ker}(\tilde{\lambda})$. Conversely, if $D$ is a one-dimensional subspace of $R/P$ supplementary to $\text{Ker}(\tilde{\lambda})$ and is a $U(g)$-module, then the intersection $\{\bar{w}\}$ of $D$ with the affine hyperplane given by the equation $\tilde{\lambda}_{\bar{f}} = 1$ satisfies the conditions above, because $D$ is then isomorphic to the $U(g)$-module $C$, which is trivial. Now the existence of such a $U(g)$-submodule supplementary to $\text{Ker}(\tilde{\lambda})$ is a consequence of the fact that every finite-dimensional $U(g)$-module is the direct sum of simple $U(g)$-submodules ((21.9.1) and (A.23.3)).

**Q.E.D.**

(21.23.4) *Every finite-dimensional real (resp. complex) Lie algebra is isomorphic to the Lie algebra of a real (resp. complex) Lie group.*

As we have already remarked (19.17.4), it is enough to prove the result for a complex Lie algebra. By virtue of (21.23.3), such an algebra is the
semidirect product of a solvable Lie algebra \( r \) and a semisimple Lie algebra \( s \). Since \( r \) (resp. \( s \)) is the Lie algebra of a complex solvable (resp. semisimple) Lie group, by virtue of (19.14.10) and (21.6.3), the result is a consequence of (19.14.9).

\((21.23.5)\) Let \( G \) be a simply connected Lie group. For each ideal \( n_e \) of the Lie algebra \( g_e \) of \( G \), the connected Lie group \( N \) immersed in \( G \) with Lie algebra \( n_e \) (19.7.4) is a closed (normal) subgroup of \( G \).

There exists a Lie group \( H \) whose Lie algebra \( h_e \) is isomorphic to \( g_e / n_e \) (21.23.4), and we have a homomorphism \( u: g_e \rightarrow h_e \) of Lie algebras, with kernel \( n_e \). Since \( G \) is simply connected, there exists a homomorphism of Lie groups \( f: G \rightarrow H \) such that \( f_* = u \) (19.7.6), and \( N \) is the identity component of the kernel of \( f \) (19.7.1), hence is closed in \( G \).

**PROBLEMS**

1. (a) Let \( E \) be a real or complex vector space of finite dimension; \( A, B \) two vector subspaces of \( \text{End}(E) \); \( T \) the set of \( t \in \text{End}(E) \) such that \( [t, A] \subseteq B \). Show that if \( s \in T \) is such that \( \text{Tr}(su) = 0 \) for all \( u \in T \), then \( s \) is a nilpotent endomorphism of \( E \). (Note that \( \text{Tr}(s^n) = 0 \) for all integers \( n \geq 2 \), and deduce that the eigenvalues of \( s \) are all zero, by using Newton's formulas.)

(b) Let \( g \) be a finite-dimensional Lie algebra, \( \rho: g \rightarrow \text{gl}(E) \) a Lie algebra homomorphism, and \( B_{\rho}(u, v) = \text{Tr}(\rho(u)\rho(v)) \) the symmetric bilinear form associated with \( \rho \) (21.5.5). In order that \( \rho(g) \) should be solvable, it is necessary and sufficient that \( \mathfrak{D}(g) \) should be orthogonal to \( g \), relative to the form \( B_{\rho} \). (To show that the condition is necessary, reduce to the case where \( g \) and \( \text{gl}(E) \) are complex Lie algebras, and use Lie's theorem. To show that the condition is sufficient, reduce to the case where \( g \subseteq \text{gl}(E) \) and use (a), with \( A = g \) and \( B = \mathfrak{D}(g) \).)

2. Let \( g \) be a finite-dimensional complex Lie algebra.
   (a) Show that if \( r \) is the radical of \( g \), we have \( \{g, r\} \subseteq \mathfrak{D}(g) \cap r \). (Use Levi's theorem.)
   (b) For each finite-dimensional complex vector space \( E \) and each Lie algebra homomorphism \( \rho: g \rightarrow \text{gl}(E) \), show that \( \rho(\{g, r\}) \) consists of nilpotent endomorphisms. (Observe that the elements of \( \rho(\{r, r\}) \) are nilpotent by virtue of Lie's theorem, and then argue as in (21.22.2).) In particular, \( \{g, r\} \) is a nilpotent ideal of \( g \).
   (c) Show that \( r \) is the orthogonal supplement of \( \mathfrak{D}(g) \) relative to the Killing form of \( g \). (To show that \( r \) is contained in the orthogonal supplement \( r' \) of \( \mathfrak{D}(g) \), use (a). Then observe that \( r' \) is an ideal containing \( r \), and that \( \text{ad}(r') \) is solvable by virtue of Problem 1(b).)
   (d) Show that for each automorphism \( \tau \) of \( g \) we have \( \tau(r) = r \).
   (e) For each ideal \( a \) of \( g \), show that \( a \cap r \) is the radical of \( a \). (Observe that, by (d) above, the radical of \( a \) is an ideal of \( g \).)

3. (a) Let \( E \) be a finite-dimensional complex vector space, and let \( F = \mathbb{C} \times E \). Let \( \sigma: g \rightarrow \text{gl}(E) \) be a homomorphism of a complex Lie algebra \( g \) into \( \text{gl}(E) = \text{End}(E) \). If
222 XXI COMPACT LIE GROUPS AND SEMISIMPLE LIE GROUPS

Let \( f : g \to E \) be a \( C \)-linear mapping, define a \( C \)-linear mapping \( \rho : g \to \text{End}(F) \) by the formula

\[
\rho(u) \cdot (\xi, x) = (0, \xi \cdot f(u) + \sigma(u) \cdot x)
\]

for all \( u \in g \). Show that for \( \rho \) to be a homomorphism of \( g \) into \( \text{gl}(F) \) it is necessary and sufficient that \( f \) should satisfy the condition

\[
\sigma(u_1) \cdot f(u_2) - \sigma(u_2) \cdot f(u_1) = f([u_1, u_2])
\]

for all \( u_1, u_2 \in g \).

(b) Suppose that \( g \) is semisimple. Show that if \( f \) satisfies the condition in (a), there exists an element \( x_0 \in E \) such that \( f(u) = -\sigma(u) \cdot x_0 \) for all \( u \in g \). (Observe that the subspace \( \{0\} \times E \) of \( F \) is stable under \( \rho \).)

4. Let \( g \) be a finite-dimensional complex Lie algebra, \( r \) its radical, and \( s, s' \) two semisimple Lie subalgebras of \( g \) such that \( g = s + r = s' + r \). We propose to prove that there exists an element \( a \in [g, r] \) such that, putting \( v = \exp(\text{ad}(a)) \) in \( \text{gl}(g) \), we have \( v(s') = s \) (Malcev's theorem). Distinguish three cases:

(1) \( [g, r] = \{0\} \); then \( r \) is the center of \( g \), and \( g \) is the direct product of the ideals \( r \) and \( \mathcal{D}(g) \), and \( \mathcal{D}(g) = s = s' \).

(2) \( r \) is commutative and \( r = [g, r] \). Then for each \( x \in s' \) there exists a unique element \( h(x) \in r \) such that \( x + h(x) \in s \). By using Problem 3(b), show that there exists an element \( a \in r \) such that \( h(x) = -[x, a] \) for all \( x \in s' \), and observe that \( (\text{ad}(a))^2 = 0 \).

(3) The general case. Observe that \( [g, r] \) is a nilpotent algebra, hence has center \( c \neq \{0\} \) (Section 19.12, Problem 3). Choose in \( r \) an ideal \( m \neq \{0\} \) of smallest dimension. We may limit our attention to the case where \( m = r \); consider the algebra \( g/m \) and proceed by induction on the dimension of \( r \) using case (2) above.

5. Let \( g \) be a finite-dimensional complex Lie algebra and \( a \) an ideal of \( g \) such that \( g/a \) is semisimple. Show that there exists in \( g \) a semisimple Lie subalgebra \( s \) supplementary to \( a \). (Use (21.23.3) and (21.6.4).)

6. (a) Let \( G \) be a simply connected complex Lie group, \( H \) a connected normal Lie subgroup of \( G \), and \( \pi : G \to G/H \) the canonical mapping. Show that the principal bundle \( G \) with base \( G/H \) and fiber \( H \), is trivializable. (To prove the existence of a holomorphic section over \( G/H \) (16.14.5), proceed by induction on \( \text{dim}(G/H) \), by using (16.14.9) to reduce to the case where the group \( G/H \) is either 1-dimensional or almost simple.) Deduce that \( H \) is simply connected.

(b) Let \( G \) be a connected complex Lie group and \( H \) a connected normal Lie subgroup of \( G \). Show that the canonical mapping \( \pi_1(H) \to \pi_1(G) \) (16.27.6) is injective. (Use (a).)

7. Extend the proof of Levi's theorem and the results of Problems 1 to 6 to real Lie groups.

8. Let \( G \) be a connected real Lie group. We propose to prove that there exists in \( G \) a maximal compact subgroup \( K \) and a finite number \( L_1, \ldots, L_m \) isomorphic to \( R^n \) or \( T^n \), with \( n > 0 \) if \( G \) is not semisimple. (Use Section 19.12, Problem 2, applied to the radical of the Lie algebra of \( G \).)
(c) Now proceed by induction on the dimension of $G$. Show first that if $L'$ is a closed subgroup of $G/J$ isomorphic to $R$, then there exists a closed subgroup $L$ of $G$ isomorphic to $R$ such that $L \cap J = \{e\}$ and such that the projection $p: G \to G/J$, restricted to $L$, is an isomorphism of $L$ onto $L'$. (Use Section 12.9, Problem 10.) Then observe that if $J$ is isomorphic to $R^n$ and $K'$ is a compact subgroup of $G/J$, the inverse image $p^{-1}(K')$ is the semidirect product of $J$ and a compact subgroup (Section 19.14, Problem 3).

9. (a) Let $G$ be a connected real Lie group. The radical of $G$ is defined to be the connected Lie group $R_0$ immersed in $G$ whose Lie algebra is the radical of the Lie algebra of $G$. Show that $R_0$ is closed in $G$ and that the quotient group $G/R_0$ is semisimple.

(b) Let $Z'$ be the (discrete) center of $G/R_0$. Show that every solvable normal subgroup of $G$ is contained in the inverse image $R$ of $Z'$ in $G$. (Use Section 12.8, Problem 5.) The group $R_0$ is the identity component of $R$.

(c) If $G$ is simply connected, then so is $R_0$ (Problem 6), and $G$ is the semidirect product $R_0 \times_n S$ of $R_0$ and a simply connected semisimple group $S$. Show that when $R_0$ is commutative, the structure of $G$ can be completely described in terms of $S$ and its finite-dimensional continuous linear representations.

(d) If $u: G \to G'$ is a surjective homomorphism of $G$ onto a Lie group $G'$, show that $u(R_0)$ is the radical of $G'$ (cf. Problem 5).

(e) Show that the radical of a product $G_1 \times G_2$ of connected Lie groups is the product of the radicals of $G_1$ and $G_2$.

10. A connected Lie group $G$ is said to be reductive if its adjoint representation $\text{Ad}: G \to \text{GL}(g)$ is completely reducible.

(a) Show that the following conditions are equivalent:

- (a) $G$ is reductive.
- (b) $\mathfrak{d}(g)$ is semisimple.
- (c) The radical $R_0$ of $G$ is contained in the center of $G$.

(b) If $G$ is a simply connected reductive group, it is the product of a simply connected semisimple group and a group isomorphic to $R^n$. Deduce from this the description of an arbitrary reductive Lie group. Give an example of a reductive group $G$ whose commutator subgroup is not closed in $G$ (cf. Section 21.18, Problem 18).

(c) Let $G$ be a connected Lie group. Show that for every continuous linear representation of $G$ on a finite-dimensional complex vector space to be completely reducible, it is necessary and sufficient that $G$ should be reductive and $G/\mathfrak{Z}(G)$ compact. (To show that the condition is sufficient, consider a linear representation $\rho$ of $G$ on a vector space $V$ and a subspace $W$ of $V$ stable under $\rho$, and observe that $G$ acts on the vector subspace $E$ consisting of endomorphisms $v$ such that $\rho(s) \circ v = v \circ \rho(s)$ for all $s \in \mathfrak{Z}(G)$ and $v(W) \subseteq W$, and such that the restriction of $v$ to $W$ is a homothety.)

11. (a) Let $G$ be a connected Lie group, $Z$ its center, $Z_0$ the identity component of $Z$, and $\pi: G/Z_0 \to G/Z$ the canonical homomorphism, whose kernel $Z/Z_0$ is discrete. Identify the differential manifold $G/Z$ with the product $K \times E$, where $K$ is a maximal compact subgroup of $G$ and $E$ is diffeomorphic to a vector space $R^n$ (Problem 9). Then, if $\pi^{-1}(K) = M$ and if $F$ is the identity component of $\pi^{-1}(E)$, the manifold $G/Z_0$ may be identified with $M \times F$; $M$ is a connected covering group of $K$, and $F$ is diffeomorphic to $R^n$.

(b) If $G$ is solvable, show that $M$ is commutative and is of the form $N/Z_0$, where $N$ is a connected nilpotent Lie subgroup of $G$, containing $Z$. Deduce that $Z$ is contained in a connected commutative Lie subgroup of $G$ (cf. Section 19.14, Problem 7(b)).

(c) If $G$ is semisimple, so that $Z_0 = \{e\}$, then $M$ is of the form $K_1 \times R^n$, where $K_1$ is a
compact subgroup of $G$ (21.6.9), and $Z$ is contained in $Z_1 \times \mathbf{R}^*$, where $Z_1$ is the center of $K_1$. Deduce that $Z$ is contained in a connected commutative Lie subgroup of $G$.

(d) Deduce from (b) and (c) that for every connected Lie group $G$, the center $Z$ of $G$ is contained in a connected commutative Lie subgroup of $G$. (Consider first the case where $G$ is simply connected, and apply Problem 9(c), by observing that if $A$ is a connected commutative Lie subgroup of $S$, then $R_0 A$ is a connected solvable Lie subgroup of $G$. Then pass to the general case by using (20.22.5.1).)

(e) Deduce from (d) that $Z$ is an elementary commutative group (Section 19.7, Problem 5). In particular, if $Z$ is not compact, there exists an element $c \in Z$ such that the group generated by $c$ (consisting of the powers $c^n$ for $n \in Z$) is infinite.

12. Let $G$ be a connected Lie group and $H$ a connected Lie group immersed in $G$ and dense in $G$. Then we know (Section 19.11, Problem 3) that, if $g$ and $h$ are the Lie algebras of $G$ and $H$, respectively, $h$ is an ideal in $g$, and $g/h$ is commutative.

(a) Let $h = r \oplus s$, where $r$ is the radical of $h$, and $s$ is a semisimple Lie subalgebra of $h$. Show that if $r'$ is the radical of $g$ (which contains $r$) then $g = r' \oplus s$.

(b) Let $\tilde{G}$ be the universal covering group of $G$ and let $\pi: \tilde{G} \to G$ be the canonical homomorphism, with kernel $D$. We may write $\tilde{G} = R_0 \times S$, where $\text{Lie}(R_0) = r'$ and $\text{Lie}(S) = s$ (Problem 9(c)). Let $D_1, D_2$ be the projections of $D$ on $R_0$ and $S$, respectively; then $D_1$ is contained in the centralizer of $S$, and $D_2$ is contained in the center of $S$. Let $H'$ and $R_0$ be the connected Lie groups immersed in $\tilde{G}$ whose Lie algebras are $h$ and $r$, respectively. Then $H'$ and $R_0$ are closed in $\tilde{G}$, and we have $H' = R_0 \times s; R_0$ is the radical of $H'$, and $\pi(R_0)$ the radical of $H' = \pi(H')$.

(c) Show that $R_0 = D_1 R_0$ (closure in $\tilde{G}$). If $U$ is a connected Lie subgroup of $S$ that contains the center of $S$, deduce that $R_0 \subseteq DUR_0$, and hence that $G = \pi(U) \pi(R_0) H$.

(d) With the same hypotheses, show that $\pi(U) \pi(R_0)$ is closed in $G$ and that $\pi(U) \pi(R_0) \cap H = \pi(U) \pi(R_0)$.

13. Let $G$ be a connected Lie group and $H$ a connected Lie group immersed in $G$. For $H$ to be closed in $G$, it is necessary and sufficient that the closure in $G$ of every one-parameter subgroup of $H$ should be contained in $H$ (Malcev’s theorem). (Use Problem 12 to reduce the question to proving that $\pi(U) \pi(R_0)$ is closed in $G$; by Problem 11, we may take $U$ to be commutative, and then $\pi(U) \pi(R_0)$ is solvable, and we can apply Section 19.14, Problem 15.)

Deduce that for $H$ to be closed in $G$ it is necessary and sufficient that the intersection of $H$ with every compact subgroup $K$ of $G$ should be closed in $K$. (Use Section 12.9, Problem 10.)

14. Let $G$ be a complex connected semisimple Lie group, $g$ its Lie algebra, and consider a root decomposition (21.10.1.1) of $g$. We shall use the notation of (21.10.3). Let $B = \{\beta_1, \ldots, \beta_l\}$ be a basis of the root system $S$, and put $h_j = h_{\beta_j}, 1 \leq j \leq l$. The $h_j$ and the $x_\alpha, \alpha \in S$, form a basis of the vector space $g$.

(a) Let $B_1$ be a subset of $B$, let $S_1 \subseteq S$ be the set of roots that are linear combinations of roots belonging to $B_1$, and let $h_1 \subseteq h$ be the subspace spanned by the $h_j$ such that $\beta_j \in B_1$. Show that the (direct) sum of $h_j$ and the $g_\alpha$ such that $\alpha \in S_1$ is a semisimple Lie algebra. (To calculate the Killing form, use (21.19.8.1) and (21.20.4.2).)

(b) Let $h_2$ be the subspace of $h$ defined by the equations $\beta_j(u) = 0$ for $\beta_j \in B_1$. Show that if $p$ is the parabolic subalgebra defined in Section 21.22, Problem 12(c) with $Q = -(S_1)_+$, then the radical of $p$ is the direct sum $r_1$, of $h_2$ and the $g_\alpha$ such that $\alpha \in S_+ \cap (S_1)_+$, and $p = g_1 \oplus r_1$ is a Levi decomposition of $p$. 
Show that \( \Sigma(p) = \{p, p\} \) is the direct sum of \( \mathfrak{g} \), and that the sum \( r_2 \) of these latter subspaces is the radical of \( \{p, p\} \). Show that \( p \) is the normalizer of \( r_2 \) in \( \mathfrak{g} \).

15. (a) With the hypotheses and notation of Problem 14, let \( \lambda_j \) be the linear form on \( \mathfrak{g} \) such that \( \lambda_j(x) = 0 \) for all \( x \in \mathfrak{s} \). Show that for each element \( x \in \mathfrak{g} \) there exists an automorphism \( \tau = \exp(\operatorname{ad}(u)) \) of \( \mathfrak{g} \) and an index \( j \) such that \( \lambda_j(\tau(x)) = 0 \). (Reduce to the case where \( x \in \mathfrak{h} \).)

(b) Deduce from (a) that there exists an automorphism \( \tau_1 = \exp(\operatorname{ad}(u_1)) \) of \( \mathfrak{g} \) such that \( \tau_1(x) \) belongs to the vector subspace that is the sum of the \( \mathfrak{g}_\alpha, \alpha \in \mathfrak{s} \). (Argue by induction on the dimension of \( \mathfrak{g} \), using Problem 14.)

(c) Deduce from (b) that there exist two elements \( y, z \in \mathfrak{g} \) such that \( x = [y, z] \). (Cf. (21.7.6.3).)

16. In the group \( \text{GL}(n, \mathbb{C}) \), let \( \mathfrak{l}(n) \) denote the subgroup of all lower triangular matrices with all diagonal elements equal to 1 (in other words, matrices \( (a_{ij}) \) such that \( a_{ij} = 0 \) for \( i < j \) and \( a_{ii} = 1 \) for all \( i \)). Also let \( \mathfrak{s}(n) \) denote the subgroup of all upper triangular matrices (i.e., matrices \( (a_{ij}) \) such that \( a_{ij} = 0 \) for \( i > j \)). For each matrix \( X = (x_{ij}) \in \text{GL}(n, \mathbb{C}) \) and each integer \( k \in [1, n] \), let \( X_k \) denote the matrix \( (x_{ij})_{i,j \leq k} \), and put \( \Delta_k(X) = \det(X_k) \) (the "principal minors" of \( X \)). The set of matrices \( X \in \text{GL}(n, \mathbb{C}) \) such that \( \Delta_k(X) \neq 0 \) for \( 1 \leq k \leq n - 1 \) is a dense connected open set in \( \text{GL}(n, \mathbb{C}) \) (Section 16.3, Problem 3). Show that the mapping \( (Y, Z) \mapsto YZ \) of \( \mathfrak{l}(n) \times \mathfrak{s}(n) \) into \( \text{GL}(n, \mathbb{C}) \) is an isomorphism of complex manifolds of \( \mathfrak{l}(n) \times \mathfrak{s}(n) \) onto \( \Omega \); the inverse mapping \( X \mapsto (i(X), s(X)) \) is such that the entries of the matrices \( i(X) \) and \( s(X) \) are rational functions of the \( x_{ij} \). (Observe that \( \Delta_k(s(X)) = \Delta_k(X) \) for \( 1 \leq k \leq n \).

17. (a) With the hypotheses and notation of Problems 14 and 16, put \( n = \dim(\mathfrak{g}) \) and suppose that \( \mathfrak{g} \) has trivial center, so that \( \mathfrak{g} \) may be identified with \( \text{Ad}(\mathfrak{g}) \). Then identify \( \mathfrak{g} \) with a subgroup of \( \text{GL}(n, \mathbb{C}) \) by identifying the canonical basis of \( \mathfrak{C}^* \) with the basis of \( \mathfrak{g} \) ranged in the following order:

\[
-\mathbf{x}, \ldots, -\mathbf{x}, \mathbf{h}, \ldots, \mathbf{h}, \mathbf{x}, \ldots, \mathbf{x},
\]

where the positive roots \( \alpha_1, \ldots, \alpha_m \) are ordered so that if \( \alpha_i + \alpha_j = \alpha_k \) is a root, then \( i < k \) and \( j < k \). Let \( \mathfrak{b} = \mathfrak{h} \oplus \mathfrak{n}_- \) be the Borel subalgebra spanned by the \( \mathbf{h} \) and the \( \mathbf{x} \) with \( \alpha \in \mathfrak{s}_+ \), and let \( \mathfrak{n}_- \) be the nilpotent subalgebra spanned by the \( -\mathbf{x} \) for \( \alpha \in \mathfrak{s}_+ \), so that \( \mathfrak{g} = \mathfrak{b} \oplus \mathfrak{n}_- \). Let \( \mathfrak{b} \) and \( \mathfrak{n}_- \) be the connected Lie subgroups of \( \mathfrak{g} \) having \( \mathfrak{b} \) and \( \mathfrak{n}_- \) as their respective Lie algebras. With the notation of Problem 16, show that \( \mathfrak{b} = \mathfrak{g} \cap \mathfrak{s}(n) \) and \( \mathfrak{n}_- = \mathfrak{g} \cap \mathfrak{l}(n) \); furthermore, if \( \Omega_0 = \mathfrak{g} \cap \mathfrak{g} \), then \( \Omega_0 \) is a dense connected open set in \( \mathfrak{g} \), and \( \mathfrak{b} \) (resp. \( \mathfrak{n}_- \)) is the image of \( \Omega_0 \) under the mapping \( X \mapsto s(X) \) (resp. \( X \mapsto i(X) \)); also the mapping \( (Y, Z) \mapsto YZ \) of \( \mathfrak{n}_- \times \mathfrak{b} \) into \( \mathfrak{g} \) is an isomorphism of complex manifolds of \( \mathfrak{n}_- \times \mathfrak{b} \) onto \( \Omega_0 \).

(b) Let \( \mathfrak{n}_+ \) (resp. \( \mathfrak{n}_-^* \)) be the sum of the \( \mathfrak{g}_\alpha \) for \( \alpha \in \mathfrak{s}_+ \) (resp. \( \alpha \in \mathfrak{s}_- \cap \mathfrak{i}(\mathfrak{s}_-)_+ \)). Then we have \( \mathfrak{n}_+ = \mathfrak{n}_+^* \oplus \mathfrak{n}_-^* \), and \( \mathfrak{n}_+^* \) is a Lie subalgebra of \( \mathfrak{n}_- \), and \( \mathfrak{n}_-^* \) is an ideal of \( \mathfrak{n}_- \). If \( \mathfrak{n}_-^* \) and \( \mathfrak{n}_-^\ast \) are the connected Lie subgroups having \( \mathfrak{n}_+^* \), \( \mathfrak{n}_-^* \) as their Lie algebras, then the mapping \( (Y', Y'') \mapsto YY'' \) of \( \mathfrak{n}_-^\ast \times \mathfrak{n}_-^\ast \) into \( \mathfrak{n}_- \) is an isomorphism of complex manifolds. If \( \mathfrak{p} \) is the parabolic subgroup of \( \mathfrak{g} \) with Lie algebra \( \mathfrak{p} \), we have \( \mathfrak{n}_-^\ast \mathfrak{p} \subset \mathfrak{n}_-^\ast \mathfrak{p} \), and \( \mathfrak{b} = \mathfrak{n}_-^\ast \mathfrak{p} \) is a submanifold of \( \mathfrak{n}_-^\ast \mathfrak{p} \) of \( \mathfrak{n}_-^\ast \mathfrak{p} \).

(c) Let \( \mathfrak{p}(n) \) be the normalizer in \( \text{GL}(n, \mathbb{C}) \) of \( r_2 \), considered as a Lie subalgebra of \( \mathfrak{g}(n, \mathbb{C}) \). Show that the normalizer \( \mathcal{N}(\mathfrak{p}) \) of \( \mathfrak{p} \) in \( \mathfrak{g} \) is equal to \( \mathfrak{g} \cap \mathfrak{p}(n) \).

(d) Show that \( \mathcal{N}(\mathfrak{p}) \cap \mathfrak{n}_-^\ast = \{e\} \). (Use the fact that the exponential mapping of \( \mathfrak{n}_-^\ast \) into
Let \( \mathfrak{g} \) be a finite-dimensional real Lie algebra, and let \( G \) be a connected Lie subgroup of \( \text{Aut}(\mathfrak{g}) \). Suppose that there exists a decreasing sequence \( \mathfrak{g} = \mathfrak{g}_{-1} \supset \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \cdots \supset \mathfrak{g}_r \) of \( G \)-stable vector subspaces of \( \mathfrak{g} \) containing \( \mathfrak{g}_0 \) and such that \( \mathfrak{g}_0 \) is simple and \( \mathfrak{g}_1 \) is the radical of \( \mathfrak{g}_0 \).

(a) Show that \( \mathfrak{g}_j \neq \mathfrak{g}_{j+1} \) for \( -1 \leq j \leq r \).

(b) For each nonzero \( G \)-stable ideal \( \mathfrak{i} \) of \( \mathfrak{g}_j \), show that \( \mathfrak{g}_j = \mathfrak{g}_j \oplus \mathfrak{i} \). (Use (c) by considering the derived algebras \( \mathfrak{d}(\mathfrak{g}) \), where \( \mathfrak{g} \) is the radical of \( \mathfrak{g} \); then observe that if \( \mathfrak{g} \) is semisimple, every connected Lie subgroup of \( \text{Aut}(\mathfrak{g}) \) leaves stable the simple components of \( \mathfrak{g} \).)

(c) Show that there exists a unique \( G \)-stable ideal \( \mathfrak{i} \) of \( \mathfrak{g}_j \), and such that its restriction to \( \mathfrak{g}_j \) is the class of \( [x, y] \).

(d) Show that \( \mathfrak{g} \) is a simple Lie algebra. (Use (c) by considering the derived algebras \( \mathfrak{d}(\mathfrak{g}) \), where \( \mathfrak{g} \) is the radical of \( \mathfrak{g} \); then observe that if \( \mathfrak{g} \) is semisimple, every connected Lie subgroup of \( \text{Aut}(\mathfrak{g}) \) leaves stable the simple components of \( \mathfrak{g} \).)

(e) Show that there exists a unique \( G \)-stable ideal \( \mathfrak{i} \) of \( \mathfrak{g}_j \), and such that its restriction to \( \mathfrak{g}_j \) is the class of \( [x, y] \).

(f) Show that the Killing form \( \mathfrak{k} \) of \( \mathfrak{g} \) is nondegenerate, and that \( \mathfrak{k} \) is orthogonal to \( \mathfrak{g}_j \). (Consider the involutory automorphism \( \sigma \) of \( \mathfrak{g} \) such that \( \sigma(x) = x \) for \( x \in \mathfrak{g}_0 \).)

(g) Show that \( \mathfrak{g} \) is a simple Lie algebra. (Use (c) by considering the derived algebras \( \mathfrak{d}(\mathfrak{g}) \), where \( \mathfrak{g} \) is the radical of \( \mathfrak{g} \); then observe that if \( \mathfrak{g} \) is semisimple, every connected Lie subgroup of \( \text{Aut}(\mathfrak{g}) \) leaves stable the simple components of \( \mathfrak{g} \).)

(h) Show that, for the Killing form \( B \) of \( \mathfrak{g} \), the restriction of \( B \) to \( \mathfrak{g}_0 \) is nondegenerate, and that \( \mathfrak{k} \) is orthogonal to \( \mathfrak{g}_0 \). (Consider the involutory automorphism \( \sigma \) of \( \mathfrak{g} \) such that \( \sigma(x) = x \) for \( x \in \mathfrak{g}_0 \).)

(i) Show that there exists a Cartan decomposition \( \mathfrak{g} = \mathfrak{h} \oplus \mathfrak{p} \) such that \( \mathfrak{h} \) is a simple Lie algebra. (Use (c) by considering the derived algebras \( \mathfrak{d}(\mathfrak{g}) \), where \( \mathfrak{g} \) is the radical of \( \mathfrak{g} \); then observe that if \( \mathfrak{g} \) is semisimple, every connected Lie subgroup of \( \text{Aut}(\mathfrak{g}) \) leaves stable the simple components of \( \mathfrak{g} \).)
APPENDIX

MODULES

(The numbering of the sections in this Appendix continues that of the Appendix to Volume IV.)

22. SIMPLE MODULES

(A.22.1) The notion of a module over a commutative ring (A.8.1) may be generalized. If \( M \) is a commutative group, written additively, an action \( R \) of a set \( \Omega \) on \( M \) is any mapping \( (\alpha, x) \mapsto \alpha \cdot x \) of \( \Omega \times M \) into \( M \) such that \( \alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y \); in other words, for each \( \alpha \in \Omega \) the mapping \( x \mapsto \alpha \cdot x \) is an endomorphism of the group \( M \). By abuse of language, the group \( M \) together with an action of \( \Omega \) on \( M \) is called an \( \Omega \)-module. A homomorphism of an \( \Omega \)-module \( M \) into an \( \Omega \)-module \( N \) is any mapping \( f: M \to N \) such that \( f(x + y) = f(x) + f(y) \) and \( f(\alpha \cdot x) = \alpha \cdot f(x) \) for all \( x, y \in M \) and \( \alpha \in \Omega \). An isomorphism of \( \Omega \)-modules is a bijective homomorphism; the inverse mapping is then also an isomorphism.

(A.22.2) If \( M \) is an \( \Omega \)-module, a subgroup \( N \) of \( M \) is said to be stable for the action of \( \Omega \) (or \( \Omega \)-stable) if for all \( x \in N \) and \( \alpha \in \Omega \) we have \( \alpha \cdot x \in N \); the subgroup \( N \) is also said to be an \( \Omega \)-submodule of \( M \). Intersections and sums of \( \Omega \)-submodules of \( M \) are again \( \Omega \)-submodules. If \( f \) is any homomorphism of \( M \) into an \( \Omega \)-module \( M' \), and if \( N \) (resp. \( N' \)) is any \( \Omega \)-submodule of \( M \) (resp. \( M' \)), then \( f(N) \) is an \( \Omega \)-submodule of \( M' \), and \( f^{-1}(N') \) is an \( \Omega \)-submodule of \( M \). In particular, the image \( f(M) \) is an \( \Omega \)-submodule of \( M' \), and the kernel \( f^{-1}(0) \) is an \( \Omega \)-submodule of \( M \).
(A.22.3) In any $\Omega$-module $M$, $\{0\}$ and $M$ are always $\Omega$-submodules, called the trivial submodules. An $\Omega$-module $M$ is called simple if $M \neq \{0\}$ and there exist no $\Omega$-submodules of $M$ except for the trivial ones.

(A.22.4) (Schur's lemma) Let $f$ be a homomorphism of an $\Omega$-module $M$ into an $\Omega$-module $N$. If $M$ is simple, then $f$ is either injective or identically zero. If $N$ is simple, then $f$ is either surjective or identically zero. If both $M$ and $N$ are simple, then $f$ is either bijective or identically zero.

For if $M$ is simple, $f^{-1}(0)$ can only be $M$ or $\{0\}$; and if $N$ is simple, $f(M)$ can only be $N$ or $\{0\}$.

23. SEMISIMPLE MODULES

(A.23.1) The notion of direct sum of $\Omega$-modules is defined as in (A.1.5). If $M = \bigoplus_{\lambda \in L} M_\lambda$ is the direct sum of a family $(M_\lambda)$ of $\Omega$-modules, we define as in (A.2.3) the canonical injection $j_\lambda: M_\lambda \to M$ and the canonical projection $p_\lambda: M \to M_\lambda$ for each index $\lambda$; they are $\Omega$-module homomorphisms. All the results of (A.3.1)-(A.3.5) remain valid without modification if we replace "subspace" by "$\Omega$-submodule" and "linear mapping" by "homomorphism."

(A.23.2) An $\Omega$-module $M$ is said to be semisimple if it is a direct sum of a family of simple $\Omega$-modules. We shall limit our attention to semisimple $\Omega$-modules that are direct sums of at most denumerable families of simple $\Omega$-modules.

(A.23.3) Let $M$ be an $\Omega$-module that is the sum (not necessarily direct) of a finite or infinite sequence $(N_k)_{0 \leq k < \omega}$ (where $\omega$ is an integer or $+\infty$) of simple $\Omega$-submodules. Let $E$ be an $\Omega$-submodule of $M$. Then:

(a) There exists a subset $J$ of the set $[0, \omega[$ such that $M$ is the direct sum of $E$ and the $N_k$ with $k \in J$ (so that $E$ has as a supplement in $M$ the semisimple $\Omega$-submodule $F$ which is the direct sum of the $N_k$ with $k \notin J$).

(b) There exists a subset $H$ of the set $[0, \omega[$ such that $J \cap H = \emptyset$ and such that $M$ is the direct sum of the $N_k$ with $k \in J \cup H$ (and therefore $M$ is semisimple); $E$ is isomorphic to the direct sum of the $N_k$ with $k \in H$.

(a) We shall define $J$ to be the set of elements of a (finite or infinite) sequence $(k_m)$ that is constructed inductively as follows: $k_m$ is the smallest
integer (if it exists) such that \( N_{k_m} \) is not contained in the sum

\[
E + N_{k_1} + \cdots + N_{k_{m-1}}
\]

(when \( m = 1 \), this sum is replaced by \( E \)). The construction stops if \( E + N_{k_1} + \cdots + N_{k_{m-1}} \) contains all the \( N_k \) and hence is equal to \( M \). If \( k_m \) is defined, the intersection \( N_{k_m} \cap (E + N_{k_1} + \cdots + N_{k_{m-1}}) \), being a submodule of \( N_{k_m} \) distinct from \( N_{k_m} \), must be zero; hence (A.3.3) the sum of \( E \) and the \( N_k \) such that \( k \in J \) is direct. It remains to be shown that, when \( J \) is infinite, this sum \( M' \) is equal to \( M \). If not, there would exist at least one index \( h \notin J \) such that \( N_h \notin M' \); but if \( m \) is the smallest integer such that \( k_m > h \), then \( N_h \) is not contained in \( E + N_{k_1} + \cdots + N_{k_{m-1}} \), contrary to the definition of \( k_m \).

(b) The set \( H \) is defined by applying (a) to the \( \Omega \)-submodule \( F \) of \( M \). The isomorphism of \( E \) with the direct sum of the \( N_k \) such that \( k \in H \) then follows from (A.3.5).

(A.23.4) A semisimple \( \Omega \)-module \( M \) is said to be isotypic if it is a direct sum of isomorphic simple \( \Omega \)-submodules. It follows from (A.23.3) that any two simple \( \Omega \)-submodules of \( M \) are isomorphic (since a simple \( \Omega \)-module cannot be isomorphic to a direct sum of two nonzero submodules). Two isotypic semisimple \( \Omega \)-modules are said to be of the same type if every simple submodule of one is isomorphic to every simple submodule of the other. It follows from (A.23.3) that every submodule of an isotypic semisimple \( \Omega \)-module is isotypic semisimple and of the same type.

(A.23.5) Let \( M \) be a semisimple \( \Omega \)-module, the direct sum of a (finite or infinite) sequence \( (N_k)_{0 \leq k < \omega} \) of simple \( \Omega \)-submodules of \( M \). We define by induction a sequence of submodules \( N'_k \) of \( M \) as follows. We take \( N'_0 = N_0 \); \( N'_{k+1} \) is equal to \( N_m \) for the smallest index \( m \) such that \( N_m \) is not isomorphic to any of the \( \Omega \)-modules \( N'_0, \ldots, N'_k \). (If all the \( N_k \) are isomorphic to one or other of these \( \Omega \)-modules, the induction stops at \( N'_k \).) Let \( J \) be the set of indices \( k \in [0, \omega[ \) so obtained, and for each \( k \in J \) let \( I_k \) be the set of integers \( m \) such that \( N_m \) is isomorphic to \( N'_k \). If \( P_k \) is the direct sum of the \( \Omega \)-submodules \( N_m \) for \( m \in I_k \), then it is clear that \( P_k \) is an isotypic semisimple \( \Omega \)-module, that \( P_k \) and \( P_h \) are not of the same type if \( h \neq k \), and that \( M \) is the direct sum of the \( P_k \) for \( k \in J \).

(A.23.6) Every simple \( \Omega \)-submodule \( N \) of \( M \) is contained in one of the \( P_k \) (and hence is of the same type as \( P_k \)).

It follows from (A.23.3) that \( N \) must be isomorphic to one of the \( N_m \), hence to one of the \( N'_k \); if \( N \) were not contained in \( P_k \), we should have \( N \cap P_k = \emptyset \) because \( N \) is simple, and the projection \( N' \) of \( N \) on the direct
sum $M_k$ of the $P_h$ such that $h \neq k$ would be isomorphic to $N$ (A.22.4); but by reason of (A.23.3) applied to $M_k$, $N'$ would be isomorphic to one of the modules $N'_k$ with $h \neq k$, which is absurd.

We may therefore define the $P_k$ independently of any decomposition of $M$ as a direct sum of simple $\Omega$-submodules: $P_k$ is the sum of all the simple $\Omega$-submodules of $M$ that are isomorphic to $N'_k$. The $P_k$ are called the isotypic components of $M$. The result of (A.23.6) then generalizes as follows:

$$(A.23.7) \quad \text{Every } \Omega\text{-submodule } N \text{ of } M \text{ is the direct sum of the } N_k = M \cap P_k \text{ that are not equal to } 0, \text{ and these are the isotypic components of } N.$$ 

This is an immediate consequence of (A.23.3) and (A.23.6), because $N$ is a direct sum of simple $\Omega$-submodules of $M$.

24. EXAMPLES

(A.24.1) Let $K$ be a (commutative) field and $E$ a vector space over $K$. It is clear that $E$ is a simple $K$-module if and only if $E$ is one-dimensional (i.e., a "line"). Every $K$-vector space that is spanned by an at most denumerable family of vectors is therefore an isotypic semisimple $K$-module (there is only one "type"), and the results of (A.23) therefore include as particular cases the propositions (A.4.6) and (A.4.5) for vector spaces that admit an at most denumerable basis.

(A.24.2) Now let $(u_\lambda)_{\lambda \in L}$ be a set of endomorphisms of the $K$-vector space $E$ (A.2.1) and let $\Omega$ be the sum (1.8) of the sets $L$ and $K$. If we define $\lambda \cdot x = u_\lambda(x)$, then $\Omega$ acts on $E$. It is clear that the notions of linear representation introduced in (15.5) and (21.1) are particular cases of this general notion, and correspond to taking $L$ to be an algebra or a group. The notion of equivalent linear representations corresponds to that of isomorphism of $\Omega$-modules (subjected to supplementary conditions when $E$ is infinite-dimensional and endowed with a topology); the notion of a finite Hilbert sum of representations corresponds to a particular case of the notion of direct sum of $\Omega$-modules. Finally, if $E$ is finite-dimensional, it comes to the same thing to say that a representation is irreducible or that the corresponding $\Omega$-module is simple.

(A.24.3) Consider in particular the case of a single endomorphism $u$ of the vector space $E$; it is said to be semisimple when the corresponding $\Omega$-module $E$ is semisimple. The nature of the simple $\Omega$-modules will depend on the field
K. For example, if $K = \mathbb{R}$ and $E$ is a plane, a rotation $u$ (relative to the usual scalar product) other than $\pm 1$ will make $E$ a simple $\text{O}$-module, and it is easy to give examples of vector spaces $E$ of any given finite dimension $n$ over a suitable field $K$ that are simple $\text{O}$-modules for certain endomorphisms.

The most important case in analysis is that in which $K$ is algebraically closed and $E$ is finite-dimensional. The simple $\text{O}$-modules corresponding to an endomorphism $u$ are then the "lines" $Kx$, where $x$ is an eigenvector of $u$ (A.6.9), because the restriction of $u$ to a subspace $F$ of $E$ that is stable under $u$ always admits at least one eigenvector in $F$. Hence, in this case, to say that $u$ is semisimple means that there exists a basis $(e_j)_{1 \leq j \leq n}$ of $E$ consisting of eigenvectors for $u$, or equivalently that the matrix of $u$ with respect to this basis is diagonal; for this reason the endomorphism $u$ is also said to be diagonalizable. If $\lambda_1, \ldots, \lambda_r$ are the distinct eigenvalues of $u$, the isotypic components of $E$ (for $u$) are the eigenspaces $E(\lambda_j; u)$ for $1 \leq j \leq r$ (11.1). The description of the vector subspaces of $E$ that are stable under $u$ can be read off immediately from (A.23.7): they are the direct sums $F_1 \oplus F_2 \oplus \cdots \oplus F_r$, where $F_j$ is any vector subspace of $E(\lambda_j; u)$ for $1 \leq j \leq r$.

(A.24.4) The example of a semisimple $\text{O}$-module that comes up in the theory of Lie groups is that in which $K$ is an algebraically closed field, $E$ a $K$-vector space with an at most denumerable basis, and $\text{O}$ the sum (or disjoint union) of $K$ and a $K$-vector space $L$. Suppose that $E$ is the sum of a finite or infinite sequence $(E_n)_{0 \leq n < \omega}$ (where $\omega$ is an integer or $+\infty$) of subspaces having the following property: for each $n$ such that $0 \leq n < \omega$ there exists a linear form $p_n: L \to K$ on $L$ such that $u \cdot x = p_n(u)x$ for all $u \in L$ and all $x \in E_n$, the forms $p_n$ being all distinct. It is then clear that every "line" $Kx$ contained in some $E_n$ is a simple $\text{O}$-module, that two lines $Kx$, $Ky$ contained in the same $E_n$ are isomorphic $\text{O}$-modules, and that if $Kx \subseteq E_n$, $Ky \subseteq E_m$ with $m \neq n$, then $Kx$ and $Ky$ are not isomorphic as $\text{O}$-modules. It follows immediately from (A.23.3) and (A.23.6) that in fact $E$ is the direct sum of all the $E_n$, which are the isotypic components of the semisimple $\text{O}$-module $E$. Moreover, every simple $\text{O}$-submodule of $E$ is a line $Kx$ contained in one of the $E_n$, and more generally every $\text{O}$-submodule $F$ of $E$ is the direct sum of the $F \cap E_n$ (A.23.7).

25. THE CANONICAL DECOMPOSITION OF AN ENDOMORPHISM

(A.25.1) Part of the proof of (11.3.3) for a compact operator on a normed space can be adapted to the case of an arbitrary endomorphism $u$ of a finite-dimensional vector space $E$ over an algebraically closed field $K$, and gives a more precise result than (A.6.10). Namely,
If $\lambda_1, \ldots, \lambda_r$ are the distinct eigenvalues of $u$, the space $E$ is the direct sum of $r$ subspaces $E_1, \ldots, E_r$ each stable under $u$, such that the restriction of $u$ to $E_j$ has only the eigenvalue $\lambda_j$. Moreover, if $v$ is the diagonalizable endomorphism of $E$ such that $v(x) = \lambda_j x$ for $x \in E_j$ ($1 \leq j \leq r$), then $w = u - v$ is nilpotent, and both $u$ and $w$ may be written as polynomials in $u$ with zero constant terms, say $v = b_1 u + \cdots + b_p u^p$, $w = c_1 u + \cdots + c_q u^q$, with coefficients in $K$ (and hence $vw = wv$).

We proceed by induction on the dimension of $E$ and, by replacing $u$ by $u - \lambda_1 \cdot 1_E$, we may assume that $\lambda_1 = 0$. We then form as in (11.3.3) the sequences of subspaces $N_1 = u^{-1}(0)$, $N_k = u^{-1}(N_{k-1})$ for $k > 1$, $F_1 = u(E)$, $F_k = u(F_{k-1})$ for $k > 1$. The dimensions of the $N_k$ (resp. $F_k$) form an increasing (resp. decreasing) sequence, and it is clear that there is a smallest integer $n$ such that $N_{k+1} = N_k$ for $k \geq n$, and a smallest integer $m$ such that $F_{k+1} = F_k$ for $k \geq m$. We have $N_n \cap F_n = \{0\}$, because if $y \in F_n \cap N_n$ there exists $x \in E$ such that $y = u^n(x)$, and on the other hand $u^n(y) = 0$, so that $u^{2n}(x) = 0$; which implies that $x \in N_{2n} = N_n$ and hence that $y = u^n(x) = 0$.

Next, we have $F_m \subset F_n$, and indeed $F_m = F_n$. For otherwise we should have $m > n$; let $z \in F_m \setminus F_n$ be such that $z \notin F_m$; since $u(z) \in F_m = u(F_m)$, there exists $t \in F_m$ such that $u(z) = u(t)$, hence $z - t \in N_1 \subset N_n$; since $z - t \in F_n$, it follows that $z = t$, which contradicts the choice of $z$. Finally, for each $x \in E$, we have $u^n(x) \in F_n = F_m$, and since $u^n(F_n) = F_n$ by the definition of $m$, there exists $y \in F_n$ such that $u^n(x) = u^n(y)$, hence $x - y \in N_n$, and consequently $E = F_n + N_n$, the sum being direct because $F_n \cap N_n = \{0\}$. The restriction of $u$ to $F_n$ is surjective, with kernel $F_n \cap N_1 \subset F_n \cap N_n = \{0\}$, hence is bijective; and the restriction of $u$ to $N_n$ is nilpotent by definition.

We now apply the inductive hypothesis to $u|F_n$ in order to obtain the decomposition $u = v + w$, where $v$ is diagonalizable and $w$ nilpotent; the restriction of $v$ to each $E_j$ is scalar multiplication by $\lambda_j$, hence commutes with every endomorphism of $E_j$, and in particular with $w|E_j$, from which it follows that $vw = wv$.

It remains to prove the last assertion. We distinguish three cases:

1. $r = 1$, so that $u$ has only one eigenvalue $\lambda$. If $\lambda = 0$, then $v = 0$ and $w = u$. If $\lambda \neq 0$, then $w^n = 0$, where $n = \dim(E)$, and $v = \lambda \cdot 1_E$, so that $(u - \lambda \cdot 1_E)^n = 0$ and therefore
\[ v = \binom{n}{1} u - \binom{n}{2} \lambda^{-1} u^2 + \cdots + (-1)^{n-1} \lambda^{-n+1} u^n \]
and $w = u - v$, which proves the result in this case.

2. Let $u_j = u|E_j$ and suppose that $u_h = 0$ for all $h \neq j$. We can then
apply the result of (1) to $E_j$ and $u_j$. If $u_j = P(u_j) + Q(u_j)$, where $P$ and $Q$ are polynomials with zero constant terms, $P(u_j)$ being diagonalizable and $Q(u_j)$ nilpotent, it is clear that $v = P(u)$ and $w = Q(u)$.

(3) General case: suppose first that $\lambda_j \neq 0$. Put

$$f_j = u \prod_{h \neq j} (u - \lambda_h \cdot 1_E)^{n_h}$$

where $n_h = \dim(E_h)$; it is clear that the restriction $f_j|_{E_h}$ is 0 for $h \neq j$, and $f_j|_{E_j}$ has only one eigenvalue, namely $\mu_j = \lambda_j \prod_{h \neq j} (\lambda_j - \lambda_h)^{n_h} \neq 0$. By case (2), there exists a polynomial $R_j$ with zero constant term such that $R_j(f_j)|_{E_j} = 1_{E_j}$ and $R_j(f_j)|_{E_h} = 0$ if $h \neq j$; but by definition $f_j = S_j(u)$, where $S_j$ is a polynomial with zero constant term; hence $P_j(u) = R_j(S_j(u))$ is a polynomial in $u$ with zero constant term, such that $P_j(u)|_{E_j} = 1_{E_j}$ and $P_j(u)|_{E_h} = 0$ for $h \neq j$. If $\lambda_j = 0$, then we take $P_j(u) = 0$. We have then $v = \sum_{j=1}^{r} \lambda_j P_j(u)$, and $w = u - v$, and the proof is complete.

(A.25.3) There exists only one decomposition $u = f + g$ of an endomorphism $u$ of $E$ such that $f$ is diagonalizable, $g$ nilpotent, and such that $fg = gf$.

Let $\mu_k$ ($1 \leq k \leq s$) be the distinct eigenvalues of $f$. Then $E$ is the direct sum of the eigenspaces $L_k = E(\mu_k; f)$ (A.24.3). Let us first show that $g(L_k) \subseteq L_k$ for all $k$. Indeed, let $x \in L_k$; we may write $g(x) = \sum_{h=1}^{s} z_h$, with $z_h \in L_h$ for $1 \leq h \leq s$, whence $f(g(x)) = \sum_{h=1}^{s} \mu_h z_h$; on the other hand, $f(x) = \mu_k x$, so that $g(f(x)) = \sum_{h=1}^{s} \mu_k z_h$, and the relation $f(g(x)) = g(f(x))$ therefore takes the form $\sum_{h=1}^{s} (\mu_k - \mu_h) z_h = 0$, so that we have $z_h = 0$ for all $h \neq k$, because the $\mu_k$ are all distinct. We may therefore (A.6.12) take a basis of $E$ that is the union of bases of the $L_k$, such that the restriction of $u$ to each $L_k$ is represented by a lower triangular matrix with diagonal elements all equal to $\mu_k$. Consequently the $\mu_k$ are the eigenvalues of $u$, and $L_k$ is the subspace $N(\mu_k)$ consisting of vectors $x \in E$ such that $(u - \mu_k \cdot 1_E)^m(x) = 0$ for large enough $m$. This proves that $f = v$ and $g = w$.

26. FINITELY GENERATED Z-MODULES

(A.26.1) A $\mathbb{Z}$-module $M$ (A.8.1) that admits a system of generators $(a_j)_{1 \leq j \leq n}$ consisting of $n$ elements is isomorphic to a quotient $\mathbb{Z}^n/N$ of a finitely generated free $\mathbb{Z}$-module. For if $(u_1, \ldots, u_n)$ is the canonical basis of
\(\mathbb{Z}^n\), we may define a surjective homomorphism \(f: \mathbb{Z}^n \to M\) by putting \(f(u_j) = a_j\) for \(1 \leq j \leq n\). The study of finitely generated \(\mathbb{Z}\)-modules is therefore reduced to that of the submodules and quotient modules of a finitely generated free \(\mathbb{Z}\)-module.

(A.26.2) Every submodule of a finitely generated free \(\mathbb{Z}\)-module is finitely generated and free.

Let \(L\) be a \(\mathbb{Z}\)-module having a basis \((a_1, \ldots, a_n)\) and let \(M\) be a submodule of \(L\). Denote by \(L_j = M \cap L_j\) the submodule of \(L\) with basis \(a_1, \ldots, a_j\), and put \(M_j = M \cap L_j\). If \((a_1^*, \ldots, a_n^*)\) is the basis dual to \((a_1, \ldots, a_n)\) in the dual \(\mathbb{Z}\)-module \(L^*\) (A.9.2), then the set of integers \(\langle x, a_j^* \rangle\), where \(x \in M_j\), is evidently an ideal in \(\mathbb{Z}\), hence is of the form \(m_j \mathbb{Z}\), where \(m_j\) is an integer \(\geq 0\). Hence there exists an element \(b_j \in M_j\) such that \(\langle b_j, a_j^* \rangle = m_j\); if \(m_j = 0\), we take \(b_j = 0\). Let \(M_j^*\) be the submodule of \(M\) generated by \(b_1, \ldots, b_j\); we shall show that \(M_j^* = M_j\). This is obvious when \(j = 1\), since \(M_1\) is the set of multiples \(p \cdot a_1\) of \(a_1\) that belong to \(M\), and \(\langle p a_1, a_j^* \rangle = p\). We proceed by induction on \(j\). If \(x \in M_j\), we have \(\langle x, a_j^* \rangle = p m_j\) for some \(p \in \mathbb{Z}\), hence \(\langle x - p b_j, a_j^* \rangle = 0\), and since by hypothesis \(x\) and \(b_j\) are linear combinations of \(a_1, \ldots, a_j\), it follows that \(x - p b_j \in M_{j-1}\), which by the inductive hypothesis is equal to \(M_{j-1}\); hence \(x \in M_j^*\) as required. Taking \(j = n\), we see that \(M\) is generated by \(b_1, \ldots, b_n\), and it remains to show that the nonzero \(b_j\) form a free system. Suppose then that we have a relation \(\sum_{j=1}^n k_j b_j = 0\), where the \(k_j b_j\) are not all zero. If \(h\) is the largest of the indices \(j\) such that \(k_j b_j \neq 0\), we have \(\langle k_h b_h, a_h^* \rangle = \langle \sum_{j=1}^n k_j b_j, a_h^* \rangle = 0\), because \(k_j b_j = 0\) for \(j > h\), and \(k_j b_j\) is a linear combination of \(a_1, \ldots, a_j\) for \(j < h\). Hence we have \(k_h m_h = 0\), contradicting \(k_h b_h \neq 0\).

(A.26.3) Let \(L\) be a finitely generated free \(\mathbb{Z}\)-module and \(M\) a submodule of \(L\). Then there exists a basis \((e_1, \ldots, e_n)\) of \(L\) and \(r \leq n\) integers \(\alpha_1, \ldots, \alpha_r\) which are \(> 0\) such that \(\alpha_j\) divides \(\alpha_{j+1}\) for \(1 \leq j \leq r - 1\), and such that \(\alpha_1 e_1, \ldots, \alpha_r e_r\) form a basis of \(M\). Furthermore, the numbers \(r\), \(n\) and \(\alpha_j\) \((1 \leq j \leq r)\) are uniquely determined by these properties.

Let \((a_1, \ldots, a_n)\) be a basis of \(L\) and \((a_1^*, \ldots, a_n^*)\) the dual basis of \(L^*\). We may assume that \(M \neq \{0\}\). Consider the integers \(\langle x, y^* \rangle\) for \(x \in M\) and \(y^* \in L^*\); by hypothesis, they are not all 0, and since \(\langle -x, y^* \rangle = -\langle x, y^* \rangle\), there exists \(x_1 \in M\) and \(y_1^* \in L^*\) such that \(\langle x_1, y_1^* \rangle = \alpha_1\) is the smallest of the nonzero integers \(|\langle x, y^* \rangle|\) for \(x \in M\) and \(y \in L^*\). We deduce first that for
each \( x \in M \), the integer \( \beta = \langle x, y^* \rangle \) is a multiple of \( \alpha_1 \); for otherwise the highest common factor \( \delta \) of \( \beta \) and \( \alpha_1 \) would be such that \( 0 < \delta < \alpha_1 \), and we should have \( \delta = \lambda \beta + \mu \alpha_1 \), by Bézout's identity, where \( \lambda \) and \( \mu \) are suitable integers; but this would imply \( \langle \lambda x + \mu x_1, y^*_1 \rangle = \delta \), contradicting the definition of \( \alpha_1 \). One proves in the same way that \( \langle x, y^*_1 \rangle \) is a multiple of \( \alpha_1 \) for each \( y^* \in L^* \). In particular, all the integers \( \langle x, \alpha_1 \rangle \) are multiples of \( \alpha_1 \), and hence there exists \( e_1 \in L \) such that \( x_1 = \alpha_1 e_1 \). Let \( L_1 = \text{Ker}(y^*_1) \); we shall show that \( L \) is the direct sum of \( \mathbb{Z} \alpha_1 e_1 \) and \( L_1 \). We have \( \langle e_1, y^*_1 \rangle = 1 \) by definition; hence, for any \( y \in L \), if \( \langle y, y^*_1 \rangle = \gamma \), we have \( \langle y - \gamma e_1, y^*_1 \rangle = 0 \), that is to say, \( y - \gamma e_1 \in L_1 \). Also, we cannot have \( \lambda e_1 \in L_1 \) unless \( \lambda = 0 \), by the definition of \( L_1 \), and this establishes our assertion. Likewise, \( M \) is the direct sum of \( \mathbb{Z} \alpha_1 e_1 \) and \( M_1 = M \cap L_1 \). Namely, for each \( x \in M \) we have \( \langle x, y^*_1 \rangle = \mu \alpha_1 \) for some \( \mu \in \mathbb{Z} \), hence \( \langle x - \mu \alpha_1 e_1, y^*_1 \rangle = 0 \), that is to say, \( x - \mu \alpha_1 e_1 \in L_1 \cap M = M_1 \).

By virtue of (A.26.2), \( L_1 \) admits a basis, and from the previous paragraph and the invariance of the number of elements in a basis of \( L \) (A.8.3), any basis of \( L_1 \) must have \( n - 1 \) elements. By induction on \( n \), we may assume that there is a basis \( (e_2, \ldots, e_n) \) of \( L_1 \) and \( r - 1 \leq n - 1 \) integers \( \alpha_2, \ldots, \alpha_r \), such that \( \alpha_j \) divides \( \alpha_{j+1} \) for \( 2 \leq j \leq r - 1 \) and such that \( \alpha_2 e_2, \ldots, \alpha_r e_r \) form a basis of \( M_1 \). It remains therefore to prove that \( \alpha_1 \) divides \( \alpha_2 \). If \( (e_1^*, \ldots, e_n^*) \) is the basis of \( L^* \) dual to \( (e_1, \ldots, e_n) \), we have \( \langle \alpha_1 e_1, e_1^* \rangle = \alpha_1 \) and \( \langle \alpha_2 e_2, e_2^* \rangle = \alpha_2 \). If \( \alpha_2 \) were not a multiple of \( \alpha_1 \), there would exist \( \lambda, \mu \in \mathbb{Z} \) such that \( \delta = \lambda \alpha_1 + \mu \alpha_2 \) satisfied \( 0 < \delta < \alpha_1 \), and since

\[
\langle \alpha_1 e_1 + \alpha_2 e_2, \lambda e_1^* + \mu e_2^* \rangle = \delta,
\]

this would contradict the definition of \( \alpha_1 \).

It is clear that the quotient \( \mathbb{Z} \)-module \( L/M \) is isomorphic to the direct sum of \( \mathbb{Z}^{n-r} \) and \( r \) cyclic groups \( \mathbb{Z}/\alpha_j \mathbb{Z} \) (\( 1 \leq j \leq r \)); the integers \( \lambda \) such that \( \lambda(L/M) \) is free are therefore exactly the multiples of \( \alpha_j \), and for these integers \( \lambda(L/M) \) is isomorphic to \( \mathbb{Z}^{n-r} \). This already shows (A.8.3) that the integers \( n \) and \( r \) are well determined, as is the submodule \( T \) of \( L/M \) consisting of the elements of finite order in this group. Observe next that if \( \mathbb{Z}/m \mathbb{Z} \) is a cyclic group and \( p \) a prime number, we have \( p^k(\mathbb{Z}/m \mathbb{Z}) = \mathbb{Z}/m \mathbb{Z} \) if \( p \) does not divide \( m \); whereas if \( m = p^k m' \), where \( p \) does not divide \( m' \), we have \( p^k(\mathbb{Z}/m \mathbb{Z}) = \mathbb{Z}/(p^{k-1}m') \mathbb{Z} \) if \( k < h \), and \( p^k(\mathbb{Z}/m \mathbb{Z}) = \mathbb{Z}/m' \mathbb{Z} \) if \( k \geq h \). If \( p_1, \ldots, p_h \) are the prime numbers dividing \( \alpha_j \), it follows that the orders of the groups \( p_j^k \mathbb{T} \) determine the exponents of the \( p_j \) in the \( \alpha_j \); the order of \( p_j^k \mathbb{T} \) is the product of the order of \( p_j^{k+1} \mathbb{T} \) by \( p_j^v \), where \( v \) is the number of \( \alpha_i \) divisible by \( p_j^{k+1} \). This shows that the \( \alpha_i \) are well determined.

The numbers \( \alpha_i \) are called the invariant factors of \( M \) with respect to \( L \).
We have also established:

(A.26.4) Every finitely generated \( \mathbb{Z} \)-module \( N \) is isomorphic to the product of a free \( \mathbb{Z} \)-module \( \mathbb{Z}^s \) and \( r \) cyclic groups \( \mathbb{Z}/\alpha_j \mathbb{Z} \) \((1 \leq j \leq r)\) such that \( \alpha_j \) divides \( \alpha_{j+1} \) for \( 1 \leq j \leq r - 1 \); and the numbers \( s, r, \) and \( \alpha_j \) \((1 \leq j \leq r)\) are uniquely determined by these properties.

(A.26.5) Keeping the notation of (A.26.3), suppose in addition that \( r = n \), so that \( L/M \) is a finite group. If we put \( f_j = \alpha_j e_j \), the \( f_j \) \((1 \leq j \leq n)\) form a basis of \( M \), and the matrix of the canonical injection \( u: M \to L \) relative to the bases \((f_j)\) and \((e_j)\) (A.5.2) is the diagonal matrix \( \text{diag}(\alpha_1, \ldots, \alpha_n) \). This is therefore also the matrix of the transpose \( 'u: L^* \to M^* \) relative to the dual bases \((f^*)\) and \((e^*)\) (A.9.4). Hence \( L^* \) may be canonically identified with the submodule of \( M^* \) having as basis the \( \alpha_j f_j^* \), and \( M^*/L^* \) is isomorphic to \( L/M \).

(A.26.6) In order that a submodule \( M \) of a finitely generated free \( \mathbb{Z} \)-module \( L \) should admit a supplement in \( L \), it is necessary and sufficient that the invariant factors of \( M \) with respect to \( L \) should all be equal to 1.

The condition is clearly sufficient by virtue of (A.26.3): the \( e_j \) such that \( r + 1 \leq j \leq n \) form a basis of a supplement of \( M \). Conversely, if \( M \) admits a supplement \( N \), then \( L/M \) is isomorphic to \( N \) and hence is a free \( \mathbb{Z} \)-module (A.26.2); this implies that all the cyclic modules \( \mathbb{Z}/\alpha_j \mathbb{Z} \) must be trivial, hence \( \alpha_j = 1 \) for \( 1 \leq j \leq r \).
REFERENCES

VOLUME I


237
REFERENCES

VOLUME II


VOLUME III


REFERENCES


VOLUME IV

REFERENCES

VOLUMES V AND VI

INDEX

In the following index the first reference number refers to the chapter and the second to the section within the chapter.

A
Abelian character: 21.3
Action of a set on a commutative group: A.22
Affine Weyl group: 21.15, prob. 11
Alcove: 21.15, prob. 11
Almost simple Lie group: 21.6
Anti-invariant element: 21.14

B
Basis of a reduced root system: 21.11
Borel subalgebra: 21.22, prob. 7
Borel subgroup: 21.22, prob. 7
Borel’s conjugacy theorem: 21.22, prob. 10
Bruhat decomposition: 21.22, prob. 13
Burnside’s theorem: 21.3, prob. 8
Chevalley’s theorem: 21.16, prob. 16
Class of a linear representation: 21.4
Classical groups: 21.12
Coefficients of a linear representation: 21.2, prob. 1, and 21.4, prob. 5
Completely reducible linear representation: 21.1
Complex special orthogonal group: 21.12
Complex symplectic group: 21.12
Complexification of a real Lie group: 21.17, prob. 1
Conjugacy of maximal tori: 21.7
Conjugation in a complex Lie algebra: 21.18
Continuous linear representation: 21.1
Coxeter element in a simple Lie algebra: 21.15, prob. 13
Coxeter element in a Weyl group: 21.11, prob. 14
Coxeter number: 21.11, prob. 14

D
Degree of a linear representation: 21.1
Diagonal of a simple Lie algebra: 21.11, prob. 8
Diagonalizable endomorphism: A.23
Diagonalizable Lie algebra: 21.22, prob. 8
Dimension of a linear representation: 21.1
Direct sum of linear representations: 21.1
Direct sum of $\Omega$-modules: A.23
Discrete decomposition of a linear representation: 21.4, prob. 4
Dominant weight: 21.15
Dual lattice: 21.7
Dual root system: 21.11
Engel's theorem: 21.22
Equivalent linear representations: 21.1
Extension of a continuous unitary representation: 21.1

Fundamental classes of linear representations of a semisimple group: 21.16
Fundamental weights: 21.16

Highest root: 21.15, prob. 10
Highest weight: 21.15
Hilbert sum of unitary representations: 21.1
Homomorphism of \( \Omega \)-modules: A.22

Intertwining operator: 21.1, prob. 6
Invariant factors of a submodule of a free \( \mathbb{Z} \)-module: A.26
Irreducible components of a linear representation: 21.4
Irreducible linear representation: 21.1
Irreducible reduced root system: 21.11, prob. 10
Isomorphism of \( \Omega \)-modules: A.22
Isotypic components of a linear representation: 21.4, prob. 4
Isotypic components of a semisimple module: A.23
Isotypic linear representation: 21.4, prob. 3
Isotypic semisimple \( \Omega \)-module: A.23
Iwasawa decomposition: 21.21
Iwasawa's theorem: 21.23, prob. 8

Killing form on a Lie algebra: 21.5
Kostant's formula: 21.15, prob. 15

Leading term: 21.14
Lepage decomposition: 21.16, prob. 3
Levi's theorem: 21.23
Lexicographic order: 21.20
Lie triple system: 21.18, prob. 3
Lie's theorem: 21.22, prob. 2
Linked roots: 21.11, prob. 13

Malcev's theorems: 21.23, pros. 4 and 13
Maximal torus: 21.7
Miniprincipal subgroup: 21.15, prob. 12
Multiplicity of a root: 21.21, prob. 2
Multiplicity of a weight in a character, or in a representation: 21.13
Multiplicity of an irreducible representation, or of a class of irreducible representations: 21.4 and 21.4, prob. 4

Negative roots with respect to a basis: 21.11
Nice subgroup: 21.11, prob. 7
Nilpotent component of an element of a splitable Lie algebra: 21.19, prob. 1
Nilpotent Lie algebra: 21.21
Nilpotent Lie group: 1.21
Nonreduced root system: 21.21, prob. 2
Normal real form of a complex semisimple Lie algebra: 21.18

Parabolic subalgebra: 21.22, prob. 12
Parabolic subgroup: 21.22, prob. 12
Peter–Weyl theorem: 21.2
Pivotal root: 21.11, prob. 16
Positive roots with respect to a basis: 21.11
Primary linear representation: 21.4, prob. 3
Primitive element in a \( U(sl(2, \mathbb{C})) \)-module: 21.9
Principal alcove: 21.15, prob. 11
Principal diagonal of a simple Lie algebra: 21.11, prob. 8
Principal nice subgroup: 21.11, prob. 8

Q

Quaternionic linear representation: 21.1, prob. 8

R

Radical of a connected Lie group: 21.23, prob. 9
Radical of a Lie algebra: 21.23
Rank of a compact Lie group: 21.7
Real linear representation: 21.1, prob. 7
Reduced root system: 21.11
Reductive Lie group: 21.23, prob. 10
Regular element in a compact connected Lie group: 21.7
Regular element in a Lie algebra: 21.7 and 21.22, prob. 4
Regular linear form on t: 21.14
Regular representation: 21.1
Representative function: 21.2, prob. 1
Ring of classes of continuous linear representations of a compact group: 21.4
Root decomposition of a semisimple Lie algebra: 21.20
Root system: 21.11
Roots of a compact Lie group, relative to a maximal torus: 21.8
Roots of a semisimple Lie group: 21.19

S

S-extremal set of weights: 21.15, prob. 3
S-saturated set of weights: 21.15, prob. 1
Schur's lemma: A.22; 21.1, probs. 5 and 6
Semisimple component of an element of a splittable Lie algebra: 21.19, prob. 1
Semisimple Lie algebra: 21.6
Semisimple Lie group: 21.6
Semisimple Ω-module: A.23
Simple Lie algebra: 21.6
Simple Ω-module: A.22

Singular element in a compact connected Lie group: 21.7
Singular element in a Lie algebra: 21.7 and 21.22, prob. 4
Singular linear form on t: 21.14
Special point: 21.10, prob. 2
Splittable Lie algebra: 21.22, prob. 8
Square-integrable linear representation: 21.4, prob. 5
Stable subgroup: A.22
Stable subspace: 21.1
Subrepresentation: 21.1
Symmetrized Lie algebra, symmetrization of a Lie algebra: 21.18, prob. 12

T

Tensor product of representations: 21.4
Topologically irreducible linear representation: 21.1
Torus: 21.7
Trivial character: 21.3
Trivial class (of representations): 21.4
Trivial linear representation: 21.1

U

Unitarian trick: 21.18
Unitary linear representation: 21.1

W

Weight contained in a character (or in a representation): 21.13
Weight lattice: 21.13
Weights of a torus: 21.7
Weyl basis of a semisimple Lie algebra: 21.10
Weyl chamber in it*: 21.14
Weyl chamber in it: 21.15, prob. 11
Weyl chamber of a symmetric space: 21.21, prob. 1
Weyl group of a compact Lie group: 21.7
Weyl group of a reduced root system: 21.10
Weyl group of a symmetric space: 21.21, prob. 1
Weyl's formulas: 21.15
Weyl's theorem on isomorphisms of semisimple Lie algebras: 21.20
Pure and Applied Mathematics
A Series of Monographs and Textbooks

Editors Samuel Eilenberg and Hyman Bass
Columbia University, New York

RECENT TITLES

E. R. KOLCHIN. Differential Algebra and Algebraic Groups
GERALD J. JANUSZ. Algebraic Number Fields
A. S. B. HOLLAND. Introduction to the Theory of Entire Functions
WAYNE ROBERTS AND DALE VARBERG. Convex Functions
A. M. OSTROWSKI. Solution of Equations in Euclidean and Banach Spaces, Third Edition
of Solution of Equations and Systems of Equations
H. M. EDWARDS. Riemann's Zeta Function
SAMUEL EILENBERG. Automata, Languages, and Machines: Volumes A and B
MORRIS HIRSCH AND STEPHEN SMALE. Differential Equations, Dynamical Systems, and
Linear Algebra
WILHELM MAGNUS. Noneuclidean Tessellations and Their Groups
FRANÇOIS TREVES. Basic Linear Partial Differential Equations
WILLIAM M. BOOTHBY. An Introduction to Differentiable Manifolds and Riemannian
Geometry
BRAYTON GRAY. Homotopy Theory: An Introduction to Algebraic Topology
ROBERT A. ADAMS. Sobolev Spaces
JOHN J. BENEDETTO. Spectral Synthesis
D. V. WIDDER. The Heat Equation
IRVING EZRA SEGAL. Mathematical Cosmology and Extragalactic Astronomy
J. DIEUDONNÉ. Treatise on Analysis: Volume II, enlarged and corrected printing;
Volume IV; Volume V.
WERNER GREUB, STEPHEN HALPERIN, AND RAY VANSTONE. Connections, Curvature, and
Cohomology: Volume III, Cohomology of Principal Bundles and Homogeneous Spaces
I. MARTIN ISAACS. Character Theory of Finite Groups
JAMES R. BROWN. Ergodic Theory and Topological Dynamics
C. TRUESDELL. A First Course in Rational Continuum Mechanics: Volume 1, General
Concepts
GEORGE GRATZER. Lattice Theory
K. D. STROYAN AND W. A. J. LUXEMBURG. Introduction to the Theory of Infinitesimals
B. M. PUTTASWAMAIAH AND JOHN D. DIXON. Modular Representations of Finite
Groups
MELVYN BERGER. Nonlinearity and Functional Analysis: Lectures on Nonlinear Problems
in Mathematical Analysis
JAN MIKUSINSKI. The Bochner Integral

In preparation

MICHEL HAZEWINKEL. Formal Groups and Applications