

CLASSICS OF SOVIET MATHEMATICS

L. S. PONTRYAGIN
SELECTED WORKS

IN FOUR VOLUMES

VOLUME TWO

Topological
Groups

Gordon and Breach Science Publishers

**L. S. PONTRYAGIN
SELECTED WORKS**

Volume 2
Topological Groups

Classics of Soviet Mathematics

L. S. PONTRYAGIN SELECTED WORKS

Edited by R. V. Gamkrelidze

Volume 1: **Selected Research Papers**

Volume 2: **Topological Groups**

Volume 3: **Algebraic and Differential Topology**

Volume 4: **The Mathematical Theory of Optimal Processes**

ISSN 0743-9199

This book is part of a series. The publishers will accept continuation orders which may be cancelled at any time and which provide for automatic billing and shipping of each title in the series upon publication. Please write for details.

L. S. PONTRYAGIN SELECTED WORKS

Volume 2

Topological Groups

by L. S. PONTRYAGIN
Third Edition

Translated from the Russian by Arlen Brown
with additional material translated by P. S. V. Naidu

Gordon and Breach Science Publishers
New York • London • Paris • Montreux • Tokyo

© 1986 by Gordon and Breach Science Publishers S.A., P.O. Box 161, 1820 Montreux 2,
Switzerland. All rights reserved.

Gordon and Breach Science Publishers

P.O. Box 786
Cooper Station
New York, NY 10276
United States of America

P.O. Box 197
London WC2E 9PX
England

58, rue Lhomond
75005 Paris
France

14-9 Okubo 3-chome
Shinjuku-ku, Tokyo 160
Japan

English language publication dates:
Second Edition Published 1966
Reprinted 1977
Third Edition 1986

Second English-language Edition © 1966 by Gordon and Breach, Science Publishers,
Inc. Sections reprinted with permission of the Publisher

Library of Congress Cataloging-in-Publication Data

Pontryagin, L. S. (Lev Semenovich), 1908–
Topological groups.

(L. S. Pontryagin selected works ; v. 2) (Classics
of Soviet mathematics, ISSN 0743-9199)

Translation of: Nepreryvnye gruppy.

Bibliography: p.

Includes index.

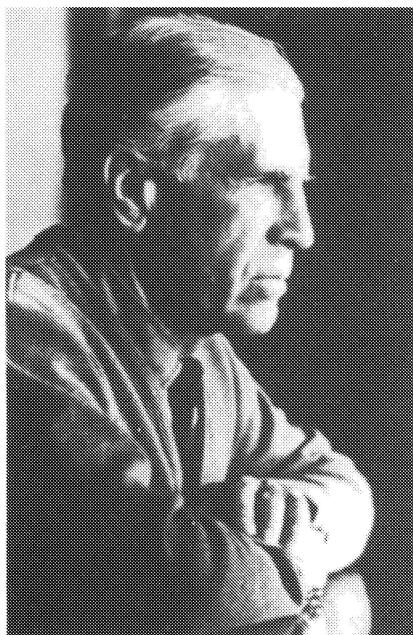
1. Topological groups. 2. Groups, Continuous.

I. Title. II. Series: Pontryagin, L. S. (Lev
Semenovich), 1908– . Selections. Polyglot.
1985 ; v. 2. III. Series: Classics of Soviet
mathematics.

QA3.P76 1985 vol. 2 [QA387] 510 s [512'.55] 86-4726

ISBN 2-88124-133-6 (Switzerland)

Volume 2: ISBN 2-88124-133-6; 4-volume set: ISBN 2-88124-134-4. No part of this
book may be reproduced or utilized in any form or by any means, electronic or mechani-
cal, including photocopying and recording, or by any information storage or retrieval
system, without permission in writing from the publishers. Printed in Great Britain by
Bell and Bain Ltd., Glasgow.



Lev Semenovich Pontryagin



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contents

Editor's Preface	ix
Translator's Preface to the Second Edition	xi
Foreword to the Third Edition	xxiii
Introduction	xxv
Notation	xxix
Chapter 1 Groups.....	1
Chapter 2 Topological Spaces.....	51
Chapter 3 Topological Groups.....	95
Chapter 4 Topological Division Rings	153
Chapter 5 Linear Representations of Compact Topological Groups.....	185
Chapter 6 Locally Compact Commutative Groups.....	235
Chapter 7 The Concept of a Lie Group	281
Chapter 8 The Structure of Compact Groups	323
Chapter 9 Locally Isomorphic Groups	345
Chapter 10 Lie Groups and Lie Algebras.....	377
Chapter 11 The Structure of Compact Lie Groups.....	445
References.....	521
Index	525



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Editor's Preface

On 3 September 1983 Lev Semenovich Pontryagin was seventy-five. To mark this important event in the life of this outstanding contemporary mathematician we are beginning the publication of his scientific works in four volumes, according to a decision taken by the Mathematics Division of the USSR Academy of Sciences. The first volume contains the most important mathematical papers of L. S. Pontryagin and also includes a bibliography of his basic scientific works, the second is his well-known monograph *Topological Groups*, the third comprises two monographs, *Foundations of Algebraic Topology* and *Smooth Manifolds and Their Applications in Homotopy Theory*, and the fourth is a revised edition of *The Mathematical Theory of Optimal Processes* by L. S. Pontryagin, V. G. Boltyanskii, R. V. Gamkrelidze, and E. F. Mishchenko.

The scientific activity of Lev Semenovich Pontryagin has left a deep imprint on many crucial areas of modern mathematics, both pure and applied. His work has had a definitive influence on the development of topology and topological algebra, and because of him optimal control theory is one of the topical trends in present-day applied mathematics. In a brief review we can neither delve deeply into his important works nor describe the profound, multifaceted impact of these works on the advancement of the respective fields. This is, therefore, only a broad outline that may be of help in studying his works.

While still a second-year student at Moscow State University, Pontryagin began his scientific activity under the guidance of P. S. Aleksandrov. In this early period, his interests concentrated mainly on two central topics of algebraic (combinatorial) topology, namely, topological duality theorems and dimension theory, which Pontryagin looked upon as a local variant of duality theory.

The discovery of "Pontryagin duality," the culmination of his work in topological duality theorems, and the construction of the general theory of characters of a locally compact commutative group are Pontryagin's two most notable contributions and are undoubtedly among the finest achievements in modern mathematics.

We begin with a survey of his main works in duality theory and topological algebra. To assess the full value of the advances made by Pontryagin in this area, it is apt to recall here that at the time when Pontryagin had just begun his activity, homology groups were hardly used in topology; instead, Betti numbers with respect to different moduli and torsion coefficients were used, and the Alexander duality theorem was formulated as an equality of Betti numbers (modulo 2) of dimensions $n - r - 1$ and r of a polyhedron

$K \subset R^n$ and its complement $R^n \setminus K$,

$$p^r(R^n \setminus K) = p^{n-r-1}(K).$$

In his first published paper,^{1*} Pontryagin improved this theorem by extending the duality between the Betti numbers of a polyhedron and its complement in R^n to the duality between the r - and $(n - r - 1)$ -dimensional homology groups (modulo 2) of the polyhedra $(R^n \setminus K)$ and K . The full statement of this theorem follows. In $R^n \setminus K$ and K , two bases

$$z_1^r, \dots, z_s^r \quad \text{and} \quad \zeta_1^{n-r-1}, \dots, \zeta_s^{n-r-1}$$

of homology (mod 2) of dimensions r and $(n - r - 1)$, respectively, can be chosen, such that the square matrix of linking coefficients (mod 2)

$$\| (z_i^r, \zeta_j^{n-r-1}) \| (i, j = 1, \dots, s)$$

is the identity matrix.

Thus, the duality between the homology groups (mod 2) established here by means of the linking coefficients led to a group isomorphism.

The next paper² deals with the same problem in modulus 2, but the polyhedron K is now imbedded in an arbitrary closed n -dimensional manifold M^n . Its solution demanded, probably for the first time in the history of topology, a study of homological properties of continuous mappings. That is, Pontryagin was led to the study of kernels and images of homomorphisms of homology groups (mod 2) for the inclusions $K \subset M^n$ and $M^n \setminus K \subset M^n$, and the duality theorem was formulated in terms of the ranks of the corresponding kernels. Later, the study of the homological properties of mappings acquired immense significance in topology and greatly influenced the creation of homological algebra.

This paper also contained a statement, known subsequently as the "Pontryagin cycle removal theorem," that asserted: If an r -dimensional cycle Z' in M' intersects every $(n - r)$ -dimensional cycle in K with a zero intersection index, then the cycle Z' can be "homologically removed" from K , i.e., there exists in $M^n \setminus K$ an r -dimensional cycle that is homologous to Z' in M^n . This theorem found successful applications in the topological theory of variational problems; Pontryagin himself used it in estimating the category of a manifold.

From the foregoing it is clear how far one of the central problems of algebraic topology of the late twenties had been advanced in two short papers of a 19-year old sophomore.

* Reference numbers refer to the bibliography of Pontryagin's publications, pp. 609–618.

The next work concerning duality theorems, his master's thesis,⁶ was stimulated by the course in algebra given by E. Noether. It gives a profound analysis of the algebraic nature of topological duality theorems. Duality for an arbitrary modulus $m > 0$ obtained a final solution in the form of an isomorphism of the corresponding groups, in view of the fact, now well understood, that a finite cyclic group is the Pontryagin dual of itself (a concept which Pontryagin had not yet arrived at that time).

A particular corollary of the results of the paper is that, for any $m > 0$, the homology groups (mod m), $H_r^{(m)}(R^n \setminus K)$ and $H_{n-r-1}^{(m)}(K)$ of dimensions r and $n - r - 1$, respectively, are isomorphic, and, consequently, all homology groups (mod m) of the complement $R^n \setminus K$ are invariant, i.e., they depend only on the homology groups of the polyhedron K , but do not depend on the inclusion of K in R^n .

Duality theorems for full homology groups with integral coefficients cannot be formulated in terms of isomorphisms and, therefore, could not be fitted into the framework of the paper. For instance, the full r -dimensional integral homology group $H_r(R^n \setminus K)$ is neither isomorphic to the group $H_{n-r-1}(K)$ nor even determined by it. There exist only isomorphisms (also noted in the paper) separately between the r - and $(n - r - 1)$ -dimensional weak homology groups and between the r - and $(n - r - 2)$ -dimensional torsion groups of the sets K and $R^n \setminus K$, obviously implying the invariance of the full integral homology groups of the complement $(R^n \setminus K)$.

If, instead of a finite polyhedron K , an arbitrary compact set F is considered in R^n , then the corresponding integral and weak homology groups are, in general, no longer finitely generated, and a special investigation is needed to establish the invariance of the homology groups of the complement $R^n \setminus F$. Pontryagin also studied the duality for an arbitrary compact set $F \subset R^n$ and established the invariance of the groups $H_r^{(m)}(R^n \setminus F)$, $m > 0$, as well as the invariance of weak homology groups of $R^n \setminus F$, thereby significantly advancing the problem.

But the central question of the independence of the full group of integral homology $H_r(R^n \setminus F)$ of the inclusion of the compact set $F \subset R^n$ still remained unsolved. Its solution demanded the introduction of a new homological invariant of the set F , namely, a homology group related not to a discrete but to a compact coefficient group. This permitted him, while rejecting the narrow concept of duality as an isomorphism, to define "Pontryagin duality." In 1931–32, he made this decisive step and completely solved all problems relating to duality and also the longstanding problem of the proper definition of homology groups of compact metric spaces.

In constructing the homology group $H_r(F)$ of the set F , the coefficients

are not taken from a discrete group of residues (modulo m) or from the group of integers, but are taken from a compact topological group of rotations of a circle. The group $H_r(F)$ is, in itself, a compact commutative topological group. The group $H_r(F)$ and the $(n - r - 1)$ -dimensional integral homology group $H_{n-r-1}(R^n \setminus F)$ proved to be Pontryagin duals, i.e., each is the character group of the other (for a detailed exposition of the theory of characters, see reference 110 or the second volume of the *Selected Works*).

Generally, let Γ, G be a dual group pair, i.e., each is the character group of the other, and let Γ be compact and G discrete. Take Γ as the coefficient group for constructing the homology group $H_r^\Gamma(F)$. Then its dual (i.e., its character group) is the homology group of the complement $H_{n-r-1}^G(R^n \setminus F)$, which is constructed, using G , the dual of Γ , as the coefficient group. Duality is realized through linking coefficients.

The general duality theorem for a closed set $F \subset R^n$ was first reported as a short communication in the Proceedings of the International Mathematics Congress held in Zurich in 1932, while its full exposition is given in reference 18.

This paper actually marks the end of Pontryagin's research into topological duality theorems. These theorems, being a powerful tool for studying general homological problems in topology, resolved the crucial question in algebraic topology of the thirties. Particularly after Pontryagin's duality theorems, homology groups have gained a firm foothold in topology as the basic homological invariants in place of the Betti numbers and torsion coefficients, which had fully served the purpose of homology groups until the main circle of topological problems led to finitely generated groups.

Topological duality theorems for a (finite) polyhedron in an arbitrary closed n -dimensional manifold are given in their final formulation in reference 54.

A logical continuation of the duality theorems is the general theory of characters of locally compact commutative groups created by Pontryagin. The main result of this theory is the assertion that every compact commutative group is the character group of some discrete group. Its proof rests on the construction of the invariant measure introduced by Haar in 1933, which had played a key role in the development of topological algebra.

The general theory of characters had enabled Pontryagin to elucidate the structure of compact and locally compact groups, the results obtained for compact and locally compact commutative groups being final. A positive answer to Hilbert's fifth problem for a compact and locally compact commutative group follows directly from these results. (For a detailed

exposition of the structure of compact and locally compact commutative groups, refer to the third edition of *Topological Groups*, Volume 2 of the *Selected Works*.) However, the significance of the theory of characters of locally compact topological groups does not end here. Its creation has indeed laid the foundation of topological algebra as an independent discipline, which has been primarily responsible for the development of general harmonic analysis on topological groups. Pontryagin's works in duality theory and character theory had a deep impact on algebraic-topological reasoning in the thirties and, in particular, made a great contribution to "functorial thinking" in mathematics.

His first publications on the general theory of characters of commutative topological groups, on the structure of compact groups, and on locally compact commutative groups are references 16, 17, and 19, respectively.

His remarkable theorem (see reference 10) that asserts that the field of real numbers, the field of complex numbers, and the division ring of quaternions are the only locally compact connected division rings should also be classified under topological algebra.

The methods developed here were later fully utilized by Pontryagin in elucidating the structure of locally compact commutative groups with the help of the theory of characters, as we have already pointed out.

The outcome of his studies in topological algebra was the famous monograph *Topological Groups*, first published in 1938, which has had several editions both in the USSR and in many other countries, in most of the major European languages. It became a classic that influenced many generations of mathematicians and that has not lost its value even today, forty-five years since its first publication, a rare event in mathematics. Its third English edition forms the second volume of the *Selected Works* of L. S. Pontryagin.

The early works of Pontryagin also deal with dimension theory. He constructed examples of compact metric spaces that have different dimensions in different moduli. He later used these examples (see reference 4) to construct the famous "dimensionally deficient" continua, which disproved the longstanding hypothesis that the dimension of compact sets is additive under topological multiplication. He found two two-dimensional compact sets whose product is of dimension three, instead of four. His theorem that any n -dimensional compact set is homeomorphically mapped into R^{2n+1} (see reference 7) also fits into the category of dimension theory.

The homological dimension theory due to P. S. Aleksandrov owes much to Pontryagin's work in dimension theory. For Pontryagin himself, his studies in dimension theory had a far-reaching consequence — under their influence he began, in the mid-thirties, a systematic investigation of homotopic problems in topology.

His studies in homotopic topology likewise reached their climax (at the beginning of the forties) in the discovery of methods that basically paved the way for a new field in modern mathematics, differential topology. Here we have in mind his discovery of characteristic classes and his contributions to the theory of fiber bundles.

Prior to taking up the “homotopic period,” mention should be made of his outstanding topological paper written in 1935,²¹ a full exposition of which is given in reference 21. It gives the solution to the Cartan problem of calculating the homology groups of compact group manifolds for the four main series of compact Lie groups. Historically, in this paper, the homological invariants were first found for a large and extremely important class of manifolds defined, not by triangulation, but by analytical (in this case, by algebraic) relations. To solve this problem, Pontryagin used, instead of Cartan’s method based on the algebra of exterior invariant forms on a group (R. Brauer applied this method later), Morse’s method of defining a smooth function on a manifold with isolated critical points and constructing trajectories orthogonal to level surfaces of the function. He refined this method further — the critical points were no longer “isolated,” but formed “critical manifolds.”

The methods developed in this paper were fruitfully used by H. Hopf and others to advance further the topology of group manifolds and homogeneous spaces, and later by Pontryagin himself to solve certain auxiliary problems in homotopy theory, and, in particular, to calculate the homology groups of Grassmann manifolds.

A direct consequence of this work is an elegant result obtained by Pontryagin many years later.³⁹ The point is that, for all compact simple Lie groups, the Betti numbers are equal to the corresponding Betti numbers of the direct products of spheres of different dimensions. The question therefore naturally arose: is a compact simple Lie group homeomorphic to the product of spheres of appropriate dimensions? Through the use of homotopic techniques, he found the answer to be negative. The special unitary group of third-order matrices has the same Betti numbers as the product of a 3-dimensional sphere and a 5-dimensional sphere, but the group itself is not homeomorphic to the product of the spheres: this was established through the use of the classification of the mappings of S^4 into S^3 .

We shall now outline the homotopic works of L. S. Pontryagin. The topical problem in homotopic topology in the early stages of its development centered around the homotopic classification of the mappings of a sphere into a sphere of lesser dimension. Pontryagin encountered this problem while making fruitless attempts at giving a local characterization

of the dimension of a compact set in R^n in terms of the homological characteristics of its complement.

In the beginning, he tried to solve the homotopic classification problem of the mappings of the sphere S^{n+k} into S^n using homological methods. But, shortly after learning about Hopf's work on the classes of mappings of S^3 onto S^2 , he came to fully appreciate the situation; that was the beginning of a fifteen-year period during which Pontryagin was completely engaged in homotopic topology.

First, he demonstrated that the Hopf invariant is unique and, consequently, that Hopf's construction gives all the classes of the mappings of S^3 into S^2 ; thus, he obtained the full classification of the mappings of S^3 into S^2 . Soon after, in 1936, he discovered an amazing result: the number of classes of mappings of S^{n+1} into S^n , for $n \geq 3$, is two (see reference 28). A mistake was made, however, in classifying the mappings of S^{n+2} into S^n , which led to an erroneous result. It was noticed and corrected by Pontryagin in 1950 (see reference 63). For these mappings, too, the number of classes was found to be two.

The initial proofs of these theorems were incredibly cumbersome. Only later, after the discovery of the method of framed manifolds (see below), could they be greatly simplified.

Then followed the solution to a series of problems in the homotopic classification of mappings of polyhedra into spheres and vice versa. Of these papers we mention here only two, reference 40 and 43. These papers introduced such basic concepts in homotopy theory as "obstructions" and "difference cochains" and a new cohomological operation – the Pontryagin square, the predecessor of Steenrod's cohomological operations.

But the major problem, the classification of the mappings of S^{n+k} into S^n for $k \geq 3$, still defied solution. This is exactly the problem that led Pontryagin to discover the so-called "framed manifold method," to define new invariants of smooth manifolds – characteristic classes known as "Pontryagin classes," and to create the theory of fiber bundles, i.e., to create a new and very important field in modern mathematics, differential topology.

Among the pioneers in this field, besides L. S. Pontryagin, we should name H. Hopf, E. Stiefel, H. Whitney, and C. S. Chern.

The framed manifold technique was designed to study the homotopic properties of mappings with the help of the information available about the differential-topological structure of a manifold. It was only fruitful in classifying the mappings of S^{n+k} into S^n for $k \leq 3$ (as had already been noted at the beginning of the fifties by Pontryagin for $k = 1, 2$, and by Rokhlin for $k = 3$), because, for $k > 3$, information was needed about smooth manifolds of dimensions > 3 , which could not be obtained by the

methods available in the early fifties. However, the framed manifold technique is equally effective for the opposite purpose, studying smooth manifolds when we have homotopic information at our disposal, which can be more successfully derived with the help of Leray's algebraic (spectral sequence) method. This reversal of the method, known as bordism theory, is due to R. Thom. Most of the far-reaching results in the modern theory of smooth manifolds have been obtained precisely through a combination of the Pontryagin–Thom differential-topological method and Leray's algebraic method.

Today, characteristic classes constitute the central topic not only in differential topology, but also in modern differential geometry as a whole; fiber bundle theory has long since become a common research tool in topology, geometry, and analysis.

The theory of characteristic classes and the closely related theory of singularities of vector fields are presented in three large papers.^{56,57,61} The results of these papers were reported in earlier preliminary works.^{45,48–50} Reference 49 also reports briefly on the theory of classifying spaces, which subsequently played an important role in the development of fiber bundle theory.

The framed manifold method and a full classification of the mappings of S^{n+k} into S^n for $k = 0, 1$, and 2 are presented in reference 69 (see also Volume 3 of the *Selected Works*), which was the original exposition in the literature of the fundamentals of differential topology.

The “topological period” in the activity of L. S. Pontryagin ends with reference 69; from the early fifties on, he switched over exclusively to applied fields. Up until this time he had turned his attention to applied and nontopological topics only occasionally, but with great success.

We begin the survey of his earlier nontopological works with the famous paper written in collaboration with A. A. Andronov,²⁹ in which the concept of the structural stability of a dynamical system in a plane was first introduced, using the term “rough system,” and the roughness condition was formulated.

In a broad context there are two motives behind the idea of roughness: physical and mathematical. The physical motive arose in connection with Andronov's investigations into auto-oscillations and consists of the following: if a dynamic system describing a physical phenomenon is known only approximately, then the qualitative portrait of the system's phase plane can reflect the phenomenon only if this portrait does not change under small perturbations of the dynamic system. The mathematical motive is related to the idea of “typicality,” or “general position,” which is not at all specific to differential equations and which is widely used in different fields of

mathematics, including some topological works of L. S. Pontryagin. For the “general position” case, the phase portrait should be expected to be simpler than in exceptional cases; thus, the “general position” case deserves the utmost attention.

In this paper, smooth flow (of class C^1) in a domain $O \subset R^2$ bounded by a smooth closed curve everywhere transversal to the trajectories is called rough, if, for any flow sufficiently C^1 -close to the initial flow, there exists a homeomorphism of the domain O onto itself, C^0 close to the identity, that sends the trajectories of one flow into the trajectories of another, preserving the direction of motion along these trajectories.

After giving this definition, the authors show that the rough systems on a plane are typical (they form an everywhere dense open set) and that their qualitative portrait is quite simple. Here the three ideas, “simplicity”, “roughness”, and “typicality”, merge together (the corresponding classes of the systems coincide). This merger is specific to the small dimension of the phase space and fails for higher dimensions. But these three ideas are themselves of great interest for higher-dimensional systems also, and the questions of the behavior of trajectories for the corresponding class of systems and of the mutual relations between these classes have dominated the study of dynamic systems through the past twenty or twenty-five years, and go back, in the final analysis, to reference 29.

Still earlier, reference 29 had influenced the development of the two-dimensional qualitative theory of differential equations. First, it outlines the role of “singular” (orbitally unstable) trajectories, subdividing the phase plane into “cells” filled with trajectories of identical behavior. Second, the solution of the problem concerning rough systems on a plane paved the way for studies of “typical” bifurcations of a parameter-dependent dynamic system in the two-dimensional case.

Of his early works on dynamic systems, mention should be made of one more paper,¹³ which gives simple conditions, conveniently applied, for the birth of a cycle from a closed trajectory of a plane nonlinear Hamiltonian system under small autonomous (nonconservative) perturbations.

Among the early nontopological works of Pontryagin, reference 47 also deserves special mention, and had a considerable impact on the development of functional analysis on spaces with an indefinite metric. It was written during World War II at Kazan in connection with a purely applied problem of stability in ballistics. Its main result is that any Hermitian operator in a Hilbert space with an indefinite metric of index k has a k -dimensional invariant subspace on which all eigenvalues of the operator have nonnegative imaginary parts, and the main (indefinite) form of the space is nonnegative.

One more work completed during wartime at Kazan concerns stability theory. It formulates the conditions that must be fulfilled for a quasipolynomial to have roots with negative real parts (see reference 42). These conditions were later extended to functions of the type f/g having no poles, where f is a quasi-polynomial and g a polynomial (see reference 66).

We shall now take up the period that dates approximately from the beginning of the fifties, when Pontryagin was basically devoting himself to problems in applied mathematics.

Here, too, he displays with great strength his exceptional talent to perceive amidst the primal chaos in each new problem the main path, which leads to the goal via the shortest route. He forges ahead on this pathway, overcoming technical difficulties that seem, at times, to be insurmountable.

To study new topics, Pontryagin founded a special seminar in oscillation and control theory in 1952 at the Steklov Mathematics Institute. He believed that, to gain success in any applied field of mathematics, one should not confine oneself to the existing mathematical models, but start the study with technical problems, not only to gain a deeper insight into the existing models, but also to formulate new mathematical problems that have a pure mathematical interest as well as a technical interest.

Soon, as a result of this seminar, two basic advances emerged: the theory of relaxation (discontinuous) oscillations and the optimal control theory, which later Pontryagin began to elaborate on with great success jointly with his younger collaborators V. G. Boltyanskii, R. V. Gamkrelidze, and E. F. Mishchenko.

Relaxation oscillations are encountered in physical, and, in particular, in radio engineering systems described by differential equations with a small parameter ϵ attached to higher derivatives. Mathematically, relaxation oscillations can be defined as the periodic solutions of differential equations (or a system of differential equations) with a small parameter attached to higher derivatives that contain “slow motion” sections traversed by a phase point in a finite time, as well as “junction points” where the “fast motion” sections start and which are traversed in infinitely small time as $\epsilon \rightarrow 0$. A classical example of these oscillations is the Van der Pohl equation. The study of the asymptotic behavior of these oscillations in relation to ϵ is a very difficult mathematical problem and was only partially solved in some simplest cases. Pontryagin’s studies have made much headway with this problem for general systems and are of fundamental value.

Of great help to Pontryagin in these investigations was his phenomenal ability to do long mental calculations and to memorize complicated expressions.

Pontryagin’s works on relaxation oscillations are listed in that part of the bibliography which comprises papers published in 1955–1963.

In the mid-fifties, he discovered the famous “Pontryagin maximum principle,” which, though universal, is easily formulated and is an effective tool in solving a broad range of optimization problems from purely applied questions in diverse engineering fields to complicated theoretical questions. The maximum principle includes the first-order theory of the classical calculus of variations, which had proved futile in tackling many new technical problems, the analysis of which has led to the discovery of the maximum principle.

The maximum principle is simple to formulate and we state it for the important time-optimal case.

A process is called controlled if it can be described by an n -dimensional vector differential equation

$$\dot{x} = f(x, u),$$

where $x \in R^n$ is the phase point and u is an r -dimensional vector control parameter that takes values from some given subset $U \subset R^r$, which is, as a rule, a closed domain. The problem then is to choose a control $u(t) \in U$, as a function of time t , such that the corresponding trajectory $x(t)$ of the equation

$$\dot{x} = f(x, u(t))$$

is shifted from a given point x_0 to some other given point x_1 in minimum time. This control and its corresponding trajectory are called optimal. Let us introduce the following scalar function

$$H(x, \psi, u) = \psi f(x, u),$$

where $\psi f(x, u)$ is the scalar product of an n -dimensional vector ψ and f , and write the canonical system of equations

$$\dot{x} = f = \frac{\partial H}{\partial \psi}, \quad \dot{\psi} = -\psi \frac{\partial f}{\partial x} = -\frac{\partial H}{\partial x}.$$

The Pontryagin maximum principle asserts that, for a control $u(t)$, $t_0 \leq t \leq t_1$, and the corresponding trajectory $x(t)$ to be optimal, it is necessary that there exist a nonzero variable vector $\psi(t)$ such that $u(t)$, $x(t)$, and $\psi(t)$ satisfy the above canonical system of equations and “Pontryagin’s maximum condition”:

$$H(x(t), \psi(t), u(t)) = \max_{u \in U} H(x(t), \psi(t), u), \quad \forall t \in [t_0, t_1].$$

The discovery of the maximum principle proved a startling event that soon gave birth to a new advance, the optimal control theory, which, at

present, is a vital and flourishing area in applied mathematics – and the stream of papers brought forth by this theory is truly immense.

Among the works of Pontryagin that have greatly influenced the development of optimal control theory, we may mention his Plenary Address to the International Congress of Mathematicians held in Edinburgh in 1958⁸⁹ and his monograph “The Mathematical Theory of Optimal Processes” written jointly with V. G. Boltyanskii, R. V. Gamkrelidze, and E. F. Mishchenko (see Volume 4 of the *Selected Works*).

A natural development of optimal control theory proposed by Pontryagin himself is differential game theory, which he is presently pursuing. A review of this theory is outlined in his Plenary Address to the International Congress of Mathematicians held at Nice in 1970.¹²⁶ A full exposition of his theory of linear differential games is given in references 127 and 143, which are also included in this volume.

Since 1934, L. S. Pontryagin has been working at the Steklov Mathematics Institute of the USSR Academy of Sciences; he was made a full-time member of the Institute and given the position of Head of the Topology Division in 1939. From 1961 to the present, he has held the position of Head of the Division of the Theory of Ordinary Differential Equations and Control Theory. At the same time, he has always attached great importance to the teaching of mathematics and has devoted much time to giving lectures at Moscow State University. Being an excellent teacher, he always prepared his lectures with utmost care, even designing notation to the minutest detail. Four of his books, *Topological Groups* (Volume 2 of the *Selected Works*), *Combinatorial Topology, Algebraic and Differential Topology* (Volume 3 of the *Selected Works*), and *Ordinary Differential Equations* (English edition¹⁰⁰), which have been translated into many languages, were based on his lecture courses at Moscow State University; they have greatly influenced the education of many generations of mathematicians all over the world.

R. V. GAMKRELIDZE

Translator's Preface to the Second Edition

This is not a verbatim translation. While remaining faithful, I hope, to the author's characteristic style, I have made a considerable number of small changes in the text, in the interests of both euphony and clarity. In one or two cases in longer proofs I have even rearranged the order of whole paragraphs.

Changes have also been made in terminology, in order to bring it into keeping with current American usage and also to avoid burdensome repetition. The most notable of these changes is the use of "compact" in place of "bicomplete" (and of "countably compact" in place of "compact"). Likewise, "separable" has replaced "possessing a countable base of open sets", "full linear group" has replaced "group of all matrices with determinant different from zero" and, in the discussion of the structure of discrete Abelian groups the terms "torsion" and "torsion-free" have been used where they are appropriate.

Changes in the substance of the text, in the skeletal structure of definitions and proofs, have been made only where they proved necessary. Thus, the assumption that the underlying space be Hausdorff was interpolated in the definition of a manifold (Sec. 45, A) since, as is well known, this restriction is needed to exclude undesirable pathology. The same hypothesis has also been added in the formulations of Theorems 20 and 66, in the former theorem for the very good reason that the theorem is false without it, and in the latter theorem because its proof depends on Theorem 20.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Foreword to the Third Edition

From a purely logical point of view, a continuous or topological group is nothing but a union of two basic mathematical structures: a group and a topological space; that is the elements of a set form a group as well as a topological space. Clearly there would be no meaning in such a union were the algebraic and topological operations on the set not interconnected. This connection does exist and consists in the fact that the group operations of multiplication and inversion are continuous in the sense of the given topology. The concept thus developed is exactly the topological group. A topological ring or a topological field can be defined similarly. For example:

- (1) A finite dimensional vector space under group addition is a topological group,
- (2) The totality of square matrices of a given order with real elements under usual matrix addition and multiplication is a topological ring,
- (3) The totality of square matrices of a given order with real elements and nonzero determinants under usual matrix multiplication is a topological group, and
- (4) Real numbers, complex numbers and quaternions each form a topological division ring.

That algebraic topological structures of this kind are often encountered in mathematics is by itself not a sufficiently convincing ground for their investigation. But, by imposing upon an algebraic topological object certain quite general constraints (axioms), we come to very definite mathematical concepts. For instance, a continuous algebraic division ring, if connected and locally bicompact, is isomorphic either to the real number field, to the complex number field, or to the quaternion division ring (a result I discovered in the early thirties [42]). Later I found [45] that there exists between commutative bicompact topological groups and discrete commutative groups a natural one-to-one correspondence through the character group. Results of this kind enriched the topological group theory and attracted the general attention.

Working from my lecture notes, I published the first edition of *Topological Groups* in 1938; the second, revised and enlarged, edition came out in 1954.

The third edition does not differ much from the second — a slight inaccuracy in Chapter VII of the second edition has been corrected and some minor changes have been made in Chapter X.

I should draw the reader's attention to the fact that at two instances I use somewhat outdated terminology.

(1) Lately the term compactness has superseded the term bicompactness, as the former is no longer used in its original meaning; yet I retain the latter.

(2) Sometimes the algebraic properties of a topological group have to be studied without regard to the topological structure. A topological group in this context I call an algebraic group, though the latter term has nowadays an entirely different meaning that is not used in this book.

L. S. PONTRYAGIN

INTRODUCTION

The concept of a continuous, or topological, group arose originally in connection with the study of continuous transformation groups. These groups of continuous transformations—for example, geometric motions—presented themselves in a natural way as topological manifolds, and in the course of time it became clear that for the purposes of treating most problems it was unnecessary to regard the group as a group of transformations but sufficed to study it in its own right, recalling, however, that there was defined in it a notion of passage to a limit. Thus there arose a new mathematical concept: the topological group.

From the purely logical point of view a topological group is nothing but the union of two basic mathematical structures: a group and a topological space. For this reason the axiomatic definition of a topological group is very natural. In studying groups we study the algebraic operation of multiplication in its purest form. In exactly the same fashion, in studying topological spaces we study in pure form the operation of passage to a limit. Since both operations are among the most basic in all mathematics they are often encountered together, and the topological group is just the mathematical structure in which they are united and interrelated. From the constructive point of view the definition of a topological group presents little of interest, consisting, as it does, mainly of a repetition of the definition of an abstract group. The same may be said of the first few steps in the theory of topological groups; they possess little of a specific character. Nevertheless, the presence in one and the same set of interrelated algebraic and topological operations leads to a comparatively large measure of concreteness. This shows up particularly clearly in the case of continuous division rings, which receive a detailed study in the

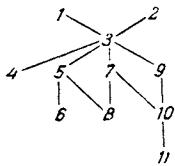
fourth chapter. The third chapter is devoted primarily to the study of axiomatics of topological groups and the verification of their simplest properties. In the first two chapters are collected those parts of the theory of groups and general topology needed in subsequent chapters.

Once the axiomatics are out of the way and the basic general theory of topological groups has been established, a more interesting task presents itself: to make a constructive investigation of the new abstract concept, i.e., to relate it to older more concrete concepts. The fruits of this investigation are twofold: on the one hand, the older concrete concepts are illuminated from the new point of view; on the other hand, the new abstract concept becomes more concrete. The detailed analysis of continuous division rings carried out in the fourth chapter without the application of any special apparatus cannot be duplicated for topological groups with such simple means. The basic apparatus in the investigation of topological groups is the theory of linear representations presented in the fifth chapter. With the aid of this tool it is possible to make a detailed study of the structure of commutative groups (Chapter VI) and also of compact groups (Chapter VIII).

Among the concrete structures in the theory of topological groups a prominent role is played by the Lie group. Indeed, it was the guise of Lie groups that topological groups originally made their appearance. As is customary in comparatively old theories, a number of fundamental problems are left unsettled in the classical theory of Lie groups. It is to the solution of these fundamental problems that the seventh chapter is devoted. At the same time this prepares the way for Chapter VIII, since the study of compact groups is based on relating them to Lie groups. A more detailed study of Lie groups is made in Chapters X and XI where the basic theory is developed and the classification of compact Lie groups is undertaken. The ninth chapter is concerned with the study of the universal covering of a group, a construct establishing the link between the local and global properties of topological groups.

Almost every paragraph of the book concludes with a sequence of examples, the character of which is extremely varied. On the one hand, almost trivial illustrations of the theoretical material are found here; on the other hand, brief discussions of the proofs of theorems possessing great independent significance are frequently given.

It is not necessary to read the book in order. A scheme showing the dependence of the various chapters is indicated as follows:



The book does not demand of the reader a broad mathematical knowledge, but does require a significant mathematical maturity. All that is basically required is a knowledge of the most elementary mathematical material, such as analytic geometry, the theory of matrices, the theory of ordinary differential equations, etc.

References to the bibliography are indicated by numbers in square brackets.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

NOTATION

The concept of set is fundamental to the exposition of the entire book and is assumed known (see [13]). I introduce here some notation relevant to sets and to elementary operations upon sets.

A. The notation $a \in M$ means that the element a belongs to the set M . Sometimes we will indicate a set M by simply enumerating the elements belonging to it: $M = \{a_1, \dots, a_n, \dots\}$. It is then to be understood that the set M consists of the elements a_1, \dots, a_n, \dots .

B. The notation $M = N$ means that the sets M and N coincide.

C. The notation $M \subset N$ or $N \supset M$ means that every element of M belongs to N , i.e., that the set M constitutes a part of the set N . The possibility of the two sets coinciding is not excluded.

D. By $M \cap N$ is denoted the intersection of the sets M and N , i.e., the set consisting of those elements belonging to both of the sets M, N .

E. By $M \cup N$ is denoted the union of the sets M and N , i.e., the set consisting of those elements belonging to at least one of the sets M, N .

F. By $M \setminus N$ is denoted the difference between the two sets M and N , i.e., the set consisting of those elements belonging to M but not belonging to N . Observe that this operation is considered as well defined independently of whether or not N is a subset of M . If $M \subset N$ the result of subtraction is the empty set, i.e., the set possessing no elements.

G. Let M and N be two sets. Suppose that to each element $x \in M$ there corresponds a single definite element $y = f(x)$ of the set N . Then we shall say that there is given a mapping f of the set M into the set N . The element y is called the image of the

element x under the mapping f and the element x the inverse image or one of the inverse images of the element y . We shall say that f is a mapping of M onto N if every element b of the set N possesses at least one inverse image under the mapping f , i.e., there is some $a \in M$ such that $b = f(a)$.

If A is a subset of the set M , $A \subset M$, then by $f(A)$ we shall denote the set consisting of all those elements of N which are images of elements belonging to A ; the set $f(A)$ is the image A under the mapping f . If $B \subset N$ then by $f^{-1}(B)$ we shall denote the set of all those elements of M whose images under the mapping f belong to B ; the set $f^{-1}(B)$ is the inverse image of B under the mapping f .

A mapping f of a set M onto a set N is said to be one-to-one if every element of N possesses exactly one inverse image under the mapping f . If f is a one-to-one mapping then the equation $y = f(x)$ can be solved for x , i.e., for given $y \in N$ the equation is satisfied by one and only one $x \in M$. We shall denote this solution by $x = f^{-1}(y)$; the mapping f^{-1} is called the mapping inverse to f , or, more briefly, the inverse of f .

1

GROUPS

The theory of groups studies an algebraic operation in its purest form: the elements constituting the group are considered only from the point of view of the operation defined in the group, all other possible properties of the elements being ignored. The present chapter is devoted to the exposition of the fundamental concepts of group theory.

SECTION 1 THE CONCEPT OF A GROUP

Definition 1. A set G is called a group if there is defined in G an operation associating with each pair of elements a, b in G a definite element c in G in such a way that conditions 1), 2), 3), formulated below and known as the group axioms, are satisfied. The operation itself is usually referred to as multiplication and its result is indicated by ab , $c = ab$. (The product ab may depend upon the order of the factors a and b : generally speaking, ab is not equal to ba .)

- 1) Associativity: for each triple of elements a, b, c in G the relation $(ab)c = a(bc)$ is satisfied.
- 2) G possesses a left identity, i. e., an element e such that $ea = a$ for every element a in G .
- 3) Every element a in G possesses a left inverse, i. e., an element a^{-1} such that $a^{-1}a = e$.

The set G may be either finite or infinite. If G is finite then the group is said to be finite and the number of elements in the group is its order; otherwise the group is said to be infinite.

If, in addition to the three axioms listed above, the group also satisfies the commutative law, i. e., if for every pair of elements a and b in G the equation

$$ab = ba \quad (1)$$

is satisfied, then the group is said to be commutative or abelian. For commutative groups it is frequently convenient to employ additive rather than multiplicative notation, i. e., to write the sum $a + b$ rather than ab to indicate the result of applying the group operation to the pair of elements a, b . In this case the group operation is referred to as addition rather than as multiplication, the identity element e of the group is called its zero and is denoted by 0 , while the element a^{-1} inverse to a is called the negative of a and is denoted by $-a$.

A) According to axiom 1) $(ab)c = a(bc)$; thus we may and shall indicate this element simply by abc . In exactly the same way, when four elements are multiplied, as for instance $((ab)c)d$, the product, as is easily seen, does not depend upon the grouping of the factors indicated by the parentheses and may be written simply $abcd$. The same principle applies to the product of any number of factors.

B) A left identity e of a group is also a right identity, i. e., $ae = a$ for every element a . A left inverse a^{-1} of an element a is also a right inverse, i. e., $aa^{-1} = e$. The element a^{-1} has a for its inverse, $(a^{-1})^{-1} = a$.

Indeed it follows from axioms 2) and 3) that $a^{-1}aa^{-1} = a^{-1}$; multiplying both sides of this equation on the left by a left inverse of a^{-1} we obtain $aa^{-1} = e$, so that the left inverse element is simultaneously a right inverse; moreover a is inverse to a^{-1} . Finally we have $ae = aa^{-1} a = ea = a$ which shows that the left identity e is simultaneously a right identity.

C) In a group G each of the equations

$$ax = b \quad (2)$$

and

$$ya = b \quad (3)$$

possesses one and only one solution x, y , respectively. From this follows in particular the uniqueness of the identity and the uniqueness of the inverse element, for e is the solution of the equation $xa = a$ while a^{-1} is the solution of the equation $xa = e$.

In order to prove the solvability of (2) and (3) it is sufficient to observe that $a^{-1}b$ is a solution of (2) while ba^{-1} is a solution of (3). Moreover it is obvious that these solutions are the only ones for, multiplying (2) on the left by a^{-1} , we obtain $x = a^{-1}b$ while multiplying (3) on the right by a^{-1} yields $y = ba^{-1}$.

D) In view of the uniqueness of the identity and of inverse elements it is natural to introduce the exponential notation of ele-

mentary algebra. If m is a natural number then a^m is defined inductively by $a^{m+1} = a^m a$ and $a^1 = a$, negative exponents are introduced by the equation $a^{-m} = (a^{-1})^m$ and the 0-th power a^0 is defined $a^0 = e$. If p and q are integers it is not difficult to show that the usual rules hold: $a^p a^q = a^{p+q}$, $(a^p)^q = a^{pq}$. If the additive notation is used we write na instead of a^n .

E) If for an element a of a group there exists a natural number m such that $a^m = e$ we shall say that a possesses finite order; otherwise we shall say that a possesses infinite order or that a is free. If a possesses finite order then the order of a is the smallest positive integer r for which $a^r = e$. If a is an element of order r and if $a^n = e$ where n is an arbitrary whole number then n is divisible by r .

In order to prove the last assertion divide n by r , i.e., write n in the form $n = pr + q$ with

$$0 \leq q < r. \quad (4)$$

Then

$$e = a^n = a^{pr+q} = (a^r)^p a^q = a^q.$$

Thus $a^q = e$ and according to the definition of the order r it follows that $q = 0$, i.e., that n is divisible by r .

A very important example of a group is the group of transformations of a set. Indeed groups first made their appearance in the mathematics in the form of groups of transformations and only later as a result of abstraction did they come to be considered independently of transformations.

F) A one-to-one mapping of an arbitrary set Γ onto itself is called a transformation of Γ . If x and y are two transformations of Γ then their product $z = xy$ is defined by the relation $z(\xi) = x(y(\xi))$ for arbitrary $\xi \in \Gamma$. It is easy to see that the mapping z thus defined is again a transformation of Γ . The role of the identity for this multiplication is played by the identity mapping e defined by the equation $e(\xi) = \xi$ for arbitrary $\xi \in \Gamma$. Clearly, for any transformation x , $ex = xe = x$. Moreover the transformation x^{-1} inverse to x was defined above to carry each element $x(\xi)$ of the set Γ into its inverse image ξ so that $x^{-1}x = e$ and x^{-1} acts as a left inverse to x . Shortly it will be shown that associativity holds for the operation of composition of transformations just defined. Thus every non-empty set G of transformations of Γ which contains along with each pair of transformations their product and along with each transformation its inverse is a group under the operation of composition of transformations. Any such group is called a transformation group acting on the set Γ . A transformation group G acting on Γ is said to be transitive if for each pair of elements

ξ, η of Γ there exists a transformation $x \in G$ such that $x(\xi) = \eta$. In particular the group of all transformations of Γ is transitive; a transformation x carrying ξ to η may be defined by the relation

$$x(\xi) = \eta, \quad x(\eta) = \xi, \quad x(\zeta) = \zeta \text{ for } \zeta \neq \xi, \zeta \neq \eta.$$

In order to prove the associativity of the multiplication of transformations let x, y and z be three transformations of Γ and let $\xi \in \Gamma$. Then:

$$(xy)z(\xi) = (xy)(z(\xi)) = x(y(z(\xi))),$$

$$x(yz)(\xi) = x(yx(\xi)) = x(y(z(\xi))),$$

so that $(xy)z = x(yz)$.

Example 1. Let G_n denote the group of all transformations of a finite set Γ_n containing exactly n elements, e.g., the set $\{1, 2, \dots, n\}$. Each transformation of Γ_n is called a permutation and the group G_n is known as the full group of permutations of Γ_n . Every permutation, as is well known, may be factored uniquely (except for order) into a product of cyclic permutations. The cyclic permutation (i_1, i_2, \dots, i_k) carries the number i_1 into the number i_2 , the number i_2 into the number i_3 , and so forth and, finally, the number i_k into the number i_1 . The group G_n of transformations of Γ_n contains $n!$ elements. Let us list, for example, the elements of the group G_3 . Here the elements are $a = (1, 2)(3)$; $b = (1, 3)(2)$; $ab = (1, 3, 2)$; $ba = (1, 2, 3)$; $aba = (1)(2, 3)$; $e = (1)(2)(3) = a^0$. Thus every element of G_3 may be expressed in terms of two of its elements a and b . These last serve as an example of a set of generators of G_3 . The elements $(1, 2)(3)$, $(1, 3)(2)$, and $(1)(2, 3)$ have order 2 while $(1, 2, 3)$ and $(1, 3, 2)$ have order 3. The group G_3 is non-commutative since $ab \neq ba$.

Example 2. Let $r = ||r_{ij}||$ and $s = ||s_{kj}||$, $i = 1, \dots, a$; $j = 1, \dots, b$; $k = 1, \dots, c$ be two matrices with complex entries and such that, as the notation indicates, the number of columns of r is equal to the number of rows of s . In this case we define the product rs of the matrices r and s to be the matrix $t = ||t_{ki}||$ where

$$t_{ki} = \sum_{j=1}^b r_{ij}s_{kj}, \quad i = 1, \dots, a; \quad k = 1, \dots, c.$$

If r and s are square matrices of order n , i.e., if $a = b = c = n$ then rs is also a square matrix of order n . A square matrix is said to be singular or non-singular according as its determinant is

equal to zero or different from zero. We shall show that the set G of all non-singular square matrices of order n forms a group with respect to the operation of matrix multiplication.

The associativity of the multiplication is easily seen to be an immediate consequence of the definition of product. The identity element is the unit matrix $e = \|\delta_{ij}\|$ where $\delta_{ii} = 1$ and $\delta_{ij} = 0$ if $i \neq j$. Finally, in order to find a matrix $r = \|r_{ij}\|$ inverse to a given matrix $s = \|s_{ij}\|$ it suffices to solve the system of equations

$$\sum_{j=1}^n r_{ji} s_{kj} = \delta_{ki}$$

with respect to the unknowns r_{ji} , which is always possible since, for fixed i , this is nothing but a system of n equations in n unknowns, the determinant $|s_{kj}|$ of which is, by assumption, different from zero.

It is easy to see that the subset G' of G consisting of the matrices with real entries is also a group.

SECTION 2

SUBGROUP. NORMAL SUBGROUP. FACTOR GROUP.

In the sequel we shall frequently have occasion to consider various subsets of a group, and to perform certain operations upon them. We here introduce some fundamental notation to facilitate such operations.

A) If A and B are subsets of a group G then by AB we denote the set consisting of all those elements of the form xy where $x \in A$, $y \in B$, while by A^{-1} we denote the set consisting of all those elements of the form x^{-1} where $x \in A$. If m is a natural number we define A^m inductively by $A^1 = A$ and $A^{m+1} = A^m A$, and also A^{-m} by $A^{-m} = (A^{-1})^m$. Finally, A^0 is defined by $A^0 = \{e\}$. According to these notational agreements it is clear what meaning to assign to the product of an arbitrary number of subsets raised to arbitrary integral powers. In the sequel we shall not always distinguish between a subset consisting of a single element and that element itself; thus we regard as meaningful such a formal product as Ab where $A \subset G$, $b \in G$. Note that, unless A is empty,

$$AG = GA = G \quad (1)$$

$$G^{-1} = G \quad (2)$$

$$Ae = eA = A. \quad (3)$$

When the additive notation is used, instead of AB we write $A + B$ and instead of A^n we write nA .

Starting from a given group G we may construct new groups. The simplest method of construction is indicated in the following definition.

Definition 2: A subset H of a group G is said to be a subgroup of G if H is itself a group with respect to the operation of composition defined in G .

B) In order that a subset H of a group G should be a subgroup it is necessary and sufficient that either of the two following equivalent conditions should be satisfied:

(a) Along with each pair of elements a and b in H the product ab^{-1} belongs to H . Employing the notation introduced in A) this condition may be written

$$HH^{-1} \subset H. \quad (4)$$

(b) Along with each pair of elements a and b in H the product ab and the inverse b^{-1} belong to H . Employing the notation introduced in A) these conditions may be written

$$H^2 \subset H \quad (5)$$

and

$$H^{-1} \subset H. \quad (6)$$

The necessity of the given conditions is obvious; it remains only to prove their sufficiency. If $a \in H$ then by virtue of (a) we have $aa^{-1} = e \in H$. Then, since $e \in H$ and $a \in H$, using condition (a) again, we have $ea^{-1} = a^{-1} \in H$. Next, if a and b are two elements of H then, as we have just seen, $b^{-1} \in H$ and consequently according to (a) we have $ab = a(b^{-1})^{-1} \in H$. Thus, when (a) is satisfied, the set H is in fact a subgroup. The sufficiency of condition (b) may be shown in a completely analogous fashion.

Among the subgroups of any group are those consisting of all integral powers of an arbitrary one of its elements. A group consisting exclusively of the powers of some one of its elements is said to be cyclic. An infinite cyclic group is said to be free: all of its elements (with the natural exclusion of the identity) are free. (See Section I, E.).

In the construction of new concepts in contemporary mathematics a prominent role is played by the notion of an equivalence relation which we now formulate.

C) An equivalence relation is said to be defined in a set M when it is possible to say of any two elements a and b of M that

they are equivalent or not, in symbols $a \sim b$ or $a \not\sim b$, where the following conditions are satisfied:

- (a) Reflexivity: $a \sim a$
- (b) Symmetry: if $a \sim b$ then $b \sim a$
- (c) Transitivity: if $a \sim b$ and $b \sim c$ then $a \sim c$

Whenever an equivalence relation is defined in a set M , then M is automatically partitioned into disjoint classes of mutually equivalent elements.

We now apply the general concept of an equivalence relation to groups.

D) Let H be a subgroup of a group G . If a and b are two elements of G then we define $a \sim b$ to mean that $ab^{-1} \in H$. It turns out that the relation thus defined in G does in fact satisfy the conditions stated above in C) and accordingly that G is partitioned into classes of mutually equivalent elements. Each of the equivalence classes thus obtained is called a right coset of the subgroup H . If A is any right coset of H and if $a \in A$ then $A = Ha$; moreover every subset of the form Hb is in fact a right coset. Since $H = He$, the subgroup H itself is one of its own right cosets. From what has just been said and from the unicity of the solution of the equation $c = xa$ (see Section I, C)) it follows that the cardinal number of each right coset is equal to the cardinal number of H . In particular, if G is a finite group of order g and the subgroup H has order h then g is divisible by h and g/h , known as the index of the subgroup H in the group G , is the number of right cosets.

Let us prove first of all that the relation just introduced is an equivalence relation. Indeed, $a \sim a$ since $aa^{-1} = e \in H$. Also if $a \sim b$, i.e., if $ab^{-1} \in H$ then also $(ab^{-1})^{-1} = ba^{-1} \in H$ so that $b \sim a$.

Finally if $a \sim b$ and $b \sim c$, i.e., if $ab^{-1} \in H$ and $bc^{-1} \in H$ then also $ac^{-1} = ab^{-1} bc^{-1} \in H$ so that $a \sim c$. Thus the three conditions of (C) are satisfied.

Let now A be a right coset of H and let $a \in H$. If $x \in A$ then $xa^{-1} \in H$ and accordingly $x \in Ha$. Also if $y \in Ha$ then $ya^{-1} \in H$ and accordingly $y \in A$. Thus $A = Ha$.

Finally we show that an arbitrary subset of the form Hb is a right coset. Indeed the element b belongs to some right coset, say B ; but then $B = Hb$ as has just been shown. Thus D) is demonstrated.

E) It is possible to introduce a different but fully analogous equivalence relation by defining $a \sim b$ to mean $a^{-1}b \in H$. Once again the defining conditions of C) are satisfied. The equivalence classes obtained from this equivalence relation are called left cosets of H . Exactly as before it turns out that each left coset

has the form aH and conversely that every subset of the form bH is a left coset.

We now ask under what conditions on the subgroup H the two partitions of G into left and right cosets, respectively, coincide. If A is simultaneously a right and a left coset of the subgroup H then $A = Ha = aH$ where a is an arbitrary element of A . If every right coset is simultaneously a left coset then we must have $Ha = aH$ for every $a \in G$. Multiplying the last relation on the left by a^{-1} we obtain $a^{-1}Ha = H$. We are thus led to the following definition.

Definition 3: A subgroup N of a group G is an invariant or normal subgroup of G if for every $n \in N$ and every $a \in G$ we have $a^{-1}na \in N$ or, what comes to the same thing, if $a^{-1}Na \subset N$ for every $a \in G$.

If N is a normal subgroup, i.e., if $a^{-1}Na \subset N$ for every $a \in G$, then in fact $a^{-1}Na = N$ for every $a \in G$. Indeed let $a = b^{-1}$; then $bNb^{-1} \subset N$, and, multiplying this relation on the left by b^{-1} and on the right of b , we obtain $N \subset b^{-1}Nb$. But b is an arbitrary element of G ; thus $b^{-1}Nb = N$ for arbitrary $b \in G$. The last equation may also be expressed in the form

$$Nb = bN. \quad (7)$$

F) In order that the partition of the group G into the left and right cosets of the subgroup N should coincide it is necessary and sufficient that N should be an invariant subgroup.

The necessity of the condition has already been shown. In order to show the sufficiency, let A be a right coset of the subgroup N . Then $A = Na$; but $Na = aN$ and accordingly A is also a left coset.

We now set forth a second method of constructing new groups starting from a given group G .

Definition 4: Let N be a normal subgroup of the group G and let A and B be cosets of N , $A = Na$, $B = Nb$. For the product AB we have $AB = NaNb = NNab = Nab$ so that AB is again a coset of N . Thus there is defined in a natural way in the set of cosets an operation of multiplication which, as we show immediately, satisfies the group axioms. The group of cosets thus obtained is called the factor group of the group G by the normal subgroup N and is denoted by G/N .

We must show that axioms 1), 2), and 3) of Definition 1 are satisfied by G/N . Now, associativity is obvious since it holds in G .

Also the identity of G/N is just N . Indeed if Na is an arbitrary coset then $N(Na) = Na$. Finally, the inverse of aN is Na^{-1} since $(Na^{-1})(aN) = N$.

G) Every group G possesses at least two normal subgroups, to wit, the subgroup $\{e\}$ consisting of the identity element e alone, and the subgroup G . If G possesses no normal subgroups other than these two trivial ones, then G is said to be a simple group.

Example 3: Let $s = \|s_{ij}\|$ be an arbitrary matrix. The transpose matrix $s^* = \|t_{ji}\|$ is defined by $t_{ji} = s_{ij}$. It is easy to see that for an arbitrary pair of matrices r and s for which the product rs is defined (see Ex. 2) we have $(rs)^* = s^*r^*$. A square matrix s with real entries is said to be orthogonal if $s^*s = e$. We show that the set H of all orthogonal matrices of order n is a subgroup of the group G' of all real non-singular matrices.

Let r and s be two matrices in H , so that $r^*r = e$, $s^*s = e$. Then $(rs)^*rs = s^*r^*rs = s^*s = e$, i.e., $rs \in H$. Moreover from $r^*r = e$ it follows that $r^* = r^{-1}$ and hence that $rr^* = e$. Transposing this equation we obtain $(rr^*)^* = e^* = e$, i.e., $r^{**}r^* = e$ so that r^* is also orthogonal. Thus $r^{-1} = r^*$ is orthogonal and $r^{-1} \in H$.

It is easy to show that for $n \geq 2$ the subgroup H is not a normal subgroup of G' .

Example 4. Let G be the group of matrices introduced in Example 2. Denote by H the set of all matrices in G with determinant equal to one. Recalling that the determinant of the product of two matrices is equal to the product of their determinants, we see at once that H is a normal subgroup of G .

SECTION 3 ISOMORPHISM. HOMOMORPHISM

At the beginning of the present chapter it was stated that group theory studies a group only from the point of view of its group operation. This idea may be clearly formulated in terms of the following definition.

Definition 5: A mapping f of a group G onto a group G' is said to be an isomorphic mapping or briefly an isomorphism if it is one-to-one and preserves the group operation, i.e., $f(xy) = f(x)f(y)$ for every pair of elements x, y in G . It is easy to see that if f is an isomorphism then the mapping inverse to f is also an isomorphism. Two groups G and G' are said to be isomorphic if there exists an isomorphism of one onto the other.

A) We may consider the isomorphic mappings of a group G onto itself. Such isomorphisms are called automorphisms of G . Every automorphism of G is a one-to-one mapping of G onto itself and is therefore a transformation of the set G (see Section I, F)). Thus two automorphisms may be multiplied and the product thus obtained also turns out to be an automorphism. It is clear, moreover, that the identity mapping is an automorphism and that the inverse of an automorphism is again an automorphism. Thus the set of all automorphisms of a group G is itself a group.

B) Let a be an arbitrary fixed element of the group G . In terms of a we define an automorphism f_a of G by writing

$$f_a(x) = axa^{-1} \quad (1)$$

for every $x \in G$. An automorphism so obtained is said to be inner. The set of all inner automorphisms of a group G is a subgroup of the group of all automorphisms; moreover

$$f_a f_b = f_{a b} . \quad (2)$$

In order to show that (1) does in fact define an automorphism we begin by observing that f_a is a transformation of G with inverse given by the equation

$$f_a^{-1} = f_{a^{-1}} . \quad (3)$$

Indeed $f_a(f_a^{-1}(x)) = a(a^{-1}xa)a^{-1} = x$. But then the fact that f_a is an automorphism follows from the elementary computation

$$f_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = f_a(x)f_a(y).$$

Similarly, (2) follows from

$$f_a(f_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = f_{a b}(x).$$

Finally, since the inverse of an inner automorphism and the composition of two inner automorphisms are now known to be inner, the set of all inner automorphisms is a subgroup of the group of all automorphisms according to Section II, B).

A relation between two groups weaker than isomorphism is established by a homomorphic mapping.

Definition 6: A mapping g of a group G into a group G^* is said to be a homomorphic mapping or briefly a homomorphism if it preserves the group operation, i. e., if

$$g(xy) = g(x)g(y) \quad (4)$$

for every pair of elements x, y in G . The set $g^{-1}(e^*)$ of all elements of the group G mapped into the identity e^* of G^* by a homomorphism g is called the kernel of g .

If g is a homomorphism of G into G^* then

$$g(e) = e^* \quad (5)$$

i. e., the identity e of G is carried into the identity e^* of G^* ; moreover

$$g(x^{-1}) = (g(x))^{-1} \quad (6)$$

for arbitrary $x \in G$. To see this note first of all that $g(e)g(x) = g(ex) = g(x)$. Thus $g(e) = e^*$. But then also $g(x^{-1})g(x) = g(x^{-1}x) = g(e) = e^*$ which shows that $g(x^{-1}) = (g(x))^{-1}$.

The following theorem establishes a connection between homomorphisms and isomorphisms.

Theorem1: Let g be a homomorphism of a group G onto a group G^* and let N be the kernel of g . Then N is a normal subgroup of G , and G^* is isomorphic with G/N . More precisely, if x^* is an arbitrary element of G^* and if $X = g^{-1}(x^*)$ then X is a coset of the subgroup N , i. e., $X \in G/N$. The one-to-one mapping thus obtained between the group G/N and G^* is an isomorphism. This isomorphism we will call the natural isomorphism associated with g to distinguish it from any other possible isomorphism between these two groups.

Proof: We begin by showing that N is a group. If $x, y \in N$ then $g(x) = e^*, g(y) = e^*$ and therefore $g(xy) = g(x)g(y) = e^*e^* = e^*$ so that $xy \in N$. Similarly; if $x \in N$ so that $g(x) = e^*$ then $g(x^{-1}) = (g(x))^{-1} = e^{*-1} = e^*$ and $x^{-1} \in N$. Thus N is a subgroup of G . In order to show that N is a normal subgroup let $x \in N$, $a \in G$. Then $g(a^{-1}xa) = g(a^{-1})g(x)g(a) = (g(a))^{-1}e^*g(a) = e^*$ which shows that $a^{-1}xa \in N$.

Now let a^* be an arbitrary element of G^* and let $A = g^{-1}(a^*)$. If a and a' are two elements of A then

$$g(a'a^{-1}) = g(a')g(a^{-1}) = g(a')(g(a))^{-1} = a^*a^{*-1} = e^*$$

and $a'a^{-1} \in N$, i. e., a and a' belong to the same coset of N . Conversely, if x belongs to the same coset as does a , i. e., if $xa^{-1} \in N$, then $g(x)a^{*-1} = g(x)g(a^{-1}) = g(xa^{-1}) = e^*$ so that $g(x) = a^*$.

Thus A is a complete coset. Hence the mapping which assigns to each $a^* \in G^*$ the coset $g^{-1}(a^*)$ is a one-to-one mapping between the cosets of N and the group G^* . But these cosets are just the elements of the group G/N so that, denoting by f the inverse mapping, i. e., writing $f(A) = a^* \in G^*$ for $A \in G/N$, it follows that f is a one-to-one mapping of G/N onto G^* . It remains only to verify that f is an isomorphism. Let A and B be two elements of G/N and let $a \in A$, $b \in B$. Let also $g(a) = a^*$, $g(b) = b^*$; then $f(A) = a^*$, $f(B) = b^*$ and moreover $ab \in AB$; consequently

$$f(AB) = g(ab) = a^*b^* = f(A)f(B)$$

and the proof is complete.

The following proposition stands in close relation to Theorem 1:

C) Let G be a group, N a normal subgroup. We define a mapping g of G onto G/N by placing in correspondence with each element $x \in G$ that element $g(x) = X \in G/N$ which, considered as a coset, contains x , $x \in X$. The mapping thus obtained is a homomorphism. We shall call this the natural projection of a group onto its factor group to distinguish it from any other possible homomorphism.

Indeed let a and b be two elements in G and suppose $a \in A \in G/N$, $b \in B \in G/N$; then by definition

$$g(a) = A \tag{7}$$

$$g(b) = B. \tag{8}$$

On the other hand $ab \in AB$ and consequently

$$g(ab) = AB. \tag{9}$$

Comparing (7), (8), (9) we see that $g(ab) = g(a)g(b)$, which says that g is a homomorphism.

D) Note that if a homomorphism g has for its kernel the trivial subgroup $\{e\}$ then g is an isomorphism. Indeed in this case each element of g^* possesses a unique inverse image in G since each coset contains only one element.

E) If a homomorphism g maps the group G into G^* but not onto G^* then $H^* = g(G)$ is a subgroup of G^* .

If x^* and y^* are two elements of H^* then $x^* = g(x)$, $y^* = g(y)$ so that $x^*y^{*-1} = g(xy^{-1})$ and $x^*y^{*-1} \in H^*$. Thus H^* is a subgroup of G^* .

F) Let g be a homomorphism of G onto G^* . If H is any subgroup of G then $g(H)$ is a subgroup of G^* . If H is normal in G then $g(H)$ is also normal in G^* .

The fact that $g(H)$ is a subgroup follows from Proposition E) since g defines a homomorphism of H into G^* . Let us consider the state of affairs when H is normal. Let $x^* \in G^*$. Then there exists an element $x \in G$ such that $g(x) = x^*$ and since $x^{-1}Hx = H$ it follows that $x^{-1}g(H)x^* = g(x^{-1}Hx) = g(H)$. Thus $g(H)$ is a normal subgroup in G^* .

G) Let g be a homomorphism of G into G^* . If H^* is a subgroup of G^* then $g^{-1}(H^*)$ is a subgroup of G . If H^* is normal in G^* then $g^{-1}(H^*)$ is also normal in G .

Let H^* be a subgroup and let $a \in g^{-1}(H^*)$, $b \in g^{-1}(H^*)$. Then $g(ab^{-1}) = g(a)(g(b))^{-1} \in H^*$ so that $ab^{-1} \in g^{-1}(H^*)$, and $g^{-1}(H^*)$ is a subgroup. Suppose next that H^* is normal and let $a \in g^{-1}(H^*)$, $x \in G$. Then $g(x^{-1}ax) = (g(x))^{-1}g(a)g(x) \in H^*$ so that $x^{-1}ax$ is in $g^{-1}(H^*)$. Thus $g^{-1}(H^*)$ is also normal in G .

H) It is easy to see that if g is a homomorphism of a group G into a group G^* and g^* a homomorphism of G^* into a third group G^{**} then the mapping $h = g^*g$ is again a homomorphism of G into G^{**} .

We shall now broaden the definition of transformation group given in Section 1, F):

I) A group G is said to be a transformation group acting on the set Γ if to each element $x \in G$ there corresponds a transformation x^* of Γ , $x^* = \tau(x)$, such that $\tau(xy) = \tau(x)\tau(y)$. (See Section 1, F.) It is obvious that $G^* = \tau(G)$ is a transformation group acting on Γ in the narrow sense of the earlier definition, and that τ is a homomorphism of G onto G^* . The kernel of τ is called the kernel of ineffectiveness of G . If τ is an isomorphism then G is said to be an effective transformation group. In this case it is possible to identify it with G^* , letting $x = x^*$ so that the elements of G may be regarded as transformations of Γ . The transformation group G is said to be transitive if G^* is transitive, i. e., if for every pair of elements ξ and η of Γ there exists an element $x \in G$ such that $x^*(\xi) = \eta$. If G is a transformation group acting on Γ and G' a transformation group acting on Γ' then the pair of mappings φ , ψ is called a similarity of the pair G , Γ onto the pair G' , Γ' if φ is an isomorphic mapping of G onto G' and ψ is a one-to-one mapping of Γ onto Γ' such that if $x' = \varphi(x)$ and $\xi' = \psi(\xi)$ then $x'^*(\xi') = \psi(x^*(\xi))$. The pairs G , Γ and G' , Γ' are said to be similar if there exists a similarity of one onto the other.

We turn now to the consideration of transitive transformation groups:

J) Let G be a group, H a subgroup, and let G/H denote the set of left cosets of the subgroup H in G . To each element $x \in G$ we associate a mapping x^* of the set G/H into itself by defining $x^*(\Xi) = x \Xi$; $\Xi \in G/H$. It turns out that the mapping x^* thus defined

is a transformation of the set G/H and that, by virtue of the correspondence $x \rightarrow x^*$, the group G becomes a transitive transformation group acting on the set G/H . The collection K of all the elements $x \in G$ satisfying the condition $x^*(H) = H$ coincides with H . The kernel of ineffectiveness N of the transformation group G is contained in H and contains all the normal subgroups of G that are contained in H . In other words, N is the maximal normal subgroup of G contained in H .

Indeed, let x and y be two elements of G , let $z = xy$ and let $\Xi \in G/H$. We have then $z^*(\Xi) = z \Xi = xy \Xi = x^*(y^*(\Xi))$. Thus $(xy)^* = x^*y^*$. Since e^* is the identity mapping of the set G/H onto itself, every mapping x^* possesses an inverse, namely $(x^{-1})^*$, and is therefore a transformation of G/H . Thus the equation $(xy)^* = x^*y^*$ shows that G is a transformation group acting on G/H . Moreover, if aH and bH are an arbitrary pair of elements of G/H then $x = ba^{-1}$ obviously yields a transformation x^* satisfying the condition $x^*(aH) = bH$ so that G is transitive.

If $x \in K$ then $x^*(H) = xH = H$ and therefore $x \in H$. If $x \in H$ then $x^*(H) = xH = H$ and therefore $x \in K$. Thus $K = H$. Finally, if $x \in N$, $g \in G$, then $x^*(gH) = xgH = gH$ so that $g^{-1}xg \in H$ or $x \in gHg^{-1}$. On the other hand, if $x \in gHg^{-1}$ for every $g \in G$ then $g^{-1}xg \in H$ and $x^*(gh) = gh$ whence $x \in N$. Thus N is the intersection of all sets of the form gHg^{-1} and that intersection is easily seen to be the maximal normal subgroup of G contained in H .

K) Let G be a transitive transformation group acting on Γ and let α denote an arbitrary fixed element of Γ . Designate by $\psi(\xi)$ the set of all those elements $x \in G$ satisfying $x^*(\alpha) = \xi$ and let $H_\alpha = \psi(\alpha)$. Then H_α is a subgroup of G (such a subgroup is known as a stabilizer) while each set $\psi(\xi)$ is a left coset of H_α in G and ψ is a one-to-one mapping of Γ onto the set G/H_α of all left cosets. Let φ denote the identity mapping of the group G onto itself. It turns out that the pair of mappings φ , ψ is a similarity of the pair G , Γ onto the pair G , G/H_α . Moreover, if $\beta \in \Gamma$ and if x is an element of G such that $x^*(\alpha) = \beta$, then $H_\beta = xH_\alpha x^{-1}$.

Let us prove Proposition K). The set $\psi(\xi)$ is not empty since G is transitive. Let x and y be two elements of $\psi(\xi)$. Then $x^*(\alpha) = y^*(\alpha)$ and we obtain $(x^{-1}y)^*(\alpha) = \alpha$. In the special case $\xi = \alpha$ this relation implies $H_\alpha^{-1}H_\alpha \subset H_\alpha$, in other words that H_α is a subgroup of G . For arbitrary ξ it shows also that x and y belong to one and the same left coset of H_α . On the other hand if $y \in \psi(\xi)$ and if x belongs to the left coset containing y then $(x^{-1}y)^*(\alpha) = \alpha$ so that $x^*(\alpha) = y^*(\alpha) = \xi$ and therefore $x \in \psi(\xi)$. Thus $\psi(\xi)$ is exactly a left coset of the subgroup H_α in G . Clearly if ξ and η are distinct elements of Γ then the sets $\psi(\xi)$ and $\psi(\eta)$ do not intersect and in particular $\psi(\xi) \neq \psi(\eta)$. Moreover, if xH_α is

an arbitrary left coset then $\psi(x^*(\alpha)) = xH_\alpha$. Thus ψ is a one-to-one mapping of Γ onto G/H_α . To each element $x \in G$ there corresponds both the transformation x^* of the set Γ and the transformation of the set G/H_α defined above (see J)) which we also designate by x^* . Applying to the element $\psi(x^*(\alpha)) = xH_\alpha \in G/H_\alpha$ the transformation y^* we obtain

$$\begin{aligned} y^*(\psi(x^*(\alpha))) &= y^*(xH_\alpha) = yxH_\alpha = (yx)^*(H_\alpha) = \psi((yx)^*(\alpha)) \\ &= \psi(y^*(x^*(\alpha))). \end{aligned}$$

If in this relation we replace $x^*(\alpha)$ by ξ we obtain $y^*(\psi(\xi)) = \psi(y^*(\xi))$, which says that the pair of mappings φ , ψ (φ denoting the identity mapping) is a similarity of the pair G , Γ onto the pair G , G/H_α . Finally, if $x^*(\alpha) = \beta$ then the transformations corresponding to elements of $xH_\alpha x^{-1}$ leave β fixed so that $xH_\alpha x^{-1} \subset H_\beta$. Analogously we obtain $x^{-1}H_\beta x \subset H_\alpha$, and from these two relations it follows that $H_\beta = xH_\alpha x^{-1}$.

Example 5: Let Γ denote the Euclidean plane considered as a set of points. Recall that a motion of the plane is a transformation which preserves the distance between any two points and which carries a counterclockwise rotation into a counterclockwise rotation. It is obvious that the result of the action of two motions, one after the other, i. e., the product of two motions considered as transformations, is again a motion. Similarly the transformation inverse to a motion is again a motion. Thus the collection G of all motions of the plane is a transformation group. This group is clearly transitive and effective. Fixing an arbitrary point α of the plane we form the subgroup H_α of all motions leaving α fixed, i. e., of all rotations of the plane about the point α . From J) and K) it follows that the subgroup H_α contains no normal subgroups of G except the trivial subgroup $\{e\}$. In particular, H_α is not itself a normal subgroup. (This shows that G is not commutative.) On the other hand, the subgroup N of all parallel translations of the plane is easily seen to be a normal subgroup of G . Considered in its own right as a transformation group N is also transitive.

Example 6: Let G be the additive group of all real numbers, G' the multiplicative group of all positive real numbers. We show that the groups G and G' are isomorphic. Indeed, the mapping f which associates with each $x \in G$ the element $f(x) = e^x \in G'$ is an isomorphism of G onto G' .

Example 7: Let G be the group of matrices of Example 2 and

and let G^* be the multiplicative group of all complex numbers different from zero. If for each matrix $s \in G$ we write $g(s) = |s|$ where $|s|$ denotes the determinant of s then $g(st) = |st| = |s||t|$ so that g is a homomorphism of G into G^* . Moreover, G contains matrices with arbitrary determinant ($\neq 0$) so that g is in fact onto. Since the identity element of G^* is the number 1 the kernel of g is exactly the collection of all matrices with determinant equal to one.

SECTION 4 COMMUTATOR SUBGROUP

In the present paragraph we study the dependence of the group operation on the order of the factors.

A) Two elements a and b of group G are said to commute with each other if their product does not depend upon the order of the factors, $ab = ba$.

Definition 7: An element z of a group G is said to be central if it commutes with every element of G , i. e., if $zx = xz$ for every $x \in G$ or, what comes to the same thing, if $x^{-1}zx = z$. The set Z of all central elements of G is called the center of G .

The center Z is a subgroup. Indeed if z and z' are elements of Z then for every $x \in G$ we have $xzz' = zxz' = zz'x$, so that $zz' \in Z$. Also, multiplying the equation $xz = zx$ on both left and right by z^{-1} , we obtain $z^{-1}x = xz^{-1}$ so that $z^{-1} \in Z$.

B) Every subgroup H of the center Z is a normal subgroup in G . Indeed if $h \in H$ then $h \in Z$ and therefore $x^{-1}hx = h \in H$ for every $x \in G$. In particular the center itself is a normal subgroup. Subgroups of Z are called central normal subgroups.

C) In order to decide whether two elements a and b commute with each other it suffices to compute the product $ab(ba)^{-1} = aba^{-1}b^{-1}$; if this product is the identity then a and b commute, if it is not, then they do not commute. The product $aba^{-1}b^{-1}$ is called the commutator of a and b .

Definition 8: The set Q of all elements of a group G of the form $q_1 q_2 \dots q_m$, where each factor q_i is the commutator of some pair of elements of G , is called the commutator subgroup of G .

The commutator subgroup Q is a subgroup of G and in fact a normal subgroup. To see this let x and y be elements of Q , say $x = q_1 \dots q_m$, $y = q'_1 \dots q'_n$ where all of the factors on the right are commutators. Then $xy = q_1 \dots q_m q'_1 \dots q'_n$ so that $xy \in Q$. Moreover if q is a commutator, so that q has the form $q = aba^{-1}b^{-1}$,

then $q^{-1} = bab^{-1}a^{-1}$, and q^{-1} is also a commutator. Thus $x^{-1} = q_m^{-1} \dots q_1^{-1}$ also belongs to Q . This shows that Q is a subgroup of G . In order to see that Q is normal, note first that if $q = aba^{-1}b^{-1}$ then $c^{-1}qc = (c^{-1}ac)(c^{-1}bc)(c^{-1}ac)^{-1}(c^{-1}bc)^{-1}$ is also a commutator. But then for $x = q_1 \dots q_m$ we have $c^{-1}xc = (c^{-1}q_1c) \dots (c^{-1}q_mc)$ so that $c^{-1}xc \in Q$ for every $c \in G$ and every $x \in Q$.

D) The factor group G/Q of a group G by its commutator subgroup is commutative; moreover Q is the smallest normal subgroup in G yielding a commutative factor group, i.e., if N is a normal subgroup in G and if G/N is commutative then $Q \subset N$.

Let A and B be cosets of Q and consider the product $ABA^{-1}B^{-1}$. This product contains a commutator, namely $aba^{-1}b^{-1}$ where $a \in A$, $b \in B$. Since $ABA^{-1}B^{-1}$ must be a coset it follows that $ABA^{-1}B^{-1} = Q$. Thus if we regard A and B as elements of the group G/Q then $ABA^{-1}B^{-1}$ is the identity element of that group, i.e., A and B commute with each other in G/Q and G/Q is commutative.

Now let N be any normal subgroup of G such that $N \not\supseteq Q$. If N contained all commutators of pairs of elements of G it would contain the whole subgroup Q which we assume not to be the case. Consequently there exist elements a and b in G such that $aba^{-1}b^{-1} \in N$. Let A and B denote the cosets of N which contain a and b . Since $aba^{-1}b^{-1}$ is not in N it follows that $ABA^{-1}B^{-1}$, considered as an element of G/N , is not the identity, i.e., that A and B do not commute in G/N . Thus G/N is non-commutative.

E) Let N be a normal subgroup of a group G and let Q be the commutator subgroup of N . Then Q is also a normal subgroup of G .

Clearly Q is a subgroup of G . Let q be a commutator of elements of the group N : $q = aba^{-1}b^{-1}$ where $a, b \in N$. Then for every $c \in G$ we have $c^{-1}qc = (c^{-1}ac)(c^{-1}bc)(c^{-1}ac)^{-1}(c^{-1}bc)^{-1}$ and since N is normal in G , $c^{-1}ac \in N$ and $c^{-1}bc \in N$ so that $c^{-1}qc$ is also a commutator of elements of N . The result now follows exactly as in C).

Definition 9: Let G be a group. We define the sequence of subgroups Q_1, \dots, Q_i, \dots , where Q_1 denotes the commutator subgroup of G and Q_{i+1} the commutator subgroup of Q_i . Each Q_i is a normal subgroup of G . If this sequence of subgroups contains the trivial subgroup $\{e\}$ then G is said to be solvable.

The concepts of center and of commutator subgroup play an important role in the theory of topological groups.

Example 8: Let G be the group of matrices of Example 2. Denote by Z the set of all scalar matrices, i.e., of matrices of the form λe where λ is a complex number and e is the unit matrix.

It is easy to see that Z is a central normal subgroup of G . It may in fact be shown that Z is exactly the center of G . Denote also by Q the normal subgroup of G consisting of all matrices of determinant 1. Since G/Q is a commutative group (see Ex. 7) the commutator subgroup of G is contained in Q . It may in fact be shown that Q is exactly the commutator subgroup of G .

Example 9: Consider once again the group of motions of the Euclidean plane introduced in Example 5. It is shown in analytic geometry that if a Cartesian coordinate system is introduced in the plane then each motion f is defined by pair of equations of the form

$$x' = x \cos \varphi - y \sin \varphi + a; \quad y' = x \sin \varphi + y \cos \varphi + b,$$

where $(x, y) = \xi$ is an arbitrary point of the plane and $(x', y') = \xi' = f(\xi)$ is the point into which ξ is carried by the motion f . The parameters φ, a, b determine f . The angle φ is called the angle of rotation of f , the point (a, b) is the image of the origin of the coordinate system under f . The stabilizer subgroup H_0 of all those motions leaving the origin of the coordinate system fixed consists of the motions for which $a = b = 0$; the subgroup N of parallel translations of the plane consists of the motions for which $\varphi = 0$. Both subgroups H_0 and N are commutative, their intersection is the trivial subgroup $\{e\}$, but the group G itself is non-commutative. It is easy to verify that N is a normal subgroup in G and that the factor group G/N is isomorphic with H_0 . It follows that the commutator subgroup of G is contained in N and that G is a non-commutative solvable group.

SECTION 5 DIRECT PRODUCTS OF GROUPS

The concept of direct product plays an important role in group theory: it permits the construction of new groups from given ones and also permits the reduction of the study of relatively complicated groups to the investigation of their simpler constituents. We here discuss first the direct product of two groups and subsequently introduce the appropriate definition of the direct product of an arbitrary collection of groups.

A) Let N_1 and N_2 be two groups with identity elements e_1 and e_2 , respectively. Denote by G' the set of all pairs of the form (x_1, x_2) where $x_1 \in N_1, x_2 \in N_2$. There is a natural way of introducing a multiplication in the set G' ; namely if $(x_1, x_2) \in G'$, $(y_1, y_2) \in G'$ then we define $(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$. The

algebraic operation thus defined satisfies all of the group axioms. Indeed associativity is obvious since it holds in each of the groups N_1 and N_2 . Also as identity element we have the pair $e' = (e_1, e_2)$. Finally the inverse of (x_1, x_2) is the pair $(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$. The group G' is called the direct product of the groups N_1, N_2 ; in symbols: $G' = N_1 \times N_2$. We define a mapping f_1 of N_1 into G' by writing $f_1(x_1) = (x_1, e_2) \in G'$ for each $x_1 \in N_1$. Analogously we define a mapping f_2 of N_2 into G' by $f_2(x_2) = (e_1, x_2)$. It turns out that f_i , $i = 1, 2$, is an isomorphism of N_i into G' , that the subgroup $N'_i = f_i(N_i)$ is a normal subgroup in G' and, finally, that the following relations are satisfied:

$$N'_1 N'_2 = G' \quad (1)$$

$$N'_1 \cap N'_2 = \{e'\}. \quad (2)$$

We begin by showing that f_1 is an isomorphism. We have

$$f_1(x_1 y_1) = (x_1 y_1, e_2) = (x_1, e_2)(y_1, e_2) = f_1(x_1)f_1(y_1).$$

Thus f_1 is homomorphic. But if $f_1(x_1) = e'$ then $(x_1, e_2) = (e_1, e_2)$ so that $x_1 = e_1$. Thus f_1 is a homomorphism whose kernel consists of the identity element only, i.e., f_1 is an isomorphism. In exactly the same fashion it follows that f_2 is an isomorphism.

Next let (x_1, e_2) be an arbitrary element of N'_1 and let (c_1, c_2) be an arbitrary element of G' ; then $(c_1, c_2)^{-1}(x_1, e_2)(c_1, c_2) = (c_1^{-1}x_1 c_1, e_2) \in N'_1$. Thus N'_1 is normal in G' . Similarly N'_2 is normal in G' .

Finally we prove relations (1) and (2). If (x_1, x_2) is an arbitrary element of G' the $(x_1, x_2) = (x_1, e_2)(e_1, x_2)$, and this establishes (1). Also if $(x_1, e_2) = (e_1, x_2)$ then $x_1 = e_1$, $x_2 = e_2$, and $(x_1, e_2) = (e_1, x_2) = e'$ which verifies (2).

Properties (1) and (2) of the normal subgroups N'_1 and N'_2 of the group G' provide a new way of viewing the concept of direct product.

B) If for two normal subgroups N_1 and N_2 of a group G with identity element e the conditions.

$$N_1 N_2 = G \quad (3)$$

$$N_1 \cap N_2 = \{e\} \quad (4)$$

are satisfied, we shall say that G factors into the direct product of its subgroups N_1 and N_2 . It turns out that, when these conditions are satisfied, each element of the subgroup N_1 commutes

with every element of the subgroup N_2 and that every element of the group G possesses a unique expression in the form $x_1 x_2$ where $x_i \in N_i$, $i = 1, 2$. Moreover the mapping f of the group $G' = N_1 \times N_2$ onto G defined by $f(x_1, x_2) = x_1 x_2$ is an isomorphism of G' onto G such that ff_1 is the identity mapping of N_1 onto itself.

We establish the above assertions in the order stated. Let $x_1 \in N_1$, $x_2 \in N_2$, and form the commutator $q = x_1 x_2 x_1^{-1} x_2^{-1}$. Then $q = (x_1 x_2 x_1^{-1})$ and since N_2 is a normal subgroup we have $x_1 x_2 x_1^{-1} \in N_2$ and consequently $q \in N_2$. Similarly $q = x_1 (x_2 x_1^{-1} x_2^{-1}) \in N_1$ and it follows from (4) that $q = e$, i.e., that $x_1 x_2 = x_2 x_1$.

It is an immediate consequence of (3) that every element of G possesses an expression of the indicated form. In order to verify the uniqueness of the expression, suppose also that $y_1 y_2 = x_1 x_2$ where $y_i \in N_i$, $i = 1, 2$. Multiplying on the left by x_1^{-1} and on the right by y_2^{-1} we obtain $x_1^{-1} y_1 = x_2 y_2^{-1}$ and since the left member belongs to N_1 while the right member belongs to N_2 it follows from (4) that $x_1^{-1} y_1 = x_2 y_2^{-1} = e$ and hence that $x_1 = y_1$, $x_2 = y_2$.

The uniqueness of expression just established shows that f is a one-to-one mapping of G' onto G . It remains only to show that f preserves the group operation. To this end let $(x_1, x_2) \in G'$, $(y_1, y_2) \in G'$; then, using the fact that the elements of N_1 and N_2 commute with one another, we obtain

$$\begin{aligned} f((x_1, x_2)(y_1, y_2)) &= f((x_1 y_1, x_2 y_2)) = x_1 y_1 x_2 y_2 \\ &= x_1 x_2 y_1 y_2 = f((x_1, x_2))f((y_1, y_2)). \end{aligned}$$

Finally, to show that ff_1 is the identity mapping on N_1 let $x \in N_1$; the $f(f_1(x_1)) = f((x_1, e)) = x_1 e = x_1$. (Since N_1 and N_2 possess the common identity element e we have here $e_1 = e_2 = e$.) In exactly the same fashion it follows that ff_2 is the identity mapping on N_2 and the proof is complete.

We proceed now to the construction of the direct product of an arbitrary collection of groups. In order to arrive at a suitable generalization of relations (3), (4) we begin with a discussion of the product and intersection of arbitrary collections of subgroups.

C) Let Ω be a collection of subsets of a group G and denote by $\Delta(\Omega)$ the intersection of all the sets of the collection Ω . If all the sets of the collection Ω are subgroups of G then $\Delta(\Omega)$ is also a subgroup; if all of the subgroups are normal in G then so is $\Delta(\Omega)$.

Indeed suppose that Ω consists exclusively of subgroups and let $x \in \Delta(\Omega)$. If $H \in \Omega$ then $x \in H$, $y \in H$ and, therefore, $xy^{-1} \in H$; since H is an arbitrary element of Ω it follows that $xy^{-1} \in \Delta(\Omega)$, which shows that $\Delta(\Omega)$ is subgroup. Next suppose that Ω consists exclusively of normal subgroups and let $x \in \Delta(\Omega)$, $c \in G$. If $N \in \Omega$ then $x \in N$ and, therefore, $c^{-1} xc \in N$. As before, $c^{-1} xc \in \Delta(\Omega)$ and the proof is complete.

D) Let M be an arbitrary subset of a group and denote by Ω the collection of all subgroups of G containing M . The subgroup $H(M) = \Delta(\Omega)$ is the minimal subgroup of G containing M , i. e., every subgroup $H \subset G$ satisfying the condition $M \subset H$ also satisfies the condition $H(M) \subset H$. The subgroup $H(M)$ consists exactly of the set of all elements of the form

$$x = x_1 x_2 \dots x_r \quad (5)$$

where x_1, x_2, \dots, x_r is an arbitrary finite system of elements of the set $M \cup M^{-1}$. $H(M)$ is said to be the subgroup generated by M . Again, denote by Ω' the collection of all normal subgroups of G containing M . The normal subgroup $N(M) = \Delta(\Omega')$ is the minimal normal subgroup of G containing M , i. e., every normal subgroup $N \subset G$ satisfying the condition $M \subset N$ satisfies also the condition $N(M) \subset N$. The normal subgroup $N(M)$ consists exactly of the set of all elements of the form

$$x = c_1^{-1} x_1 c_1 c_2^{-1} x_2 c_2 \dots c_r^{-1} x_r c_r \quad (6)$$

where c_1, \dots, c_r is an arbitrary finite system of elements of G , x_1, \dots, x_r an arbitrary finite system of elements of the set $M \cup M^{-1}$.

Let us show that $H(M)$ consists of all elements of the form (5). Since $H(M)$ is a subgroup of G containing M it is clear that $H(M)$ contains all elements of the form (5). On the other hand, the inverse of an element of the form (5), and the product of two elements of the form (5), are again elements of the same form, so that the set of all elements of the form (5) is a subgroup containing M which therefore belongs to the collection Ω . It follows at once that the collection of all elements having the specified form coincides with $H(M)$. Analogously it may be shown that $N(M)$ consists of all elements of the form (6); the only extra remark needed is that if x is an element of the form (6) and if $c \in G$ then $c^{-1}xc$ also is of the form (6); indeed

$$\begin{aligned} c^{-1}xc &= (c_1 c)^{-1} x_1 (c_1 c) (c_2 c)^{-1} x_2 (c_2 c) \\ &\dots (c_r c)^{-1} x_r (c_r c). \end{aligned}$$

E) If H is a subgroup and N a normal subgroup of a group G then $HN = NH$ and HN is a subgroup of G ; if H is also normal in G then so is HN . It follows by induction that for an arbitrary finite collection N_1, \dots, N_r of normal subgroups the product $N_1 N_2 \dots N_r$ is again a normal subgroup, and is independent of the order

of the factors. Now let Ω be an arbitrary collection of normal subgroups of G and construct the union M of the sets of the collection Ω ; then $N(M)$, the minimal normal subgroup of G containing all of the subgroups of the collection Ω , turns out to be the union of all normal subgroups of the form $N_1 N_2 \dots N_r$ where $N_i \in \Omega$, $i = 1, \dots, r$. Since the product $N_1 N_2 \dots N_r$ is independent of the order of the factors we may suppose that each factor appears in it only once. It is natural to call the normal subgroup $N(M)$ the product of the normal subgroups of the collection Ω . We denote it by $\Pi(\Omega)$. If the collection Ω is finite, consisting, say, of the normal subgroups N_1, \dots, N_r , then $\Pi(\Omega)$ is just the subgroup $N_1 N_2 \dots N_r$.

The equation $HN = NH$ follows from the fact that $hN = NH$ for arbitrary $h \in H$. That HN is a subgroup may be seen as follows:

$$HN(HN)^{-1} = HNN^{-1}H^{-1} = HNH^{-1} = NH = HN. \quad (6_2)$$

Moreover if H and N are both normal and if $c \in G$ then $c^{-1}HNC = c^{-1}Hcc^{-1}Nc = HN$ so that HN is normal too.

In order to show that $N(M)$ consists of the union of the normal subgroups of the form $N_1 N_2 \dots N_r$, note first that $M^{-1} = M$ and that for arbitrary $c \in G$ we have $c^{-1}Mc = M$. It follows that every product of the form (6) may be written simply $y_1 y_2 \dots y_r$, where y_1, y_2, \dots, y_r is a finite system of elements of M . But for each y_i there exists a normal subgroup N_i belonging to Ω for which $y_i \in N_i$. Thus: $y_1 y_2 \dots y_r \in N_1 N_2 \dots N_r$ and consequently the normal subgroup $N(M)$ is contained in the union of the subgroups $N_1 N_2 \dots N_r$. The other assertions of the proposition are obvious.

We are now ready to introduce the definition of the direct product of an arbitrary collection of groups.

Definition 10: Let Ω be a collection of groups and let α denote a function associating with each group $N \in \Omega$ an element $\alpha(N)$ of the group N itself. We denote by G^* the collection of all such functions and introduce in G^* an operation of multiplication as follows: if α and β are two elements of G^* we define their product $\gamma = \alpha \beta$ by $\gamma(N) = \alpha(N)\beta(N)$ for each $N \in \Omega$. The set G^* with the operation of multiplication thus defined is a group: indeed, multiplication is associative in G^* since it is in each of the groups of Ω ; the identity element of G^* is the function e' associating with each N its own identity element $e'(N)$; finally the element β inverse to α is defined by the relation $\beta(N) = (\alpha(N))^{-1}$. The group G^* thus obtained is known as the full direct product of the collection Ω . We also single out in G^* the subset G' consisting of all those functions α which agree with the identity element e' except for some finite collection of N 's in Ω . (The finite collection of N 's for which $\alpha(N) \neq e'(N)$ may be different for different α 's.) It is obvious

that G' is a subgroup of G^* ; it is called the direct product of the collection Ω .

While the full direct product G^* plays a role in the theory of topological groups, we shall here concentrate attention on the direct product G' . Observe that if the set Ω is finite the full direct product G^* and the direct product G' coincide; also if Ω consists of but two groups then the direct product here defined coincides in an obvious sense with the direct product defined in A).

F). Let G' denote the direct product of a collection Ω of groups and let $x \in N \in \Omega$. To the pair N, x we associate an element $\alpha_{N,x}$ in G' by defining $\alpha_{N,x}(P) = x$ for $P = N$; $\alpha_{N,x}(P) = e'(P)$ for $P \neq N$.

We also define $f_N(x) = \alpha_{N,x}$. Thus for each group $N \in \Omega$ the function f_N is a mapping of N into G' . The mapping f_N is an isomorphism of N onto the normal subgroup N' of G' consisting of all functions $\alpha \in G'$ satisfying the condition

$$\alpha(P) = e'(P) \text{ for } P \neq N. \quad (7)$$

Denote by Ω' the collection of all normal subgroups N' corresponding in this way to various $N \in \Omega$ and by $\Omega'_{N'}$ the set obtained by deleting from Ω' the single group N' , and let $K'_{N'} = \Pi(\Omega'_{N'})$.

Then $K'_{N'}$ consists of all $\alpha \in G'$ satisfying the condition

$$\alpha(N) = e'(N). \quad (8)$$

Finally denote by $\hat{\Omega}'$ the collection of all subgroups $K'_{N'}$, $N' \in \Omega'$. Then the following relations,

$$\Pi(\Omega') = G' \quad (9)$$

$$\Delta(\hat{\Omega}') = \{e'\}, \quad (10)$$

the analogs in the present case of the relations (1), (2) of A), are satisfied. If the collection Ω is finite, consisting, say, of the groups N_1, \dots, N_r , then $K'_{N_1} = N'_1 N'_2 \dots N'_{i-1} N'_{i+1} \dots N'_r$.

Indeed the fact that f is an isomorphism of N onto a normal subgroup of G' may be established exactly as in A). Equation (9), as well as the fact that $K'_{N'}$ is a normal subgroup and consists of all $\alpha \in G'$ satisfying (8), are immediate consequences of (7) and the properties of the operation Π established in E) above. Finally, (10) is an immediate consequence of (8).

Once again, proposition F) provides a new way of viewing direct products.

Definition 10': Let G be a group and let Ω be a collection of

normal subgroups. For each $N \in \Omega$ let $\Omega_N = \Omega \setminus N$, $K_N = \prod(\Omega_N)$ and denote by $\hat{\Omega}$ the set of all normal subgroups K_N for $N \in \Omega$. Then we shall say that G factors into the direct product of the set of subgroups Ω if the following conditions are satisfied.

$$\prod(\Omega) = G \quad (11)$$

$$\Delta(\hat{\Omega}) = \{e\}. \quad (12)$$

G) Suppose that G factors into the direct product of a set Ω of its subgroups. Then each element of each group $N \in \Omega$ commutes with every element of every other group $P \in \Omega$ ($N \neq P$) and every element $x \in G$, different from the identity e , may be written uniquely, except for order, in the form of a product

$$x = x_1 x_2 \dots x_r \quad (13)$$

of elements x_1, x_2, \dots, x_r , likewise different from the identity, where different factors belong to different groups of the set Ω : $x_i \in N_i$, with $N_i \neq N_j$ for $i \neq j$. Denote also by G' the direct product of the groups of the set Ω as in Definition 10. We define a mapping f of G' into G as follows: if $\alpha \in G'$ then

$$f(\alpha) = \alpha(N_1) \alpha(N_2) \dots \alpha(N_r). \quad (14)$$

where N_1, N_2, \dots, N_r is the collection of those groups of Ω to which α assigns values other than the identity. (Note that the identities of all the groups of Ω coincide with the identity e of G .) Then f is an isomorphism of G' onto G and each $f f_N$ (see F)) is the identity mapping of N onto itself.

As before we begin by establishing the asserted commutativity. Denote by $\hat{\Omega}_N$ the set of all groups K_P for $P \in \Omega$, $P \neq N$. Since for $P \neq N$ the group K_P contains N we have

$$N \subset \Delta(\hat{\Omega}_N). \quad (15)$$

From this and (12) follows

$$N \cap K_N = \{e\}. \quad (16)$$

But also from the very definition of K_N it follows that

$$NK_N = G. \quad (17)$$

Thus G factors into the direct product of its subgroups N and K_N . Consequently the elements of N commute with the elements of K_N and therefore in particular with the elements of P , $P \neq N$, since

$P \subset K_N$. Next let $x \in G$, $x \neq e$. From (11) it follows that x possesses a factorization

$$x = x_1 x_2 \dots x_r, \quad (18)$$

where $x_i \in N_i \in \Omega$, $i = 1, 2, \dots, r$ and where we may assume that N_1, N_2, \dots, N_r are distinct (see E)). Since $x \neq e$ there must be some $x_i \neq e$ in the expression (18), whereupon any identical factors may simply be suppressed. Thus each $x \neq e$ possesses a factorization of the form (13); it remains to verify the uniqueness of the expression, except for order. To this end suppose that x possesses another such factorization

$$x = y_1 y_2 \dots y_s, \quad (19)$$

where $y_j \in P_j \in \Omega$, $y_j \neq e$, $j = 1, 2, \dots, s$. Suppose now, if possible, that the group N_1 does not appear in the collection P_1, P_2, \dots, P_s . Then $x = y_1 y_2 \dots y_s \in K_{N_1}$ but also

$$x = x_1(x_1 \dots x_{i-1} x_{i+1} \dots x_r) \quad (20)$$

where $x_i \in N_i$, $x_1 \dots x_{i-1} x_{i+1} \dots x_r \in K_{N_1}$ whence, using the fact that G factors into the direct product of N_i and K_{N_1} , it would follow that $x_i = e$, which is impossible. Thus each N_i appears in the collection P_1, P_2, \dots, P_s . Similarly each P_j appears in the collection N_1, N_2, \dots, N_r . In particular, $r = s$ and, re-enumerating if necessary, we may assume that $N_i = P_i$, $i = 1, \dots, r$. But then

$$x_1(x_1 \dots x_{i-1} x_{i+1} \dots x_r) = y_1(y_1 \dots y_{i-1} y_{i+1} \dots y_r),$$

and employing once again the fact that G is the direct product of N_i and K_{N_1} , we conclude $x_1 = y_1$. This establishes the uniqueness of the factorization of (13). The other parts of proposition G) may be established as in B).

H) Let G' be the direct product of the groups of a set Ω and let Ω be the union of two disjoint subsets Ω_1 and Ω_2 . Denote by N_1' the set of all functions $\alpha \in G'$ associating with each group of the set Ω_2 its identity element, and analogously by N_2' the set of all functions $\alpha \in G'$ associating with each group of the set Ω_1 its identity element. It may be immediately verified that N_1' and N_2' are normal subgroups of G' and that $N_1' N_2' = G'$ while $N_1' \cap N_2' = \{e'\}$. In other words, G' factors into the direct product of the two subgroups N_1' and N_2' . In view of the equivalence of Definitions 10 and 10' just established, we conclude that if G factors into the direct product of a set Ω of subgroups where Ω is the union of

two disjoint subsets Ω_1 and Ω_2 , then G also factors into the direct product of the two subgroups $\Pi(\Omega_1)$ and $\Pi(\Omega_2)$.

I) Suppose the group G factors into the direct product of two subgroups N_1 and N_2 . Then the factor group G/N_1 is isomorphic with the group N_2 . Indeed, associating with each element $x \in N_2$ its coset $f(x) \in G/N_1$ yields an isomorphism of N_2 onto G/N_1 .

We append yet another natural and useful way of viewing the concept of direct product.

J) Let G be a group, Ω a collection of subgroups. Suppose that each element of each subgroup $N \in \Omega$ commutes with every element of every other subgroup $P \in \Omega$, $P \neq N$, and also that each element $x \in G$ distinct from the identity e possesses a factorization, unique except for order, into a product

$$x = x_1 x_2 \dots x_r \quad (21)$$

of elements likewise distinct from the identity, and belonging to distinct groups of the collection Ω . Then G factors into the direct product of the collection Ω .

That each $N \in \Omega$ is normal in G follows from the existence of a factorization of the form (21) and the assumed commutativity. Moreover (11) follows from the existence of a factorization (21) while (12) follows from its uniqueness. Thus the conditions of Definition 10' are verified and proposition J) is proved.

Example 10: Let G denote the multiplicative group of all $n \times n$ real matrices having positive determinant. Denote by N_1 the normal subgroup of G consisting of all matrices with determinant equal to 1 and by N_2 the normal subgroup consisting of all matrices of the form λe where λ is a positive number and e denotes the identity matrix. It is easy to see that $N_1 N_2 = G$ and that $N_1 \cap N_2 = \{e\}$; thus G factors into the direct product of the two subgroups N_1 and N_2 .

Example 11: Let G be a commutative group every element of which, with the exception of the identity, possesses one and the same prime order p . Then G factors into the direct product of some collection of cyclic subgroups of order p .

That this is so may be seen as follows. Enumerate the elements of G , with the exception of the identity, in a transfinite sequence x_0, x_1, \dots and denote by N_0 the cyclic subgroup generated by x_0 . Suppose already constructed a transfinite sequence N_0, N_1, \dots of cyclic groups of order p , for all indices less than some transfinite number α and satisfying the conditions that, if H_α

denotes the subgroup generated by them, then (1) H_α factors into the direct product of the groups $N_0, N_1 \dots$ and (2) H_α contains all elements $x_0, x_1 \dots$ with indices less than some transfinite number β where $\beta \geq \alpha$. Then let γ be the smallest transfinite number such that x_γ does not belong to the subgroup H_α and define N_γ to be the cyclic subgroup generated by x_γ . It is easy to see that continuing the transfinite construction until it breaks off yields a factorization of the desired sort.

Example 12: Let G be the group of all rational numbers different from 0 under ordinary multiplication. Enumerate the prime numbers in increasing order, denoting them by p_1, p_2, \dots , and let $p_0 = -1$. The cyclic subgroup of G generated by p_1 we denote by P_1 . For $i > 0$ the group P_i is free while P_0 is a group of order 2. It is easy to verify that G factors into the direct product of the subgroups P_0, P_1, P_2, \dots .

SECTION 6 COMMUTATIVE GROUPS

The main purpose of the present paragraph is to prove the fundamental theorem on abelian groups (Theorem 2). The result will be employed only in Chapter 5 and is not necessary to the understanding of other parts of the book. We shall be concerned exclusively with commutative groups and will employ the additive notation; in particular, direct products will be called direct sums.

A) A finite system g_1, \dots, g_k of elements of a group G is linearly independent if

$$a_1 g_1 + \dots + a_k g_k = 0, \quad (1)$$

where the coefficients a_1, \dots, a_k are whole numbers, implies that

$$a_1 = 0, \dots, a_k = 0.$$

An infinite system of elements of G is linearly independent if each of its finite subsystems is linearly independent. Obviously a linearly independent system can contain no elements of finite order.

B) A finite or infinite system M of elements of a group G is a system of generators for that group if every $g \in G$ admits an expression of the form

$$g = a_1 g_1 + \dots + a_k g_k \quad (2)$$

where $g \in M$ and a_i is a whole number, $i = 1, \dots, k$. If the system

(1) is linearly independent then the representation (2) is easily seen to be unique. A commutative group possessing a system of linearly independent generators is said to be free.

C) Let G be a free group admitting a finite system

$$g_1, \dots, g_k \quad (3)$$

of linearly independent generators. Then every subgroup $H \subset G$ is also free and admits a finite system of linearly independent generators in number not exceeding k .

Proof by induction. For $k = 0$ the proposition is obviously valid since in that case G is trivial and H must coincide with it. We suppose the proposition holds for $k = m$ and prove it for $k = m + 1$.

Let $k = m + 1$ and denote by G' the subgroup of G generated by g_1, \dots, g_m , and by H' the intersection of H with G' , $H' = H \cap G'$. By virtue of the inductive hypothesis, the subgroup H' does admit a finite system of linearly independent generators

$$h_1, \dots, h_n \quad (4)$$

where $n \leq m$. Let now

$$h = a_1 g_1 + \dots + a_m g_m + a_{m+1} g_{m+1}$$

be an arbitrary element of H . Since the generators are linearly independent the number a_{m+1} is uniquely determined by h . If, for every choice of h , $a_{m+1} = 0$ then $H \subset G'$, i.e., $H = H'$ and consequently H possesses a system of generators of the desired sort, namely (4). Suppose then that for some choice of $h \in H$ the coefficient a_{m+1} is different from 0. Then there is an h for which the coefficient a_{m+1} is positive for, along with h , H contains the negative element $-h$. Denote now by h_{n+1} some element for which the coefficient a_{m+1} achieves its smallest positive value a'_{m+1} ,

$$h_{n+1} = a'_1 g_1 + \dots + a'_m g_m + a'_{m+1} g_{m+1}.$$

We shall show that, for every $h \in H$, a_{m+1} is divisible by a'_{m+1} . Indeed, writing a_{m+1} in the form $a_{m+1} = b_{n+1} a'_{m+1} + r$, where b_{n+1} and r are whole numbers with $0 \leq r < a'_{m+1}$, we find that the element

$$\begin{aligned} h - b_{n+1} h_{n+1} &= (a_1 - b_{n+1} a'_1) g_1 + \dots + (a_m - b_{n+1} a'_m) g_m \\ &\quad + r g_{m+1} \end{aligned}$$

belongs to H and has coefficient $a_{m+1} = r$. It follows at once that $r = 0$, i.e., that a_{m+1} is divisible by a'_{m+1} , and that the element $h - b_{n+1}h_{n+1}$ belongs to G' and therefore to H' ; accordingly, we have

$$h - b_{n+1}h_{n+1} = b_1h_1 + \dots + b_nh_n$$

or

$$h = b_1h_1 + \dots + b_nh_n + b_{n+1}h_{n+1}.$$

Thus h_1, \dots, h_n, h_{n+1} is a system of generators for H . The linear independence of the system follows immediately from the linear independence of the system (4) and the definition of h_{n+1} .

The following lemma is needed in the proof of Theorem 2:

D) Let $a = \|a_{ij}\|$ be an integral matrix (i.e., one having integral entries) with p rows and q columns. Then there exist square integral matrices s and t (of order p and q respectively) each having determinant of absolute value one and such that $b = \|b_{ij}\| = sat$ is in canonical form, i.e., such that the following conditions are satisfied:

- a) $b_{ij} = 0$ for $i \neq j$;
- b) b_{i+1}^{i+1} is an integral multiple of b_i^i ;
- c) $b_i^i \geq 0$.

For the purposes of the proof we introduce the concept of an elementary operation on an integral matrix x . Operation 1) consists in multiplying some one of the rows of x by -1 ; operation 2) consists in the interchange of an arbitrary pair of rows of x ; operation 3) consists in adding to some one row of x an integral multiple of a different row. Analogously we define operations 1'), 2') and 3') applying not to the rows but to the columns of x . It is easy to verify that each operation 1), 2), 3) may be effected by means of multiplying x on the left by a suitably chosen square integral matrix, the determinant of which is of absolute value 1. Analogously, each of the operations 1'), 2'), 3') may be effected by multiplying x on the right by a square integral matrix, the determinant of which is of absolute value 1. Thus the proof of D) reduces to showing that it is possible to carry a matrix a into canonical form by means of a sequence of elementary operations.

We show first that if, in the matrix $x = \|x_{ij}\|$, the entry x_1^1 divides all the other entries of the first row and the first column, then by means of a sequence of elementary operations it is possible to carry x into a matrix $y = \|y_{ij}\|$ such that $y_1^1 = x_1^1$ while all other entries of y in the first row and the first column are zeros.

Indeed since x_{i^1} is by assumption divisible by x_{i^1} we may write $x_{i^1} = rx_{i^1}$ where r is a whole number so that, adding to the i -th row of x the first row multiplied by r , yields a new matrix in which 0 stands in the i -th row and the first column. Applying the same operation to each row, beginning with the second, and then carrying out the analogous operations on the columns, we obtain the desired result.

For the sake of brevity let us denote by (x) the minimum of the absolute values of the non-zero entries of a matrix $x \neq 0$. We next show that either every entry of x is divisible by (x) or else it is possible by means of a sequence of elementary operations to carry x into a matrix y for which $(y) < (x)$.

Clearly by interchanging rows and columns, and changing the sign of a row if necessary, we may arrange things so that $(x) = x_{1^1}$. If now in the first column of x there is an entry x_{1^1} not divisible by x_{1^1} , write $x_{1^1} = -rx_{1^1} + n$ where $0 < n < x_{1^1}$. Then, adding to the i -th row of x its first row multiplied by r , we obtain a new matrix y for which $(y) \leq n < (x)$. If all of the entries of the first column of x are divisible by x_{1^1} but not all the entries of its first row, then by applying an analogous operation on the columns we arrive again at a matrix y satisfying $(y) < (x)$. If, on the other hand, all entries of the first column and the first row are divisible by x_{1^1} then, as we have seen, it is possible to transform x into a matrix in which all of the entries of the first row and the first column, with the exception of x_{1^1} , are zeros. If in the matrix thus obtained there is an entry x_{1^1} not divisible by x_{1^1} then we may add the i -th row to the first row and obtain a matrix in which not all of the entries of the first row are divisible by x_{1^1} , whereupon the preceding argument may be applied again.

It follows that if x is a non-zero integral matrix it is always possible by a sequence of elementary operations to transform x into a matrix z for which each entry is divisible by (z) . Indeed if this is not true of the matrix x then, as we have just seen, we may transform x into a matrix y for which $(y) < (x)$. But since we are dealing here exclusively with positive whole numbers the indicated reduction in (x) may occur only a finite number of times; therefore after a finite number of steps our process must result in the reduction to a matrix of the desired form.

Let us now assemble the information so far acquired. Starting from a non-zero matrix x we may, in the first place, transform it into a matrix z in which every entry is divisible by (z) ; then, without losing this property of divisibility, we may also arrange for $(z) = z_{1^1}$ and for all other entries in the first row and first column to be zeros. Let us say that such a matrix is in semi-canonical form.

Now consider the given matrix a . If $a = 0$ then it is already in canonical form. If not, transform it into a matrix x in semi-canonical form and denote by x' the matrix obtained by striking out the first row and first column of x . Then every entry of x' is divisible by x_1^{-1} . If x' is the zero matrix we have arrived at canonical form; if not, then x' in turn may be transformed into a matrix in semi-canonical form. Continuing this process we eventually arrive at a matrix in canonical form. Thus D) is proved.

E) Let X be a free group and let Y be a subgroup. Then it is possible to select a system x_1', \dots, x'_q of linearly independent generators in X such that elements

$$d_1 x_1', \dots, d_r x_r', \quad r \leq q,$$

constitute a system of linearly independent generators for Y , where $d_i > 0$, $i = 1, \dots, r$ and d_{i+1} is divisible by d_i , $i = 1, \dots, r - 1$.

Let

$$x_1, \dots, x_q \tag{5}$$

be a system of linearly independent generators for X ,

$$y_1, \dots, y_p \tag{6}$$

a system of linearly independent generators for the subgroup Y (see C)). Expressing the y 's in terms of the x 's we obtain equations

$$y = a_1^i x_1 + \dots + a_q^i x_q, \quad i = 1, \dots, p, \tag{7}$$

where $\|a_j^i\| = a$ is an integral matrix. Let now $s = \|s_{1^k}\|$ and $t = \|t_{1^j}\|$ be any two square integral matrices of orders p and q respectively having determinant of absolute value 1. We may use these matrices to introduce in X and Y new systems of generators

$$x_1', \dots, x_q' \tag{8}$$

$$y_1', \dots, y_p' \tag{9}$$

by means of the equations

$$x = t_1^j x_1' + \dots + t_q^j x_q', \quad j = 1, \dots, q, \tag{10}$$

$$y_k' = s_{1^k} y_1 + \dots + s_{p^k} y_p, \quad k = 1, \dots, p. \tag{11}$$

That these equations do in fact introduce new systems of linearly independent generators for X and Y follows from the fact that the matrices t and s possess determinant ± 1 so that (10) and (11) may be solved for the unknowns (8) and (6), the latter being ex-

pressible as linear forms in the elements (5) and (9) with integral coefficients. In terms of the new systems of generators we have in place of equation (7)

$$y_k' = \sum_{i=1}^p \sum_{j=1}^q \sum_{l=1}^q s_i{}^k a_j{}^l t_l{}^j x_l' = b_1{}^k x_1' + \dots + b_q{}^k x_q'$$

where $\|b_i{}^k\| = b$ is just the matrix $b = \text{sat}$. Thus we have but to choose s and t in such a way that the matrix b is in canonical form in order to obtain a system of generators x_1', \dots, x_q' of the desired sort.

Theorem 2: Any abelian group G admitting a finite system of generators factors into the direct sum of cyclic subgroups

$$U_1, \dots, U_m; V_1, \dots, V_n,$$

where each U_i , $i = 1, \dots, m$, is a free cyclic group, while V_j , $j = 1, \dots, n$, is a cyclic subgroup of the finite order $\tau_j > 1$ where $\tau_j + 1$ is divisible by τ_j for $j = 1, \dots, n - 1$. Such a decomposition of G is, generally speaking, not unique, but for any two such decompositions the numbers m and τ_1, \dots, τ_n are the same.

Proof. Let g_1, \dots, g_q be a finite system of generators for G and denote by X the set of all linear forms

$$x = a_1 x_1 + \dots + a_q x_q \quad (12)$$

with integral coefficients a_1, \dots, a_q in the indeterminants x_1, \dots, x_q . We turn X into a group with x_1, \dots, x_q as a system of linearly independent generators by defining addition in the natural way. To each element $x \in X$ associate the element $f(x) = a_1 g_1 + \dots + a_q g_q \in G$. Then f is obviously a homomorphism of X onto G ; let Y denote its kernel and choose a system

$$x_1', \dots, x_q' \quad (13)$$

of linearly independent generators according to proposition E). Let $g_i' = f(x_i')$, $i = 1, \dots, q$. Then g_1', \dots, g_q' is a system of generators of G satisfying relations

$$d_1 g_1' = 0, \dots, d_r g_r' = 0$$

(see E)). On the other hand if a linear relation

$$b_1 g_1' + \dots + b_q g_q' = 0$$

holds then, letting

$$x' = b_1 x_1' + \dots + b_q x_q',$$

we obtain $f(x') = 0$, i.e., $x' \in Y$. Inasmuch as the elements $d_1 x_1'$, ..., $d_r x_r'$ constitute a linearly independent system of generators for Y , it follows that b_i is divisible by d_i for $i = 1, \dots, r$ while $b_i = 0$ for $i = r+1, \dots, q$.

Let now d_1, \dots, d_s be those numbers of the system d_1, \dots, d_r which are equal to one and designate the numbers d_{s+1}, \dots, d_r by τ_1, \dots, τ_n . Let moreover $g_{s+j} = v_j$, $j = 1, \dots, n$; $g_{r+i} = u_i$, $i = 1, \dots, q-r = m$ and denote by U_1, V_j the subgroups of G generated by u_i, v_j respectively. It may readily be established that G factors into the direct sum of the system of subgroups thus obtained.

In order to establish the invariance of the numbers m, τ_1, \dots, τ_n we first introduce an auxiliary concept. If A is a commutative group and p^k a power of a prime number p then $p^k A$, the set of all elements of A of the form $p^k x$, $x \in A$, forms a subgroup and in fact a subgroup of the group $p^{k-1} A$ for $k \geq 1$. The factor group $p^{k-1} A / p^k A$ we shall denote by $A p^k$. It is easy to verify that if A is the direct sum of groups A_1, \dots, A_t then $A p^k$ is the direct sum of the groups $A_1 p^k, \dots, A_t p^k$. Let us compute $A p^k$ when A is a cyclic group.

Let a generate A . If A is free then $p^{k-1} A$ has the free generator $a' = p^{k-1} a$ while $p^k A$ has the free generator pa' . From this it is immediately clear that $A p^k$ is, in this case, a cyclic group of order p . On the other hand if A is a finite cyclic group of order α , let p^l be the greatest common divisor of the numbers α and p^k and let $\alpha'' = \alpha/p^l$.

The group $p^k A$ is generated by $a'' = p^k a$ which turns out to have order α'' . Indeed, in order that $rp^k a$ should be zero, it is necessary and sufficient that the number rp^k should be divisible by α which is the case when and only when r is divisible by α'' . Similarly we may compute the order α' of the group $p^{k-1} A$ and, in terms of α' , α'' the order of the group $A p^k$ may be expressed simply as $\frac{\alpha'}{\alpha''}$ (see Section 2, D)). It follows that in this case $A p^k$ is trivial unless α is divisible by p^k , in which case it is a cyclic group of order p . Thus $G p^k$ is the direct sum of a finite number of cyclic groups of order p ; denote their number by $g(p^k)$. Since the order of $G p^k$ is just $p^{g(p^k)}$ the number $g(p^k)$ is uniquely determined by G and consequently by G and the number p^k . Since each direct summand U_1 gives rise to a cyclic summand of order p in $G p^k$ we have $g(p^k) = m + h(p^k)$ where $h(p^k)$ is the number of direct summands of order p accounted for by the summands

V_j , the subgroup V_j giving rise to a direct summand of G_{p^k} order p when and only when τ_j is divisible by p^k . Since the number of numbers τ_1, \dots, τ_n divisible by p^k is equal to 0 for sufficiently large k we have $\lim_{k \rightarrow \infty} g(p^k) = m$. Thus m is an invariant of G .

The number $h(p^k) - h(p^{k+1})$ is equal to the number of the numbers τ_1, \dots, τ_n which are divisible by p^k but not divisible by p^{k+1} . Recalling that τ_{j+1} is divisible by τ_j we see that from a knowledge of $g(p^k)$, as a function of the two variables p and k , it is possible to reconstruct the system τ_1, \dots, τ_n , and Theorem 2 is proved.

F) Let G be a commutative group. A sequence

$$x_1, \dots, x_k \quad (14)$$

of linearly independent elements in G is said to be maximal if for any element $x \in G$ the sequence x, x_1, \dots, x_k is linearly dependent. It turns out that if there exists a maximal system of linearly independent elements in G of length k , i.e., consisting of k elements, then every sequence of elements in G of length greater than k is linearly dependent. This fact permits the definition of an invariant, called the rank of the group G , as the length of a maximal sequence of linearly independent elements in G . In the event that G contains no maximal linearly independent sequence, it must contain linearly independent sequences of arbitrary length and its rank is declared to be infinity. It is easy to verify that if G admits a finite system of generators then in the resolution described in Theorem 2 the rank is equal to the number of free summands.

We shall show that if (14) is a maximal system of linearly independent elements then every sequence

$$y_1, \dots, y_l \quad (15)$$

of length $l > k$ is linearly dependent. In view of the maximality of (14) we obtain equations

$$b_j y_j = \sum_{i=1}^k a_{ij} x_i, \quad j = 1, \dots, l \quad (16)$$

where the coefficients a_{ij} and b_j are integers with $b_j \neq 0$. Since the integral matrix $\|a_{ij}\|$ has more rows than columns there must exist a relation of linear dependence between its rows with rational coefficients, not all equal to 0. Multiplying these coefficients by their least common denominator, we obtain integral coefficients c_1, \dots, c_l which are also the coefficients of a linear relation between the rows of the matrix $\|a_{ij}\|$. Thus, multiplying (16) by c_j , we obtain

$$\sum_{j=1}^l c_j b_j y_j = \sum_{j=1}^l \sum_{i=1}^k c_j a_i j x_i = 0.$$

which is a linear dependence relation between the elements (15) since not all of the numbers $c_1 b_1, \dots, c_l b_1$ are equal to 0.

Example 13: Let R denote the set of all rational numbers under the operation of ordinary addition. It is easy to see that R is a commutative group of rank 1, every element of which, with the natural exception of 0, possesses infinite order. The group R does not admit a finite system of generators for if it did then, according to Theorem 2, it would be a free cyclic group, i. e., every rational number would be expressible in the form ar_0 where r_0 is a fixed rational number and a is an integer.

Let γ be a function associating with each prime number p either an integer or $-\infty$ and taking on only a finite number of positive values. We denote by R_γ the subgroup of R consisting of 0 and all rational numbers of the form

$$r = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where p_1, \dots, p_k is an arbitrary finite system of distinct prime numbers containing all those prime numbers for which the function γ assumes positive values, and $\alpha_1, \dots, \alpha_k$ are integers satisfying the conditions $\alpha_i \geq \gamma(p_i)$, $i = 1, \dots, k$. It is easy to see that the groups R_γ exhaust the subgroups of R . The group R_γ is cyclic when, and only when, the sum of all the values of γ is finite. If R_γ is not cyclic then every one of its elements r admits unbounded division, i. e., there exist arbitrarily large natural numbers n such that $\frac{r}{n} \in R_\gamma$. R_γ and $R_{\gamma'}$ are isomorphic with one another when and only when the functions γ and γ' differ at only a finite number of primes and for every prime differ by only a finite number. From this it is easy to see that R possesses a continuum of non-isomorphic subgroups.

Example 14: Denote by R^k the set of all linear forms

$$r_1 \xi_1 + \dots + r_k \xi_k \tag{17}$$

with rational coefficients r_1, \dots, r_k . It is easy to see that, under the usual definition of addition for forms, the set R^k is a commutative group of rank k . Denote by R_i the subgroup consisting of all those forms (17) for which $r_1 = 0, \dots, r_{i-1} = 0, r_{i+1} = 0, \dots, r_k = 0$. Then R^k factors into the direct sum of the subgroups R_1, \dots, R_k and each group R_i is isomorphic to the additive group of rational

numbers.

Now let G be a commutative group of rank k , every element of which with the exception of 0 is free. We shall show that G is isomorphic with some subgroup of R^k .

Let x_1, \dots, x_k be a maximal linearly independent system of elements in G . Then for each $x \in G$ there exist integers a and a_1, \dots, a_n such that

$$ax = a_1 x_1 + \dots + a_k x_k, \quad a \neq 0. \quad (18)$$

Suppose that some other integral relation

$$bx = b_1 x_1 + \dots + b_k x_k, \quad b \neq 0 \quad (19)$$

also holds. Multiplying (18) by b , (19) by a , and subtracting one from the other, we obtain

$$(ba_1 - ab_1)x_1 + \dots + (ba_k - ab_k)x_k = 0$$

which, in view of the linear independence of the elements x_1, \dots, x_k , yields

$$ba_1 - ab_1 = 0 \text{ or } \frac{b_1}{b} = \frac{a_1}{a}.$$

Thus for a fixed system x_1, \dots, x_k the rational numbers $r_1 = \frac{a_1}{a}, i = 1, \dots, k$ are uniquely determined by x . On the other hand, if for a given system r_1, \dots, r_k of rational numbers there exists in G an element x to which these numbers correspond in the indicated fashion, then x is uniquely determined by them since G possesses no elements of finite order. Thus the numbers r_1, \dots, r_k may be used as coordinates of the elements $x \in G$ and assigning to each $x \in G$ with coordinates r_1, \dots, r_k the element $\varphi(x) = r_1 \xi_1 + \dots + r_k \xi_k \in R^k$, we obtain an isomorphism of G onto some subgroup of R^k .

Example 15: Theorem 2 shows that a commutative group with a finite number of generators factors into the direct sum of groups of the simplest sort, namely cyclic groups. We shall show that an analogous theorem cannot hold for groups without a finite number of generators. More precisely, we construct a group G of rank 2 which is irreducible, i. e., does not admit a decomposition of the form $G = N_1 \times N_2$ where N_1 and N_2 are non-trivial groups.

Let R^2 be the additive group of all linear forms $r\xi + s\eta$ with rational coefficients r and s . Consider the subgroup G of R^2 gen-

erated by the set of elements η , $\xi_0 = \xi$, ξ_1, ξ_2, \dots where the sequence of ξ 's is defined recursively by the relation

$$\xi_{i+1} = \frac{\xi_i + \eta}{2^{k_{i+1}}}, \quad i \geq 0, \quad (20)$$

the sequence k_1, k_2, \dots being any sequence of positive integers containing arbitrarily large terms. Since division by a positive integer is a well defined operation in R^2 the definition makes sense. A simple computation shows that

$$\xi_i = \frac{\xi + (1 + 2^{k_1} + 2^{k_1+k_2} + \dots + 2^{k_1+k_2+\dots+k_{i-1}})\eta}{2^{k_1+k_2+\dots+k_i}}, \quad i = 1, 2, \dots \quad (21)$$

Now from (20) it is clear that each term of the sequence $\xi_0, \xi_1, \xi_2, \dots$ is an integral combination of the following term and the element η whence it follows that for every $x \in G$ there is a natural number i sufficiently large so that x may be expressed as an integral combination of ξ_i and η . From this and (21) we conclude that if $s\eta \in G$ then s must be a whole number. We show next that G contains no non-zero element which admits unbounded division; in other words, that for every non-zero element $x \in G$ there exists a natural number n so large that for $a > n$ the equation $ay = x$ is not solvable in G , i.e., the element $y = \frac{x}{a} \in R^2$ does not belong to G .

Indeed suppose, on the contrary, that in G there is some $x \neq 0$ admitting unbounded division. Then all of its integral multiples also admit unbounded division and accordingly we may assume that $x = a\xi + b\eta$ where a and b are whole numbers. From the fact that in (21) only powers of two appear in the denominator, it is easy to conclude that if x admits unbounded division then x can be divided by arbitrarily large powers of two and therefore by every power of two. Thus G must contain the element

$$u_1 = \frac{x}{2^{k_1+k_2+\dots+k_1}} = \frac{a\xi + b\eta}{2^{k_1+k_2+\dots+k_1}}$$

for every i . Subtracting $a\xi_i$ from u_1 and using (21) we obtain

$$u_1 - a\xi_i = \frac{b - a(1 + 2^{k_1} + \dots + 2^{k_1+\dots+k_{i-1}})}{2^{k_1+\dots+k_1}} \eta = s_i \eta.$$

Replacing the sum $1 + 2^{k_1} + \dots + 2^{k_1+\dots+k_{i-1}}$ by a geometric progression we obtain

$$\frac{1 + 2^{k_1} + \dots + 2^{k_1 + \dots + k_{j-1}}}{2^{k_1 + \dots + k_i}} < \frac{2}{2^{k_i}}.$$

whence it follows that $|s_i| < \frac{2(|a| + |b|)}{2^{k_i}}$. Since a and b are

fixed while k_i may be arbitrarily large, and since s_i must be a whole number, it follows that for k_i sufficiently large $s_i = 0$, i.e.,

$$b - a(1 + 2^{k_1} + \dots + 2^{k_1 + \dots + k_{i-1}}) = 0$$

which is obviously impossible since, once more, k_i may be arbitrarily large. Thus G contains no non-zero elements admitting unbounded division.

Suppose now that G factors into the direct sum of two non-trivial subgroups N_1 and N_2 . The rank of each of these must be equal to one since rank is additive over direct sums and \mathbb{R}^2 contains no non-zero element of finite order. Also neither of the groups N_1, N_2 possesses non-zero elements admitting unbounded division and, for groups of rank 1, this signifies that they must be free cyclic groups (see Exs. 13 and 14). Thus we are lead to the conclusion that G is the direct sum of two free cyclic groups, a manifest contradiction.

SECTION 7 RINGS AND FIELDS

Along with groups an important role is played in mathematics by rings and fields. These are algebraic structures in which are defined two operations, addition and multiplication. In the present paragraph these concepts are defined and their simplest properties established. At its conclusion appears a description of the projective geometry over an arbitrary division ring. The results of this paragraph will be employed only in Sections 25–27.

Definition 11. A commutative group R , written additively, is a ring if, along with the operation of addition, there is defined an operation of multiplication associating with each pair of elements x, y in R their product $xy \in R$ in such a way that the following conditions are satisfied:

- 1) **Associativity:** If x, y, z are three elements of R then $(xy)z = x(yz)$.
- 2) **Distributivity:** If x, y, z are three elements of R then $(x + y)z = xz + yz$ and $z(x + y) = zx + zy$.

The zero of the additive group R is called the zero of the ring

R. R is said to be a division ring if the following additional condition is satisfied:

3) The elements of R, different from zero, form a group with respect to the operation of multiplication defined in the ring R. The identity element of that group is called the unit of the division ring.

Multiplication in a ring is, generally speaking, non-commutative; if it is commutative then the ring is said to be commutative. A commutative division ring is called a field.

Let R be a ring and let $x \in R$; then $0x = x0 = 0$. Indeed $0x = (0 + 0)x = 0x + 0x$ and consequently $0x = 0$. A similar argument shows that $x0 = 0$. Moreover, let $y \in R$; then $(-x)y = x(-y) = -xy$. Indeed $(-x)y + xy = (-x + x)y = 0y = 0$ which shows that $(-x)y = -xy$; the result $x(-y) = -xy$ may be similarly established.

A) A mapping g of a ring R into a ring R' is homomorphic if it preserves both operations of addition and multiplication, i.e., if for arbitrary $x, y \in R$ we have $g(x + y) = g(x) + g(y)$ and $g(xy) = g(x)g(y)$. The set of elements of R carried into the zero of R' by a homomorphism g is called the kernel of g. The kernel I of a homomorphism g, being the kernel of a homomorphism of the additive group R into the additive group R', is a subgroup of the additive group R; moreover it satisfies the conditions

$$R \cap I \subset I \quad (1)$$

$$I \cap R \subset I. \quad (2)$$

Indeed let $x \in R, y \in I$; then $g(xy) = g(x)g(y) = g(x)0 = 0$, i.e., $xy \in I$; similarly $yx \in I$.

B) A subset I of a ring R is a left ideal in R if it is a subgroup of the additive group R and satisfies condition (1); analogously an additive subgroup satisfying (2) is a right ideal. A subset I that is simultaneously a left and a right ideal is said to be a two-sided ideal or, more simply, an ideal. Clearly a division ring R possesses no ideals, either left or right, with the exception of the trivial ones: {0} and R. Partitioning the additive group of a ring R into the cosets of an ideal I we obtain an additive group R/I in which it is possible to define multiplication in a natural way so that R/I becomes a ring, known as the factor ring or the ring of residue classes of R modulo the ideal I. Indeed, if X and Y are two elements of R/I and if $x \in X, y \in Y$ then the product xy belongs to one and the same coset Z independently of the choice of the elements x and y in the cosets X and Y, and Z is defined to be the product of X and Y in R/I . There is no difficulty in showing that this definition of multiplication turns R/I into a ring. Associating with each $x \in R$ that element $g(x)$ of R/I which contains x we obtain the natural projection

g of R onto R/I . The natural projection is a homomorphism and its kernel is precisely I .

C) A homomorphism of one ring onto another is an isomorphism if it is one-to-one. It is easy to see that the mapping inverse to an isomorphism is itself isomorphic. Two rings are said to be isomorphic if there exists an isomorphism of one of them onto the other.

D) Let I be the kernel of a homomorphism of a ring R onto a R^* . It is easily shown that the natural isomorphism f of the additive group R/I onto the additive group R^* associated with the given homomorphism (see Theorem 1) is simultaneously an isomorphism of the ring R/I onto the ring R^* .

In propositions E), F), G), H) we introduce certain elementary ideas from the theory of fields.

E) A non-zero element a of a ring is said to be a divisor of zero in that ring if there exists in the ring another non-zero element b such that $ab = 0$ or $ba = 0$. Clearly a division ring contains no divisors of zero. Let R be a commutative ring without divisors of zero. Then it is possible to imbed R in a field R^* which contains no proper subfields containing the ring R . Moreover, if f is an isomorphism of R into some division ring K and if R' denotes the minimal subdivision ring of K containing $f(R)$ then f may be extended in a unique fashion to an isomorphism of R^* onto the division ring R' . In this sense the field R^* is uniquely determined by R ; it is called the quotient field of the ring R . The quotient field of the ring of whole numbers in the field of rational numbers.

In order to construct R^* we begin by considering the set M of all pairs $\frac{a}{b}$ where a and b are elements of R , $b \neq 0$. We define two pairs $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ of the set M to be equivalent, $\frac{a_1}{b_1} \sim \frac{a_2}{b_2}$, if $a_1 b_2$

$= a_2 b_1$. Clearly the relation thus defined is reflexive and symmetric; it is also transitive. Indeed let

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \sim \frac{a_3}{b_3};$$

then

$$a_1 b_2 = b_1 a_2, \quad a_2 b_3 = b_2 a_3,$$

and, multiplying the first equation by b_3 and the second by b_1 we obtain $a_1 b_2 b_3 = b_2 a_3 b_1$. Since R contains no divisors of zero we may cancel the factor b_2 in this last equation, obtaining $a_1 b_3 = a_3 b_1$, i.e., $\frac{a_1}{b_1} \sim \frac{a_3}{b_3}$. The equivalence relation thus defined partitions

M into classes of mutually equivalent elements. The set of all such equivalence classes we denote by R^* , and we denote by $\left\{ \frac{a}{b} \right\}$

the class containing the pair $\frac{a}{b}$. We shall turn R^* into a field by defining, in a natural fashion, operations of addition and multiplication. The sum and product in R^* are defined by

$$\left\{ \frac{a_1}{b_1} \right\} + \left\{ \frac{a_2}{b_2} \right\} = \left\{ \frac{a_1 b_2 + b_1 a_2}{b_1 b_2} \right\}, \quad \left\{ \frac{a_1}{b_1} \right\} \cdot \left\{ \frac{a_2}{b_2} \right\} = \left\{ \frac{a_1 a_2}{b_1 b_2} \right\}.$$

It is immediately seen that the operations thus defined do not depend upon the choice of the pairs $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ in the classes $\left\{ \frac{a_1}{b_1} \right\}$ and $\left\{ \frac{a_2}{b_2} \right\}$.

The zero of R^* is the class $\left\{ \frac{0}{b} \right\}$, the unit is the class $\left\{ \frac{b}{b} \right\}$, and the inverse of the class $\left\{ \frac{a}{b} \right\} \neq 0$ is the class $\left\{ \frac{b}{a} \right\}$. Thus R^* is a field.

Finally, assigning to each element of $a \in R$ the element $\left\{ \frac{ac}{c} \right\}$ of R^* , we obtain the natural isomorphic imbedding of R in R^* . Let now $a, b \in R$ be arbitrary elements of R with $b \neq 0$. Any subfield of R^* containing R must also contain the element $\left\{ \frac{ac}{c} \right\} \left\{ \frac{bc}{c} \right\}^{-1} = \left\{ \frac{ac}{c} \right\} \left\{ \frac{c}{bc} \right\} = \left\{ \frac{a}{b} \right\}$. Thus R^* is a minimal field containing R .

Finally, suppose given an isomorphic mapping f of R into some division ring K and let R' denote the minimal subdivision ring of K containing $f(R)$. We define the mapping g of the field R^* into K by $g \left\{ \frac{a}{b} \right\} = f(a) (f(b))^{-1}$. It is immediately verified that the map

g thus defined is an isomorphism of R^* onto the division ring R' and that g is the only isomorphism of R^* into K which agrees with f on R . Thus proposition E) is proved.

F) Let K be a division ring with unit e . The element e , considered as an element of the additive group of K , possesses a certain order which we denote by r (see Section I, E)). The number r is called the characteristic of K . It is easy to see that every element $a \neq 0$ of the additive group K possesses the same order r . It turns out that the characteristic r is either zero or a prime number. In the first case, associating with every whole number m the element $f(m) = me \in K$, we obtain an isomorphism of the ring Z of whole numbers onto a subring $f(Z) \subset K$. Thus if the characteristic is zero K contains the quotient field P^0 of the ring $f(Z)$ consisting of all elements of the form $(me)(ne)^{-1}$. The field P^0

is isomorphic with the field of rational numbers; its elements may be denoted by $\frac{m}{n} = (me)(ne)^{-1}$. In the case of prime characteristic $r = p$ the collection of multiples of the unit e coincides with the set $P^p = \{0, e, 2e, \dots, (p - 1)e\}$ which is isomorphic with the field of residue classes modulo p . The subfield P^r , $r = 0, p$, is the minimal subfield of the division ring K and is called its prime subfield.

In order to prove proposition F) we consider the mapping f of the ring Z of whole numbers into K defined by $f(m) = me$, $m \in Z$. Clearly f is a homomorphism. Let I be its kernel. It is easily seen that I consists of all integral multiples of the fixed number r . If $r = 0$ then f is an isomorphism. The case $r = 1$ is excluded since $e \neq 0$. Suppose $r > 1$. We must show that r is then a prime. Suppose the contrary, i. e., that $r = mn$ where m and n are positive integers different from one. Then we would have $me \neq 0$, $ne \neq 0$, $(me)(ne) = re = 0$, which is impossible since a division ring contains no divisors of zero. But if the generator r of I is the prime number p then the residue class ring $Z/I = P^p$ is a field, and F) is proved.

G) Let P be an arbitrary field. An expression of the form $a_0 + a_1x + \dots + a_nx^n$ where a_0, a_1, \dots, a_n are elements of P and x is a letter or, as we say, an indeterminant, is called a polynomial over P . The collection $P[x]$ of all polynomials over P is, in a natural way, a ring, the operations of addition and multiplication of polynomials being defined in the usual way. The ring $P[x]$ is commutative and possesses no divisors of zero. Consequently it may be imbedded in its own quotient field $P(x)$ (see E)) known as the field of rational functions over P in the indeterminant x . The ring $P[x]$ and the field $P(x)$ are uniquely determined by P .

H) The center of a division ring K is the collection of all elements of K that commute with every element of K . It is easy to see that the center of division ring K is a subfield. Every subfield of the center is known as a central subfield of K . Clearly the prime subfield P^r of every division ring is central. Let P be any central subfield of a division ring K and let t be an element of K . If no polynomial $\varphi(x)$ over the field P yields 0 upon substitution of t for the indeterminant x , except the zero polynomial $\varphi(x) = 0$, then t is said to be transcendental over P . Let $t \in K$ be transcendental over the central subfield P . Associating with every element $\varphi = \varphi(x) \in P[x]$ the element $f(\varphi) = \varphi(t)$, we obtain an isomorphism of the ring $P[x]$ of polynomials onto a ring $P[t] \subset K$. The extension of f to the quotient field $P(x)$ yields an isomorphism of $P(x)$ onto a field $P(t) \subset K$ known as the field of rational functions in t over the subfield P .

The balance of this paragraph is devoted to the consideration

of certain geometric concepts, namely, vector spaces and projective geometries over an arbitrary division ring.

I) Let K be a division ring and let R be a commutative group, written additively. Suppose there is defined an operation of multiplication of elements of R by elements of K , i.e., an operation assigning to each $a \in K$, $x \in R$ a product $ax \in R$. Then R is called a vector space over the division ring K if the multiplication by elements of K satisfies the conditions

$$\begin{aligned} ex &= x, \quad (a+b)x = ax + bx \\ a(bx) &= (ab)x, \quad a(x+y) = ax + ay, \end{aligned}$$

where a, b are arbitrary elements of K ; x, y arbitrary elements of R ; and e denotes the unit of K . The elements of a vector space are known as vectors. A system u_1, \dots, u_n of vectors in a vector space R over a division ring K is said to be linearly independent if from the equation

$$a_1 u_1 + \dots + a_n u_n = 0, \quad a_i \in K, \quad i = 1, \dots, n.$$

it follows that $a_1 = \dots = a_n = 0$. If the space R contains a system of n linearly independent vectors, while every system of $n+1$ vectors is linearly dependent, then $R = R^n$ is said to be finite dimensional and to have dimension n . All vector spaces appearing hereafter are understood to be finite dimensional unless the contrary is specified. A linearly independent system u_1, \dots, u_n of n vectors in an n -dimensional vector space R^n is called a basis. Once a basis u_1, \dots, u_n is fixed, every vector $x \in R$ may be written uniquely in the form

$$x = x_1 u_1 + \dots + x_n u_n; \quad x_i \in K, \quad i = 1, \dots, n.$$

The elements x_1, \dots, x_n of the division ring K are called the coordinates of x with respect to the basis u_1, \dots, u_n . If $x = \{x_1, \dots, x_n\}$ and $y = \{y_1, \dots, y_n\}$ are two vectors of R given in terms of their coordinates with respect to the basis u_1, \dots, u_n , and if $a, b \in K$, then the vector $z = ax + by$ has the coordinate representation

$$z = \{ax_1 + by_1, \dots, ax_n + by_n\}. \quad (3)$$

In particular the collection of all sequences $\{x_1, \dots, x_n\}$ of elements of K , with the operations of addition and multiplication by elements of K defined according to (3), constitutes an n -dimensional vector space over K . It follows that for each n there exists an

n -dimensional vector space R over a given division ring K and, moreover, that R is unique up to isomorphism.

J) Let R be a vector space over a division ring K . A subgroup S of the additive group R is called a vector (or linear) subspace or simply a subspace of R if $ax \in S$ for $a \in K$, $x \in S$. Every subspace S of the space R is itself a vector space over K and possesses a well defined dimension.

K) Let R^{n+1} be a vector space of dimension $n + 1$ over a division ring K and denote by G_k the set of all $(k + 1)$ -dimensional subspaces of R^{n+1} . The system P^n of sets G_0, G_1, \dots, G_n is called the n -dimensional projective geometry over K . The elements of the set G_0 are called points in the geometry P^n , the elements of G_1 lines, the elements of G_2 planes. In general for the elements of G_k we use the term k -dimensional planes. If the subspaces $a \in G_k$ and $b \in G_l$, $0 \leq k \leq l \leq n$, of the vector space R^{n+1} are connected by the relation $a \subset b$ then we say that the plane a lies on the plane b or that b passes through a , and we write $a \rightarrow b$. The incidence relation \rightarrow is the fundamental relation of projective geometry. Two projective geometries $P^n = \{G_0, G_1, \dots, G_n\}$ and $\bar{P}^n = \{\bar{G}_0, \bar{G}_1, \dots, \bar{G}_n\}$ are said to be isomorphic if there exists a one-to-one mapping f of the set $Q = G_0 \cup G_1 \cup \dots \cup G_n$ onto the set $\bar{Q} = \bar{G}_0 \cup \bar{G}_1 \cup \dots \cup \bar{G}_n$ preserving dimension and the relation \rightarrow , i. e., satisfying the conditions

$$f(G_k) = \bar{G}_k, \quad k = 0, 1, \dots, n; \quad (4)$$

$$\text{if } a \rightarrow b, a \in Q, b \in Q \quad \text{then} \quad f(a) \rightarrow f(b), \quad (5)$$

$$\text{if } \bar{a} \rightarrow \bar{b}, \bar{a} \in \bar{Q}, \bar{b} \in \bar{Q} \quad \text{then} \quad f^{-1}(\bar{a}) \rightarrow f^{-1}(\bar{b}). \quad (6)$$

Clearly the n -dimensional projective geometry over a division ring K is uniquely determined up to isomorphism by K .

L) The incidence relation \rightarrow in the projective geometry $P^n = \{G_0, \dots, G_n\}$ over a division ring K satisfies the conditions I-VII listed below. These relations are known as the incidence axioms of projective geometry. In order to be able to formulate the axioms conveniently we introduce the concept of linear dependence. A system of points, a_0, a_1, \dots, a_q is said to be linearly dependent if all of the points belong to some one plane $a \in G_{q'}$, where $q' < q$; otherwise the system is said to be linearly independent.

I If $a \rightarrow b, b \rightarrow c$ then $a \rightarrow c$.

II Every line passes through at least three distinct points.

III Through every $q + 1$ linearly independent points there passes one and only one q -dimensional plane, $q = 1, \dots, n$.

IV Every q -dimensional plane contains $q + 1$ linearly independent points, $q = 1, \dots, n$.

V Let b be a plane of arbitrary dimension containing a system a_0, \dots, a_q of $q + 1$ linearly independent points, and let a denote the q -dimensional plane passing through the points a_0, \dots, a_q . Then $a \rightarrow b$.

VI If a_0, \dots, a_p are linearly independent points of a p -dimensional plane a and b_0, \dots, b_q linearly independent points of a q -dimensional plane b and if the system of points $a_0, \dots, a_p, b_0, \dots, b_q$ is linearly dependent, then the planes a and b possess at least one common point.

VII There is a unique n -dimensional plane, i.e., the set G_n consists of a single element.

Conditions I-VII are easily verified. We indicate the proof of II; the verification of the others will be left to the reader. Let l be an arbitrary line, i.e., a 2-dimensional subspace of the vector space R^{n+1} , and let a and b be a basis of that subspace. Then the 1-dimensional subspaces containing the vectors a , b , and $a + b$ respectively are obviously distinct and constitute points lying on l . Observe that if K is the field of residue classes modulo two, then l does not, in fact, contain any other points.

Example 16. We shall also give a synthetic definition of a projective geometry.

A system P^n of sets G_0, G_1, \dots, G_n is said to be an n -dimensional projective geometry if there is defined in it an incidence relation \rightarrow , i.e., if for each pair of elements $a \in G_k, b \in G_l$, $0 \leq k \leq l \leq n$, either $a \rightarrow b$ or $a \not\rightarrow b$, in such a way that conditions I-VII of L) are satisfied. The elements of G_0 are called points the elements of G_1 lines, the elements of G_2 planes, etc. An isomorphism between two projective geometries is defined exactly as in J).

In a projective geometry of dimension ≥ 3 the incidence axioms alone imply the important Theorem of Desargue. In order to formulate this theorem we introduce the following terminology. A triangle is a system of three linearly independent points of geometry P_n . Two sequences of points a_1, \dots, a_r and b_1, \dots, b_r are said to be in perspective if there exists a center s of perspectivity, i.e., a point s with the property that the three points a_i, b_i, s are linearly dependent for every $i = 1, \dots, r$.

Theorem of Desargue. Let a_1, a_2, a_3 and b_1, b_2, b_3 be two triangles of the projective geometry P^n , $n \geq 3$. If the triangles a_1, a_2, a_3 and b_1, b_2, b_3 are in perspective, then there exist three points c_1, c_2, c_3 such that all of the following triples (7) are linearly dependent:

$$\begin{aligned} & a_1, a_2, a_3; b_1, b_2, b_3; a_1, a_3, c_2; b_1, b_3, c_2; a_2, a_3, c_1; \\ & b_2, b_3, c_1; c_1, c_2, c_3. \end{aligned} \tag{7}$$

Conversely, if there exist three points c_1, c_2, c_3 , such that all triples (7) are linearly dependent then the triangles a_1, a_2, a_3 and b_1, b_2, b_3 are in perspective.

It is easy to verify that if the hypotheses of the Theorem of Desargue (either direct or converse) are satisfied then all the points $a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3$, and s lie in one and the same 3-dimensional plane. If they do not also, at the same time, all lie in a common 2-dimensional plane, then the proof of the Theorem of Desargue may be given very simply. If, on the other hand, the triangles a_1, a_2, a_3 and b_1, b_2, b_3 both lie in the same 2-dimensional plane $f \in G_2$ then, in order to prove the theorem, it is necessary to construct an auxiliary triangle b'_1, b'_2, b'_3 not lying in the plane f and simultaneously in perspective with each of the triangles a_1, a_2, a_3 and b_1, b_2, b_3 . Otherwise the Theorem of Desargue cannot be proved. Indeed, for 2-dimensional projective geometries it does not hold in general, i.e., there exist 2-dimensional non-Desargian geometries.

The fundamental problem of projective geometry is to decide, given an axiomatically defined projective geometry, whether or not it is isomorphic with a projective geometry over some division ring. The question may be answered in the affirmative for a projective geometry of dimension $n \geq 3$, the Theorem of Desargue playing an important role in the argument. We shall here merely indicate the method of solving the problem.

Let l be an arbitrary fixed line of the projective geometry P^n , $n \geq 3$ and let $0, e, u$ denote three distinct points lying on l . Let K denote the set of all points lying on l and distinct from the point u . It turns out that, employing projective constructions, it is possible, in one and only one way, to define in the set K operations of addition and multiplication in such a way that K becomes a division ring with zero 0 and unit e , and such that the n -dimensional projective geometry over K is isomorphic with the originally given geometry P^n .

We define addition in K as follows (Fig. 1). Let a and b be two points of l distinct from u . Let m be some 2-dimensional plane containing the line l and let l_a, l_b, l_u' be three non-concurrent lines distinct from l , lying on m , and passing through the points a, b, u , respectively. Denote by a' and b' the points of intersection of l_u' with the lines l_a and l_b , respectively. Denote also by a'' the point of intersection of the line $(0, b')$ with l_a and by b'' the

point of intersection of the line (a'', u) with l_b . Finally, denote by d the point of intersection of the line (a', b'') with l . We define then $a + b = d$. To show the correctness of the definition it is necessary first to establish that the point d is uniquely determined by the points $a, b, 0, u$ and does not depend upon the choice of the lines l_a, l_b, l_u' or on the choice of the plane m . To this end let $\bar{l}_a, \bar{l}_b, \bar{l}_u'$ be three other lines (see the dotted lines in Fig. 1) analogous to the lines l_a, l_b, l_u' and lying in some plane \bar{m} ,

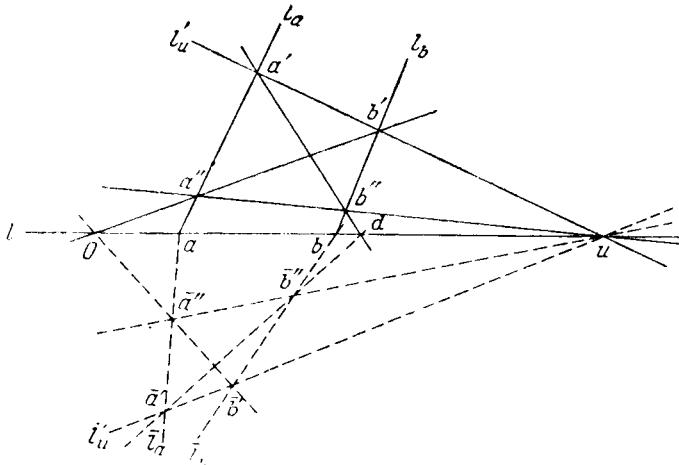


Figure 1.

and denote by $\bar{a}', \bar{a}'', \bar{b}', \bar{b}''$ the points analogous to the points a', a'', b', b'' . Then the triangles a', b', a'' , and $\bar{a}', \bar{b}', \bar{a}''$ are in perspective by virtue of the converse of the Theorem of Desargue; and similarly for the triangles b', b'', a'' and $\bar{b}', \bar{b}'', \bar{a}''$. It follows that the sequences of points a', b', a'', b'' and $\bar{a}', \bar{b}', \bar{a}''$, \bar{b}'' are in perspective, and hence, in particular, that the triangles a', a'', b'' and $\bar{a}', \bar{a}'', \bar{b}''$ are in perspective. From this in turn it follows from the direct Theorem of Desargue that the lines (a', b'') and (\bar{a}', \bar{b}'') intersect on the line $(a, u) = l$. Thus the point d is uniquely determined.

The commutativity of the operation of addition thus defined follows from the fact that if the roles of the points a and b are interchanged in the construction, then the lines $l_u' = (a', b')$ and $l_u'' = (a'', b'')$ simply interchange roles, the point d remaining unchanged. Obviously $a + 0 = a$. Moreover, carrying out the construction of Fig. 1 in reverse order, starting from the points $0, a, d, u$, we may construct the point b , so that the equation $a + b = d$ may be solved for b .

In order to prove the associativity of addition we complement

Fig. 1 by adding another arbitrary point $c \neq u$ on l (Fig. 2). Denote by c' the point of intersection of the line $(0, b'')$ with l_u' and by l_c the line (c, c') . Denote also by c'' the point of intersection of the lines l_c and l_u'' . Then taking for l_{a+b} the line (a', b'') we find that $(a + b) + c$ is the point of intersection of l with the line (a', c'') . Moreover the point $b + c$ lies on the line (b', c'') which we take to be l_{b+c} .

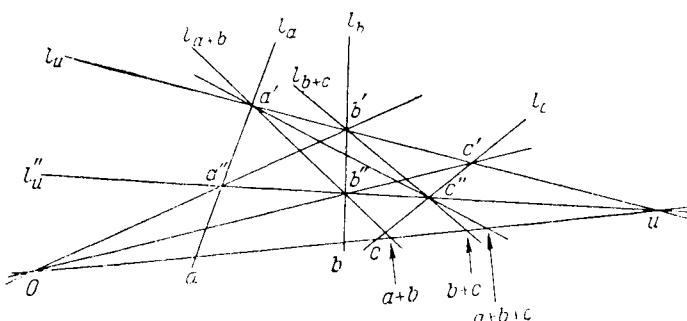


Figure 2.

But with this choice of the line l_{b+c} it is at once seen that $a + (b + c)$ must lie on the line (a', c'') , i. e., must coincide with $(a + b) + c$. Thus K is an additive group.*

We define multiplication in K in the following analogous manner (Fig. 3). Let a and b be two points of l distinct from u . As before let m be a 2-dimensional plane passing through l and let l_a , l_b , and l_u be three non-concurrent lines lying on m , distinct from l , and passing through the points a , b , u , respectively. Denote once more by a' and b' the points of intersection of the line l_u' with l_a and l_b , respectively. This time let a'' denote the point of intersection of the line (e, b') with l_a and let b'' denote the point of intersection of the line $(0, a'')$ with l_b . Then the product ab is defined to be the point of intersection of the line (a', b'') with l . The correctness of this definition is demonstrated word for word as in the case of addition. The equation $ea = a$ and the

* Observe that the required non-concurrence of the various auxiliary lines in this construction offers no difficulty. Indeed the point c' constructed above cannot coincide with b' unless $b = 0$, in which case the argument becomes trivial, while $c' = a'$ can occur only when $a + b = 0$, so that it is only necessary to prove that $a + (b + c) = c$. But in this case $a + (b + c)$ is easily seen to be the point of intersection of the line (a', c'') with l , while, since $a' = c'$, we have $(a', c'') = l_c$.

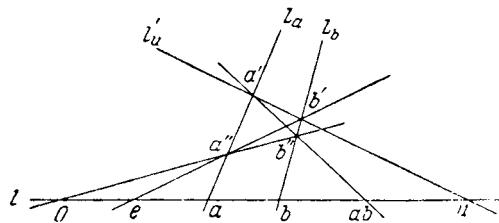


Figure 3.

existence of inverse elements are immediately established. Finally, the associativity and distributivity of multiplication may be verified by means of constructions analogous with the foregoing. Thus, with addition and multiplication so defined, K becomes a division ring which is, generally speaking, non-commutative. In projective geometry it is shown that the n -dimensional projective geometry over K is isomorphic with the given geometry.

A necessary and sufficient condition that a division ring K should be commutative is the validity in the projective geometry over K of the Theorem of Pascal on hexagons inscribed in degenerate second degree curves (i. e., in the figure formed by two intersecting lines).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

2

TOPOLOGICAL SPACES

Just as group theory investigates a single algebraic operation in its purest form, so general topology sets as its goal the study of the operation of passage to the limit to the exclusion of all other possible properties of the objects under investigation.

If we are given an arbitrary set M of real numbers then we are able to say of every real number either that it is a limit point of the set M or that it is not. And in terms of limit points we may formulate the definition of convergence of a sequence of real numbers and, in general, all the concepts relating to passage to the limit. Now the idea of a limit point is at the basis of the definition of a topological space. However, as it turns out, it is more convenient to axiomatize, not the concept of a limit point directly, but rather the fully equivalent notion of closure. Joining to the given set M all of its limit points we obtain the closure \bar{M} of M , i. e., the closure consists of all the points belonging to M along with all the points which are limit points of M . Thus, once we are in possession of the notion of limit point, we may immediately define that of closure. Conversely, in terms of closure it is possible to formulate the concept of limit point. Indeed, if the point a does not belong to M then a is a limit point of M when and only when $a \in \bar{M}$. When $a \in M$ this criterion is inadequate since a might be an isolated point of M , but if a is both a point of M and a limit point of M then it must be also a limit point of the set $M \setminus a$, i. e., $a \in \bar{M} \setminus a$. The latter condition is also sufficient; more than that, it is applicable even in case $a \notin M$ since in that event $M = M \setminus a$. Thus we may say generally that a is a limit point of M when and only when $a \in \bar{M} \setminus a$.

By axiomatizing the notion of closure we arrive at the concept of a topological space.

SECTION 8. DEFINITION OF A TOPOLOGICAL SPACE

Definition 12. A set R of arbitrary elements is said to be a topological space if to each subset $M \subset R$ there is associated a set \bar{M} , called the closure of M , such that the following conditions are satisfied:

- 1) If M contains only one element a then $\bar{M} = M$ or, equivalently, $\bar{a} = a$;
- 2) If M and N are any two subsets of R then $\bar{M \cup N} = \bar{M} \cup \bar{N}$, i.e., the closure of the union is equal to the union of the closures;
- 3) $\bar{\bar{M}} = \bar{M}$, i.e., two applications of the operation of closure yields the same results as does applying the operation only once.

The elements of a topological space are called its points. The point a is said to be an adherent point of the set M if $a \in \bar{M}$ and to be a limit point of M if $a \in \bar{M} \setminus M$.

A) We show that $M \subset \bar{M}$.

Indeed let $a \in M$. Then $M = M$ a and, forming the closure of both sides of this equation, we obtain $\bar{M} = \bar{M \cup a} = \bar{M} \cup \bar{a} = \bar{M} \cup a = \bar{M \cup a}$, i.e., $a \in \bar{M}$.

B) If $M \subset N$ then $\bar{M} \subset \bar{N}$

Indeed $N = M \cup N$ and closing both sides of the equation we obtain $\bar{N} = \bar{M \cup N}$, i.e., $\bar{N} \supset \bar{M}$.

Definition 13. A set F in a topological space R is closed if $\bar{F} = F$. A set G is open if $R \setminus G$ is closed.

According to Definition 13, closed sets and open sets are dual to one another in any topological space. Therefore to every assertion relating to closed sets there corresponds another assertion relating to open sets. We shall exploit this fact in proving the following simple propositions.

C) The union of a finite number of closed sets is again a closed set.

Indeed if E and F are two closed sets then

$$\overline{E \cup F} = \overline{E} \cup \overline{F} = E \cup F;$$

consequently $E \cup F$ is closed. The result extends by induction to an arbitrary finite number of sets.

The dual proposition for open sets reads:

D) The intersection of an arbitrary finite number of open sets is open. The proof is completely trivial and in the sequel such proofs will be omitted, but it is worthwhile giving the details just once. Let G and H be two open sets in R . Then $E = R \setminus G$ and $F = R \setminus H$ are closed sets and the intersection $G \cap H$ is the

complement of $E \cup F$, i.e., $G \cap H = R \setminus (E \cup F)$. But $E \cup F$ is closed and consequently $G \cap H$ is open.

E) Let Σ be an arbitrary collection of closed sets in a space R and let D denote the intersection of all the sets belonging to Σ . Then D is also a closed set.

Indeed let F be an arbitrary set of the system Σ . Then $D \subset F$ and consequently $\overline{D} \subset \overline{F} = F$ (see B)). Since F is an arbitrary element of Σ we have $\overline{D} \subset D$ which suffices to show $\overline{D} = D$ since $D \subset \overline{D}$ is always true.

The dual proposition for open sets reads:

F) The union of an arbitrary collection of open sets is open.

G) Observe that, except for the trivial case when the space R contains only one point, the set R itself and the empty set are simultaneously closed and open.

Indeed the closure of any set is contained in R , in particular $\overline{R} \subset R$, and it follows that R is closed. On the other hand, if R contains two distinct points a and b then the empty set is the intersection of the two one-point sets consisting of a and b , respectively, and is therefore closed too.*

H) A set M in a space R is said to be everywhere dense if $\overline{M} = R$.

Example 17. Let R be an arbitrary infinite set. We define in R an operation of closure in the following manner: if M is a finite subset of R we let $\overline{M} = M$; if M is an infinite subset of R we let $\overline{M} = R$. It is easy to verify that this definition of closure satisfies the conditions of Definition 12.

Example 18. Let R be an arbitrary set; we define in it an operation of closure by letting $\overline{M} = M$ for every set $M \subset R$. Once again, it is easy to verify that conditions (1), (2), (3) of Definition 12 are satisfied so that, with this definition, R becomes a topological space. Every subset of R is closed. Such a space is said to be discrete.

* In the usual definition of a topological space in terms of a closure operation (see, e.g., [3]) condition 1) of Definition 12 is replaced by the two requirements that the closure of the empty set should be empty and that the closure \overline{M} of an arbitrary set M should contain M . Thus propositions A) and G), taken together, may be viewed as saying that, except for one trivial exception, viz., the case of a space S consisting of a single point with $\overline{0} = \overline{S} = S$, the class of topological spaces as here defined is a subclass of the class of all topological spaces according to the customary definition.
(Trans.)

SECTION 9. NEIGHBORHOODS

In the present paragraph we give a means of defining a topological space in terms of neighborhoods. This method is particularly important and is, indeed, frequently made the basis of the definition of a topological space.

According to Definition 12, in order to define a topological space R it is necessary to associate with each subset $M \subset R$ its closure \bar{M} . It turns out however that there is no need to give the closure of every set; it suffices to define the closed sets, for then the closure of every set is uniquely determined. The justification of this assertion is the following proposition:

A) Let M be an arbitrary subset of R and let Σ be the collection of all closed subsets of R containing M . Denote by D the intersection of the collection Σ . Then $\bar{M} = D$; in other words, \bar{M} is the minimal closed set containing M .

Indeed M is a closed set since $M = \bar{M}$. Moreover $\bar{M} \supset M$ and consequently $\bar{M} \in \Sigma$ so that $D \subset \bar{M}$. Finally $D \supset M$ and since D is an intersection of closed sets we have $D = \bar{D} \supset M$. Thus $D = \bar{M}$.

Now in order to define the closed sets of a space R it suffices to give the open sets, for every closed set is simply the complement of a certain open set and every complement of an open set is closed. Thus to define a topological space R it suffices to define the open sets of R . Finally, making use of the fact that the union of an arbitrary collection of open sets is open, we are led to a further simplification.

Definition 14: A collection Σ of open sets of a space R is said to be a base for R if every open set of R is the union of some collection of open sets belonging to Σ . A base Σ for a space R is also sometimes called a complete system of neighborhoods for R and every open set of the system Σ is a neighborhood of every point of that open set. There exist bases of minimal cardinality among all the bases of a space, since any collection of cardinal numbers is well ordered. This minimal cardinal number is called the weight of R . A space with countable weight, i.e., one possessing a countable base, will be said to be separable.

The simplest example of a base consists of the collection of all open sets in R .

If we know a base for a space R then we also know all of its open sets and consequently the closure operation in R is uniquely defined. Thus in order to define a space R it suffices to give any one base.

As is clear from Definition 14, the concept of a neighborhood

is not defined uniquely by the closure operation defined in R but also depends upon the choice of a base Σ . Whenever in the sequel reference is made to neighborhoods, it will be assumed that a certain definite base Σ has been selected.

B) In order that a system of open sets Σ of a space R should be a base it is necessary and sufficient that for every open set G and every point $a \in G$ there should exist an open set $U \in \Sigma$ such that $a \in U \subset G$.

Indeed, if Σ is a base for R then there exists a subcollection Σ' consisting of sets of Σ such that G is the union of Σ' . Consequently there is an open set $U \in \Sigma'$ such that $a \in U$. Since, moreover, G is the union of a collection of sets to which U belongs we have $U \subset G$.

Suppose next that the above formulated condition is satisfied for Σ and let G be an arbitrary open set in R . Then for every point $x \in G$ may be found an open set $U_x \in \Sigma$ such that $x \in U_x \subset G$. The union of the open sets U_x , $x \in G$, is clearly equal to G and consequently Σ is a base.

By analogy with the criterion B), we make the following definition:

B') A collection Σ' of neighborhoods of a point a is said to be a base at a , or a complete system of neighborhoods of a , if for every open set G containing a there is an open set $U \in \Sigma'$ such that $U \subset G$. It follows immediately from B) that if Σ is a base for the whole space then the collection of all the open sets of Σ that contain a forms a base at a .

As has been observed above, a complete system of neighborhoods in a space R determines the closure operation uniquely. We next show explicitly how to make the transition from neighborhoods to closure operation.

C) Let a be a point and M a set in R . Then $a \in \overline{M}$ when and only when every neighborhood U of a contains a point of M . By a neighborhood of a is to be understood here an element of some base Σ' at a .

Indeed, suppose a does not belong to \overline{M} . Then $R \setminus \overline{M}$ is an open set containing a . Consequently there exists a set $U \in \Sigma'$ such that $a \in U \subset R \setminus \overline{M}$. But then U is a neighborhood of a that does not meet M . On the other hand, if V is a neighborhood of a which does not meet M then $M \subset R \setminus V = F$ where F is closed since V is open. But then $M \subset \overline{F} = F$, i.e., \overline{M} does not contain a . Thus we have shown that a necessary and sufficient condition in order that $a \notin \overline{M}$ is that a possess a neighborhood not meeting M , and this assertion is equivalent with proposition C.)

D.) If Σ is a complete system of neighborhoods of a topological space R then the following conditions are satisfied:

(a) For every pair of distinct points a and b of R there is a neighborhood $U \in \Sigma$ of a that does not contain b .

(b) For every pair of neighborhoods $U, V \in \Sigma$ of a point $a \in R$ there is a neighborhood $W \in \Sigma$ of the same point such that $W \subset U \cap V$.

In order to see that (a) holds, observe that $R \setminus b$ is open and consequently, by virtue of B), contains some neighborhood U of a . To verify (b), apply B) once again to the open set $U \cap V$.

The conditions (a) and (b) just formulated are important in that they may in their turn be taken as the axioms in a definition of a topological space by means of neighborhoods. A more precise formulation of this idea is given in Theorem 3, which at the same time provides a converse for C) and D) taken together.

Theorem 3: Let R be any set and let Σ be any collection of subsets of R satisfying the following two conditions:

(a) For every pair of distinct points a and b in R there exists a set $U \in \Sigma$ such that $a \in U$ while $b \notin U$.

(b) For every pair of sets U and V of the collection Σ that contain the point $a \in R$ there exists a set $W \in \Sigma$ such that $a \in W \subset U \cap V$.

Introduce a closure operation in R by defining $a \in \bar{M}$ when, and only when, every set of the collection Σ that contains a also meets M . The operation thus defined satisfies the conditions of Definition 12 so that R is turned into a topological space. For the space R thus defined Σ is a complete system of neighborhoods.

Proof: We must show first that the closure operation defined above satisfies conditions 1), 2), 3) of Definition 12. In so doing we shall, for brevity's sake, refer to a set $U \in \Sigma$ as a neighborhood of each of its points.

Let M consist of a single point a . Since every neighborhood of a contains a we have $a \in \bar{M}$. But if b is any point of R distinct from a then by condition (a) there exists a neighborhood U of b such that $a \notin U$ whence $b \notin \bar{M}$. Thus $\bar{M} = a$ and (1) is satisfied.

Let M and N be two subsets of R . If $a \in \bar{M} \cup \bar{N}$ then every neighborhood U of a meets either M or N . But then U meets $M \cup N$, i. e., $a \in \bar{M \cup N}$. On the other hand if $a \notin \bar{M} \cup \bar{N}$ then there exist neighborhoods U and V of a such that U does not meet M and V does not meet N . By (b) there exists a neighborhood W of a contained in the intersection $U \cap V$. But then W does not meet $M \cup N$ and consequently $a \in \bar{M \cup N}$. Thus $\bar{M \cup N} = \bar{M} \cup \bar{N}$ and 2) is satisfied.

Prior to taking up the third condition of Definition 12, we observe that for the operation of closure defined in Theorem 3 it is certainly the case that $N \subset \bar{N}$. Indeed if $x \in N$ then every neighborhood of x meets N since it contains x , and therefore $x \in \bar{N}$.

Now let $a \in \overline{\overline{M}}$, this means that every neighborhood U of a meets \overline{M} , i.e., that there exists a point $b \in \overline{M}$ such that $b \in U$; but then U is a neighborhood of b and since $b \in \overline{M}$, U must meet M . Thus an arbitrary neighborhood U of a meets M and $a \in \overline{M}$ and $M \subset \overline{M}$. On the other hand we have just seen that the inclusion $\overline{M} \subset \overline{\overline{M}}$ holds quite generally. Thus $\overline{M} = \overline{\overline{M}}$ and condition (3) is also satisfied.

It remains only to show that Σ is a complete system of neighborhoods for the topological space R . We begin by showing that every set $U \in \Sigma$ is open in R . To this end it suffices to show that the set $F = R \setminus U$ is closed. But if a point x does not belong to F , $x \notin F$, then $x \in U$ so that the neighborhood U of x does not meet F . Thus $x \notin \overline{F}$ and we have $\overline{F} = F$. Consequently U is open. If now G is any open set and if $a \in G$ then the set $R \setminus G = E$ is closed and does not contain a . Consequently there exists a neighborhood W of a not meeting E . In other words, for an arbitrary open set G and $a \in G$ there exists a neighborhood $W \in \Sigma$ such that $a \in W \subset G$ which shows that Σ is a base for R . Thus Theorem 3 is proved.

E) Theorem 3 shows that in order to define a topological space R it is unnecessary to define a closure operation in R directly but suffices to set forth a collection Σ of subsets of R satisfying (a) and (b). Whenever in the sequel we employ this method to define a topological space, it is to be understood that the closure operation is defined as in Theorem 3. The collection Σ itself is then known as the defining system of neighborhoods.

Note that, while a defining system of neighborhoods in a topological space R determines the space uniquely, the contrary is false; a given space R admits, in general, many different defining systems of neighborhoods. Thus it becomes necessary to determine under what conditions two defining systems of neighborhoods in one and the same set R lead to the same closure operation.

F) Two defining systems of neighborhoods Σ and Σ' are said to be equivalent if they lead to the same closure operation in R . In order that two defining systems Σ and Σ' of neighborhoods in the space R should be equivalent it is necessary and sufficient that for every point a and every one of its neighborhoods $U \in \Sigma$ there should be a neighborhood $U' \in \Sigma'$ of a such that $U' \subset U$, and conversely that for every neighborhood $V' \in \Sigma'$ of a there should be a neighborhood $V \in \Sigma$ of a such that $V \subset V'$.

In order to show the necessity of the condition we observe that, in the above notation, U is an open set containing a while Σ' is a base for R so that there exists a neighborhood $U' \in \Sigma'$ such that $a \in U' \subset U$. The same argument the other way around shows the existence of a V for given V' .

Let us verify sufficiency, i.e., that if the condition of

equivalence for Σ and Σ' is satisfied then they lead to one and the same closure operation. To this end let $a \in \overline{M}$ where closure is defined starting from Σ , and let V' be an arbitrary neighborhood of a selected from the system Σ' . By the condition of equivalence there exists a neighborhood $V \in \Sigma$ of a such that $V \subset V'$. But V meets M so that V' must also meet M . Since V' is an arbitrary neighborhood of a in the system Σ' we have $a \in \overline{M}$ where this time the closure operation is defined starting from Σ' . Since the argument also applies with the roles of Σ and Σ' reversed, the proof is complete.

We now formulate in terms of neighborhoods a necessary and sufficient condition that a subset G of a space R should be open. The condition is the following:

G) A subset G of a space R is open when and only when, for every point $a \in G$, there is a neighborhood U of a contained in G .

The necessity of the condition follows immediately from the fact that the defining system of neighborhoods is a base in R . Suppose on the other hand that G satisfies the above conditions; we must show that $R \setminus G = F$ is a closed set. Let $a \in F$. Then $a \notin G$ and consequently there is a neighborhood U of a not meeting F .

Thus $a \notin \overline{F}$. Consequently F is closed.

We also state in terms of neighborhoods a necessary and sufficient condition that a point a should be a limit point of a set M . The appropriate condition may be formulated as follows:

H) In order that a point a should be a limit point of a set M it is necessary that every neighborhood of a contain an infinite set of points of M and sufficient that every neighborhood of a should contain at least one point of M distinct from a .

Indeed suppose that $a \in \overline{M \setminus a}$ and that some neighborhood U contains only a finite set N of points of $M \setminus a$. Then $U \setminus N$ is open and contains a . Consequently there exists a neighborhood V of a contained in $U \setminus N$. But then V is a neighborhood of a that fails to meet $M \setminus a$, which is impossible. If, on the other hand, every neighborhood of a contains at least one point of M distinct from a , then every neighborhood of a meets $M \setminus a$, i.e., $a \in \overline{M \setminus a}$.

Example 19: Let R^n denote n -dimensional Euclidean space. Each point of R^n is determined by its n Cartesian coordinates. Consider a sequence of points x_k , $k = 1, 2, \dots$. We denote by x_k^i , $i = 1, \dots, n$ the coordinates of the point x_k . The sequence x_1, x_2, \dots is said to converge to the point x with coordinates x^i if $\lim_{k \rightarrow \infty} x_k^i = x^i$ for each i . Let M be a set of points in R^n . Then

x is said to be a limit point of M if there exists in M a sequence of points distinct from x that converges to x . The closure \bar{M} of M is then defined to be the collection of all the points belonging to M along with all the limit points of M . It is easy to see that the closure so defined satisfies all the requirements of Definition 12. In this way R^n is turned into a topological space.

Since R^n is a Euclidean space the distance between any pair of points is a well defined number. The set of all points in R^n at distance less than a fixed positive number r from a fixed point a is called the sphere with center a and radius r . It is easy to see that every sphere is an open set in R^n . Moreover it is not difficult to verify that the set of all spheres is a base in the space R^n . Similarly the set of all spheres with rational centers and rational radii is a base in R^n .

Example 20: In this paragraph a method was given of defining closure by means of neighborhoods. Another very important method of defining closure is by means of a metric. It is not possible, to be sure, to define the closure operation of an arbitrary topological space by means of a metric. Accordingly we single out the very important class of those topological spaces that are metrizable.

A collection R of arbitrary elements is said to be a metric space if to each pair of points $x, y \in R$ there is associated a distance, i.e., a non-negative real number $\rho(x, y)$ satisfying the following conditions:

- (a) $\rho(x, y) = 0$ when and only when $x = y$;
- (b) $\rho(x, y) = \rho(y, x)$;
- (c) $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$

Condition (c) is known as the triangle inequality.

There is a natural definition of closure in a metric space which turns it into a topological space. Let M be an arbitrary subset of a metric space R and let a be any point. Then the distance of the point a from the set M is defined to be the lower bound $\rho(a, M)$ of the set of numbers $\rho(a, x)$, $x \in M$, and the closure \bar{M} of M is defined to be the collection of all points at distance 0 from M . A topological space is said to be metrizable if its closure operation may be so defined in terms of some suitably chosen metric.

The sphere with center a and radius $\epsilon > 0$ in a metric space R is defined to be the set of all points at distance less than ϵ from a . It is easy to see that every sphere is open and that the collection of all spheres is a base for the topological space R .

The finite dimensional Euclidean spaces of Example 19 are important examples of metric spaces, as is their infinite dimensional generalization H , known as Hilbert space. The elements of H are the sequences $x = \{x_1, \dots, x_n, \dots\}$ of real numbers for which the series $x_1^2 + \dots + x_n^2 + \dots$ is convergent, and distance in H is defined by the equation.

$$\rho(x, y) = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2 + \dots}$$

SECTION 10. HOMEOMORPHISM. CONTINUOUS MAPPING

From the topological point of view two topological spaces whose closure operations have the same structure are indistinguishable; they are said to be homeomorphic. This idea is given more precise formulation in the following definition.

Definition 15: A mapping f of a topological space R onto a topological space R' is said to be homeomorphic or topological if it is one-to-one, and preserves the operation of closure; $f(\overline{M}) = \overline{f(M)}$ for every $M \subset R$. A homeomorphic mapping is known as a homeomorphism. It is easy to see that if f is a homeomorphism then the inverse mapping f^{-1} is also a homeomorphism. Two topological spaces R and R' are said to be homeomorphic if it is possible to map one of them homeomorphically onto the other.

The concept of a homeomorphism is the analog for topological spaces of the concept of isomorphism for groups. The topological properties of a topological space are precisely those which are preserved by all homeomorphisms. From Definition 15 it is clear that the topological properties are precisely those which may be expressed in terms of closure. Thus the property of a set of being open or of being the closure of some set is topological; on the other hand, the property of being a neighborhood is not topological, since one and the same open set may appear in one base of a space but not appear in another. In view of the non-invariance of the property of being a neighborhood, it will be necessary, whenever a definition is formulated in terms of neighborhoods, to give a proof of the topological invariance of that definition. The proof of the invariance of the definition consists in each case in showing that replacing one defining system of neighborhoods by another equivalent with it (see Section 9, F)) has no effect on the defined object.

A connection between two spaces weaker than that of homeomorphism is given by a continuous mapping. If homeomorphism

is the analog of isomorphism then continuous mapping is the analog of homeomorphism.

Definition 16: A mapping g of a topological space R into a topological space R' is said to be continuous if for every set $M \subset R$ the condition

$$g(\overline{M}) \subset \overline{g(M)}$$

is satisfied.

A) We show that if a mapping g is one-to-one and onto and also both ways continuous, i.e., if both g and g^{-1} are continuous, then g is a homeomorphism.

Since g is continuous we have $g(\overline{M}) \subset \overline{g(M)}$. Denoting the set $g(M)$ by M' and applying the mapping g^{-1} , we obtain from this that $g^{-1}(\overline{M'}) \subset g^{-1}(M')$. But, since g^{-1} is also continuous, $g^{-1}(\overline{M'}) \subset \overline{g^{-1}(M')}$. The last two relations taken together show that $g^{-1}(\overline{M'}) = \overline{g^{-1}(M')}$. Since M' is an arbitrary subset along with M it follows that g^{-1} is a homeomorphism. But if g^{-1} is homeomorphic so must g be.

B) Each of the following two conditions is both necessary and sufficient for the continuity of a mapping g of a space R into a space R' .

(a) If F' is an arbitrary closed set in R' then the inverse image $F = g^{-1}(F')$ is also closed.

(b) If G' is an arbitrary open set in R' then the inverse image $G = g^{-1}(G')$ is also open.

Let us show first that conditions (a) and (b) are equivalent. Let F' and G' be disjoint sets in the space R' with union equal to R' . It is clear that the sets $g^{-1}(F')$ and $g^{-1}(G')$ are also disjoint and have union equal to R . If condition (a) is satisfied and if G' is open then F' is closed, $g^{-1}(F')$ is also closed, and therefore $g^{-1}(G')$ is open, i.e., (b) is satisfied. Analogously, if (b) is satisfied so is (a).

Next we show that if (a) is satisfied then g is continuous. Let M be an arbitrary subset of R and let $M' = g(M)$. The set M' is closed so that its inverse image $F = g^{-1}(\overline{M'})$ is closed too. But since $M \subset F$ it follows that $\overline{M} \subset \overline{F} = F$. Thus $g(\overline{M}) \subset \overline{M'} = g(\overline{M})$ and Definition 16 is satisfied.

Finally, suppose that g is a continuous mapping, let F' be a closed set in R' , and let $F = g^{-1}(F')$. Since g is continuous we have $g(\overline{F}) \subset \overline{g(F)} = \overline{F'} = F'$ and, since F is the inverse image of F' , the relation $g(\overline{F}) \subset F'$ implies that $\overline{F} \subset F$, i.e., that F is

closed. Thus condition (a) is satisfied.

We state yet another criterion for the continuity of a mapping—a criterion possessing the advantages of intuitive clarity and of being frequently applicable.

C) A mapping g of a space R into a space R' is continuous when and only when for each point $a \in R$ and for each neighborhood U' of $a' = g(a)$ there exists a neighborhood U of a such that $g(U) \subset U'$. If this condition is satisfied at any one point a the mapping is said to be continuous at a .

The proof is based upon condition (b) of proposition B). Suppose g is continuous. Then $g^{-1}(U')$ is open and contains a so that there exists a neighborhood U of a contained in $g^{-1}(U')$, whence $g(U) \subset U'$. On the other hand, if the given condition is satisfied and if G' is open in R' we shall show that $G = g^{-1}(G')$ is also open in R . Let $a \in G$. Then $a' = g(a) \in G'$ and since G' is open there exists a neighborhood U' of a' contained in G' . Then by hypothesis there exists a neighborhood U of a such that $g(U) \subset U' \subset G'$. Since G is the inverse image of the open set G' , the relation $g(U) \subset G'$ implies that $U \subset G$. Thus G is open (see Section 9, G)).

D) It is readily seen that if g is a continuous mapping of a space R into a space R' and g' is also a continuous mapping of R' into another space R'' , then $h = g'g$ is a continuous mapping of R into R'' .

Along with continuous mappings another type of mapping, known as an open mapping, plays an important role in the theory of topological groups.

E) A mapping f of a topological space R into a topological space R' is said to be open if every open set $U \subset R$ is carried by f onto an open set: $f(U)$ is open. The mapping f is open when and only when for every point $a \in R$ and for every one of its neighborhoods V there exists a neighborhood V' of the point $f(a) = a'$ such that $V' \subset f(V)$.

Indeed if the mapping f is open then the existence of the desired neighborhood V' is obvious since $f(V)$ is itself open and contains a' . Suppose on the other hand that the given condition is satisfied and let U be an arbitrary open set in R . We show that $f(U)$ is also open. Let $a' \in f(U)$; then $a' = f(a)$ where $a \in U$ and since U is open there exists a neighborhood V of a contained in U . But then, by hypothesis, there exists a neighborhood V' of a' such that $V' \subset f(V)$ and since $V \subset U$ we have $f(V) \subset f(U)$ and consequently $V' \subset f(U)$. It follows that $f(U)$ is open (see Section 9, G)).

SECTION 11. SUBSPACE

As has been noted, it is possible to draw a parallel between the concepts of this chapter and those of the first, the analogs of isomorphism and homomorphism being homeomorphism and continuous mapping respectively. We turn now to the consideration of the appropriate analog of the concept of subgroup.

Definition 17. Let R be a topological space and let R^* be an arbitrary subset of R . There is a natural way of defining a topology in R^* , known as the topology induced by that of R , which turns R^* into a topological space in its own right. When equipped with this topology, R^* is called a subspace of R . The closure \tilde{M} of a set M in the subspace R^* is defined as follows: $\tilde{M} = \overline{M \cap R^*}$. We verify that conditions (1), (2), (3) of Definition 12 are satisfied.

If M contains only a single point a then $M = \overline{M} \cap R^* = M \cap R^* = M$. Thus (1) is satisfied.

Let M and N be two sets in R^* . Then

$$\widetilde{M \cup N} = \overline{\overline{M} \cup \overline{N}} \cap R^* = (\overline{M} \cup \overline{N}) \cap R^* = (\overline{M} \cap R^*) \cup (\overline{N} \cap R^*) = \widetilde{M} \cup \widetilde{N},$$

and (2) is satisfied.

Turning to condition 3) we observe first that $N \subset \widetilde{N}$. Indeed $\widetilde{N} = \overline{N \cap R^*} \supset N \cap R^* = N$. Moreover, we have $\overline{M \cap R^*} \subset \overline{M}$ so that $M \cap R^* \subset \overline{M}$ and consequently

$$M = \widetilde{M} \cap R^* = (\overline{M} \cap R^*) \quad R^* \subset \overline{M} \cap R^* = M$$

Since the reverse inclusion $\widetilde{M} \subset \widetilde{\widetilde{M}}$ holds quite generally, condition (3) follows.

We next establish some elementary properties of subspaces.

A) Let R^* be an arbitrary subspace of a space R . If F is a closed set in R then $E = F \cap R^*$ is closed in R^* ; conversely, every closed set E in R^* is the intersection with R^* of a suitably chosen closed set F in the space R .

Indeed let F be a closed set in R and let $R = F \cap R^*$. Then $E \subset F$ and $\overline{E} \subset \overline{F} = F$. Intersecting both sides of this relation with R^* we obtain $\widetilde{E} \subset F \cap R^*$, i.e., $\widetilde{E} \subset E$. Thus E is closed in R^* .

On the other hand suppose E is a closed set in R^* . This says that $E = \widetilde{E} = \overline{F} \cap R^*$ and E is the intersection of the closed set \overline{F} with R^* .

B) Let R^* be an arbitrary subspace of a space R . If G is

an open set in R then $H = G \cap R^*$ is open in R^* . Conversely, every open set H in R^* is the intersection with R^* of a suitably chosen open set G in R .

Let G be open in R . Then $F = R \setminus G$ is closed. Let $H = G \cap R^*$ and $E = F \cap R^*$. Clearly then $H = R^* \setminus E$ and from what has just been shown we know that E is closed in R^* . Thus H is open in R^* .

On the other hand, if H is open in R^* then $E = R^* \setminus H$ is a closed set in R^* so that $E = F \cap R^*$ where F is closed in R . But then $G = R \setminus F$ is open in R and $H = G \cap R^*$.

C) Let R be a topological space with base Σ and let R^* be a subspace of R . Then the collection Σ^* consisting of all sets of the form $U \cap R^*$, $U \in \Sigma$, is a base in R^* . The analogous proposition holds also for a base at a point.

Indeed since the sets of Σ are all open in R it follows that Σ^* is a collection of open sets in R^* . We must show that every open set H in R^* is a union of sets belonging to Σ^* . But we know that H may be written as $H = G \cap R^*$ where G is open in R . Since Σ is a base in R the set G is the union of some collection Δ of open sets belonging to Σ . Denote by Δ^* the collection of all sets of the form $U \cap R^*$, $U \in \Delta$. Then $\Delta^* \subset \Sigma^*$ and H is the union of the set sets belonging to Δ^* .

D) Let R^* be a subspace of a space R . Associate with each point $x \in R^*$ the point $f(x) = x \in R$. Then f is a continuous mapping of R^* into R .

We employ A) and condition(a) of Section 10, B). If F is a set in R then the inverse image of F under f is just $F \cap R^*$. If F is closed then $F \cap R^*$ is closed in R^* and the result follows.

E) Let g be a continuous mapping of a space R into a space R' . Suppose that $g(R) \subset R' \subset R'$. Then g is also a continuous mapping of R into the subspace R^* of R' .

To establish this assertion it suffices to observe that if $F \subset R'$ then the inverse image of F under the mapping g coincides with the inverse image of the set $F \cap R^*$ under the same mapping, and then to apply this observation when F is closed in R' .

Propostions D) and E), taken together, may be viewed as showing that Definition 17 is correctly given. If we set ourselves the task of defining a topology in an arbitrary subset of a topological space it would be natural to require of that definition that D) and E) should be valid. It is interesting to remark that, from this point of view, the induced topology on subspaces is uniquely determined. Indeed if we require that propositions D) and E) should be universally valid, we are led necessarily to Definition 17.

Example 21. Let R denote the set of all real numbers; R may

equivalently be viewed as the set of all points on a number axis. We assume the topology on R to be the natural topology defined in Example 19 ($n = 1$). Let R^* be the subspace of R consisting of all numbers y for which $-1 < y < +1$. Then R and R^* are homeomorphic. Indeed, the relation $y = \frac{e^x - e^{-x}}{e^x + e^{-x}}$ associates with each $x \in R$ a point $y \in R^*$, the correspondence being one-to-one and both ways continuous.

Example 22. Let R denote the plane in its natural topology (see Ex. 19) and denote by R^* the subspace of R consisting of all the points of the unit circle, i.e., of all those points (x, y) satisfying the condition $x^2 + y^2 = 1$. Denote also by R^{**} the set of all points of the axis of abscissas for which the abscissa φ satisfies the condition $0 \leq \varphi < 2\pi$. It is easy to verify that the mapping defined by $x = \cos \varphi$, $y = \sin \varphi$ is a one-to-one and continuous mapping of R^{**} onto R^* . The interesting feature of this example is that the mapping is not both ways continuous, i.e., the inverse mapping of R^* onto R^{**} is discontinuous. Indeed the point with coordinates $(1, 0)$ is a point of discontinuity.

SECTION 12. SEPARATION AXIOMS

Those topological spaces that are of mathematical interest satisfy, for the most part, various restrictive conditions. Among the most important of these restrictive conditions are the so-called separation axioms. Two of these axioms are intimately connected with the question of the existence on the topological space of non-constant continuous real valued functions. Accordingly we preface our discussion of the axioms with a brief consideration of such functions.

A) The space D of real numbers in its natural topology possesses a base Σ consisting of the collection of all intervals $I_{p,q}$ ($p < q$) where $I_{p,q}$ denotes the set of all real numbers x for which $p < x < q$. The base Σ contains an equivalent base Σ' (see Section IX, F)) consisting of those intervals $I_{p,q}$ with rational end-points p, q ; thus D admits a countable base. A continuous mapping of a topological space R into the topological space D is called a continuous real function on R . The function f associating with each point $x \in R$ the real number $f(x)$ is continuous at the point $a \in R$ when and only when for every positive number ϵ there exists a neighborhood U of the point a in R such that for $x \in U$ we have $|f(x) - f(a)| < \epsilon$.

Let us verify the validity of this criterion. Let $a \in R$ and let $a' = f(a)$. Suppose the criterion satisfied and let $I_{p,q}$ be an interval in the base Σ containing a' . Since $p < a' < q$ the smaller of the two numbers $a' - p$ and $q - a'$ is positive; taking this for ε we see that if $|f(x) - f(a)| < \varepsilon$ then $f(x) \in I_{p,q}$. It follows that f is continuous. On the other hand, if f is continuous then setting $p = a' - \varepsilon$, $q = a' + \varepsilon$, we obtain a neighborhood $I_{p,q}$ such that $f(x) \in I_{p,q}$ implies $|f(x) - f(a)| < \varepsilon$.

Definition 18. The following four separation axioms are formulated in increasing order of strength:

1) For every pair of distinct points a and b of the space R there exist disjoint open sets G and H such that $a \in G$, $b \in H$. This axiom bears the name of its author, Hausdorff, and a space R in which it holds is accordingly said to be Hausdorff.

2) For every point a and every closed set B not containing a in the space R there exist disjoint open sets G and H such that $a \in G$, $B \subset H$. A space satisfying this axiom is said to be regular.

3) For every point a and every closed set B not containing a in the space R there exists a continuous real function f defined on R such that $0 \leq f(x) \leq 1$ for every $x \in R$, $f(a) = 0$, and $f(x) = 1$ for every $x \in B$. A space R satisfying this axiom is said to be completely regular.

4) For every pair of disjoint closed sets A and B of the space R there exist disjoint open sets G and H such that $A \subset G$, $B \subset H$. A space R satisfying this axiom is said to be normal.

We shall show that each of the conditions 2), 3), 4) implies its predecessor. That 2) implies 1) is clear. To show that

2) follows from 3), denote by I the set of all real numbers $< 1/2$ and by I' the set of all real numbers $> 1/2$. Then the sets $G = f^{-1}(I)$ and $H = f^{-1}(I')$ are disjoint and open while $a \in G$, $B \subset H$. Thus

2) holds. Finally, that 4) implies 3) is an immediate consequence of Urysohn's Lemma (see below).

It turns out that each of the conditions 1), 2), 3), 4) represents an essentially new restriction upon a topological space: there exist topological spaces not satisfying condition 1) and for each of the conditions 2), 3), 4) there exist spaces not satisfying the condition but satisfying its predecessor.

We reformulate axioms 1), 2), and 4) in somewhat different terms.

B) Conditions 1), 2), 4) of Definition 18 are equivalent to the following conditions respectively:

1a) For every pair of distinct points a and b there exists an open set G such that $a \notin G$ while $b \in \bar{G}$.

2a) For every point a and every closed set B not containing a there exists an open set G such that $a \in G$ while $B \cap \bar{G} = \emptyset$.

4a) For every pair of disjoint closed sets A and B there exists an open set G such that $A \subset G$ while $B \cap \bar{G} = \emptyset$.

In conditions 1a), 2) and 2a) the open set G may be replaced by a neighborhood selected from an arbitrary base; and similarly in condition 1) for both G and H. Moreover condition 2) may also be formulated as follows:

2b) For every neighborhood U of an arbitrary point a there exists a neighborhood V of a such that $\bar{V} \subset U$.

The proofs of the various parts of proposition B) are trivial.

We turn now to the formulation and proof of a result which plays an important role in general topology, the definitely non-trivial Lemma of Urysohn.

Urysohn's Lemma. Given two disjoint closed sets E and F in a normal topological space R there exists a continuous real function f defined on R such that $0 \leq f(x) \leq 1$ for $x \in R$, $f(x) = 0$ for $x \in E$, $f(x) = 1$ for $x \in F$.

The idea of the proof may be briefly stated. To each proper dyadic fraction r ($0 < r \leq 1$) we associate an open set $G_r \subset R$ such that $E \subset G_r$ while $\bar{G}_r \cap F = \emptyset$ and such that $\bar{G}_{r'} \subset G_r$ for $r' < r''$. Once such a system of open sets has been constructed, the value $f(x)$ of the function f at the point $x \in R$ is simply defined to be the lower bound of the numbers r for which $x \in G_r$; if x does not belong to any of the open sets G_r we define $f(x) = 1$.

Proof. We begin by constructing in R a finite system Σ_n of open sets G_r for every rational number r of the form $q/2^n$ ($q = 1, 2, \dots, 2^{n-1}$) such that the following conditions are satisfied:

a) $E \subset G_r$, $\bar{G}_r \cap F = \emptyset$; b) $\bar{G}_{r'} \subset G_{r''}$ for $r' < r''$.

The construction is by induction on n, the system Σ_{n+1} being obtained by enlarging the system Σ_n .

For Σ_1 we need but one open set $G_{\frac{1}{2}}$. By virtue of condition 4a) of B) there exists an open set G such that $E \subset G$ while $\bar{G} \cap F = \emptyset$ and we simply let $G_{\frac{1}{2}} = G$. Then a) is satisfied by Σ_1 , while b) is nugatory.

Suppose now that the system Σ_n has been constructed. We proceed to construct Σ_{n+1} . Let $r = q/2^{n+1}$; if q is even, say $q = 2p$, then $r = p/2^n$ so that $G_r \in \Sigma_n$ and G_r is already constructed. Accordingly we may suppose that $q = 2q + 1$. Let $s = p/2^n$, $t = (p + 1)/2^n$. In order to define G_r we first define a pair of closed sets A, B, taking care to distinguish three cases: (1) $s > 0, t < 1$; in this case G_s and G_t are already constructed and we let $A = \bar{G}_s$, $B = R \setminus G_t$. 2) $s = 0$; then G_t is already constructed and we let $A = E$, $R = R \setminus G_t$. 3) $t = 1$; then G_s is already constructed and we let $A = \bar{G}_s$, $B = F$. The sets A, B are disjoint; in case 1) this follows from the inclusion $\bar{G}_s \subset G_t$, in case 2) from $E \subset G_t$ and in case 3) from $\bar{G} \cap F = \emptyset$. Hence it follows from the normality of the space R (see 4a) of B)) that, in any case, there exists an open set G such that $A \subset G$ and $\bar{G} \cap B = \emptyset$, and we define $G_r = G$.

We must show that the enlarged system Σ_{n+1} satisfies the inductive hypotheses a) and b). The former condition is readily verified by cases: thus, a) holds in case 1) since $E \subset G_s \subset G_r$ while $\bar{G}_r \subset G_t \subset R \setminus F$; in case 2) since $E \subset G_r$ while $\bar{G}_r \subset G_t \subset R \setminus F$; and in case 3) since $E \subset G_s \subset G_r$ while $\bar{G}_r \subset R \setminus F$.

We turn next to condition b). Let $r' < r''$ where $r' = q'/2^{n+1}$, $r'' = q''/2^{n+1}$. If q' and q'' are both even then $G_{r'}$ and $G_{r''}$ belong to Σ_n and $\bar{G}_{r'} \subset \bar{G}_{r''}$ holds by the inductive hypothesis. Suppose that $q' = 2p'$, $q'' = 2p'' + 1$. Let $s = p''/2^n$. Then $r' \leq s$ and we have $\bar{G}_{r'} \subset \bar{G}_s \subset \bar{G}_{r''}$ so that $G_{r'} \subset G_{r''}$. If, on the other hand, $q' = 2p' + 1$, $q'' = 2p'' + 1$, let $t = (p' + 1)/2^n$. Then $t \leq r''$ and we obtain $\bar{G}_{r'} \subset G_t \subset \bar{G}_{r''}$ so that, once again, $\bar{G}_{r'} \subset \bar{G}_{r''}$. Finally, if $q' = 2p' + 1$, $q'' = 2p'' + 1$, let $s = p''/2^n$. Then $r' < s$ and, as has already been shown, we have $\bar{G}_{r'} \subset \bar{G}_s \subset \bar{G}_{r''}$ so that again $\bar{G}_{r'} \subset \bar{G}_{r''}$. Thus condition b) is satisfied and the inductive construction is complete.

Let Σ' denote the union of the systems Σ_n , $n = 1, 2, \dots$. Joining to Σ' the open set $G_1 = R$ we obtain a system Σ'' containing an open set G_r for dyadic fraction r , $0 < r \leq 1$, and satisfying the following two conditions: a) $E \subset G_r$ for every such r while $\bar{G}_r \cap F = \emptyset$ except in the case $r = 1$; b) if $0 < r' < r'' \leq 1$ then $\bar{G}_{r'} \subset \bar{G}_{r''}$.

Now let x be an arbitrary point of R . Denoting by $f(x)$ the lower bound of those numbers r for which $x \in G_r$, we obtain a function f satisfying the conditions of the lemma. Indeed if $x \in E$ then $x \in G_r$ for every r and since the lower bound of all numbers r is 0 we have $f(x) = 0$. If $x \in F$ then $x \in G_r$ only in case $r = 1$ so that $f(x) = 1$. Moreover since r takes on only positive values not exceeding 1 we have $0 \leq f(x) \leq 1$ for every $x \in R$. It remains only to verify the continuity of f at an arbitrary point $a \in R$. Let ϵ be a positive number. Suppose first that $f(a) = 0$ and let r be a positive dyadic fraction less than ϵ . Then $a \in G_r$. Let U be a neighborhood of a such that $U \subset G_r$. Then for every $x \in U$ we have $f(x) \leq r < \epsilon$ and since $f(x) \geq 0$ it follows that $|f(x) - f(a)| < \epsilon$. Suppose next that $f(a) > 0$ and select three dyadic fractions r , s , t not exceeding 1 such that, if $f(a) < 1$, then $f(a) - \epsilon < r < s < f(a) < t < f(a) + \epsilon$ or else, such that $f(a) - \epsilon < r < s < f(a) = t = 1$ in the event that $f(a) = 1$. Clearly $a \notin G_s$ and since $r < s$ it follows that $a \notin \bar{G}_r$; but also $a \in G_t$. Thus a belongs to the open set $G_t \setminus \bar{G}_r$. Denote by U a neighborhood of a such that $U \subset G_t \setminus \bar{G}_r$. Then for every $x \in U$ we have $r \leq f(x) \leq t$ and consequently $|f(x) - f(a)| < \epsilon$. This shows that f is continuous and Uryshon's Lemma is proved.

It is interesting to note that if Urysohn's Lemma holds in a topological space R , i. e., if for every pair of disjoint closed sets E , F there exists a continuous real function f satisfying the

conditions $0 \leq f(x) \leq 1$ for $x \in R$, $f(x) = 0$ for $x \in E$, $f(x) = 1$ for $x \in F$, then R is normal. Indeed, denoting by I the set of numbers $< 1/2$ then by I' the set of numbers $> 1/2$ we see that $G = g^{-1}(I)$ and $H = f^{-1}(I')$ are disjoint open sets such that $E \subset G$, $F \subset H$.

C) A property of a topological space is said to be hereditary if every subspace of a space possessing the property also possesses it. It turns out that properties 1), 2), 3) of Definition 18 are hereditary while property 4) is not.

We shall show that 1), 2), 3) are hereditary. Let R be a topological space and let R^* be an arbitrary subspace of R . If $a \in \overline{R^*}$ while B is a closed set in R^* which does not contain a , then $B = \overline{B} \cap R^*$ so that the closed set \overline{B} of the space R also fails to contain a . Hence, if 2) is satisfied by R then there exist in R disjoint open sets G and H such that $a \in G$, $\overline{B} \subset H$. But then the open sets $G' = G \cap R^*$ and $H' = H \cap R^*$ in the space R^* contain a and B respectively. This shows that the property 2) of regularity is hereditary. The same argument also works for property 1); we have but to take B to consist of the single point b . Finally, if 3) is satisfied by R then there exists on R a continuous real function f such that $0 \leq f(x) \leq 1$ for all $x \in R$, $f(a) = 0$, $f(x) = 1$ for $x \in B$. But then the function f restricted to the subspace R^* establishes condition 3) on that subspace.

Any attempt to apply a similar argument in the case of axiom 4) must fail. Indeed, examples show that normality is not a hereditary property.

Example 23: Any metric space is normal. Let R be a metric space and let A , B be two disjoint closed sets in R . If $x \in A$ and $y \in B$ denote by U_x the sphere with center x and radius $\frac{1}{2}\rho(x, B)$ and by V_y the sphere with center y and radius $\frac{1}{2}\rho(y, A)$. It is easy to verify that the union G of all open sets U_x , $x \in A$, is disjoint from the union H of all the open sets V_y , $y \in B$. Thus A and B are contained in disjoint open sets G and H .

Example 24: A regular separable topological space is normal. This result is due to A. N. Tichonov [52].

Let R be a regular space with a countable base Σ and let A , B be two disjoint closed sets. For each point $x \in A$ there exists a neighborhood $U_x \in \Sigma$ whose closure \overline{U}_x does not meet B (see B)). Thus there exists a finite or countably infinite sequence of open sets U_1, U_2, \dots , the union of which contains A and the closure of each of which is disjoint from B . Let V_1, V_2, \dots be an analogous sequence for the pair B , A . Define now $G_1 = U_1$, $H_1 = V_1 \setminus \overline{G}_1$

and generally $G_n = U_n \setminus (\overline{H}_1 \cup \dots \cup \overline{H}_{n-1})$, $H_n = V_n \setminus (\overline{G}_1 \cup \dots \cup \overline{G}_n)$. If G denotes the union of the open sets G_1, G_2, \dots and H the union of the open sets H_1, H_2, \dots then it is easy to see that $A \subset G$, $B \subset H$ and that G and H are disjoint.

SECTION 13. COMPACTNESS

Among the most important of the restrictive conditions that are frequently imposed on topological spaces is the condition of compactness first introduced by P. S. Alexandrov, who not only was the first to employ the idea but also gave for it a number of different but mutually equivalent formulations. An important part of the present paragraph is the proof of the equivalence of four different criteria for compactness.

Compactness is the generalization to a general topological space of the well known properties of a closed interval of the number axis: every infinite set in the interval possesses a limit point, every covering of the interval by open intervals contains a finite covering; finally, every decreasing sequence of non-empty closed intervals possesses a non-empty intersection.

To facilitate the definition of compactness we introduce the following terminology:

A) A collection Σ of sets in a space R is called a covering of a set $M \subset R$ if the union of the sets of Σ contains M . A collection Δ of sets of a space R is said to have the finite intersection property if every finite sub-collection of Δ possesses non-empty intersection. A point a of a space R is said to be a complete limit point of a set $M \subset R$ if the intersection of every neighborhood of a with M has cardinal number equal to that of the set M itself.

Definition 19: A topological space R is compact if from every covering of R by open sets it is possible to select a finite covering. A subset $M \subset R$ is compact if it is compact considered as a topological subspace (See Def. 17); clearly a subset is compact when and only when every covering of it by sets open in the space R contains a finite covering. A topological space R is locally compact if every one of its points possesses a neighborhood whose closure is compact.

Theorem 4: The following four conditions are mutually equivalent, so that each of them is equivalent with the compactness of the space R :

- 1) From every covering of R by open sets it is possible to

select a finite covering.

- 2) Every collection of closed subsets of R possessing the finite intersection property has non-empty intersection.
- 3) Every infinite subset of R possesses at least one complete limit point.
- 4) Every transfinite sequence F_0, F_1, \dots of non-empty closed sets in R , satisfying the condition that $F_\alpha \supset F_\beta$ for $\alpha < \beta$, has non-empty intersection.

Proof. We show first that 1) and 2) are equivalent. Let Δ be an arbitrary collection of closed subsets of R possessing the finite intersection property and suppose that Δ has empty intersection. Denote by Σ the collection of all open sets of the form $R \setminus F$ where $F \in \Delta$. Then Σ covers R so that by 1) it is possible to select a finite covering G_1, \dots, G_k from Σ . But then the finite collection of sets $R \setminus G_1, \dots, R \setminus G_k$ belongs to Δ and has empty intersection, thus violating the finite intersection property. Suppose on the other hand that condition 2) is satisfied and let Σ' be an arbitrary covering of R by open sets. Denote by Δ' the collection of all closed sets of the form $R \setminus G$ for $G \in \Sigma'$. Since Σ' is a covering of R the collection Δ' has empty intersection and therefore cannot possess the finite intersection property. It follows that there is a finite subcollection F_1, \dots, F_k in Δ' such that $F_1 \cap \dots \cap F_k = 0$. Thus Σ' contains the finite covering $R \setminus F_1, \dots, R \setminus F_k$.

We next show that 1) implies 3). Let M be an infinite subset of R and suppose that M does not possess a complete limit point, i.e., that for every point $x \in R$ there exists a neighborhood U_x whose intersection with M has cardinality less than that of M . The collection Σ of all such open sets U_x , $x \in R$, covers R so that we may extract from it a finite covering U_{x_1}, \dots, U_{x_k} . Since each of the sets U_{x_i} meets M in a set of cardinality less than that of M we have the set M represented as the union of a finite number of sets each having cardinality less than itself, which is impossible. Thus condition 3) must hold.

We next show that either 3) or 4) implies 2). Indeed, suppose that 2) is not satisfied, i.e., that there exists a collection of closed sets possessing the finite intersection property and having empty intersection, and among all such collections select one, say Δ , with minimal cardinal number m . The cardinal number m is clearly infinite. Denote by ω_m the least transfinite ordinal such that the collection of preceding ordinals has cardinality m , and enumerate the collection Δ by means of the ordinal numbers less than ω_m : $\Delta = \{F_0, F_1, \dots\}$. We then define $E_0 = R$ and for each ordinal number α , $0 < \alpha < \omega_m$ we define E_α to be the intersection of the sets F_β for $\beta < \alpha$. Thus each of the sets E_α ,

$0 < \alpha < \omega_m$ is the intersection of a collection of sets F_β , $\beta < \alpha$, possessing the finite intersection property and having cardinal number $<^m$ so that E_α is non-empty. Moreover, the intersection of all the sets E_α coincides with the intersection of the sets of the original collection Δ and is therefore empty according to our assumption. Thus if 4) holds we have arrived at the desired contradiction. Suppose on the other hand that 3) holds; in this case also we produce a contradiction. To begin with, it is no loss of generality to suppose the sets of the transfinite sequence E_α , $0 \leq \alpha < \omega_m$, to be pair-wise distinct. Indeed, should repetitions occur, then partitioning the sequence into classes of coinciding sets, and choosing in each class the set with the smallest index, yields a transfinite sequence of pair-wise distinct sets indexed by some collection of ordinal numbers $< \omega_m$, and since the intersection of the new family is clearly still the empty set it follows from the minimality of m and ω_m that the new family can then be reindexed by all the ordinal numbers $< \omega_m$ without changing the order. Accordingly, we assume that for any pair of ordinal numbers $0 \leq \alpha < \beta < \omega_m$ the difference $E_\beta \setminus E_\alpha$ is not empty. In particular each E_α of the sequence contains a point x_α which does not belong to the immediately succeeding set $E_{\alpha+1}$. Thus $x_\alpha \neq x_\beta$ for $\alpha < \beta$ and it follows that the set M of all points x_α has cardinal number m . Moreover, since 3) is assumed to hold, M has at least one complete limit point a . We shall show that for every set E_α we have $a \in E_\alpha$. Indeed, the open set $G_\alpha = R \setminus E_\alpha$ contains only points x_β for $\beta < \alpha$ and the cardinal number of the set of all such points is $<^m$. Since a is a complete limit point it follows that $a \notin G_\alpha$, i.e., $a \in E_\alpha$. But then a is in the intersection of all sets E_α , which is contrary to the assumption that the intersection is empty.

Finally, we note that 2) implies 4). Indeed a transfinite sequence F_0, F_1, \dots of non-empty closed sets satisfying the condition $F_\alpha \supset F_\beta$ for $\alpha < \beta$ clearly possesses the finite intersection property so that if 2) holds the intersection of the sequence cannot be empty.

Thus it has been shown that any two of the four given conditions are equivalent and Theorem 4 is proved.

We now discuss certain elementary properties of compact spaces.

B) A closed subset of compact space is compact. A closed subset of a locally compact space is locally compact, considered as a subspace.

Indeed let M be a closed set of the compact space R and let

Σ be a covering of M by open sets of R . Adjoining to Σ the open set $G = R \setminus M$ we obtain a collection Σ' of open sets that covers R and from which can therefore be selected a finite covering Σ'_1 . Deleting, if necessary, the set G from the collection Σ'_1 we arrive at a finite covering of M selected from the given covering Σ .

Next let R^* be a closed set in a locally compact space R and let $a \in R^*$. Select a neighborhood U of a in the space R such that \overline{U} is compact. We shall show that the neighborhood $U^* = U \cap R^*$ of the point a in the space R^* has compact closure \widetilde{U}^* in R^* . Indeed $\widetilde{U}^* = U^* \cap R^*$ is the intersection of two closed subsets of the space R and is itself closed. But also $\widetilde{U}^* \subset \overline{U}$ so that U^* is a closed set in the space \overline{U} . Since the latter is compact it follows from the first part of B) that \widetilde{U}^* is compact too.

C) A compact set in a Hausdorff space is closed (see Def. 18). Indeed, let M be a compact subset of a Hausdorff space R and let $a \in R \setminus M$. Then for each point $x \in M$ there exist disjoint neighborhoods U_x and V_x of the points x and a respectively. The open sets U_x , $x \in M$, constitute a covering of M from which we may select a finite covering U_{x_1}, \dots, U_{x_k} . But then the intersection $V_{x_1} \cap \dots \cap V_{x_k}$ contains a neighborhood V of a which cannot intersect M . Thus a does not belong to \overline{M} and M is closed.

D) A continuous image of a compact space is compact. Indeed, let f be a continuous mapping of a compact space R onto a space R' and let Σ' be an arbitrary covering of R' by open sets. Denote by Σ the covering of R consisting of the sets $f^{-1}(G')$, $G' \in \Sigma'$. From the covering Σ it is possible to select a finite covering G_1, \dots, G_k . But then the open sets $f(G_1), \dots, f(G_k)$ belong to Σ' and constitute a finite covering of R' .

E) A one-to-one continuous mapping of a compact space onto a Hausdorff space has continuous inverse and is therefore a homeomorphism.

Indeed, let f be a continuous and one-to-one mapping of a compact space R onto a Hausdorff space R' . To verify the continuity of the mapping f^{-1} it suffices to show that the image of a closed set F in R under the mapping f is closed in R' (see Section 10, B)). Since R is compact it follows from B) that the closed set F is itself compact and from this in turn it follows from D) that $f(F)$ is compact in R' . Finally, using C), we see that $f(F)$ is closed.

F) A compact Hausdorff space is normal (see Def. 18). Indeed, let R be a compact Hausdorff space. We begin by showing that it is regular. Let a be a point in R and let B be a closed set not containing a . For each point $x \in B$ there exist disjoint neighborhoods U and V of the points a and x , respectively. From the covering

of the compact set B consisting of the open sets V_x , $x \in B$, we select a finite covering V_{x_1}, \dots, V_{x_k} and denote by H the union $V_{x_1} \cap \dots \cap V_{x_k}$. Denote also by G the intersection $U_{x_1} \cap \dots \cap U_{x_k}$. Then G and H are open and disjoint and contain a and B respectively. Thus R is regular.

Now let A and B be two disjoint closed sets in R . As we have just seen, for each $x \in A$ there exist disjoint open sets G_x and H_x such that $x \in G_x$, $B \subset H_x$. From the covering of the compact set A consisting of the open sets G_x , $x \in A$, we select a finite covering G_{x_1}, \dots, G_{x_k} and denote by G the union $G_{x_1} \cup \dots \cup G_{x_k}$. Denote also by H the intersection $H_{x_1} \cap \dots \cap H_{x_k}$. Then G and H are disjoint open sets and $A \subset G$, $B \subset H$.

G) A continuous real function on a compact space is bounded and assumes a greatest and a least value.

Indeed, let f be a continuous mapping of a compact space R into the space D of real numbers. Since the set $f(R) \subset D$ is compact, it is both closed and bounded and therefore contains its upper and lower bounds.

H) Let R be a compact space, let Δ be a system of closed sets in R with intersection F and let G be an open set containing F . Then there exist a finite number of sets of the system Δ the intersection of which is contained in G . If, moreover, Δ has the property that the intersection of any pair of sets in it contains a third set in the same collection, then there must be a set of Δ contained in G .

Consider the system Δ' consisting of all sets of the form $(R \setminus G) \cap A$, $A \in \Delta$. Since the intersection of Δ is F the intersection of the collection Δ' is $(R \setminus G) \cap F$, i.e., is empty, so that the collection Δ' cannot have the finite intersection property. It follows that Δ must contain a finite collection of sets the intersection of which is contained in G . The second assertion of the proposition is an immediate consequence of the first.

Example 25: We here discuss a property of topological spaces which, prior to the introduction of the concept of compactness, received a considerable amount of attention. This property, which we here call countable compactness, is analogous with compactness and may, like it, be formulated in four different ways:

- From every countable covering of a space R by open sets it is possible to select a finite covering.
- Every countable collection of closed subsets of R possessing the finite intersection property has non-empty intersection.
- Every countable (and therefore every infinite) subset of R possesses at least one limit point.

d) Every sequence F_1, F_2, \dots of non-empty closed sets in R indexed by the natural numbers and satisfying the condition $F_i \supset F_j$ for $i < j$ has non-empty intersection.

A proof of the equivalence of these conditions may be modeled on that of Theorem 4; matters are somewhat simpler, in fact, since the definitions by transfinite induction are replaced by ordinary inductive definitions.

A space is said to be locally countably compact if every point possesses a neighborhood having countably compact closure.

We give a proof of the fact that a countably compact separable space R is compact.

To this end let Ω be a countable base for the space R and let Σ be an arbitrary collection of open sets covering R . Each of the open sets of Σ may be written as the union of certain open sets of the system Ω . Thus, denoting by Ω' the collection of all sets of the basis Ω , each of which is a subset of at least one of the open sets of Σ , we obtain a countable covering Ω' . Since R is countably compact the covering Ω' contains a finite covering U_1, \dots, U_k . But by construction each of the sets U_i is contained in some open set $G_i \in \Sigma$ and the sets G_1, \dots, G_k thus obtained constitute a finite open covering of R selected from the covering Σ .

Example 26: A countably compact metric space is always separable and is therefore compact (see Exs. 20, 25).

Let R be a countably compact metric space. We begin by constructing in R a finite ϵ -net, i.e., a finite set N_ϵ such that each point $x \in R$ is at distance less than ϵ from some point of N_ϵ . To show that such a set exists, suppose the contrary and employ mathematical induction. Suppose already constructed a finite sequence a_1, \dots, a_n of points, the distance between each pair of which is at least ϵ . Since the sequence a_1, \dots, a_n does not itself constitute an ϵ -net, there exists a point a_{n+1} whose distance from each of the points a_1, \dots, a_n is at least ϵ . Thus the assumption that no finite ϵ -net exists in R leads inductively to the construction of a sequence of points a_1, a_2, \dots each two of which are at distance $\geq \epsilon$ from one another. Since this is impossible in a countably compact space, it follows that a finite ϵ -net N_ϵ exists. Next, constructing ϵ -nets for $\epsilon = 1, 1/2, 1/3, \dots$ and forming their union, we obtain a countable everywhere dense set. Finally, the set of all spheres with rational radii and with centers at the points of a countable everywhere dense set is easily seen to constitute a countable base.

It is worth mentioning that, in general, a topological space may very well possess a countable everywhere dense set without

at the same time possessing a countable base.

SECTION 14. PRODUCTS OF TOPOLOGICAL SPACES

The topological product or, briefly, product of topological spaces is an analog of the direct product of groups; it provides a way of constructing a new topological space from given ones as well as a way of reducing the investigation of complicated spaces to the investigation of simpler ones. The best known example of a topological product is the plane, considered as the collection of all pairs of real numbers; so regarded, the plane appears as the product of two number axes. The present paragraph is devoted to the definition of the concept of the product of spaces and to the study of the basic properties of products. The definition will be given first for two factors in a form which generalizes in obvious fashion to any finite number of factors. Subsequently a definition will be given of the product of an arbitrary collection of factors. The latter concept, due to A. N. Tichonov, turns out to be most useful in connection with compact spaces.

A) Let R_1 and R_2 be two topological spaces. Denote by T the set of all pairs (x_1, x_2) for $x_1 \in R_1$, $x_2 \in R_2$. If $M_1 \subset R_1$, $M_2 \subset R_2$ we denote by (M_1, M_2) the subset of T consisting of all pairs (x_1, x_2) , $x_1 \in M_1$, $x_2 \in M_2$. Starting from bases Σ_1 and Σ_2 in the spaces R_1 and R_2 , respectively, we construct a base Σ defining a topology in the set T . The collection Σ is defined to consist of the collection of all sets (U_1, U_2) where $U_1 \in \Sigma_1$, $U_2 \in \Sigma_2$. It turns out that Σ satisfies the conditions of Theorem 3 and accordingly turns T into a topological space; moreover the topology thus defined in T does not depend upon the choice of the bases Σ_1 , Σ_2 but is uniquely determined by the spaces R_1 , R_2 . The space T thus obtained is called the topological product or briefly the product of R_1 and R_2 : $T = R_1 \times R_2$. If G_1 and G_2 are open sets in R_1 and R_2 then (G_1, G_2) is open in T while if F_1 and F_2 are closed in R_1 , R_2 then (F_1, F_2) is closed in T . Finally if R_1^* and R_2^* are subspaces of R_1 and R_2 then their product $R_1^* \times R_2^*$ is naturally homeomorphic with the subspace (R_1^*, R_2^*) of T .

We show first that Σ satisfies the conditions of Theorem 3. Let (x_1, x_2) and (y_1, y_2) be two distinct points of T . Since they are distinct at least one of the inequalities $x_1 \neq y_1$, $x_2 \neq y_2$ must hold. For the sake of definiteness suppose that $x_1 \neq y_1$. Then there exists a neighborhood U_1 of x_1 not containing y_1 . If U_2 is an arbitrary neighborhood of x_2 in R_2 then (U_1, U_2) is a neighborhood of (x_1, x_2) in T which does not contain (y_1, y_2) . Thus condition a) is satisfied. Next let (U_1, U_2) and

(V_1, V_2) be two neighborhoods of a point (x_1, x_2) . There exists then a neighborhood W_1 of x_1 contained in $U_1 \cap V_1$ and a neighborhood W_2 of x_2 contained in $U_2 \cap V_2$. The neighborhood (W_1, W_2) of (x_1, x_2) is obviously contained in $(U_1, U_2) \cap (V_1, V_2)$. Thus both conditions of Theorem 3 are satisfied. With equal ease it may be shown that if Σ' is the base obtained in similar fashion starting from bases Σ'_1 and Σ'_2 equivalent, respectively, with Σ_1 and Σ_2 , then Σ and Σ' are themselves equivalent.

If $(x_1, x_2) \in (G_1, G_2)$ then $x_1 \in G_1$, $x_2 \in G_2$ and since G_1 and G_2 are open there exist neighborhoods U_1 and U_2 of x_1 and x_2 such that $U_1 \subset G_1$, $U_2 \subset G_2$. But then $(x_1, x_2) \in (U_1, U_2) \subset (G_1, G_2)$, which shows that (G_1, G_2) is open in T . If F_1 and F_2 are closed sets then their complements $G_1 = R_1 \setminus F_1$ and $G_2 = R_2 \setminus F_2$ are open and it is easy to verify that the complement of (F_1, F_2) in T may be represented as the union $(R_1, G_2) \cup (G_1, R_2)$ which, according to the preceding remark, is the union of two open sets and therefore itself open in T . Thus (F_1, F_2) is closed.

To each point (x_1, x_2) of the product $R_1^* \times R_2^*$ we associate the point (x_1, x_2) of the product $R_1 \times R_2$. Employing proposition C) of Section 11, it is easy to verify that this mapping of $R_1^* \times R_2^*$ onto the subspace (R_1^*, R_2^*) of $R_1 \times R_2$ is a homeomorphism.

We now give a definition of product applicable to an arbitrary collection of factors and coinciding in the case of two factors with the concept of product just defined.

Definition 20: Let Ω be an arbitrary collection to topological spaces. We consider functions α associating with each space $R \in \Omega$ a point $\alpha(R) \in R$ and denote by T the collection of all such functions. It will be convenient to employ the notation $\alpha(R) = R(\alpha)$ so that the letter R is used not only to denote a topological space but also to denote the "projection" of T onto that space. According to this notational convention, if $M \subset R$ then $R^{-1}(M)$ is a well defined subset of T . We now define a topology in T by defining a base Σ : the general neighborhood $U \in \Sigma$ we take to be the set $U = R_1^{-1}(U_1) \cap \dots \cap R_k^{-1}(U_k)$ where R_1, \dots, R_k is an arbitrary finite subcollection of the collection Ω and, for $i = 1, \dots, k$, U_i denotes an arbitrary neighborhood in the space R_i . It turns out that the system Σ thus defined satisfies the conditions of Theorem 3 and is therefore a complete system of neighborhoods turning T into a topological space. Moreover the topology thus defined does not depend upon the choice of bases in the various spaces of the collection Ω but is uniquely determined by those spaces themselves. The topological space T thus obtained is called the topological product or briefly the product of the collection Ω .

As before we shall show only that the system Σ satisfies the conditions of Theorem 3; the proof that the topology thus obtained is independent of the choice of bases in the various factors is equally simply and may be omitted. Let α and β be two distinct points of T . Then there exists a space $R_1 \in \Omega$ for which $\alpha(R_1) \neq \beta(R_1)$. Let U_1 be a neighborhood of the point $\alpha(R_1)$ in R_1 not containing $\beta(R_1)$. Then $U = R_1^{-1}(U_1)$ is a neighborhood of the point α in T that does not contain β . Thus a) holds. Turning to condition b), we observe first that a neighborhood U defined in terms of some finite number of spaces R_1, \dots, R_k of the collection Ω may also be defined in terms of any larger finite set of factors by adding in an arbitrary number of other spaces R_{k+1}, \dots, R_l selected from Ω and letting $U_{k+1} = R_{k+1}, \dots, U_l = R_l$. Accordingly if U and V are two neighborhoods of a point α in T we may, without loss of generality, suppose that both are defined in terms of the same collection of factors R_1, \dots, R_k ;

$$U = R_1^{-1}(U_1) \cap \dots \cap R_k^{-1}(U_k), \quad V = R_1^{-1}(V_1) \cap \dots \cap R_k^{-1}(V_k)$$

Denoting by W_1 a neighborhood of the point $\alpha(R_1)$ contained in the intersection $U_1 \cap V_1$ and denoting further by W the intersection $W = R_1^{-1}(W_1) \cap \dots \cap R_k^{-1}(W_k)$, we obtain a neighborhood of α such that $W \subset U \cap V$. Thus the conditions of Theorem 3 are both satisfied and the system Σ may be taken as a complete system of neighborhoods.

The following property of products is extremely simple but nevertheless of great importance:

B) A product of Hausdorff spaces is Hausdorff.

Indeed, let T be the product of a collection Ω of Hausdorff spaces and let α and β be two distinct points of T . Then there exists a factor R_1 such that $\alpha(R_1) \neq \beta(R_1)$ and since R_1 is Hausdorff it contains disjoint neighborhoods U_1, V_1 of the points $\alpha(R_1), \beta(R_1)$. But then $U = R_1^{-1}(U_1)$ and $V = R_1^{-1}(V_1)$ are disjoint neighborhoods of α and β in T .

We turn next to the important and non-trivial theorem of Tichonov.

Theorem 5: The product of an arbitrary collection of compact spaces is compact.

We preface the proof of the theorem with two propositions, C) and D), which, taken together, provide a slight reformulation

of one of the definitions of compactness, viz., condition 2) of Theorem 4.

C) In order that a topological space should be compact it is necessary and sufficient that an arbitrary collection of subsets of the space having the finite intersection property should possess a common adherent point (see Def. 12).

Indeed, let R be a space satisfying the given condition and let Δ be an arbitrary system of closed sets in R having the finite intersection property. By hypothesis there is a point $a \in R$ which is simultaneously an adherent point of all of the sets of Δ . Since the sets are assumed to be closed, it follows that a belongs to each of them so that their intersection is not empty. Accordingly R is compact. On the other hand, if R is a compact space and if Δ is an arbitrary collection of subsets of R having the finite intersection property, consider the collection $\bar{\Delta}$ consisting of all sets of the form \bar{M} for $M \in \Delta$. Clearly the new system also has the finite intersection property so that there must be a point a common to all the sets of $\bar{\Delta}$. But then a is a common adherent point of all of the sets of the original system Δ .

D) A collection of sets having the finite intersection property is said to be maximal if it is impossible to adjoin any new set to the collection without destroying the finite intersection property. Obviously a collection of sets maximal with respect to the finite intersection property is multiplicative, i.e., the intersection of any two members of the collection is itself a member of the collection. It turns out that any collection of sets with the finite intersection property is contained in a maximal such collection. Thus we may say that, in order that the topological space should be compact, it is necessary and sufficient that every collection of sets maximal with respect to the finite intersection property should possess a common adherent point.

We must show that if Δ is a collection of sets in a space R having the finite intersection property then there exists another collection Δ' maximal with respect to the finite intersection property and satisfying the condition $\Delta' \supset \Delta$. Enumerate all of the subsets of R in a single transfinite sequence M_0, M_1, \dots using as indices all ordinal numbers less than some ordinal number θ . We proceed to define inductively a non-decreasing transfinite sequence $\Delta'_0, \Delta'_1, \dots$ of collections of sets having the finite intersection property. To begin with, let $\Delta_0 = \Delta$ and suppose collections Δ_α already defined for all ordinals α less than some ordinal number β . Since for $\alpha < \beta$ the collections Δ_α form a non-decreasing sequence and since each of them has the finite intersection property it is easy to see that their union Δ'_β also has this property. Adjoining to Δ'_β the

set M_β we obtain a new system Δ''_β . If this enlarged system still has the finite intersection property then we define $\Delta_\beta = \Delta''_\beta$; otherwise we define $\Delta_\beta = \Delta'_\beta$. There is no difficulty in showing that by continuing the construction through all numbers $\beta < \theta$, and taking the union of the collection of sets thus obtained, we arrive at a collection of sets maximal with respect to the finite intersection property.

Proof of Theorem 5: Let Ω be a collection of compact topological spaces, let T denote their product, and let Δ be any collection of subsets of T maximal with respect to the finite intersection property. According to D) we have but to show that the sets of the system Δ possess a common adherent point. For each $R \in \Omega$ denote by $R(\Delta)$ the collection of subsets of the space R of the form $R(M)$ where $M \in \Delta$. The collection $R(\Delta)$ possesses the finite intersection property along with Δ and therefore possesses a common adherent point $\alpha(R)$ since R is compact by hypothesis. We shall show that this point $\alpha \in T$ is a common adherent point of the collection Δ . To this end let U be a neighborhood of α , say $U = R_1^{-1}(U_1) \cap \dots \cap R_k^{-1}(U_k)$. Since $\alpha(R_i)$ is an adherent point of each of the sets of the collection $R_i(\Delta)$, the neighborhood U_i must meet every set of the collection $R_i(\Delta)$ and it follows that the neighborhood $R_i^{-1}(U_i)$ meets every set of the collection Δ . But then the set $R_i^{-1}(U_i)$ actually belongs to Δ . To show this it suffices to show that the system Δ_i obtained by adjoining to Δ the single set $R_i^{-1}(U_i)$ retains the finite intersection property, since Δ is maximal. Let M_1, \dots, M_s be an arbitrary finite collection of sets in Δ . Since Δ is multiplicative the intersection $M = M_1 \cap \dots \cap M_s$ also belongs to Δ and consequently the intersection $M_1 \cap \dots \cap M_s \cap R_i^{-1}(U_i) = M \cap R_i^{-1}(U_i)$ is non-empty. Thus Δ has the finite intersection property and $R_i^{-1}(U_i) \in \Delta$. But if each of the sets $R_i^{-1}(U_i)$, $i = 1, \dots, k$ belongs to Δ then, since Δ is multiplicative, their intersection U must also be an element of Δ , from which it follows that U has non-empty intersection with every set of the collection Δ . This shows that the point α is indeed an adherent point of all of the sets of Δ and Theorem 5 is proved.

The following result is an immediate consequence of Theorem 5:

E) The product of a finite number of locally compact spaces is locally compact.

It suffices to prove the theorem for a product of two locally compact spaces R_1 and R_2 . Let (x_1, x_2) be an arbitrary point of $R_1 \times R_2$ and let U_1 be a neighborhood of x_1 in R_1 such that the closure \bar{U}_1 is compact, $i = 1, 2$. Since $(U_1, U_2) \subset (\bar{U}_1, \bar{U}_2)$ and

since $(\overline{U_1}, \overline{U_2})$ is closed it follows that $(\overline{U_1}, \overline{U_2}) \subset (\overline{\overline{U_1}}, \overline{\overline{U_2}})$. But the set $(\overline{U_1}, \overline{U_2})$ is the product of two compact spaces and is therefore compact by Theorem 5. Hence the closed subset $(\overline{U_1}, \overline{U_2})$ is also compact and it follows that $R_1 \times R_2$ is locally compact.

The following theorem, also due to A. N. Tichonov, finds no application in the theory of topological groups but is of sufficient importance that, for the sake of completeness of the treatment of compact spaces, I here give a proof of it. To facilitate the statement of the theorem we first introduce the space R_t .

F) Let t be an arbitrary infinite cardinal number and let Γ be any set having cardinal number t . To each element $\gamma \in \Gamma$ we associate a copy I_γ of the unit interval of real numbers $0 \leq t_\gamma \leq 1$, and denote by R_t the product of all the spaces I_γ , $\gamma \in \Gamma$. The space thus defined is determined up to homeomorphism by t . A point $t \in R_t$ may be viewed as a real valued function associating with each element $\gamma \in \Gamma$ the real number $t(\gamma) = t_\gamma$. Since each of the spaces I_γ is a compact Hausdorff space it follows that R_t is also compact and Hausdorff.

Theorem 6: Every completely regular topological space R of weight t is homeomorphic with some subspace of the space R_t (see Defs. 18 and 14).

Proof. If t is finite then R consists of a finite number of points and the theorem is obvious. Let Σ be a base for R having the infinite cardinal number t . A pair of neighborhoods $G, H \in \Sigma$ will be said to be distinguished if there exists a continuous real function f defined on R and satisfying the conditions

$$0 \leq f(x) \leq 1 \text{ for } x \in R;$$

$$f(x) < \frac{1}{2} \text{ for } x \in G; \quad f(x) = 1 \text{ for } x \in R \setminus H. \quad (1)$$

For any neighborhood H of a point a there exists a neighborhood G of the same point such that the pair G, H is distinguished. Indeed, since R is completely regular there exists a continuous real function f defined on R and satisfying the conditions: $0 \leq f(x) \leq 1$ for $x \in R$; $f(a) = 0$; $f(x) = 1$ for $x \in R \setminus H$. Denote by G' the set of points $x \in R$ for which $f(x) < 1/2$. Since G' is open in R and contains a there exists a neighborhood G of a contained in G' and the neighborhoods G, H form a pair of the desired sort. Since we assume t to be infinite it follows that the cardinal number of the set of all distinguished pairs is also equal to t . Accordingly the collection of distinguished pairs can be put in one-to-one correspondence

with the set Γ . For each $\gamma \in \Gamma$ denote by G_γ, H_γ , the distinguished pair associated with γ and let f_γ be a fixed but arbitrary function on R satisfying condition 1) with respect to the pair G_α, H_α .

We now associate with each point $x \in R$ the point $t = \varphi(x) \in R_t$ defined by the equation $t(\gamma) = f_\gamma(x)$ and show that φ is a one-to-one and both ways continuous mapping of the space R onto the subspace $S = \varphi(R) \subset R_t$.

To begin with, let a and b be distinct points of R and let H be a neighborhood of a not containing b . Let also G be a neighborhood of a such that G, H forms a distinguished pair. Then for some γ we have $G = G_\gamma, H = H_\gamma$ and since f_γ assumes different values at a and b ($f_\gamma(a) < 1/2, f_\gamma(b) = 1$) it follows that $\varphi(a) \neq \varphi(b)$.

In order to show that φ is continuous let $U = I_{\gamma_1}^{-1}(U_{\gamma_1}) \cap \dots \cap I_{\gamma_k}^{-1}(U_{\gamma_k})$ be an arbitrary neighborhood of the point $\varphi(a)$, $a \in R$. Since the functions $f_{\gamma_1}, \dots, f_{\gamma_k}$ are continuous, there exists a neighborhood V of a such that $f_{\gamma_i}(x) \in U_{\gamma_i}$ for $x \in V$, $i = 1, \dots, k$. But then clearly $\varphi(V) \subset U$.

It remains to show that the mapping φ^{-1} of S onto R is continuous. Let $\varphi(a)$, $a \in R$, be any point of S , let H be an arbitrary neighborhood in R of the point a and let G be another neighborhood of a such that the pair G, H is distinguished. Select γ such that $G = G_\gamma, H = H_\gamma$. Finally let U_γ denote the open set of the interval I_γ consisting of all numbers less than $1/2$. Then $\varphi^{-1}(U) \subset H$ where $U = I_\gamma^{-1}(U_\gamma)$ and the continuity of φ^{-1} is established. Thus Theorem 6 is proved.

Theorem 7, which follows, will be employed in Chapter V, in connection with the theory of integral equations on a compact topological group, to establish the possibility of approximating a continuous kernel in an integral equation by "degenerate kernels." Prior to stating the theorem we give the definition of a continuous function of two variables; the definition extends in obvious fashion to functions of an arbitrary finite number of variables.

G) Let R and S be two topological spaces and let f be a real valued function of the two variables $x \in R$ and $y \in S$. Then f may be viewed as a mapping of the product $R \times S$ into the space D of real numbers that associates with each pair $(x, y) \in R \times S$ the real number $f(x, y)$. The function f is said to be a continuous function of the two variables x, y if this mapping is continuous. It is easy to verify that the function f is continuous when, and only when, for each pair $a \in R, b \in S$ and for every positive number ϵ there exist neighborhoods U and V of the points a and b such that for $x \in U, y \in V$ we have $|f(x, y) - f(a, b)| < \epsilon$ (see Section 12, A)).

Theorem 7. Let R and S be compact Hausdorff spaces and let h be a continuous real function of the two variables $x \in R$, $y \in S$. Then for every $\epsilon > 0$ there exists a natural number n , continuous real functions f_1, \dots, f_n defined on R , and corresponding continuous real functions g_1, \dots, g_n defined on S such that

$$|h(x, y) - \sum_{i=1}^n f_i(x)g_i(y)| < \epsilon \quad (1)$$

for all $x \in R$, $y \in S$.

Proof. We give the proof as a series of lemmas.

a) Let ξ denote a real variable varying over the segment $-\alpha \leq \xi \leq \alpha$; we begin by showing that the function $|\xi|$ may be developed on the given segment in a uniformly convergent series of polynomials or, what comes to the same thing, that it may be uniformly approximated by polynomials.

Consider the function $\sqrt{1 - \xi^2}$ of the real variable ξ . For $-1 < \xi < 1$ this function may be expanded in a binomial series:

$$\sqrt{1 - \xi^2} = 1 - \sum_{k=1}^{\infty} \alpha_k \xi^k, \quad (2)$$

where

$$\alpha_1 = \frac{1}{2}, \quad \alpha_k = \frac{1 \cdot 3 \dots (2k-3)}{2 \cdot 4 \dots 2k}, \quad k \geq 2.$$

Since all the coefficients α_k are positive and the series (2) converges to a non-negative number for $0 \leq \xi < 1$, it follows that for $0 \leq \xi < 1$ and for arbitrary r we have: $\sum_{k=1}^r \alpha_k \xi^k \leq 1$. Consequently

$\sum_{k=1}^r \alpha_k \leq 1$ holds for every r , and from this follows that the series

(2) converges uniformly to $\sqrt{1 - \xi^2}$ on the entire interval $-1 \leq \xi \leq 1$. But now for $-\alpha \leq \xi \leq \alpha$ we have

$$|\xi| = \sqrt{1 - \left(1 - \frac{\xi^2}{\alpha^2}\right)}.$$

Accordingly, upon multiplying (2) by α and substituting $\xi = 1 - \frac{\xi^2}{\alpha^2}$ we obtain an expression for the function $|\xi|$ on the interval $-\alpha \leq \xi \leq \alpha$ as a uniformly convergent series of polynomials.

b) Let η_1, \dots, η_s be real variables. Consider the function m of these variables which has for its value $m(\eta_1, \dots, \eta_s)$ the

largest of the numbers η_1, \dots, η_s . The function m can be uniformly approximated by polynomials in an arbitrary cube $-\beta \leq \eta_i \leq \beta$, $i = 1, \dots, s$.

It suffices to give the proof for two variables; the stated result then follows by an easy induction. But for $s = 2$ a simple computation shows that $m(\eta_1, \eta_2) = \frac{1}{2}|\eta_1 - \eta_2| + \frac{1}{2}(\eta_1 + \eta_2)$. Since we have just shown that the function $|\eta_1 - \eta_2|$ can be uniformly approximated by polynomials it follows at once that the same is true of the function m .

c) Let T be a compact Hausdorff, and therefore normal, topological space with a fixed base Σ . As before we call a pair W, W' of neighborhoods in the base Σ distinguished if $\overline{W} \subset W'$. By a Urysohn function for the distinguished pair W, W' we shall mean a continuous real function w defined on T taking the value 0 on $T \setminus W'$, the value 1 on W , and satisfying the condition $0 \leq w(z) \leq 1$ for all $z \in T$. Associating with each distinguished pair a fixed but arbitrary Urysohn function (see Urysohn's Lemma in Section 12) we obtain a collection Ω of functions which we shall call a complete system of Urysohn functions for the space T . It turns out that an arbitrary continuous real function h defined on T can be uniformly approximated by means of polynomials in the functions belonging to the set Ω .

Since an arbitrary continuous real function defined on T differs from a positive function by an additive constant (see Section 13, G)) it is no loss of generality to assume that the given function h is positive. Let δ be any positive number. For each point $c \in T$ select a neighborhood $W'_c \in \Sigma$ such that for $z \in W'_c$ we have

$|h(z) - h(c)| < \frac{\delta}{2}$ and then select another neighborhood $W_c \in \Sigma$ of the point c such that $\overline{W}_c \subset W'_c$. Then Ω contains a Urysohn function w_c associated with the distinguished pair W_c, \overline{W}_c and if we denote by h_c the minimum of the function h on the set \overline{W}_c it is obvious that

$$h_c w_c(z) \leq h(z) \text{ for } z \in T,$$

$$h(z) \leq h_c w_c(z) + \delta, \text{ for } z \in W_c. \quad (3)$$

Now the collection of neighborhoods W_c , $c \in T$, covers T . Select a finite covering W_{c_1}, \dots, W_{c_s} and define $h'(z) = m(h_{c_1} w_{c_1}(z), \dots, h_{c_s} w_{c_s}(z))$. Then it follows from (3) that $|h(z) - h'(z)| < \delta$ and since, by b), it is possible to approximate the function m uniformly by means of polynomials, the proof of c) is complete.

d) Finally, to prove Theorem 7, select complete systems of

Urysohn functions Ω' and Ω'' on the given topological space R and S . It is easy to see that the set Ω of all functions of the form $w(x, y) = u(x)v(y)$, where $u \in \Omega'$, $v \in \Omega''$ is a complete system of Urysohn functions on the space T . Thus, since an arbitrary polynomial of functions of the form $u(x)v(y)$ has the form

$$\sum_{i=1}^n f_i(x)g_i(y), \text{ Theorem 7 follows from c).}$$

Example 27: Consider the space R_t (see F)) when the cardinal number t is countably infinite. In this case we may select for the set Γ the collection of all natural numbers so that the points $t \in R_t$ are ordinary infinite sequences of real numbers: $t = (t_1, t_2, \dots, t_n\dots); 0 \leq t_n \leq 1, n = 1, 2, \dots$. We associate with each $t \in R_t$ a point

$x = \psi(t)$ of Hilbert space H (see Ex. 20) by defining $x_n = \frac{1}{n} t_n$, where

x_1, x_2, \dots are the coordinates of the point x in H . It is a simple task to show that ψ is a homeomorphic mapping of R_t onto the subspace $Q = \psi(R_t) \subset H$ consisting of all sequences $x = (x_1, x_2, \dots)$ which satisfy the condition $0 \leq x_n \leq \frac{1}{n}, n = 1, 2, \dots$. The space Q , known as the Hilbert parallelopiped, is compact. Since a regular separable space is normal (see Ex. 24) and therefore completely regular we see that, in the case of countably infinite t , Theorem 6 reduces to the well known metrization theorem of Urysohn:

A regular separable space is homeomorphic with a subspace of the Hilbert parallelopiped and is in particular metrizable.

Example 28: We give an example of a countably compact space which is not compact (see Ex. 25). To this end consider the space R_t where t is not countable. We define a subspace R_t^* as follows: the point $t \in R_t$ belongs to R^* when and only when all but a countable number of its coordinates t_γ are equal to 0. Then for any countable subset M of R_t^* , since each point $t \in M$ has only a countable number of coordinates distinct from 0, it is possible to select a sequence $\gamma_1, \gamma_2, \dots$ of elements of Γ such that if t is a point belonging to M and if t_γ is one of its coordinates different from 0 then γ belongs to the sequence $\gamma_1, \gamma_2, \dots$. Now the product R of the intervals $I_{\gamma_1}, I_{\gamma_2}, \dots$ may, in a natural way, be viewed as a subspace of the space R^* and since R is compact it follows that the set M has a limit point in R^* . Thus we have shown that R^* is countably compact. On the other hand,

it is easy to verify that R_t^* is everywhere dense in R_t while clearly $R_t^* \neq R_t$ since t is not countable. This shows that R_t^* is not closed in R_t and hence, since R_t is a Hausdorff space, that R_t^* cannot be compact (see Section 13, C)).

SECTION 15. CONNECTEDNESS

Another of the restrictive conditions that a topological space may be required to satisfy is the condition of connectedness, to the study of which the present paragraph is devoted.

A) A topological space R is said to be connected if it is impossible to partition it into the union of two non-empty disjoint closed sets A and B . Clearly this definition could also be formulated as follows: a topological space R is connected if it is impossible to partition it into the union of two non-empty disjoint open sets A and B .

Applying this definition to a subspace we obtain the definition of a connected set: a subset M of the space R is connected if it is connected as a subspace.

It is frequently convenient to employ the following criterion for the connectedness of a set:

B) A subset M of the space R is connected if it is impossible to partition it into the union of two non-empty disjoint sets A and B such that the intersection $(\overline{A} \cap \overline{B}) \cap M$ is empty. Clearly this agrees with the definition given in A) in the event that $M = R$.

C) Let Δ be an arbitrary collection of connected subsets of a space R , each of which contains the point a . Then the union M of the sets belonging to Δ is also connected.

Suppose, on the contrary, that M can be partitioned into the union of two non-empty disjoint sets A and B such that $(\overline{A} \cap \overline{B}) \cap M$ is empty. Let $a \in A$ and let b be any point in B . Finally let P be some set of the collection Δ that contains b and write $A' = A \cap P$, $B' = B \cap P$. Then A' and B' are non-empty disjoint sets whose union coincides with P . Moreover $\overline{A'} \subset \overline{A}$, $\overline{B'} \subset \overline{B}$ and $P \subset M$ so that $(\overline{A'} \cap \overline{B'}) \cap P \subset (\overline{A} \cap \overline{B}) \cap M$. Since the right member of the last relation is empty the left member must be empty also. Thus P is disconnected, and we have a contradiction.

D) Let a be any point of the topological space R . Then there exists a maximal connected subset K of R containing the point a . The maximality of K is here understood to mean that every connected subset of R which contains a is necessarily a subset of K . The set K is automatically closed and is called the component of a in the space R . It is clear that the component K of a is

simultaneously the component of every other point belonging to K . For this reason it is also customary to call K simply a component of R . If all the components of R are one point sets then R is said to be totally disconnected.

Let Δ be the collection of all connected subsets of R containing a . The union K of the collection Δ is connected, according to C), and is the maximal connected set containing the point a by its very construction. It remains only to show that K is closed. And to this end it suffices to show that \bar{K} is connected for then, by maximality, it will follow that $\bar{K} \subset K$ and consequently $\bar{K} = K$. Suppose on the contrary that \bar{K} is disconnected and partition it into the union of two disjoint sets A and B such that $\bar{A} \cap \bar{B} \cap \bar{K}$ is empty. Let $A' = A \cap K$, $B' = B \cap K$. We suppose without loss of generality that $a \in A'$ and show that B' must then be empty. Indeed if $B' \neq \emptyset$ then A' , B' would provide a partition of K into the union of two non-empty disjoint sets which would contradict the connectedness of K , for $A' \cap B' \cap K \subset \bar{A} \cap \bar{B} \cap \bar{K}$ and the latter set is empty by hypothesis. Thus B' is empty and therefore $K \subset A$. But then $\bar{A} \cap \bar{B} \cap \bar{K} \supset \bar{K} \cap \bar{B} \cap \bar{K} = \bar{K} \cap \bar{B} \supset \bar{K} \cap B = B$. Thus $B = \emptyset$, contrary to assumption.

E) If g is a continuous mapping of a connected space R onto a space R' then R' is also connected.

Suppose the contrary and partition R' into two non-empty disjoint closed sets E' and F' . Then the inverse images E and F of these sets partition R in exactly similar fashion, which contradicts the connectedness of R .

The following proposition, first established by M. R. Šura-Bura, finds application in the investigation of totally disconnected topological groups (see Section 22).

F) Every component of a compact Hausdorff space is the intersection of all the closed-open sets containing it (by closed-open set we here mean, of course, a set that is simultaneously closed and open).

We prove proposition F). Let R be a compact Hausdorff space, let K be any one of its components, and denote by L the intersection of all closed-open subsets of R that contain K . In order to show that $K = L$ it suffices to prove that L is connected. Suppose the contrary. Then L may be partitioned into the union of two non-empty disjoint closed sets A and B . Since K is connected it must be contained either in A or B ; suppose, without loss of generality, that $K \subset A$. Since R is normal (see Section 13, F)) there exist disjoint open sets G and H in R such that $A \subset G$, $B \subset H$. Then also, of course, $L \subset G \cup H$. Now the collection of all closed-open sets containing K is multiplicative and,

since L is the intersection of the collection, it follows that there must be a closed-open set P such that $L \subset P \subset G \cup H$ (see Section 13, H)). It is easy to see that the sets $G' = P \cap G$ and $H' = P \cap H$ are also closed-open sets in R . Finally since $K \subset A$ we see that G' is a closed-open set containing K but not containing L , which contradicts the construction of L .

As an immediate consequence of F) we obtain the following proposition, which is also of use in the theory of topological groups.

G) Let R be a locally compact Hausdorff space and let K be a compact component of R . Then for any open set G containing K there exists a compact-open set P such that $K \subset P \subset G$.

For each $x \in K$ select a neighborhood U_x such that \bar{U}_x is compact and contained in G . From the covering of K consisting of the sets U_x , $x \in K$, select a finite covering and denote by U the union of the open sets U_x in this finite covering. Then \bar{U} is compact, contains K , and is contained in G . Clearly K is also a component of the subspace \bar{U} . Since the collection of all closed-open subsets of \bar{U} that contain K is multiplicative and has intersection K , there exists a closed-open set P of the space \bar{U} such that $K \subset P \subset U$. The set P is the desired compact-open subset of R .

The following concept, intimately related to connectedness, also finds application in the theory of topological groups (see Section 38).

H) A topological space is locally connected if for every point a and every neighborhood U of a there exists a neighborhood V of a such that $V \subset U$ and such that for every point $x \in V$ there exists in U a connected set containing both a and x . It is easy to see that the image of a locally connected space under an open continuous mapping is itself locally connected (see Section 10, E)).

SECTION 16. DIMENSION

The concept of the dimension of a space plays an essential role throughout mathematics and is particularly important in topology. We here give a definition of dimension and derive those basic properties of the concept needed in the theory of topological groups.

To facilitate the definition of dimension we first introduce some terminology.

A) Let Σ be a finite system of subsets of a set M . For each $x \in M$ denote by $r(x)$ the number of sets of the system Σ that contain x . The maximum of the function r thus defined on M is called the multiplicity of Σ . Also, another system Σ' of subsets of M is

said to be a refinement of Σ , or to refine Σ , if for every $A' \in \Sigma'$ there exists a set $A \in \Sigma$ such that $A' \subset A$. It turns out that for any finite covering Ω of compact Hausdorff space R by open sets there exists a finite covering Δ of R by closed sets that refines Ω . Moreover we can always arrange things so that the multiplicity of Δ does not exceed that of Ω .

Indeed, each point $x \in R$ is contained in a neighborhood U_x , the closure \bar{U}_x of which is contained in some one of the open sets of the collection Ω . Selecting from the covering U_x , $x \in R$, a finite covering, we obtain a finite covering Δ of the space R consisting of closed sets of the form \bar{U}_x and this covering refines Ω . Now denote by F_u the union of all sets of Δ that are contained in the open set $U \in \Omega$. Then the collection of closed sets F_u , $U \in \Omega$, constitutes another covering Δ' of R that also refines Ω and the multiplicity of Δ' does not exceed the multiplicity of Ω .

Definition 21: A compact Hausdorff space R has dimension $n \geq 0$ if the following two conditions are satisfied: 1) For every finite covering of R by open sets there exists a finite covering Δ by closed sets that refines the given covering and has multiplicity $\leq n + 1$. 2) There exists a finite covering of R by open sets such that every finite covering Δ by closed sets that refines it has multiplicity $> n$. Clearly these conditions can be satisfied for at most one non-negative integer n . In the event that no n exists satisfying the given conditions we shall say that R has dimension infinity.

The main justification of the definition is the following theorem, the proof of which (see [47]) will not be given here since it is complicated and requires apparatus foreign to the main interests of this book. By the n -dimensional Euclidean cube is here meant the set of points in n -dimensional Euclidean space whose coordinates satisfy the inequalities $0 \leq x_i \leq 1$, $i = 1, \dots, n$.

Theorem 8: The dimension (in the sense of Def. 21) of the n -dimensional Euclidean cube is n .

We turn now to the proof of some properties of dimension, stated in C) and D) below, that play an essential role in the later study of the theory of topological groups. The preceding propositions B) and C) are of an ancillary nature.

B) Let A_1, \dots, A_k and A'_1, \dots, A'_k be two finite systems of sets in one-to-one correspondence: $A_i \rightarrow A'_i$. We say that the systems possess identical intersection scheme if, from the fact

that the intersection $A_{1_1} \cap A_{1_2} \cap \dots \cap A_{1_r}$ is not empty, it follows that the intersection $A'_{1_1} \cap A'_{1_2} \cap \dots \cap A'_{1_r}$ is also not empty, and conversely. If Γ is an arbitrary finite system of closed sets in a compact Hausdorff space R then it is possible to associate with each set $E \in \Gamma$ an open set U_E such that $E \subset U_E$ and such that the system of open sets U_E , $E \in \Gamma$, possesses identical intersection scheme with the original system Γ . From this fact and from A) it follows, in particular, that the significance of Definition 21 would have been the same had the system Δ been required to consist of open sets instead of closed sets.

To prove B) we begin by showing that if E is any set of the given system then there exists an open set $U_E \supset E$ such that replacing E by \overline{U}_E results in a system with identical intersection scheme with that of Γ . Denote by F the union of all those intersections of subsystems of Γ that do not meet E . Then U_E can be taken to be any open set containing E whose closure \overline{U}_E does not meet F . Carrying out the indicated substitution for the sets of Γ one at a time, in some order, we obtain a collection of open sets U_E , $E \in \Gamma$, possessing identical intersection scheme with that of Γ . But then the system of open sets U_E satisfies all the desired conditions.

C) Let Γ be a finite collection of closed sets in a compact space R and suppose there is associated with each $E \in \Gamma$ an open set U_E containing it. Then there exists a finite covering Ω_Γ of R by open sets such that if $E \in \Gamma$, $V \in \Omega_\Gamma$ and if the intersection $E \cap V$ is not empty then $V \subset U_E$.

For each $x \in R$ let E_1, \dots, E_r denote the sets of the collection Γ which contain x , let F_1, \dots, F_s denote those sets of the collection Γ which do not, and let

$$V_x = U_{E_1} \cap U_{E_2} \cap \dots \cap U_{E_r} \quad (F_1 \cup F_2 \cup \dots \cup F_s),$$

Among the apparently infinite collection of open sets V_x , $x \in R$, there can be but a finite number of distinct sets, which accordingly form the desired covering Ω_Γ .

D) The dimension of the union of a finite number of closed subsets in a compact Hausdorff space is equal to the largest of the dimensions of the various subsets.

By mathematical induction it suffices to consider the case of two sets: $R = A \cup B$. Moreover, it is obvious that the dimension of R is no smaller than the dimensions of A , B . Let the larger of these two dimensions be n . We must show then that the dimension of R does not exceed n .

Let Ω be an arbitrary finite covering of R by open sets and

let Γ be a covering of A by closed subsets of A that is a refinement of Ω and has multiplicity $\leq n + 1$. Using B) we associate with each set $E \in \Gamma$ a neighborhood U_E such that the system of open sets U_E , $E \in \Gamma$, is a refinement of Ω and possess identical intersection scheme with that of the system Γ . Next, starting from the system Γ of closed sets E and their neighborhoods U_E , we construct a covering Ω_r of R satisfying the condition of proposition C). Finally let Δ be a finite covering of B by means of closed subsets of B which is simultaneously a refinement of Ω and Ω_r and has multiplicity $\leq n + 1$.

Now let E_1, \dots, E_k be an enumeration of those sets of the system Γ that meet B . To each of the sets E_1, \dots, E_k we adjoin certain sets of the system Δ , taking care to arrange things so that to each E_i is adjoined only sets that meet it, and so that every set of the collection Δ that meets A is adjoined to one and only one of the sets E_1, \dots, E_k . In this way we obtain a new sequence E'_1, \dots, E'_k . Let Γ' denote the result of replacing each $E_i \in \Gamma$ by the corresponding set E'_i , $i = 1, \dots, k$. Since Δ is a refinement of the covering Ω_r it follows that any set of Δ adjoined to E_i in the formation of E'_i must be contained in U_{E_i} . Thus for each i we have $E'_i \subset U_{E_i}$. But from this it follows at once that Γ' still refines Ω and possesses identical intersection scheme with Γ ; in particular Γ' has multiplicity $\leq n + 1$. Denote by Δ' the sub-collection of Δ consisting of those sets which do not meet A , and denote by Σ the union of the collections Γ' and Δ' . Then Σ is a finite covering of R by closed sets that refines the covering Ω . We shall show that the multiplicity of Σ is $\leq n + 1$.

Let $x \in R$. If $x \in A$ then no one of the sets of Δ' contains x so that x can belong only to sets of the collection Γ' , the multiplicity of which does not exceed $n + 1$. Accordingly x cannot belong to more than $n + 1$ sets of Σ . Suppose next that $x \in R \setminus A$ and let $E'_{i_1}, \dots, E'_{i_\alpha}$ be those sets of the sequence E'_1, \dots, E'_k that contain x . Similarly let F_1, \dots, F_β be those sets of the collection Δ' that contain x . Since x is not in A and belongs to E'_{i_j} it cannot belong to E_{i_j} and must therefore belong to one of the sets of Δ which were adjoined to E_{i_j} in constructing E'_{i_j} . Denote any one such set in Δ by F'_{i_j} . Since the sets $E_{i_1}, \dots, E_{i_\alpha}$ are distinct, it follows that the sets $F'_{i_1}, \dots, F'_{i_\alpha}$ are distinct sets of the system Δ . Thus, altogether, the sets $F'_{i_1}, \dots, F'_{i_\alpha}$, all of which are distinct and belong to Δ , contain x . Since the multiplicity of Δ does not exceed $n + 1$ it follows that $\alpha + \beta \leq n + 1$. Thus, in any case, it is impossible for x to belong to more than $n + 1$ sets of Σ and D) is proved.

E) Let f be a continuous mapping of a compact Hausdorff space

R onto a Hausdorff space S and let Ω be a finite covering of R by open sets. We shall say that f refines the covering Ω if the inverse image $f^{-1}(y)$ of every point $y \in S$ is contained in some one of the open sets of Ω . If the space R has finite dimension let n be that dimension; otherwise let n be an arbitrary natural number. Then there is a finite covering Ω of R by open sets with the property that for arbitrary Hausdorff space S and arbitrary continuous mapping f of R onto S , if f refines Ω then the dimension of S is at least n . Indeed, Ω may be taken to be any finite covering with the property that any finite covering of R by means of closed sets that refines Ω has multiplicity at least $n + 1$.

Let Ω be selected as indicated above and suppose that f is a continuous mapping of R onto S that refines Ω . Since the intersection of the closures of all those open sets in S that contain a fixed point $y \in S$ coincides with y , it follows that the intersection of their inverse images coincides with $f^{-1}(y)$ and therefore is contained in one of the open sets $U \in \Omega$. Accordingly, there exists in S an open set V_y containing y such that the inverse image $f^{-1}(\bar{V}_y) \subset U$ (see Section 13, H)). The sets V_y , $y \in S$, constitute a covering of S from which we select a finite covering Ω' . By construction, the inverse image of each of the open sets of Ω' is contained in some one of the open sets of Ω . Suppose now that the dimension of S is less than n . Then there exists a finite closed covering Δ' of S that refines Ω' and has multiplicity $\leq n$. Denote by Δ the collection of all sets $f^{-1}(F)$, $F \in \Delta'$. Clearly Δ' and Δ have the same multiplicity while Δ is a refinement of Ω . Since this contradicts our hypothesis regarding R the result is proved.

F) A compact Hausdorff space has dimension 0 when and only when it is totally disconnected (see Section 15, D)).

Suppose first that R is a totally disconnected compact Hausdorff space and let Ω be an arbitrary finite covering of R by open sets. To each point $x \in R$ we associate some one of the open sets $U_x \in \Omega$ that contains x . Then, according to Section 15, G), there exists a closed-open set V_x such that $x \in V_x \subset U_x$. From the covering R consisting of the sets V_x , $x \in R$, we select a finite covering W_1, \dots, W_k and let

$$F_1 = W_1, F_2 = W_2 \setminus W_1, \dots, F_k = W_k \setminus (W_1 \cup \dots \cup W_{k-1}).$$

The system of closed sets F_1, \dots, F_k thus obtained is a refinement of Ω and is also a finite covering of multiplicity one. Since Ω is arbitrary it follows that the dimension of R is 0.

On the other hand, let R be a 0-dimensional compact Hausdorff space and let a, b be two distinct points. The open sets $U = R \setminus a$

and $V = R \setminus b$ constitute an open covering of R so there exists a closed covering F_1, \dots, F_k of R refining the covering U, V and having multiplicity one. We suppose, without loss of generality, that $a \in F_1$. Since R is the union of the two disjoint closed sets F_1 and $F_2 \cup \dots \cup F_k$, it follows that the component of a must be contained in F_1 and must therefore be a subset of $R \setminus b$. Thus the component of a does not contain b and since b was arbitrary it follows that the component of a coincides with a itself.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

3

TOPOLOGICAL GROUPS

From a purely logical point of view a topological group is obtained by uniting the concepts of group and of topological space; it is simply assumed that in one and the same set G there is defined an operation of group multiplication turning G into a group, as well as an operation of topological closure turning G into a topological space. These operations, however, are not independent but are connected by a continuity condition: the group operations in G are required to be continuous in the topological space G . Such being the definition, it is not surprising that the first few steps in the development of the theory of topological groups disclose almost nothing that is specific to it. The basic facts and concepts pertinent to groups, and to topological spaces are simply translated more or less immediately into the context of topological groups. Thus we encounter subgroups, normal subgroups, factor groups, and so forth. To be sure, certain situations specifically pertaining to topological groups do turn up in the process but they are comparatively superficial. It is to the study of these quite general properties of topological groups that the present chapter is devoted. A deeper investigation of topological groups will be given in subsequent chapters.

Historically topological groups arose in connection with the study of groups of continuous transformations. If some continuous manifold, for example Euclidean space, is subject to the action of a group of continuous transformations, then limit processes in the group itself appear in a natural way; the group is turned into a topological group. Thus, in the beginning, topological groups were regarded as groups of continuous transformations. Further development of the theory showed, however, that the most interesting properties of such groups were unrelated to the fact that the groups

were transformation groups but rather depended only on the existence in the groups themselves of suitably defined limit processes.

Accordingly it is expedient to give first the theory of topological groups not regarding them as transformation groups and only thereafter as an application of the theory to indicate the connection with continuous transformations.

SECTION 17. DEFINITION OF A TOPOLOGICAL GROUP

We here state the definition of a topological group and set forth the simplest properties thereof.

Definition 22: A set G is said to be a topological group if:

- 1) G is a group;
- 2) G is a topological space;
- 3) The group operations in G are continuous in the topological space G .

This requirement may be formulated more precisely thus:

a) If a and b are two elements of G then for every neighborhood W of ab there exist neighborhoods U and V of a and b such that $UV \subset W$ (see Def. 14 and Section 2, A)).

b) If a is any element of G then for every neighborhood V of a^{-1} there exists a neighborhood U of a such that $U^{-1} \subset V$.

It is not hard to see that conditions a) and b) may be replaced by the single condition:

c) If a and b are two elements of G then for every neighborhood W of ab^{-1} there exists neighborhoods U and V of a and b such that $UV^{-1} \subset W$.

The topological invariance of this definition, i.e., the independence of condition 3) of the choice of the defining system of neighborhoods, is readily verified (see Section 9, F)). If at any time in discussing a topological group we wish to emphasize the fact that we are speaking only of its algebraic properties and are taking no account of its topological structure we shall refer to it as an algebraic group*.

We now list certain very elementary properties of topological groups.

A) Let a_1, \dots, a_n be any finite system of elements of a topological group and let $a_1^{r_1} a_2^{r_2} \dots a_n^{r_n} = c$ be any product of their powers, either positive or negative. Then for any neighborhood W of c there exist neighborhoods U_1, \dots, U_n of the elements a_1, \dots, a_n respectively such that $U_1^{r_1} U_2^{r_2} \dots U_n^{r_n} \subset W$; moreover, if $a_i = a_j$ we can arrange for

* In modern group theory, the term algebraic group has an entirely different meaning. Here I retain my old terminology. There is however no room for confusion because everywhere in this book I use algebraic group as a synonym for abstract group.

U_i and U_j to be the same, and similarly for a larger number of equal elements.

The assertion is verified by the repeated application of condition 3) of Definition 22 bearing in mind the fact that the intersection of a finite number of neighborhoods always contains a neighborhood.

B) Let $f(x) = xa$, $f'(x) = ax$, $\varphi(x) = x^{-1}$ where a is a fixed element of the group G and x denotes a variable element of the same group. Then all three of the functions f , f' and φ are homeomorphisms of the topological space G onto itself.

We treat only the case of f . In the first place, f is a one-to-one mapping of G onto itself since for each y' there exists one and only one element x' such that $y' = x'a$. Moreover f is continuous. Indeed if $y' = x'a$ and if W is a neighborhood of y' then by condition 3) of Definition 22 there exist neighborhoods U and V of x' and a such that $UV \subset W$, i.e., $f(U) \subset W$ which implies that f is continuous. The same argument also establishes the continuity of the inverse mapping $f^{-1}(y) = ya^{-1}$.

C) Let F denote a closed set, U an open set, P an arbitrary set and a an arbitrary element of a topological group G . Then Fa , aF , F^{-1} are closed sets; UP , PU , U^{-1} are open sets.

The proof follows immediately from B). Indeed $f(x) = xa$ is a homeomorphism and therefore carries the closed set F onto the closed set $f(F) = Fa$. Similarly Ua is open; but then UP is the union of a collection of open sets and is itself open.

D) A topological group G is homogeneous. By this is meant that for each pair of elements p and q of G there is a homeomorphism of G onto itself which carries p into q . Indeed the mapping f of B) satisfies $f(p) = q$ if we make the choice $a = p^{-1}q$.

E) From the homogeneity of a topological group G it follows that it suffices to verify its local properties at a single point. For example, in order to show that G is locally compact it suffices to show that the identity element e admits a neighborhood U whose closure \bar{U} is compact. Similarly for the regularity of G . Moreover if the identity element e admits a neighborhood containing only e then every other element of the group G also admits a neighborhood consisting of a single element.

F) The topological space G of a topological group G is regular (see Def. 18).

As just noted it suffices to consider neighborhoods of the identity e . Let U be such a neighborhood. Since $ee^{-1} = e$ it follows from A) that there exists a neighborhood V of the identity such that $VV^{-1} \subset U$. We shall show that $\bar{V} \subset U$. Indeed let p be a point of \bar{V} . Then every neighborhood of p meets V . Since the open set pV

contains a neighborhood of p there must exist in V a point b such that $pb = a \in V$; but then $p = ab^{-1} \in VV^{-1} \subset U$; thus $\overline{V} \subset U$.

G) If P and Q are two compact sets in a topological group G then their product PQ is also compact.

Consider the mapping f of the topolgocial product $P \times Q$ of the subspaces P and Q onto the set PQ defined for each element $(x, y) \in P \times Q$ by $f(xy) = xy$. The mapping is continuous. Indeed let $a \in P$, $b \in Q$, $c = ab$ and let W be an arbitrary neighborhood of c in G . Since group multiplication is continuous there exist neighborhoods U and V of a and b in P and Q , respectively, such that $UV \subset W$, i.e., such that $f((U, V)) \subset W$ and (U, V) is a neighborhood of (a, b) in $P \times Q$. Since the product $P \times Q$ is compact by Theorem 5 it follows that the image PQ under the mapping f is also compact (see Section 13, D)).

Example 29: The set of vectors in r -dimensional Euclidean space is an additive group. In Example 19 a topology was defined in the set. It is easy to verify that the operation of vector addition is continuous in that topology. Accordingly the resulting structure is a topological group, known as the r -dimensional vector group.

SECTION 18. SYSTEMS OF NEIGHBORHOODS OF THE IDENTITY

The results of the preceding paragraph make clear that condition 3) of Definition 22 effects a very close bond between the algebraic and topological operations in a topological group. A particular consequence of this is that if G is given initially simply as a group then in order to define a topology in G so as to turn it into a topological group it is not necessary to give a base of the entire space G but suffices to give a complete system of neighborhoods of the identity (see Section 9, B)). The simplest illustration of this idea is provided by the so-called discrete groups.

A) A topological group G is said to be discrete if there are no limit points in G , i.e., if every element admits a neighborhood consisting of that element only (see Ex. 18). As has been noted, G is discrete when and only when its identity is an isolated point of the group.

No matter what group we start from, the topology thus defined clearly turns it into a discrete topological group. Thus we may say that the theory of discrete topological groups coincides essentially with abstract group theory.

The following proposition B) and Theorem 9 show how the topology of a topological group is determined by a complete system

of neighborhoods of its identity and how this fact may be exploited to introduce a topology into a given group.

B) Let G be a topological group, let Σ^* be a complete system of neighborhoods of its identity e and let M be any set everywhere dense in G . Then the collection Σ of all sets of the form Ux where $U \in \Sigma^*$, $x \in M$, is a complete system of neighborhoods of the space G . Moreover Σ^* satisfies the following five conditions:

- a) The intersection of all of the sets of Σ^* consists of e only.
- b) The intersection of any two sets of Σ^* contains a third set belonging to Σ^* .
- c) For every set $U \in \Sigma^*$ there exists a set $V \in \Sigma^*$ such that $VV^{-1} \subset U$.
- d) For every set $U \in \Sigma^*$ and every element $a \in U$ there exists a set $V \in \Sigma^*$ such that $Va \subset U$.
- e) If $U \in \Sigma^*$ and if a is an arbitrary element of G then there exists a set $V \in \Sigma^*$ such that $a^{-1}Va \subset U$.

According to C), Section 17, the sets of the system Σ are open. We must show that they constitute a base for the space G . Let W be an arbitrary open set in G and let $a \in W$. Then Wa^{-1} is open and contains e . Hence there is a neighborhood $U \in \Sigma^*$ such that $UU^{-1} \subset Wa^{-1}$. Since M is everywhere dense in G so is the set aM^{-1} ; consequently the sets U and aM^{-1} have an element d in common. Note that then $d^{-1}a \in M$. From this it follows that $Ud^{-1}a \in \Sigma$. On the other hand, $Ud^{-1}a \subset W$. Indeed $UU^{-1} \subset Wa^{-1}$ and since $d \in U$ we have $Ud^{-1} \subset Wa^{-1}$ which implies that $Ud^{-1}a \subset W$. Finally, since $d \in U$ it follows that $e \in Ud^{-1}$ and consequently that $a \in Ud^{-1}a$. Thus the condition insuring that Σ is a base is fulfilled (see Section 9, B)).

As for the conditions a), ..., e) we observe that a) and b) are satisfied in an arbitrary topological space while c), d) and e) are immediate consequences of A), Section 17.

Theorem 9: Let G be an algebraic group and let Σ^* be any system of subsets of G satisfying the five conditions of B) above. Then there is one and only one way of introducing a topology into G in such a way that G becomes a topological group and the system Σ^* becomes a complete system of neighborhoods of the identity. This may be reformulated by saying that G admits one and only one topologization with respect to which Σ^* is a complete system of neighborhoods of the identity.

Observe that in the case of a commutative group condition e) is automatically satisfied.

Proof: If G admits any topologization which turns it into a topological group and with respect to which Σ^* is a complete system of neighborhoods of the identity then, as has already been shown in B), the collection Σ of all sets of the form Ux where $U \in \Sigma^*$, $x \in G$, is a base for that topology. From this it follows at once that the topology satisfying the two given conditions is unique if it exists. We complete the proof of the theorem by showing, first, that Σ satisfies the conditions of Theorem 3, second, that the group operations in G are continuous in the topology so defined and, third and finally, that Σ^* is a base at e in that topology.

Let a and b be distinct elements of G . Since e is the only element common to all the sets of the system Σ^* there exists $U \in \Sigma^*$ such that $ba^{-1} \in U$; but then Ua does not contain b . Thus condition a) is satisfied.

In order to verify b) of Theorem 3 we begin by observing that if $b \in Ua$ where $U \in \Sigma^*$ then there exists a neighborhood $V \in \Sigma^*$ such that $Vb \subset Ua$. Indeed $ba^{-1} \in U$ so that by d) there exists $V \in \Sigma^*$ such that $Vba^{-1} \subset U$; but then $Vb \subset Ua$.

Let now Ua and Vb be two neighborhoods of the point c , i.e., let $c \in Ua$, $c \in Vb$ where $U, V \in \Sigma^*$. By the remark just made there exist neighborhoods U' , $V' \in \Sigma^*$ such that $U'c \subset Ua$ and $V'c \subset Vb$. Choosing then, by condition b) of the present theorem, a neighborhood $W \in \Sigma^*$ contained in the intersection $U' \cap V'$ we obtain $Wc \subset Ua$, $Wc \subset Vb$ which shows that condition b) of Theorem 3 is also satisfied.

We next show that the group operations are continuous in the topology thus obtained. Let $c = ab^{-1}$ and $W'c'$ be an arbitrary neighborhood of c . Then, as has been shown, there exists a neighborhood $W \in \Sigma^*$ such that $Wc \subset W'c'$. We next use c) to obtain a neighborhood $U \in \Sigma^*$ such that $UU^{-1} \subset W$ and finally e) to obtain another neighborhood $V \in \Sigma^*$ such that $ab^{-1}Vba^{-1} \subset U$. Then $ab^{-1}V^{-1} \subset U^{-1}ab^{-1}$ and consequently

$$Ua(Vb)^{-1} = Uab^{-1}V^{-1} \subset UU^{-1}ab^{-1} \subset Wab^{-1} = Wc \cap W'c' \quad (0_1)$$

Thus condition 3) of Definition 22 is satisfied, and G is a topological group with respect to the topology introduced by the neighborhood system Σ .

It remains to show that Σ^* is a base at e (see Section 9, B')). Let W be an arbitrary open subset of G which contains e . Since Σ is a base for G there exists a neighborhood $Ua \in \Sigma$ of the point e such that $Ua \subset W$. From $e \in Ua$ it follows that $a^{-1} \in U$ and consequently, by virtue of condition d), there exists a neighborhood $V \in \Sigma^*$ such that $Va^{-1} \subset U$. But then $V \subset Ua \subset W$ which shows that Σ^* is a base at e .

SUBGROUP. NORMAL SUBGROUP. FACTOR GROUP 101

Example 30: Let G denote the additive group of whole numbers. We introduce in G a series of different topologies.

Let p be an arbitrary prime number and denote by U_k the set of all whole numbers divisible by p^k . It is not difficult to verify that all of the conditions imposed on the system Σ^* in Theorem 9 are satisfied by the collection of sets U_k , $k = 1, 2, \dots$. Consider, for example, condition c); if $a \in U_k$ and $b \in U_k$ then also $a - b \in U_k$, so that c) is realized here in a particularly simple form.

It is easy to verify that the topologies obtained in this fashion starting from two different primes p and p' are distinct. Indeed the sequence $p, p^2, \dots, p^k, \dots$ converges to 0 in the first topology but does not converge to 0 in the second.

Example 31: Let G denote the set of all non-singular complex square matrices of order n . In Example 2 an operation of multiplication was defined in G turning it into a group. We now introduce in G a topology. Denote by U_k the set of all matrices $x \in G$ with the property that all entries of the matrix $x - e$ are less than $1/k$ in absolute value (e is the unit matrix). For Σ^* we take the collection of all sets U_k , $k = 1, 2, \dots$. It may be readily verified that Σ^* satisfies all conditions of Theorem 9 and that the topological group G thus obtained is locally compact and separable.

SECTION 19. SUBGROUP. NORMAL SUBGROUP. FACTOR GROUP

In this paragraph we extend to topological groups those concepts introduced in Section 2 for algebraic groups.

Definition 23: Let G be a topological group. Then a subset H is said to be a subgroup of the topological group G if a) H is a subgroup of the algebraic group G , b) H is a closed set in the topological space G . A subgroup N of the topological group G is said to be a normal subgroup if N is a normal subgroup of the algebraic group G .

Thus the fact that G is not simply a group but a topological group leads only to the imposition on H and N of the single extra condition of closure.

A) Let G be a topological group and let H be a subset of it which is a subgroup of G considered as an algebraic group. Then H is also a topological group with respect to the topology it receives as a subspace of the space G . In particular, a subgroup of a topological group is itself a topological group.

To prove the assertion it suffices to show that the group operations in H are continuous in the topological space H . Let a and b be two elements of H and let $ab^{-1} = c$. Every neighborhood W' of c in the space H may be written as the intersection with H of some neighborhood W of c in the space G . $W' = H \cap W$ (see Section 11, B)). Since G is a topological group there exist neighborhoods U and V of a and b such that $UV^{-1} \subset W$. But then the intersections $U' = H \cap U$ and $V' = H \cap V$ are neighborhoods of a and b in the space H and we have $U'V'^{-1} \subset W$ as well as $U'V'^{-1} \subset H$ so that $U'V'^{-1} \subset W'$, i.e., condition 3) of Definition 22 holds in H .

B) As above let G be a topological group and let H be a subgroup of the algebraic group G . Then \bar{H} is a subgroup of the topological group G . If H is a normal subgroup of the algebraic group G then H is also normal. If H is open in G then $\bar{H} = H$.

We must show that if $a \in \bar{H}$ and $b \in \bar{H}$ then $ab^{-1} \in \bar{H}$. Let W be an arbitrary neighborhood of ab^{-1} and choose neighborhoods U and V of the elements a and b such that $UV^{-1} \subset W$. Then there exist elements x and y in H such that $x \in U$, $y \in V$. Thus we have simultaneously $xy^{-1} \in H$ and $xy^{-1} \in W$. Accordingly the neighborhood W meets H and it follows that $ab^{-1} \in \bar{H}$. Thus \bar{H} is a subgroup of the algebraic group G and since \bar{H} is automatically closed in G it is a subgroup of the topological group G .

Suppose now that H is a normal subgroup of the algebraic group G and let $a \in \bar{H}$, $c \in G$. Let V be an arbitrary neighborhood of the element $c^{-1}ac$. Then there exists a neighborhood U of a such that $c^{-1}Uc \subset V$ and since $a \in \bar{H}$ there exists an element $x \in H$ belonging to U . But then $c^{-1}xc \in H$ and $c^{-1}xc \in V$ so that V meets H . It follows that $c^{-1}ac \in \bar{H}$ and consequently that \bar{H} is a normal subgroup of the topological group G .

Finally, if H is an open set in G and if $a \in \bar{H}$ then a is contained in the open set aH , which must meet H . Hence $a \in HH^{-1} = H$ and $\bar{H} = H$.

In Section 2 the concept of coset was introduced. In the case of topological groups the collection of cosets of a subgroup becomes in a natural way a topological space which plays an important role.

Definition 24: Let G be a topological group and let H be a subgroup of G . Denote by G/H the collection of all right cosets of the subgroup H in G (see Section 2, D)). We introduce a topology in G/H in the following manner. Let Σ be a base of open sets in G and for each $U \in \Sigma$ denote by U^* the collection of all cosets of the form Hx where $x \in U$. The collection Σ^* of all sets of the form U^* , $U \in \Sigma$, satisfies the condition of Theorem 3 and accordingly constitutes a complete system of neighborhoods for

a unique topology in G/H . The topological space G/H thus defined will be called the space of right cosets of the subgroup H in the topological group G . Analogously we define the space of left cosets which may also be denoted by G/H . In case there is no danger of confusion we shall not bother to distinguish between the spaces of left and right cosets.

It is readily verified that the topologies in the space G/H here defined are invariant, i.e., that they do not depend on the choice of Σ .

We must show that Σ^* satisfies the conditions of Theorem 3. Let A and B be distinct cosets and let $a \in A$. Since $B = Hb$ is a closed set and since a does not belong to B there exists a neighborhood U of a that does not meet B . But then the set U^* of cosets of the form Hx , $x \in U$, is a neighborhood of A not containing B . Thus condition a) of Theorem 3 is satisfied.

Next let U^* and V^* be two neighborhoods of some coset A , and let $a \in A$. Select in Σ neighborhoods U and V such that U^* is the collection of cosets of the form Hx , $x \in U$, while V^* is the collection of cosets of the form Hy , $y \in V$. Then HU and HV are open sets in G containing a . Accordingly there is a neighborhood W of a contained in the intersection of HU and HV and it is easy to see that W^* is a neighborhood of A contained in the intersection $U^* \cap V^*$. Thus condition b) of Theorem 3 is also satisfied.

C) Let G be a topological group, H a subgroup and let G/H be the space of cosets. Associate with each element $x \in G$ the element $X = f(x)$ of the space G/H where $f(x)$ is taken to be the coset containing x . The mapping f of G onto G/H thus obtained is a continuous open mapping known as the natural projection of G onto G/H .

Suppose for the sake of definiteness that G/H is the space of right cosets. Let $a \in G$ and let $A = Ha$ so that $f(a) = A$. Finally, let U^* be an arbitrary neighborhood of A in G/H . Then there exists a neighborhood U in the space G such that U^* consists of all cosets of the form Hx , $x \in U$. The set HU is also open in G and contains a ; accordingly there exists a neighborhood V of a contained in HU . It is easy to see that $f(V) \subset U^*$ so that f is continuous.

Let once again $a \in G$ and $A = Ha = f(a)$. This time let U be an arbitrary neighborhood of a . Then it is immediately clear that $f(U) = U^*$; in particular $U^* \subset f(U)$ so that f is also open.

A particularly important case arises when the subgroup H is normal. In this event we introduce the following definition:

Definition 25: Let G be a topological group and let N be a normal subgroup of G . The set of cosets G/N is a group by Definition 4 and a topological space by Definition 24. We show below

that the group operations in the group G/N are continuous in the topological space G/N so that G/N is a topological group. It is called the factor group of the topological group G by the normal subgroup N .

We must verify the continuity of the group operations in G/N . Let A and B be two elements of G/N , $C = AB^{-1}$, and let W^* be an arbitrary neighborhood of C . Then W^* is the collection of all cosets of the form Nz , $z \in W$, where W is some neighborhood in G . Since $C \in W^*$ there exists an element $c \in W$ such that $C = Nc$. Let b be an arbitrary element of B and let $a = cb$; then $a \in A$. Since G is a topological group there exist neighborhoods U and V of a and b such that $UV^{-1} \subset W$. Denote by U^* the neighborhood of A consisting of all cosets of the form Nx , $x \in U$, and by V^* the neighborhood of B consisting of all cosets of the form Ny , $y \in V$. We have then

$$Nx(Ny)^{-1} = Nxy^{-1}N^{-1} = NN^{-1}xy^{-1} = Nxy^{-1} \in W^*. \quad (0_1)$$

Thus $U^*V^{*-1} \subset W^*$, i.e., condition 3) of Definition 22 is satisfied.

D) Every topological group G possesses at least two normal subgroups, namely the group G itself and the trivial subgroup $\{e\}$. In contrast to the terminology employed in group theory (see Section 2, G)), a topological group G is said to be simple when each of its normal subgroups either coincides with G itself or is discrete (see Section 18, A)). In general it may be said that discrete normal subgroups play a distinguished role in the theory of topological groups.

We now establish certain properties of coset spaces.

E) The space G/H of cosets of a subgroup H in a topological group G is homogeneous, i.e., for each pair of elements A and B in the space there exists a homeomorphism φ of the whole space onto itself which carries A to B . From this it follows in particular that in order to verify local properties of the space G/H , for example, regularity, local compactness, etc., it suffices to establish their validity at a single point, the most natural choice for this purpose being $H \in G/H$.

In order to define the mapping φ we suppose for the sake of definiteness that G/H is the space of right cosets. Let $A = Ha$, $B = Hb$. The φ is defined by $\varphi(X) = Xa^{-1}b$, $X \in G/H$. It is immediately verified that φ has all the desired properties.

F) The space of cosets of a subgroup of a topological group is regular.

In order to prove the assertion, let G be a topological group, let H be a subgroup and suppose that G/H is the space of, say,

right cosets of H . As just noted, it is enough to show that, given an arbitrary neighborhood U^* of H in G/H , there exists a neighborhood V^* of the same element such that $\overline{V^*} \subset U^*$. We may assume without loss of generality that U^* consists of all cosets of the form Hx , $x \in U$, where U is a neighborhood of the identity in G . Let V be another neighborhood of the identity in G such that $UV^{-1} \subset U$. We shall show that $\overline{HV} \subset HU$. Indeed let $x \in \overline{HV}$; then every neighborhood of x meets the open set HV and in particular the neighborhood xV has a point in common with HV . Thus there exist elements $h \in H$, $a \in V$, $b \in V$ such that $ha = xb$. But then $x = hab^{-1} \in HVV^{-1} \subset HU$. Thus $\overline{HV} \subset HU$. The desired neighborhood V^* may now be taken to be the set of cosets of the form Hy , $y \in V$. Indeed, let f be the natural projection of G onto G/H . Then $f(HV) = V^*$, $f(HU) = U^*$. Since multiplication on the left by an element $h \in H$ is a homeomorphism of the group G onto itself which leaves HV fixed it follows that the closure \overline{HV} also remains fixed. From this it follows that the set \overline{HV} and its complement $G \setminus \overline{HV}$ both consist of unions of entire cosets and hence that their images under the natural projection f are also complementary in G/H . From this and from the fact that the mapping f is open it follows that the set $f(\overline{HV})$ is closed. Thus:

$$\overline{V^*} \subset f(\overline{HV}) \subset f(HU) = U^*,$$

and the regularity of G/H is established.

The following result represents an essential advance beyond proposition F) and answers an important abstract question concerning the structure of the space of a topological group and its various coset spaces. We shall have no occasion in the future, however, to employ the theorem. Its proof is similar to the proof of Urysohn's Lemma.

Theorem 10: Any space of cosets of a topological group, in particular the space of the topological group itself, is completely regular.

Proof. Let G be a topological group and let H be a subgroup of it. Let G/H denote the space of, say, right cosets of H . As has been noted G/H is homogeneous so that it suffices to construct for an arbitrary neighborhood U^* of $H \in G/H$ a continuous real function f^* on G/H satisfying the following conditions:

$$f^*(X) = 1 \text{ for } X \in G/H \setminus U^*; \quad f^*(H) = 0$$

$$0 \leq f^*(X) \leq 1 \text{ for all } X \in G/H.$$

Without loss of generality we suppose that U^* consists of all cosets of the form Hx , $x \in U$, where U is a neighborhood of the identity in G . We begin by constructing a continuous real function f on the group G satisfying the conditions

$$f(x) = 1 \text{ for } x \in G \setminus HU; \quad f(e) = 0; \quad (1)$$

$$0 \leq f(x) \leq 1 \text{ for all } x \in G.$$

and constant on each coset $X \in G/H$. Once such an f has been constructed, the proof will be completed by making the obvious transition from f to f^* .

Let $U_0 = U$, U_1 , U_2 , ... be an infinite sequence of neighborhoods of the identity e in G satisfying the condition

$$U_{k+1}^2 \subset U_k, \quad k = 0, 1, 2, \dots \quad (2)$$

That such a sequence exists follows from A), Section 17, since $e^2 = e$. Let now

$$V_{n,k} = \{e\}; \quad V_{n,k} = U_{n+1} U_{n+2} \dots U_k, \quad 0 \leq n < k. \quad (3)$$

We show by induction that

$$V_{n,k} \subset U_n \quad (4)$$

Indeed, for $k = n$ the inclusion reduces to equality while for $k = n + 1$ we have $V_{n,k} = U_{n+1}$ so that (4) coincides with (2). The inductive step consists in showing that (4) implies $V_{n,k+1} \subset U_{n+1}$. But now:

$$V_{n,k+1} \subset U_{n+1} = V_{n,k} \cup U_{n+1} \subset V_{n,k} \cup U_k \subset U_n. \quad (4_1)$$

Now let $r = q/2^m$ be a proper dyadic fraction, $0 < r < 1$. Then r can be written in one and only one way in the form

$$r = \frac{a_1}{2^m} + \frac{a_2}{2^2} + \dots + \frac{a_k}{2^k} \quad (5)$$

where $k \geq m$ and each of the numbers a_1, a_2, \dots, a_k is either zero or one. Employing this representation we assign to each number r an open set W_r containing e :

$$W_r = HU_1^{a_1} U_2^{a_2} \dots U_k^{a_k} \quad (6)$$

Clearly the set W_r is uniquely determined by r . Moreover for arbitrary r we have

$$W_r \subset HU \quad (7)$$

Indeed $W_r \subset HU_1 U_2 \dots U_k = HV_{0,k} \subset HU_0 = HU$. We next show that

$$W_r \subset W_{r'} \quad \text{for } r < r' \quad (8)$$

For let $r' = \frac{a'_1}{2} + \frac{a'_2}{2^2} + \dots + \frac{a'_k}{2^k}$ be the representation of the number r' as in (5) and let n be the smallest natural number i for which $a'_i \neq a_i$. Then $a_n = 0$, $a_{n'} = 1$ and we have

$$\begin{aligned} W_r &\subset HU_1^{a_1} U_2^{a_2} \dots U_{n-1}^{a_{n-1}} V_{n,k} \subset HU_1^{a_1} U_2^{a_2} \\ &\dots U_{n-1}^{a_{n-1}} U_n \subset W_{r'}. \end{aligned}$$

We now define the value $f(x)$ of the function f at a point $x \in G$ as follows: if x belongs to any one of the open sets W_r then $f(x)$ is defined to be the greatest lower bound of those values of r for which $x \in W_r$; if, on the other hand, x belongs to none of the sets W_r then we define $f(x) = 1$. Since all the values of r under consideration lie in the interval $(0, 1)$ it follows that for every x , $0 \leq f(x) \leq 1$. Also, since e belongs to all the sets W_r we have $f(e) = 0$. Moreover, by virtue of (7), $f(x) = 1$ for $x \in G \setminus HU$. Thus (1) is satisfied for the function f . Note also that

$$\text{for } f(x) < r_0 \text{ we have } x \in W_{r_0}. \quad (9)$$

Indeed if x does not belong to any of the open sets W_r then $f(x) = 1$ so that $f(x) < r_0$ is impossible since r_0 is by hypothesis a proper fraction; if on the other hand there exist numbers r for which $x \in W_r$ but the number r_0 is not among them, then r_0 must be smaller than all numbers r for which $x \in W_r$ whence $f(x) \geq r_0$.

To prove that f is continuous it suffices to show that if $x^{-1}y \in U_k \cap U_k^{-1} = U_k^*$ then

$$|f(x) - f(y)| \leq \frac{1}{2^{k-1}}.$$

(This shows in fact that f is even uniformly continuous (see Section 28, B)) but that is of no interest to us here). Also we may suppose

without loss of generality that $f(x) \leq f(y)$ since the relation $x^{-1}y \in U_k$ is symmetric in x and y . In other words, it suffices to show that for $x^{-1}y \in U_k$ and $f(x) \leq f(y)$ we have

$$f(y) - f(x) \leq \frac{1}{2^{k-1}}.$$

Now among the numbers $1, 2, 3, \dots, 2^k$ choose that number q such that

$$\frac{q-1}{2^k} \leq f(x) < \frac{q}{2^k}.$$

Then

$$\frac{q}{2^k} - f(x) \leq \frac{1}{2^k}.$$

Hence if $q = 2^k$ or $q = 2^k - 1$ then $1 - f(x) \leq \frac{1}{2^{k-1}}$ and since $f(y) \leq 1$ we are done.

Suppose, accordingly, that $q < 2^k - 1$ and let $r = \frac{q}{2^k}$. Then $x \in W_r$

by (9) and, in the representation (5) of r , not all of the numbers a_1, \dots, a_k can be ones. Let a_n be the last zero appearing in the list and define

$$r' = \frac{a_1}{2} + \frac{a_2}{2} + \dots + \frac{a_{n-1}}{2^{n-1}} + \frac{1}{2^n}.$$

Since $x^{-1}y \in U_k$ and $W_r U_k \subset W_{r'}$ it follows that $y \in W_{r'}$ and hence that $f(y) \leq r'$. Since $r' - r = 1/2^n$ we have

$$f(y) - f(x) \leq r' - (r - \frac{1}{2^k}) = \frac{1}{2^{k-1}}.$$

Since each of the open sets W_r is a union of complete cosets (see (6)) it follows that the function f is constant on each coset $X \in G/H$.

We now define f^* by writing simply $f^*(X) = f(x)$ where $x \in X$. Since f is constant on the coset X the equation $f^*(X) = f(x)$ defines f^* uniquely. Since f is continuous and since the natural projection of G onto G/H is open it follows that the inverse image of an open set under the mapping f^* is itself open and hence that f^* is continuous. Thus Theorem 10 is proved.

We next establish certain connections between the properties of the topological spaces G , H and G/H .

G) Let G be a topological group and let H be a subgroup. Then

the weights of the spaces H and G/H do not exceed the weight of G (see Def. 14).

The validity of this assertion is an immediate consequence of the construction of bases in the spaces H and G/H in C), Section 11, and in Definition 24.

H) Let G be a topological group and let H be a subgroup. If G is compact then both H and G/H are also compact. If G is locally compact then both H and G/H are also locally compact.

As far as H is concerned this follows from B), Section 13. If G is compact then G/H is the continuous image of a compact space and must therefore be compact also (see Section 13, D)). It remains only to show that if G is locally compact then G/H is locally compact. Let f denote the natural projection of G onto G/H and let a be an arbitrary element of G , $A = f(a)$. Finally, let U be a neighborhood of a in G such that \bar{U} is compact. The set $f(\bar{U})$ is compact in G/H and must therefore be closed since G/H is a Hausdorff space (see F)). Since $U \subset \bar{U}$ we have $f(U) \subset f(\bar{U})$ and consequently $f(U) \subset \bar{f}(U)$. Accordingly, $\bar{f}(U)$ is a compact set. On the other hand it is obvious that the neighborhood U^* of A in G/H consisting of all cosets that meet U coincides with $f(U)$, $U^* = f(U)$. Thus \bar{U}^* is a compact set and G/H is locally compact.

I) Let G be a topological group and let f be the natural projection of G onto G/H where H is a compact subgroup. Then if the set $Q \subset G/H$ is compact it follows that $P = f^{-1}(Q)$ is also compact. In particular, if G/H is compact or locally compact then G is compact or locally compact respectively.

Let Δ be a collection of closed subsets of the subspace P having the finite intersection property; we shall show that it also has non-empty intersection. We assume, without loss of generality, that Δ is multiplicative (see Section 15, F)). We also suppose, for the sake of definiteness, that G/H is the space of right cosets. Consider now in the space Q the collection Δ^* af all sets of the form $f(F)$, $F \in \Delta$. The system Δ^* has the finite intersection property along with Δ and, while the sets of this new system need not be closed, they do all possess a common adherent point A since Q is compact by hypothesis. Now let U be an arbitrary neighborhood of the identity element in G . Then the set U^* consisting of all cosets contained in AU is open in G/H and contains A . Consequently U^* meets every set of the system Δ^* . It follows that AU meets every set of Δ , or in other words, that every set of the form FU^{-1} where $F \in \Delta$ meets A . From this it follows that the system Δ' of all sets of the form $(FU^{-1}) \cap A$, where $F \in \Delta$ and U is an arbitrary neighborhood of the identity, also has the finite intersection property. Since the coset A , being homeomorphic with the compact space H , is

compact it follows that the sets of the collection Δ' possess a common adherent point a . Hence for an arbitrary neighborhood V of the identity element in G the sets FU^{-1} and a V have non-empty intersection and consequently F meets the open set aVU . Since for an arbitrary neighborhood W of the identity there exist neighborhoods V and U of the identity such that $VU \subset W$, this in turn implies that an arbitrary neighborhood W of a meets every one of the sets $F \in \Delta$, and since F is closed we have $a \in F$. Thus a is common to all the sets of the system Δ which shows that P is compact.

Example 32: Only shortly after the first precise formulation of the definition of a topological group, the regularity of the space of a group was observed by A. N. Kolmogorov. The complete regularity of a topological group was also discovered comparatively early. There then arose the much more difficult question of whether a topological group was necessarily normal. This question was answered in the negative by A. A. Markov by the construction of a very interesting and delicate example [34]. Although it is not possible to reproduce Markov's construction here in anything like full detail, I shall indicate briefly the line of argument. Markov showed that every completely regular topological space R may be imbedded as a closed set in the space of a suitably constructed topological group G . Now it is easy to see that a closed subspace of a normal space is itself normal. Thus if the group G were normal the original space R would have to be normal too; but it is known that there exist completely regular topological spaces which are not normal. Accordingly there exist topological groups which are not normal.

Example 33: We shall find all subgroups of the r -dimensional vector group G introduced in Example 29.

Let

$$e_1, \dots, e_s, f_1, \dots, f_t \quad (10)$$

be an arbitrary linearly independent system of vectors in G . Then the set of all vectors of the form

$$\lambda^1 e_1 + \dots + \lambda^s e_s + \mu^1 f_1 + \dots + \mu^t f_t, \quad (11)$$

where $\lambda^1, \dots, \lambda^s$ are whole numbers and μ^1, \dots, μ^t are arbitrary real numbers, is clearly a subgroup of G . It turns out that for an arbitrary subgroup H of G it is possible to select a linearly independent system of vectors (10) such that H coincides with

all vectors of the form (11). Moreover, if H is discrete then $t = 0$.

The proof is by induction on the dimension r of the vector group G . For $r = 0$ the assertion is trivial. Also if r is positive and if K is a one dimensional subspace of the vector space G then $G^* = G/H$ may itself be viewed as a vector group of one lower dimension. We use this observation below writing φ for the natural projection of G onto G^* . Consider, in the first place, the case when H is discrete. Let e be a vector of minimal positive length α belonging to H and choose for K the one dimensional subspace containing e . It is easy to see that the intersection $H \cap K$ consists of all vectors λe where λ is a whole number. Moreover the distance between the sets $H \setminus K$ and K is not less than $\alpha/2$. Indeed if $\rho(x, y) < \alpha/2$ where $x \in H \setminus K$, $y \in K$ and if we write $y = (\lambda + \theta)e$, where $|\theta| \leq 1/2$ and λ is a whole number then $\rho(x, \lambda e) < \alpha$, i.e., $\rho(x - \lambda e, 0) < \alpha$ which contradicts the minimality of α . But then $H^* = \varphi(H)$ is a discrete subgroup of G^* and by the inductive hypothesis there exist in G^* linearly independent vectors e_1^*, \dots, e_s^* such that H^* consists of all vectors $\lambda^1 e_1^* + \dots + \lambda^s e_s^*$ where $\lambda_1, \dots, \lambda_s$ are whole numbers. Choose vectors e_i in H such that $\varphi(e_i) = e_i^*$, $i = 1, \dots, s$. If now $x \in H$ then $\varphi(x) = \lambda^1 e_1^* + \dots + \lambda^s e_s^*$ and therefore $x - \lambda^1 e_1 - \dots - \lambda^s e_s = \lambda e$. Accordingly, letting $e_{s+1} = e$ we arrive at the desired system e_1, \dots, e_{s+1} . Next suppose that H is not discrete and let x_1, \dots, x_n, \dots be a sequence of non-zero vectors in H converging to zero. Let $y_n = x_n / |x_n|$ and let f be a limit point of the sequence y_1, \dots, y_n, \dots . It is easy to see that the one dimensional subspace K containing f is included in H since H is closed in G and contains all vectors of the form $m |x_n| y_n$ where m is an arbitrary whole number. From this it follows that $H^* = \varphi(H)$, which is certainly a subgroup of the algebraic group G^* , is a closed set in G^* so that, by the inductive hypothesis, it is possible to select in it linearly independent vectors $e_1^*, \dots, e_s^*, f_1^*, \dots, f_t^*$. Choose vectors e_i and f_j in H such that $\varphi(e_i) = e_i^*$, $\varphi(f_j) = f_j^*$. We first show that every vector of the form $\mu^1 f_1 + \dots + \mu^t f_t$, where μ^1, \dots, μ^t are arbitrary real numbers, belongs to H . Indeed choose $x \in H$ such that $\varphi(x) = \mu^1 f_1^* + \dots + \mu^t f_t^*$; then $x - \mu^1 f_1 - \dots - \mu^t f_t = \mu f$ and therefore $\mu^1 f_1 + \dots + \mu^t f_t = x - \mu f \in H$. Finally, let $y \in H$. Then $\varphi(y) = \lambda^1 e_1^* + \dots + \lambda^s e_s^* + \mu^1 f_1^* + \dots + \mu^t f_t^*$. Accordingly

$$y = \lambda^1 e_1 + \dots + \lambda^s e_s + \mu^1 f_1 + \dots + \mu^t f_t + \mu f_{t+1}$$

where $f_{t+1} = f$.

Example 34: Let G be the topological group of all non-singular complex square matrices of order n (see Ex. 31). The set G' of all real matrices in G is a subgroup of G . Similarly the set G'' of all real matrices with positive determinant is a subgroup of G' . The set H' of orthogonal matrices in G' (see Ex. 3) is a subgroup of G' while the set H'' of orthogonal matrices in G'' is a subgroup of G'' . The groups G' and G'' are locally compact while H' and H'' are compact. All of these groups admit countable bases.

SECTION 20. ISOMORPHISM. HOMOMORPHISM

In this section the definitions and relations established in Section 3 for abstract groups are extended to topological groups.

From the point of view of our theory two topological groups are regarded as indistinguishable if they possess identical topologo-algebraic structure. This idea is formulated more precisely in the following definition.

Definition 26. A mapping f of a topological group G onto a topological group G' is said to be an isomorphic mapping or an isomorphism if 1) f is an isomorphism of the algebraic group G onto the algebraic group G' ; 2) f is a homeomorphism of the topological space G onto the topological space G' . If $G' = G$ the isomorphism is called an automorphism. Two topological groups are isomorphic if there exists an isomorphism of one of them onto the other.

Below it will be shown by examples that two topological groups can be isomorphic as algebraic groups without being isomorphic topological groups.

Definition 27: A mapping g of a topological group G into a topological group G^* is a homomorphism if: (1) g is a homomorphism of the algebraic group G into the algebraic group G^* ; 2) g is a continuous mapping of the topological space G into the topological space G^* . A homomorphism g of a topological group G into a topological group G^* is said to be open if g is an open mapping of the topological space G into the topological space G^* (see Section 10 E)).

The distinction between open and non-open homomorphisms is very important in the theory of topological groups. Indeed, as we shall see, the open homomorphism is the natural generalization to topological groups of the concept of homomorphism in group theory.

A) Let G and G^* be two topological groups and let g be a homomorphism of the algebraic group G into the algebraic group G^* . Then in order that g should be a continuous or an open mapping it suffices that it should be so at the identity element e in G , i.e., it is sufficient that condition a) or b) respectively should be satisfied:

- a) For every neighborhood U^* of the identity e^* in G^* there exists a neighborhood U of e such that $g(U) \subset U^*$;
- b) For every neighborhood V of e there exists a neighborhood V^* of e^* such that $g(V) \supset V^*$.

Indeed suppose a) is satisfied. Let $a \in G$, $g(a) = a^*$ and let U^* be an arbitrary neighborhood of a^* . Then U^*a^{*-1} is an open set containing e^* so that by a) there exists a neighborhood U' of e such that $g(U') \subset U^*a^{*-1}$. The open set $U = U'a$ contains a neighborhood V of a and we have $g(V) \subset g(U')$ $g(a) \subset U^*a^{*-1}a^* = U^*$. Thus g is continuous. In analogous fashion it may be shown that b) implies that g is open.

B) Let G be a topological group, N a normal subgroup and G/N the factor group. Then the natural projection g (i.e., the mapping assigning to each element $x \in G$ that coset $X \in G/N$ which contains x) is an open homomorphism of G onto G/N .

Indeed, it was shown in Section 3 that g is a homomorphism of the algebraic group G onto the algebraic group G/N and in Section 19 it was shown that g is an open continuous mapping of the topological space G onto the topological space G/N (see Section 19, C)). Thus the conditions of Definition 27 are satisfied.

The following theorem provides a converse to B):

Theorem 11: Let G and G^* be two topological groups and let g be an open homomorphism of G onto G^* having kernel N . Then N is a normal subgroup of G and the isomorphism of the algebraic group G/N onto the algebraic group G^* defined in Theorem 1 (and which we continue to call the natural isomorphism associated with g) is an isomorphism of the topological group G/N onto the topological group G^* .

Proof: It follows from Theorem 1 that N is a normal subgroup of the algebraic group G . Since N is the inverse image of the single point e^* under the continuous mapping g it follows that N is also a closed subset in G and is therefore a normal subgroup of the topological group G .

Now let x^* be an arbitrary element of G^* and let $X = g^{-1}(x^*)$. By Theorem 1, X is a coset of N in G . Define $f(x^*) = X$. It was also shown in Theorem 1 that f is an isomorphism between the algebraic groups G^* and G/N . Thus it remains only to show that

f is a homeomorphism between the topological spaces G^* and G/N . We shall verify that both f and f^{-1} are continuous.

Let $a^* \in G^*$ and let $f(a^*) = A$. Denote by U^* an arbitrary neighborhood of A in the space G/N . According to Definition 24, U^* consists of all cosets of the form Nx , $x \in U$, where U is some fixed neighborhood in the space G . Let a be an element in U such that $A = Na$. Then $g(a) = a^*$ and since g is open there exists a neighborhood V^* of a^* such that $g(U) \supset V^*$. From this it follows that $f(V^*) \subset U^*$. Indeed let $x^* \in V^*$. Then there exists an element $x \in U$ such that $g(x) = x^*$. Consequently $f(x^*) = Nx \in U^*$. Thus f is continuous.

Next let $A = Na \in G/N$ and let $f^{-1}(A) = a^*$. Let also U^* be an arbitrary neighborhood of a^* . Then $g(a) = a^*$ and since g is continuous there exists a neighborhood V of a such that $g(V) \subset U^*$. Denote by V^* the neighborhood of A in G/N consisting of all cosets of the form Nx , $x \in V$. Since $g(V) \subset U^*$ it follows that $f^{-1}(V^*) \subset U^*$. Thus f^{-1} is also continuous. This completes the proof of Theorem 11.

It is worth noting that if g is not open then the proof of the continuity of f^{-1} goes through as above but the mapping f will fail to be continuous.

C) Note that if an open homomorphic mapping g of a topological group G onto the topological group G^* has kernel consisting of the identity only then the mapping is an isomorphism.

Indeed in this case g is one-to-one and coincides with the isomorphism between the groups G/N and G^* constructed in Theorem 11.

D) Let G and G^* be topological groups and let f be an open homomorphic mapping of G onto G^* . Denote by N' the kernel of f . Then f gives rise to a one-to-one correspondence between the subgroups of G^* and those subgroups of G which contain N' as follows: if N^* is a subgroup of G^* then the subgroup N of G corresponding to it is just the inverse image $N = f^{-1}(N^*)$; if N is a subgroup of G containing N' then the subgroup N^* of G^* corresponding to it is just the image $N^* = f(N)$. The two correspondences thus defined are mutually inverse to one another. Moreover, normal subgroups correspond to one another. Finally if N and N^* are two normal subgroups corresponding to one another in this fashion then the factor groups G/N and G^*/N^* are isomorphic.

We consider first the correspondence of N to N^* . As the inverse image of the closed subset N^* , N is also closed and contains N' . Moreover N is a subgroup of the algebraic group G (see Section 3 G)). Thus N is a subgroup of the topological group G . Moreover if N^* is a normal subgroup of G^* and if g denotes the natural

projection of G^* onto the factor group $G^*/N^* = G^{**}$ then $h = gf$ is an open homomorphism of G onto G^{**} with kernel N . Accordingly, by Theorem 11, N is a normal subgroup of G and the factor groups G/N and G^*/N^* are isomorphic with one another.

Consider next the correspondence of N^* to N where $N^* = f(N)$ and $N \supset N'$. We first show that the inverse image of N^* under the mapping f coincides with N . Indeed if $f(a) \in N^*$ then there exists an element $b \in N$ such that $f(a) = f(b)$; but then $f(ab^{-1}) = e^*$, i.e., $ab^{-1} \in N' \subset N$ so that $a \in Nb = N$. But from this it follows that $f(G \setminus N) = G^* \setminus N^*$. Since f is open and $G \setminus N$ is an open set this shows that $G^* \setminus N^*$ is also open and hence that the set N^* is closed in G^* . The fact that N^* is a subgroup and indeed a normal subgroup if N is normal may be immediately verified (see Section 3 F)).

The following theorem shows that, for a broad class of topological groups, homomorphisms are automatically open.

Theorem 12: Let G be a locally compact topological group the space of which can be represented as the set theoretical union of a countable number of compact subsets and let g be a homomorphism of G onto a locally compact group G^* . Then g is open.

Proof. By A) it suffices to show that for an arbitrary neighborhood U of the identity element of the group G there exists a neighborhood U^* of the identity element of G^* such that $g(U) \supset U^*$. Select a neighborhood V of the identity in G such that the set $F = \overline{V}$ is compact and such that $FF^{-1} \subset U$. Let Σ be a countable collection of compact sets in G with union equal to G . For each set $E \in \Sigma$ the collection of open sets Vx , $x \in E$, covers E so there is a finite covering of E by means of open sets of the form Vx , $x \in E$. Since Σ is countable it follows that there exists in G a sequence a_1, a_2, \dots such that the sets $F_i = Fa_i$, $i = 1, 2, \dots$ cover G . Let $F^* = g(F_i)$. Then the sets F_{1*}, F_{2*}, \dots likewise cover G^* .

We shall show that $g(F)$ contains an open set in the space G^* . Indeed, if not then no one of the sets F_{i*} could contain an open set. We shall show that this is impossible. Let W_{0*} be an arbitrary neighborhood in G^* with compact closure. If F_{1*} contains no open set it follows that there exists a neighborhood W_{1*} the closure of which is compact and entirely contained in the set $W_{0*} \setminus F_{1*}$. Then if F_{2*} contains no open set there exists a neighborhood W_{2*} the closure of which is compact and contained in the set $W_{1*} \setminus F_{2*}$. Continuing this process inductively we obtain an infinite sequence of neighborhoods $W_{0*}, W_{1*}, W_{2*}, \dots$ with compact closures and satisfying the condition $W_{i*} \subset W_{i-1*} \setminus F_i$, $i = 1, 2, \dots$ Since the sets W_{i*} are compact and non-empty their intersection is not empty (see Th. 4) and cannot be contained in the union

of the set F_i^* , $i = 1, 2, \dots$. But this is impossible since the latter sets cover G^* . Thus it follows that $g(F)$ contains some open set V^* .

Now let $a^* \in V^*$ and let a be a point in F such that $g(a) = a^*$. Since $FF^{-1} \subset U$ it follows that $Fa^{-1} \subset U$ and consequently $g(U) \supset g(F)a^{*-1} \supset V^*a^{*-1}$. But V^*a^{*-1} as an open set containing the identity element of G^* . Thus Theorem 12 is proved.

Observe that the hypothesis of local compactness in the group G^* was not fully used in the above proof; the argument remains valid if G^* is only locally countably compact (see Ex. 25).

We point out here two important classes of topological groups to which Theorem 12 is applicable.

E) A locally compact topological group G the space of which is separable may be represented as the union of a countable number of compact subsets.

Selecting one point each from the neighborhoods of a countable base in G we obtain a countable everywhere dense set M in G . Let U be a neighborhood of the identity in G having compact closure. Since M is everywhere dense it follows that for every $x \in G$ the open set $U^{-1}x$ meets M . Consequently there exists a point $a \in M$ belonging to $U^{-1}x$ and we obtain $x \in Ua$. Thus the compact sets $\bar{U}a$, $a \in M$, cover the entire group G .

F) We shall say that a topological group G is compactly generated if there exists a neighborhood V of the identity element with compact closure \bar{V} which generates the entire group G (by the latter is meant that the minimal subgroup of the algebraic group G containing V is G itself). Then $U = V \cup V^{-1}$ is a symmetric ($U^{-1} = U$) neighborhood of the identity element with compact closure which generates G so that $G = \bigcup U \cup U^2 \cup \dots \cup U^n \cup \dots$ Since each of the sets \bar{U}^n is compact (see Section 17 G)) it follows that G is the union of a countable number of compact sets and Theorem 12 is applicable to G . An important class of compactly generated groups is the class of connected locally compact groups (see Th. 14). Observe also that if G possesses a compact normal subgroup N such that the factor group G/N is compactly generated then G itself is compactly generated.

We prove the last assertion. Let f be the natural projection of G onto G/N and let V^* be a neighborhood with compact closure which generates G/N . Then $V = f^{-1}(V^*)$ is a neighborhood generating G and since $f^{-1}(\bar{V}^*)$ is a compact set (see Section 19 I)) it follows that $\bar{V} \subset f^{-1}(\bar{V}^*)$ is also compact.

The following is a simple corollary of Theorem 12:

G) Let G be a locally compact group the space of which is the union of a countable number of compact sets and let H and N be a subgroup and a normal subgroup respectively in G . Suppose that HN is a closed set in G . Then $HN = NH$ is a subgroup of G , $H \cap N$ is a normal subgroup of the group H and the factor groups $(HN)/N$ and $H/(H \cap N)$ are isomorphic with one another.

Since the normal subgroup N commutes with every element of G it is immediate that $HN = NH$. Therefore $HN(HN)^{-1} = HNN^{-1}H^{-1} = HN$ and HN is a subgroup of the algebraic group G . Since HN is closed in G by hypothesis, it follows that HN is a subgroup of the topological group G . Denote by f the natural projection of HN onto the factor group $(HN)/N$. Since G is locally compact so is $(HN)/N$ (see Section 19 H)). Since N is the kernel of f we have $f(HN) = f(H)$ and the kernel of the homomorphism f restricted to H is just $H \cap N$. Finally, since H is locally compact and its space is also the union of a countable number of compact sets, Theorem 12 is applicable to the homomorphism f of H onto $(HN)/N$ and therefore, by Theorem 11, the groups $(HN)/N$ and $H/(H \cap N)$ are isomorphic.

Example 35: Let G denote the additive group of real numbers with the discrete topology and let G^* denote the additive group of real numbers in the natural topology. Associate with each real number $x \in G$ the same real number $x^* \in G^*$, $g(x) = x^*$. It is obvious that g is a homomorphic mapping of G onto G^* . The algebraic mapping g is even an isomorphism. However g is not open and is therefore not an isomorphism between the topological groups G and G^* . Indeed each element x in G forms, all by itself, an open set. But this is by no means true of the corresponding element x^* . The impossibility of applying Theorem 12 here is explained by the fact that G cannot be represented as the union of a countable number of compact sets.

Example 36: Let G denote the plane with a fixed Cartesian coordinate system. The points, or, what comes to the same thing, the vectors, of the plane form an additive topological group. Let also H be a line in G passing through the origin. The slope of the line we denote by α . H is obviously a subgroup of the topological group G . Denote also by N the set of all points in the plane G possessing integral coordinates. Then N is also a subgroup of G . Let $G^* = G/N$ and denote by g the natural projection of G onto G^* . The homomorphism g carries the subgroup H onto a set H^* which is necessarily a subgroup of the algebraic group G^* (see Section 3 F)). However, H^* need not be a closed set in the topological space G^* . If α is a rational number then it is not difficult

to verify that H^* is a closed set, in fact, a closed curve, in G^* . If, on the other hand, α is irrational then H^* is everywhere dense in G^* .

In order to prove the latter assertion we anticipate the result discussed in Example 65. It is easy to see that if α is irrational then there exists a number β such that β and $\alpha\beta$ are linearly independent, i.e., such that $p\beta + q\alpha\beta = r$ where p , q , and r are whole numbers implies $p = q = r = 0$. Denote by a the element of G with coordinates β and $\alpha\beta$ respectively, and by A the subgroup generated by a . Then $A \subset H$. moreover, according to Example 65, it follows that $g(A)$ is everywhere dense in G^* . Accordingly the subgroup H^* is also everywhere dense.

We see that in the case of irrational α the subgroup H^* is by no means closed. Thus in this case H^* is not a subgroup of the topological group G^* ; nonetheless H^* is a topological group in its own right (see Section 19 A)). Moreover the mapping g of H onto H^* is continuous and is algebraically a homomorphism, even an isomorphism, but it is not open. It is not difficult to verify that H^* is not locally compact, which explains the inapplicability here of Theorem 12. Note that the algebraic group H and H^* are isomorphic while the topological groups H and H^* are not isomorphic. They are not even homeomorphic since once of them is locally compact and the other is not.

Example 37: Let G be a compact topological group. Then in every neighborhood U of the identity e of G there exists a normal subgroup N such that the factor group G/N is separable. This proposition permits the reduction of the proof of many theorems on compact groups to the separable case.

According to Urysohn's Lemma there exists on G a continuous real function f which is everywhere non-negative, vanishes on the set $G \setminus U$ and is positive at e . We introduce among the elements of G an equivalence relation by defining the elements a and b to be equivalent, $a \sim b$, if $f(xay) = f(xby)$ for every x and y in G . It is obvious that this relation is reflexive, symmetric and transitive. The equivalence class containing the identity e we denote by N . We shall show that N is a normal subgroup of the topological group G and that the various equivalence classes are nothing but the cosets in G of the subgroup N .

That N is a closed set follows from the continuity of f . Let a and b be two elements of N . We have: $f(xay) = f(xy)$; since this relation holds for arbitrary x and y we may replace x by xa^{-1} obtaining $f(xy) = f(xa^{-1}y)$, i.e., $a^{-1} \in N$.

Moreover $f(xaby) = f(xa(by)) = f(xby) = f(xy)$; thus $a, b \in N$. Accordingly N is a subgroup of the topological group G . Next let z be an arbitrary element of G . Then $f(xay) = f(xy)$ for arbitrary x and y . Replacing x by xz^{-1} and y by zy we obtain $f(xz^{-1}azy) = f(xy)$, i.e., $z^{-1}az \in N$. Thus N is normal. Finally suppose $c \sim d$. Then $f(xcy) = f(xdy)$ and replacing y by $d^{-1}y$ we obtain $f(xcd^{-1}y) = f(xy)$, i.e., $cd^{-1} \in N$. If, on the other hand, $cd^{-1} \in N$ then $f(xcd^{-1}y) = f(xy)$ and replacing y by dy we obtain $f(xcy) = f(xdy)$, i.e., $c \sim d$.

From what has been shown it follows that, for fixed x and y , the function $f(xay)$ of the argument a is constant on the coset A of a , so that we may define $f(xAy)$ by letting $f(xAy) = f(xay)$ where $a \in A$. We next introduce a metric into the algebraic group G/N by defining $\rho(A, B)$ to be the maximum of the absolute values $|f(xAy) - f(xBy)|$ as x, y take on all values in G . It is not difficult to show that the topology defined by this metric coincides with the topology of the factor group G/N (see Def. 24). Since a compact metric space admits a countable base (see Ex. 26) the proposition is proved.

SECTION 21. THE DIRECT PRODUCT OF TOPOLOGICAL GROUPS

In the present paragraph is given a definition of direct product of topological groups obtained by simply uniting the concept of the direct product of groups introduced in Section 5 with that of the product of topological spaces introduced in Section 14. I shall first define the direct product of a finite number of arbitrary topological groups and subsequently the direct product of an arbitrary collection of compact groups. The latter definition coincides with the former in the case of a finite number of factors; however the corresponding concept of the resolution of a topological group into a direct product of its subgroups is useful only for compact groups even in the case of a finite number of subgroups. In view of this fact, I am unable here to reduce the study of a finite number of factors to the case of two factors as was done for algebraic groups in Section 5.

Definition 28: Let N_1, \dots, N_k be a finite sequence of topological groups. Denote by G' the collection of all sequences $x = (x_1, \dots, x_k)$ where $x_i \in N_i$, $i = 1, \dots, k$. Then, according to Section 5 A) and Definition 10, the set G' is an algebraic group while, according to Section 14 A) and Definition 20, G' is also a topological space. Moreover the group operations in G' are continuous in the topological

space G' so that, according to Definition 22, G' is a topological group. The topological group G' is called the direct product of the groups N_1, \dots, N_k : $G' = N_1 \times \dots \times N_k$.

We must show that the group operations in G' are continuous in the topological space G' . Let $x = (x_1, \dots, x_k)$ and $y = (y_1, \dots, y_k)$ be two elements of G' and let $xy^{-1} = z = (z_1, \dots, z_k)$, i.e., $z_i = x_i y_i^{-1}$, $i = 1, \dots, k$. Let also $W = (W_1, \dots, W_k)$ be an arbitrary neighborhood of z in G' . Then W_i is a neighborhood of z_i in the space N_i . Since the group operations are continuous in the topological group N_i there exist in its neighborhoods U_i and V_i of the elements x_i and y_i such that $U_i V_i^{-1} \subset W_i$. It follows readily that the neighborhoods $U = (U_1, \dots, U_k)$ and $V = (V_1, \dots, V_k)$ of x and y in G' satisfy the condition $UV^{-1} \subset W$.

A) Let N_1, \dots, N_k be topological groups with identity elements e_1, \dots, e_k respectively and let G' denote their direct product. Denote by $e' = (e_1, \dots, e_k)$ the identity element of G' . To each element $x_i \in N_i$ we associate the element $f_i(x_i) = (e_1, \dots, x_1, \dots, e_k) \in G'$. The mapping f_i is an isomorphism of the topological group N_i onto a normal subgroup N'_i of G' . It follows from F) Section 5 that the algebraic group G' resolves into the direct product of the subgroups N'_1, \dots, N'_k (see Def. 10'). Moreover, for arbitrary neighborhoods U'_1, \dots, U'_k of e' relative to the subgroups N'_1, \dots, N'_k the group product $U'_1 U'_2 \dots U'_k$ contains a neighborhood U' of e' relative to the whole group G' .

The fact that f_i is an isomorphism of the algebraic group N_i onto a normal subgroup of the algebraic group G' has already been proved in F) Section 5; that the set N'_i is closed follows from A) Section 14. Thus it remains only to show that f_i is a continuous open mapping of the topological group N_i onto the topological group N'_i . That this is so follows immediately from an examination of what is meant by a neighborhood U'_i of the identity e' relative to the group N'_i . We here regard N'_i as a subspace of the topological space G' and neighborhoods are to be constructed accordingly. Thus to obtain a neighborhood U'_i we begin with neighborhoods U_1, \dots, U_k of the identities in the spaces N_1, \dots, N_k , form the neighborhood $U' = (U_1, \dots, U_k)$ of e' in G' and finally take U'_i to be the intersection $N'_i \cap U'$. But then $U'_i = f_i(U_i)$. Hence for an arbitrary neighborhood U'_i of e' in the group N'_i there exists a neighborhood U_i of the identity in N_i such that $U'_i = f_i(U_i)$, and conversely if U_i is an arbitrary neighborhood of the identity in N_i then $U'_i = f_i(U_i)$ is a neighborhood of the identity in N'_i . This shows that f_i is both open and continuous so that it is, in fact, an isomorphic mapping of the topological

group N_i onto the topological group N'_i . Moreover, it is obvious that the product $U_1'U_2' \dots U_k'$ is simply U' . Thus the last assertion of proposition A) is also proved.

Proposition A) leads to an alternative formulation of the definition of direct product.

Definition 28': Let G be a topological group and let N_1, \dots, N_k be normal subgroups. We shall say that the topological group G resolves into the direct product of the subgroups N_1, \dots, N_k if the algebraic group G resolves into the direct product of the subgroups N_1, \dots, N_k (see Def. 10') and if, moreover, the following condition is satisfied: for arbitrary neighborhoods U_1, \dots, U_k of the identity element e relative to the groups N_1, \dots, N_k the groups product $U_1U_2 \dots U_k$ contains a neighborhood U of e relative to the group G .

The connection between Definitions 28 and 28' is established by proposition A) and by the following result.

B) Suppose the topological group G resolves into the direct product of subgroups N_1, \dots, N_k and let G' denote the direct product of the topological groups N_1, \dots, N_k (see Def. 28). To each element $x = (x_1, \dots, x_k) \in G'$ we associate the element $f(x) = x_1x_2 \dots x_k \in G$. Then f is an isomorphism of the topological group G' onto the topological group G and ff_i (f_i defined as in A)) is the identity mapping of N_i onto itself.

The purely algebraic parts of this proposition have already been proved in Section 5 (see Section 5B), G)); we will be done if we show that f is open and continuous at the identity element (see Section 20 A)). We begin by showing continuity. Let U be a neighborhood of the identity in G and let V be another neighborhood of the identity in G such that $V^k \subset U$. Let $V_i = N_i \cap V$; then $V' = (V_1, \dots, V_k)$ is a neighborhood of the identity in G' . Clearly $f(V') = V_1V_2 \dots V_k \subset V^k \subset U$. Thus f is continuous. Next let $U' = (U_1, \dots, U_k)$ be any neighborhood of the identity in G' ; here U_i is a neighborhood of the identity in the group N_i . By virtue of Definition 28' the group product $U_1U_2 \dots U_k$ contains a neighborhood U of the identity in the group G , i.e., $f(U') = U_1U_2 \dots U_k \supset U$. Accordingly the mapping f is also open.

The following theorem shows that in certain important cases the conditions of Definition 28' may be weakened.

Theorem 13: Let G be a locally compact topological group whose space is the union of a countable number of compact sets and let N_1, \dots, N_k be normal subgroups of G . Then if the algebraic group G resolves into the direct product of N_1, \dots, N_k the

same must be true of the topological group G .

Proof: It suffices to show that, for arbitrary neighborhoods U_1, \dots, U_k of the identity relative to the subgroups N_1, \dots, N_k , the product $U_1 U_2 \dots U_k$ is open in G . Consider once again the algebraic isomorphism f of the direct product $G' = N_1 \times \dots \times N_k$ onto G that assigns to each $x = (x_1, \dots, x_k) \in G'$ the product $f(x) = x_1 x_2 \dots x_k \in G$. If $U' = (U_1, \dots, U_k)$ then $f(U') = U_1 U_2 \dots U_k$; hence it suffices to show that f is an open mapping. Also the continuity of f may be proved exactly as above. Thus Theorem 12 may be invoked to obtain the desired conclusion as soon as we verify that the necessary hypotheses are satisfied by the group G' . In the first place, since each N_i is closed in G and therefore locally compact (Section 13 B)), the local compactness of G' follows from Section 14 E). Moreover, it is clear that each N_i is the union of a countable number of compact sets, and since the product of compact sets is compact, it follows at once that the same is true of G' . Thus the hypotheses of Theorem 12 are satisfied and the result follows.

To facilitate the definition of the direct product of an arbitrary collection of compact topological groups we here interpolate some remarks on the intersection and product of collections of normal subgroups of a topological group.

C) Let Ω be a collection of normal subgroups of the topological group G . Then the intersection $\Delta(\Omega)$ of the subgroups belonging to Ω , being the intersection of normal subgroups, is a normal subgroup of the algebraic group G and is also a closed set in G , being the intersection of closed sets. Accordingly $\Delta(\Omega)$ is a normal subgroup of the topological group G . The minimal normal subgroup $\Pi(\Omega)$ (see Section 5 E)) of the algebraic group G containing all the normal subgroups in the set Ω is in general not a normal subgroup of the topological group G since it need not be closed; however its closure $\overline{\Pi}(\Omega) = \overline{\Pi(\Omega)}$ is a normal subgroup of the topological group G according to Section 19 B) and this last subgroup, as is easily seen, is the minimal normal subgroup of a topological group G containing the normal subgroups of the set Ω .

Definition 29: Let Ω be an arbitrary collection of compact topological groups and let α be a function associating with each group $N \in \Omega$ an element $\alpha(N) \in N$. The set of all such functions α we denote by G^* . Now, on the one hand, G^* is nothing other than the full direct product of all the groups of the collection Ω (see Def. 10) and is, in particular, an algebraic group; on the other hand, G^* is a compact topological space (see Def. 20 and

Th. 5). Moreover the group operations defined in G^* are continuous in the topological space G^* . The compact topological group G^* thus obtained is the direct product of the set Ω of topological groups.

Clearly if Ω is a finite collection of compact groups then Definitions 28 and 29 agree.

We must establish the continuity of the group operations in G^* . Let α and β be two elements of G^* and let $\gamma = \alpha\beta^{-1}$. Moreover let $W = N_1^{-1}(W_1) \cap \dots \cap N_k^{-1}(W_k)$ be a neighborhood of γ in G^* (see Def. 20). Since $\alpha(N_i)(\beta(N_i))^{-1} = \gamma(N_i)$ and since N_i is a topological group there exist neighborhoods U and V of the elements $\alpha(N_i)$ and $\beta(N_i)$ such that $U_i V_i^{-1} \subset W_i$. It is easy to verify that the neighborhoods $U = N_1^{-1}(U_1) \cap \dots \cap N_k^{-1}(U_k)$ and $V = N_1^{-1}(V_1) \cap \dots \cap N_k^{-1}(V_k)$ of the elements α and β respectively satisfy the condition $UV^{-1} \subset W$.

D) Let G^* denote the direct product of a collection Ω of compact topological groups and let $x \in N \in \Omega$. To the pair N, x we associate the function $\alpha_{N,x} \in G^*$ defined by $\alpha_{N,x}(P) = x$ for $P = N, \alpha_{N,x}(P) = e^*(P)$ for $P \neq N$. We define also $f_N(x) = \alpha_{N,x}$. The function f_N , depending on N , associates with each element $x \in N$ the element $f_N(x) \in G^*$. Now f_N is an isomorphism of the topological group N onto a normal subgroup N^* of the topological group G^* . Denote by Ω^* the collection of all normal subgroups N^* , $N \in \Omega$, and let $\Omega^*_{N^*} = \Omega^* \setminus N^*$, $K^*_{N^*} = \overline{\Pi}(\Omega^*_{N^*})$. Finally denote by $\hat{\Omega}^*$ the collection of all normal subgroups $K^*_{N^*}$ for $N \in \Omega$. Then

$$\overline{\Pi}(\Omega^*) = G^* \quad (1)$$

$$\Delta(\hat{\Omega}^*) = \{e^*\} \quad (2)$$

The fact that f_N is an isomorphism of the algebraic group N onto a normal subgroup of the algebraic group G^* was proved in Section 5 F). The fact that f_N is continuous follows as in A). The continuity of f_N^{-1} and the fact that N^* is closed in G^* follow from D), C), E) of Section 13 since N is compact. A brief examination shows that the group N^* consists of all functions $\alpha \in G^*$ satisfying the condition $\alpha(P) = e^*(P) \neq N$. Accordingly, $\Pi(\Omega^*_{N^*})$ consists of all functions $\beta \in G^*$ satisfying the condition $\beta(N) = e^*(N)$ and taking values different from the identity at only a finite number of groups of the collection Ω . Recalling the definition of the topology in the space G^* we conclude at once that the closure $\overline{\Pi}(\Omega^*_{N^*}) = K^*_{N^*}$ of the set $\Pi(\Omega^*_{N^*})$ consists of all functions $\beta \in G$ satisfying the condition $\beta(N) = e^*(N)$. Thus (2) is obvious. Sim-

ilarly, it is easy to see that $\Pi(\Omega^*)$ consists of all functions $\alpha \in G^*$ taking values different from the identity at only a finite number of groups of the collection Ω , whence (1) follows immediately and proposition B) is proved

Proposition B) leads to a reformulation of a definition of direct product for collections of compact topological groups.

Definition 29': Let G be a compact topological group with identity element e and let Ω be a collection of normal subgroups in G . For each $N \in \Omega$ let $\Omega_N = \Omega \setminus N$ and $K_N = \overline{\Pi}(\Omega_N)$. Finally denote by $\hat{\Omega}$ the collection of all normal subgroups K_N , $N \in \Omega$. We shall say that the compact topological group G resolves into the direct product of the subgroups $N \in \Omega$ if the following conditions are satisfied:

$$\Pi(\Omega) = G, \quad (3)$$

$$\Delta(\hat{\Omega}) = \{e\}. \quad (4)$$

If the set Ω is finite then the equivalence of Definitions 28' and 29' follows from Theorem 13.

The connection between Definitions 29 and 29' is established in D) and the following proposition.

E) Suppose the compact topological group G resolves into the direct product of a collection Ω of its subgroups. Then

$$G = N \times K_N \quad (5)$$

for each group $N \in \Omega$ and for each pair of distinct groups N and P in Ω every element of N commutes with every element of P . Moreover, if G^* denotes the direct product of the groups of the collection Ω according to Definition 29, then there exists one and only one isomorphism f of the topological group G^* onto the topological group G such that composition ff_N is the identity mapping of the group N onto itself for each group $N \in \Omega$.

We begin by establishing (5). In the first place, that

$$NK_N = G \quad (6)$$

follows from the definition of K_N and from (3). Let now $\hat{\Omega}_N = \Omega \setminus K_N$ and let $N' = \Delta(\hat{\Omega}_N)$. Clearly $N \subset N'$, but by (4) $N' \cap K_N = e$. Thus

$$N \cap K_N = e \quad (7)$$

But by Theorem 13, (6) and (7) together imply (5).

The commutativity of the elements of P and N now follows from the fact that $P \subset K_N$ for $P \neq N$.

We note also that the requirement that ff_N should be the identity mapping on each group $N \in \Omega$ determines f uniquely on the everywhere dense subset $\Pi(\Omega^*)$ in the space G^* . Thus f is unique if it exists.

We proceed now to the construction of the mapping f . For each finite subset

$$\Sigma = \{N_1, N_2, \dots, N_k\} \quad (8)$$

of the set Ω we define

$$K(\Sigma) = K_{N_1} \cap K_{N_2} \cap \dots \cap K_{N_k} \quad (9)$$

Each of the sets $K(\Sigma)$ thus obtained is a normal subgroup of G and satisfies the condition

$$N \subset K(\Sigma) \text{ for all } N \in \Sigma. \quad (10)$$

We next define for $\alpha \in G^*$

$$K(\alpha, \Sigma) = \alpha(N_1) \alpha(N_2) \dots \alpha(N_k) K(\Sigma) \quad (11)$$

and show that the collection of all subsets $K(\alpha, \Sigma)$, where α denotes a fixed element of the group G^* while Σ denotes an arbitrary finite subset of Ω , possesses the finite intersection property. To this end it suffices, as is easily seen, to show that if

$$\Sigma' = \{N_1, N_2, \dots, N_k, N_{k+1}, \dots, N_l\} \quad (12)$$

is, as the notation indicates, a finite subset of Ω containing the set Σ then $K(\alpha, \Sigma') \subset K(\alpha, \Sigma)$. But the latter inclusion follows from (10) inasmuch as $\alpha(N_{k+1}) \alpha(N_{k+2}) \dots \alpha(N_l) K(\Sigma') \subset K(\Sigma)$. It follows that the intersection of the collection of all sets $K(\alpha, \Sigma)$ is non-empty; we shall show that it contains only one point. Indeed suppose the contrary: let x and y be two distinct points belonging to the intersection. Since $xy^{-1} \neq e$, while the intersection of the normal subgroups $K(\Sigma)$ contains only the identity, there exists a finite subset $\Sigma \subset \Omega$ such that $xy^{-1} \in K(\Sigma)$. On the other hand

$$xy^{-1} \in K(\alpha, \Sigma)(K(\alpha, \Sigma))^{-1} = K(\Sigma)(K(\Sigma))^{-1} = K(\Sigma)$$

Thus for fixed $\alpha \in G^*$ there exists one and only one point x belonging to all of the sets $K(\alpha, \Sigma)$; this point we define to be $f(\alpha)$. Accordingly we have

$$f(\alpha) \in K(\alpha, \Sigma), \quad \Sigma \subset \Omega \quad (13)$$

which may be regarded as the defining relation for $f(\alpha)$. A trivial calculation shows that ff_N is the identity mapping of N onto itself.

We next show that f is an algebraic homomorphism. Let α and β be two elements of G^* and let $\gamma = \alpha\beta$; then

$$f(\alpha)f(\beta) \in K(\alpha, \Sigma)K(\beta, \Sigma) = K(\gamma, \Sigma), \quad \Sigma \subset \Omega,$$

so that, by (13), $f(\alpha)f(\beta) = f(\gamma)$.

We next show that f is continuous. Let U be a neighborhood of the identity element in G . Since the intersection of all subgroups $K(\Sigma)$ contains only the identity there exists a finite subset $\Sigma \subset \Omega$ such that $K(\Sigma) \subset U$ (see Section 13 H)). We suppose Σ enumerated as in (8). Note now that the compact set $K(\Sigma)$ coincides with the intersection of all sets of the form $\overline{V}^k K(\Sigma)$ where V runs over all neighborhoods of the identity; consequently, using proposition H) of Section 13 once again, we see that there exists a neighborhood V of the identity such that

$$V^k K(\Sigma) \subset U$$

Now let $V_i = N_i \cap V$, $i = 1, \dots, k$ and define a neighborhood V^* of the identity in the group G^* by:

$$V^* = N_1^{-1}(V_1) \cap N_2^{-1}(V_2) \cap \dots \cap N_k^{-1}(V_k).$$

Let $\alpha \in V^*$; then $f(\alpha) \in \alpha(N_1)\alpha(N_2) \dots \alpha(N_k)K(\Sigma) \subset V^k K(\Sigma) \subset U$. Thus $f(V^*) \subset U$ and f is continuous.

We show next that $f(G^*) = G$. Since ff_N is the identity mapping on N the set $f(G^*)$ contains all groups of the collection Ω and therefore contains $\Pi(\Omega)$; since f is continuous the set $f(G^*)$ is also closed, whereupon the equation $f(G^*) = G$ follows from (3).

Next suppose $f(\alpha) = e$; then $e \in \alpha(N)K_N$ according to (13) so that $\alpha(N) \in K_N$. But according to (7) this implies $\alpha(N) = e$. It follows that $\alpha = e$ so that f is a one-to-one mapping.

We have thus shown that f is an isomorphism of the algebraic group G^* onto the algebraic group G and also that f is continuous; since G^* is compact it follows that f is also open. Accordingly f is an isomorphism of the topological group G^* onto the topological

group G and proposition E) is proved in full.

F) Let G^* be the direct product of a set Ω of topological groups. (If all the groups of the collection Ω are compact G^* is constructed according to Definition 29; otherwise we assume Ω to be finite and construct G^* according to Definition 28.) Suppose also that Ω is the union of two disjointing sets Ω_1 and Ω_2 . Denote by N_1^* the set of all functions $\alpha \in G^*$ associating with each group of the set Ω_2 its identity element, and analogously by N_2^* the set of all functions $\alpha \in G^*$ associating with each group of the set Ω_1 its identity element. It may be verified immediately that N_1^* and N_2^* are normal subgroups of the topological group G^* , that the algebraic group G^* resolves into the direct product of its subgroups N_1^* and N_2^* . that the condition of Definition 28' bearing on neighborhoods of the identity is satisfied. Thus the topological group G^* resolves into the direct product of the subgroups N_1^* and N_2^* . From this, and from the equivalence of Definitions 28 and 28' or 29 and 29' respectively, it follows that if the topological group G resolves into the direct product of a collection Ω of subgroups and if the collection Ω is the union of two disjoint collections Ω_1 and Ω_2 then the topological group G resolves onto the direct product of the subgroups $\bar{\Pi}(\Omega_1)$ and $\bar{\Pi}(\Omega_2)$.

G) Let the topological group G resolve into the direct product of two of its subgroups N_1 and N_2 . Then the factor group G/N_1 is isomorphic with N_2 ; indeed it may be immediately verified that associating with each element $x \in N_2$ the coset $f(x) \in G/N_1$ that contains x yields an isomorphism of N_2 onto G/N_1 .

Example 38: We continue the considerations of Example 36. As before, let G denote the plane with a fixed Cartesian coordinate system, let H denote a line through the origin of slope α and let N denote the set of all points with integral coordinates. Then H and N are normal subgroups of G . Denote by P the sum $H + N$, i.e., the set of all points of the form $h + n$ where $h \in H$, $n \in N$. If α is a rational number then the set P is closed in G while if α is irrational the set P is not closed.

Consider again the case in which α is irrational. The set P still forms a topological group (see Section 19 A)). But though the intersection $D = H \cap N$ contains only the origin, it is obvious that the condition of Definition 28' bearing on neighborhoods of the identity is not satisfied in this case so that the topological group P does not resolve into the direct product of the subgroups H and N .

Example 39: We construct an example of a countably compact topological group which is not compact; the construction is analogous to that in Example 28 of a countably compact topological

space that is not compact.

Let Ω denote an arbitrary non-countable collection of compact topological groups each of which contains at least two elements and denote by G^* the direct product of the groups of the collection Ω . Denote also by G the collection of all functions $\alpha \in G^*$ with the property that α takes values different from the identity at only a finite or countable set of groups in Ω . Since Ω is not itself countable it follows that $G \neq G^*$. On the other hand it is obvious that the closure \overline{G} of the set G does coincide with G^* , $G^* = \overline{G}$. Since G is a subgroup of the algebraic group G^* it is itself a topological group (see Section 19 A)). The fact that G is countably compact but not compact may be proved exactly as in Example 28.

Example 40: Let Ω denote a countable collection N_1, N_2, \dots of cyclic groups of order two. We regard each of the groups of the collection as a topological group in its discrete topology and we construct their compact direct product G^* . Each element $\alpha \in G^*$ may be represented as a sequence $\alpha = \{x_1, x_2, \dots\}$ of numbers where each x_i is either 0 or 1, x_k being taken to be 0 when $\alpha(N_k)$ is the identity of the group N_k and equal to one when $\alpha(N_k)$ is not the identity. The rule for multiplying or, better, for adding, elements of the group G^* is obvious. It is interesting to remark that the space G^* is homeomorphic with the Cantor set. Indeed every element of the Cantor set may also, as is well known, be represented by a sequence x_1, x_2, \dots of zeros and ones and the one-to-one correspondence thus established between the elements of G^* and the points of the Cantor set is readily verified to be a homeomorphism. Since the space of a topological group is homogeneous it follows that the Cantor set is likewise homogeneous.

It is not difficult to show that the direct product of a countable collection of finite groups, each containing at least two elements, is always homeomorphic with the Cantor set.

SECTION 22. CONNECTED AND TOTALLY DISCONNECTED GROUPS

In this paragraph we consider certain properties of topological groups specifically related to their topological structure and which possess no analogs in the theory of abstract groups.

A) Let G be an arbitrary topological group and denote by N

the component of the identity e in the topological space G (see Section 15 D)). Then N is a normal subgroup of G .

Let a and b be two elements of N . Since N is connected the set aN^{-1} is also connected and contains e . Accordingly $aN^{-1} \subset N$ and in particular $ab^{-1} \in N$, i.e., N is a subgroup of the algebraic group G . Since components are closed (see Section 15 D)) it follows that N is a subgroup of the topological group G . That N is normal may be shown in a similar fashion; if x is any element of G than $x^{-1}Nx$ is a connected set containing the identity so that $x^{-1}Nx \subset N$.

B) If the topological group G is connected, i.e., if the space G is connected, then the component of the identity in G coincides with G itself. If, on the other hand, the component of the identity in G consists of the identity only then by the homogeneity of G all components consist of single points and G is totally disconnected.

C) Let G be an arbitrary topological group and denote by N the component of the identity in G . Then the factor group $G/N = G^*$ is totally disconnected.

Let f be the natural projection of G onto G^* . Denote by P^* the component of the identity in G^* and by P the inverse image of P^* under f , $f^{-1}(P^*) = P$. We shall show that the mapping f of the space P onto P^* is open. Let U be an arbitrary open set in P . Then there exists an open set V in G such that $U = P \cap V$. It is easy to see that $f(U) = P^* \cap f(V)$. Since f is an open mapping of G onto G^* the set $f(V)$ is open in G^* and consequently $f(U)$ is open in P^* .

Suppose now that P^* contains elements different from the identity. Then N is a proper subset of P and P is not connected. Accordingly P may be written as the union of two disjoint sets A and B , each of which is non-empty and open in P (see Section 15 A)). If $a \in A$ then $Na \subset A$ since if the set Na met B it would be partitioned into two disjoint closed sets, which is impossible since Na is connected along with N . From this it follows that the sets $f(A)$ and $f(B)$ are disjoint. But these sets are open in the space P^* as we have seen. Thus P^* is partitioned into two disjoint open subsets which contradicts the assumption that P^* is connected.

We now take a somewhat closer look at the properties of connected groups.

Theorem 14: A connected topological group G is generated by an arbitrary neighborhood U of the identity. By this is meant

that G coincides with the union of all sets of the form U^n , $n = 1, 2, \dots$, or, what comes to the same thing, that every element of G may be written as a finite product of elements belonging to U .

Proof: Let V denote the union of the sets U^n . Since each U^n is open it follows that V is open. We shall show that V is also a closed set. Let $a \in \overline{V}$. Since aU^{-1} is a neighborhood of a it follows that there exists an element $b \in V$ such that $b \in aU^{-1}$. Since $b \in V$ there exists a number m such that $b \in U^m$ and consequently $b = u_1 u_2, \dots, u_m$ where $u_i \in U$, $i = 1, \dots, m$. Since also $b \in aU^{-1}$ we have $b = au_{m+1}^{-1}$ where $u_{m+1} \in U$. But then $a = u_1 u_2, \dots, u_m u_{m+1}$ where $u_j \in U$, $j = 1, \dots, m+1$ and consequently $a \in U^{m+1} \subset V$. Thus V is closed. Now let $W = G \setminus V$. Since V is a closed-open set, W is also and if W were not empty, the pair V, W would constitute a partition of G into two disjoint non-empty closed sets which would contradict the assumption that G is connected. Thus $G = V$.

D) The center Z of the algebraic group G (see Def. 7) is also called the center of the topological group G . The center is a normal subgroup. Every subgroup N of the topological group Z is also a normal subgroup of G and is called a central normal subgroup.

It was shown in Section 4 that Z is a normal subgroup of the algebraic group G . Thus it remains only to show that Z is closed. Let $a \in \overline{Z}$ and suppose there exists an element $x \in G$ such that $a' = x^{-1}ax \neq a$. Since G is Hausdorff (see Section 17) there exist disjoint neighborhoods U and U' of a and a' respectively. Let $V = Z \cap U$. Clearly $a \in \overline{V}$. But then $a' = x^{-1}ax \in x^{-1}\overline{V}x = x^{-1}Vx = V$ (see Section 17 B)). But this is impossible since U' is disjoint from \overline{V} . Thus $x^{-1}ax = a$ for every x so that $a \in Z$, i.e., $Z = Z$.

Finally, if N is a subgroup of Z then, being closed in Z , N is also closed in G (see Section 11 A)) and since N is a normal subgroup of the algebraic group G (see Section 4B) it follows that N is a normal subgroup of the topological group G .

Theorem 15: Every discrete normal subgroup N of a connected topological group G is a central normal subgroup.

Proof: Since N is discrete it follows that for each $a \in N$ there exists a neighborhood V not containing any other elements of N and since $e^{-1}ae = a$ there exists a neighborhood U of the identity such that $U^{-1}aU \subset V$. Let now $u \in U$; then $u^{-1}au \in V$ while, since N is a normal subgroup of G , we have also $u^{-1}au \in N$. Consequently $u^{-1}au = a$. If now x is an arbitrary element of G then by Theorem

$x = u_1 u_2 \dots u_n$ where $u_i \in U$, $i = 1, \dots, n$. Since a commutes with each of the factors u_i it follows that a commutes with x , i.e., $x^{-1}ax = a$. Thus N is contained in the center Z of the group G .

Theorem 15 is of considerable importance in that it facilitates the finding of the discrete normal subgroups of a connected group. Discrete normal subgroups play a major role in the theory of topological groups.

We turn now to the consideration of totally disconnected groups, limiting ourselves to the case of groups which are also locally compact.

Theorem 16: Let G be a locally compact totally disconnected topological group. Then for any neighborhood U of the identity element of G there exists a compact-open subgroup H such that $H \subset U$. Since H is open the space G/H is discrete.

Proof: Since e is a component in the space G it follows from proposition G) Section 15 that there exists a compact-open set P such that $e \in P \subset U$. Denote by Q the set of all elements $q \in G$ such that $Pq \subset P$. We shall show that $Q \cap Q^{-1} = H$ is a compact open subgroup of G contained in U .

We first show that Q is open. Let q be a fixed point in Q and let x be an arbitrary point in P . Since $xq \in P$ and P is open there exist neighborhoods U_x and V_x of the points x and q such that $U_x V_x \subset P$. The open sets U_x cover P and since P is also compact we may select a finite covering U_{x_1}, \dots, U_{x_k} . Let $V = V_{x_1} \cap V_{x_2} \cap \dots \cap V_{x_k}$; then $PV \subset P$ and consequently $V \subset Q$. Thus Q is open.

We next show that Q is closed by showing that $G \setminus Q$ is also open. Indeed, let $r \in G \setminus Q$. Since Pr is not contained in P there exists a point $p \in P$ such that $pr \in G \setminus P$. Since $G \setminus P$ is open there exists a neighborhood W of r such that $pW \subset G \setminus P$ which implies that $W \subset G \setminus Q$. Thus $G \setminus Q$ is open.

Since $e \in P$ we have $y = ey \in P$ for $y \in Q$ so that $Q \subset P$. Moreover since $Pe = P \subset P$ it follows that $e \in Q$. Since P is compact we conclude finally that Q is a compact-open set containing the identity from which it follows that $H = Q \cap Q^{-1}$ is also a compact-open set containing the identity.

It remains to show that H is a subgroup of the algebraic group G . Let h_1 and h_2 be elements of H . Then $h_1 \in Q$, $h_2^{-1} \in Q$ and we have $P(h_1 h_2^{-1}) = (Ph_1)h_2^{-1} \subset P$, i.e., $h_1 h_2^{-1} \in Q$. Similarly it may be shown that $(h_1 h_2^{-1})^{-1} = h_2 h_1^{-1} \in Q$ so that in fact $h_1 h_2^{-1}$ belongs to H and Theorem 16 is proved.

If G is compact the preceding theorem may be strengthened.

Theorem 17: Let G be a compact totally disconnected topological group and let U be an arbitrary neighborhood of the identity. Then there exists an open normal subgroup N contained in U . Since the factor group G/N is discrete and compact simultaneously it must be finite.

Proof: By Theorem 16 there exists a compact open subgroup H contained in U . Denote by N the intersection of all groups $x^{-1}Hx$ for $x \in G$. Clearly N is a normal subgroup of G so that all that is needed is to show that N is also open. Since $x^{-1}ex = e \in H$ there exist neighborhoods V_x and W_x of the identity e and the element x such that $W_x^{-1}V_xW_x \subset H$. The open sets W_x , $x \in G$, constitute a covering of the compact space G so that we may select a finite covering W_{x_1}, \dots, W_{x_k} . Let $V = V_{x_1} \cap V_{x_2} \cap \dots \cap V_{x_k}$; then $x^{-1}Vx \subset H$ for $x \in G$. Thus $V \subset N$ and consequently for an arbitrary element $n \in N$ we have $Vn \subset N$ which proves that N is open.

Theorem 16 admits the following obvious converse:

E) If every neighborhood U of the identity e of a topological group G contains an open subgroup H then G is totally disconnected.

In fact G may be partitioned into the union of the two disjoint open sets H and $G \setminus H$. Thus the component of the identity in G , being connected, must be contained in H and consequently in U . But since U is an arbitrary neighborhood of the identity it follows that the component of the identity must coincide with the identity itself.

Example 41: Let G^* be the compact direct product of a collection Ω of finite groups, each in its discrete topology. For an arbitrary finite subset Ω_2 of the collection Ω we write $\Omega_1 = \Omega / \Omega_2$ and construct normal subgroups N_1^* and N_2^* starting from the sets Ω_1 and Ω_2 as was done in proposition F) Section 21. It is easy to see that for any neighborhood U^* of the identity in G^* it is possible to select the finite set Ω_2^* such that $N_1^* \subset U^*$. Moreover, by proposition G) Section 21 the factor group G^*/N_1^* is isomorphic with N_2^* and is therefore finite. It follows that G^* is totally disconnected.

Example 42: Let G denote the additive topological group of real numbers and denote by H the set of all rational numbers. Then H is a subgroup of the algebraic group G so that H is itself a topological group (see Section 19 A)). It is easy to see that

the component of 0 in H contains 0 only so that H is a totally disconnected group. Note also, however, that for any neighborhood U of 0 in the group H the entire group H is generated by that neighborhood. Thus a group need not be connected in order to enjoy the property formulated in Theorem 14. Moreover, it is clear that H does not possess any open subgroup contained in U so that Theorem 16 does not hold in general for totally disconnected groups. The group H is not locally compact.

SECTION 23. LOCAL PROPERTIES. LOCAL ISOMORPHISM.

Specific to the theory of topological groups are the so-called local properties, i.e., those properties of a topological group which may be defined in terms of the behavior of the group in the vicinity of the identity element. The most important concept in this connection is that of local isomorphism.

Definition 30: Two topological groups G and G' are said to be locally isomorphic if there exist neighborhoods U and U' of their identity elements e and e' and a homeomorphism f of U onto U' such that:

- a) if x, y and xy belong to U then $f(xy) = f(x)f(y)$;
- b) if x', y' and $x'y'$ belong to U' then $f^{-1}(x'y') = f^{-1}(x')f^{-1}(y')$.

A) We observe that if the conditions just formulated are satisfied then so also are the conditions c) $f(e) = e'$ and d) if x and x^{-1} belong to U then $f(x^{-1}) = (f(x))^{-1}$.

Indeed the elements e, e and $ee = e$ certainly belong to U so that $f(e) = f(e)f(e)$ whence $f(e) = e'$. Moreover if x and x^{-1} belong to U then since $x^{-1}x = e \in U$ we obtain $e' = f(e) = f(x^{-1})f(x)$, i.e., $f(x^{-1}) = (f(x))^{-1}$.

B) We also observe that even condition b) of Definition 30 is superfluous. More precisely: if there exist neighborhoods U and U' satisfying condition a) then there exist neighborhoods V and V' satisfying both a) and b).

Let V be a neighborhood of the identity such that $V^2 \subset U$ and define $V' = f(V)$. It is easy to see that condition a) remains valid for the neighborhoods V and V' . But now suppose x', y' and $x'y'$ belong to V' . Let $x = f^{-1}(x'), y = f^{-1}(y')$.

Since x and y belong to V it follows that $xy \in U$ and $f(xy) = f(x)f(y) = x'y'$; from this we obtain

$$f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y'),$$

i.e., condition b) is also satisfied.

C) Let G be a topological group and let N be a discrete normal subgroup of G . Then G and $G/N = G'$ are locally isomorphic.

Let f be the natural projection of G onto G' . Denote by W a neighborhood of the identity element in G containing no element of N except e and let U be a neighborhood of the identity such that $UU^{-1} \subset W$. Finally let $f(U) = U'$. It is easy to see that f is one-to-one on U . Indeed, suppose two elements, x and y , belonging to U are carried into one and the same element by f . Then $xy^{-1} \in N$ but also $xy^{-1} \in W$ and consequently $xy^{-1} = e$ or $x = y$. Since f is continuous and open it follows that as a mapping between U and U' f is both ways continuous. Condition a) of Definition 30 holds for the mapping f since f is a homomorphism but then, according to B), f is a local isomorphism and G and G' are locally isomorphic.

Proposition C) gives a means of constructing groups locally isomorphic with a given group. The following theorem shows that the method is rather general.

Theorem 18: Let G and G' be two connected locally isomorphic topological groups. Then there exists a group H such that G is isomorphic with a factor group H/N and G' is isomorphic with a factor group H/N' where N and N' are discrete normal subgroups in H .

In proving this theorem the only consequence of the connectedness of G and G' that we employ is that each is generated by an arbitrary neighborhood of its identity (see Th. 14).

Proof. Let U and U' be neighborhoods of the identity elements of the groups G and G' for which the conditions of Definition 30 are satisfied and let f be the corresponding mapping. For the sake of simplicity we assume that U is symmetric, i.e., that $U^{-1} = U$. Denote by K the direct product of G and G' and by V the set of all elements of the form $(x, f(x))$ where $x \in U$. Next, let H denote the union of all sets of the form V^n , $n = 1, 2, \dots$. In other words H consists of the collection of all elements of K which may be written in the form of a finite product of elements belonging to V . It is obvious that H is a subgroup of the algebraic group K , though H need not be a closed set. We proceed to ignore the topology H acquires as a subspace of K and give it a new topology.

Let $\{U_\alpha\}$ be a complete system of neighborhoods of the identity in G where the index α runs over a possibly non-countable set.

We assume without loss of generality that $U_\alpha \subset U$ for all α . Let $U'_\alpha = f(U_\alpha)$ and denote by V_α the set of all elements of K of the form $(y, f(y))$ where $y \in U_\alpha$. We now refer to Theorem 9 and the immediately preceding proposition B) Section 18. The five conditions there set forth are characteristic of a complete system of neighborhoods of the identity in a topological group and are therefore certainly satisfied by the system $\{U_\alpha\}$. But then the same properties are also satisfied by the system of neighborhoods $\{U'_\alpha\}$ and consequently also by the system of sets $\{V_\alpha\}$ in the algebraic group H .† Hence, according to Theorem 9 we may and do topologize H in such a way that the sets V_α form a complete system of neighborhoods of the identity.

† Translator's Note: The last of the five relevant conditions offers considerably more difficulty than the others and we here give a proof of condition e) (see Section 18 B)) Let V_{α_0} be an arbitrary set of the system $\{V_\alpha\}$ and let (a, a') be an arbitrary element of the group H . Then according to the definitions above V_{α_0} consists of all pairs of the form $(x, f(x))$ where $x \in U_{\alpha_0}$ while $a = u_1 \dots u_k$ with $u_i \in U$, $i = 1, \dots, k$ and $a' = f(u_1) \dots f(u_k)$. First use conditions b) and d) in the group G to choose a neighborhood U_β such that $u_i^{-1}U \subset U$ for $i = 1, \dots, k$. Next use condition e) repeatedly (still in G) to choose neighborhoods $U_{\alpha_1}, \dots, U_{\alpha_k}$ such that

$$u_{k-i+1}^{-1} U_{\alpha_i} u_{k-i+1} \subset U_{\alpha_{i-1}} \cap U_\beta, \quad i = 1, \dots, k.$$

Finally let $U_\gamma = U_{\alpha_1} \cap U_{\alpha_2} \cap \dots \cap U_{\alpha_k} \cap U_\beta$. If then for $x \in U_\gamma$ we write $w_0 = x$ and

$$w_i = u_i^{-1} u_{i-1}^{-1} \dots u_1^{-1} x u_1 \dots u_{i-1} u_i, \quad i = 1, \dots, k$$

an easy induction shows that

$$w_i = u_i^{-1} w_{i-1} u_i, \quad w_i \in U_{\alpha_{k-i}} \cap U_\beta$$

and

$$f(w_i) = f(u_i)^{-1} \dots f(u_1)^{-1} f(x) f(u_1) \dots f(u_i), \quad i = 1, \dots, k.$$

In particular, letting $i = k$, we obtain $w_k = a^{-1} x a \in U_{\alpha_0}$ and also $f(w_k) = a'^{-1} f(x) a'$. Thus $(a, a')^{-1}(x, f(x))(a, a') \in V_{\alpha_0}$ for $x \in U_\gamma$ and V_γ is a neighborhood with the desired property.

We now define a mapping g by associating with each element $z = (x, x') \in K$ the element $g(z) = x \in G$. Then g is a homomorphism of K onto G so that g is also a homeomorphism of the algebraic group H onto a subgroup G^* of the algebraic group G . But now $G^* = G$. Indeed $g(V) = U$ so that $U \subset G^*$ and since G is generated by any neighborhood of the identity we obtain $G = G^*$.

We next show that g is an open homomorphism of the topological group H onto the topological group G . Indeed, the relation $g(V_\alpha) = U_\alpha$ shows at once that g is continuous and open at the identity, whence the assertion follows by Section 20 A).

Thus, according to Theorem 11, G is isomorphic with the factor group H/N where N is the kernel of g . It remains to show that N is a discrete subgroup of H , and to this end it suffices to verify that there exists a neighborhood of the identity in H containing no element of N except the identity. But this condition is satisfied by an arbitrary neighborhood of the system $\{V\}$ since g is one-to-one on the set V .

In exactly the same way it may be shown that G' is isomorphic with a factor group H/N' where N' is also a discrete normal topological group of H . Thus Theorem 18 is proved.

Theorem 18 will be further developed and deepened in Chapter 9. There we shall define a single group H , not just for two, but rather for an entire class of mutually locally isomorphic groups, though to be sure groups of a rather special type. Such a result permits the drawing of a sharp distinction between the local and global investigations of topological groups.

By a local property of a topological group we mean a property which obtains simultaneously in all mutually locally isomorphic groups. It should be noted that the local behavior of a group has a strong influence on its behavior in the large so that the local investigation of a group is of great importance.

Since in studying the local properties of a topological group G we concern ourselves only with the behavior of G in an arbitrarily small neighborhood U of the identity, it is natural to wonder whether it is not possible to study U as an object in its own right, without paying any attention to the fact that it is only a part of the global group G . Indeed this is exactly the setting of the classical theory of Lie groups (see the seventh and ninth chapters). In that theory a mathematical object is studied which later turns out to be a neighborhood of the identity in a topological Lie group. I shall here define the concept of a local group, a construct possessing the most important properties of a neighborhood of the identity in a topological group. In the balance of the present paragraph the discussion will be somewhat less detailed than in other parts

of the book inasmuch as it consists largely of a repetition, in a somewhat new context, of facts discussed earlier. The following topics are necessary only for the understanding of the seventh, eighth, and ninth chapters.

D) A topological space G is said to be a local group, if, for certain pairs a, b of elements of G , there is defined a product $a b \in G$ in such a way that the following conditions are satisfied.

- a) if all of the products ab , $(ab)c$, bc , $a(bc)$ are defined then the equality $(ab)c = a(bc)$ holds.
- b) If the product ab is defined then for every neighborhood W of ab there exist neighborhoods U and V of the elements a and b such that for $x \in U$, $y \in V$ the product xy is also defined and $xy \in W$.
- c) There is in G a distinguished element e , called the identity of G , possessing the property that if $a \in G$ then the product ea is defined and $ea = a$.
- d) If for a pair of elements a, b the product $a b$ is defined and $a b = e$ then it is said that a is a left inverse element for b , $a = b^{-1}$. If for b there exists a left inverse element b^{-1} then for every neighborhood U of b^{-1} there exists a neighborhood V of the element b such that every element $y \in V$ also possesses a left inverse element y^{-1} such that $y^{-1} \in U$.

E) If G is a local group and n is any positive integer then there exists in G a neighborhood U of the identity e such that for each element $a \in U$ there exists an inverse a^{-1} in G and such that for any n elements a_1, \dots, a_n in U the product

$$((a_1 a_2) a_3) \dots a_n = b,$$

is defined and does not depend upon the distribution of the parentheses so that it makes sense to write $b = a_1, \dots, a_n$.

From condition c) it follows that the product ee is defined and that $ee = e$. From this it follows immediately by b) and d) that there exists a neighborhood W of e such that if $a \in W$ then there exists an inverse element a^{-1} and for $a \in W$, $b \in W$ the product $a b$ is defined. Moreover by condition b) there exists a neighborhood V such that $V^2 \subset W$. Clearly E) is already satisfied by V for $n = 3$. Continuing this construction we obtain a neighborhood U possessing the desired properties for any positive integer n .

F) If G is a local group then there exist neighborhoods of the identity U and V such that $V \subset U$ and such that the following conditions are satisfied:

- a) if $a \in U$ then the product $a \cdot e$ is defined and $a \cdot e = a$;
- b) if $a \in U$ then there exists an element a^{-1} such that the products aa^{-1} and $a^{-1}a$ are defined and $aa^{-1} = a^{-1}a = e$;
- c) if a and b belong to V then the equations $ax = b$ and $ya = b$ possess one and only one solution in the open set U .

Proposition F) may be proved by arguments precisely parallel to those in the proofs of B) and C) of Section 1. The only thing necessary is to select neighborhoods U and V sufficiently small so that the computations carried out in Section 1 are meaningful, and the existence of such neighborhoods is in each case assured by E).

G) Let G be a local group. Any neighborhood U of the identity e in G will be called a part of G . Every part U of a local group G is itself a local group with respect to the operations defined in G . We simply agree that the product ab is defined in U if it is defined in G and belongs to U and that e is the identity in U .

H) Let G and G' be local groups. Then a mapping f is said to be a local isomorphism of G onto G' if f is a homeomorphism of a part U of G onto a part U' of G' in such a way that the following conditions are satisfied:

- 1) if the product ab is defined in U then the product $f(a)f(b)$ is defined in U' and $f(ab) = f(a)f(b)$.
 - 2) f carries the identity of U into the identity of U' .
 - 3) the mapping f^{-1} inverse to f also satisfies these conditions.
- If there exists a local isomorphism of a local group G onto a local group G' we shall say that G and G' are locally isomorphic. Two local isomorphisms f and f' of a local group G onto a local group G' are said to be equivalent if they coincide on some part of G . In the sequel we shall study local isomorphisms only up to equivalence.

It is clear that Definition 30 is just the special case of definition H) that arises when G and G' are global topological groups.

The object proper of the investigation is not all properties of local groups but only those which are preserved under local isomorphisms.

The following question now arises naturally concerning the concept of local groups: is not every local group locally isomorphic with some topological group? The question is answered in the

positive for Lie groups by means of the application of special and quite complicated apparatus (see Section 59). For the most general local group the answer is negative [31].

We proceed now to the definition of the fundamental concepts of subgroup, normal subgroup, factor group, and homomorphism for local groups.

I) Let G be a local group and let H be a subset of G containing e . By Definition 17 H is a topological space. We agree that for a pair of elements a, b of H the product is defined if it is defined in G and belongs to H . If the topological and algebraic operations thus defined in H satisfy the conditions of Definition D) then H is itself a local group. If moreover there exists a neighborhood U of the identity e in which the intersection $U \cap H$ is closed then H is said to be a subgroup of the local group G .† A local subgroup N of a local group G is a normal subgroup if there exists in G a neighborhood V of the identity e such that for $x \in V$, $y \in V \cap H$ we have $x^{-1}yx \in H$. Two subgroups H and H' of a local group G are said to be equivalent if there exists a neighborhood U of the identity such that $H \cap U = H' \cap U$.

It is easy to see that the relation of equivalence between subgroups of a local group G is invariant under local isomorphism. In studying the structure of subgroups we shall concern ourselves only with such properties as remain unchanged under the replacement of a subgroup by an equivalent subgroup.

J) Let G be a local group and let H be a subgroup of G . We define the local space G/H of left cosets of the subgroup H in the

† Translators Note: This condition, which says that some part of H is open relative to its own closure, is sometimes tedious to verify directly, and it is convenient to have a general criterion to apply. The following line of reasoning seems to cover all the situations to be encountered in the sequel. In the first place, a suitably small part of a local group is a Hausdorff space (proof as usual, using E) and F)). In the second place, a locally compact subspace of a Hausdorff space is open in its own closure (see, e.g., [7], p. 69). It follows at once that if H is a subset of a local group G which is a local group in its own right, and if H is locally compact in its relative topology, then H is a subgroup. Finally, using this observation and the concepts introduced below in J), K) and N), it is not difficult to establish the following fact: if G and G^* are local groups with G locally compact, and if f is a homomorphism of G into G^* , then the range of f is a subgroup of G^* .

group G . To this end we select a neighborhood U of the identity in G , the smallness of which will be determined by the following constructions. We partition the set U into left cosets of the subgroup H by putting the elements x and y of U in the same coset if $x^{-1}y \in H$. If U is chosen small enough the axioms of equivalence (see Section 2 C)) will be satisfied. Moreover every coset X will have the form $X = U \cap (xH)$ where x is an arbitrary element of X and conversely every set of the form $U \cap (xH)$, $x \in U$, will constitute one left coset. Now let Σ be a base in the space U . If $W \in \Sigma$ we denote by W^* the collection of all left cosets meeting W . The collection Σ^* of all sets W^* , $W \in \Sigma$, is easily seen to satisfy the conditions of Theorem 3 so that we may and do use it as a base in the space $G \setminus H$. Thus the local space G/H of left cosets is not uniquely determined by the local group G and the subgroup H but also depends upon the choice of the neighborhood U . The local space of right cosets is defined in analogous fashion. Finally, if $H = N$ is a normal subgroup of the local group G we define the factor group G/N . There exists a neighborhood V of the identity in G so small that if X and Y are two cosets meeting V then $U(XY) = Z$ is again a coset. In this case we define the product $XY = Z$. Thus for any two elements of the space G/N belonging to V^* there is defined a product belonging to G/N . With respect to the topological and algebraic operations thus defined the set G/N turns out to be a local group called the factor group.

It is clear that the group $G/N = G^*$ is not uniquely determined by the local group G and the normal subgroup N but also depends upon the choice of the neighborhoods U and V ; however it is not difficult to see that all of the factor groups G/N obtained in this manner are locally isomorphic with one another so that, as far as our interest extends, the properties of the factor group G/N are uniquely determined. Similarly, if we replace the normal subgroup N by an equivalent group N' we obtain a factor group G/N' locally isomorphic with G/N .

K) Let G and G^* be two local groups. We shall say that a mapping f is a local homomorphism of the group G into G^* if f is a continuous mapping of a part U of G into a part U^* of G^* satisfying the following conditions: If the product ab is defined in U then the product $f(a)f(b)$ is defined in U^* and $f(ab) = f(a)f(b)$ and f carries the identity in U into the identity in U^* . The set N of elements carried into the identity by f is called the kernel of f and turns out to be a normal subgroup of the local group G . If f is an open mapping of U onto U^* then f is said to be an open homomorphism of the local group G onto the local group G^* . In

this case there is associated with f a natural local isomorphism between the groups G^* and the factor group G/N . Two local homomorphisms f and f^* of group G into a group G^* are said to be equivalent if they coincide on some part of G . In the sequel we shall study local homomorphisms only up to equivalence.

L) Let N_1 and N_2 be two local groups with identities e_1 and e_2 . The set of all pairs of the form (x_1, x_2) , $x_1 \in N_1$, $x_2 \in N_2$, we denote by G' . Then G is a topological space in the product topology (see Section 14 A)). We also define in G' an operation of multiplication by agreeing that the pairs (x_1, x_2) and (y_1, y_2) may be multiplied if the products of the elements x_1 and y_1 in N_1 and of the elements x_2 and y_2 in N_2 are defined, in which case we write $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$. For the identity element we choose the pair $e' = (e_1, e_2)$. It is easy to verify that with this law of multiplication the space G' is a local group. The local group G' is called the direct product of the local groups N_1 and N_2 . To each element $x \in N_1$ we associate the element $f_1(x_1) = (x_1, e_2) \in G'$ and to each element $x_2 \in N_2$ we associate the element $f_2(x_2) = (e_1, x_2) \in G'$. It may be readily verified that f_i is a local isomorphism of N_i onto a local subgroup N'_i of the local group G' and that the local normal subgroups N'_1 and N'_2 satisfy the following conditions:

- 1) $N'_1 \cap N'_2 = e'$;
- 2) for arbitrary neighborhoods U'_1 and U'_2 of the identity e' relative to the subgroups N'_1 and N'_2 respectively, the group product $U'_1 U'_2$ contains a neighborhood U' of the identity e' in G' .

As before, these properties of normal subgroups lead us to an alternative definition of the direct product. We shall say that the local group G resolves into the direct product of two local normal subgroups N_1 and N_2 if:

- 1) $N_1 \cap N_2 = e$ where e is the identity in G and
- 2) for arbitrary neighborhoods U_1 and U_2 of the identity e relative to the subgroups N_1 and N_2 respectively, there exists a neighborhood U of e in G such that $U \subset U_1 U_2$.

It is easy to verify that in this case the direct product G' of the local groups N_1 and N_2 is locally isomorphic with G . Indeed, associating with each pair (x_1, x_2) , where x_1 and x_2 belong to suitably chosen neighborhoods of the identity e , the element $f(x_1, x_2) = x_1 x_2 \in G$, we obtain a local isomorphism of G' onto G ; moreover $f|_{N'_i}$ is the identity mapping of the local group N'_i onto itself. The definition here given of the direct product of two local groups

extends in obvious fashion to the product of an arbitrary finite number of local groups.

We here introduce one more quite special but nevertheless important concept.

M) Let G be a local group and let D denote the additive topological group of real numbers. Then a local homomorphism g of D into G will be called a one-parameter subgroup of G . Given such a local homomorphism there exists a positive number α so small that for

$$|s| < \alpha, |t| < \alpha, |s + t| < \alpha$$

the values $g(s)$, $g(t)$, $g(s + t)$ of the function g are defined and the condition

$$g(s + t) = g(s)g(t). \quad (1)$$

is satisfied. Such an interval $|t| < \alpha$ will be called a domain of existence of the one-parameter subgroup g . If g and h are two one-parameter subgroups with domains of existence $|t| < \alpha$ and $|t| < \beta$ respectively and if there exists a positive number γ such that for $|t| < \gamma$ we have $g(t) = h(t)$ then, by virtue of (1), $g(t) = h(t)$ for $|t| < \min(\alpha, \beta)$. If G is a topological group then a one-parameter subgroup g may, by virtue of (1), be extended, in one and only one way, to a homomorphism of the whole topological group D into G .

N) Let G be a local group. If there exists a neighborhood U of the identity in G such that the set \bar{U} is compact then the local group G is said to be locally compact. If another neighborhood V of the identity in G is contained in a neighborhood U with compact closure \bar{U} then \bar{V} is also compact. Thus the property of being locally compact is a locally invariant property of local groups. If U is a sufficiently small neighborhood of the identity of the local group G possessing compact closure \bar{U} and if V is a neighborhood of the identity contained in U then \bar{U} is contained in the union of a finite number of the sets of the form aV , $a \in \bar{U}$, so that the set \bar{U} has the same dimension as the set \bar{V} (see Section 16). Thus it is possible to define the dimension of the local group G to be the dimension of \bar{U} . If G is a compact topological group then its dimension as a local group is equal to the dimension of the space G since in this case U may be taken to be the entire group.

Example 43: Let G be the additive topological group of real numbers and let N be the subgroup of whole numbers. According to proposition C) the groups G and G/N are locally isomorphic. It is obvious, however, that the groups themselves are not isomorphic. We have here the simplest example of locally isomorphic groups which are not globally isomorphic. More complicated examples will appear later.

Example 44: Let G^n denote the additive topological vector group of n -dimension Euclidean space with a fixed Cartesian coordinate system. Denote by G^k the subgroup of G^n generated by the first k coordinate axes and by N^k the collection of vectors in G^k having integral coordinates. Then N^k is a discrete subgroup of G^n and consequently the factor group $G^n/N^k = G_k^n$ is locally isomorphic with G^n itself. Consequently all the groups G_k^n , $k = 0, \dots, n$ are locally isomorphic with one another, but no two distinct groups in this list are isomorphic. Indeed no two are homeomorphic. The only one of the groups that is compact is G_0^n . The group G_0^n is isomorphic with G^n .

It turns out that every connected group that is locally isomorphic with G^n is in fact isomorphic with one of the groups G_k^n (see Ex. 97).

SECTION 24

TOPOLOGICAL TRANSFORMATION GROUPS

In Sections 1 and 3 the concept of a group of transformations of an arbitrary set was considered (see Section 1 F); Section 3 I), J), K)). In the event that the transformed set is also a topological space it is natural to single out from the collection of all transformations those transformations which are homeomorphisms of the space onto itself. Since the product of two homeomorphisms is again a homeomorphism, it follows that the collection of all homeomorphisms of a topological space onto itself is a group. However, in geometry and in other branches of mathematics the interesting object of investigation is ordinarily not the group of all homeomorphisms of a given space but rather some particular subgroup. Moreover, it is almost always the case that the group is topologized in some way so as to be a topological group. In this context a question of great interest is how and to what extent the topology of the transformation group is determined by the topology of the transformed space. In classical problems it is always clear precisely what topology should be

introduced in the group of transformations, this topology being uniquely determined by the nature of the problem itself. It is highly desirable nonetheless to establish a general theorem of uniqueness for the topology of a transformation group and to set forth easily verifiable criteria permitting one to determine whether the choice of a topology has been appropriate. It is with the solution of these two problems that Theorem 19 and Definition 31 are concerned. Another important problem in the general theory of transformation groups is, given a topological group, to determine those topological spaces on which the given group may act as a transitive topological transformation group. The solution of this problem is to be found in Theorem 20; it is analogous to proposition K) Section 3.

Definition 31: A topological group G is said to be a topological transformation group acting on the topological space Γ if to each element $x \in G$ there is associated a transformation x^* of Γ , $x^* = \tau(x)$, such that $\tau(xy) = \tau(x)\tau(y)$ and such that the function σ of two variables $x \in G$ and $\xi \in \Gamma$ defined by the equation $\sigma(x, \xi) = x^*(\xi)$ is continuous, i.e., is a continuous mapping of the product $G \times \Gamma$ onto Γ .[†] It is obvious that if these conditions are satisfied then all of the transformations x^* , $x \in G$, are homeomorphisms. If distinct transformations correspond to distinct elements of G then G is said to be an effective transformation group. In this case the group elements may be identified with their corresponding transformations ($x = x^*$).

It is easy to see that the kernel of ineffectiveness N of the algebraic group (see Section 3 I)) is closed in the space G . The factor group $G^* = G/N$ is then, in the obvious sense, an effective topological transformation group on Γ . A topological transformation group is said to be transitive if it is transitive considered as an algebraic group of transformations of the set Γ (see Section 3 I)).

Theorem 19. Let Γ be a Hausdorff space and let G be an effective group acting on Γ . Suppose also that two topologies are defined in the group G turning it into topological transformation groups G' and G'' acting on Γ . If each of the groups G , and G'' is locally compact and may be represented as the union of a countable

[†] Translators Note: It is customary in western literature to say that the topology of G is admissible if this condition is satisfied. The concept was first introduced by Arens [4].

number of compact subsets then the topologies in the groups G' and G'' must be the same; i. e., the two topological groups G' and G'' coincide.

We preface the proof of Theorem 19 with a useful criterion for the compactness of a subset of a topological group.

A) Let M be an arbitrary subset of a topological group G . Then the closure \bar{M} of M is compact if and only if every collection of subsets of M possessing the finite intersection property has a common adherent point in G . Since every system of sets with the finite intersection property is contained in a system which is maximal with respect to that property (see Section 14 D)) this criterion may equally well be formulated in terms of maximal collections (in M) having the finite intersection property.

One half of the theorem is obvious. If \bar{M} is compact then a collection of subsets of M having the finite intersection property is also a collection of subsets of \bar{M} and therefore possesses in \bar{M} a common adherent point. Suppose on the other hand that the above criterion is satisfied. Let Δ^* be an arbitrary collection of subsets of \bar{M} having the finite intersection property and let Σ be a complete system of neighborhoods of the identity in G . Denote by Δ the collection of all sets of the form $M \cap (AU)$ where $A \in \Delta^*$ while $U \in \Sigma$. It may be immediately verified that Δ also has the finite intersection property, and since all the sets of Δ are subsets of M they possess, by hypothesis, a common adherent point a belonging to \bar{M} . We shall show that a is also a common adherent point of the system Δ^* . Let V be an arbitrary neighborhood of the identity in G and let U be a neighborhood of the identity such that $UU^{-1} \subset V$. Then for any set A of Δ^* the set $M \cap (AU)$ belongs to Δ and therefore meets the neighborhood aU of the point a . From this it follows immediately that A meets the set aUU^{-1} and must therefore also meet the neighborhood aV . Thus an arbitrary neighborhood aV of the point a meets an arbitrary set $A \in \Delta^*$ so that a is indeed a common adherent point of Δ^* . It follows that \bar{M} is compact.

Proof of Theorem 19. Let Σ' and Σ'' be complete systems of neighborhoods for the spaces G' and G'' respectively and denote by Σ_0 the collection of all non-empty sets of the form $U' \cap U''$ where $U' \in \Sigma'$, $U'' \in \Sigma''$. We shall show that Σ_0 satisfies conditions a) and b) of Theorem 3, i.e., that Σ_0 is a complete system of neighborhoods for a uniquely determined topological space G_0 , the points of which are the elements of the set G . To see that a) holds, let x and y be distinct points of the set G , let

$U' \in \Sigma'$ be a neighborhood of x in G' not containing y and let $U'' \in \Sigma''$ be any neighborhood of x in G'' . Then $U' \cap U'' \in \Sigma_0$ contains x but does not contain y . To see that b) holds, let $U' \cap U''$ and $V' \cap V''$ be two sets of the system Σ_0 both containing the point x . Here U' and V' belong to Σ' while U'' and V'' belong to Σ'' . Let also $W' \in \Sigma'$ and $W'' \in \Sigma''$ be neighborhoods of x such that $W' \cap U' \cap V'$ and $W'' \cap U'' \cap V''$. Then $W' \cap W''$ belongs to Σ_0 , satisfied the condition $W' \cap W'' \subset (U' \cap U'') \cap (V' \cap V'')$, and contains x . Thus the conditions of Theorem 3 are satisfied.

We next show that G_0 is a topological group, i.e., that the algebraic operations in G are continuous in the topology defined by the base Σ_0 . Let x and y be two elements of G and let $W' \cap W''$ be a neighborhood of $z = xy^{-1}$ selected from the base Σ_0 . Here $W' \in \Sigma'$ and $W'' \in \Sigma''$. Since G' and G'' are topological groups there exist neighborhoods U' and V' of x and y in the base Σ' and other neighborhoods U'' and V'' of x and y in the base Σ'' such that $U'V'^{-1} \subset W'$ and $U''V''^{-1} \subset W''$. Then $U' \cap U''$ and $V' \cap V''$ are neighborhoods of x and y in the base Σ_0 and satisfy the condition $(U' \cap U'')(V' \cap V'')^{-1} \subset W' \cap W''$. Thus G_0 is a topological group.

We next show that if M is a subset of G with the property that the closures \bar{M}' and \bar{M}'' of M in the topological spaces G' and G'' respectively are both compact, then the same is true of the closure \bar{M} in the space G_0 . Let Δ be any collection of subsets of M which is maximal with respect to the finite intersection property (see Section 14 D)). In order to show that \bar{M} is compact it suffices, according to A) and the accompanying remark, to show that the system Δ possesses a common adherent point in G_0 . Since by hypothesis the set \bar{M}' is compact it follows that Δ does possess at least one common adherent point x' in the topological space G' . Moreover, if $U' \in \Sigma'$ is any neighborhood of x' , it follows from the maximality of Δ that the intersection $U' \cap M$ actually belongs to Δ . This permits us to show that x' is in fact the only common adherent point of the system Δ in G' . Indeed suppose y' is another such point. Since the space of the group G' is Hausdorff there exist disjoint neighborhoods U' and V' of the points x' and y' respectively. But then the sets $U' \cap M$ and $V' \cap M$ are also disjoint and both belong to Δ which contradicts the finite intersection property. In exactly the same way it may be shown that Δ possesses a unique common adherent point x'' in the topological space G'' . We next show that the points x' and x'' must coincide. It may be noted that this is the one and only step in the argument where we make use of the assumption that the groups G' and G'' are effective topological transformation groups. Suppose, indeed, that $x' \neq x''$.

Then x' and x'' are distinct transformations of the space Γ and there must exist a point $\alpha \in \Gamma$ such that $x'(\alpha) \neq x''(\alpha)$. Since Γ is also a Hausdorff space the points $x'(\alpha)$ and $x''(\alpha)$ possess disjoint neighborhoods H' and H'' respectively. But then, since G' is a continuous transformation group, there exists in G' a neighborhood U' of the transformation x' with the property that all the transformations belonging to U' carry the point α into a point of H' . Similarly there exists a neighborhood U'' of the transformation x'' in the group G'' all the transformations of which carry α into a point of H'' . Since H' and H'' are disjoint it follows that U' and U'' must also be disjoint; on the other hand, as has already been seen, the two sets $U' \cap M$ and $U'' \cap M$ must both belong to Δ and must therefore intersect. Thus we arrive at a contradiction and conclude that $x' = x''$. But then, since $x' = x'' = x$ is a common adherent point of Δ in the topological space G' as well as in the space G'' , it follows that for arbitrary neighborhoods $U' \in \Sigma'$ and $U'' \in \Sigma''$ of the point x the intersections $U' \cap M$ and $U'' \cap M$ both belong to the maximal system Δ whence also the intersection $U' \cap U'' \cap M$ must. But this says that an arbitrary neighborhood of x in G_0 meets each of the sets of Δ so that x is in fact a common adherent point of Δ in G_0 . Thus \bar{M} is compact.

We may now show that the topological space G_0 is locally compact and is the union of a countable collection of compact subsets. In the first place, since the spaces G' and G'' are locally compact by hypothesis it is easily seen that the bases Σ' and Σ'' may be so chosen as to consist exclusively of sets with compact closures. But then, from what has just been proved, it follows that every neighborhood in the base Σ_0 possesses compact closure in G_0 which shows that G_0 is locally compact. For the rest, let F_1', F_2', \dots be a sequence of sets, compact in the space G' and covering G , let similarly F_1'', F_2'', \dots be a sequence of sets, compact in G'' and covering G , and let $F_{ij} = F_i' \cap F_j''$. Using, once more, the criterion of compactness just established we see that all of the sets F_{ij} are compact in G_0 . Since these sets obviously provide a countable covering of G the desired properties are fully established.

The upshot of the foregoing arguments is that all the hypotheses of Theorem 12 are satisfied by the topological group G_0 . To complete the proof of the present theorem we consider the identity mapping of the algebraic group G onto itself, first as a mapping of the topological group G_0 onto the topological group G' . The mapping is an algebraic isomorphism and is also continuous by the very definition of the topology in G_0 . But then by Theorem 12 it must in fact be an isomorphism between the topological groups

G_0 and G' ; in particular the identity mapping is a homeomorphism between the topological spaces of G_0 and G' which says precisely that the topology of the space G' coincides with the topology of G_0 . In exactly the same manner it follows that the topology of G'' also coincides with that of G_0 and consequently that the topologies of G' and G'' coincide with each other. Thus Theorem 19 is proved.

B) It is a simple matter now to complete the considerations of Section 3 J). Let G be a topological group, H a subgroup, and form the topological space G/H of left cosets (see Def. 24). By associating with each $x \in G$ the transformation x^* defined by $x^*(\Xi) = x\Xi$ where $\Xi \in G/H$ we turn G into a transitive group of transformations of the set G/H . It turns out that G is a topological transformation group acting on the space G/H , the kernel of ineffectiveness of G being the maximal normal subgroup of G contained in H .

We must show that the function σ of Definition 31 is continuous. Let $x \in G$, $\Xi = aH \in G/H$ and let $x^*(\Xi) = xaH = H$. Recall that the most general neighborhood W^* of H in G/H consists of the collection of all cosets contained in WH where W is some neighborhood of xa in the group G . Let now U and V be neighborhoods of x and a in G such that $UV \subset W$ and denote by V^* the neighborhood of Ξ in the space G/H consisting of all cosets contained in VH . Since $UV \subset W$ it follows at once that $\sigma(U, V^*) \subset W^*$ and the desired result is established.

C) Let G and G' be topological transformation groups acting on the spaces Γ and Γ' respectively. A pair of mappings φ , ψ is said to be a similarity of the pair G , Γ onto the pair G' , Γ' , if φ is an isomorphism of the topological group G onto the topological group G' while ψ is a homeomorphism of the topological space Γ onto the topological space Γ' and if the relations $x' = \varphi$, $\xi' = \psi(\xi)$ imply $x'^*(\xi') = \psi(x^*(\xi))$. The pairs G , φ and G' , Γ' are similar if there exists a similarity of G , Γ onto G' , Γ' .

Theorem 20: Let G be a transitive topological transformation group acting on the (Hausdorff) space Γ and let α be an arbitrary but fixed point in Γ . Denote by $\psi(\xi)$ the set of all elements $x \in G$ satisfying the condition $x^*(\alpha) = \xi$. Then $H_\alpha = \psi(\alpha)$ is a subgroup of the topological group G . According to proposition K) Section 3, ψ is a one-to-one mapping of the set Γ onto the set G/H of left cosets. The inverse map ψ^{-1} is continuous in any event. If both of the spaces G and Γ are locally compact and if, moreover, the space G is the union of a countable collection of compact subsets,

then the pair φ, ψ is a similarity of the pair G, Γ onto the pair $G, G/H_\alpha$ where φ denotes the identity map of G onto itself.

Proof. All but the topological parts of the theorem have been taken care of in proposition K) Section 3. Thus we need only prove that the set H_α is closed, that the mapping ψ^{-1} is continuous in general and is a homeomorphism if the special hypotheses are satisfied. Moreover the fact that H_α is closed follows at once from the continuity of σ (see Def. 31).

Denote now by f the natural projection of G onto G/H_α and let $g = \psi^{-1}f$. Then the continuity of ψ^{-1} follows from the continuity of g . Indeed let L be an arbitrary open set in Γ ; then $\psi(L) = f(g^{-1}(L))$. If g is continuous then $g^{-1}(L)$ is open in G and since f is an open mapping it follows that $f(g^{-1}(L))$ is open in G/H_α and since ψ is one-to-one, this is equivalent with the continuity of ψ^{-1} . In a similar fashion the continuity of ψ follows from the openness of the mapping g ; if M is an arbitrary open set in G/H_α then $\psi^{-1}(M) = g(f^{-1}(M))$ which is open if g is an open mapping since f is continuous. Thus our task reduces to showing that g is continuous in any case and is an open mapping if the special hypotheses are satisfied.

It is easy to see that the mapping g is defined by the equation $g(x) = x(\alpha)$, $x \in G$, so that the continuity of g is an immediate consequence of the continuity of σ . Henceforth we shall assume that both G and Γ are locally compact and that G is the union of a countable collection of compact sets. The proof that g is then open is analogous with the proof of Theorem 12.

Let U be a neighborhood of the identity in G ; we begin by showing that $g(U)$ contains some neighborhood of the point α in Γ . Select a neighborhood V of the identity in G such that the set $F = \bar{V}$ is compact and satisfies $F^{-1}F \subset U$. Let also Σ be a countable collection of compact subsets of the space G which covers G . For each of the sets $E \in \Sigma$ the system of open sets xV , $x \in E$, covers E so that E possesses a finite covering consisting of sets of the form xV , $x \in E$. Since the whole system Σ is countable it follows that there exists a sequence x_1, x_2, \dots of group elements such that the sets $F_i = x_i F$, $i = 1, 2, \dots$, constitute a covering of G . Let $C_i = g(F_i)$. Then C_1, C_2, \dots is a covering of Γ .

We shall show that $g(F)$ contains an open set in Γ . To that end it suffices to show that at least one of the sets C_i contains an open set. Indeed $C_i = g(x_i F) = x_i * (g)(F)$ so that C_i is the image of $g(F)$ under a homeomorphism $x_i *$ of the space Γ onto itself. Suppose now on the contrary that no one of the sets C_i contains an open set, and let L_0 be an arbitrary open set in Γ , the closure of which is compact. Since C_1 contains no open set there exists

in Γ an open set L_1 whose closure is compact and contained in $L_0 \setminus C_1$.[†] Then since C_2 does not contain any open set there exists an open set L_2 the closure of which is compact and contained in $L_1 \setminus C_2$. Continuing this process we obtain an infinite sequence of open sets L_0, L_1, L_2, \dots with compact closures and satisfying the condition $L_i \subset L_{i-1} \setminus C_i$, $i = 1, 2, \dots$. Since the sets \bar{L}_i are compact and non-empty their intersection is also non-empty (see Th. 4) and cannot belong to any of the sets C_i , $i = 1, 2, \dots$. But this contradicts the fact that the sets C_i cover Γ . Thus it follows that $g(f)$ contains some open set L .

Now let $\beta \in L$ and let x be a point of F such that $g(x) = \beta$, i.e., such that $x^*(\alpha) = \beta$. Since $F^{-1}F \subset U$ it follows that $x^{-1}F \subset U$ and consequently $g(U) \supset g(x^{-1}F) = (x^{-1})^*(g(F)) \supset (x^{-1})^*(L)$. But $(x^{-1})^*(L)$ is an open set in Γ containing the point α . Thus we have shown that for an arbitrary neighborhood U of the identity in G the set $g(U)$ contains some neighborhood of α .

The proof that g is an open mapping may now be easily completed. Let $x \in G$, and let W be an arbitrary neighborhood of x . Let also $g(x) = \gamma$, i.e., $x^*(\alpha) = \gamma$. Then the open set $x^{-1}W$ contains the identity of G so that $g(x^{-1}W)$ contains some neighborhood L' of the point α ; $L' \subset g(x^{-1}W)$. Applying the homeomorphism x^* we obtain $\gamma = x^*(\alpha) \in x^*(L') \subset x^*(g(x^{-1}W)) = g(W)$. Thus $g(W)$ contains the open set $x^*(L')$ about the point γ and Theorem 20 is proved.

Example 45: Let Γ be a metric space and consequently also a topological space (see Ex. 20). A transformation x of the space

[†] Translators Note: It is at this point that the assumption that Γ is Hausdorff which I have taken the liberty of adding to the hypotheses of Th. 20, comes into play. In fact Th. 20 is not valid without this hypothesis as the following example shows. Let G be the additive topological group of whole numbers taken in the discrete topology and let Γ be the same collection of whole numbers, but topologized as in Example 17. The space Γ has the interesting property that any transformation of it is a homeomorphism of it onto itself, and we may define the action of G on Γ by defining $x^*(\xi) = x + \xi$ for $x \in G$, $\xi \in \Gamma$. Since the discrete topology is always admissible (provided the transformations of the group are homeomorphism) it follows that we have here a topological transformation group acting on the space Γ . The action of the group is of course transitive and effective and the stabilizer H_0 is trivial. Clearly all of the hypotheses of Theorem 20 are satisfied, the space Γ being in fact compact, but G and Γ are not homeomorphic.

Γ is an isometric transformation or a motion of Γ if it preserves distances, i.e., if for arbitrary ξ and η in Γ we have

$$\rho(x(\xi), x(\eta)) = \rho(\xi, \eta).$$

It is obvious that the set of all isometric transformations of Γ forms a group. The various subgroups of this group are called groups of isometric transformations of the space Γ .

Let G be an arbitrary group of isometric transformations of a compact metric space Γ . We introduce in G a metric and consequently also a topology by defining the distance $\rho(x, y)$ between two transformations x and y to be the maximum of the distances $\rho(x(\xi), y(\xi))$ taken over all $\xi \in \Gamma$. The distance function thus obtained in G satisfies the axioms of a metric space. It is readily verified that the topological group G is a topological transformation group acting on Γ . In case G is the group of all isometric transformations of Γ then, as is easily seen, G is countably compact and consequently compact (see Ex. 26) whence it follows from Theorem 19 that the topology introduced in G is the only compact topology with respect to which G is a topological transformation group on Γ . In the event that the group G of all isometric transformations of Γ is transitive then Theorem 20 can also be applied. This is, for instance, the case with the group of all isometric transformations of the unit sphere $\sum x_i^2 = 1$ in Euclidean space of dimension $n + 1$. This particular transformation group is isomorphic with the topological group of all orthogonal matrices of order $n + 1$ (see Ex. 34).

Example 46: Let Γ denote real Euclidean space of dimension n with a fixed coordinate system and denote by G the topological group of all real non-singular square matrices of order n (see Ex. 34). To each matrix $\|x_j^i\| \in G$ we associate a transformation x of the space Γ carrying the vector $\xi = (\xi^1, \dots, \xi^n)$ into the vector $x(\xi) = (\eta^1, \dots, \eta^n)$ defined by the relations

$$\eta^i = \sum_{j=1}^n x_j^i \xi^j, \quad i = 1, \dots, n.$$

It is easy to see that distinct matrices determine distinct transformations and that the product of matrices corresponds to the product of transformations. Thus the algebraic group G becomes an effective transformation group acting on Γ . It is also easy to verify that the topological group G is a topological transformation group acting on the topological space Γ . Since G is locally compact and separable we may here apply Theorem 19 to conclude that the topology we have introduced in G is the only topology turning

G into a locally compact separable topological transformation group acting on Γ . We observe that G consists of all automorphisms of Γ considered as a topological group (see Def. 26). Thus we have introduced in the group G of all automorphisms of the vector group Γ the natural topology turning G into a topological group.

4

TOPOLOGICAL DIVISION RINGS

Along with topological groups an important role is played in mathematics by topological rings and fields, i. e., rings and fields in which the algebraic operations are continuous. Although we shall consider in this chapter topological rings in general, the entire chapter is aimed at the investigation of topological division rings or, more precisely, of continuous division rings, i. e., locally compact non-discrete topological division rings.

A continuous division ring is defined by a small number of entirely natural axioms; nevertheless the concept possesses an extraordinary concreteness. It turns out that there exist but three distinct connected continuous division rings, viz., the field of real numbers, the field of complex numbers, and the division ring of quaternions. Disconnected continuous division rings exist in greater abundance and no complete description of them will be given; nevertheless they are comparatively concrete. It turns out that each of them is a finite extension, either of the field of p -adic numbers or of the field of power series over the field of residue classes modulo p (Section 26).

The concrete examples of continuous division rings just mentioned—the field of real numbers, the field of complex numbers, the quaternions, the field of p -adic numbers, and the field of power series over the field of residue classes modulo p —may be considered the classical continuous division rings. They have been familiar for a comparatively long time and play an essential role in mathematics. The uniqueness results formulated above show that the importance of the classical continuous division rings is not to be regarded as a historical accident but rather as a logical necessity. Thus the results of the present chapter possess a certain philosophical interest, giving, as they do, a logical justification of the

historical development of the concepts of the real and complex numbers.

The results of this chapter will not be used in the sequel.

SECTION 25. TOPOLOGICAL RINGS AND DIVISION RINGS

In this paragraph we define topological rings and investigate their simplest properties.

Definition 32: A set R is said to be a topological ring if:

- 1) R is a ring (see Definition 11);
- 2) R is a topological space;
- 3) The algebraic operations defined in R are continuous in the topological space R . In greater detail: for arbitrary elements a and b in R and for arbitrary neighborhoods W and W' of the elements $a - b$ and ab respectively, there exists neighborhoods U and V of a and b such that $U - V \subset W$ and $UV \subset W'$.

In the event that R is a division ring it will be said to be a topological division ring if in addition the following condition is satisfied:

- 4) for any $a \neq 0$ in R and for an arbitrary neighborhood W of a^{-1} there exists a neighborhood U of a satisfying the condition $U^{-1} \subset W$.

A commutative topological division ring is a topological field.

If, in discussing a topological ring, we wish to underline the fact that we refer only to its algebraic properties and disregard its topological structure, we shall refer to it as an algebraic, i.e., abstract ring.

A) A mapping g of a topological ring R into a topological ring R' is a homomorphism if it is a homomorphism of the algebraic ring R into the algebraic ring R' and is also a continuous mapping of the topological space R into the topological space R' . The set of all elements in R that are carried by g into the zero element R' is the kernel of the homomorphism. Clearly the kernel of a homomorphism is an ideal in the algebraic ring R and a closed set in the topological space R .

B) A subset I of a topological ring R is an ideal of that ring if it is both an ideal of the algebraic ring R and a closed subset in the topological space R . Forming the factor group R/I of the additive topological group R of the topological ring R by the ideal I we obtain an additive topological group R/I in which is defined an operation of multiplication (see Section 7, B)). It is easy to verify that this multiplication is continuous with respect to the topology of the space R/I so that R/I is itself a topological ring,

known as the factor ring or the ring of residue classes of the topological ring R modulo the ideal I . The natural projection g of the algebraic ring R onto the algebraic ring R/I is an open continuous mapping of the topological space R onto the topological space R/I . Accordingly g is an open homomorphism of the topological ring R onto the topological ring R/I .

C) A mapping of a topological ring R onto a topological ring R' is an isomorphism if it is an isomorphic mapping of the algebraic ring R onto the algebraic ring R' and also a homeomorphism of the topological space R onto the topological space R' .

Clearly the mapping inverse to an isomorphism is itself an isomorphism.

D) Let I be the kernel of an open homomorphism g of a topological ring R onto a topological ring R^* . The natural isomorphism f of the algebraic ring R/I onto the algebraic ring R^* associated with g (see Section 7, D)) is in fact an isomorphism of the topological ring R/I onto the topological ring R^* (see Theorem 11). Observe also that Theorem 12 continues to hold for rings; if R and R^* are locally compact and if R is the union of a countable collection of compact subsets then a homomorphism of the topological ring R onto the topological ring R^* is necessarily open.

In Section 27 it will be shown that every locally compact topological division ring satisfies the first axiom of countability, i.e., possesses a countable base of neighborhoods at each point. This state of affairs permits us to base our investigation of topological division rings in large measure on the concept of a convergent sequence. We here exploit sequences to establish certain facts about topological division rings which will be of use in the following two paragraphs.

E) Let K be a topological division ring satisfying the first axiom of countability. Then a sequence a_1, \dots, a_n, \dots of elements in K is said to converge to the element a —in symbols, $\lim_{n \rightarrow \infty} a_n = a$ —if for every neighborhood U of a there exists a positive integer k such that $a_n \in U$ for $n > k$. Let U_1, \dots, U_n, \dots be any countable base of neighborhoods at a point $b \in K$; defining $V_n = U_1 \cap U_2 \cap \dots \cap U_n$ we obtain a countable base at b consisting of a decreasing sequence of neighborhoods:

$$V_1 \supset V_2 \supset \dots \supset V_n \supset \dots \quad (1)$$

If M is any set having b in its closure, $b \in \bar{M}$, then, employing the sequence (1), we may find a sequence b_1, \dots, b_n, \dots of points in the set M converging to b . Indeed if b_n is any point of $M \cap V_n$ then clearly $\lim_{n \rightarrow \infty} b_n = b$. If in addition b is a limit point of M , $b \in M \setminus \{b\}$,

then it is possible to select in M a sequence b_1, \dots, b_n, \dots of points distinct from b and converging to b . If

$$\lim_{n \rightarrow \infty} a_n = a, \quad \lim_{n \rightarrow \infty} b_n = b$$

then, by virtue of the continuity of the algebraic operations in K , we have:

$$\begin{aligned} \lim_{n \rightarrow \infty} (a_n + b_n) &= a + b, \quad \lim_{n \rightarrow \infty} (a_n b_n) = ab \\ \lim_{n \rightarrow \infty} (-a_n) &= -a \quad \text{and for } a \neq 0 \lim_{n \rightarrow \infty} a_n^{-1} = a^{-1}. \end{aligned}$$

A sequence a_1, \dots, a_n, \dots in the division ring K is said to be fundamental if for every neighborhood U of 0 there exists a natural number k such that

$$a_n - a_m \in U \text{ for } n > k, m > k.$$

Two fundamental sequences a_1, \dots, a_n, \dots and b_1, \dots, b_n, \dots are equivalent if the sequence $a_1, b_1, \dots, a_n, b_n, \dots$ is also fundamental. It may be verified at once that if two sequences converge to one and the same point then they are equivalent fundamental sequences. It may also be shown without difficulty that if K is locally compact then every fundamental sequence in K is convergent.

The following propositions, the proofs of which are based upon the concept of a fundamental sequence, will be of use later on. We assume for the time being that all locally compact division rings satisfy the first axiom of countability.

F) Let R be a topological division ring satisfying the first axiom of countability, let T be an everywhere dense subring in R , and let f be an isomorphism of the topological ring T onto a topological subring T' of a locally compact division ring K' . Then there exists one and only one isomorphism φ of the topological division ring R onto a topological subdivision ring R' of the division ring K' which coincides with f on T .

We prove the proposition by constructing φ . Let α be a fixed but arbitrary element of R and let a_1, \dots, a_n, \dots be a sequence of elements of T converging to α . Since a_1, \dots, a_n, \dots is a convergent sequence in R it is fundamental and is therefore a fundamental sequence in T . But then, since f is an isomorphism between the topological rings T and T' , it follows that, letting $a'_n = f(a_n)$, we obtain another fundamental sequence $a'_1, a'_2, \dots, a'_n, \dots$ in T' . This latter sequence is also fundamental in K' and consequently must converge to some element α' since K' is locally

compact. It is easy to see that α' is determined uniquely by α and does not depend upon the choice of the sequence a_1, \dots, a_n, \dots . Moreover it is clear that if $\alpha \in T$ then $\alpha' = f(\alpha)$. By the same token, if a continuous extension φ of the mapping f exists it must satisfy the relation $\varphi(\alpha) = \alpha'$ and is therefore uniquely determined by f . Accordingly we regard this relation as defining φ and we show that the mapping thus obtained is an isomorphism of the topological division ring R onto the topological division ring $R' = \varphi(R) \subset K'$.

We show first that φ preserves addition and multiplication, i.e., that it is a homomorphism of the algebraic division ring R into K . Indeed we have:

$$\begin{aligned}\varphi(\alpha) + \varphi(\beta) &= \lim_{n \rightarrow \infty} f(a_n) + \lim_{n \rightarrow \infty} f(b_n) = \lim_{n \rightarrow \infty} (f(a_n) + f(b_n)) \\ &= \lim_{n \rightarrow \infty} f(a_n + b_n) = \varphi(\alpha + \beta).\end{aligned}$$

That $\varphi(\alpha) \varphi(\beta) = \varphi(\alpha\beta)$ is proved in exactly the same fashion. Inasmuch as a division ring possesses no non-trivial ideals, the kernel of the homomorphism φ must be $\{0\}$, and it follows that φ is an isomorphism of the algebraic division ring R onto the algebraic division ring $R' = \varphi(R)$.

We next show that φ is continuous and open at 0; this implies that it is a homeomorphism (see Section 20, A)). Let Λ' be an arbitrary neighborhood of 0 in R' , let M' be another neighborhood of 0 such that $M' \subset \Lambda'$ (closure being taken with respect to R'), and let $V' = T' \cap M'$. Define $V = f^{-1}(V')$ and let M be a neighborhood of 0 in R such that $M \cap T = V$. We shall show that $\varphi(M) \subset \Lambda'$, thus proving the continuity of φ . Indeed let α be an arbitrary element of M ; then, as is easily seen, there exists a sequence a_1, \dots, a_n, \dots of elements in V converging to α so that $\varphi(\alpha) = \lim_{n \rightarrow \infty} f(a_n) \in \bar{V}' \subset \bar{M}' \subset \bar{\Lambda}'$. It remains to show that φ is open. This time let Λ be an arbitrary neighborhood of 0 in R , let M be another neighborhood of 0 such that $\bar{M} \subset \Lambda$, and let $V = M \cap T$. Define $V' = f(V)$ and let M' be a neighborhood of 0 in R' such that $V' = M' \cap T'$. We shall show that $\varphi(\Lambda) \supset M'$ thus completing the proof of the theorem. Indeed let α' be an arbitrary element of M' , according to the definition of R' there exists in T a sequence a'_1, \dots, a'_n, \dots converging to some element $\alpha \in R$ such that if $a'_n = f(a_n)$ then the sequence a'_1, \dots, a'_n, \dots of elements of T' converges to α' . Since M' is open and contains α' all terms of the sequence from some point on must lie in $M' \cap T' = V'$. Thus we may and do assume that all elements of the sequence a'_1, \dots, a'_n, \dots

lie in V' . But then the sequence a_1, \dots, a_n, \dots is contained in V whence it follows that $\alpha = \lim_{n \rightarrow \infty} a_n \in \bar{V} \subset \bar{M} \subset \Lambda$ which shows that $\varphi(\Lambda) \supset M'$. Thus proposition F) is proved.

G) A topological division ring is said to be continuous if it is locally compact and not discrete. We shall say that a topological division ring admits continuous closure if it is not discrete and can be mapped isomorphically onto a subdivision ring of some continuous ring or, as we shall say, if it can be imbedded in a continuous division ring. Let L be a topological division ring admitting continuous closure and let K be some continuous division ring containing L ; then the continuous division ring \bar{L} is uniquely determined by the original topological division ring L and is not dependent upon the choice of the englobing ring K . The division ring \bar{L} is called the continuous closure of L .

That L is in fact independent of the choice of K may be seen as follows. Let f be an isomorphism of L onto a topological subdivision ring L' of an arbitrary continuous division ring K' . Then by the preceding proposition there exists one and only one isomorphism φ of \bar{L} onto the division ring \bar{L}' which coincides with f on L .

SECTION 26. THE CLASSICAL CONTINUOUS DIVISION RINGS

The topological field D^1 of real numbers and the topological field D^2 of complex numbers find the widest application in mathematics generally and are well known to everyone. We here introduce the division ring D^4 of quaternions, the field K_0^p of p -adic numbers, and the field K_t^p of power series over the field of residue classes modulo p . The role of these topological division rings will be elucidated in the following paragraph where it will be shown that the fields D^1 , K_0^p and K_t^p , where p is an arbitrary prime number, are simple and that every simple continuous field is isomorphic with one of these. In greater detail, it will be shown that D^1 and K_0^p contain no proper continuous subfields while every continuous subfield of K_t^p is isomorphic with K_t^p itself. Moreover it will be shown that every continuous division ring contains as a subfield one of the fields D^1 , K_0^p , K_t^p and is a finite extension thereof.

The significance of the field of complex numbers and the division ring of quaternions is something else again. In the present paragraph we prove the theorem of Frobenius (see B) which asserts that every division ring that is a finite extension of the field D^1 of real numbers either coincides with D^1 or is isomorphic either with the field D^2 of complex numbers or with the division ring D^4 .

of quaternions. Combining the theorem of Frobenius with the above formulated results, borrowed from the following paragraph, we are led to the conclusion that every connected locally compact division ring is isomorphic with either the field of real numbers or the field of complex numbers or the division ring of quaternions.

We begin with the definition of the quaternions.

A) Denote by D^4 a four-dimensional Euclidean vector space in which an orthogonal Cartesian coordinate system has been fixed. The vectors $x = (x^0, x^1, x^2, x^3) \in D^4$ will be written in the form $x = x^0 + ix^1 + jx^2 + kx^3$ where i, j, k are the quaternion units. We define a law of multiplication in D^4 by agreeing that multiplication should be distributive, that real numbers should commute with the quaternion units, and that the quaternion units themselves are multiplied according to the formulas

$$ij = -ji = k; \quad jk = -kj = i; \quad ki = -ik = j; \quad ii = jj = kk = -1. \quad (1)$$

It turns out that with this law of multiplication and the ordinary law of addition D^4 becomes a continuous division ring known as the division ring of quaternions. It is readily verified that the operation of multiplication here defined in D^4 is associative. The quaternion \bar{x} conjugate to the quaternion x is defined to be $\bar{x} = x^0 - ix^1 - jx^2 - kx^3$. A simple calculation shows that

$$\bar{xy} = \bar{y} \bar{x} \quad (2)$$

Defining the norm of x to be the non-negative real number

$$|x| := \sqrt{\bar{x}x} = [(x^0)^2 + (x^1)^2 + (x^2)^2 + (x^3)^2]^{1/2}$$

we obtain

$$|xy|^2 = xy\bar{xy} = xy\bar{y}\bar{x} = x \cdot |y|^2 \cdot \bar{x} = |y|^2 x\bar{x} = |x|^2 |y|^2.$$

Consequently

$$|xy| = |x| \cdot |y|. \quad (3)$$

If $x \neq 0$ then $|x| \neq 0$ and there exists a quaternion x^{-1} inverse to x , viz., $x^{-1} = \bar{x}/|x|^2$. Thus D^4 is a continuous division ring. The division ring D^4 contains a copy D^1 of the field of real numbers consisting of all quaternions of the form $x = x^0 + 0i + 0j + 0k$. The collection G of all quaternions x satisfying the condition $|x| = 1$ constitutes, by virtue of (3), a topological group under multiplication. The set G is just the three dimensional unit sphere in the Euclidean space D^4 . Quaternions of the form $x^1i + x^2j + x^3k$ are said to be pure imaginary. The collection I of all pure imaginary quaternions forms a three dimensional vector space orthogonal in D^4 to the real axis D^1 .

We now prove the theorem of Frobenius.

B) Let K be a division ring and suppose that K is a finite extension of the field D^1 of real numbers which we suppose to be contained in the center of K . By this is meant that there exists in K a system $1, e_1, \dots, e_k$ of elements linearly independent over D^1 such that every element $x \in K$ may be represented uniquely in the form

$$x = d^0 + d^1 e_1 + \dots + d^k e_k, \quad d^i \in D^1,$$

and such that the elements e_1, \dots, e_k commute with all elements of D^1 . Then either K coincides with D^1 or is isomorphic with the field D^2 of complex numbers or the division ring D^4 of quaternions.

We may assume that $K \neq D^1$. Denote by I the set of all elements $z \in K$ satisfying the conditions $z^2 \in D^1, z^2 \leq 0$. We shall show that every element $x \in K$ possesses a unique expression of the form

$$x = d + z, \quad \text{where } d \in D^1, z \in I. \quad (4)$$

Consider the sequence of powers of x :

$$1, x, x^2, \dots, x^n, \dots \quad (5)$$

Since K is a finite dimensional vector space, the elements of the sequence (5) are necessarily linearly dependent over D^1 . Consequently there exists a non-zero polynomial $f(y)$ with real coefficients which vanishes at $x f(x) = 0$. The polynomial $f(y)$ may, of course, be assumed to have lead coefficient one and may also be assumed to be irreducible; but, as is well known, an irreducible polynomial over the field of real numbers has degree one or two. Now if $f(y) = y - d$ then $x = d \in D^1$ and (4) holds with $z = 0$. If on the other hand $f(y) = y^2 + py + q$ then, completing squares and recalling that $f(y)$ is irreducible, we may find real numbers c and d such that $f(y) = (y - d)^2 + c^2$. But then $x = d + z$ where $x - d = z \in I$. Thus (4) is obtained in either case.

Next suppose given an arbitrary resolution of x of the form (4): $x = d' + z'$ where $d' \in D^1, z' \in I$. Then $z' = z + d - d'$ and, squaring both sides, we have $z'^2 = z^2 + (d - d')^2 + 2(d - d')z$ whence it follows that $(d - d')z \in D^1$. But it is clear that $(d - d')z \in I$ so that $(d - d')z = 0$. Thus either $d - d' = 0$ or $z = 0$, and in either case the uniqueness of the expression (4) follows at once.

We next establish the important fact that I is a linear subspace in K , i. e., that

$$ax + by \in I \quad (6)$$

whenever $x \in I, y \in I$ and a and b are real numbers.

Consider first the case when $x, y, 1$ are linearly dependent over D^1 , i.e., when there exist real numbers α, β, γ , not all zero, such that $\alpha x = \beta y + \gamma$. Clearly αx and βy belong to I so that by the uniqueness of (4) $\gamma = 0$. By then $y = \alpha/\beta x$ so that $\alpha x + \beta y = (\alpha + \beta) x$ and (6) holds.

It remains to consider the case in which the element $ax + by$ belongs to D^1 only when $a = b = 0$. Using (4) we let

$$ax + by = d' + z', \quad (7)$$

with $d' \in D^1$, $z' \in I$ where d' and z' depend upon the coefficients a and b . According to our hypothesis, z' can vanish only when $a = b = 0$. We shall show that $d' = 0$ for all choices of a and b . Let

$$xy + yx = d + z \quad (8)$$

as in (4). Squaring both sides of (7) we obtain

$$\begin{aligned} d'^2 + z'^2 + 2d'z' &= a^2x^2 + b^2y^2 + ab(xy + yx) = \\ &= a^2x^2 + b^2y^2 + abd + abz. \end{aligned} \quad (9)$$

Since the expression (4) is unique, (9) implies

$$2d'z' = abz. \quad (10)$$

where z is independent of a and b . Suppose now that $d' \neq 0$ for some choice of a and b . Then $z' \neq 0$ whence it follows from (10) that $z \neq 0$. But this says that $d' \neq 0$ whenever $ab \neq 0$. Thus we obtain

$$z' = \frac{ab}{2d'} z, \quad (11)$$

whenever $ab \neq 0$. Consequently

$$ax + by = \frac{ab}{2d'} z + d' \quad (12)$$

for any choice of a and b such that $ab \neq 0$. Since z does not depend upon a and b we may obtain from (12) two independent equations connecting x, y , and z . But then the elimination of z leads to a relation of the form $a'x + b'y = c'$ thus contradicting the hypothesis of independence. Hence we are led to the conclusion that $d' = 0$ independently of a and b , i.e., that I is a linear subspace.

Suppose now given o elements i and j of K such that $i^2 = j^2 = -1$ and satisfying the condition that $k = ij \in I$. We shall show that in this case i, j, k are linearly independent over D^1 and form a system of quaternion units, i.e., satisfy relation (1).

Since $ij \in I$ it follows that ij may be written in the form al where $a \in D^1$ while $l^2 = -1$. Now $(ij)(ji) = i(-1)i = 1$ so that $ji = (al)^{-1}$.

But $(al)^{-1}$ is just $-a^{-1}l$ as is easily verified so that $j i = -a^{-1}l$. Also since I is a subspace of K and i and j belong to I we have $i + j \in I$ so that $(i + j)^2 = i^2 + j^2 + ij + ji$ is real, whence it follows that $ij + ji$ is also real. From this we conclude that $(a - \frac{1}{a})l \in D^1$, i.e., that $a^2 = 1$ so that $k = al$ satisfies the condition $k^2 = -1$. Thus we have

$$i^2 = -1, j^2 = -1, k^2 = -1. \quad (13)$$

Taking the reciprocal of both sides of the equation

$$ij = k, \quad (14)$$

we next obtain $j^{-1}i^{-1} = k^{-1}$ or, what comes to the same thing, (see (13)) $ji = -k$. Next multiplying (14) on the left by $-i$ we obtain $j = -ik$. The remaining equations of the table (1) may be verified in similar fashion.

Suppose now that

$$bi + cj + dk = 0 \quad (15)$$

where b, c and d are real coefficients. Multiplying on the left by k we obtain $bj = c i + d$. But then, by virtue of the uniqueness of (4) it follows that $d = 0$ and hence that $bij = -c$ which is possible only when $b = c = 0$ since $(ij)^2 = -1$. Thus i, j, k are linearly independent.

Suppose now that every pair of elements of I is linearly dependent over D^1 . Since, as we assume, $K \neq D^1$ it follows that I contains non-zero elements and consequently an element i satisfying the equation $i^2 = -1$. Since every other element of I is by assumption linearly dependent on i it follows from (4) that every element of K may be written in one and only one way in the form $a + bi$ where a and b are real numbers. But then, as is seen at once, K is isomorphic with the field D^2 of complex numbers.

The only case remaining to be considered is when I contains two elements x and y which are linearly independent over D^1 . We shall show that in this case K contains a subdivision ring D^4 of quaternions. Indeed let $xy = z + d$ where $z \in I$, $d \in D^1$ as in (4). Since x^2 is a real number distinct from 0 there exists a real number a such that $ax^2 = -d$ and for this choice of a we have $x(y + ax) = z$. On the other hand, since x and y are linearly independent we have $y' = y + ax \neq 0$; moreover $y' \in I$ since I is linear. Thus, normalizing x and y' by multiplying by suitable real numbers, we obtain elements i and j such that $i^2 = j^2 = -1$ and such that $ij = k \in I$.

But then, as has been shown, the elements i, j, k are linearly

independent and satisfy (1) so that the set of all linear combinations $a + bi + cj + dk$ with coefficients a, b, c, d belonging to D^1 constitutes a subdivision ring of K which is isomorphic with the division ring of quaternions. We complete the proof of the theorem of Frobenius by showing that, in the case under consideration, $K = D^4$.

Suppose indeed that K contains an element not belonging to D^4 . Then there exists an elements $z \in I$ linearly independent of the units i, j, k . Let

$$iz = d_1 + z_1, \quad jz = d_2 + z_2, \quad kz = d_3 + z_3$$

according to (4). Let, moreover,

$$l = a(z + d_1 i + d_2 j + d_3 k),$$

where a denotes a real number. Then all three of the elements $i l, j l, k l$ belong to I by linearity. Also, by the same token, $l \in I$ and $l \neq 0$ since z is not linearly dependent on i, j, k . Accordingly the parameter a may be chosen such that $l^2 = -1$ and with this choice the elements i, l, il also form a system of quaternion units (see (13) and (14)). In particular $il = -li, (il)^2 = -1$. The same holds for the elements j, k and we obtain the relations

$$(il)^2 = (jl)^2 = (kl)^2 = -1, \quad il = -li, \quad jl = -lj, \quad kl = -lk. \quad (16)$$

From this it follows on the one hand that

$$(il)k = (-li)k = l(-ik) = lj, \quad (17)$$

and on the other hand that

$$(il)k = i(lk) = i(-kl) = (-ik)l = jl. \quad (18)$$

But from (16), (17) and (18) we conclude that $2jl = 0$ which contradicts the relation $(jl)^2 = -1$. Thus the assumption $K \neq D^4$ leads to a contradiction and proposition B) is proved.

To each prime number p there correspond two separable continuous fields K_0^p and K_t^p uniquely determined by the number p . The field K_0^p is the field of p -adic numbers; the field K_t^p is the field of power series over the field P^p of residue classes modulo p . The fields K_0^p and K_t^p are, in a natural fashion, homeomorphic with one another and are also similar in other respects so that it will be convenient to treat their definitions simultaneously.

C) Let R_0^p denote the topological field of rational numbers with the ordinary definitions of multiplication and addition but having, as a complete system of neighborhoods of 0, the sequence of sets $V_0, V_1, \dots, V_n, \dots$ where V_n consists of all rational numbers

of the form $\frac{ap^n}{b}$ where a and b are integers and b is not divisible by p (here p denotes a fixed prime number, the choice of which determines the field R_0^p). Then R_0^p admits continuous closure K_0^p (see Section 25, G)). The continuous field K_0^p is called the field of p -adic numbers. Let R_t^p denote the topological field of rational functions in the indeterminate t with coefficients in the field P^p of residue classes modulo p , with the ordinary definitions of multiplication and addition (see Section 7, G)) and having, as a complete system of neighborhoods of 0, the sequence of sets $V_0, V_1, \dots, V_n, \dots$ where V_n consists of the collection of all rational functions of the form $\frac{a(t)t^n}{b(t)}$, $a(t)$ and $b(t)$ being polynomials with $b(t)$ not divisible by t . Then R_t^p also admits continuous closure K_t^p . The continuous field K_t^p is the field of power series over P^p .

In order to establish proposition C) it is necessary, in the first place, to verify that the systems of neighborhoods given in the fields R_0^p and R_t^p really define topologies and also that the algebraic operations are continuous in these topologies. The proofs of these facts are straightforward and will be omitted. Considerably more complicated is the proof of the fact that the two fields R_0^p and R_t^p admit continuous closure. In fact this will be proved by actually constructing the fields K_0^p and K_t^p .

We begin by constructing a topological space K^p from which the fields K_0^p and K_t^p will then be obtained by introducing suitable algebraic operations. The set K^p is defined to consist of the collection of all formal series of the form

$$x = f(t) = \sum_{i=k}^{\infty} a_i t^i. \quad (19)$$

where t is an indeterminate, k is an arbitrary integer, so that the series (19) may contain an arbitrary finite number of terms of negative degree, while the coefficients a_i are integers satisfying the condition $0 \leq a_i < p$. The finite series

$$\pi_n(x) = \sum_{i=k}^n a_i t^i. \quad (20)$$

will be termed a segment of the series (19). In terms of this concept we define the neighborhood $U_n(a)$, $a \in K^p$, to consist of the collection of all $x \in K^p$ satisfying the relation $\pi_n(x) = \pi_n(a)$. For neighborhoods of the zero series we shall employ the abbreviation $U_n(0) = U_n$. It is easily verified that the system of all sets $U_n(a)$, $a \in K^p$, $n = 0, \pm 1, \pm 2, \dots$ is countable and defines a topology in K^p (see Theorem 3). It is obvious that in this topology K^p is

locally compact and totally disconnected (see Section 15, D)). The local compactness follows from the fact that each of the neighborhoods U_n (a) is countably compact and separable (see Example 25).

In order to define addition and multiplication in K^p we first define these operations in the everywhere dense set S^p consisting of all finite series in K^p . Let S_0^p denote the collection of all numbers in R_0^p having the form $\frac{a}{p^m}$ where $a \geq 0$ and m are integers. Analogously let S_t^p denote the set of all rational functions in R_t^p having the form $\frac{a(t)}{t^m}$ where $a(t)$ is a polynomial and m is an integer.

We proceed to define a mapping ω_δ of the set S^p onto S_δ^p , $\delta = 0, t$. In order to define ω_0 we simply replace the indeterminate t in the finite series $u = f(t)$ with the prime number p , thus defining $\omega_0(u) = f(p)$. On the other hand, in order to define ω_t we replace the coefficients a_i (see (19)) in the finite series $u = f(t)$ with their respective residue classes modulo p , thus obtaining a rational function $f^*(t)$ in the indeterminate t over the field P^p of residue classes modulo p , and then define $\omega_t(u) = f^*(t)$. It may be verified without difficulty that ω_δ is a homeomorphism of S^p onto the set $S_\delta^p \subset R_\delta^p$, $\delta = 0, t$. Clearly in either case the subset S_δ^p of the field R_δ^p is closed with respect to the operations of addition and multiplication, while S_t^p is even closed with respect to the operation of subtraction so that S_t^p is a subring of the field R_t^p . Using ω_δ^{-1} to carry into S^p the operations of addition and multiplication already defined in S_δ^p , we define corresponding algebraic operations in the set S^p itself, and this in two ways: $\delta = 0, t$. These operations, extended by continuity to the entire space K^p , turn this space into the fields K_0^p and K_t^p respectively. It remains, then to prove that the algebraic operations thus defined in S^p can in fact be extended by continuity and that the result of doing so is, in each case, a field.

We note that if u and v are two elements of S^p then their sum and product, as defined with the aid of the mapping ω_δ , may be written in the form:

$$u + v = \omega_\delta^{-1}(\omega_\delta(u) + \omega_\delta(v)), \quad (21)$$

$$uv = \omega_\delta^{-1}(\omega_\delta(u)\omega_\delta(v)). \quad (22)$$

Our task is to extend these operations to the entire space K^p . If $x \in K^p$ and if we define

$$\pi_n(x) = x_n \quad (23)$$

then, as is easily seen,

$$\pi_n(x_{n+1}) = x_n, \quad (24)$$

and the sequence

$$x_1, x_2, \dots, x_n, \dots \quad (25)$$

converges to x . Conversely, given a sequence (25) of elements of S satisfying (24), the sequence must converge to some element $x \in K^p$ for which (23) holds.

Now suppose given a sequence

$$\psi_1, \dots, \psi_n, \dots \quad (26)$$

of functions, of either one or two variables, defined on a set $M \cap S^p$ and taking values in S^p , where M is a closed-open subset of K^p . Suppose also that the following conditions are satisfied by these functions:

$$\pi_n(\psi_{n+1}(u, v)) = \psi_n(u, v), \quad (27)$$

$$\psi_n(u, v) = \psi_n(\pi_k(u), \pi_l(v)) \quad \text{for } k \geq n + h, l \geq n + h \quad (28)$$

where h is independent of u and v , $u, v \in M \cap S^p$. Relation (28) implies that the functions ψ_n are continuous (and even uniformly continuous, see Section 28, B) while (27) implies that the sequence (26) converges.

Starting from a sequence of functions (26) satisfying conditions (27), (28) we now construct a continuous function ψ taking values in K^p , defined on the entire set M , and satisfying the condition

$$\begin{aligned} \pi_n(\psi(u, v)) &= \psi_n(u, v); \quad u \in M \cap S^p, \\ v &\in M \cap S^p. \end{aligned} \quad (29)$$

Indeed let x and y be any two elements of M . Since M is open it follows that $\pi_n(x)$, $\pi_n(y)$ belong to M for sufficiently large n . Accordingly we may define

$$z_n = \psi_n(\pi_{n+h}(x), \pi_{n+h}(y)). \quad (30)$$

From (27) it follows then that

$$\begin{aligned} \pi_n(z_{n+1}) &= \pi_n(\psi_{n+1}(\pi_{n+h+1}(x), \pi_{n+h+1}(y))) \\ &= \psi_n(\pi_{n+h+1}(x), \pi_{n+h+1}(y)) = z_n. \end{aligned}$$

Thus the sequence

$$z_1, z_2, \dots, z_n, \dots$$

satisfies (24) and accordingly converges to an element z satisfy-

ing the condition

$$\pi_n(z) = z_n.$$

We now define

$$\psi(x, y) = z.$$

Since, according to (30), the n -th approximation z_n to the element z depends only on the $(n + h)$ -th approximation to the elements x and y it follows that ψ is continuous.

The process here set forth for extracting a continuous function ψ from a sequence (26) will now be employed to define continuous operations of addition and multiplication in K^p corresponding to the two cases $\delta = 0, t$ (see (21), (22)). Indeed let

$$\psi_n(u, v) = \pi_n(u + v) \text{ where } M = K^p, h = 0, \quad (31)$$

$$\psi'_n(u, v) = \pi_n(uv) \text{ where } M = U_{-h}. \quad (32)$$

It may readily be verified that the functions ψ_n, x_n' defined by these equations satisfy conditions (27), (28) no matter whether the operations are taken as defined by means of ω_0 or by means of ω_t . Thus the operations of addition and multiplication may be extended in a continuous manner from S^p to the entire space K^p . Moreover since they are associative and distributive on S^p it follows by continuity that they remain associative and distributive on K^p .

We proceed now to define subtraction. For the field K_t^p this presents no difficulty since S_t^p is a ring in which the operation of subtraction is already defined so that in this case it suffices to let

$$\psi_n(u) = -\pi_n(u).$$

The limit ψ then satisfies

$$x + \psi(x) = 0, \quad x \in K^p$$

since the functions ψ_n satisfy the condition

$$\pi_n(u) + \psi_n(u) = 0.$$

For the mapping ω_0 things are more complicated since subtraction is not defined in S_0^p . In this case, for $u \in S^p$, we let $u_n = \pi_n(u)$, $u_n' = \omega_0(u_n)$. It is easy to see that u_n' does not exceed p^{n+1} and consequently that for the number $w_n' = p^{n+1} - u_n'$ the image $w_n = \omega_0^{-1}(w_n')$ is defined. Let $\psi_n(u) = \pi_n(w_n)$. Clearly $w_{n+1}' - w_n'$ is divisible by p^{n+1} from which it follows that $\pi_n(\pi_{n+1}(w_{n+1}')) = \pi_n(w_n)$ so that the sequence ψ_n satisfies (27). Condition (28) is also satisfied since, by construction, w_n' depends only on $\pi_n(u)$. Since $u_n' + w_n'$ is divisible by p^{n+1} it follows that $\pi_n(u) + \psi_n(u)$ belongs to the neighborhood U_{n+1} :

$$\pi_n(u) + \psi_n(u) \in U_{n+1}.$$

But this implies that for the limit function ψ we have

$$\pi_n(x) + \pi_n(\psi(x)) \in U_{n+1}, \quad x \in K^p.$$

Thus $x + \psi(x) = 0$ so that ψ defines subtraction as a continuous operation in K_0^p . Moreover, from what has been said, it is clear that every element of the set $-S_0^p$ is a limit point of S_0^p .

Finally we show that in the topological rings K_{δ}^p , $\delta = 0, t$, every element $x \neq 0$ possesses an inverse x^{-1} which depends continuously on x . The necessary construction will be carried out simultaneously in the two cases $\delta = 0, t$. Denote by M the set of all series $x \in K^p$ satisfying $k = 0, a_0 \neq 0$ (see (19)). Clearly M is both closed and open, and every element $x^* \neq 0$ in K^p may be written uniquely in the form $t^k x$, $x \in M$. Thus if $x \in M$ has an inverse x^{-1} then $t^k x$ has for inverse the element $t^{-k} x^{-1}$. Moreover the continuity of $t^{-k} x^{-1}$ follows from the continuity of x^{-1} , $x \in M$, since all elements belonging to a suitably small neighborhood of $t^k x$ necessarily possess the same k . Thus it suffices to consider the case $x \in M$. Let $u \in M \cap S^p$. We define $u_n = \pi_n(u)$, $u'_n = \omega_\delta(u_n)$, $t'_{n+1} = \omega_\delta(t^{n+1})$. If $\delta = 0$ then u'_n and t'_{n+1} are relatively prime integers while if $\delta = t$ then u'_n and t'_{n+1} are relatively prime polynomials. Thus in either case the equation

$$u'_n w'_n + t'_{n+1} s'_n = 1. \quad (33)$$

possesses a solution where, in case $\delta = 0$, the quantities w'_n and s'_n are integers of which the former w'_n may be assumed positive while, in case $\delta = t$, the quantities w'_n and s'_n are polynomials in R_t^p . Now let $w_n = \omega_\delta^{-1}(w'_n)$, $\psi_n(u) = \pi_n(w_n)$ where $u \in M \cap S^p$. We shall show that condition (27) is satisfied.

In the first place $u'_{n+1} = u'_n + at'_{n+1}$ where a denotes either an integer or a residue class modulo p . Accordingly we have

$$(u'_n + at'_{n+1}) w'_{n+1} + t'_{n+2} s'_{n+1} = 1. \quad (34)$$

Subtracting (33) from (34) we obtain

$$u'_n (w'_{n+1} - w'_n) = t'_{n+1} s_n - at'_{n+1} w'_{n+1} - t'_{n+2} s'_{n+1},$$

and since u'_n is relatively prime to t'_{n+1} it follows that $w'_{n+1} - w'_n$ is divisible by t'_{n+1} which implies that $\pi_n(w_{n+1}) = \pi_n(w_n)$. Thus (27) is established. Condition (28) is also satisfied since w'_n depends, by definition, only on u_n . Applying the mapping $\pi_n \omega_\delta^{-1}$ to (33) we obtain

$$\pi_n(\pi_n(u)\psi_n(u)) = 1, \quad n \geq 1. \quad (35)$$

Now let x be an arbitrary element of M ; letting $u = \pi_n(x)$ we obtain from (35):

$$\pi_n(\pi_n(x)\pi_n(\psi(x))) = 1.$$

Thus recalling (32) and taking the limit we obtain

$$x\psi(x) = 1.$$

In other words the inverse exists and is continuous. Moreover from what has been said it is clear that every element of the set $(S_{\delta^p} 0)^{-1}$ is a limit point of S_{δ^p} , whence it follows that S_{δ^p} is everywhere dense in the field R_{δ^p} .

In summary we may say that, in either case $\delta = 0, t$, the result of our construction is a homeomorphism of the set S_{δ^p} onto $S^p \subset K_{\delta^p}$ which preserves the operations of addition and multiplication. In case $\delta = t$ the set S_{δ^p} is in fact a subring of R_{δ^p} and we define $T_t = S_t^p$, $\omega_t^{-1} = f_t$. In case $\delta = 0$ the set S_{δ^p} is not a subring but may easily be extended to one by writing $T_0 = S_0^p \cup (-S_0^p)$. Clearly T_0 is a subring of R_0^p and the mapping ω_0^{-1} may be extended from S_0^p to an isomorphism f_0 of the topological ring T_0 into the field K_0^p by defining, for $x \in S_0^p$, $f_0(x) = \omega_0^{-1}(x)$, $f_0(-x) = -\omega_0^{-1}(x)$. Since in either case T_{δ} is everywhere dense in R_{δ^p} , it follows by proposition F), Section 25, that there exists a unique isomorphism φ of the field R_{δ^p} into the field K_{δ^p} which extends f_{δ} . Moreover since S^p is everywhere dense in K^p it follows that the field K_{δ^p} is precisely the continuous closure of R_{δ^p} (see Section 25, G)). Thus proposition C) is proved.

Example 47. Let D^4 be the division ring of quaternions, let I denote the collection of all purely imaginary quaternions, and let

$$u = u_1 i + u_2 j + u_3 k, \quad v = v_1 i + v_2 j + v_3 k$$

be two elements of I . A simple computation shows that the product uv has the expression

$$\begin{aligned} uv = & -(u_1 v_1 + u_2 v_2 + u_3 v_3) + (u_2 v_3 - u_3 v_2) i + \\ & +(u_3 v_1 - u_1 v_3) j + (u_1 v_2 - u_2 v_1) k. \end{aligned}$$

This expression bears an interesting relation to the scalar product (u, v) and the vector product $[u, v]$ of the vectors u and v defined by the following formulas:

$$(u, v) = u_1 v_1 + u_2 v_2 + u_3 v_3,$$

$$[u, v] = (u_2 v_3 - u_3 v_2) i + (u_3 v_1 + u_1 v_3) j + (u_1 v_2 - u_2 v_1) k.$$

Indeed, in terms of these products we have simply

$$uv = - (u, v) + [u, v].$$

SECTION 27.
THE STRUCTURE OF CONTINUOUS DIVISION RINGS

The present paragraph is devoted to a thoroughgoing analysis of the structure of a continuous division ring. The most definitive result relates to the connected case. Here the relevant theorem, which is due to me [42], asserts that every locally compact connected division ring is isomorphic with either the field of real numbers, the field of complex numbers or the division ring of quaternions. For an arbitrary continuous division ring (without the requirement of connectedness) we have Theorem 22, first obtained by Kowalski [27], which, while falling short of a complete classification, elucidates the structure of such rings in quite satisfactory fashion.* In essence the proof given here follows the route indicated in [42] however we also make use of some ingenious constructions borrowed from [27], which make it possible to extend my argument to the disconnected case. In Example 48 at the end of the paragraph is presented a discussion of a remark due to A. N. Kolmogorov [26] concerning the application of Theorem 21 to the axiomatics of projective geometry.

Theorem 21: Every connected locally compact topological division ring is isomorphic either with the field of real numbers, the field of complex numbers, or the division ring of quaternions.

Proof: Since a division ring contains at least the two distinct elements 0 and 1 it is clear that a connected division ring cannot be discrete. Thus a connected locally compact division ring is automatically continuous in the sense of Section 25, G) and Theorem 21 is therefore an immediate consequence of the following result along with the theorem of Frobenius proved in the preceding paragraph (see Section 26, B)).

Theorem 22: Let K be a continuous division ring with prime subfield P . Then one and only one of the following three mutually

* The trichotomy of Theorem 22 was, in fact, first obtained by Jacobson [19] who gave a complete classification. The literature relating to this theorem is extensive. Some other papers of particular factual or historic importance are [11], [12], [40], [50], [23]. In particular, it is interesting to note that the ideas of Kowalski, which were first worked out by Kaplansky [23], may be traced directly back to Shafarevich [50].

exclusive possibilities must obtain.

1) K has characteristic 0 so that P is algebraically isomorphic with the field P^0 of rational numbers (see Section 7, F)), and the closure $D^1 = \overline{P}$ of the prime subfield is isomorphic with the topological field of real numbers. In this case K is connected.

2) K has characteristic 0 but the closure $K_0^p = \overline{P}$ of the prime subfield is isomorphic with the topological field of p -adic numbers (see Section 26, C)). In this case K is disconnected.

3) K has characteristic $p > 1$ so that P is isomorphic with the field P^p of residue classes modulo p (see Section 7, F)). In this case K contains elements $t \neq 0$ such that the sequence of powers $t, t^2, \dots, t^n, \dots$ converges to 0, and any such element t is transcendental over P so that K also contains subfields $P^p(t)$ isomorphic with the field of rational functions in t with coefficients in P^p (see Section 7, G)). Moreover the closure $K_t^p = \overline{P^p(t)}$ of any such subfield is isomorphic with the field of formal power series over P^p constructed in Section 26, C)). In this case also K is disconnected.

In each of the three cases here enumerated let K^* denote the appropriate one of the subfields D^1 , K_0^p or K_t^p . Clearly K^* is a central subfield in case 1) and 2). It turns out that in all three cases K is a finite extension of K^* , i. e., there exists a finite system $e = x_1, x_2, \dots, x_r$ of elements in K such that every element $x \in K$ is expressible in one and only one way in the form

$$x = a_1 x_1 + \dots + a_r x_r,$$

the coefficients a_1, \dots, a_r belonging to the subfield K^* .

The proof of Theorem 22 is completely elementary but quite long and involved; accordingly we begin by giving a series of auxiliary results which, once established, permit a fairly brief proof of Theorem 22 itself.

A) A topological division ring K is either connected or totally disconnected.

Indeed, if K is not totally disconnected then the component L of zero contains some element $a \neq 0$. But then for any element $b \neq 0$ in K the connected set $L' = ba^{-1}L$ contains both 0 and b whence it follows that K is connected.

Lemma 1: Let K be a continuous division ring. Then at every point of K there is a countable base of neighborhoods (see Section 9, B')). Accordingly there exist in K sequences of non-zero elements which converge to zero. Let

$$a_1, a_2, \dots, a_n, \dots \quad (1)$$

be any such sequence. Then if F is any countably compact subset of K and W any neighborhood of zero there exists a positive integer ν sufficiently large so that

$$Fa_n \subset W, a_n F \subset W \quad \text{for } n \geq \nu. \quad (2)$$

From this it follows that a closed and countably compact subset of the space K is in fact compact. Moreover, it follows that if U is any neighborhood of zero with countably compact closure then the sequence

$$Ua_1, \dots, Ua_n, \dots \quad (3)$$

is a complete system of neighborhoods of zero. Finally, the sequence

$$a_1^{-1}, \dots, a_n^{-1}, \dots \quad (4)$$

has no limit point in K . Thus K itself is not compact.

Proof. Let W be a neighborhood of zero in K and let E be an arbitrary compact set. Then there exists a neighborhood V of zero such that

$$EV \subset W. \quad (5)$$

Indeed since $x_0 = 0$ and since multiplication is continuous, it follows that for every $x \in E$ there exist neighborhoods V_x and V'_x of 0 and x respectively such that $V'_x V_x \subset W$. The covering $\{V'_x\}$, $x \in E$, of the set E contains a finite covering $V'_{x_1}, \dots, V'_{x_m}$ and it is clear that (5) is satisfied by the intersection $V = V_{x_1} \cap \dots \cap V_{x_m}$.

Since K is, by hypothesis, not discrete it follows that there exists a countable set of elements distinct from 0 and having 0 as a limit point. Let b_1, \dots, b_ν, \dots be an enumeration of any such set and let U be any neighborhood of zero having compact closure. We shall show that the collection of neighborhoods Ub_1, \dots, Ub_n, \dots constitutes a base at zero. Indeed for any neighborhood W of zero let $E = \bar{U}$ and choose V so as to satisfy (5). Since 0 is a limit point of the set $\{b_1, \dots, b_n, \dots\}$ it follows that V contains some b_m whereupon we have $Ub_m \subset W$. Thus there exists a countable base of neighborhoods at zero, and it follows (see Section 17, D) that the same is true at every point.

Suppose now that (1) is a sequence of non-zero elements in K converging to zero. For an arbitrary neighborhood W of zero and an arbitrary countably compact subset F we verify the first part of (2), i.e., we show there exists a positive integer ν such that $Fa_n \subset W$ for every $n \geq \nu$, the proof of the other inclusion in

(2) being completely analogous. Indeed, if (2) is false then for a suitably selected subsequence we have $Fa_n \not\subset W$ and we assume without loss of generality that the subsequence has already been selected so that for every n there is an element $c_n \in F$ such that $c_n a_n \notin W$. Since F is countably compact and every one of its points possesses a countable base of neighborhoods it follows that the sequence c_1, \dots, c_n, \dots contains a convergent subsequence. Once again we may assume without loss of generality that the sequence c_1, \dots, c_n, \dots is itself convergent to some element c . But then by the continuity of multiplication we obtain $\lim_{n \rightarrow \infty} c_n a_n = c0 = 0$ which is impossible since each of the points $c_n a_n$ lies outside of W .

Next let W be any neighborhood having compact closure and let F be a closed and countably compact set. Then for suitably chosen n we have $Fa_n \subset W$. Since multiplication by a_n is a homeomorphism it follows that Fa_n is closed along with F . But then, as a closed subset of the compact set \bar{W} , Fa_n is compact, and so then is F .

Similarly, if U and W are neighborhoods of zero and if U has compact closure, then for suitably large n we obtain $\bar{U}a_n \subset W$ and it follows that the sets Ua_n constitute a base at zero.

It remains to show that the sequence (4) has no limit points. Indeed if a limit point d existed it would be possible to select from (4) a subsequence converging to d . Once again it is no loss of generality to assume that (4) is itself convergent to d , but then by the continuity of multiplication it would follow that $e = \lim_{n \rightarrow \infty} a_n a_n^{-1} = 0d = 0$, which is impossible. Thus Lemma 1 is proved.

Lemma 2: Let K be a continuous division ring and for each element $x \in K$ form the sequence of positive integral powers

$$x, x^2, \dots, x^n, \dots \quad (6)$$

Denote by A the set of all elements x for which (6) converges to zero, by C the set of all elements x for which (6) is divergent, i.e., has no limit points, and by B the set of all elements x with the property that (6) possesses neither a subsequence converging to zero nor a subsequence having no limit points. Then

$$K = A \cup B \cup C. \quad (7)$$

Moreover A is an open set about zero with compact closure \bar{A} , B is compact and C is open. Finally for any sequence

$$a_1, \dots, a_n, \dots \quad (8)$$

having no limit points the reciprocal sequence

$$a_1^{-1}, \dots, a_n^{-1}, \dots \quad (9)$$

converges to zero, whence it follows that

$$C^{-1} = A \setminus 0, B^{-1} = B. \quad (10)$$

Proof: Let U be a neighborhood of zero, the closure of which is compact and does not contain the unit e and let $F = \bar{U} \cup e$. We shall show that if some positive integral power x^k of an element x satisfies the condition

$$Fx^k \subset U \quad (11)$$

then the sequence (6) converges to zero. As a first step in this direction, we show that if x satisfies (11) then for an arbitrary positive integer n we have also

$$Fx^{nk} \subset U \quad (12)$$

Proof by induction. Suppose (12) holds for n ; then multiplying by x^k we obtain

$$Fx^{(n+1)k} \subset Ux^k \subset Fx^k \subset U$$

Since $e \in F$ it follows in particular from (12) that

$$x^{nk} \in U$$

Thus the sequence

$$x^k, x^{2k}, \dots, x^{nk}, \dots \quad (13)$$

must possess a limit element c in the compact set \bar{U} . Moreover c cannot be different from zero. Indeed if $c \neq 0$ then, since every neighborhood of c contains arbitrarily large powers x^{nk} of x^k and since division is continuous in K , it would follow that every neighborhood of the unit e also contained arbitrarily large powers x^{mk} of x^k which is impossible since $x^{mk} \in \bar{U}$ while $e \notin \bar{U}$. Thus (13) can contain no subsequence converging to any element other than zero, and since \bar{U} is compact, it follows that (13) actually converges to zero. But then, multiplying (13) by the powers x, x^2, \dots, x^{k-1} , we conclude that (6) converges to zero also.

Suppose on the other hand that (6) does converge to zero. By Lemma 1 there exists a power x^k satisfying (11) (see (2)). Thus an element x belongs to A when and only when there exists a positive integer k for which (11) holds.

We next show that if (11) holds for some x then it continues to hold for all elements of a suitably chosen neighborhood V of x , thus verifying that A is open. Indeed for every $z \in F$ there exist neighborhoods V'_z of z and V_z of x such that $V'_z V_z^k \subset U$. The covering $\{V'_z\}$, $z \in F$, of the compact set F contains a finite covering $V_{z_1}', \dots, V_{z_m}'$ and we define $V = V_{z_1} \cap \dots \cap V_{z_m}'$. Then $Fy^k \subset U$ clearly holds for every $y \in V$.

Now let t be an arbitrary but fixed element of K distinct from

zero and satisfying the conditions

$$Ft \subset U, tF \subset U \quad (14)$$

It follows from the foregoing that the sequence of positive powers of t converges to zero, and hence by Lemma 1 that the sequence of negative powers contains no convergent subsequence. Thus if a is any non-zero element of K then $a t^n$ belongs to \bar{U} for sufficiently large positive n and does not belong to \bar{U} for sufficiently large negative n , so that for each such $a \neq 0$ there is an integer r such that $a t^n \notin \bar{U}$ for $n < r$ while $a t^r \in \bar{U}$. Thus, writing $r = r(a)$, we have

$$a t^{r(a)} \in \bar{U} \setminus t\bar{U}. \quad (15)$$

In exactly the same manner it may be shown that there exists an integer $s(a)$ satisfying

$$t^{s(a)} a \in \bar{U} \setminus t\bar{U} \quad (16)$$

We next show that if (8) contains no convergent subsequence then (9) converges to zero. It is seen at once that (9) cannot have a limit point distinct from zero. Accordingly it suffices to show that (9) contains a convergent subsequence. Since (8) contains no convergent subsequence it follows that the sequence of integers $r_n = r(a_n)$ becomes infinitely large. If (9) also contained no convergent subsequence it would follow similarly that the sequence $s_n = s(a_n^{-1})$ also became infinitely large. Let

$$b_n = a_n t^{r_n}, \quad c_n = t^{s_n} a_n^{-1}. \quad (17)$$

The sequence b_1, \dots, b_n, \dots belongs to $\bar{U} \setminus t\bar{U}$ and consequently possesses a subsequence converging to some element $b \neq 0$. Dropping down as usual to such a subsequence we suppose without loss of generality that b_1, \dots, b_n, \dots itself converges to $b \neq 0$. Similarly we may suppose that c_1, \dots, c_n, \dots converges to some $c \neq 0$. But then

$$c_n b_n = t^{s_n + r_n}$$

and, letting $n \rightarrow \infty$, we arrive at the contradiction $c b = 0$.

Thus if (8) contains no convergent subsequence then the reciprocal sequence (9) must converge to zero so that $C^{-1} \subset A \setminus 0$, whence the equation $C^{-1} = A \setminus 0$ follows by Lemma 1.

It is now a simple matter to verify that $K = A \cup B \cup C$. Indeed if (6) contains a subsequence converging to zero then there exists a positive power x^k satisfying (11) whence, as we have seen, it follows that $x \in A$. If, on the other hand, (6) contains a subsequence having no limit point then, taking reciprocals, we find that $x^{-1} \in A$, and hence $x \in C$. Thus if x belongs neither to A

nor to C it must belong to B.

Finally, since $A \setminus 0$ is open it follows that $C = (A \setminus 0)^{-1}$ is also open and, since A, B, C are pairwise disjoint, this shows that B is closed. Thus the proof of the lemma will be complete if we can show $A \cup B$ to be countably compact. Suppose the contrary, i.e., that $A \cup B$ contains a sequence (8) having no limit points. Then the reciprocal sequence (9) converges to zero and there exists an element a_n^{-1} belonging to A. But then a_n must belong to C which contradicts the assumption $a_n \in A \cup B$. Thus Lemma 2 is proved.

B) Let L be a topological division ring admitting continuous closure (see Section 25, D)) and let A denote the set of those elements x for which the sequence of powers $x, x^2, \dots, x^n, \dots$ converges to zero. It follows from Lemma 2 that A is an open set about zero in L; we shall call A the principal neighborhood of L. It turns out that the topology of a topological division ring admitting continuous closure is uniquely determined by its principal neighborhood. More precisely: let L and L' be two topological division rings admitting continuous closure, let A and A' denote their principal neighborhoods, and let f be an isomorphism of the algebraic division ring L onto the algebraic division ring L' satisfying $f(A) = A'$. Then f is necessarily a homeomorphism and is therefore an isomorphism of the topological division ring L onto the topological division ring L'.

Let c be any element of A so that $c, c^2, \dots, c^n, \dots$ converges to zero. Since L may be considered as a subring of a continuous division ring K it follows from Lemmas 1 and 2 that the sequence $Ac, Ac^2, \dots, Ac^n, \dots$ is a complete system of neighborhoods of zero in L. Let now $c' = f(c)$. Then $c' \in A'$ so that $c', c'^2, \dots, c'^n, \dots$ also converges to zero and the sequence $A'c', A'c'^2, \dots, A'c'^n, \dots$ is again a complete system of neighborhoods of zero, this time in L' . But now $f(Ac^n) = A'c'^n$ so that f is both ways continuous at zero. Since L and L' are, in particular, additive topological groups and f is an algebraic isomorphism it follows from A) Section 20 that f is, in fact, homeomorphic.

C) Denote by P^0 the topological field of rational numbers in its topology as a subspace of the field of real numbers and denote by R_0^p the topological field of rational numbers in the p-adic topology (see Section 26, C)). Denote also by R_t^p the topological field of rational functions in the indeterminate t over the field P^p of residue classes modulo p in the topology introduced in Section 26, C). All three of the fields P^0 , R_0^p , R_t^p admit continuous

closure, and the following may be immediately verified: a) the principal neighborhood of P^0 consists of all rational numbers r satisfying the condition $|r| < 1$; b) the principal neighborhood of $R_0 P$ consists of those rational numbers r of the form $r = \frac{ap}{b}$

where a is an integer and b is a positive integer relatively prime to p ; c) the principal neighborhood of $R_t P$ consists of those rational functions r of the form $\frac{at}{b}$ where a is an arbitrary polynomial in $R_t P$ while b is a polynomial in $R_t P$ not divisible by t .

D) Let A , B , and C be the subsets of a continuous division ring K defined in Lemma 2 and let x and y be two commuting elements of K . The following are all immediate consequences of the definitions of A , B , C :

$$\text{if } x \in A, y \in A \text{ then } xy \in A \quad (18)$$

$$\text{if } x \in A, y \in B \text{ then } xy \in A \quad (19)$$

$$\text{if } x \in B, y \in B \text{ then } xy \in B, y^{-1} \in B \quad (20)$$

$$\text{if } x \in C, y \in B \text{ then } xy \in C \quad (21)$$

$$\text{if } x \in C, y \in C \text{ then } xy \in C \quad (22)$$

Lemma 3: A connected continuous division ring K has characteristic 0 and the closure $\overline{P^0}$ of the prime subfield P^0 is isomorphic with the field of real numbers.

Proof: Let A , B , C be the sets defined in Lemma 2 and let

$$A_n = nA = A + A + \dots + A, \quad n = 1, 2, \dots \quad (23)$$

Since A is an open set it follows that A_n is also open. Moreover, since A is compact, so is \overline{A}_n and

$$n\overline{A} = \overline{A}_n. \quad (24)$$

Finally, since the whole division ring K is not compact but is connected the boundary \dot{A}_n of the open set A_n , defined as

$$\dot{A}_n = \overline{A}_n \setminus A_n, \quad (25)$$

cannot be empty. From the definition of A_n and from (24) we clearly have

$$A_m + A_n = A_{m+n}, \quad (26)$$

$$\overline{A}_m + \overline{A}_n = \overline{A}_{m+n} \quad (27)$$

We shall show that, in fact,

$$\overline{A_m} + A_n = A_{m+n}. \quad (28)$$

Indeed, Let $x \in \overline{A_m}$, $y \in A_n$ and let V be a neighborhood of zero such that $y - V \subset A_n$. Since $x \in \overline{A_m}$ it follows that V contains an element v such that $x + v \in A_m$ whence $x + y = (x + v) + (y - v) \in A_m + A_n = A_{m+n}$.

We show next that for every positive integer $m \geq 2$ there exists an element $w_m \in \overline{A}$ satisfying the condition

$$m w_m \in K \setminus \overline{A}_{m-1}. \quad (29)$$

Let U be a neighborhood of zero so small that

$$m U \subset A. \quad (30)$$

and select from the covering $a + U$, $a \in A$ of the compact set A , a finite covering $a_1 + U, \dots, a_k + U$. Let also $n = k m$ and let $z \in \dot{A}_n$. Then

$$z = x_1 + x_2 + \dots + x_n; \quad x_j \in \overline{A}, \quad j = 1, \dots, n. \quad (31)$$

Since there are $n = k m$ of the elements x_j and only k of the covering sets $a_i + U$ it follows that among the covering sets there must be at least one say $a_1 + U$, containing at least m of the elements x_j , $j = 1, \dots, n$; reenumerating if necessary we may suppose that the elements x_1, \dots, x_m all belong to $a_1 + U$. From the relations

$$\begin{aligned} z &= x_1 + \dots + x_m \in \overline{A}_m, \\ y &= x_{m+1} + \dots + x_n \in \overline{A}_{n-m}, \\ x + y &= z \in A_n \end{aligned}$$

and from (28) it follows that

$$x \in \dot{A}_m. \quad (32)$$

Moreover we have $x_i = a_1 + u_i$, $u_i \in U$, $i = 1, \dots, m$. Thus

$$ma_1 + u \in \dot{A}_m. \quad (33)$$

where $u = u_1 + \dots + u_m$, $u_i \in U$, so that

$$u \in A. \quad (34)$$

Employing (28) once again we see that (29) is satisfied for $w_m = a_1$.

It is now easy to see that K has characteristic 0. Indeed (29) implies that $m\omega = m\omega_m \neq 0$ so that, in particular, $m \neq 0$ for every $m \geq 2$. Thus the prime subfield P^0 of K consists of all elements of the form $r e$ where r is a rational number. It remains to show that the closure P^0 is isomorphic with the field of real numbers.

According to B) it suffices to show that the principal neighborhood of P^0 consists of all elements of the form $r e$ where $|r| < 1$. Let m and n be positive integers; we shall show that if $m > n$ then

$$\frac{m}{n} e \in C \quad (35)$$

Suppose on the contrary $\frac{m}{n} e \notin A \cup B$. Since $\frac{m}{n} e$ commutes with every element of A it follows from D) that $A \cdot \frac{m}{n} e \subset A$ and hence that $\bar{A} \cdot \frac{m}{n} e \subset \bar{A}$. Thus we obtain

$$\omega_m \circ \frac{m}{n} e \in \bar{A}. \quad (36)$$

or, multiplying by n ,

$$m \omega_m \epsilon \bar{A}_n,$$

which contradicts (29) since $\bar{A}_n \subset \bar{A}_{m-1}$. Thus (35) holds, whence it follows by Lemma 2 that $r e$ belongs to A when and only when $|r| < 1$.

Lemma 4: If a totally disconnected continuous division ring K has characteristic 0 then the closure $K_0^p = \overline{P^0}$ of its prime subfield P^0 is isomorphic with the field of p -adic numbers, the prime p being uniquely determined by K .

Proof: Let A , B , C be as defined in Lemma 2 and let G be compact open subgroup of the additive topological group K contained in the open set A (See Theorem 16). Denote also by Z the ring of all integral multiples of the unit e . If $a \in G$, $a \neq 0$, then, since G is a subgroup, $ma = (m e) a$ belongs to G for every integer m . In other words, Za is contained in G , or, equivalently, Z is a subset of Ga^{-1} . Now if Z contained an element of C , the powers of that element would also lie in Z and would constitute a sequence without limit points lying in the compact set $G a^{-1}$ which is impossible. Thus we see that

$$Z \subset A \cup B. \quad (37)$$

We next show that there exists a unique prime p such that

$$pe \in A. \quad (38)$$

To begin with, since $A \cup B$ is compact it follows from (37) that Z has limit points and hence, since Z is an additive group, that zero is a limit point of Z . Thus $A \cap Z$ contains elements other than zero so that $m e \in A$ for at least one positive integer m . Let

$m = m_1 m_2$ be a factorization of m into factors distinct from one. Then $m_1 e$ and $m_2 e$ belong to $A \cup B$ by (37) while their product $m e$ belongs to A and it follows from (20) that at least one of the factors $m_1 e$ and $m_2 e$ must also belong to A . A finite number of repetitions of this argument shows that there exists a prime p satisfying (38). Suppose, now, there is a prime $q \neq p$ such that $qe \in A$. Since pe and qe are in A there exists a positive integer n so large that $p^n e$ and $q^n e$ both belong to the neighborhood G . But then, being an additive group, G must also contain all elements of the form

$$\mu p^n e + \nu q^n e,$$

where μ and ν are arbitrary whole numbers. Choosing μ and ν such that $\mu p^n + \nu q^n = 1$, which is possible since p^n and q^n are relatively prime, we arrive at the contradiction $e \in G \subset A$. Thus there is one and only one prime p satisfying (38).

From (37) along with (18), (19), (20) it follows that the element $m e$ of the ring Z belongs to A when and only when m is divisible by p . Further recourse to the relations of D) shows that the element $\frac{cp^k}{d} e$, where c and d are integers relatively prime to p , belongs to A when $k > 0$, to B when $k = 0$, and to C when $k < 0$. Thus the principal neighborhood $A \cap P^0$ of the topological field P^0 consists precisely of the elements of the form $\frac{ap}{b} e$ where a and $b > 0$ are integers with b relatively prime to p . But from this it follows by proposition C) that the closure $\overline{P^0}$ of the prime subfield P^0 is isomorphic with the field of p -adic numbers and Lemma 4 is proved.

Lemma 5: If K is a continuous division ring with characteristic $p \neq 0$ then every non-zero element $t \in A$ is transcendental over the prime subfield P^p and the closure K_t^p of the field $P^p(t)$ is isomorphic with the field of formal power series over P^p (see Section 26, C)).

Proof: The argument is similar to that of Lemma 4. Since a connected division ring has characteristic 0 by Lemma 3 it follows from A) that K is totally disconnected, and hence by Theorem 16 that there exists a compact open subgroup G of the additive group of K contained in the open set A .

We begin by observing that if ξ and η are elements of any field of characteristic $p \neq 0$ then

$$(\xi + \eta)^p = \xi^p + \eta^p. \quad (39)$$

That this is so may be seen by expanding the left side according to Newton's formula and observing that all of the coefficients that appear, except the first and the last, are divisible by p . Next, raising (39) repeatedly to the p -th power we obtain

$$(\xi + \eta)^{p^l} = \xi^{p^l} + \eta^{p^l}. \quad (40)$$

Moreover if ξ, η, ζ are three elements then it follows from (40)

$$(\xi + \eta + \zeta)^{p^l} = \xi^{p^l} + \eta^{p^l} + \zeta^{p^l}. \quad (41)$$

and analogously for an arbitrary finite number of elements

Now let t be an arbitrary but fixed non-zero element of A and denote by $P^p[t]$ the ring of polynomials in t with coefficients in P^p . We shall show that

$$P^p[t] \subset A \cup B. \quad (42)$$

and also that, if $\varphi(x) \in P^p[x]$ is an arbitrary polynomial in the indeterminant x with coefficients in P^p , then $\varphi(t)$ belongs to A when and only when $\varphi(x)$ has zero constant term or, in other words, when $\varphi(x)$ is divisible by x . From these two facts it follows, in particular, that $\varphi(t) = 0$ when and only when $\varphi(x) = 0$, i. e., that t is transcendental over P^p .

Let k be a positive integer so large that

$$t^n \in G \quad \text{for } n \geq p^k. \quad (43)$$

Since G is an additive group it follows from (43) that G contains every element $\psi(t)$ where $\psi(x)$ is a polynomial divisible by x^{p^k} . Hence if $\varphi(x)$ is divisible by x then $[\varphi(t)]^{p^k} \in G \subset A$, whence it follows, as we have seen, that $\varphi(t)$ also belongs to A . If we suppose, on the other hand, that $\varphi(x)$ has constant term different from zero then for $l \geq k$ we have

$$[\varphi(x)]^{p^l} = a + \psi(x)$$

where $a \in P^p$, $a \neq 0$, while $\psi(x)$ is divisible by x^{p^k} (see (39)) so that $\psi(t) \in G$. Moreover $a \in B$ so that $[\varphi(t)]^{p^l} \in B + G$ for all sufficiently large l . Since $B + G$ is compact it follows that $(t) \notin C$ and hence that $\varphi(t) \in A \cup B$. But, finally, if we assume $\varphi(t) \in A$ then, for sufficiently large l , we obtain $[\varphi(t)]^{p^l} \in G$ and therefore $a = [\varphi(t)]^{p^l} - \psi(t) \in G \subset A$ which is impossible. Thus we see that $\varphi(t) \in A \cup B$ in any case, while $\varphi(t) \in A$ when and only when $\varphi(x)$ is divisible by x .

Consider now an element $\frac{c(t)t^n}{d(t)}$ of the field $P^p(t)$ where $c(x)$ and $d(x)$ are polynomials not divisible by x . Since, as has been

shown, $\frac{c(t)}{d(t)} \in B$, the element $\frac{c(t)t^n}{d(t)}$ belongs to A when $n > 0$, to B when $n = 0$ and to C when $n < 0$. Thus the principal neighborhood $A \cap P^p(t)$ of the topological field $P^p(t)$ consists of those elements of the form $\frac{a(t)t}{b(t)}$ where $a(x), b(x)$ are polynomials over P^p with $b(x)$ not divisible by x . It now follows from C) just as in Lemma 4 that the closure $\bar{P}^p(t)$ of $P^p(t)$ is isomorphic with the field of formal power series with coefficients in P^p introduced in Section 26, C), and Lemma 5 is proved.

Proof of Theorem 22: The immediately preceding Lemmas 3, 4, 5 show that, in fact, one and only one of the three possibilities listed in Theorem 22 must hold for any continuous division ring K . Thus it only remains for us to prove the last part of the theorem, i.e., that K is a finite extension of K^* .

Let E denote the set consisting of the two elements $0, e$ and choose in K^* an element $u \in A$, $u \neq 0$, such that all the series

$$\varepsilon_0 + \varepsilon_1 u + \varepsilon_2 u^2 + \dots + \varepsilon_n u^n + \dots \quad (44)$$

with coefficients in E are convergent. That it is always possible to find such an element may be seen by considering the various cases. Indeed, in case 1) we may choose $u = \frac{1}{2}e$; in case 2) we may choose $u = p e$; finally in case 3) it suffices to choose $u = t$. We next select a finite system

$$v_1, \dots, v_m \quad (45)$$

of elements of the set \bar{A} in such a way that for every $z \in \bar{A}$ there exists a linear form

$$\varepsilon_1 v_1 + \dots + \varepsilon_m v_m$$

with coefficients in E satisfying the condition

$$z - \varepsilon_1 v_1 - \dots - \varepsilon_m v_m \in uA. \quad (46)$$

In order to construct such a system, consider the open covering of the compact set \bar{A} consisting of sets of the form $v + uA$, $v \in \bar{A}$, and select a finite covering $v_1 + uA, \dots, v_m + uA$; it is then clear that for any element $z \in \bar{A}$ there exists some v_i such that $z - v_i \in uA$, i.e., that (46) is satisfied.

We shall now show that every element $z \in K$ may be written in the form

$$z = a_1 v_1 + \dots + a_m v_m. \quad (47)$$

where the coefficients a_1, \dots, a_m belong to the subfield K^* , reserving for later the question of the uniqueness of the representation.

Since for any $z \in K$ there exists a positive integer n sufficiently large so that $u^n z \in \bar{A}$, it suffices to obtain a resolution (47) when $z \in \bar{A}$. Let $z_0 \in \bar{A}$ and let $\epsilon_{01}v_1 + \dots + \epsilon_{0m}v_m$ be a linear form with coefficients in E such that

$$z_0 - \epsilon_{01}v_1 - \dots - \epsilon_{0m}v_m \in uA$$

as in (46); then

$$z_0 = \epsilon_{01}v_1 + \dots + \epsilon_{0m}v_m + uz_1, \quad (48)$$

where z_1 is again an element of \bar{A} . Starting from z_1 and repeating the construction we obtain

$$z_1 = \epsilon_{11}v_1 + \dots + \epsilon_{1m}v_m + uz_2, \quad z_2 \in \bar{A}. \quad (49)$$

Continuing this process inductively we find

$$z_n = \epsilon_{n1}v_1 + \dots + \epsilon_{nm}v_m + uz_{n+1}; z_{n+1} \in \bar{A}, n = 0, 1, \dots, \quad (50)$$

whence it follows that

$$z_0 = \sum_{i=1}^m (\epsilon_{0i} + \epsilon_{1i}u + \epsilon_{2i}u^2 + \dots + \epsilon_{ni}u^n)v_i + u^{n+1}z_{n+1}; \\ z^{n+1} \in \bar{A}. \quad (51)$$

Letting $m \rightarrow \infty$ in this last relation we obtain

$$z_0 = a_1v_1 + \dots + a_mv_m$$

where a_1, \dots, a_m are elements of K^* .

Finally if the elements v_1, \dots, v_m are linearly dependent over K^* , i. e., if an equation

$$b_1v_1 + \dots + b_mv_m = 0$$

holds, where the coefficients b_i are elements of K^* , and not all are equal to 0, then the equation may be solved for some one of the elements v_i , $i = 1, \dots, m$ and the system v_1, \dots, v_m replaced by a system with one fewer element. Continuing this process as long as possible, we arrive finally at an linearly independent basis x_1, \dots, x_r . Moreover it is easy to arrange matters so that $x_1 = e$. Thus the proof of Theorem 22 is complete.

Example 48: Let K be a topological division ring, let R^{n+1} be the vector space of dimension $n+1$ over K , and let $P^n = \{G_0, G_1, \dots, G_n\}$ denote the associated projective geometry over K (see Section 7, K), L)). The vector space R^{n+1} is, in a natural fashion, the direct sum of $n+1$ copies of the additive topological group K and thus acquires a natural topology. We proceed to topologize the sets G_k , $0 \leq k \leq n$. Let a be an element of G_k , i. e.,

a $(k+1)$ -dimensional linear subspace of R^{n+1} and let u_1, \dots, u_{k+1} be a basis in a. We choose neighborhoods U_1, \dots, U_{k+1} of the vectors u_1, \dots, u_{k+1} in the space R^{n+1} such that a system of vectors v_1, \dots, v_{k+1} is linearly independent whenever $v_i \in U_i$ and then define the neighborhood V of a in the space G_k to consist of the collection of all elements $x \in G_k$ having bases v_1, \dots, v_{k+1} with $v_i \in U_i$. It may be verified that this definition turns G_k into a topological space. Clearly if the points a_0, a_1, \dots, a_k are linearly independent then the plane $a \in G_k$ of dimension k passing through them is a continuous function of them. Using the results of the present paragraph it may be shown that, if the division ring K is continuous, then each of the spaces G_k is compact. Moreover, if K is totally disconnected then each of the spaces G_k is also totally disconnected. Thus we arrive at the projective geometry $P^n = \{G_0, G_1, \dots, G_n\}$ over a continuous division ring K where the sets G_0, G_1, \dots, G_n are compact topological spaces satisfying the condition that the operation of passing k -dimensional planes through linearly independent points is continuous.

We next consider the synthetic point of view. A projective geometry $P^n = \{G_0, G_1, \dots, G_n\}$ (see Example 16) will be said to be continuous if the sets G_0 and G_1 of points and lines are infinite compact topological spaces such that the line (x, y) joining two distinct points x, y depends continuously on those points. It turns out that every continuous projective geometry is continuously isomorphic with the projective geometry over some continuous division ring K . Moreover if the space of points G_0 is connected then the corresponding continuous division ring K is also connected, so that in this case K is isomorphic either with the field of real numbers or the field of complex numbers or the division ring of quaternions (see Theorem 21).

We prove only the last assertion. The division ring K is defined in the construction given in Example 16 and since the line (x, y) depends continuously on x and y there is no trouble in defining in K a topology turning it into a topological division ring. From the fact that G_0 is compact it follows that the set of all points lying on any one line l is a compact set. Since K may be obtained by removing from l a single point u , it follows that K is even continuous. Moreover if K is disconnected then it is totally disconnected and consequently G_0 is also totally disconnected; thus the connectedness of K follows from the connectedness of G_0 .

5

LINEAR REPRESENTATIONS OF COMPACT TOPOLOGICAL GROUPS

In the third chapter the general theory of topological groups was developed; there only the most general concepts and relations were considered. We turn now to the problem of making a deeper, constructive investigation of topological groups. Our aim is to connect the general topological group with more concrete objects such as, for instance, groups of matrices and Lie groups (for the latter see Chapters 7 and 10) which are amenable to more direct investigation. Once such connections are established, the possibility is opened of reducing questions bearing on topological groups in general to the corresponding questions bearing on such relatively accessible objects. It will be found that topological groups of a quite general character can be constructed from such concrete examples. The basic technique in the program here outlined is the method of linear representations.

A linear representation of a topological group G is any homomorphism of G into the topological group of non-singular matrices of some finite order. Now it is clear that every group admits the trivial linear representation sending every element of the group into the identity element of the matrix group, but this trivial representation can give no assistance in the investigation of the group. Thus there arises the question of the existence of non-trivial linear representations. Even more far reaching is the question of the existence of an adequate system of linear representations.

The group G is said to admit an adequate system of linear representations if for every element g of the group G different from the identity there exists a linear representation of G which does not carry g into the identity matrix. The question of the existence of an adequate system of linear representations for a locally

compact topological group has been answered in the negative in the general case [5]. It is possible, however, to construct an adequate system of linear representations for every compact topological group and the present chapter is devoted to the development of this construction. Some applications will be given in the sixth and eighth chapters where, upon the basis of the existence of an adequate system of representations for compact groups, it will be possible to solve certain central problems in the general theory of topological groups.

The first step in the construction is the definition in the group of an invariant measure or, what comes to the same thing, an invariant integral. To every set M belonging to a sufficiently wide class of measurable subsets of G there is assigned, as its measure, a certain non-negative number in such a way that the condition of invariance is satisfied, i. e., the measure of M is equal to the measure of Ma for every element a of G . Once an invariant measure is defined in G it is possible to define an invariant integral. An invariant measure on an arbitrary locally compact separable topological group was first constructed by Haar (see [16]). A little later, von Neumann (see [38]) gave a direct definition of the invariant integral on a separable compact group and this definition generalizes automatically to the general compact group. Since the construction of von Neumann is markedly simpler than that of Haar and since, in the sequel, we shall have need of the invariant integral only in the compact case, I shall here follow von Neumann.

Even before the construction of an invariant integral on an arbitrary compact topological group, it had been employed by Peter and Weyl (see [41]) for the construction of an adequate system of linear representations of compact Lie groups; on these groups the invariant integral may be defined in a direct and simple fashion. Peter and Weyl based their work on the study of certain integral equations on the group; in so doing they made essential use of its compactness. Once it was known that an invariant integral exists on an arbitrary compact group, their construction automatically generalized to the general compact case. To extend it to locally compact groups, even in the separable case, is impossible.

SECTION 28 CONTINUOUS FUNCTIONS ON A TOPOLOGICAL GROUP

Since a topological group is, in particular, a topological space, it makes sense to speak of continuous functions defined on G (see

Section 12, A)). The fact that G is also a group makes it possible to formulate the definition of continuity in a slightly different way and also, what is much more important, to introduce a concept of uniform continuity.

A) Let G be a topological group and let M be an arbitrary subset of G . A numerical function f defined on the subspace M is continuous at the point $a \in M$ when and only when, for an arbitrary positive number ϵ , there exists a neighborhood V of the identity such that for $x \in M$, $xa^{-1} \in V$ we have $|f(x) - f(a)| < \epsilon$.

To prove the assertion it suffices to observe that xa^{-1} belongs to V when and only when x belongs to the neighborhood $U = Va$ of the point a .

B) Let M be an arbitrary subspace of a topological group G and let f be a numerical valued function defined on M . Then f is said to be uniformly continuous if for arbitrary positive ϵ there exists a neighborhood V of the identity $e \in G$ such that for $x, y^{-1} \in V$, $x \in M$, $y \in M$ we have $|f(x) - f(y)| < \epsilon$. Along with this definition of uniform continuity it is possible to give another, slightly different but fully analogous, definition saying that the function f is uniformly continuous if for arbitrary positive ϵ there exists a neighborhood V' of e such that $|f(x) - f(y)| < \epsilon$ whenever $x^{-1} y \in V'$. The two definitions of uniform continuity here formulated are, generally speaking, not equivalent. However they do turn out to be equivalent in all the cases that are of interest to us (see C)). Note that a function that is uniformly continuous in either sense is automatically continuous.

It turns out that in certain important cases the simple continuity of a function implies its uniform continuity.

C) Let G be a topological group and let M be a compact subset of G . Then a continuous function f defined on M is automatically uniformly continuous in both of the above senses.

Indeed let ϵ be any positive number. Since f is continuous there exists for each point $a \in M$, a neighborhood V_a of e such that if $xa^{-1} \in V_a$ and $x \in M$, then $|f(x) - f(a)| < \epsilon/2$. Let W_a be a neighborhood of e such that $W_a^2 \subset V_a$. Clearly the collection of open sets W_{a_i} , $a_i \in M$, covers M and since M is compact it is possible to select a finite covering. Thus there exists the finite system a_1, \dots, a_n of points of M such that the open sets W_{a_i} , $i = 1, \dots, n$, covers M . Denote by V the intersection of the neighborhoods W_{a_i} . We shall show that if $xy^{-1} \in V$, $x \in M$, $y \in M$ then $|f(x) - f(y)| < \epsilon$, i.e., that f is uniformly continuous in the sense

of the first of the above definitions. Indeed, since the sets $W_{a_1}a_1$ cover M , there exists a number k such that $ya_k^{-1} \in W_{a_k}$ and consequently $|f(y) - f(a_k)| < \epsilon/2$. Moreover, we have

$$xa_k^{-1} = xy^{-1}y a_k^{-1} \in VW_{a_k} \subset W_{a_k}^2 \subset V_{a_k}$$

so that $|f(x) - f(y)| < \epsilon$.

Along with the concept of uniform continuity of a single function an essential role will be played in the sequel by the concept of the uniform equi-continuity of a family of functions.

D) Let M be an arbitrary subspace of a topological group G . A set Δ of functions defined on M is said to be uniformly equicontinuous if for arbitrary positive ϵ there exists a neighborhood V of the identity in G such that for $x, y \in M$, $y \in V$, $x \in M$ we have $|f(x) - f(y)| < \epsilon$ for every function f belonging to Δ . Clearly every function belonging to a uniformly equicontinuous family of functions is itself uniformly continuous. The set Δ is also said to be uniformly bounded if there exists a number m such that for $x \in M$, $f \in \Delta$, we have $|f(x)| < m$.

We now recall the concept of a uniformly convergent sequence of functions.

E) A sequence of functions f_n , $n = 1, 2, \dots$, defined on a set M is said to be uniformly convergent to the function f (also defined on M) if for every positive number ϵ there exists an integer m such that for $n > m$ we have $|f(x) - f_n(x)| < \epsilon$ for arbitrary $x \in M$.

Exactly as in classical analysis it may be shown that a necessary and sufficient condition that a sequence f_n of functions converge uniformly (to some limit function f) is the following Cauchy criterion of uniform convergence.

F) The sequence of functions f_n , $n = 1, 2, \dots$, defined on a set M is uniformly convergent when and only when for arbitrary positive number ϵ there exists a positive integer m such that for $p > m$, $q > m$ we have $|f_p(x) - f_q(x)| < \epsilon$ for arbitrary $x \in M$.

G) If a sequence of continuous functions converges uniformly then the limit function is itself continuous. This assertion may be proved exactly as in classical analysis.

H) A uniformly convergent sequence f_1, f_2, \dots of continuous functions defined on an arbitrary compact subspace M of a topological group G is automatically uniformly equicontinuous and

uniformly bounded.

Indeed let f be the limit function. Since f is continuous it is uniformly continuous; hence for given ϵ there exists a neighborhood V of e such that for $x \in M$, $y \in M$, $xy^{-1} \in V$ we have $|f(x) - f_n(y)| < \epsilon/3$. On the other hand there also exists a positive integer p such that for $n > p$ we have $|f(x) - f_n(x)| < \epsilon/3$, $|f(y) - f_n(y)| < \epsilon/3$. Combining these three inequalities we find that for $x \in M$, $y \in M$, $xy^{-1} \in V$ and $n > p$ we have $|f_n(x) - f_n(y)| < \epsilon$. Denote now by V_i , $i = 1, \dots, p$ a neighborhood of e such that for $x \in M$, $y \in M$, $xy^{-1} \in V_i$, we have $|f_i(x) - f_i(y)| < \epsilon$. Denoting by U the intersection of the neighborhoods V , V_1, \dots, V_p we see that for $x \in M$, $y \in M$, $xy^{-1} \in U$, the inequality $|f_n(x) - f_n(y)| < \epsilon$ is satisfied for $n = 1, 2, \dots$. Accordingly the sequence f_1, f_2, \dots is uniformly equicontinuous. Uniform boundedness follows from the fact that the functions f, f_1, \dots, f_p are bounded (see Section 13, G) while, for $n > p$, we have $|f_n(x)| < |f(x)| + (\epsilon/3)$.

By way of converse to the last proposition we now prove the following important theorem.

Theorem 23: Let G be a topological group, M a compact subset of G , and let Δ be a uniformly bounded and uniformly equicontinuous set of real functions defined on M . Then any sequence of functions belonging to Δ contains a uniformly convergent subsequence.

Proof: Let ϵ be a positive number and denote by V_ϵ a neighborhood of the identity in G such that

$$\text{for } x \in M, y \in M, xy^{-1} \in V_\epsilon, f \in \Delta \text{ we have } |f(x) - f(y)| < \epsilon. \quad (1)$$

Let also Δ' be an arbitrary infinite subset of Δ and let $a \in M$. Then there exists an infinite subset Δ'_a of the set Δ' such that

$$\text{for } x \in M, x \in V_\epsilon a, f, g \in \Delta'_a \text{ we have } |f(x) - g(x)| < 3\epsilon. \quad (2)$$

Indeed, since Δ is uniformly bounded the values of all the functions of the family at the point a are distributed on a bounded interval of the real numbers and consequently there exists a subinterval I of that interval having length ϵ such that the values at the point a of all the functions of some infinite subset Δ'_a of Δ' all belong to I . Accordingly

$$\text{for } f \in \Delta'_a, g \in \Delta'_a \text{ we have } |f(a) - g(a)| < \epsilon. \quad (3)$$

Moreover, by virtue of (1),

$$\text{for } x \in M, x \in V_\epsilon a, f \in \Delta'_a, g \in \Delta'_a$$

we have $|f(x) - f(a)| < \varepsilon$, $|g(x) - g(a)| < \varepsilon$. (4)

and (2) is a consequence of (3) and (4).

We next strengthen the last assertion by eliminating from (2) the requirement $x \in V_\varepsilon a$. Denote once more by ε an arbitrary positive number and by Δ' any infinite subset of Δ . Then there exists an infinite subset Δ'' of the set Δ' such that

for $x \in M$, $f \in \Delta''_x$, $g \in \Delta''_x$ we have $|f(x) - g(x)| < 3\varepsilon$. (5)

Indeed, the collection of neighborhoods of the form $V_\varepsilon a$ (see Section (1)), $a \in M$, where V_ε denotes a fixed neighborhood of e , covers M and since the latter is compact we may select a finite covering $V_\varepsilon a_1, \dots, V_\varepsilon a_r$. By what has just been shown there exists an infinite subset Δ'_{a_1} of Δ' satisfying condition (2) for $a = a_1$. In exactly the same fashion it follows that the set Δ'_{a_1} contains an infinite subset Δ'_{a_1, a_2} satisfying the condition

for $x \in M$, $x \in V_\varepsilon a_2$, $f \in \Delta'_{a_1, a_2}$, $g \in \Delta'_{a_1, a_2}$

we have $|f(x) - g(x)| < 3\varepsilon$.

Continuing in this manner we obtain a set $\Delta'_{a_1, \dots, a_r}$ satisfying condition (5).

Let now

$$f_1, f_2, \dots, f_n, \dots \quad (6)$$

be any sequence of functions belonging to the set Δ , and denote by Δ' the set of functions belonging to the sequence. If Δ' is finite the validity of the assertion is clear. We suppose accordingly that Δ' is infinite. Let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m, \dots$ be a sequence of positive numbers tending to zero. According to what has just been proved it is possible to select from Δ' an infinite subset $\Delta'_{\varepsilon_1} = \Delta'_1$ satisfying condition (5) for $\varepsilon = \varepsilon_1$. For exactly the same reason Δ'_1 contains an infinite subset Δ'_2 satisfying the condition:

for $x \in M$, $f \in \Delta'_2$, $g \in \Delta'_2$ we have $|f(x) - g(x)| < 3\varepsilon_2$.

Continuing in this manner we construct a sequence

$$\Delta'_1 \supset \Delta'_2 \supset \dots \supset \Delta'_n \supset \dots$$

of infinite subsets of Δ' satisfying the condition:

for $x \in M$, $f, g \in \Delta'_n$ we have $|f(x) - g(x)| < 3\varepsilon_n$ (7)

$$n = 1, 2, \dots$$

We now select from Δ'_1 an arbitrary function g_1 ; from Δ'_2 an

arbitrary function g_2 , the index of which in the sequence (6) follows the index of g_1 ; then from Δ'_3 an arbitrary function g_3 , the index of which in (6) follows that of g_2 , etc. The subsequence g_1, g_2, g_3, \dots of (6) is then uniformly convergent by virtue of (7). Thus the theorem is proved.

We remark yet another fact concerning continuous functions.

I) Let M be a compact topological space and let f be a continuous function defined on M . Denote by $K(f)$ the minimum of f and by $L(f)$ its maximum (see Section 13, G)). The number $S(f) = L(f) - K(f)$ is called the oscillation of f . If a sequence of continuous functions f_1, f_2, \dots converges uniformly to f then the following are easily verified:

$$\lim_{n \rightarrow \infty} K(f_n) = K(f), \quad \lim_{n \rightarrow \infty} L(f_n) = L(f), \quad \lim_{n \rightarrow \infty} S(f_n) = S(f).$$

Example 49: Let G be a compact topological group and consider the set R of all continuous functions on G . There is a natural way of defining a metric in R . Indeed if f and g are two continuous functions on G we define the distance between them to be the maximum of the function $|f(x) - g(x)|$ for $x \in G$.

It is easy to show that with this definition R becomes a metric space (see Example 20). In the first place the maximum of $|f(x) - g(x)|$ is equal to zero when and only when $f = g$. Moreover if f, g and h are three elements of R then the triangle inequality follows from the inequality

$$|f(x) - h(x)| \leq |f(x) - g(x)| + |g(x) - h(x)|,$$

valid for every $x \in G$.

The concept of uniform convergence of a sequence of functions f_n , $n = 1, 2, \dots$ may be formulated very simply in terms of the metric on R . Indeed, a sequence of continuous functions converges uniformly to the continuous limit f if and only if the sequence f_n converges to f in the sense of the metric just defined in R .

Let Δ be a uniformly bounded, uniformly equicontinuous family of functions defined on G . Then $\Delta \subset R$. The content of Theorem 23 may be formulated by saying that the closure $\bar{\Delta}$ of the set Δ is compact in the space R .

Example 50: If G denotes the additive topological group of real numbers and M a closed interval in G , then the propositions introduced in this paragraph all reduce to well known facts in classical analysis.

SECTION 29. INVARIANT INTEGRATION

In this paragraph, following von Neumann, I construct an invariant integral on a compact topological group.

Definition 33: If G is a compact topological group then we will say that an invariant integral is defined on G if to every continuous real function f defined on G there is associated a real number, denoted by $\int f(x) dx$ and called the integral of f over G , such that the following conditions are satisfied:

- 1) If α is a real number then

$$\int \alpha f(x) dx = \alpha \int f(x) dx;$$

- 2) If f and g are two continuous functions then

$$\int (f(x) + g(x)) dx = \int f(x) dx + \int g(x) dx;$$

- 3) If the function f is everywhere non-negative then

$$\int f(x) dx \geq 0;$$

- 4) If $f(x) = 1$ for every x then $\int f(x) dx = 1$;

5) If the function f is everywhere non-negative and not identically zero then $\int f(x) dx > 0$;

- 6) If a is an arbitrary element of G then

$$\int f(ax) dx = \int f(x) dx;$$

- 7) If a is an arbitrary element of G then

$$\int f(ax) dx = \int f(x) dx;$$

- 8) $\int f(x^{-1}) dx = \int f(x) dx.$

Of these eight requirements the first five are natural for any concept of integral; the last three express the special group property of invariance.

Observe that conditions 1), 2), 3) permit the integration of inequalities and make it possible to obtain the usual estimate concerning the integral of absolute values, namely, if $f(x) \leq g(x)$ then

$$\int f(x) dx \leq \int g(x) dx, \quad \left| \int f(x) dx \right| \leq \int |f(x)| dx.$$

Indeed $g(x) - f(x) \geq 0$ so that by 4) we have $\int (g(x) - f(x)) dx \geq 0$, whence by 1) and 2) it follows that $\int g(x) dx - \int f(x) dx \geq 0$, i.e.

$$\int f(x) dx \leq \int g(x) dx.$$

Moreover - $|f(x)| \leq f(x) \leq |f(x)|$ whence, by what has just been shown, it follows that $\int |f(x)| dx \leq \int f(x) dx \leq \int |f(x)| dx$, and this inequality may be reformulated as

$$\left| \int f(x) dx \right| \leq \int |f(x)| dx.$$

Theorem 24: On any compact topological group G it is possible to define an invariant integral in one and only one way. If, moreover, there is given on G any integral satisfying conditions 1) - 4) and 6) then the remaining conditions 5), 7) and 8) hold automatically.

The proof of Theorem 24 is not simple and falls naturally into a sequence of steps. We give these steps in the form of preliminary remarks and designate only the last part as the proof of the theorem. Throughout the proof G will denote a compact topological group.

A) Let f be a continuous function defined on G and let $A = \{a_1, \dots, a_m\}$ be a finite sequence of elements belonging to G . (The sequence A may have repetitions.) We introduce the following notation:

$$M(A, f; x) = \sum_{i=1}^m \frac{f(xa_i)}{m}. \quad (1)$$

The function $M(A, f)$ of the argument $x \in G$ defined by (1) is continuous; it constitutes the foundation of the definition of the invariant integral. The following three properties of this function are easily verified.

$$K(M(A, f)) \geq K(f), \quad (2)$$

$$L(M(A, f)) \geq L(f), \quad (3)$$

$$S(M(A, f)) \geq S(f). \quad (4)$$

It is moreover easy to verify that if $A = \{a_1, \dots, a_m\}$ and $B = \{b_1, \dots, b_n\}$ are two finite sequences of elements in G then

$$M(A, M(B, f)) = M(AB, f), \quad (5)$$

where AB denotes the sequence consisting of the $m n$ elements $a_i b_j$, $i = 1, \dots, m$, $j = 1, \dots, n$.

B) If f is a non-constant continuous function defined on G then G contains a finite system of elements A such that

$$S(M(A, f)) < S(f) \quad (6)$$

Indeed, denote by k and l the minimum and maximum, respectively, of f . Since f is continuous and $k < l$ there exists an open set $U \subset G$ such that for every $x \in U$ the inequality $f(x) \leq h < l$ is satisfied. The collection of open sets of the form Ua_i^{-1} covers G and consequently there exists a finite system $A = \{a_1, \dots, a_m\}$ such that the open sets Ua_i^{-1} , $i = 1, \dots, m$; cover G . We shall show that the function $M(A, f)$ has maximum not exceeding

$$\frac{(m - 1)(l + h)}{m} < h.$$

Indeed for every x we have $f(xa_i) \leq l$, $i = 1, \dots, m$; but also for any element x there is always an integer j such that $x \in Ua_j^{-1}$, i.e., $x a_j \in U$, so that $f(xa_j) \leq h$. Since the minimum of $M(A, f)$ is not less than k the result follows.

C) Let f be a continuous function defined on G . We call a right mean of f any real number p satisfying the following condition: for every positive number ϵ there exists a finite system A of elements belonging to G such that for arbitrary $x \in G$

$$|M(A, f; x) - p| < \epsilon \quad (7)$$

We shall show that for an arbitrary continuous function f defined on G there exists at least one right mean.

Denote by Δ the collection of all functions of the form $M(A, f)$ where f is a fixed continuous function defined on G and A denotes an arbitrary finite system of elements belonging to G . From (2) and (3) it follows that the family is uniformly bounded; we shall show that it is also uniformly equicontinuous.

The function f , being continuous, is automatically uniformly continuous (see Section 28, C)); hence for any positive ϵ there exists a neighborhood V of the identity such that for $x, y \in V$ we have $|f(x) - f(y)| < \epsilon$. But if $xy^{-1} \in V$ then also $(xa_i)(ya_i)^{-1} = xy^{-1} \in V$ so that $|f(xa_i) - f(ya_i)| < \epsilon$. Summing this inequality for $i = 1, \dots, m$ and dividing the result by m we obtain $|M(A, f; x) - M(A, f; y)| < \epsilon$. Since this holds for $xy^{-1} \in V$ and for arbitrary A it follows that Δ is uniformly equicontinuous.

Denote now by s the lower bound of the set of all numbers $S(M(A, f))$, i.e., the lower bound of the oscillations of all the functions belonging to Δ . Then there exists a sequence

$$f_1, \dots, f_n, \dots \quad (8)$$

of functions belonging to Δ such that

$$\lim_{n \rightarrow \infty} S(f_n) = s.$$

But also, since Δ is uniformly bounded and equicontinuous, we may, by Theorem 23, select from (8) a uniformly convergent subsequence

$$g_1, \dots, g_n, \dots . \quad (9)$$

If g denotes the limit of this subsequence then $S(g) = s$ (see Section 28, I)). We show first that g is constant or, what comes to the same thing, that $s = 0$.

Suppose the contrary. It then follows from B) that there exists a finite system A of elements belongs to G such that

$$S(M(A, g)) = s' < s. \quad (10)$$

Let $\epsilon = \frac{s - s'}{3}$. Since (9) converges to g uniformly there exists an index k such that $|g(x) - g_k(x)| < \epsilon$. Substituting x a for x in this inequality, summing the inequalities thus obtained over $i = 1, \dots, m$ and dividing the result by m we obtain

$$|M(A, g; x) - M(A, g_k; x)| < \epsilon \quad (11)$$

From (10) and (11) it follows that

$$S(M(A, g_k)) \leq s' + 2\epsilon < s.$$

But now according to (5) the function $M(A, g_k)$ is itself one of the functions belonging to Δ and consequently must have oscillation at least as great as the lower bound s . Thus we have arrived at a contradiction and conclude that g is a constant: $g(x) \equiv p$.

It is now a simple matter to complete the proof of the original assertion. Indeed since (9) converges to g uniformly it follows that for arbitrary positive ϵ there exists an index n such that $|g_n(x) - p| < \epsilon$ for every x . But $g_n \in \Delta$ whence it follows that there exists a finite system A of elements of G such that (7) is satisfied. Consequently p is a right mean of f .

D) By analogy with A) we introduce a new function $M'(B, f)$ of the argument $x \in G$ writing

$$M'(B, f; x) = \sum_{j=1}^n \frac{f(b_j x)}{n}, \quad (12)$$

where

$$B = \{b_1, \dots, b_n\}.$$

It is immediately seen that

$$M(A, M'(B, f)) = M'(B, M(A, f)). \quad (13)$$

E) By analogy with C) we also introduce the notion of a left mean. The real number q will be said to be a left mean of the continuous function f defined on G if it possesses the following property: for every positive ϵ there exists a finite system B of elements of G such that

$$|M'(B, f; x) - q| < \epsilon. \quad (14)$$

Now any continuous function defined on G also possesses at least one left mean. Perhaps the easiest way to see this is to replace the given topological group G by a new group G' having the same elements and topology as those of G but with a new group operation $a \times b$ defined by $a \times b = ba$ where ba denotes the product in the given group G . It is not difficult to verify that with multiplication so defined G' is indeed a topological group and that a right mean for a continuous function defined on G' is a left mean for the same function on the group G ; since the existence of a right mean has already been demonstrated it follows at once that every continuous function also possesses a left mean.

F) For any continuous function f defined on G there exists only one right mean and also only one left mean, and these two numbers coincide. The unique number thus associated with f will be called its mean and denoted by $M(f)$.

Let p be any right mean of the function f and let q be any left mean of the same function. Then for suitable choices of A and B relations (7) and (14) are satisfied. Substituting b, x for x in (7), summing over $j = 1, \dots, n$, and dividing by n we obtain:

$$|M'(B, M(A, f); x) - p| < \epsilon. \quad (15)$$

Again, substituting x_{ai} for x in (14), summing over $i = 1, \dots, m$, and dividing by m we obtain:

$$|M(A, M'(B, f); x) - q| < \epsilon. \quad (16)$$

Taking into account relation (13) we conclude $|p - q| < 2\epsilon$ and since this last inequality holds for arbitrary positive ϵ it follows that $p = q$.

G) Let f and g be two continuous functions defined on G . Then

$$M(f + g) = M(f) + M(g) \quad (17)$$

We begin by showing that

$$M(M(B, f)) = M(f). \quad (18)$$

Let

$$M(f) = p. \quad (19)$$

Then p is, in particular, a left mean for f so that for arbitrary positive ϵ there exists a finite system C of elements of G such that

$$|M'(C, f; x) - p| < \epsilon.$$

Substituting x_B for x in this inequality, summing over $j = 1, \dots, n$ and dividing by n we obtain

$$|M(B, M'(C, f); x) - p| < \epsilon.$$

According to (13) the last relation may be written

$$|M(C, M(B, f); x) - p| < \epsilon.$$

Thus p is also a left mean of the function $M(B, f)$ and (18) follows.

Let now

$$M(g) = q. \quad (20)$$

Then q is, in particular, a right mean for g and consequently for arbitrary positive ϵ there exists a finite system B of elements in G such that

$$|M(B, g; x) - q| < \epsilon.$$

It follows that

$$|M(A', M(B, g); x) - q| < \epsilon,$$

for any finite system of elements A' . Moreover, according to (5) the last inequality may be reformulated as

$$|M(A'B, g; x) - q| < \epsilon. \quad (21)$$

But now, according to (18) and (19), p is a right mean for $M(B, f)$, i.e., there exists a finite system A of elements of G such that

$$|M(A, M(B, f); x) - p| < \epsilon,$$

which may also be rewritten by (5) in the form

$$|M(AB, f; x) - p| < \epsilon. \quad (22)$$

Finally, choosing $A' = A$ in (21) we obtain

$$|M(AB, f + g; x) - (p + q)| < 2\epsilon.$$

Thus $p + q$ is a right mean of the sum $f + g$ and (17) is proved.

H) Let f be a continuous function defined on G and let a be an arbitrary element of G . We define $f'(x) = f(xa)$, $f''(x) = f(ax)$. Then

$$M(f') = M(f), \quad (23)$$

$$M(f'') = M(f). \quad (24)$$

Observe first of all that

$$M(A, f') = M(Aa, f)$$

(see (1)). From this it follows immediately that the right means of the functions f' and f coincide, whence (23) follows. In analogous fashion, using left means instead of right, we obtain (24).

I) Let f be a non-negative continuous function defined on G which is not identically zero. Then

$$M(f) > 0. \quad (25)$$

Indeed, there exists an open set $U \subset G$ such that for $x \in U$ we have $f(x) > h > 0$. The open sets Ua^{-1} cover G and since G is compact there exists a finite system $A = \{a_1, \dots, a_m\}$ such that the open sets Ua_i^{-1} , $i = 1, \dots, m$, cover G . For every x we have $f(x) \geq 0$; moreover for any x there is an index k such that $x \in Ua_k^{-1}$, i.e., $xa_k \in U$, so that $f(xa_k) > h$. Consequently $M(A, f; x) \geq \frac{h}{m}$, whence it follows that $M(f) = M(M(A, f)) \geq \frac{h}{m}$ also.

Proof of Theorem 24. We define the integral $\int f(x) dx$ of an arbitrary continuous function f defined on G by writing

$$\int f(x) dx = M(f) \quad (26)$$

Conditions 1), 3) and 4) of Definition 33 are clearly satisfied, while conditions 2), 5), 6), and 7) have been proved above in propositions G), I) and H).

We show next that an arbitrary integral $\int^* f(x) dx$ satisfying conditions 1)–4) and 6) of Definition 33 must also satisfy

$$\int^* f(x) dx = M(f). \quad (27)$$

Let p be a right mean of the function f so that, for suitably chosen A ,

$$|M(A, f; x) - p| < \epsilon.$$

As has been noted, we need only conditions 1)–4) of Definition 33 in order to integrate this inequality, thus obtaining

$$|\int^* M(A, f; x) dx - p| \leq \epsilon$$

whence, invoking 6), we have

$$|\int^* f(x) dx - p| \leq \epsilon. \quad (28)$$

Since (28) holds for arbitrary positive ϵ it follows that (27) holds also. Thus the uniqueness of the integral satisfying condition 1)–4), 6) of Definition 33 is proved.

It remains only to show that condition 8) is also satisfied. To that end we define on G a new integral $\int^* f(x) dx$, writing

$$\int^* f(x) dx = \int f(x^{-1}) dx. \quad (29)$$

It is not difficult to verify that the integral thus defined also satisfies conditions 1)–4), 6) of Definition 33. For instance, verification of 6) goes as follows:

$$\begin{aligned} \int^* f(xa) dx &= \int f(x^{-1}a) dx = \int f(a^{-1}x)^{-1} dx = \\ &= \int f(x^{-1}) dx = \int^* f(x) dx \end{aligned}$$

(see (24)). By virtue of the uniqueness just established it follows that $\int f(x^{-1}) dx = \int f(x) dx$, which completes the proof of Theorem 24.

In the sequel it will be necessary to integrate not only real but also complex valued functions, i. e., functions of the form $h = f + ig$ where f and g are real functions. Such a function h is continuous if both f and g are continuous and its integral is defined by the equality

$$\int h(x) dx = \int f(x) dx + i \int g(x) dx.$$

It is easy to verify that the integral of a complex function continues to satisfy conditions 1)–8) of Definition 33 where the number a in condition 1) may be allowed to assume complex values. It will also be necessary for us to consider not only single but double integrals. In this connection we need to know that the integral does not depend on the order of integration.

J) Let G and H be compact topological groups and let f be a continuous function of two variables $x \in G$, $y \in H$ (see Section 14, G)). For fixed y the function f is a continuous function of x so that we can form the integral $\int f(x, y) dx = g(y)$. We now show

that the function g is continuous on H .

Denote by P the direct product of the topological groups G and H . (See Definition 28.) The function f may be viewed as a continuous function of the single variable $z = (x, y) \in P$. Since P is compact the function f , being continuous, is automatically uniformly continuous (see Section 28, C)). Accordingly, for arbitrary positive ε there exists a neighborhood W of the identity in P such that for $z' z^{-1} \in W$ we have $|f(z') - f(z)| < \varepsilon$. The neighborhood W consists of all pairs (x, y) such that $x \in U$, $y \in V$, where U and V are neighborhoods of the identity in the groups G and H . Thus if $x'x^{-1} \in U$, $y'y^{-1} \in V$ then $|f(x', y') - f(x, y)| < \varepsilon$. In particular, for $y'y^{-1} \in V$ we have $|f(x, y') - f(x, y)| < \varepsilon$ whence it follows that

$$|g(y') - g(y)| \leq \int |f(x, y') - f(x, y)| dx < \varepsilon,$$

Thus g is uniformly continuous on H .

Theorem 25: Let G and H be compact topological groups and denote by P their direct product. Let f be a continuous function of the two variables $x \in G$ and $y \in H$, $f(x, y) = f(z)$, $z = (x, y) \in P$. Then

$$\begin{aligned} \int (\int f(x, y) dx) dy &= \int (\int f(x, y) dy) dx = \int f(z) dz \\ &= \int f(x, y) dx dy \end{aligned}$$

The iterated integrals in the first and second members of this equation exist since the functions standing under the integral sign are continuous. The last member is to be viewed as defined by the relation itself.

Proof. It suffices to prove the equality $\int (\int f(x, y) dx) dy = \int f(z) dz$. To this end we define $\int^* f(z) dz = \int (\int f(x, y) dx) dy$. It is easy to verify that the integral $\int^* f(z) dz$ thus defined satisfies all conditions of Definition 33. We here verify only condition 6). Let $c \in P$, $c = (a, b)$, $a \in G$, $b \in H$; then

$$\begin{aligned} \int^* f(zc) dz &= \int (\int f(xa, yb) dx) dy = \int (\int f(x, yb) dx) dy \\ &= \int (\int f(x, y) dx) dy = \int^* f(z) dz. \end{aligned}$$

The desired equality now follows from the uniqueness of the invariant integral.

When H coincides with G the function $f(x, y)$ is a continuous function of two variables defined on G . It is in this case that we shall most frequently have occasion to apply the result.

Example 51: Of the group G is finite then the integral of any function defined on the group is simply the arithmetic mean of the various values taken on by the function.

Example 52: Denote by G^* the additive topological group of real numbers and let φ be a continuous periodic function defined on G^* and having period one: $\varphi(x^* + 1) = \varphi(x^*)$. Denote by N the subgroup of G^* consisting of all integers. The periodicity of φ implies that it is constant on the various cosets of the subgroup N and consequently defines a continuous function f on the factor group $G^*/N = G$. Conversely, every continuous function f on G may be obtained in this fashion. Since G is compact there is defined on it an integral $\int f(x) dx$ satisfying the conditions of Definition 33. It is not difficult to see that

$$\int f(x) dx = \int_0^1 \varphi(x^*) dx^*$$

where the right member denotes the ordinary integral of a function of a real variable.

SECTION 30. INTEGRAL EQUATIONS ON A GROUP

The integral constructed in the preceding section makes possible the study of integral equations on a compact group and it is to the discussion of certain results, indispensable in the sequel, in the theory of integral equations with symmetric kernel that the present section is devoted. Throughout the paragraph G will denote a compact topological group and all functions on G will be assumed to be continuous.

A) A vector space R over a field P (see Section 7, I) is said to be Euclidean [unitary] if P is the field of real [complex] numbers and if there is defined a scalar product $(f, g) \in P$ for every pair of elements f and g in R such that the following conditions are satisfied:

$$(\lambda f + \mu g, h) = \lambda(f, h) + \mu(g, h), \quad (g, f) = (\overline{f}, g), \quad (f, f) \geq 0,$$

where the last inequality reduces to equality only when $f = 0$. (Here $\bar{\lambda}$ denotes, as usual, the complex conjugate of the number λ .) †

† It is customary also to impose one further requirement known as completeness but, as this will play no role in the present discussion, we omit it.

The norm $\|f\|$ of an element f is defined to be the non-negative real number $\sqrt{(f, f)}$. The following important inequalities hold and will be proved below:

$$|(f, g)|^2 \leq (f, f)(g, g), \quad (1)$$

$$\|f+g\| \leq \|f\| + \|g\|, \quad (2)$$

Two elements f and g in R are said to be orthogonal to one and other if $(f, g) = 0$; the element f is said to be normalized if $\|f\| = 1$. A system of elements in R is said to be orthonormal if it is composed of normalized elements that are orthogonal in pairs. Clearly an orthonormal system f_1, \dots, f_n is always linearly independent. On the other hand, if g_1, \dots, g_n is any linearly independent system of elements in R then the vectors f_1, \dots, f_n defined by the recurrence relations

$$f_1 = \frac{g_1}{\|g_1\|}, \quad f_i = \frac{g_i - (g_1, f_1)f_1 - \dots - (g_{i-1}, f_{i-1})f_{i-1}}{\|g_i - (g_1, f_1)f_1 - \dots - (g_{i-1}, f_{i-1})f_{i-1}\|}, \quad i = 2, \dots, n.$$

comprise an orthonormal system. (The process for obtaining the f 's from the given g 's is known as orthogonalization.) It follows that a finite dimensional Euclidean or unitary space R always admits an orthonormal basis e_1, \dots, e_r . Relative to such a basis the scalar product of an arbitrary pair of elements $f = \alpha_1 e_1 + \dots + \alpha_r e_r$, $g = \beta_1 e_1 + \dots + \beta_r e_r$ assumes the particularly simple form $(f, g) = \alpha_1 \beta_1 + \dots + \alpha_r \beta_r$. Accordingly inequality (1) assumes the special form ("Cauchy's inequality")

$$|\alpha_1 \bar{\beta}_1 + \dots + \alpha_r \bar{\beta}_r|^2 \leq (\alpha_1 \bar{\alpha}_1 + \dots + \alpha_r \bar{\alpha}_r)(\beta_1 \bar{\beta}_1 + \dots + \beta_r \bar{\beta}_r), \quad (3)$$

valid for arbitrary complex numbers $\alpha_1, \dots, \alpha_r$ and β_1, \dots, β_r . It is easy to see that in the resolution $f = \alpha_1 e_1 + \dots + \alpha_r e_r$ of an arbitrary element f with respect to an orthonormal basis we have $\alpha_1 = (f, e_1)$ and therefore

$$(f, f) = (f, e_1)(\bar{f}, \bar{e}_1) + \dots + (f, e_r)(\bar{f}, \bar{e}_r). \quad (4)$$

On the other hand, if e_1, \dots, e_n is any finite orthonormal system, not necessarily a basis for R , which may even be allowed to be infinite dimensional, then, as will be proved below, the following important inequality ("Bessel's inequality") holds:

$$(f, e_1)(\bar{f}, \bar{e}_1) + \dots + (f, e_n)(\bar{f}, \bar{e}_n) \leq (f, f), \quad (5)$$

In order to prove (1) consider the vector $h = \lambda f + \mu g$. Since the scalar product of a vector with itself is non-negative we have

$$(h, h) = (f, f) \lambda \bar{\lambda} + (f, g) \lambda \bar{\mu} + (\bar{f}, \bar{g}) \bar{\lambda} \mu + (g, g) \mu \bar{\mu} \geq 0 \quad (6)$$

for arbitrary λ, μ . Now if both f and g are zero the validity of (1) is clear. If not we suppose, for the sake of definiteness, that $g \neq 0$ and choose in (6) $\lambda = (g, g)$, $\mu = -(f, g)$; then

$$(f, f)(g, g)^2 - (f, g)(g, g)\overline{(f, g)} - (\bar{f}, \bar{g})(g, g)(f, g) + (g, g)(f, g)\overline{(f, g)} \geq 0,$$

whence (1) follows since $(g, g) > 0$.

To prove (2) we first write

$$(f + g, f + g) = (f, f) + (f, g) + (g, f) + (g, g),$$

and then employ (1) to obtain

$$(f + g, f + g) \leq (f, f) + 2\sqrt{(f, f)(g, g)} + (g, g).$$

Taking square roots on both sides now yields (2).

Finally, in order to prove (5), consider the vector $h = f - (f, e_1)e_1 - \dots - (f, e_n)e_n$. Since, once again, the scalar product of a vector with itself is non-negative, we have $(h, h) \geq 0$ whence (5) follows after a simple computation.

B) From our point of view the most important example of a Euclidean [unitary] space is the set of real [complex] valued functions on a group G with the scalar product of f and g defined by the formula $(f, g) = \int f(x)\overline{g(x)}dx$. In this case, inequality (1) assumes the special form ("Bunjakovskii's inequality")

$$\left| \int f(x)\overline{g(x)}dx \right|^2 \leq \int f(x)\overline{f(x)}dx \cdot \int g(x)\overline{g(x)}dx. \quad (7)$$

If Ω is any orthonormal system of functions then the scalar products (f, φ) , $\varphi \in \Omega$, are called the Fourier coefficients of f with respect to the system Ω . If $\varphi_1, \dots, \varphi_n$ is a finite orthonormal system and f is an arbitrary continuous function then the Fourier coefficients of f satisfy Bessel's inequality (5) which here assumes the special form

$$\sum_{i=1}^n \left| \int f(x)\overline{\varphi_i(x)}dx \right|^2 \leq \int f(x)\overline{f(x)}dx. \quad (8)$$

We now turn to a discussion of the fundamental results of the theory of integral equations with real symmetric kernel. Throughout the balance of the paragraph all functions are assumed to be real valued and continuous.

C) Let K be a continuous real function of two variables defined on G and satisfying the symmetry condition $k(x, y) = k(y, x)$.

We consider the integral equation

$$\varphi(x) = \lambda \int k(x, y) \varphi(y) dy. \quad (9)$$

The function $k(x, y)$ is called the kernel of the equation. Here φ denotes a real continuous function and λ is a real parameter. If the pair λ, φ satisfies (9) and if the function φ is not identically zero then λ is said to be an eigenvalue of the kernel k and φ an eigenfunction of k belonging to the eigenvalue λ . Clearly $\lambda = 0$ cannot be an eigenvalue. Clearly also the set R_λ , consisting of all the eigenfunctions of k belonging to one and the same eigenvalue λ , along with the function identically zero, forms a real vector space. This space will be shown below that every eigenspace is finite dimensional so that for any eigenvalue λ $\dim R_\lambda$ is a well defined positive integer; this dimension is the multiplicity of the eigenvalue λ . It will also be shown below that eigenfunctions belonging to different eigenvalues are orthogonal to one another. Thus, selecting in each eigenspace R_λ an arbitrary orthonormal basis, and uniting all of these bases, we obtain an orthonormal system of functions. Such a system is called a fundamental system of eigenfunctions for the kernel k . If $\varphi_1, \dots, \varphi_n$ is a finite orthonormal system of eigenfunctions belonging respectively to the eigenvalues $\lambda_1, \dots, \lambda_n$ (repetitions allowed) then the following inequalities hold:

$$\sum_{i=1}^n \frac{(\varphi_i(x))^2}{\lambda_i^2} \leq \int (k(x, y))^2 dy, \quad (10)$$

$$\sum_{i=1}^n \frac{1}{\lambda_i^2} \leq \int \int (k(x, y))^2 dx dy. \quad (11)$$

We begin by verifying (10) and (11). Note first that $\int k(x, y) \varphi_i(y) dy = \varphi_i(x)/\lambda_i$. Since this says that the Fourier coefficients of the functions $k(x, y)$, considered as a function of y (x fixed), with respect to the system $\varphi_1, \dots, \varphi_n$ are the numbers

$$\frac{\varphi_1(x)}{\lambda_1}, \dots, \frac{\varphi_n(x)}{\lambda_n},$$

(10) is just a special case of Bessel's inequality (8), while (11) follows from (10) upon integration.

We show next that the dimension of the eigenspace R_λ is finite. Letting $\lambda_1 = \dots = \lambda_n = \lambda$ in (11) we obtain

$$n \leq \lambda^2 \int \int (k(x, y))^2 dx dy.$$

Thus the dimension of R_λ cannot exceed the number λ^2

$$\int \int (k(x, y))^2 dx dy.$$

Finally let φ and ψ be eigenfunctions of the kernel k belonging to distinct eigenvalues λ and μ so that

$$\varphi(x) = \lambda \int k(x, y) \varphi(y) dy, \quad \psi(x) = \mu \int k(x, y) \psi(y) dy.$$

Multiplying the first equality by $\mu \psi(x)$, the second by $\lambda \varphi(x)$, integrating both with respect to x , and subtracting the second from the first, we obtain $(\mu - \lambda) \int \varphi(x) \psi(x) dx = 0$ whence, since $\mu - \lambda \neq 0$, it follows that φ and ψ are orthogonal.

The following Theorems 26 and 27 are concerned with the construction of a fundamental system of eigenfunctions for a given real symmetric kernel.

Theorem 26: Let $k(x, y)$ be a symmetric kernel for which the "quadratic form"

$$K(f, f) = \int \int k(x, y) f(x) f(y) dx dy \quad (12)$$

assumes positive value for at least one function f defined on G . Then on the set S of all functions f defined on G and satisfying the condition $(f, f) = 1$ the form (12) assumes a maximum value $\rho > 0$. Moreover, there is an "extremal" function $\varphi \in S$, i.e., a function for which $K(\varphi, \varphi) = \rho$, which is an eigenfunction of the kernel K belonging to the eigenvalue $1/\rho$.

Proof: We begin by showing that for arbitrary positive ϵ there exists a symmetric kernel $l(x, y)$ having the form

$$l(x, y) = \sum_{i=1}^m \alpha_i l_i(x) l_i(y), \quad (13)$$

and satisfying the condition

$$|k(x, y) - l(x, y)| < \epsilon. \quad (14)$$

where $\alpha_1, \dots, \alpha_m$ denote real numbers while the functions l_1, \dots, l_m constitute an orthonormal systems on G .

Now according to Theorem 7 there exist funcitons f_1, \dots, f_n and g_1, \dots, g_n such that

$$|k(x, y) - \sum_{i=1}^n f_i(x) g_i(y)| < \epsilon.$$

Let $l(x, y) = \frac{1}{2} \sum_{i=1}^n \{f_i(x) g_i(y) + g_i(x) f_i(y)\}$. Then l satisfies (14) and is symmetric. Next, expressing the $2n$ functions $f_1, \dots, f_n, g_1, \dots, g_n$, in any fashion, as linear combinations of some orthonormal system p_1, \dots, p_m , we may write l in the form

$$l(x, y) = \sum_{i,j=1}^m \alpha_{ij} p_i(x) p_j(y). \quad (15)$$

Multiplying by $p_s(x)p_t(y)$ and integrating we obtain

$$\alpha_{st} = \int \int l(x, y) p_s(x)p_t(y) dx dy,$$

whence it follows from the symmetry of l that $\alpha_{st} = \alpha_{ts}$, i.e., that the bilinear form $\sum_{i,j=1}^m \alpha_{ij} \xi_i \eta_j$ is symmetric. Finally, reducing this form to principal axes or, what comes to the same thing, subjecting the functions p_1, \dots, p_m to an appropriate orthogonal transformation, we reduce l to the form (13).

We now consider the quadratic form

$$L(f, f) = \int \int l(x, y) f(x)f(y) dx dy \quad (16)$$

on the set S . Introducing the Fourier coefficients $\xi_i = (f, l_i)$ we may write this form more simply as

$$L(f, f) = \sum_{i=1}^m \alpha_i \xi_i^2 \quad (17)$$

where, moreover, according to (8) we have

$$\sum_{i=1}^m \xi_i^2 \leq 1. \quad (18)$$

since $f \in S$. We shall suppose α_1 is the largest of the numbers $\alpha_1, \dots, \alpha_m$, i.e., that $\alpha_1 \geq \alpha_i$, $i = 2, \dots, m$, and we write $\alpha_1 = \sigma$. It is clear that the maximum of (17) subject to condition (18) is equal to σ that that it is assumed for $\xi_1 = 1$, $\xi_2 = \dots = \xi_m = 0$. Thus (16) assumes its maximum σ on the set S at $f = l_1 = \psi$. Moreover, it is not difficult to verify that

$$\psi(x) = \frac{1}{\sigma} \int l(x, y) \psi(y) dy. \quad (19)$$

Now, from inequality (7) applied to the functions $k(x, y)$ and $f(x)f(y)$ defined on the group $G \times G$ it follows that

$$\text{for } f \in S \text{ we have } (K(f, f))^2 \leq \int \int (k(x, y))^2 dx dy. \quad (20)$$

In particular, the form $K(f, f)$ is bounded on S and has a positive upper bound which we denote by ρ . From (14) it follows that

$$|\rho - \sigma| < \epsilon. \quad (21)$$

Indeed, another application of (7) yields

$$|K(f, f) - L(f, f)|^2 \leq \int \int (k(x, y) - l(x, y))^2 dx dy < \epsilon^2.$$

for $f \in S$. But then, since the functions $K(f, f)$ and $L(f, f)$ differ

by less than ϵ for every $f \in S$, it follows that their upper bounds ρ and σ must also differ by less than ϵ .

Now let $l_n(x, y)$ be a kernel of the form (13) satisfying the inequality

$$|k(x, y) - l_n(x, y)| < \frac{\rho}{2^n}. \quad (22)$$

We denote by σ_n and ψ_n the number and function constructed, as above, for the kernel $l(x, y) = l_n(x, y)$, so that (19) and (21) assume the form

$$\psi_n(x) = \frac{1}{\sigma_n} \int l_n(x, y) \psi_n(y) dy, \quad (23)$$

$$|\rho - \sigma_n| < \frac{\rho}{2^n}. \quad (24)$$

Since the sequence $l_1(x, y), l_2(x, y), \dots$ converges uniformly to $k(x, y)$ (see (22)) it follows that the set of function appearing in the sequence is uniformly equicontinuous (see Section 28, H)) i.e., for arbitrary positive δ there exists a neighborhood U of the identity in G such that

for $x'x^{-1} \in U$ we have $|l_n(x', y) - l_n(x, y)| < \delta$.

Applying (7) once again and taking into account relations (23) and (24) we thus obtain

$$(\psi_n(x') - \psi_n(x))^2 \leq \frac{\delta^2}{\sigma_n^2} \leq \frac{4\delta^2}{\rho^2},$$

which says that the set of functions ψ_1, ψ_2, \dots is also uniformly equicontinuous. A similar argument shows that the set is uniformly bounded. Indeed, from (7), (22), (23) and (24) it follows that

$$(\psi_n(x))^2 \leq \frac{1}{\sigma_n^2} \int (l_n(x, y))^2 dy \leq \frac{4}{\rho^2} \int (|k(x, y)| + \frac{\rho}{2})^2 dy$$

Hence, by virtue of Theorem 23, the sequence ψ_1, ψ_2, \dots contains a subsequence converging uniformly to some function φ and, passing to the limit along this subsequence in (23), we obtain

$$\varphi(x) = \frac{1}{\rho} \int k(x, y) \varphi(y) dy. \quad (25)$$

Clearly $\varphi \in S$. Finally, multiplying (25) by $\rho\varphi(x)$ and integrating we obtain

$$K(\varphi, \varphi) = \rho.$$

Thus Theorem 26 is proved.

We are now in a position to formulate and prove a theorem which describes the construction of a fundamental system of eigenfunctions for a symmetric kernel (see C)).

Theorem 27: Let $k = k(x, y)$ be a symmetric kernel defined on G . If for some real function f defined on G the quadratic form $K(f, f)$ assumes a positive value let φ_1 be any extremal eigenfunction of k and let λ_1 denote the corresponding eigenvalue (see Theorem 26). If the symmetric kernel

$$k_1(x, y) = k(x, y) - \frac{\varphi_1(x)\varphi_1(y)}{\lambda_1}$$

likewise possesses the property that its quadratic form $K_1(f, f)$ assumes, for some f , a positive value, let φ_2 be any extremal eigenfunction of k_1 and denote by λ_2 the corresponding eigenvalue. If the symmetric kernel

$$k_2(x, y) = k_1(x, y) - \frac{\varphi_2(x)\varphi_2(y)}{\lambda_2}$$

continues to possess the property that its quadratic form $K_2(f, f)$ assumes positive values let φ_3 be any extremal eigenfunction of K_2 and denote by λ_3 the corresponding eigenvalue. Continuing in this way as long as possible we obtain a finite or infinite sequence of functions $\varphi_1, \varphi_2, \dots$ and a corresponding sequence of positive numbers $\lambda_1, \lambda_2, \dots$. Likewise, applying the same process to the kernel $-k(x, y)$, we obtain another finite or infinite sequence of functions $\varphi_{-1}, \varphi_{-2}, \dots$ and a corresponding sequence of positive numbers $-\lambda_{-1}, -\lambda_{-2}, \dots$. Uniting these two sequences of functions yields a double sequence

$$\dots, \varphi_{-2}, \varphi_{-1}, \varphi_1, \varphi_2, \dots, \quad (26)$$

which constitutes a fundamental system of eigenfunctions for the original kernel k , the function φ_n being an eigenfunction belonging to the eigenvalue λ_n , $n = \pm 1, \pm 2, \dots$. Each of the two sequences $\lambda_1, \lambda_2, \dots$ and $-\lambda_{-1}, -\lambda_{-2}, \dots$ is non-decreasing and each is unbounded above if infinite. Finally we write

$$k_{mn}(x, y) = k(x, y) - \sum_{i=1}^m \frac{\varphi_{-i}(x)\varphi_{-i}(y)}{\lambda_{-i}} - \sum_{i=1}^n \frac{\varphi_i(x)\varphi_i(y)}{\lambda_i} \quad (27)$$

and

$$K_{mn} (g, h) = \iint k_{mn} (x, y) g(x) h(y) dx dy.$$

(If the double sequence (26) breaks off at either end the kernel k_{mn} is defined by $k_{mn} = k_{m'n}$ where m', n' are the nearest indices to m, n for which there exist functions in the sequence (26).) Then for arbitrary g and h

$$\lim_{m,n \rightarrow \infty} K_{mn} (g, h) = 0. \quad (28)$$

Proof: The hypothesis that the normalized functions

$$\varphi_{-m}, \dots, \varphi_{-1}, \varphi_1, \dots, \varphi_n \quad (29)$$

constitute an orthonormal system of eigenfunctions of k belonging, respectively, to the eigenvalues

$$\lambda_{-m}, \dots, \lambda_{-1}, \lambda_1, \dots, \lambda_n.$$

will be referred to as hypothesis $\{m, n\}$. If f is any function defined on G let $c_i = (f, \varphi_i)$ and write

$$f_{mn} = f - \sum_{i=1}^m c_{-i} \varphi_{-i} - \sum_{i=1}^n c_i \varphi_i.$$

A simple calculation shows that if hypothesis $\{m, n\}$ holds then

$$K_{mn} (f_{mn}, f_{mn}) = K_{mn} (f, f). \quad (30)$$

(The only things needed for the proof, besides hypothesis $\{m, n\}$ are the definition (27) and the orthogonality of f_{mn} to all of the functions of the system (29).) If now $f_{mn} \neq 0$ then $f'_{mn} = \frac{f_{mn}}{\|f_{mn}\|}$ belongs to S and, assuming $f \in S$, we obtain

$$K_{mn} (f'_{mn}, f'_{mn}) = \frac{1}{(f_{mn}, f_{mn})} K_{mn} (f, f) \geq K_{mn} (f, f), \quad (31)$$

where, moreover, equality holds only in case the function f is orthogonal to all of the functions (29). Indeed,

$$(f_{mn}, f_{mn}) = 1 - \sum_{i=1}^m c_{-i}^2 - \sum_{i=1}^n c_i^2,$$

so that $(f_{mn}, f_{mn}) \leq 1$ with equality holding only if $c_{-m} = \dots = c_{-1} = c_1 = \dots = c_n = 0$.

We turn now to the proof of hypothesis $\{m, n\}$. The validity of hypothesis $\{0, 1\}$ is an immediate consequence of the definition of φ_1 and λ_1 . We suppose hypothesis $\{0, n\}$ is valid and show that then hypothesis $\{0, n+1\}$ is also valid. Observing that $k_{0n} = k_n$

we obtain from (30) :

$$K_n(f_{0n}, f_{0n}) = K_n(f, f). \quad (32)$$

Letting $f = \varphi_{n+1}$ and recalling that this is a point on S at which the form K_n assumes its positive maximum, we conclude from (32) that $f_{0n} \neq 0$, whereupon (31) yields

$$K_n(f'_{0n}, f'_{0n}) \geq K_n(f, f). \quad (33)$$

But now $f = \varphi_{n+1}$ yields the maximum of K_n on S while $f'_{0n} \in S$, so that (33) must reduce to an equality whence, according to the above, $f = \varphi_{n+1}$ is orthogonal to the functions $\varphi_1, \dots, \varphi_n$. Since moreover

$$\varphi_{n+1}(x) = \lambda_{n+1} \int k_n(x, y) \varphi_{n+1}(y) dy$$

it follows from the orthogonality just demonstrated that

$$\varphi_{n+1}(x) = \lambda_{n+1} \int k(x, y) \varphi_{n+1}(y) dy.$$

Thus the validity of hypothesis $\{0, n+1\}$ is demonstrated and it follows, by mathematical induction, that hypothesis $\{0, n\}$ holds for all n . Next, this fact applied to the kernel $-k[x, y]$ shows that hypothesis $\{m, 0\}$ is also valid for all m . Finally, the validity of hypothesis $\{m, n\}$ follows from the validity of $\{m, 0\}$ and $\{0, n\}$ since eigenfunctions belonging to distinct eigenvalues are always orthogonal to one another (see C)).

We next prove that

$$\lambda_{n+1} \geq \lambda_n. \quad (34)$$

Indeed, since φ_{n+1} is orthogonal to φ_n it follows that

$$K_n(\varphi_{n+1}, \varphi_{n+1}) = K_{n-1}(\varphi_{n+1}, \varphi_{n+1}). \quad (35)$$

But also φ_{n+1} yields the maximum of K_n on S , this maximum being $1/\lambda_{n+1}$, while the maximum of K_{n-1} on S is $1/\lambda_n$. Thus (35) implies $1/\lambda_{n+1} \leq 1/\lambda_n$ whence (34) follows. Moreover, applying this result to the kernel $-k$, we learn that $-\lambda_{-(n+1)} \geq -\lambda_{-n}$.

We next show that the sequences of positive and negative eigenvalues must either be finite or tend to $\pm\infty$ respectively. To this end it suffices to prove that the double sequence

$$\dots, \lambda_{-2}, \lambda_{-1}, \lambda_1, \lambda_2, \dots \quad (36)$$

has no limit points. Now (11) shows that the number r of eigenvalues of the kernel k not exceeding a in absolute value must satisfy the inequality

$$r \leq a^2 \int \int (k(x, y))^2 dx dy.$$

Thus no bounded segment of the number axis can contain more than a finite number of eigenvalues, and the result follows.

It remains to verify (28). Denote by ρ_{n+1} the upper bound of the form K_{0n} on S . For any n for which the eigenfunction φ_{n+1} is defined we have $K_{0n} = K_n$ so that $\rho_{n+1} = \frac{1}{\lambda_{n+1}}$. Accordingly, if the sequence $\varphi_1, \varphi_2, \dots$ is infinite it follows that $\lim_{n \rightarrow \infty} \rho_n = 0$.

On the other hand, if the sequence is finite, containing, say, n' elements, then for $n > n'$ we have $K_{0n} = K_{n'}$, and the upper bound of $K_{n'}$ on S is zero, so that in this case also $\lim_{n \rightarrow \infty} \rho_n = 0$. Thus in any event

$$\lim_{n \rightarrow \infty} \rho_n = 0. \quad (37)$$

But now, by virtue of the definition of ρ_n , we have for arbitrary f

$$K_{0n}(f, f) \leq (f, f) \rho_{n+1}. \quad (38)$$

In exactly the same fashion it follows that:

$$\lim_{m \rightarrow \infty} \rho_{-m} = 0. \quad (39)$$

$$K_{m0}(f, f) \geq -(f, f) \rho_{-(m+1)}, \quad (40)$$

where $\rho_{-(m+1)}$ notes the upper bound of $-K_{m0}$ on S . It is now a simple matter to verify (28) in the special case $g = h = f$. Indeed, since f_{mn} is orthogonal to all of the functions (29) it follows from (30) that

$$K_{mn}(f, f) = K_{mn}(f_{mn}, f_{mn}) = K_{m0}(f_{mn}, f_{mn}) = K_{0n}(f_{mn}, f_{mn}). \quad (41)$$

Since $(f_{mn}, f_{mn}) \leq (f, f)$, relations (38), (40) and (41) imply

$$-(f, f) \rho_{-(m+1)} \leq K_{mn}(f, f) \leq (f, f) \rho_{n+1},$$

whence

$$\lim_{m, n \rightarrow \infty} K_{mn}(f, f) = 0 \quad (42)$$

follows by (37) and (39). But now, for arbitrary functions g and h we have

$$K_{mn}(g + h, g + h) = K_{mn}(g, g) + K_{mn}(h, h) + 2K_{mn}(g, h),$$

and (28) follows by virtue of (42).

The fact that (26) is a fundamental system of eigenfunctions for the kernel k now follows at once from (28). Indeed, let f be an eigenfunction belonging to the eigenvalue λ . The orthonormal system (26) can contain only a finite number of eigenfunctions belonging to λ (see C); accordingly, all of the eigenfunctions belonging to λ that appear in the orthonormal system (26) will appear in some system (29) for sufficiently large m and n . Suppose now that f cannot be expressed as a linear combination of the eigenfunctions belonging to λ that appear in (26). Then $f_{mn} \neq 0$ is also

an eigenfunction belonging to λ . Denoting by φ the normalized function $\varphi = f_{mn}$ we have: $\varphi(x) = \lambda \int k(x, y) \varphi(y) dy$. Multiplying by $\frac{1}{\lambda} \varphi(x)$ and integrating yields $K(\varphi, \varphi) = \frac{1}{\lambda}$. But now φ is orthogonal to all of the functions (26) so that we have also $K_{mn}(\varphi, \varphi) = \frac{1}{\lambda}$ for all m and n which contradicts (28).

Thus we see that the eigenfunctions belonging to λ that appear in (26) form an orthonormal basis in the eigenspace R_λ ; since λ here denotes an arbitrary eigenvalue of k , this shows that (26) is indeed a fundamental system of eigenfunctions. Thus the proof of Theorem 27 is complete.

It is not Theorem 27 itself but rather the following corollary that will be needed in the study of group representations.

D) Let $k = k(x, y)$ be a symmetric kernel and let g be any function defined on G . Then the function $f(x) = \int k(x, y) g(y) dy$ may be resolved into a uniformly and absolutely convergent series

$$f(x) = \sum_n \psi_n(x),$$

where ψ_1, ψ_2, \dots are eigenfunctions of k .

Denote by $b_i = (g, \varphi_i)$, $i = \pm 1, \pm 2, \dots$, the Fourier coefficients of g with respect to the orthonormal system (26). The Fourier coefficients of f are then given by the formula $(f, \varphi_i) = \frac{b_i}{\lambda_i}$, $i = \pm 1, \pm 2, \dots$. We shall prove D) by showing that the Fourier series

$$\sum \frac{b_i}{\lambda_i} \varphi_i(x) \quad (43)$$

converges to f uniformly and absolutely on G .

In the first place, by virtue of (10) and Cauchy's inequality (see (3)) we have

$$\left(\sum \left| \frac{b_i}{\lambda_i} \varphi_i(x) \right|^2 \right)^{\frac{1}{2}} \leq \left(\sum b_i^2 \right)^{\frac{1}{2}} \cdot \left(\sum \frac{(\varphi_i(x))^2}{\lambda_i^2} \right)^{\frac{1}{2}} \leq \left(\sum b_i^2 \right)^{\frac{1}{2}} \int (k(x, y))^2 dy,$$

where the summation may be extended over an arbitrary finite system of indices i . Since the numbers b_i are Fourier coefficients, it follows by Bessel's inequality (see (8)) that the series of their squares is convergent. Accordingly, for any positive ϵ there exists an index p so large that $\sum b_i^2 < \epsilon$ whenever the summation is extended over a finite set of indices i satisfying $|i| > p$. From this and from the fact that the function $\int (k(x, y))^2 dy$ is bounded we conclude, on the basis of the Cauchy criterion, that the series

(43) does, in fact, converge uniformly and absolutely to some limit f' . The proof will be completed by showing that $f' = f$.

Indeed let h be any function on G . Then

$$\int \left(f(x) - \sum_{i=1}^m \frac{b_{-i}}{\lambda_{-i}} \varphi_{-i}(x) - \sum_{i=1}^n \frac{b_i}{\lambda_i} \varphi_i(x) \right) h(x) dx = K_{mn}(g, h).$$

Passing to the limit as $m, n \rightarrow \infty$ we obtain, by virtue of (28)

$$\int (f(x) - f'(x)) h(x) = 0.$$

Thus $f - f'$ is orthogonal to every function so that $f - f' = 0$, i.e., $f = f'$.

Example 53: Let G be a compact topological group and let Ω be an arbitrary orthonormal system of functions defined on G . We shall show that the cardinality of Ω cannot exceed the weight of G (see Definition 14).

The case of a finite group is easily disposed of: if G consists of r elements then the space G is discrete and consequently of weight r while the collection of all functions defined on G is a vector space of dimension r .

Consider now the case of an infinite group G . For any function f defined on G denote by Ω_f the set of all functions $\varphi \in \Omega$ for which $(f, \varphi) \neq 0$. We begin by showing that Ω_f is always finite or countable. To this end denote by Ω_f^k the collection of functions $\varphi \in \Omega_f$ for which $|(f, \varphi)| > \frac{1}{k}$. If $\varphi_1, \dots, \varphi_n$ is any finite subset of Ω_f^k

then by Bessel's inequality (8) we have $n < k^2(f, f)$. Thus Ω_f^k is finite, and since Ω_f is the union of the sets Ω_f^k , $k = 1, 2, \dots$ it follows that Ω_f cannot be more than countable. Next let Ω^* be any complete system of Urysohn functions on G constructed with respect to a base Σ of minimum cardinality (see the proof of Theorem 7, c)), so that the cardinality of Ω^* is equal to the weight of G and let $\varphi \in \Omega$. Since $(\varphi, \varphi) = 1$ there exists a neighborhood $U^* \in \Sigma$ in which either the real or imaginary part of φ does not change sign. Let $U \in \Sigma$ be a neighborhood such that $\bar{U} \subset U^*$ and let u be the function in Ω^* associated with the pair of neighborhoods U, U^* . Then $(u, \varphi) \neq 0$. Thus every $\varphi \in \Omega$ belongs to some Ω_u and since the set Ω_u is at most countable while the cardinality of Ω^* is the same as the weight of G , it follows that the cardinality of Ω cannot exceed the weight.

That the cardinality of an arbitrary orthogonal set of (non-zero) functions is also bounded by the weight of G may be seen by normalizing the functions.

Example 54: Denote by G^* the additive topological group of real numbers, by N the subgroup of integers, and let $G = G^*/N$. As has already been observed in Example 52, every function φ defined on G may be viewed as a periodic function of a real variable with period 1, and conversely. Consider the functions $\varphi_n(x) = e^{2\pi i n x}$ of the real variable x where e denotes Napier's constant, $i = \sqrt{-1}$, and n is any integer. Then $\varphi_n(x)$ has period 1 and may be regarded as a function defined on G . A simple computation shows that the system of functions $\varphi_n(x)$, $n = 0, \pm 1, \pm 2, \dots$, is an orthonormal system on G .

SECTION 31 PRELIMINARY REMARKS CONCERNING MATRICES

I here recall some elementary facts from the theory of matrices and present a proof of Shur's lemma, which plays an important role in the theory of linear representations.

A) Let R be an r -dimensional vector space over a field P (see Section 7, I)) and let f be any linear transformation of R into itself, i. e., suppose that

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y), \quad (1)$$

where x and y are any two vectors of R while α and β denote elements of P . Select a basis in R and denote by x_1, \dots, x_r the coordinates of the vector x and by $f_1(x), \dots, f_r(x)$ the coordinates of $f(x)$. These coordinates are connected by relations of the form

$$f_1(x) = \sum_{j=1}^r d_j^1 x_i \quad (2)$$

where the coefficients $d_j^i \in P$ depend only on f and not on the choice of the particular vector x . In this way, the choice of a fixed basis determines a one-to-one correspondence between the collection of all linear transformations of the space of R into itself and the collection of all square matrices of order r :

$$f \rightarrow \|d_j^i\| = d. \quad (3)$$

If f is non-singular, i. e., possesses an inverse, then d is non-singular, and conversely. A non-singular linear transformation of a vector space R onto itself will also be called a linear automorphism of R . The product of two linear automorphisms corresponds to the product of their respective matrices (see Example 2) and the transformation f^{-1} inverse to f corresponds to the

inverse of the matrix $\|d_j^i\|$. Accordingly, the collection of all linear automorphisms forms a group under multiplication and this group is isomorphic with the group of non-singular matrices of order r . As was noted in Example 31, if P is either the field of real numbers or the field of complex numbers there is a natural way of topologizing the group of non-singular matrices so as to turn it into a separable topological group; it is this topology that is to be understood in the sequel whenever the collection of non-singular matrices is regarded as a topological group.

B) If we change from one basis in R to another then the new and the old coordinates of one and the same vector are connected by relations

$$x'_i = \sum_{j=1}^r t_j^i x_j, \quad (4)$$

where the matrix $\|t_j^i\| = t$ is non-singular. Relative to this new basis the transformation f will correspond to a new matrix $\|\tilde{d}_j^i\| = \tilde{d}$ where

$$\tilde{d} = t dt^{-1}. \quad (5)$$

It is said that d goes into \tilde{d} under transformation by t ; and if there exists a (non-singular) matrix t transforming d into \tilde{d} then d and \tilde{d} are similar. The only functions of a matrix that are invariants of the linear transformation f are those that are the same for all similar matrices. An example of such an invariant is the trace of a matrix d ,

$$\text{Tr}(d) = \sum_{i=1}^r d_i^i, \quad (6)$$

since $\text{Tr}(\tilde{d}) = \text{Tr}(d)$. Thus it makes sense to speak of the trace of the linear transformation f , $\text{Tr}(f) = \text{Tr}(d)$. If a and b are two matrices then the trace of their product does not depend upon the order of multiplication:

$$\text{Tr}(ab) = \text{Tr}(ba). \quad (7)$$

C) Suppose f is a linear transformation of the space R into itself leaving invariant some subspace S of dimension s , $f(S) \subset S$, where $0 < s < r$. If a basis is chosen in R so that the first s of its vectors belong to the subspace S , then the matrix d corresponding to f assumes the form

$$d = \begin{vmatrix} a & b \\ 0 & c \end{vmatrix}, \quad (8)$$

where a and c denote square matrices of orders s and $r - s$

respectively, while b denotes a rectangular matrix and 0 denotes a rectangular matrix all of whose entries are zeros. Denote by d^* the transpose of d (see Example 3); then the linear transformation f^* corresponding to d^* leaves invariant the $(r - s)$ - dimensional subspace generated by the last $r - s$ vectors of the basis. It should not be supposed here that f and f^* are related in an invariant fashion; the connection between them is accidental, depending as it does upon the choice of basis.

D) Let Δ be a set of linear transformations of the r -dimensional vector space R into itself. Then Δ is said to be reducible if there exists a proper subspace S of R , i. e., a subspace S of some dimension s with $0 < s < r$, which is left invariant by all transformations of Δ ; if this is not the case then Δ is said to be irreducible. If Σ is a set of matrices of order r and Δ denotes the set of linear transformations of R into itself corresponding to this set of matrices with respect to some fixed basis in R , then Σ is said to be reducible or irreducible according as Δ is reducible or irreducible. It is easy to see that the definition is correct, i. e., that the reducibility or irreducibility of Σ does not depend upon the choice of basis defining the correspondence between Σ and Δ . We show that if a set Σ of matrices is reducible then the set Σ^* of transposed matrices is also reducible.

By C) there exists a constant matrix t such that all matrices of the set $t \Sigma t^{-1}$ have the special form (8), i. e., such that if $x \in \Sigma$ then $t x t^{-1} = \tilde{x}$ has the form (8). But then, as was shown in C), the linear transformations corresponding to the matrices x^* all leave invariant one and the same subspace S' . Transposing the equation $t x t^{-1} = \tilde{x}$ and solving for x^* we obtain $t^{*-1} x^* t^* = \tilde{x}^*$, $\tilde{x}^* = t^* \tilde{x} t^{*-1}$. Since all the linear transformations corresponding to the matrices x^* leave S' invariant it follows that the linear transformations corresponding (with respect to the same basis) to the matrices x^* all leave invariant a certain subspace S'' . Thus Σ^* is reducible.

We come now to the following basic result due to I. Schur.

Schur's Lemma: Let Σ be an irreducible collection of m -rowed square matrices, let Ω be an irreducible set of n -rowed square matrices, and let a be a rectangular matrix having m rows and n columns. Suppose that

$$\Sigma a = a\Omega \tag{9}$$

i. e., that for every $u \in \Sigma$ there exists some $v \in \Omega$ such that

$$ua = av \quad (10)$$

and, conversely, that for every $v' \in \Omega$ there exists some $u' \in \Sigma$ such that

$$u'a = av'$$

Then there are just two possibilities: either a is the zero matrix, $a = 0$, or else $m = n$ and a (which is then square) is non-singular.

Proof: Let R be a vector space of dimension m and fix a basis in R . Then the matrices belonging to Σ may be interpreted as linear transformations of R into itself. Let $a = \|a_j^i\|$ and denote by a_k the vector in R having coordinates a_k^1, \dots, a_k^m so that the coordinates of a_k are the entries of the k -th column of a . Finally let S denote the subspace of R generated by the vectors a_1, \dots, a_n . We show first that S is invariant under Σ .

Let $u = \|u_j^i\|$ be any matrix of Σ and let $v = \|v_j^i\|$ be a matrix belonging to Ω such that $ua = av$. Applying u to the vector a_k we obtain b_k^i with coordinates $b_k^i = \sum_{j=1}^n u_j^i a_k^j$, $i = 1, \dots, m$, but since $ua = av$ we have also $b_k^i = \sum_{j=1}^n a_j^i v_k^j$, $i = 1, \dots, m$, so that the

coordinates of the vectors b_k are expressed linearly in terms of those of a_1, \dots, a_n which shows that $b_k \in S$. Thus S is invariant under Σ .

Since Σ is irreducible by hypothesis, there are just two possibilities: either $S = 0$ or $S = R$. In the former case, all the vectors a_k generating S must be 0 and a is the zero matrix. In the latter case, it is possible to find m linearly independent elements among the vectors, a_1, \dots, a_n , or, in other words, the matrix a contains a set of m linearly independent columns. From this it follows that

$$n \geq m. \quad (11)$$

Denote now by Σ^* the set of matrices obtained by transposing the matrices of Σ , by Ω^* the analogous set of transposes of Ω , and by a^* the transpose of a . According to D) the sets Σ^* and Ω^* are irreducible. Moreover, from (9) we obtain $\Omega^*a^* = a^*\Sigma^*$ and, applying to this relation the result just obtained, we conclude that that either $a^* = 0$ or else a^* contains n linearly independent columns. The first case has already been disposed of. In the second case it follows that a has n linearly independent rows so that $n \leq m$. But this, along with (11), says that a is square and that its determinant is different from zero. Thus Schur's Lemma is proved.

As an immediate consequence of Schur's Lemma we have the following corollary which, unlike the other results of this section, is valid only for algebraically closed fields P (i.e., fields in which every algebraic equation has a root). We formulate the results only for the field of complex numbers.

E) Let Ω be an irreducible set of complex r -rowed square matrices and let b be a square matrix, also of order r , that commutes with all the elements of Ω . Then b has the form βe where β is a complex number and e denotes the identity matrix.

Consider the matrix $a = b - \beta e$ where β is a complex number chosen so as to make the determinant of a zero. Since the determinant $|b - \beta e|$ is a polynomial in β with complex coefficients, the existence of such a number is assured. Moreover, since b commutes with all the elements of Ω the same is true of a . Thus we have, in particular, $\Omega a = a\Omega$ and according to Schur's Lemma, a must be the zero matrix since $|a| = 0$ by construction. Thus $b = \beta e$.

F) Let Ω be an irreducible set of complex square matrices, every two of which commute with each other. Then the matrices belonging to Ω are of order one.

Indeed, it follows from E) that they are all of the form βe where β denotes a complex number; but a set of matrices having this form can be irreducible only when the matrices are of order one.

We next examine in some detail the properties of unitary matrices.

G) Let R be a unitary space of finite dimension r (see Section 30, A)). A linear transformation f of R into itself is said to be unitary if it preserves the inner product, i. e., if $(f(x), f(y)) = (x, y)$ for all $x, y \in R$. The matrix of a unitary transformation with respect to an orthonormal basis is called a unitary matrix. A simple computation shows that d is unitary when and only when $\bar{d}^* d = e$, where the horizontal stroke denotes the operation of replacing every element of the matrix by its complex conjugate and the asterisk denotes transposition as usual. Equivalent formulations of this condition are: $\bar{d}^* = d^{-1}$, $d\bar{d}^* = e$. If the entries of a unitary matrix are real then this condition becomes the condition of orthogonality (see Example 3). Since the unitary transformations, by their very definition, form a group, it follows that the unitary matrices of a given order r also form a group under multiplication. Moreover, the defining equation above shows that the set of unitary matrices is closed in the topological group of all non-singular matrices of order r . Thus the group of unitary

matrices is a subgroup of the latter group and is a separable topological group in its own right known as the unitary group of order r . Finally, returning once more to the relation $d^*d = e$, we see that the absolute values of the entires of a unitary matrix do not exceed one; hence the unitary group is compact. The collection of orthogonal matrices of order r constitutes a subgroup of the unitary group.

H) Let R be a complex vector space. A complex valued function $\varphi(x, y)$ of two vectors $x, y \in R$ is called a Hermitian bilinear form if (a) $\varphi(\lambda x + \mu y, z) = \lambda\varphi(x, z) + \mu\varphi(y, z)$ where λ, μ denote complex numbers, and (b) $\varphi(y, x) = \overline{\varphi(x, y)}$. A Hermitian form $\varphi(x, y)$ is said to be positive definite if $\varphi(x, x) > 0$ for $x \neq 0$. Clearly any positive definite, Hermitian bilinear form may be taken as a scalar product in the space R , whereupon R becomes a unitary space.

I) Let Σ be a reducible set of unitary matrices of order r . Then there exists a single unitary matrix t of order r such that for every $d \in \Sigma$ the matrix $\tilde{d} = tdt^{-1}$ has the special form

$$\tilde{d} = \begin{vmatrix} a & 0 \\ 0 & b \end{vmatrix} \quad (12)$$

where a and b are unitary matrices. This fact is usually expressed by saying that a reducible set of unitary matrices is completely reducible.

We regard the matrices of Σ as the matrices of a set of unitary transformations of an r -dimensional unitary space R relative to a fixed orthonormal basis. Since Σ is reducible, these transformations all leave invariant some one subspace S of dimension s , $0 <$

$s < r$. If we now select in R a new orthonormal basis in such a way that the first s of its vectors belong to S , then the matrix t connecting the old coordinates with the new is unitary while $\tilde{d} = tdt^{-1}$ clearly has the special form (12) whenever $d \in \Sigma$.

SECTION 32. ORTHOGONALITY RELATIONS

Just as in Section 30, the symbol G will denote a compact topological group.

Definition 34: A homomorphism g of a topological group G into the topological group of real or complex non-singular matrices of some finite order (see Section 31, A)) is called a linear representation

of G . When necessary we shall distinguish between real and complex representations. Thus to each element $x \in G$ there corresponds a matrix $g(x)$, the entries of which we denote by $g_j^i(x)$, $g(x) = \|g_j^i(x)\|$. The order of $g(x)$ is known as the degree of g . Two linear representations g and h of the same group G are said to be equivalent if there exists a constant (independent of x) matrix t such that

$$h(x) = tg(x)t^{-1} \quad (1)$$

for every $x \in G$.

If g is a linear representation of G , $g(x) = \|g_j^i(x)\|$, then the functions g_j^i are continuous, for we are considering here homomorphisms of a topological group into a topological group, i.e., continuous mappings. Conversely, any homomorphism g of the algebraic group G into the algebraic group of matrices, $g(x) = \|g_j^i(x)\|$, in which the functions g_j^i are continuous on the topological space G , is a homomorphism of the topological group G into the topological group of non-singular matrices and is accordingly a linear representation of G .

Theorem 28: Let g be a complex linear representation of a compact group G . Then there exists an equivalent representation g which is unitary valued. Thus for any linear representation there exists an equivalent unitary representation.

Proof: Let R be an r -dimensional unitary space, where r denotes the degree of g , fix a basis in R , and consider the positive definite Hermitian form

$$\psi(u, v) = \sum_{i=1}^r u_i \overline{v_i}, \quad (2)$$

where $u_1, \dots, u_r; v_1, \dots, v_r$ are the coordinates of u, v . To each of the matrices $g(x)$ there corresponds a non-singular linear automorphism of R which we denote by g_x . Substituting $g_x(u), g_x(v)$ for u, v in (2) we obtain a function

$$\psi_x(u, v) = \psi(g_x(u), g_x(v)), \quad (3)$$

which is again a positive definite Hermitian form. Next we define the new Hermitian form

$$\varphi(u, v) = \int \psi_x(u, v) dx. \quad (4)$$

This form is again positive definite. Moreover, its value is invariant under the substitution of $g_y(u), g_y(v)$ for u, v . Indeed, taking into account the relation $g_x g_y = g_{xy}$ and the invariance of the integral, we have

$$\begin{aligned}\varphi(g_y(u), g_y(v)) &= \int \psi(g_{xy}(u), g_{xy}(v)) dx = \int \psi_{xy}(u, v) dx = \\ &= \int \psi(u, v) dx = \varphi(u, v).\end{aligned}$$

We now use $\varphi(u, v)$ as the inner product in R (see Section 31, H)) and select in R a basis which is orthonormal with respect to $\varphi(u, v)$. Relative to this basis, g_y corresponds to some matrix $\tilde{g}(y)$ and since g_y preserves the inner product it follows that $\tilde{g}(y)$ is unitary. Thus \tilde{g} is a unitary representation of G . Finally, denoting by t the matrix connecting the old basis with the new, we have $\tilde{g}(x) = tg(x)t^{-1}$, and the proof is complete.

Definition 35: The character $\chi(x)$ of a linear representation g is the trace of the matrix $g(x)$ (see Section 31, B)): $\chi(x) = \text{Tr}(g(x))$. Thus the character of a representation is a numerical function defined on G . Clearly two equivalent representations have the same character since $g(x)$ and $tg(x)t^{-1}$ have the same trace. The character has the property of invariance, viz.,

$$\begin{aligned}\chi(a^{-1}xa) &= \text{Tr}(g(a^{-1}xa)) = \text{Tr}((g(a))^{-1}g(x)g(a)) = \text{Tr}(g(x)) = \\ &= \chi(x).\end{aligned}$$

A) Let g be a reducible, complex representation of G . By Theorem 28 and remark I), Section 31, there exists a matrix t such that the matrices $h(x) = tg(x)t^{-1}$ have the special form

$$h(x) = \begin{vmatrix} g'(x) & 0 \\ 0 & g''(x) \end{vmatrix},$$

where $g'(x)$ and $g''(x)$ are unitary matrices. We shall say, in this case, that g splits into the two representations g' and g'' . If g' or g'' should be, themselves, reducible then they may be split again in the same manner. Thus every representation g splits into a finite system of irreducible representations g_1, \dots, g_n . If χ denotes the character of g and χ_i the character of g_i then

$$\chi = \chi_1 + \dots + \chi_n.$$

Theorem 29: Let g and h be any two non-equivalent irreducible unitary representations of G , $g(x) = \|g_j^i(x)\|$, $h(x) = \|h_j^i(x)\|$ and let χ and χ' be the characters of g and h respectively. Then the following orthogonality relations hold:

$$\int g_j^i(x) \overline{h_k^l(x)} dx = 0, \quad (6)$$

$$\int \chi(x) \overline{\chi'(x)} dx = 0. \quad (7)$$

Proof. Let m and n be the degrees of the representations g and h , and let b be any constant matrix with m rows and n columns. We define $a(x) = g(x)bh(x^{-1})$ and $a = \int a(x) dx$. (The integral of a matrix valued function $a(x)$ is obtained by integrating the entries separately and is itself a matrix with the same number of rows and columns.)

We show first that $g(y)ah(y^{-1}) = a$. Indeed

$$\begin{aligned} g(y)ah(y^{-1}) &= \int g(y)g(x)bh(x^{-1})h(y^{-1})dx \\ &= \int g(yx)bh((yx)^{-1})dx = a. \end{aligned}$$

(see Definitions 33, 7). Thus we have $g(x)a = ah(x)$ for every x , and by Schur's Lemma there are only two possible cases. But if $m = n$ and a is non-singular then it follows that $h(x) = a^{-1}g(x)$ a , i. e., the representations g and h are equivalent, contrary to hypothesis. Thus $a = 0$, i. e.,

$$\int g(x)bh(x^{-1})dx = a = 0.$$

Choose now for b the special matrix with all entries zero except for a single one in the j -th row and l -th column. Then, since $h(x^{-1}) = (h(x))^*$, (see Section 31, G)) the above relation assumes the form

$$\int g_j^i(x)\bar{h}_l^k(x)dx = 0.$$

Thus (6) is established. But, since $\chi(x)$ and $\chi'(x)$ are just the sums of the functions $g_j^i(x)$ and $h_l^j(x)$, (7) is an immediate consequence of (6), and the theorem is proved.

Theorem 30: Let g be an irreducible unitary representation of G of degree r , $g(x) = \|g_j^i(x)\|$, and denote by χ the character of g :

$$\chi(x) = \sum_{i=1}^r g_j^i(x). \quad (8)$$

Then the following relations hold:

$$\int g_j^i(x)\bar{g}_j^i(x)dx = \frac{1}{r}; \quad (9)$$

moreover, if $i \neq k$ or $j \neq l$ then

$$\int g_j^i(x)\bar{g}_l^k(x)dx = 0. \quad (10)$$

Finally,

$$\int \chi(x)\bar{\chi}(x)dx = 1. \quad (11)$$

Proof. Let $b = \|b_j^i\|$ be any constant r -rowed square matrix,

and define $a(x) = g(x)bg(x^{-1})$; $a = \int a(x)dx$. Then, as above, a has the following property of invariance:

$$g(y)ag(y^{-1}) = a. \quad (12)$$

Indeed,

$$\begin{aligned} g(y)ag(y^{-1}) &= \int g(y)g(x)bg(x^{-1})g(y^{-1})dx = \\ &= \int g(yx)bg((yx)^{-1})dx = a \end{aligned}$$

so that $g(x)a = ag(x)$ for arbitrary x . Employing, this time, remark E), Section 31, we conclude that a has the form $\alpha e'$ where e' denotes the identity matrix while α is a complex number depending only on b . Thus

$$\int g(x)bg(x^{-1})dx = \alpha e'. \quad (13)$$

It remains to determine α . To this end we compute traces on both sides of (13). In the first place

$$\begin{aligned} \text{Tr}(\int g(x)bg(x^{-1})dx) &= \int \text{Tr}(g(x)bg(x^{-1}))dx = \\ &= \int \text{Tr}(b)dx = \text{Tr}(b) \end{aligned}$$

(see Section 31, B)). On the other hand, the trace of the right member of (13) is just αr . Thus $\alpha = \frac{1}{r} \text{Tr}(b)$.

Now, choosing once again for b the special matrix all of whose entries are zero except for a single one in the j -th row and l -th column, so that $\text{Tr}(b) = \delta_{jl}$, and recalling that $g(x^{-1}) = (g(x))^*$, we obtain from (13)

$$\int g_j^i(x)\bar{g}_l^k(x)dx = \frac{1}{r} \delta_k^i \delta_l^j. \quad (14)$$

But (14) is equivalent with (9) and (10) together and, once again, the validity of (11) follows immediately. Thus Theorem 30 is proved.

We now consider some further properties of characters.

B) Denote by Δ the set of all characters of irreducible complex representations G . From (7) and (11) it follows that Δ is an orthonormal set of functions defined on G . Let g be an arbitrary representation of G and let χ be its character. According to A), g splits into a system of irreducible representations so that

$$\chi(x) = \sum_{i=1}^n m_i \chi_i(x), \quad (15)$$

where m_i is a positive integer denoting the multiplicity with which the irreducible representation g_i with character χ_i appears in the representation g . Multiplying (15) by $\bar{\chi}_k(x)$ and integrating we obtain

$$m_k = \int \chi(x) \bar{\chi}_k(x) dx.$$

Thus m_k is also the Fourier coefficient of χ with respect to the system Δ . This shows, in particular, that m_k is uniquely determined by χ and hence that the character χ of a representation g determines that representation uniquely up to equivalence.

We next multiply (15) by its own complex conjugate and integrate; in this way we obtain

$$\sum_{i=1}^n m_i^2 = \int \chi(x) \bar{\chi}(x) dx. \quad (16)$$

This relation yields a criterion for the irreducibility of g ; indeed, g is irreducible when and only when its character χ satisfies the condition

$$\int \chi(x) \bar{\chi}(x) dx = 1. \quad (17)$$

If, on the other hand, g is reducible then

$$\int \chi(x) \bar{\chi}(x) dx > 1.$$

Theorem 31: If G is commutative then any irreducible representation g is of degree 1 and thus coincides with its own character χ ; $g(x) = \|\chi(x)\|$

This fact is an immediate consequence of F), Section 31.

Example 55: Let G and H be compact topological groups and denote by F their direct product. Each element $z \in F$ is then a pair (x, y) where $x \in G$, $y \in H$. Let g be an irreducible representation of G of degree m and let h be an irreducible representation of H of degree n , $g(x) = \|g_j^i(x)\|$, $h(y) = \|h_l^k(y)\|$.

Starting from g and h , we construct a representation f of the group F which will also be irreducible. To this end consider the system of double indices (i, k) where the first index in the pair varies over the set $1, \dots, m$ while the second varies over $1, \dots, n$. It is of course possible to enumerate the pairs (i, k) using the numbers $1, \dots, mn$, but it will not be necessary to do so explicitly. We now define a new mn -rowed square matrix $f(z) = \|f_{j,l}^{i,k}(z)\|$ writing $f_{j,l}^{i,k}(z) = g_j^i(x) h_l^k(y)$ where $z = (x, y)$. A straightforward computation shows that $f(z)$ is a representation of F . We shall show that this representation is irreducible. To this end denote by χ the character of f , and by χ' the characters

of g and h respectively. Then, as is easily seen, $\chi(z) = \chi'(x) \chi''(y)$, where $z = (x, y)$, and, applying to f the irreducibility criterion (17), we find:

$$\int \chi(z) \bar{\chi}(z) dz = \int \int \chi'(x) \chi''(y) \bar{\chi}'(x) \bar{\chi}''(y) dx dy = 1$$

(see Theorem 25). Thus f is irreducible. In the following paragraph it will be shown (see Example 59) that, in fact, this construction yields all the irreducible representations of F (up to equivalence).

Example 56: Let G denote, once again, the topological group considered in Examples 52 and 54, and denote by φ_n , $n = 0, \pm 1, \pm 2, \dots$ the system of functions defined in Example 54, $\varphi_n(x) = e^{2\pi i n x}$. Consider the 1-rowed matrix $g_n(x) \parallel \varphi_n(x) \parallel$. This g_n is a linear representation of G of degree 1; moreover, g_n is unitary, and the character of g_n is just the function φ_n . Now, as is shown in analysis, there exists no normalized function orthogonal to all of the functions $e^{2\pi i n x}$. From this it follows that the representations g_n constitute a complete list of the irreducible representations of G .

SECTION 33. COMPLETENESS OF THE SET OF IRREDUCIBLE REPRESENTATIONS

In this paragraph a proof is given of the Peter-Weyl Theorem which asserts the completeness of the system of continuous functions appearing as entries in the irreducible representations of a group. The proof follows [46]. Here, as in the preceding paragraph, G will denote a compact topological group, and all functions are assumed continuous.

A) A set Δ of real or complex valued functions defined on G will be said to be uniformly complete if for every real (or, respectively, complex) function f defined on G and every positive number ϵ there exist functions f_1, \dots, f_n belonging to Δ and real (or, respectively, complex) numbers $\alpha_1, \dots, \alpha_n$ such that

$$|f(x) - \sum_{i=1}^n \alpha_i f_i(x)| < \epsilon. \quad (1)$$

It is clear that a uniformly complete set of real functions is also uniformly complete if viewed as a set of complex functions.

Theorem 32: (Peter-Weyl) Denote by Ω a class of representations

of G obtained by selecting exactly one representation out of each equivalence class of unitary representations, and let Δ be the collection of all functions g_j^i appearing as entries in the representations $g \in \Omega$, $g(x) = \| g_j^i(x) \|$. Then Δ is a uniformly complete set of complex functions.

Proof: For any real valued continuous function k defined on G and satisfying the symmetry condition

$$k(z^{-1}) = k(z) \quad (2)$$

we consider the integral equation

$$\varphi(x) = \lambda \int k(x^{-1}y) \varphi(y) dy. \quad (3)$$

It follows from (2) that the kernel of (3) is symmetric:

$$k(x^{-1}y) = k(y^{-1}x).$$

Let Δ' denote the collection of all eigenfunctions of all kernels of the form $k(x^{-1}y)$. We show first that Δ' is uniformly complete.

Let f be any continuous real function defined on G . Being continuous, f is automatically uniformly continuous (see Section 28, C)); consequently, for any positive ϵ there exists a neighborhood U of the identity e such that

$$|f(x) - f(y)| < \frac{\epsilon}{2}, \quad (4)$$

when $x^{-1}y \in U$. It is no loss of generality to suppose $U^{-1} = U$. Let V be a neighborhood of e such that $\bar{V} \subset U$. By Urysohn's Lemma there exists a continuous function q satisfying the conditions: $0 \leq q(z) \leq 1$ for every $z \in G$, $q(z) = 0$ for $z \in G \setminus U$, $q(z) = 1$ for $z \in \bar{V}$. Let $k'(z) = \alpha(q(z) + q(z^{-1}))$ where α is a positive real number chosen so that $\int k'(z) dz = 1$. Then k' vanishes outside of U and satisfies the symmetry condition (2). We next define

$$f'(x) = \int k'(x^{-1}y) f(y) dy.$$

Thanks to (4) and the special choice of k' we have

$$|f(x) - f'(x)| < \frac{\epsilon}{2}. \quad (5)$$

Indeed

$$|f'(x) - f(x)| = \left| \int k'(x^{-1}y) (f(y) - f(x)) dy \right| \leq \int k'(x^{-1}y) \frac{\epsilon}{2} dy = \frac{\epsilon}{2}.$$

But now, according to proposition D), Section 30, f' may be expanded in a uniformly convergent series

$$f'(x) = \varphi_1(x) + \dots + \varphi_n(x) + \dots, \quad (6)$$

where φ_i , $i = 1, 2, \dots$, are eigenfunctions of the kernel $k'(x^{-1}y)$. Consequently, for sufficiently large n , the real function

$$f''(x) = \sum_{i=1}^n \varphi_i(x) \quad (7)$$

satisfies

$$|f'(x) - f''(x)| < \frac{\varepsilon}{2}. \quad (8)$$

It follows that

$$|f(x) - f''(x)| < \varepsilon. \quad (9)$$

Since the functions φ_i , $i = 1, \dots, n$, all belong to Δ' and ε is arbitrarily small, it follows that Δ' is uniformly complete.

Denote now by Δ' the collection of all complex functions g_j^i appearing as entries in any (not necessarily irreducible) representation g of G , $g(x) = \|g_j^i(x)\|$. Our next step is to show that Δ' is uniformly complete. To this end it suffices, of course, to show that every function of Δ' can be expressed as a finite linear combination (with constant coefficients) of functions belonging to Δ' .

Let φ' be any function of Δ' . Then φ' satisfies equation (3) for some kernel $k(x^{-1}y)$ and some eigenvalue λ' . Let

$$\varphi_1(x), \dots, \varphi_n(x) \quad (10)$$

be an orthonormal basis in the eigenspace of the kernel $k(x^{-1}y)$ belonging to λ' . Then φ' is a linear combination of the functions (10). Thus it suffices to show that the latter functions are linear combinations of functions belonging to Δ' .

Now because of the special form of the kernel in (3) it turns out that if $\varphi(x)$ satisfies (3) for some value of λ then so does $\varphi(ax)$. Indeed, substituting ax for x in (3) and using the invariance of the integral to replace y by ay , we obtain

$$\varphi(ax) = \lambda \int k(x^{-1}a^{-1}ay) \varphi(ay) dy = \lambda \int k(x^{-1}y) \varphi(ay) dy.$$

Thus the functions

$$\varphi_1(ax), \dots, \varphi_n(ax) \quad (11)$$

are also solution of (3) for $\lambda = \lambda'$ and consequently may be expressed as linear combinations of the basic system (10). Accordingly we obtain

$$\varphi_i(ax) = \sum_{j=1}^n g_j^i(a) \varphi_j(x). \quad (12)$$

Moreover, the system (11) is still orthonormal for

$$\int \varphi_i(ax) \varphi_j(ax) dx = \int \varphi_i(x) \varphi_j(x) dx = \delta_{ij}.$$

In particular, the functions (11) are linearly independent, whence it follows that the matrix $g(x) = ||g_j^i(x)||$ is non-singular. (In fact, $g(x)$ is an orthogonal matrix, but that is of no consequence to us.) Multiplying (12) by $\varphi_k(x)$ and integrating we obtain

$$g_k^{-1}(a) = \int \varphi_1(ax) \varphi_k(x) dx$$

which shows that g_j^{-1} is continuous (see Section 29, J)). We next compute $g(ab)$. Grouping the product abx in equation (12) in two different ways, we obtain, on the one hand,

$$\varphi_1(abx) = \sum_{j=1}^n g_j^{-1}(ab) \varphi_j(x) \quad (13)$$

and, on the other hand,

$$\varphi_1(abx) = \sum_{k=1}^n g_k^{-1}(a) \varphi_k(bx) = \sum_{k,j=1}^n g_k^{-1}(a) g_j^k(b) \varphi_j(x). \quad (14)$$

Equating the right members of (13) and (14) yields

$$g_j^{-1}(ab) = \sum_{k=1}^n g_k^{-1}(a) g_j^k(b),$$

or in other words

$$g(ab) = g(a) g(b). \quad (15)$$

From (15) and the continuity of the function g_j^{-1} we conclude that g is a linear representation of G . Thus the functions

$$g_j^{-1} \quad (16)$$

all belong to Δ' .

We now return once more to equation (12) and evaluate it at $x = e$, thus obtaining

$$\varphi_1(a) = \sum_{j=1}^n g_j^{-1}(a) \varphi_j(e).$$

Thus the functions belonging to the system (10) are expressed as linear combinations of the functions (16), i.e., of functions belonging to Δ' , and it follows that the system Δ' is uniformly complete.

By definition the functions of Δ all belong to Δ' , $\Delta \subset \Delta'$. The proof of the theorem will be completed by showing that every function of Δ' is expressible as a linear combination of functions belonging to Δ .

Let p be any function belonging to Δ' . There exists, then, a representation of G , $g(x) = ||g_j^{-1}(x)||$, such that p is one of the functions

$$g_j^{-1}. \quad (17)$$

According to I), Section 31, and Theorem 28, there exists a constant matrix t such that

$$g(x) = th(x)t^{-1}, \quad (18)$$

where $h(x)$ has the special form

$$h(x) = \begin{vmatrix} g_1(x) & 0 & \dots & 0 \\ 0 & g_2(x) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & g_n(x) \end{vmatrix},$$

the functions

$$g_i, \quad i = 1, \dots, n, \quad (19)$$

being irreducible unitary representations of G . Moreover, by choosing t appropriately we may arrange matters so that the representations (19) all belong to Ω since Ω contains, by hypothesis, an irreducible representation equivalent with any given irreducible representation. But now if the representations (19) belong to Ω then (18) itself yields an expression for each of the functions (17) as a linear combination of functions belonging to Δ . In particular this holds for the function p , and the uniform completeness of Δ is demonstrated.

The following corollary of Theorem 32 plays a decisive role in the theory of compact groups.

Theorem 33: For any element a of a compact group G , distinct from the identity e , there exists an irreducible representation of G such that $g(a)$ is not the identity matrix.

Proof: Since $a \neq e$ it follows from Urysohn's Lemma that there exists a continuous function f defined on G such that $f(a) \neq f(e)$. If, contrary to assertion, it were the case that $g(a) = g(e)$ for every irreducible representation g then we would have also $g_j^{-1}(a) = g_j^{-1}(e)$ for all functions of the system Δ constructed in Theorem 32. But this would make it impossible to approximate f by linear combinations of such functions since $f(a) \neq f(e)$. Thus the theorem is proved.

We turn now to the consideration of the set of characters.

Theorem 34: Denote by Σ the collection of all characters of irreducible complex representations of G . We shall say that a complex function f defined on G is invariant if for every $a \in G$ we have

$$f(a^{-1}xa) = f(x). \quad (20)$$

According to (5), Section 32, the functions belonging to Σ are invariant. It turns out that Σ is uniformly complete in the set of all invariant complex functions on G . In other words, given an invariant function f and a positive ε , there exists a linear combination $f'(x) = \sum_{i=1}^n c_i \chi_i(x)$ of characters $\chi_i \in \Sigma$, $i = 1, \dots, n$, such that

$$|f(x) - f'(x)| < \varepsilon. \quad (21)$$

Proof: Let g be an irreducible unitary representation of G , $g(x) = \|g_j^i(x)\|$ and suppose some function of the form

$$p(x) = \sum_{i,j=1}^r b_i^j g_j^i(x) \quad (22)$$

is invariant, where r is the degree of g . We begin by showing that this implies

$$p(x) = \alpha \chi(x), \quad (23)$$

where χ is the character of g and α is a complex constant.

Indeed, by hypothesis,

$$\begin{aligned} p(a^{-1}xa) &= \sum_{i,j=1}^r b_i^j g_j^i(a^{-1}xa) = \\ &= \sum_{i,j,k=1}^r b_i^j g_k^i(a^{-1}) g_k^j(x) g_j^i(a) = p(x). \end{aligned} \quad (24)$$

But now, the functions g_j^i are linearly independent (see Theorem 30) so the coefficients in (22) and (24) must coincide, i.e.,

$$b_k^1 = \sum_{i,j=1}^r g_j^i(a) b_i^j g_k^i(a^{-1}).$$

Expressed in matrix form this relations reads $b = g(a) b g(a^{-1})$ where $b = \|b_j^i\|$, or, what comes to the same thing, $g(a) b = b g(a)$. Hence, according to E), Section 31, $b = \alpha e'$ where e' denotes the identity matrix and α is a complex number. But then (22) assumes the form (23).

Next let q be any invariant function defined on G which is a finite linear combination of functions belonging to the system Δ constructed in Theorem 32. Then q may be resolved into a finite series of

partial sums p_i , $q(x) = \sum_{i=1}^n p_i(x)$, where each p_i has the form (22)

i.e., is a linear combination composed of functions belonging to one and the same irreducible representation $g^{(1)}$. Since q is invariant it follows that all of the functions p_i are also invariant. Indeed, $p_i(a^{-1}xa)$, considered as a function of x , is a linear combination of the functions appearing as entries in $g^{(1)}$ (see (24)) and from this and the linear independence of Δ it follows that in the equation

$$\sum_{i=1}^n p_i(a^{-1}xa) = \sum_{i=1}^n p_i(x)$$

equality must hold termwise, i.e., $p_i(a^{-1}xa) = p_i(x)$, $i = 1, \dots, n$. But then each p_i has the form $p_i = \alpha_i \chi_i$ whence

$$q(x) = \sum_{i=1}^n \alpha_i \chi_i(x). \quad (25)$$

Finally, let f be any invariant function on G . By Theorem 32 there exists a finite linear combination f' of functions belonging to Δ such that

$$|f(x) - f'(x)| < \varepsilon, \quad (26)$$

where ε is any preassigned positive number. From (26) it follows that

$$\left| \int f(a^{-1}xa) da - \int f'(a^{-1}xa) da \right| < \varepsilon. \quad (27)$$

But now, f is invariant so that $\int f(a^{-1}xa) da = f(x)$, and if we write $q(x) = \int f'(a^{-1}xa) da$ then (27) assumes the form

$$|f(x) - q(x)| < \varepsilon.$$

Since $f'(x)$ is a linear combination of functions belonging to Δ the same is true of $f'(a^{-1}xa)$ considered as a function of x (see (24)) and hence also of q . Moreover, it follows easily from the invariance of the integral that q is invariant. But then, by what has been shown, q possesses an expression of the form (25) and the theorem follows.

The following result follows from Theorem 34 just as Theorem 33 followed from Theorem 32.

Theorem 35: Let a and b be non-conjugate elements of G , i.e., suppose there does not exist an element $c \in G$ for which $b = c^{-1}ac$. Then there exists a character χ belonging to an irreducible representation of G such that $\chi(a) \neq \chi(b)$.

Proof: The set B of all elements conjugate with b is compact since it is the image of the compact space G under the continuous mapping $y \rightarrow y^{-1}by$. It follows from Urysohn's Lemma that there exists a non-negative function f vanishing on B and positive at the point a . But then, as is easily seen, the function $\varphi(x) = \int f(y^{-1}xy) dy$ is invariant and satisfies $\varphi(b) = 0$, $\varphi(a) \neq 0$. Thus, by Theorem 34, φ may be uniformly approximated by linear combinations of functions belonging to Σ . In particular Σ must contain functions taking distinct values at the points a and b .

Example 57: Let R be a compact Hausdorff space and let Δ be

any uniformly complete set of, say, real functions defined on R . We shall show that the cardinality of Δ is not less than the weight of R .

If M is a finite subset of R , consisting of r points, we may assign to every real function f defined on R the corresponding function f' defined on M by $f'(x) = f(x)$, $x \in M$. It is an easy consequence of Urysohn's Lemma that there exists on R a continuous function taking arbitrarily prescribed values at the points of M . Thus the set of functions of the form f' coincides with the set of all functions on M and forms an r -dimensional vector space. If now Δ' denotes the set of functions of the form φ' , $\varphi \in \Delta$, then since Δ is uniformly complete on R it follows that Δ' is uniformly complete on M . But, now, the set of all functions on M is an r -dimensional vector space whence it follows that Δ' , and hence also Δ , must contain at least r functions. Thus if R is finite, consisting of precisely r points, then the cardinality of Δ is at least r and hence at least as great as the weight of R . Moreover, if R is infinite then Δ must be infinite also.

Suppose now that R is infinite and denote by Δ^* the set of all finite linear combinations with rational coefficients of functions belonging to Δ . Since Δ is infinite the cardinality of Δ^* is the same as that of Δ . Next we assign to each function $f \in \Delta^*$ the open set U_f consisting of those points $x \in R$ such that $f(x) > \frac{1}{2}$ and consider the set Σ consisting of the open sets U_f , $f \in \Delta^*$. Since the cardinality Σ does not exceed that of Δ^* it suffices to show that Σ is a base. To this end let a be a point of R and let V be any neighborhood of a . By Urysohn's Lemma there exists a non-negative function f on R vanishing outside $R \setminus V$ and equal to one at a , and from the uniform completeness of Δ it follows that there exists a function $f \in \Delta^*$ such that $|g(x) - f(x)| < \frac{1}{4}$. But, then, for this f we have $a \in U_f \subset V$ and the proof is complete.

Example 58: Putting together Theorems 29 and 32 and the results obtained in Examples 53 and 57 we conclude that the cardinality of the set of equivalence classes of irreducible representations of an infinite compact group G is precisely the weight of the space G .

Example 59: We here conclude the investigation begun in Example 55. Let Σ' denote the collection of all characters of irreducible representations of a group G , Σ'' the collection of all characters of irreducible representations of a group H , and denote by Σ the collection of all functions $\chi(z) = \chi'(x) \chi''(y)$ where $z = (x, y)$, $\chi' \in \Sigma'$, $\chi'' \in \Sigma''$. It was shown in Example 55 that all

the functions of the system Σ are characters of irreducible representations of $F = G \times H$. We shall show that, in fact, Σ consists exactly of the characters of all irreducible representations of F .

To begin with, let us see that Σ is uniformly complete in the set of all invariant functions on F . Let f be an invariant function defined on F . By Theorem 7 there exists a function $\varphi(x, y) = g_1(x) h_1(y) + \dots + g_n(x) h_n(y)$ which satisfies the condition $|f(x, y) - \varphi(x, y)| < \epsilon$ where ϵ is an arbitrary preassigned positive number. We define

$$g'_1(x) = \int g_1(a^{-1}xa) da, \quad h'_1(y) = \int h_1(b^{-1}yb) db, \quad i = 1, \dots, n,$$

$$\varphi'(x, y) = \int \int \varphi(a^{-1}xa, b^{-1}yb) da db.$$

It is clear that $\varphi'(x, y) = g'_1(x) h'_1(y) + \dots + g'_n(x) h'_n(y)$ and that $|f(x, y) - \varphi'(x, y)| < \epsilon$. Moreover it is easily seen that the functions g'_1, \dots, g'_n and h'_1, \dots, h'_n are invariant on G and H respectively. Accordingly, they may be uniformly approximated with arbitrary accuracy by means of linear combinations of functions belonging to Σ' and Σ'' . But from this and the inequality $|f(x, y) - \varphi'(x, y)| < \epsilon$ it follows that f also may be uniformly approximated with arbitrary accuracy by means of linear combinations of functions belonging to Σ .

We now show that Σ contains the characters of all the irreducible representations of F . Indeed, suppose the contrary and let χ be the character of an irreducible representation of F which does not belong to Σ . Then χ is orthogonal to all the functions of Σ . On the other hand there exists a linear combination $\psi(z) = \alpha_1 \chi_1(z) + \dots + \alpha_n \chi_n(z)$ of functions belonging to Σ which satisfies the condition $|\chi(z) - \psi(z)| < 1$. Thus we have $(\chi - \psi, \chi - \psi) = 1 + \alpha_1 \bar{\alpha}_1 + \dots + \alpha_n \bar{\alpha}_n < 1$, which is impossible.

Thus the construction given in Example 55 yields all the irreducible representations of the direct product F starting from the irreducible representations of the direct factors G and H .

Example 60: We shall give an application of the theory of linear representations to the theory of almost periodic functions.

A continuous complex valued function f of real variable t , $-\infty < t < +\infty$, is said to be almost periodic if every sequence of functions $f_{a_1}, \dots, f_{a_n}, \dots$ of the form $f_{a_i}(t) = f(t + a_i)$, where a_i are arbitrary real numbers, contains a uniformly convergent subsequence.

The simplest example of an almost periodic function is the periodic function $e^{i\lambda t}$ where λ is an arbitrary real number and $i = \sqrt{-1}$. Denote by Δ the collection of all functions of the form $e^{i\lambda t}$. We shall show that Δ is uniformly complete in the set of almost periodic

functions. As it happens, this fact is a fundamental theorem in the theory of almost periodic functions.

Let f be a fixed almost periodic function and denote by H the set of all functions of the form $f(t + a)$, where a is a real number. Denote also by G the set of all functions obtainable as limits of uniformly convergent sequences of functions belonging to H . Then G is compact in the sense of uniform convergence, constitutes a separable compact topological space, and H is dense in G . We define in H an operation of addition by writing $f_a + f_b = f_{a+b}$. This operation, originally defined only on H , extends uniquely by continuity to the larger set G and in this way G is turned into a commutative separable compact topological group. To this group G the entire theory of linear representations is applicable. Let g_1, \dots, g_n, \dots denote the collection of all irreducible representations of G . Since these representations are all of degree 1 by Theorem 31, each g_n is simply a homomorphism of G into the multiplicative group K of complex numbers of absolute value one. Thus $g_n(f_a)$ is a complex number of absolute value one such that

$$g_n(f_{a+b}) = g_n(f_a)g_n(f_b),$$

Hence, if we regard $g_n(f_a)$ as a function of the parameter a , we obtain a homomorphism of the additive group of real numbers into the group K . From this we conclude immediately that $g_n(f_a) = e^{i\lambda n^a}$ since every such homomorphism is of this form (see Section 36, F)).

To each function $x \in G$ of the variable t we now associate its value $x(0)$ at the point $t = 0$. The continuous function φ thus defined on G , $\varphi(x) = x(0)$, can, by Theorem 32, be uniformly approximated by linear combinations of the functions g_n . Considering such an approximation on H only, and observing that $\varphi(f_a) = f(a)$ while $g_n(f_a) = e^{i\lambda n^a}$, we obtain the desired approximation of the almost periodic function f by means of linear combination of the functions $e^{i\lambda n^t}$.

6

LOCALLY COMPACT COMMUTATIVE GROUPS

The present chapter is devoted to the detailed investigation of locally compact commutative topological groups. All the questions that arise here can be answered in full or at least reduced to questions bearing on commutative algebraic groups.

The fundamental method of investigation is the study of the relation (duality) between a given group and its character group. To every locally compact commutative topological group G there is associated another locally compact commutative group X known as the character group of G . The correspondence between G and X turns out to be symmetric; that is, the given group G may in a natural way be viewed as the character group of X . This definitely non-trivial fact is the central result of the chapter and is indeed the fundamental duality theorem from which other duality relations, a number of which will be discussed below, follow as comparatively easy consequences. Thus with every subgroup H of G we associate a subgroup Φ of X known as the annihilator of H and this correspondence between the subgroups H and Φ is also symmetric. Moreover, Φ is the character group of G/H while X/Φ is the character group of H .

If G is discrete then X is compact, and conversely. This makes it possible to regard an arbitrary compact commutative group X as the character group of a discrete commutative group G . Taking this point of view, and exploiting the various duality relations between G and X , it becomes possible to reduce, in large measure, the study of compact groups to the study of discrete groups. From the point of view of the structure problem for commutative topological groups, as well as from the point of view of applications, this is the most essential result of the whole chapter. Accordingly, the theory of duality is first presented for compact

and discrete groups. Thus the development is such that the reader may become familiar with this portion of duality theory without immersing himself in the details of the proof of the duality theorem in the general locally compact case. Indeed, the duality between compact and discrete groups will be applied to the investigation of the structure of locally compact groups, and only then will the duality theorem be developed in the general case.

It was shown in the preceding chapter that every irreducible representation of a commutative group G is of degree one, i.e., coincides with its own character. It turns out that the set of all characters of a group G is itself in a natural way a group, called the character group of G . Let us consider the definition of this group in more detail. Let g be an irreducible unitary representation of G ; being of degree one, g is just a homomorphism of G into the group of complex numbers of absolute value one. If g and h are two such homomorphisms then the mapping f defined by the formula $f(x) = g(x)h(x)$ is also a homomorphism of G into the group of complex numbers of absolute value one. In this way a product is defined in the set of characters. In an equally natural way a topology may be introduced.

In essence the results of the present chapter are due to me [44, 45]. A number of important generalizations and improvements obtained by van Kampen [20, 21] are also taken into account here. Moreover, we shall make use of certain simplifications discovered by A. Weil [56].

All topological groups appearing in the chapter are commutative and locally compact. These conditions will be assumed satisfied at all times, even though this will not always be explicitly stipulated. Since all groups under consideration are commutative we shall employ the additive notation. In view of that, it will be convenient to replace the multiplicative group of complex numbers of absolute value with an isomorphic additive group K . Since this group will play a basic role throughout the entire investigation, the symbol K will be reserved for it throughout the chapter.

SECTION 34 THE CHARACTER GROUP

In this section the character group X of a locally compact group G is defined and it is shown that X itself is also locally compact. At the same time, it will be seen that if G is compact then X is discrete, while, dually, if G is discrete then X is compact. We also introduce the natural homomorphism ω of G into the

character group G' of the group X . The significance of the homomorphism ω will become clear in subsequent sections: it will be shown that ω is, in fact, an isomorphism of G onto the entire group G' . This is the precise formulation of the fundamental duality theorem referred to in the introduction to the chapter.

A) Let D denote the additive topological group of real numbers in its natural topology and let N denote the subgroup of integers. We shall denote by K the factor group $K = D/N$, and by κ the natural projection of D onto K (see Section 20, B)). The group K is compact and separable. The set of all elements in K of the form $\kappa(d)$ where $|d| < 1/3k$ (k a positive integer) we denote by Λ_k . The open sets $\Lambda_1, \Lambda_2, \dots$ constitute a complete system of neighborhoods of zero in K . It may be easily verified that if some element $\gamma \in K$ satisfies the conditions $\gamma \in \Lambda_1, 2\gamma \in \Lambda_1, \dots, k\gamma \in \Lambda_1$ then $\gamma \in \Lambda_k$. It follows from this that if α is a homomorphism of an arbitrary group G into K satisfying the condition $\alpha(G) \subset \Lambda_1$ then α is the zero homomorphism, i.e., $\alpha(G) = \{0\}$. Indeed, for $x \in G$ we have $k\alpha(x) = \alpha(kx) \in \Lambda_1$ so that $\alpha(x) \in \Lambda_k$ for arbitrary k ; thus $\alpha(x) = 0$.

Definition 36: Let G be a locally compact commutative group. A homomorphism of G into K will be called a character of G and the set of all characters of G will be denoted by X . If $x \in G, \alpha \in X$, we shall write αx instead of $\alpha(x)$. Moreover, if $A \subset G$ and $M \subset K$ are any subsets of G and K then we denote by $W(A, M)$ the set of all characters $\alpha \in X$ satisfying the condition $\alpha(A) \subset M$.

The set X will now be turned into a commutative topological group called the character group of G . In the first place, the sum $\alpha + \beta$ of two characters α and β of the group G is defined by the equation $(\alpha + \beta)x = \alpha x + \beta x$. It may be immediately verified that the mapping $\alpha + \beta$ of G into K thus defined is again a homomorphism and therefore belongs to X . The zero of the group X is the zero homomorphism, while the negative of an element $\alpha \in X$ is just the element $-\alpha$ defined by $(-\alpha)x = -(\alpha x)$. In the second place we define a topology in X as follows: the collection Σ^* of all sets of the form $W(F, \Lambda_k)$, where F is compact, satisfies the conditions of Theorem 9 and is designated as a complete system of neighborhoods of zero in X .

Theorem 36: Let G be a locally compact commutative group and let X be its character group. Then X is also locally compact. More precisely, if U is a neighborhood of zero in G having compact closure then $W(\bar{U}, \Lambda_4)$ is a neighborhood of zero in X having compact closure. Moreover, if G is compact then X is discrete, while

if G is discrete then X is compact.

The proof is quite simple in the compact and discrete cases and I treat these cases first and independently of the general case in order that the reader may, if he so desires, limit his attention to them.

Proof: If G is compact then Σ^* contains in particular the neighborhood $W(G, \Lambda_1)$ which, according to A), contains only the zero of X ; thus in this case X is discrete.

Suppose next that G is discrete. To every element $x \in G$ we associate an exemplar K_x of the group K and form the compact direct sum T (in multiplicative notation, the direct product; see Definition 29) of all the groups K_x . An element $\alpha \in T$ may be viewed as a function defined on G and taking values in K if we agree to write $\alpha(x) = \alpha(K_x)$. Among these functions the characters of G are distinguished by the condition $\alpha(x+y) = \alpha(x) + \alpha(y)$, $x, y \in G$. But each of these conditions (for fixed x and y) defines a closed subset of T . Hence the collection X of all characters of G is also closed in T and is therefore compact. It remains only to show that the topology defined on X in Definition 36 coincides with the topology it receives as a subspace of T , and this is an immediate consequence of the fact that only finite subsets of the discrete space G are compact.

Finally, let G be an arbitrary locally compact commutative group. We must show that the closure $\overline{W(\bar{U}, \Lambda_4)}$ of the neighborhood $W(\bar{U}, \Lambda_4)$ is compact in X . But now, as is easily verified, $\overline{W(\bar{U}, \Lambda_4)} \subset W(\bar{U}, \bar{\Lambda}_4)$. Thus it suffices to verify the compactness of $W(\bar{U}, \bar{\Lambda}_4)$.

Let G' denote the topological group obtained by replacing the given topology in G by the discrete topology and let X' denote the character group of G' . We denote also by $W'(\bar{U}, \bar{\Lambda}_k)$ the set of all characters α' of the discrete group G' satisfying the conditions $\alpha'(\bar{U}) \subset \bar{\Lambda}_k$ and show first of all that $W(\bar{U}, \bar{\Lambda}_4) = W'(\bar{U}, \bar{\Lambda}_4)$. To this end it suffices to prove that every character α' of G' satisfying the condition $\alpha'(\bar{U}) \subset \bar{\Lambda}_4$ is also a character of G , i.e., is continuous on G . For given k let V be a neighborhood of zero in G such that $kV \subset U$ and let $x \in V$. Then all the elements $\alpha'(x), 2\alpha'(x), \dots, k\alpha'(x)$ belong to $\bar{\Lambda}_4 \subset \Lambda_1$ so that $\alpha'(x) \in \Lambda_k$ (see A)). Thus for each neighborhood Λ_k we find a neighborhood V of zero in G such that $\alpha'(V) \subset \Lambda_k$ and it follows that α' is continuous.

We show next that $W'(\bar{U}, \bar{\Lambda}_4)$ is closed in X' . To see this note that each individual condition $\alpha'(x) \in \Lambda_4$ (for fixed x) defines a closed subset of X' since $\bar{\Lambda}_4$ is closed. But then the collection of all such conditions for $x \in \bar{U}$ similarly defines a closed set.

The proof of the theorem will now be completed by showing

that the topology induced on the set $W'(\bar{U}, \bar{\Lambda}_4)$ is the same whether we regard it as a subspace of X or of X' . Let $\alpha \in W'(\bar{U}, \bar{\Lambda}_4)$. In the topology induced by X a general neighborhood of α consists of all elements $\alpha + \xi \in W'(\bar{U}, \bar{\Lambda}_4)$, $\xi \in W(F, \Lambda_k)$, where F denotes a compact set in G and k is a positive integer. On the other hand, the general neighborhood of α in the topology induced by X' consists of all elements $\alpha + \xi' \in W'(\bar{U}, \bar{\Lambda}_4)$, $\xi' \in W(A, \Lambda'_k)$ where A is a finite subset of G and k' is again a positive integer. Since a finite set is compact it is clear that every neighborhood of the second type is also a neighborhood of the first type. The problem is to show that, conversely, every neighborhood of the first type contains a neighborhood of the second type. This will show that the two topologies do indeed coincide and will complete the proof of the theorem.

Fix now an arbitrary neighborhood of the first type, i.e., fix F and k , and choose in G a neighborhood V' of zero such that $2kV' \subset U$. Since the collection of open sets $a + V'$, $a \in F$, covers F and F is compact it follows that there exists a finite set $A \subset F$ such that $A + V' \supset F$. Suppose now that $\xi' \in W'(A, \Lambda_{2k})$ and that $\alpha + \xi' \in W'(\bar{U}, \bar{\Lambda}_4)$. Then, by what was shown above, $\xi' = (\alpha + \xi') - \alpha$ is continuous on G . Moreover, $\xi'(\bar{U}) \subset \bar{\Lambda}_2$. Thus, if $x \in V'$ then $\xi'(x), 2\xi'(x), \dots, 2k\xi'(x)$ all belong to $\bar{\Lambda}_2 \subset \bar{\Lambda}_1$, whence it follows (see A)) that $\xi'(x) \in \Lambda_{2k}$. In other words, $\xi'(V') \subset \Lambda_{2k}$. But then $\xi'(F) \subset \xi'(A + V') \subset \Lambda_{2k} + \Lambda_{2k} \subset \Lambda_k$ so that $\xi' \in W(F, \Lambda_k)$ and the proof is complete.

In Section 40 we shall round out Theorem 36 by showing that the spaces G and X have the same weight. The proof of this assertion rests, however, on the fundamental duality theorem and we here content ourselves with the following fragment of the general results.

B) Let X be the character group of G . If the weight of G is infinite then the weight of X does not exceed the weight of G .

Let τ be the weight of G and let Σ be a base in G having cardinality τ and consisting exclusively of open sets with compact closure. Let also Δ be an arbitrary countable base in the space K . If U_1, \dots, U_n are neighborhoods belonging to Σ and M_1, \dots, M_n are neighborhoods belonging to Δ we denote by $W(\bar{U}_1, \dots, \bar{U}_n; M_1, \dots, M_n)$ the set of all elements $\xi \in X$ satisfying the conditions $\xi(\bar{U}_i) \subset M_i$, $i = 1, \dots, n$. Let Σ^* denote the collection of all sets of the form $W(\bar{U}_1, \dots, \bar{U}_n; M_1, \dots, M_n)$. According to the theory of cardinal numbers the cardinality of Σ^* does not exceed τ . Thus B) will be proved if we show that Σ^* is a base for X .

In the first place $W(\bar{U}_1, \dots, \bar{U}_n; M_1, \dots, M_n)$ is open in X. Since

$$W(\bar{U}_1, \dots, \bar{U}_n; M_1, \dots, M_n) = W(\bar{U}_1, M_1) \cap \dots \cap W(\bar{U}_n, M_n)$$

this amounts to showing that each set $W(\bar{U}_i, M_i)$ is open in X. But, now, as it happens every set of the form $W(F, M)$ is open in X where F is compact in G and M is open in K. Indeed, let $\alpha \in W(F, M)$. Then $\alpha(F)$ is a compact subset of the open set M. Thus there exists a neighborhood Λ_k of zero in K such that $\alpha(F) + \Lambda_k \subset M$. But then $\alpha + W(F, \Lambda_k) \subset W(F, M)$ which shows that $W(F, M)$ is open.

We now show that Σ^* is a base in X. Since open sets of the form $W(F, \Lambda_k)$ form a base at zero it follows that the sets of the form $\alpha + W(F, \Lambda_k)$, $\alpha \in X$, form a base of the entire space. We must show that if $\beta \in \alpha + W(F, \Lambda_k)$ then there exists a set $W \in \Sigma^*$ such that $\beta \in W \subset \alpha + W(F, \Lambda_k)$. Since $\beta \in \alpha + W(F, \Lambda_k)$ it follows that for some sufficiently large positive integer h we have $\beta + W(F, \Lambda_h) \subset \alpha + W(F, \Lambda_k)$. Now for every $x \in F$ there exists a neighborhood $M_x \in \Delta$ such that $\beta(x) \in M_x \subset \beta(x) + \Lambda_{2h}$. Moreover, since β is continuous, there exists in Σ a neighborhood U_x of the point x such that $\beta(U_x) \subset M_x$. But then, selecting a finite covering U_{x_1}, \dots, U_{x_n} of F from among the open sets U_x , $x \in F$, we obtain

$$\beta \in W(\bar{U}_{x_1}, \dots, \bar{U}_{x_n}; M_{x_1}, \dots, M_{x_n}) \subset \beta + W(F, \Lambda_h).$$

Definition 37. Let X be the character group of a group G and denote by G' the character group X. To each element $x \in G$ we associate the mapping x' of X into K defined by the formula $x'(\xi) = \xi(x)$, $\xi \in X$. Then $x' \in G'$ and the mapping ω defined by $\omega(x) = x'$ is a homomorphism of G into G' . The mapping ω is called the natural homomorphism of G into its second character group G' .

We must show that $x' \in G'$. In the first place,

$$x'(\xi + \eta) = (\xi + \eta)x = \xi x + \eta x = x'(\xi) + x'(\eta)$$

Thus x' is a homomorphism of the algebraic group X into K. In the second place, if Λ_k is a given neighborhood of zero in K then $x'(W(x, \Lambda_k)) \subset \Lambda_k$ so that $W(x, \Lambda_k)$ is a neighborhood of zero in X that is carried into Λ_k by the mapping x' . It follows that x' is a character of the topological group X.

It remains to show that the mapping ω is homomorphic. To this end we observe first that

$$\begin{aligned}\omega(x+y)\xi &= \xi(x+y) = \xi(x) + \xi(y) = \omega(x)\xi + \omega(y)\xi \\ &= (\omega(x) + \omega(y))\xi.\end{aligned}$$

Thus ω is a homomorphism of the algebraic group G into G' . To show that ω is continuous let $U' = W(\Phi, \Lambda_k)$ be any fixed neighborhood of zero in G' (here Φ denotes a compact subset of X) and choose any neighborhood U_0 of zero in the group G such that the closure \overline{U}_0 is compact. Let $W = W(\overline{U}_0, \Lambda_{2k})$. The open sets of the form $\xi + W$, $\xi \in \Phi$, cover Φ so there exists a finite covering consisting of sets $\xi_1 + W, \dots, \xi_r + W$. Choose now neighborhoods U_i of zero in G such that $\xi_i(U_i) \subset \Lambda_{2k}$, $i = 1, \dots, r$ and let $U = U_0 \cap U_1 \cap \dots \cap U_r$. If $\xi \in \Phi$ then for some i , $1 \leq i \leq r$, we have $\xi = \xi_i + \xi_0$ where $\xi_0 \in W$. But then $\xi(U) = \xi_i(U) + \xi_0(U) \subset \Lambda_{2k} + \Lambda_{2k} = \Lambda_k$. In other words, if $x \in U$ then $\omega(x)\xi = \xi x \in \Lambda_k$, i.e., $\omega(U) \subset U'$. Thus ω is continuous.

The following proposition is the one consequence of the theory of linear representations needed in the present chapter.

C) For every element $a \neq 0$ in a compact commutative group G there exists a character α such that $\alpha(a) \neq 0$.

Indeed, since G is commutative it follows from Theorem 31 that all of its irreducible representations are of the first degree while, according to Theorem 33, there exists an irreducible representation g of G such that $g(a) \neq 1$. Let $\alpha(x) = \frac{\log g(x)}{2\pi i}$. This formula defines the real number $\alpha(x)$ up to an additive integral constant and therefore defines $\alpha(x)$ as an element of K . Thus α is a character of G and since $g(a) \neq 1$ we have $\alpha(a) \neq 0$.

Example 61: Let G_p denote the additive group of p -adic integers (see Section 26, C)). The elements $x \in G_p$ may be written as formal series $x = x_0 + x_1 p + \dots + x_k p^k + \dots$ where the coefficients x_i are integers satisfying the inequality $0 \leq x_i < p$, $i = 0, 1, 2, \dots$. Denote by U_k the subgroup of G_p consisting of the elements x for which $x_0 = x_1 = \dots = x_{k-1} = 0$. The subgroups $G_p = U_0, U_1, \dots$ are open, compact, and form a base at 0. Let $g = 1 + 0p + \dots + 0p^k + \dots$. It is easy to see that the multiples of g are everywhere dense in G_p . We shall show that the character group X_p of G_p is the quasi-cyclic group of order p , i.e., is isomorphic with the subgroup K_p of the algebraic group K consisting of elements of the form $\kappa \frac{m}{p^k}$ where m and k are integers.

Indeed let $\alpha \in X_p$. Since α is a continuous mapping of G_p into K there exists a neighborhood U_k of 0 in G_p such that $\alpha(U_k) \subset \Lambda_1$

and therefore $\alpha(U_k) = 0$ (see A)). Denote by f the natural projection of G_p onto the factor group G_p/U_k . Since $\alpha(U_k) = 0$ there exists a homomorphism β of G_p/U_k into K such that $\alpha = \beta f$. But, now, as is easily seen, the group G_p/U_k is a cyclic group of order p^k generated by $f(g)$ while every element γ of K satisfying the condition $p^k \gamma = 0$ may be written in the form $\gamma = \chi(m/p^k)$. Thus $\alpha(g) = \beta f(g) = \chi(m/p^k)$ and the mapping $\alpha \rightarrow \alpha(g)$ is an isomorphism of X_p onto K_p .

SECTION 35

CHARACTER GROUPS OF FACTOR GROUPS AND OF OPEN SUBGROUPS

The investigation of subgroups and factor groups plays an important role in group theory so it is only natural to wish to determine the character groups of the subgroups and factor groups of a given group G . In this paragraph we associate with each subgroup H of a group G a subgroup $\Phi = (X, H)$ of the character group X , called the annihilator of H , in such a way that the character group of G/H is the subgroup Φ while the character group of H is the factor group X/Φ . The latter relation, however, is established in the present paragraph only in the special case of open subgroups; the general case will be established later.

A) Let X be the character group of a group G and let H be any subset of G . The set of all characters $\xi \in X$ satisfying the condition $\xi(x) = 0$ for all $x \in H$, i.e., the set of all characters vanishing on H , is clearly a subgroup of X . This subgroup is called the annihilator of H in the character group X and will be denoted by (X, H) . In the sequel the set H will ordinarily be a subgroup of G .

B) Let X_1 and X_2 be the character groups of two groups G_1 and G_2 , and let f be a homomorphism of G_1 into G_2 . To each character ξ_2 of G_2 we associate a character ξ_1 of G_1 by means of the formula $\xi_1 = \xi_2 f$. Then the mapping φ defined by $\xi_1 = \varphi(\xi_2)$ is a homomorphism of X_2 into X_1 , called the adjoint of f . It turns out the kernel of φ is exactly the subgroup $(X_2, f(G_1))$. Clearly, if f is an isomorphism of G_1 onto G_2 then φ is likewise an isomorphism of X_2 onto X_1 .

It is easy to see that φ is a homomorphism of the algebraic group X_2 into X_1 . Indeed

$$\varphi(\xi_2 + \eta_2) = (\xi_2 + \eta_2)f = \xi_2 f + \eta_2 f = \varphi(\xi_2) + \varphi(\eta_2).$$

In order to show that φ is continuous, consider a general neighborhood $W(F_1, \Lambda_k)$ of zero in X_1 (here F_1 denotes a compact subset of G_1). Then $F_2 = f(F_1)$ is compact in G_2 and $W(F_2, \Lambda_k)$ is a neighborhood of zero in X_2 satisfying the condition $\varphi(W(F_2, \Lambda_k)) \subset W(F_1, \Lambda_k)$. Thus φ is continuous.

It remains only to identify the kernel of φ . If $\xi_2 \in (X_2, f(G_1))$ then for $x_1 \in G_1$ we have $\varphi(\xi_2)x_1 = \xi_2 f(x_1) = 0$, i.e., $\varphi(\xi_2) = 0$. On the other hand, if $\varphi(\xi_2) = 0$ then $\xi_2 f(x_1) = \varphi(\xi_2)x_1 = 0$ so that $\xi_2 \in (X_2, f(G_1))$.

Theorem 37. Let X be the character group of a group G , let H be a subgroup of G , and let $\Phi = (X, H)$. If $\xi \in \Phi$ then ξ is constant on the cosets of H so that ξ may be regarded as a mapping of the factor group G/H according to the formula $\xi(x^*) = \xi(x)$, where $x \in x^* \in G/H$. The mapping ξ thus defined on G/H is a character; moreover, in this sense, Φ is precisely the character group of the factor group G/H .

Proof: Let X^* denote the character group of the factor group $G^* = G/H$ and let f be the natural projection of G onto G^* . Denote also by φ the adjoint of f . Then φ is a homomorphism of X^* into X . It is clear that the theorem is equivalent to the assertion that φ is an isomorphism of X^* onto the subgroup Φ , and it is in this form that we shall prove the theorem.

Let $\xi \in \Phi$. Since $\xi(H) = 0$ it follows that ξ is constant on the cosets of H so that there certainly exists a homomorphism η of the algebraic group G^* into K satisfying the conditions $\xi = \eta f$. We must show that η is a continuous on G^* . Let Λ_k be a fixed neighborhood of zero in K and let U be a neighborhood of zero in G such that $\xi(U) \subset \Lambda_k$. Then for the neighborhood $f(U)$ of zero in G^* we have $\eta(f(U)) = \xi(U) \subset \Lambda_k$. Thus η is continuous, and since for arbitrary $\xi \in \Phi$ we have thus found an element $\eta \in X^*$ satisfying the condition $\xi = \eta f$ it follows that $\Phi = \varphi(X^*)$. Moreover, since $(X^*, f(G)) = (X^*, G^*) = \{0\}$, the kernel of φ contains nothing but zero. Thus it remains only to show that φ is an open mapping of X^* onto Φ .

Consider an arbitrary neighborhood $W(F^*, \Lambda_k)$ of zero in X^* . We begin by constructing a compact set $F \subset G$ such that $f(F) \supset F^*$. To this end let U be a neighborhood of zero in G having compact closure. The compact set F^* is contained in the union of a finite number of open sets of the form $f(x_i + U)$, $x_i \in G$, and we take for F the union of the corresponding compact sets $x_i + \overline{U}$. Clearly $f(F) \supset F^*$. Let now $\xi \in \Phi \cap W(F, \Lambda_k)$. As has been seen, there exists a character η of G^* satisfying the conditions $\xi = \eta f$. But

then $\eta(F^*) \subset \eta(f(F)) = \xi(F) \subset \Lambda_k$ so that $\eta \in W(F^*, \Lambda_k)$. Thus $\varphi(W(F^*, \Lambda_k)) \supset \Phi = W(F, \Lambda_k)$ and it follows that φ is open considered as a mapping of X^* onto Φ .

Theorem 37 gives complete information concerning the character groups of factor groups. The following lemma answers the analogous question for subgroups, but only in the special case of open subgroups. The general form of the theorem will be proved later (see Section 40).

Lemma: Let X be the character group of a group G , let H be an open subgroup of G , and let $\Phi = (X, H)$. If $\xi^* \in X/\Phi$ then the characters ξ belonging to the coset ξ^* all agree on H so that it makes sense to regard ξ^* as a mapping of H according to the formula $\xi^*(x) = \xi(x)$ where $\xi \in \xi^*$, $x \in H$. The mapping ξ^* of H into K thus defined is a character of H ; moreover, in this sense, X/Φ is precisely the character group of H .

Proof: Denote by Ψ the character group of H , by f the identity mapping of H into G , and by φ the adjoint of f . Then φ is a homomorphism of X into Ψ with kernel $(X, f(H)) = (X, H) = \Phi$. Thus the lemma is clearly equivalent with the assertion that φ is an open homomorphism of X onto Ψ , and it is in this form that we shall prove it. Now the assertion $\varphi(X) = \Psi$ amounts to saying that every character η of the subgroup H may be extended to a character ξ of the entire group G . But since H is open it follows that any homomorphism of the algebraic group G into K that coincides with η on H is automatically continuous. Thus all that is required is to extend η in some fashion to a character of the algebraic group G . The following definition is by transfinite induction.

Select one element out of each non-zero coset of H and arrange the set thus obtained in a transfinite sequence a_0, a_1, \dots . Let θ be the first transfinite number following all the numbers employed in this enumeration and denote by H_λ , $\lambda \leq \theta$ the minimal subgroup of the algebraic group G containing H and all elements a_μ , $\mu < \lambda$. Thus, in particular, $H_0 = H$ and $H_\theta = G$. We now construct inductively, for every $\lambda \leq \theta$, a homomorphism η_λ of the algebraic group H_λ into K in such a way that for $\mu < \lambda \leq \theta$ the homomorphism η_λ is an extension of η_μ and such that $\eta_0 = \eta$. Since the last equation automatically defines η_0 we suppose that for all $\mu < \lambda$ the homomorphism η_μ is already constructed and proceed to define η_λ . If λ is a limit number then the group H_λ is the union of the groups H_μ , $\mu < \lambda$, and we define η_λ to be the unique homomorphism coinciding with each η_μ on H_μ . Suppose then that λ has a predecessor $\lambda - 1$. Then every element $y \in H_\lambda$ may be written in the form $y = x + pa_{\lambda-1}$ where $x \in H_{\lambda-1}$ and p

is an integer. We now distinguish two cases: 1) The element $pa_{\lambda-1}$ belongs to $H_{\lambda-1}$ when and only when $p = 0$. In this case the expression $y = x + pa_{\lambda-1}$ for each element $y \in H_\lambda$ is unique and, letting γ denote any fixed element of K , we may define $\eta_\lambda(y) = \eta_{\lambda-1}(x) + p\gamma$. It is not difficult to verify that this mapping satisfies all the requirements. 2) There exists an integer $p \neq 0$ such that $pa_{\lambda-1} \in H_{\lambda-1}$. Let r denote the smallest positive integer satisfying this condition. Then every element $y \in H_\lambda$ has a unique expression of the form $y = x + pa_{\lambda-1}$ with $0 \leq p < r$. Since the elements of K are divisible by any integer there exists an element $\gamma \in K$ satisfying the condition $r\gamma = \eta_{\lambda-1}(ra_{\lambda-1})$ and with γ so chosen we define $\eta_\lambda(y) = \eta_{\lambda-1}^{-1}(x) + p\gamma$. Here again it is easily seen that the mapping η_λ thus defined is a homomorphism of H_λ into K that agrees with every η_μ on H_μ , $\mu < \lambda$. The desired homomorphism ξ of G into K is now obtained by letting $\xi = \eta_0$.

It remains to show that φ is open. Let U be any neighborhood of zero in the subgroup H having compact closure. We denote by W the set $W(\bar{U}, \Lambda_4)$ considered as a neighborhood of zero in X , and by W' the same set considered as a neighborhood of zero in Ψ . Then W and W' have compact closure (see Theorem 36). Moreover, it is clear that both are symmetric and that $\varphi(W) = W'$. We define now $X_1 = W \cup 2W \cup \dots$, and $\Psi_1 = W' \cup 2W' \cup \dots$. Since $\varphi(W) = W'$ it follows that $\varphi(X_1) = \Psi_1$. But X_1 and Ψ_1 are compactly generated open subgroups of the groups X and Ψ respectively (see Section 20, F)). Consequently Theorem 12 may be applied to the homomorphism φ_1 of X_1 onto Φ_1 induced by φ . Thus φ_1 is open, but then, since X_1 is an open subgroup of X it follows at once that φ is also open.

C) Let X be the character group of G and let G' be the character group of X . For any open subgroup H of G we consider the annihilators $\Phi = (X, H)$ and $H' = (G', \Phi)$. By the lemma X/Φ is the character group of H , while by Theorem 37 H' is the character group of X/Φ . Thus H' is the second character group of the subgroup H . It turns out that the natural homomorphism ω of G into G' coincides on H with the natural homomorphism of H into H' .

In order to see this let $y \in H$, $\xi \in X$. Then

$$\omega(y)\xi^* = \omega(y)\xi = \xi y = \xi^*y,$$

which is precisely what was asserted.

Example 62: Let H be an open subgroup of a group G , let

η be a character of H and let a be any element of G not belonging to H . Then there exists a character ξ of G coinciding with η on H and differing from zero at a .

The proof of this assertion may be obtained from the proof of the above lemma by putting $a_0 = a$ and by choosing $\gamma \neq 0$ in the construction of the homomorphism η_1 . Later on, this result will be obtained for an arbitrary subgroup H (see Theorem 55). Observe that if G is discrete then H may be taken to be the trivial subgroup so that in this case also we have proved the existence of a character that does not vanish at a given non-zero element $a \in G$.

SECTION 36

THE CHARACTER GROUPS OF THE ELEMENTARY GROUPS

In this paragraph we determine the character groups of the elementary groups: the discrete cyclic groups, the group K itself, the additive group of real numbers, and all finite direct sums of such groups. Moreover, it will be shown that the fundamental duality theorem holds for these groups, i.e., that the natural homomorphism ω of an elementary group G into its second character group G° is an isomorphism onto. In the following paragraphs this fact will be used in the proof of the general case of the theorem.

We begin by establishing some special properties of the group K .

A) A subgroup of the topological group K either coincides with K itself or is finite. In the latter event it is cyclic and consists of all elements of the form

$$\kappa\left(\frac{p}{r}\right), \quad p = 0, 1, \dots, r - 1$$

where r is the order of the subgroup; thus it contains all elements of K the order of which divides r .

If N is an infinite subgroup in K then K contains a limit point of the set N and it follows that N contains distinct elements a and b that are arbitrarily close to one another. The difference $c = a - b$ is then arbitrarily close to 0 and the multiples nc , $n = 1, 2, \dots$ belong to N but are also arbitrarily dense in K . Since N is a closed set in K it follows that $N = K$.

Consider now the case of the finite subgroup N of order r . If $a \in N$ then $ra = 0$ which shows that a may be represented in

the form $\kappa(p'/r)$ and therefore also in the form $\kappa(p/r)$, $0 \leq p < r$. But, now, the collection of all elements $\kappa(p/r)$, $p = 0, \dots, r - 1$, is a group of order r . Since N is contained in this group and has r elements by hypothesis, it follows that the group of such elements must coincide with N .

B) The group K admits but two automorphisms: one the identity map, $\alpha(x) = x$, and the other, β , defined by $\beta(x) = -x$.

Let γ be an arbitrary automorphism of K . Since $\kappa(1/2)$ is the only element of K having order 2 we must have $\gamma(\kappa(1/2)) = \kappa(1/2)$. Similarly K contains but two elements of order 4, namely $\kappa(1/4)$ and $\kappa(-1/4)$; thus there are but two possibilities:

$$\gamma(\kappa(1/4)) = \kappa(1/4) \text{ or } \gamma(\kappa(1/4)) = -\kappa(1/4)$$

These two possibilities are realized by the automorphisms α and β respectively. We must show that no other automorphisms exist. Suppose, for the sake of argument, $\gamma(\kappa(1/4)) = \kappa(1/4)$. Then the element $\kappa(1/8)$ must go into one of the two elements $\kappa(1/8)$ or $\kappa(5/8)$; but γ is a homeomorphic mapping and must preserve the cyclic order of elements on K . Thus, knowing that $\gamma(0) = 0$, $\gamma(\kappa(1/4)) = \kappa(1/4)$, $\gamma(\kappa(1/2)) = \kappa(1/2)$ and $\gamma(\kappa(3/4)) = \kappa(3/4)$, we conclude that $\gamma(\kappa(1/8)) = \kappa(1/8)$. Continuing in exactly the same fashion we conclude that $\gamma(\kappa(1/2^n)) = \kappa(1/2^n)$, $n = 1, 2, \dots$. But then, multiplying this last equation by an arbitrary positive integer $m < 2^n$ we find that $\gamma(\kappa(m/2^n)) = \kappa(m/2^n)$ and from this and from the continuity of γ it follows that γ is the identity map. In exactly the same fashion it may be shown that if $\gamma(\kappa(1/4)) = -\kappa(1/4)$ then $\gamma = \beta$.

C) Every character α of the group K may be expressed in the form $\alpha(x) = mx$ where m is an integer characterizing the homomorphism α : $\alpha = \alpha_m$. Moreover, $\alpha_m + \alpha_n = \alpha_{m+n}$. Thus the character group of K is isomorphic with the additive group of integers under the isomorphism $m \rightarrow \alpha_m$.

Let N denote the kernel of α . According to A), N either coincides with K or is finite and determined by some positive integer r . If $N = K$ then $\alpha = \alpha_0$. Accordingly we assume that N is finite. But then, as is easily seen, the factor group $K' = K/N$ is isomorphic with K , and since it is impossible to map K' isomorphically onto a proper subgroup of K it follows that the isomorphism associated with α is in fact onto. But then it follows from B) that there are but two mappings it can be, and since these correspond to the cases $\alpha = \alpha_r$ and $\alpha = \alpha_{-r}$, respectively, the assertion is proved.

D) Let C be an infinite cyclic group with generator g . Then every character β of C may be expressed in the form $\beta(ng) = na$ where a denotes a fixed element of K . The element a determines the character β : $\beta = \beta_a$. Moreover we have $\beta_a + \beta_b = \beta_{a+b}$. Thus the character group of C is isomorphic with K itself under the isomorphism $a \rightarrow \beta_a$.

Proposition D) is obvious.

E) Let Z_r be a finite cyclic group of order r with generator g . Then every character α of Z_r may be expressed in the form $\alpha(ng) = na$ where $a \in K$ is of the form $\kappa(p/r)$. The character α is determined by a : $\alpha = \alpha_a$. Moreover we have $\alpha_a + \alpha_b = \alpha_{a+b}$. Thus the character group of Z_r is isomorphic with Z_r itself.

The validity of E) is an immediate consequence of A).

F) Let D denote the additive topological group of real numbers. Then every character α of D may be expressed in the form $\alpha(x) = \kappa(dx)$ where d is a fixed real number defining the character $\alpha : \alpha = \alpha_d$. Moreover, we have $\alpha_c + \alpha_d = \alpha_{c+d}$. Thus the character group of D is isomorphic with D itself under the isomorphism $d \rightarrow \alpha_d$.

Denote by N the kernel of α . If $N = D$ then $\alpha = \alpha_0$. On the other hand, if $N \neq D$ then, as is easily seen, N contains a smallest positive number t , and coincides with the infinite cyclic group generated by t . Moreover, the factor group $K' = D/N$ is isomorphic with K and it follows, as above, that there are but two possibilities for the isomorphism of K' onto K associated with α , viz., those corresponding respectively to the cases $\alpha = \alpha_{1/t}$ and $\alpha = \alpha_{-1/t}$. Thus F) is proved.

We next consider the character groups of finite direct sums.

Theorem 38: Let G be the direct sum of a finite number of groups G_i , $i = 1, \dots, n$, and denote by X the direct sum of the respective character groups X_1, \dots, X_n . An element of X , $\xi = (\xi_1, \dots, \xi_n)$, $\xi_i \in X_i$, may, in a natural way, be viewed as a character of the direct sum G ; indeed, if for $x = (x_1, \dots, x_n) \in G$, $x \in G_i$, we define $\xi(x) = \xi_1(x_1) + \dots + \xi_n(x_n)$ then, as is easily seen, the mapping ξ is a character of G . Conversely, every character of G may be so obtained, and in the sense X is the character group of G . Moreover if G'_i is the character group of X_i , $i = 1, \dots, n$ and G' is the direct sum of the groups G'_1, \dots, G'_n (so that G' is the character group of X) and if ω_i denotes the natural homomorphism of G_i into G'_i , $i = 1, \dots, n$, then the natural homomorphism ω of G into G' is defined by the relation

$$\omega(x) = (\omega_1(x_1), \dots, \omega_n(x_n)) .$$

In particular, if each of the homomorphisms $\omega_1, \dots, \omega_n$ is an isomorphism onto then ω is also an isomorphism onto.

Proof: That distinct elements of X determine distinct characters of G is immediately clear. We shall show that every character G is defined by some element of X . Let f_i be the natural isomorphism of G_i into G (see Section 21, A)). Then, for arbitrary $x = (x_1, \dots, x_n) \in G$ we have $x = f_1(x_1) + \dots + f_n(x_n)$. If now ξ' is any character of G then $\xi'_i = \xi' f_i$ is a character of G_i and we have $\xi'(x) = \xi'_1 f_1(x_1) + \dots + \xi'_n f_n(x_n) = \xi_1(x_1) + \dots + \xi_n(x_n)$. But then ξ' coincide with the element $\xi = (\xi_1, \dots, \xi_n) \in X$, considered as a character of G .

Let now $\xi = (\xi_1, \dots, \xi_n)$ and $\eta = (\eta_1, \dots, \eta_n)$ be any two elements of X and let $x = (x_1, \dots, x_n)$ be an arbitrary element of G . Adding ξ and η as characters we obtain $\xi x + \eta x = \xi_1 x_1 + \dots + \xi_n x_n + \eta_1 x_1 + \dots + \eta_n x_n = (\xi_1 + \eta_1) x_1 + \dots + (\xi_n + \eta_n) x_n = (\xi + \eta) x$ where the sum $\xi + \eta$ standing in the right member of this relation denotes the sum as formed in X . Thus addition in the group X coincides with the ordinary addition of characters.

From what has already been shown it follows that X and the character group of G are identical when considered as algebraic groups. It remains to verify that the topology defined on X as a direct sum coincides with the topology it acquires when considered as the character group of G . Let F_i be an arbitrary compact subset of G_i . Then $W(F_i, \Lambda_k)$ (see Definition 36) is a general neighborhood of zero in X_i so that the collection $W(F_1, \dots, F_n; \Lambda_k)$ of all elements $\xi = (\xi_1, \dots, \xi_n) \in X$ satisfying the conditions $\xi_i \in W(F_i, \Lambda_k)$, i.e., the conditions $\xi_i(F_i) \subset \Lambda_k$, is a general neighborhood of zero in X in the direct sum topology. In other words, the collection Σ of all sets of the form $W(F_1, \dots, F_n; \Lambda_k)$ is a complete system of neighborhoods of zero in that topology. On the other hand, a complete system Σ^* of neighborhoods of zero in X regarded as the character group of G is given by the collection of all sets of the form $W(F, \Lambda_k)$ where F denotes a compact subset of G . Thus the proof will be complete if we can show that every neighborhood in Σ contains some neighborhood in Σ^* , and conversely that every neighborhood in Σ^* contains some neighborhood in Σ . Once again we denote by f_i the natural isomorphism of G_i into G . Let $W(F_1, \dots, F_n; \Lambda_k)$ be a given neighborhood in Σ . Then $F = f_1(F_1) \cup \dots \cup f_n(F_n)$ is compact in G and if $\xi = (\xi_1, \dots, \xi_n) \in W(F, \Lambda_k)$ then $\xi_i(F_i) = \xi f_i(F_i) \subset \xi(F) \subset \Lambda_k$ so that $\xi \in W(F_1, \dots, F_n; \Lambda_k)$ or, in other words, $W(F, \Lambda_k) \subset W(F_1, \dots, F_n; \Lambda_k)$. Next, the other way around: Let $W(F, \Lambda_k)$

be any neighborhood belonging to Σ^* and let φ_1 denote the natural projection of G onto G_1 (if $x = (x_1, \dots, x_n)$ then $\varphi_1(x) = x_1$). Let $F_1 = \varphi_1(F)$. Then if $\xi = (\xi_1, \dots, \xi_n) \in W(F_1, \dots, F_n; \Lambda_{nk})$ and if $x \in F$ we obtain $\xi(x) = \xi_1(x_1) + \dots + \xi_n(x_n) = \xi_1\varphi_1(x) + \dots + \xi_n\varphi_n(x) \in \xi_1(F_1) + \dots + \xi_n(F_n) \subset n\Lambda_{nk} = \Lambda_k$. In other words, $\xi \in W(F, \Lambda_k)$.

Finally, to verify the last assertion of the theorem let $x = (x_1, \dots, x_n)$ be any element of G and let $\xi = (\xi_1, \dots, \xi_n)$ be any element of X . Then $\omega(x)\xi = \xi x = \xi_1 x_1 + \dots + \xi_n x_n = \omega_1(x_1)\xi_1 + \dots + \omega_n(x_n)\xi_n$, i.e., $\omega(x) = (\omega_1(x_1), \dots, \omega_n(x_n))$.

G) It will be convenient to use the symbol $K^a C^b D^c Z$ to stand for the direct sum of a exemplars of K , b exemplars of the free cyclic group C , c exemplars of the additive group D of real numbers, and an arbitrary finite commutative group Z . Any group isomorphic with such a group is said to be an elementary group. From the facts educed in this paragraph, along with Theorem 2, it follows that the character group of $K^a C^b D^c Z$ is isomorphic with $K^b C^a D^c Z$.

H) If G is an elementary group then the natural homomorphism ω of G into its second character group G' is an isomorphism onto.

According to Theorems 2 and 38 it suffices to prove H) for the groups K , C , D , and the finite cyclic group Z_r . But in these cases H) is an immediate consequence of C), D), F), and E) respectively.

The following proposition indicates that in a certain sense the character group of any discrete group can be approximated by elementary groups.

I) Let X be the character group of a discrete group G , and let W be an arbitrary neighborhood of zero in X . Then there exists in G a finitely generated subgroup H such that $\Phi = (X, H) \subset W$. Accordingly, the factor group X/Φ , being the character group of H , i.e., of a group of the form $C^p Z$, is itself of the form $K^p Z$.

Consider the collection Δ of all subgroups of X of the form (X, H) where $H \subset G$ is a finitely generated subgroup. If (X, H_1) and (X, H_2) are any two subgroups belonging to Δ then $(X, H_1) \cap (X, H_2) = (X, H_1 + H_2)$ and since $H_1 + H_2$ is also finitely generated it follows that $(X, H_1) \cap (X, H_2) \in \Delta$. Thus Δ is a multiplicative system of sets. Moreover, since every element of G is contained in some finitely generated subgroup, the intersection of the subgroups belonging to Δ can contain only zero. Hence it follows from A) Section 13, that, for suitably chosen H , we must

have $(X, H) \subset W$.

Example 63: Let G be a compact commutative topological group. It was pointed out in the proof of Section 34, C) that if g is a linear representation of degree one then $\alpha(x) = \log g(x)/2\pi i$ is a character of G . Conversely, if β is any character then $h(x) = e^{2\pi i \beta(x)}$ defines a linear representation of G of degree one.

Consider, in particular, the case $G = K$. Then $g_n(x) = e^{2\pi i n x}$ is a linear representation of G and the corresponding character is $\alpha_n(x) = \log g_n(x)/2\pi i = nx$. Since the characters α_n , $n = 0, +1, +2, \dots$ exhaust the character group of K (see C)) it follows that the representations g_n form a complete system of irreducible representations of K . Thus, by virtue of Theorems 31 and 32, we obtain a proof of the fact that the functions g_n form a complete orthogonal system. Conversely, this fact, which is proved in analysis, may be used to give a proof of proposition C).

SECTION 37

DUALITY THEORY FOR COMPACT AND DISCRETE GROUPS

It was seen in Theorem 36 that the character group of a compact group is discrete while the character group of a discrete group is compact. Thus compact groups and discrete groups occupy a special place in duality theory. The present paragraph is devoted to the development of this special case.

The Fundamental Duality Theorem

Theorem 39: Let G be either a compact group or a discrete group, let X be its character group, and let G' be the character group of X . Then the natural homomorphism ω of G into G' is an isomorphism onto. By virtue of this isomorphism the groups G and G' may be identified so that G may be viewed as the character group of X ; if this is done then the character of X determined by an element $x \in G$ is defined by the formula $x(\xi) = \xi(x)$, $\xi \in X$.

Proof: Suppose first that G is discrete and let H denote an arbitrary finitely generated subgroup. We define $\Phi = (X, H)$ and $H' = (G', \Phi)$. By C) Section 35, H' is the second character group of H and ω considered as a mapping on H , is the natural homomorphism of H into H' . But, now, H may be resolved into a finite direct sum of cyclic groups (see Theorem 2) and is, in particular, elementary so that ω defines an isomorphism of H onto H' . Thus

the theorem will be proved if, for arbitrary elements $a \in G$ and $b' \in G'$, we can exhibit a finitely generated subgroup H such that $a \in H$ and $b' \in H'$. To this end let W be a neighborhood of zero in X such that $b'(W) \subset \Lambda_1$ and let $H_1 \subset G$ be a finitely generated subgroup such that $(X, H_1) \subset W$ (see Section 36, I)). We now define H to be the smallest subgroup of G containing H_1 and the element a . Then also $\Phi = (X, H) \subset W$ and since $b'(\Phi) \subset \Lambda_1$ we have $b'(\Phi) = 0$ (see Section 34, A)) so that $b' \in H'$. Thus the theorem is proved in the discrete case.

Next let G be a compact group. By virtue of proposition C), Section 34 we know that if $a \in G$, $a \neq 0$, then there exists a character α such that $\alpha(a) \neq 0$, i.e., such that $\omega(a)\alpha = \alpha(a) \neq 0$. Thus ω has trivial kernel and is an isomorphism of G onto the subgroup $\omega(G)$. It remains then to show that $\omega(G) = G'$ (see Section 13, E)). But now X is discrete and therefore, according to the half of the theorem already proved, may be identified with its own second character group, i.e., with the character group of G' . Moreover, for an element $\xi \in X$, considered as a character of G' , we have $\xi\omega(x) = \xi x$, i.e., ξ , considered as a character on G' , takes at $\omega(x)$ precisely the same value that it takes at x when considered as a character of G . From this it follows that $(X, \omega(G)) = (X, G) = \{0\}$. But, by Theorem 37, $(X, \omega(G))$ is the character group of the factor group $G'/\omega(G)$. Thus $G'/\omega(G)$ is a compact commutative group with trivial character group and, referring once again to C), Section 34, we conclude that $G'/\omega(G)$ is itself trivial, i.e., that $\omega(G) = G'$. Thus, in this case also, ω is an isomorphic mapping in G onto G' .

The remaining duality theorems for compact and discrete groups (parts of which have, in some cases, already been proved) may now be obtained without much difficulty; here they are.

The Theorem on the Duality of Annihilators

A) For every element $a \neq 0$ of a compact or discrete group G there exists a character α such that $\alpha(a) \neq 0$.

This fact was proved for compact groups in Section 34, C), and for discrete groups in Example 62. Here we give another proof, based on Theorem 39. Indeed, let X be the character group of G . Then, according to Theorem 39, a is a non-zero character of X and consequently there exists an element $\alpha \in X$ such that $a(\alpha) \neq 0$. But then $\alpha(a) = a(\alpha) \neq 0$.

Theorem 40: Let X be the character group of G , where G is either compact or discrete, let H be a subgroup of G and let

$\Phi = (X, H)$, $H' = (G, \Phi)$ (the annihilator (G, Φ) is defined inasmuch as G is the character group of X). Then $H' = H$.

Proof: It is clear that $H \subset H'$. Thus if $H \neq H'$ then there exists an element $a \in H'$ not belonging to H . By Theorem 37, Φ is the character group of G/H and, since the projection a^* of a on G/H is distinct from zero, there exists a character $\alpha \in \Phi$ such that $\alpha(a^*) \neq 0$. But $\alpha(a^*) = \alpha(a)$ and consequently $\alpha(a) \neq 0$, thus contradicting the assumption $a \in H' = (G, \Phi)$.

The Character Group of a Subgroup

The following theorem complements Theorem 37 and is an immediate consequence of the latter and the fundamental duality theorem.

Theorem 41: Let X be the character group of a group G where G is either compact or discrete, let H be a subgroup of G , and let $\Phi = (X, H)$. If $\xi^* \in X/\Phi$ then the characters ξ belonging to the coset ξ^* all agree on H so that ξ^* may be regarded as a mapping of the subgroup H according to the formula $\xi^*(x) = \xi(x)$ where $\xi \in \xi^*$, $x \in H$. The mapping thus defined on H is a character; moreover, in this sense, X/Φ is precisely the character group of H .

Proof: We regard G as the character group of X so that $H = (G, \Phi)$ (see Theorem 40) and H is the character group of X/Φ (see Theorem 37), the connection between the element x regarded as a character of X/Φ the same element x regarded as a character of X being given by the equation $x(\xi^*) = x(\xi)$. But then, regarding X/Φ is the character group of H (see Theorem 39), we may reformulate the latter equation as $\xi^*(x) = \xi(x)$, and the result follows.

On the Extension of Characters

Theorem 42: Let H be a subgroup of a group G where G is either compact or discrete, let a be any element of G not belonging to H , and let β be a character of H . Then there exists a character α of G that coincides with β on H and satisfies the condition $\alpha(a) \neq 0$.

Proof: Let X be the character group of G and let $\Phi = (X, H)$. According to Theorem 41, X/Φ is the character group of H . Consequently there exists an element γ^* of X/Φ which, considered as a character of H , coincides with β . Let $\gamma \in \gamma^*$. Then γ coincides

with β on H . If also $\gamma(a) \neq 0$ we have but to let $\alpha = \gamma$. On the other hand, if $\gamma(a) = 0$ then we proceed as follows: the projection a^* of a on the factor group G/H is distinct from zero so there exists a character δ of G/H , $\delta \in \Phi$, such that $\delta(a^*) \neq 0$. But then $\delta(a) \neq 0$ and we define $\alpha = \gamma + \delta$.

The Weight of a Compact Group

Theorem 43: The weight of a compact group is equal to the cardinality of its character group.

Proof: Let X be a compact group and let G be its character group. If G and X are finite then they are isomorphic (see Section 36, G)) and the theorem follows. On the other hand, if G and X are infinite then the result is an immediate consequence of B) Section 34 and Theorem 39 since the weight of a discrete group is clearly equal to its cardinality.

Orthogonal Pairs of Groups

We here formulate the connection between a discrete group and its compact character group in a somewhat different way.

Definition 38: We shall say that a compact group X and a discrete group G constitute a pair if there is defined a distributive and continuous multiplication of the elements of X by those of G . By this is meant that to every pair $\xi \in X$, $x \in G$, there is associated an element $\xi x \in K$ in such a way that the following conditions are satisfied:

- 1) $(\xi + \eta)x = \xi x + \eta x$, $\xi(x + y) = \xi x + \xi y$;
- 2) for any element $a \in G$ and any neighborhood Λ_k of 0 in K there exists a neighborhood W of zero in X such that for $\xi \in W$ we have $\xi a \in \Lambda_k$.

If H is a subset of G then (X, H) will denote the collection of those elements $\xi \in X$ for which $\xi x = 0$ for every $x \in H$. Clearly (X, H) is a subgroup of X . Similarly, if Φ is a subset of X then (G, Φ) will denote the collection of those elements $x \in G$ for which $\xi x = 0$ for arbitrary $\xi \in \Phi$. If $(X, G) = 0$ and $(G, X) = 0$ then we shall say that X and G constitute an orthogonal pair.

Theorem 44: Let X , G be an orthogonal pair of groups. Then every element $\xi \in X$ may be viewed as a character of G according to the relation $\xi(x) = \xi x$. Similarly, every element $x \in G$ may be viewed as a character of X according to the relation $x(\xi) = \xi x$. In this sense each of the groups X , G is precisely the character

group of the other.

Proof: Let G' be the character group of X . The mapping that assigns to each element $x \in G$ the corresponding character x' of X will be denoted by $\omega : x' = \omega(x)$. From the distributivity of the multiplication of elements of X by those of G it follows that ω is a homomorphism of G into G' . The condition $(G, X) = 0$ implies that the kernel of ω is trivial so that ω is an isomorphism of G onto the subgroup $\omega(G)$, and since $(X, \omega(G)) = (X, G) = 0$ it follows that $\omega(G) = (G', \{0\}) = G'$ (see Theorem 40) so that ω is in fact an isomorphism of G onto G' . Thus G is the character group of X and consequently X is also the character group of G .

Dual Direct Sum Resolutions

B) Let G be either a compact or a discrete group and let M be any set of subgroups of G . We denote by $\Delta(M)$ the intersection of the subgroups belonging to M and by $\Pi(M)$ the smallest subgroup of G containing all the subgroups belonging to M . (In Section 21, in the case of a compact group G , this latter subgroup was denoted by $\bar{\Pi}(M)$; the notation $\Pi(M)$ is used here for the sake of uniformity). Let X be the character group of G and let Ω denote the set of subgroups of X of the form (X, H) , $H \in M$. Then $\Delta(\Omega) = (X, \Pi(M))$, whence, taking annihilators and interchanging the roles of G and X , we obtain the dual relation $\Pi(\Omega) = (X, \Delta(M))$.

We need verify only the first of the two relations. Let $\xi \in \Delta(\Omega)$; then the kernel of ξ contains all the subgroups belonging to M and consequently contains $\Pi(M)$, i.e., $\xi \in (X, \Pi(M))$. On the other hand if $\xi \in (X, \Pi(M))$ then ξ vanishes on all of the subgroups belonging to M so that $\xi \in \Delta(\Omega)$. Thus $\Delta(\Omega) = (X, \Pi(M))$.

Theorem 45: Let G be either a compact or a discrete group and suppose G resolved into the direct sum of a collection M of subgroups (see Definitions 29' and 10'). For each $H \in M$ we define $K_H = \Pi(M \setminus H)$ and $\sigma(H) = (X, K_H)$. If each $\xi \in \sigma(H)$ is identified with the character it induces on H then $\sigma(H)$ becomes precisely the character group of H . Moreover, X resolves into the direct sum of the collection $\sigma(M)$ of subgroups $\sigma(H)$, $H \in M$. This resolution of X is said to be dual to the given resolution of G . The relation of duality between direct sum resolutions thus defined is symmetric.

Proof: Denote by M the set of all groups K_H , $H \in M$. Then according to the definition of direct sums we have $\Pi(M) = G$, $\Delta(\hat{M}) = \{0\}$. Let $H' = \Delta(\hat{M} \setminus K_H)$. Clearly then $H \subset H'$. But also

$H' \cap K_H = \{0\}$ while $H' + K_H = G$ so that G resolves into the direct sum of the subgroups H' and K_H . Since G is also the direct sum of H and K_H and since $H \subset H'$ we have $H' = H$.

Let now $K_{\sigma(H)} = \Pi(\sigma(M) \setminus \sigma(H))$ and denote by $\hat{\sigma}(M)$ the collection of all such subgroups. Since $H = H' = \Delta(M \setminus K_H)$ it follows from B) that $K_{\sigma(H)} = (X, H)$, and from this and from the fact that $\Pi(M) = G$ it follows that $\Delta(\hat{\sigma}(M)) = \{0\}$. Moreover, since $\sigma(H) = (X, K_H)$ and $\Delta(\hat{M}) = \{0\}$ it follows that $\Pi(\sigma(M)) = X$. Thus X resolves into the direct sum of the collection of subgroups of the form $\sigma(H)$.

To show that the resolution of G dual to the resolution of X thus obtained coincides with the given resolution, it is only necessary to verify that $H = (G, K_{\sigma(H)})$. But this is just dual of the relation $K_{\sigma(H)} = (X, H)$ which has already been established.

It remains to show that, in the stated sense, $\sigma(H)$ is the character group of H . Now H and $\sigma(H)$ form a pair if we define $\xi_x = \xi(x)$. Thus, according to Theorem 44, all we need to show is that this pair is orthogonal. But now $(\sigma(H), H) = \sigma(H) \cap (X, H) = \sigma(H) \cap K_{\sigma(H)} = \{0\}$, and in exactly the same fashion we may show that $(H, \sigma(H)) = \{0\}$. Thus the theorem follows.

Example 64: We show 1) that if X is a compact group containing an element α the multiples of which are everywhere dense in X then the weight τ of X does not exceed the continuum and, conversely, 2) that for every cardinal number τ not exceeding the continuum there exists a compact group X having weight τ and containing an element α the multiples of which are everywhere dense.

Suppose in the first place the given condition is satisfied. We regard X as the character group of its discrete character group G . Then α is a homomorphism of G into K and since the multiples of α are everywhere dense in X the kernel of α must be trivial. In other words α is an isomorphism of G onto some subgroup of the algebraic group K . It follows in particular that the cardinality of G cannot exceed the continuum. But then, by Theorem 43, the weight of X does not exceed the continuum either.

We turn now to the second part of the assertion. If τ is finite we have but to take for X a cyclic group of order τ . Accordingly we suppose, from now on, that τ is an infinite cardinal number. It is easy to see that the group K contains a set M of linearly independent elements (in the sense of integral linear combinations) having cardinality τ . To each element $\gamma \in M$ we associate a symbol x_γ and consider the collection G of all finite linear forms with integral coefficients in the symbols x_γ . Then G is a group under addition and we give it the discrete topology. Clearly G resolves

into the direct sum of the various free cyclic subgroups generated by the symbols x_γ . But then according to Theorem 45, the character group X resolves into the direct sum of a collection of isomorphic copies of K having cardinal number τ , so that X has weight τ . We now define $\alpha \in X$ by letting $\alpha(x_\gamma) = \gamma$. Clearly the mapping α thus defined extends uniquely to a character of G which vanishes only at zero, and from this it follows that the multiples of α are everywhere dense in X .

Example 65: Let $\alpha_1, \dots, \alpha_r$ be any finite system of linearly independent irrational numbers (the sum $n_1\alpha_1 + \dots + n_r\alpha_r$, with integral coefficients n_1, \dots, n_r , is never an integer unless all the coefficients vanish). We show that for arbitrary positive ϵ and real numbers d_1, \dots, d_r there exists integers m and n_1, \dots, n_r such that

$$|m\alpha_i - d_i - n_i| < \epsilon, \quad i = 1, \dots, r.$$

This is in fact an elementary result in the theory of approximation of real numbers by integral multiples of irrational numbers. We here give a proof based upon the results of the theory of characters.

Let G be the discrete group generated by the r linearly independent generators a_1, \dots, a_r . For each integer m we define a character β_m of G in the following fashion: if $x = n_1 a_1 + \dots + n_r a_r$ then $\beta_m(x) = \kappa(m(n_1 \alpha_1 + \dots + n_r \alpha_r))$. It is easy to verify that $\beta_m + \beta_n = \beta_{m+n}$. Thus the set B of all such characters is a group. Let X denote as usual the character group of G ; B is then a subgroup of the algebraic group X . Denote by Φ the closure of B in X . It is easily seen that if $\beta_m(x) = 0$ for every m then $x = 0$; this follows from the linear independence of the numbers α_i . From this we conclude that $(G, \Phi) = \{0\}$ and consequently, by the symmetry of annihilators that $\Phi = X$. In other words, B is everywhere dense in X so that an arbitrary character β of G may be approximated with arbitrary accuracy by means of characters of the form β_m . But this is, in substance, a statement of the proposition. Indeed, if d_1, \dots, d_r are given numbers we define a character β of G by letting $\beta(a_i) = \kappa(d_i)$, $i = 1, \dots, r$, and, approximating β by means of a special character β_m , we obtain the desired relation.

SECTION 38
**DIMENSION, CONNECTEDNESS AND LOCAL
 CONNECTEDNESS IN COMPACT GROUPS**

The fundamental theorem of duality for compact and discrete groups, obtained in the preceding paragraph, makes it possible in principle to characterize the properties of a compact group X in terms of the properties of its discrete character group G and therefore in purely algebraic terms. This is in particular true as regards the purely topological properties of the space X . Thus we have already seen that the weight of the space X is precisely the cardinality of G . In this paragraph we determine the algebraic properties of G corresponding to the connectedness, the total disconnectedness, the dimension, and the local connectedness of X . These results will not be used in any other part of the book.

It will be convenient to employ the following terminology: if every element of G is of finite order then G is said to be a torsion group; if, on the other hand, every non-zero element of G is free then G is said to be torsion-free. It is easily seen that, in an arbitrary discrete abelian group G , the set P of elements of finite order forms a subgroup, called the torsion subgroup of G , and that the factor group G/P is torsion-free.

Theorem 46. Let X be a compact commutative group, let G be its character group, and let P be the torsion subgroup of G . Then the annihilator (X, P) is precisely the component of zero in X . In particular, X is connected if and only if G is torsion-free, and is totally disconnected if and only if G is a torsion group (see Section 22).

Proof: We begin by showing that if G contains a non-zero element of finite order then X is not connected. Indeed, suppose the element a generates a non-trivial finite cyclic subgroup H in G . Then letting $\Phi = (X, H)$ we see that X/Φ , being the character group of the finite group H , must itself be finite and consequently must be discrete. Thus X is not connected.

On the other hand, as we show next, if X is totally disconnected then G must be a torsion group. Indeed let $a \in G$. We regard a as a character of X and select a neighborhood W of zero in X such that $a(W) \subset \Lambda_1$. Since X is totally disconnected W contains an open subgroup Ψ (see Theorem 16) for which the factor group X/Ψ , being compact and discrete, must be finite. Let $H' = (G, \Psi)$. Then since $a(\Psi) \subset a(W) \subset \Lambda_1$ it follows that $a(\Psi) = 0$ (see Section 34, A)) so that $a \in H'$. But now, the finite group X/Ψ is the character group of H' so that H' is a finite group. Thus

a has finite order.

Now denote by X' the component of zero in X and let $Q = (G, X')$. Since X' is connected it follows from what has been shown that G/Q , having X' for its character group, must be torsion-free so that $Q \supset P$. On the other hand X/X' is totally disconnected (see Section 22, C)) so that Q , having X/X' for its character group, can contain no free elements; i.e., $Q \subset P$. Thus $P = Q = (G, X')$ and $X' = (X, P)$.

Theorem 4.7. Let X be a compact group and let G be its character group. Then the dimension of the space X (see Definition 21) is precisely the rank of G (see Section 6, F)).

Proof: We show first that the dimension of X does not exceed the rank r of G . Let Ω be an arbitrary finite open covering of X . Then for each element $\xi \in X$ there exists a neighborhood W_ξ of zero in X such that the open set $\xi + 2W_\xi$ is contained in some one of the covering sets and from the covering of X consisting of the open sets $\xi + W_\xi$, $\xi \in X$, we may select a finite covering $\xi_1 + W_{\xi_1}, \dots, \xi_k + W_{\xi_k}$. Let $W_\xi = W_{\xi_1} \cap W_{\xi_2} \cap \dots \cap W_{\xi_k}$ and let $H \subset G$ be a finitely generated subgroup such that $\Phi = (X, H) \subset W$ (see Section 36, I)). Then the natural projection of X onto the factor group X/Φ is subordinate to the covering Ω (see Section 16, E)) and since X/Φ is of the form $K^p Z$ where $p \leq r$, and since p is the dimension of this group, it follows that the dimension of X cannot exceed r (see Section 16, E)).

Now let n be any positive integer not exceeding r . We shall show that the dimension of X is at least n . Let S be a maximal system of linearly independent elements in G (in the case of infinite rank the system S may be constructed by transfinite induction). Then S cannot contain fewer than n elements and we may select from it a subsystem x_1, \dots, x_n of n linearly independent elements. Denote by S' the system that remains after the removal of these n elements from S and by H the subgroup of G consisting of all elements x for which the system $x \cup S'$ is linearly dependent. The coset of H containing x_1 we denote by x_1^* . It may easily be verified that the factor group $G^* = G/H$ is torsion-free and that x_1^*, \dots, x_n^* is a maximal linearly independent system of elements in this group. Let now $X^* = (X, H)$. Then X^* is the character group of G^* and since X^* is a closed set in X it suffices to show that the dimension of X^* is at least n . Denote by Q^n the cube in n -dimensional Euclidean space consisting of all points $d = (d_1, \dots, d_n)$ satisfying the inequalities $|d_i| \leq 1/3$, $i = 1, \dots, n$. To each point $d \in Q^n$ we associate a character ξ_d of G^* in the following manner: let

$x^* \in G^*$; then for suitably chosen integers $a, a_1, \dots, a_n, a \neq 0$, we have $ax^* = a_1x_1^* + \dots + a_nx_n^*$ and we define $\xi_d(x^*) = \kappa(\frac{a_1}{a}d_1 + \dots + \frac{a_n}{a}d_n)$ (see Section 34, A)). It may be readily verified that $d \rightarrow \xi_d$ is a homeomorphism of Q^n into X^* . Thus the dimension of X^* must be at least n , and the theorem follows.

A) If H is a subgroup of a discrete group G then it is easily seen that the factor group G/H is torsion-free if and only if H has the following property: whenever $ax \in H$, where $x \in G$ and a denotes a positive integer, it follows that $x \in H$. Such a subgroup will be said to admit division. We shall also say that a discrete group G possesses property L if every finite subset of G is contained in a finitely generated subgroup that admits division.

Theorem 48: A compact group X is locally connected when, and only when, its character group G possesses property L.

The proof of Theorem 48 will be based on the following proposition which both illuminates the problem and is also not without independent interest.

B) Let G be a discrete torsion-free group of finite rank r and let X be its character group. Then X is locally connected when, and only when, G is finitely generated.

The sufficiency of the condition is clear. Indeed, if G is finitely generated then, according to Theorem 2, it is of the form C^r so that X is of the form K^r ; in particular X is locally connected. Accordingly, we suppose from now on that G is not finitely generated. Let $F = \{x_1, \dots, x_r\}$ be a maximal linearly independent system of elements in G . We denote by W the neighborhood $W = W(F, \Lambda_1)$ (see Definition 36), by H the subgroup of G generated by F , and by Φ the annihilator $\Phi = (X, H)$. We shall show that the topological space W is homeomorphic with the product of r -dimensional Euclidean space E^r and the space Φ .

As in the proof of Theorem 47, we use F to assign a character α_d to each $d = (d_1, \dots, d_r)$ satisfying the condition $|d_i| < 1/3$, $i = 1, \dots, r$. The definition of α_d is as follows: for any $x \in G$ there exist integers $a, a_1, \dots, a_r, a \neq 0$ such that $ax = a_1x_1 + \dots + a_rx_r$ and we write $\alpha_d(x) = \kappa(s_1d_1 + \dots + s_rd_r)$ where $s_i = a_i/a$, $i = 1, \dots, r$. It is easily verified that the set E^r consisting of all characters of the form α_d is homeomorphic with an open r -dimensional cube or, what comes to the same thing, with r -dimensional Euclidean space itself. Let now ξ be an arbitrary element of W . Letting $d_i = \xi(x_i)$, $i = 1, \dots, r$, we find that the

character $\xi - \alpha_d$ vanishes at each of the elements x_1, \dots, x_r and therefore belongs to Φ . Thus $\xi = \alpha_d + \eta$ where $\alpha_d \in E^r$, $\eta \in \Phi$. Moreover, this resolution is unique. Indeed, from $\xi = \alpha_d + \eta$, $\alpha_d \in E^r$, $\eta \in \Phi$, we obtain $\xi(x_i) = \alpha_d(x_i) + \eta(x_i)$ so that α_d is uniquely determined by ξ . It follows that the mapping $\xi = \alpha_d + \eta \rightarrow (\alpha_d, \eta)$ is a one-one correspondence between W and the product $E \times \Phi$; that this correspondence is, in fact, a homeomorphism may be established by a routine verification which we omit. In particular, the projection $\xi = \alpha_d + \eta \rightarrow \eta$ is a continuous open mapping of W onto Φ . Thus (see Section 15, H)). the proposition will be proved if we show that Φ is not locally connected.

Since H is finitely generated while G is not it follows that G/H is not finitely generated either, and hence that G/H is infinite since this is a torsion group. But then Φ , being the character group of G/H , is likewise infinite, and since Φ is compact it is not discrete. But now, Φ is also a totally disconnected group (see Theorem 46) and hence cannot be locally connected (see Section 15, H)). Thus B) is proved.

Proof of Theorem 48: Suppose first that G possesses property L and let W be an arbitrary neighborhood of zero in X . It suffices to show that W contains a connected neighborhood of zero. By virtue of I) Section 36 there exists a finitely generated subgroup $H_1 \subset G$ such that $(X, H_1) \subset W$ and, selecting any finite system of generators for H_1 and employing property L, we obtain a larger finitely generated subgroup H that admits division. Since $H_1 \subset H$ we have $\Phi = (X, H) \subset W$ and since G/H is torsion-free it follows that Φ is connected (see Theorem 46). Denote now by φ the natural projection of X onto $X^* = X/\Phi$. Since X^* is of the form $K^r Z$ it possesses a base Σ^* at zero consisting of connected neighborhoods. Consider the collection of all sets $\varphi^{-1}(\bar{U})$, $U \in \Sigma^*$. Since these sets are compact and have intersection Φ , it follows that for some neighborhood $U \in \Sigma^*$ we have $V = \varphi^{-1}(U) \subset W$ (see Section 13, H)). The proof will be completed by showing that V is connected.

Suppose on the contrary that V is expressible as the union of two non-empty disjoint open sets V_1 and V_2 . Since the subgroup Φ is connected it is impossible for any of its cosets to meet both of the open sets V_1 and V_2 . But then the open sets $\varphi(V_1)$ and $\varphi(V_2)$ are disjoint, and since U is the union of these sets, this contradicts the connectedness of U . Thus V is connected.

We preface the proof of the second half of the theorem with the following remarks. Let P be the torsion subgroup of G and let X' be the component of zero in X ; $X' = (X, P)$ (see Theorem 46). If P is infinite then its character group X/X' is also infinite as well as being compact and totally disconnected. As we have seen,

this implies that X/X' is not locally connected, but then neither is X since the natural projection is open and continuous (see Section 15, H)). Thus, if the torsion subgroup P is infinite then X is certainly not locally connected. On the other hand, if P is finite then X' is an open subgroup in X and in this case X is locally connected when and only when X' is.

We suppose now that G does not possess property L and show that X is not locally connected. According to the above remarks it is no loss of generality to suppose that G is torsion-free. Let M be a finite subset of G that violates property L, i.e., that is not contained in any finitely generated subgroup of G that admits division and let H be the smallest subgroup of G that contains M and does admit division. Then H is not finitely generated. Let $\Phi = (X, H)$. According to B), the factor group X/Φ , being the character group of H , is not locally connected. But then X is not locally connected either, and the theorem follows.

In the separable case the investigation of the structure of locally connected groups can be carried to completion.

Theorem 49: A separable locally connected compact group X resolves into the direct sum of a finite subgroup and a finite or countable number of subgroups, each isomorphic with K ; in other words, X has the form $K^r Z$, where r may not only take finite values but may also be countably infinite. Conversely, any such group is locally connected.

Proof: It suffices to prove the following purely algebraic dual of Theorem 49.

C) A countable discrete group G , possessing property L, resolves into the direct sum of a finite subgroup and a finite or countable number of free cyclic subgroups; in other words, G has the form $C^r Z$ where r is either finite or countably infinite. Conversely, any such discrete group has property L.

Suppose first that G is countable and possesses property L. Then the torsion subgroup P is finite while the torsion-free factor group $G^* = G/P$ also possesses property L. Let y_1^*, y_2^*, \dots be any enumeration of the countable set G^* . We construct inductively a sequence x_1^*, x_2^*, \dots of linearly independent elements in G^* in such a way that the subgroup generated by x_1^*, \dots, x_s^* admits division and contains y_1^*, \dots, y_s^* , $s = 1, 2, \dots$. To begin with, let H_1^* be the smallest subgroup containing y_1^* that admits division. By property L, H_1^* is finitely generated and, being minimal, must be a free cyclic group. Thus we may select for x_1^* either generator of H_1^* . Suppose now that elements x_1^*, \dots, x_i^*

have already been chosen in such a way as to satisfy the inductive hypothesis, and let H_i^* denote the subgroup they generate. If $H_i^* = G^*$ the construction is complete. Otherwise, let k be the smallest positive integer j such that $y_j^* \notin H_i^*$. Since y_1^*, \dots, y_k^* belong to H_i^* we have $k \geq i + 1$. Let H_{i+1}^* be the minimal subgroup admitting division that contains the elements $x_1^*, \dots, x_i^*, y_k^*$. Since H_i^* admits division the elements $x_1^*, \dots, x_i^*, y_k^*$ are linearly independent and the rank of H_{i+1}^* is $i + 1$. Moreover, according to property L, H_{i+1}^* is finitely generated, and it follows that H_{i+1}^*/H_i^* is a finitely generated torsion-free group of rank one, i.e., a free cyclic group having, say, x_{i+1}^{**} as generator. We now take for x_{i+1}^* any element belonging to the coset x_{i+1}^{**} and verify easily that the extended sequence x_1^*, \dots, x_{i+1}^* continues to satisfy the inductive hypothesis. Finally, for each $i = 1, 2, \dots$ let x_i be any element belonging to x_i^* , considered as a coset of P, and denote by G_i the cyclic subgroup generated by x_i . It may readily be verified that G resolves into the direct sum of the subgroups G_1, G_2, \dots and the finite subgroup P.

Conversely, suppose G has the form $C^r Z$, i.e., is the direct sum of subgroups P and G_1, G_2, \dots , where P is finite, while each G_i is a free cyclic group. Then every element of G is contained in some finite sum $P + G_1 + \dots + G_i$ and consequently an arbitrary finite set of elements in G is contained in such a finite sum. But any such finite sum clearly admits division, and it follows that G possesses property L.

Example 66: Theorem 49 tells the whole story of the structure of a locally connected compact group provided the topological space of the group is separable. That an analogous theorem cannot hold in general is shown by the following example.

Let G denote the collection of all sequences $x = (x_1, x_2, \dots)$ where x_1, x_2, \dots denote arbitrary integers. The sum of two sequences $x = (x_1, x_2, \dots)$ and $y = (y_1, y_2, \dots)$ is defined to be $x + y = (x_1 + y_1, x_2 + y_2, \dots)$. In this way G becomes an additive group which we endow with the discrete topology (G may also be described as the full direct sum of a countable number of free cyclic groups; see Definition 10). Now it is shown in the book of Kuroš [28] that G possesses property L but is not a direct sum of cyclic subgroups. Moreover, it is obvious that G is torsion-free. Accordingly, the character group of G is a connected and locally connected compact group which cannot be resolved into the direct sum of subgroups isomorphic with K.

Example 67: Let X be a connected compact group, the weight of which does not exceed the continuum. We shall show that there

exists a homomorphism φ of the additive topological group D of real numbers into X such that $\varphi(D)$ is everywhere dense. In other words, X contains an everywhere dense one-parameter subgroup.

Let G be the character group of X . It follows from Theorems 46 and 43 that G is torsion-free and that its cardinality does not exceed the continuum. Using these properties we first construct an isomorphism f of G into the algebraic group D . Indeed, let M be a maximal linearly independent system of elements in G . Since the cardinal number M does not exceed the continuum it is possible to map M into D in such a way that the collection of numbers $f(x)$, $x \in M$, is also linearly independent. If now $x \in G$ then there exist integers $a, a_1, \dots, a_r, a \neq 0$ such that $ax = a_1x_1 + \dots + a_rx_r$ and we extend the mapping f by writing $f(x) = \frac{a_1}{a}f(x_1) + \dots + \frac{a_r}{a}f(x_r)$. It is clear that f is an isomorphism into. We regard f as a homomorphism of G into D and take for φ the adjoint of f (see Section 35, B)). Since the character group of D is D itself, the mapping φ is a continuous homomorphism of D into X . The fact that $\varphi(D)$ is everywhere dense follows from the fact that f has trivial kernel and is the adjoint of φ (the last assertion is an easy consequence of Theorem 39).

Example 68: In Example 15 was constructed a torsion-free discrete group G of rank two that could not be resolved into a direct sum. The character group X of G is then a connected two-dimensional compact group that cannot be resolved into a direct sum.

SECTION 39 THE STRUCTURE OF LOCALLY COMPACT GROUPS

In the present section is given a complete description of the structure of those commutative groups that are compactly generated (see Section 20, F)); more precisely, it will be shown that such a group resolves into the direct sum of a compact group and an elementary group of the form $C^p D^q$. Since a compact group may always be viewed as the character group of its own discrete character group, it follows that the study of compactly generated commutative groups is, in principle, completely reduced to the study of algebraic groups. It should be recalled that not every locally compact group is compactly generated (see Example 71).

In this connection however we have the following proposition A) which says that a locally compact group may always be approximated "from within" by means of compactly generated groups and, using such approximations, we shall in the following section obtain the duality theorem for a generally locally compact group.

A) In any locally compact group G there exists a compactly generated open subgroup H containing an arbitrarily prescribed compact set $F \subset G$.

Indeed let W be any neighborhood of zero in G having compact closure \bar{W} . We define $V = W \cup (W + F)$ and $U = V \cup (-V)$. Clearly U is a symmetric neighborhood of zero with compact closure. Hence the set $H = U \cup 2U \cup \dots$ is a subgroup satisfying the stated conditions.

We turn now to the investigation of the structure of compactly generated groups.

Lemma 1: Let a be any element of a locally compact group G and denote by A the cyclic subgroup of the algebraic group G that is generated by a . Then either 1) A is contained in some compact subset of G or else 2) A is closed in G and is a discrete free cyclic subgroup of the topological group G .

Proof: Consider the locally compact group $H = \bar{A}$. It suffices to show that if 2) does not hold then H is compact.

Let U be any symmetric ($-U = U$) neighborhood of zero in H . We show first that for any positive integer p there exists a positive integer $n > p$ such that $na \in U$. Indeed, suppose the contrary. Then the algebraic group A is clearly a free cyclic group and the neighborhood U can contain none of its elements except possibly $0, \pm a, \dots \pm pa$. But in this case there exists a neighborhood of zero in H that meets A only in the zero element, which implies 2).

Next let W be any non-empty open subset in H . We show that there exists a positive integer k such that $ka \in W$. Since A is everywhere dense in H there is certainly an integer m such that $ma \in W$. Let U be a symmetric neighborhood of zero such that $ma + U \subset W$ and select a positive integer $n > |m|$ such that $na \in U$. Then $k = m + n > 0$ and $ka = ma + na \in W$.

We fix now in H a symmetric neighborhood V of zero having compact closure \bar{V} and show that some finite collection of open sets of the form $ia + V$, where i denotes a positive integer, covers the entire group H . This will imply that H is compact and thus will complete the proof of the lemma. Let $x \in H$. By what has

been shown there is a positive integer k such that $ka \in x + V$ or, what comes to the same thing, $x \in ka + V$. Thus the sequence of all open sets of the form $ka + V$, k a positive integer, covers H . In particular, these sets cover the compact set \bar{V} so that for some positive integer q the open set V is covered by the sets $a + V$, $2a + V, \dots, qa + V$. The proof of the lemma will be completed by showing that, in fact, these same open sets cover the whole group H . Indeed, for arbitrary $y \in H$, denote by k_y the smallest positive integer k for which $ka \in y + V$. We must show $k_y \leq q$. But now $k_y a - y \in V$ and since V is covered by the sets of $ia + V$, $i = 1, \dots, q$, there exists a number i , $1 \leq i \leq q$, such that $k_y a - y \in ia + V$, i.e., such that $(k_y - i)a \in y + V$. But then from the minimality of k_y it follows that $k_y - i \leq 0$, i.e., $k_y \leq i \leq q$.

The following lemma shows the connection between compactly generated groups and compact groups.

Lemma 2. In any compactly generated commutative group G there exists a discrete subgroup N generated by a finite number of linearly independent elements such that the factor group G/N is compact.

Proof: Let U be a symmetric neighborhood of zero that has compact closure and generates G : $G = U \cup 2U \cup \dots$ (see Section 20, F)). The collection of open sets $x + U$, $x \in G$, covers G and in particular covers the compact set $\bar{2U}$. Accordingly there exist elements a_1, \dots, a_s in G such that $a_i + U$, $i = 1, \dots, s$, cover $\bar{2U}$. Let A denote the subgroup of the algebraic group G generated by a_1, \dots, a_s . Then $2U \subset A + U$ and it follows that $G = A + U$. Indeed, we have $3U = 2U + U \subset A + U + U \subset A + U$; then similarly, $4U \subset A + U$ and in general $nU \subset A + U$.

Denote now by A_i the cyclic subgroup of the algebraic group G generated by a_i . If all of the sets A_i are compact then G is itself compact since $G = \bar{A}_1 + \bar{A}_2 + \dots + \bar{A}_s + \bar{U}$ (see Section 17, G)), and in this case we may take the trivial subgroup for N . On the other hand, if not all the sets A_i are compact then by Lemma 1 there exists among the elements a_1, \dots, a_s at least one that generates a discrete free cyclic subgroup of the topological group G . Let b_1 denote any one such element and suppose already selected a subsystem b_1, \dots, b_i of the system a_1, \dots, a_s such that the elements b_1, \dots, b_i are linearly independent and generate a discrete subgroup N_i of the topological group G . We shall show that either the factor group G/N_i is compact, in which case we may choose $N = N_i$, or else that a new element b_{i+1} may be selected from among the elements a_1, \dots, a_s is such a way that the enlarged system b_1, \dots, b_{i+1} continues to satisfy the inductive

hypothesis. Thus, after making a finite number of selections of the sort described, we must arrive at last at a subgroup N satisfying the conditions of the lemma and the proof will be complete.

Suppose then that G/N_i is not compact and let f denote the natural projection of G onto G/N_i . Then $f(G) = f(A) + f(U)$ and since $f(G)$ is not compact it follows from Lemma 1 that among the elements $f(a_1), \dots, f(a_s)$ there is at least one, say $f(a_j)$, that generates a discrete free cyclic subgroup of the topological group $f(G)$. We define $b_{i+1} = a_j$. From the fact that $f(b_{i+1})$ generates a free cyclic subgroup of $f(G)$ it follows at once that the elements b_1, \dots, b_i, b_{i+1} are linearly independent and generate a discrete subgroup of G . Thus the proof of Lemma 2 is complete.

Lemma 3: Let G be a locally compact group and suppose that for some finitely generated discrete subgroup N the factor group G/N is a compact elementary group. Then G itself is elementary.

Proof: We shall prove the lemma first under the added hypothesis that G is connected. In this case G/N is also connected and is therefore of the form K^r . Since K is by its definition the factor group of the group D of real numbers by the subgroup of integers it follows that K^r may be represented as the factor group of the r -dimensional vector group $A = D^r$ by the subgroup B consisting of all vectors with integral coordinates. Denote by f the natural projection of G onto G/N and by g the natural projection of A onto $A/B = G/N$. Since the kernels of these two homomorphisms are both discrete they are both local isomorphisms. Hence there exists in A a neighborhood U of zero so small that $f^{-1}g$ induces on U a local isomorphism of A onto G (see Section 23). Since A is a vector group it follows that for any element $x \in A$ there exists an element $y \in U$ and a positive integer n such that $ny = x$. We define $h(x) = nf^{-1}g(y)$. It is easy to see that the element $h(x)$ so defined does not depend upon the choice of n and that h is an open homomorphism of A onto G . (That h is onto follows from the fact that the connected group G is generated by any neighborhood of zero; see Theorem 14.) But now since $h = f^{-1}g$ in the neighborhood U , i.e., $g = fh$, while U generates A , it follows that the relation $g = fh$ must hold on the entirety of A . In particular, the kernel C of h must be contained in B . But then, since B has a finite system of linearly independent generators, it follows from the structure theory of abelian groups that B possesses a basis e_1, \dots, e_r such that C has a basis of the form $\tau_1 e_1, \dots, \tau_r e_r$ (see Section 6, E)). Moreover, the vectors e_1, \dots, e_r constitute a basis in the vector space A . Denote by D_i the coordinate axis in A generated by e_i and by C_i the subgroup of D_i generated

by $\tau_i e_i$. It is easily seen that D_i / C_i is isomorphic with K for $\tau_i \neq 0$ and to D for $\tau_i = 0$. Thus A/C , and consequently also G , is of the form $K^p D^q$.

Now let G be any group satisfying the hypothesis of the lemma. Since G/N is compact and elementary it is of the form $K^r Z$. The finite direct summand Z may be regarded as a subgroup of G/N and the inverse image M of that subgroup under the natural projection f is a discrete and finitely generated subgroup of G with the property that G/M is of the form K^r . Thus we may, and do, without loss of generality, assume that G/N is of the form K^r .

Since N is discrete the natural projection f is a local isomorphism and therefore maps some sufficiently small neighborhood U of zero in G homeomorphically onto a neighborhood U^* of zero in G/N . Moreover, since G/N is of the form K^r we may, by passing to a smaller neighborhood, arrange matters so that U and U^* are connected and symmetric. Let $G' = U \cup 2U \cup \dots$. Then G' is a connected open subgroup of G and is therefore the component of zero in G . Since the connected group G/N is generated by U^* it follows that $f(G') = G/N$. Let $N' = G' \cap N$. Since G' and G/N are both locally compact and connected it follows from Theorem 12 (see Section 20, F)) that the mapping of G'/N' onto G/N associated with the natural projection is, in fact, an isomorphism between these two groups (see Theorem 11). Thus in the connected group G' the discrete finitely generated subgroup N' yields a factor group of the form K^r and, by virtue of the first part of the proof, G' is of the form $K^p D^q$. But now since $f(G') = f(G)$ it follows that $G' + N = G$. Moreover, since G' is open in G the group G/G' is discrete and is therefore isomorphic with N/N' . In particular G/G' is finitely generated. Let $x_1^*, \dots, x_m^*, y_1^*, \dots, y_n^*$ be a canonical basis in G/G' ; here x_i^* denotes a free generator while y_j^* has order $\tau_j > 0$ (see Theorem 2). In each coset x_i^* we select an arbitrary element x_i . Similarly in each coset y_j^* we select an arbitrary element y_j . Then $\tau_j y_j \in G'$. But G' is of the form $K^p D^q$ and it follows that every element of G' may be divided by an arbitrary positive integer. Hence there exists an element $z_j \in G'$ such that $\tau_j z_j = \tau_j y_j$. Thus we have an element $y_j = y_j - z_j$ which belongs to y_j^* and satisfies the equation $\tau_j y_j = 0$. Letting H denote the subgroup generated by $x_1, \dots, x_m, y_1, \dots, y_n$, it is readily verified that G resolves into the direct sum of the subgroups G' and H . But then, since G' and H are both elementary, the group G is elementary also.

The following theorem shows that an arbitrary compactly generated commutative group may, in a certain sense, be approximated by elementary groups.

Theorem 50: Every neighborhood V of zero in a compactly generated commutative group G contains a compact subgroup H such that the factor group G/H is elementary.

Proof: By Lemma 2 there exists in G a discrete finitely generated subgroup N such that $G^* = G/N$ is compact. Let W be a symmetric neighborhood of zero in G with compact closure \bar{W} and such that $W \subset V$ while $3W$ contains no element of N except zero. Then $f(W)$ (f denotes as usual the natural projection of G onto G^*) is a neighborhood of zero in G^* and by proposition I) Section 36 there exists a subgroup $H^* \subset f(W)$ such that G^*/H^* is elementary. Let $H' = f^{-1}(H^*)$ and $H = H' \cap W$. Observe that f induces a homeomorphic mapping of W onto $f(W)$ and hence induces a homeomorphism of H onto H^* . Thus H is compact. We show that H is a subgroup by verifying that $H - H \subset H$. Indeed, if $x, y \in H$ then $x - y \in H'$ so there exists an element $z \in H$ such that $f(z) = f(x - y)$. But then $x - y - z \in N$ and since $3W$ contains no element of N other than zero it follows that $x - y - z = 0$, i.e., that $x - y \in H$.

It remains to show that $\hat{G} = G/H$ is elementary. In the first place if $z \in H'$ then for some $x \in H$ we have $f(x) = f(z)$ and therefore $y = z - x \in N$. Thus $H' = H + N$. Moreover, since $H \subset W$ the intersection $H \cap N$ is the trivial subgroup. Denote by \hat{N} the natural projection of N on the factor group \hat{G} . Then \hat{N} is isomorphic with N and is a discrete finitely generated subgroup whose factor group \hat{G}/\hat{N} is isomorphic with $G/(H + N) = G/H'$ and therefore with G^*/H^* . Since this latter group is a compact elementary group it follows by Lemma 3 that $G = G/H$ is itself elementary.

We come now to the fundamental result of the present section.

Theorem 51: A compactly generated commutative group may be resolved into the direct sum of a compact group and an elementary group.

Proof: Select any complete system of neighborhoods of zero in the given group G and arrange it in a transfinite sequence U_0, U_1, U_2, \dots . We denote by θ the first transfinite number that follows all the indices used in the enumeration. In the transfinite argument to follow the limit numbers will play a special role and it will be convenient to begin by modifying the enumeration. Accordingly we agree to write $V_\lambda = U_{\lambda-1}$ whenever $\lambda, \lambda \leq \theta$, is an ordinal number that has a predecessor $\lambda - 1$, while for all of the other transfinite numbers $1 \leq \lambda \leq \theta$, i.e., the limit numbers, we define $V_\lambda = G$. Note that the new transfinite sequence $V_1, V_2, \dots, V_\theta$ still forms a complete system of neighborhoods of zero.

By Theorem 50 there exists a compact subgroup $H_1 \subset V_1$ such that G/H_1 is elementary, i.e., has the form $K^a C^b D^n Z$. We regard the summands D^n and $K^a Z$ as subgroups of G/H_1 and denote by H the inverse image of $K^a Z$ under the natural projection. Since H_1 and $K^a Z$ are both compact it follows that H is compact (see Section 19, I)). Denote also by G_1 the inverse image of the subgroup D^n . Then $G_1 \cap H = H_1 \subset V_1$. Let now $G' = G_1 + H$. Then G'/H is isomorphic with G_1/H_1 (see Section 20, F) and G)) and is therefore of the form D^n . Moreover, the factor group G/G' is isomorphic with C^b and, in particular, has a finite system of linearly independent generators x_1^*, \dots, x_b^* . We regard these elements as cosets of the subgroup G' and select in each a fixed element x_i , $i = 1, \dots, b$. Then the subgroup N generated by x_1, \dots, x_b is discrete, the generators x_1, \dots, x_b are independent and G resolves into the direct sum of the subgroups G' and N .

We now construct by induction a non-increasing transfinite sequence $G_1, G_2, \dots, G_\theta$ of subgroups such that $H_\lambda = G_\lambda \cap H \subset V_\lambda$ and $G_\lambda + H = G'$ for every $\lambda \leq \theta$. The subgroup G_1 has already been constructed. Suppose that for all $\mu < \lambda \leq \theta$ subgroups G_μ satisfying the inductive conditions have been constructed. We proceed to construct G_λ .

Case I: there exists a predecessor $\lambda - 1$. By the inductive hypothesis $H_{\lambda-1} = G_{\lambda-1} \cap H \subset V_{\lambda-1}$ and $G_{\lambda-1} + H = G'$. Since G is compactly generated it is a countable union of compact subsets (see Section 20, F)) and by virtue of proposition G), Section 20, the factor group $G_{\lambda-1}/H_{\lambda-1}$ is isomorphic with G'/H and is therefore of the form D^n . Since D^n is clearly compactly generated while $H_{\lambda-1}$ is compact it follows that $G_{\lambda-1}$ is also compactly generated. Accordingly by Theorem 50 there exists a compact subgroup $H_\lambda \subset V_\lambda$ of the group $G_{\lambda-1}$ such that the factor group $G_{\lambda-1}/H_\lambda$ is elementary. Moreover, this factor group contains the compact subgroup $H_{\lambda-1}/H_\lambda$ which yields a factor group isomorphic with $G_{\lambda-1}/H_{\lambda-1}$ and therefore of the form D^n .^{*} Hence $G_{\lambda-1}/H_\lambda$ is of the form $K^{a'} Z' D^n$ and we may regard the direct summands $K^{a'} Z'$ and D as subgroups of $G_{\lambda-1}/H_\lambda$. The inverse image of $K^{a'} Z'$ in $G_{\lambda-1}$ under the natural projection a' coincides with $H_{\lambda-1}$; the inverse image in $G_{\lambda-1}$ of the subgroup D^n we denote by G . Then $G_\lambda \cap H = G \cap H_{\lambda-1} = H_\lambda \subset V$ while $G_\lambda + H = G_\lambda + H_{\lambda-1} + H = G_{\lambda-1} + H = G'$ so that the inductive conditions are satisfied by G_λ .

* That H is contained in H_λ and therefore in $H_{\lambda-1}$, follows from the fact that its projection on G'/H must be trivial; see Example 69. Trans.

Case II: λ is a limit number. In this case we define G_λ to be the intersection of all groups G_μ , $\mu < \lambda$. Let H_λ denote the intersection of the subgroups H_μ , $\mu < \lambda$. Then since $G_\mu \cap H = H_\mu$ we have $G_\lambda \cap H = H_\lambda \subset G = V_\lambda$ and the inductive construction will be complete if we can show $G_\lambda + H = G'$. Let $z \in G'$ and denote by $z_\mu *$ the coset of H_μ that contains z . Since $G' = G_\mu + H$ it follows that for suitably chosen cosets $x_\mu *$ and $y_\mu *$ lying in G_μ and H respectively, we have $x_\mu * + y_\mu * = z_\mu *$. Moreover, if $\mu < \nu < \lambda$ then $z_\mu * \supset z_\nu *$ from which it follows that $x_\mu * \supset x_\nu *$ and $y_\mu * \supset y_\nu *$. Let $x_\lambda *$ denote the intersection of the sets $x_\mu *$, $\mu < \lambda$, let $y_\lambda *$ denote the intersection of the sets $y_\mu *$, $\mu < \lambda$, and finally let $z_\lambda *$ denote the intersection of the sets $z_\mu *$, $\mu < \lambda$ (these intersections are not empty; see Theorem 4). Then $x_\lambda *$ is a coset of H_λ belonging to G_λ , $y_\lambda *$ is a coset of H_λ belonging to H , and $z_\lambda *$ is a coset of H_λ belonging to G' . From this and from the inclusion $x * + y_\lambda * \subset z_\mu *$, $\mu < \lambda$, it follows that $x_\lambda * + y_\lambda * = z_\lambda *$. But then since $z \in z_\lambda *$ we must have $z = x + y$ where $x \in x_\lambda * \subset G_\lambda$, $y \in y_\lambda * \subset H$. Thus $G' = G_\lambda + H$.

As the end result of this construction we arrive at a subgroup H_θ which is contained in every neighborhood of zero in G , and must therefore be trivial. Thus $G_\theta \cap H = \{0\}$ and $G_\theta + H = G'$. Since G' is the union of a countable collection of compact subsets, these two relations imply that G' resolves into the direct sum of the subgroups G_θ and H (see Theorem 13). The subgroup H is compact while G_θ is isomorphic with G'/H and is therefore of the form D^n . Thus the original group G resolves into the direct sum of the elementary subgroup $G_\theta + N$ and the compact subgroup H .

Example 69: The resolution of a compactly generated group G indicated in Theorem 51 may always be so arranged that the elementary summand A is of the form $C^p D^q$. Under these circumstances the compact summand B is uniquely determined: B is the largest compact subgroup of G , i.e., contains every compact subgroup of G .

According to Theorem 51, G resolves into the direct sum of an elementary subgroup, i.e., a subgroup of the form $K^a C^b D^c Z$, and compact subgroup B' . Splitting out of the first summand the compact part $K^a Z$ and adding it into B' we obtain a decomposition of the stated sort. The maximality of B follows from the fact that the factor group G/B is then of the form $C^p D^q$ and contains no non-trivial compact subgroup.

Example 70: Let us call an element of a locally compact

commutative group compact if all of its multiples are contained in some compact subset. It turns out that the set B of all compact elements in a group G is a subgroup and that the factor group G/B contains no compact elements. In the event that G is compactly generated B is precisely the largest compact subgroup (see Example 69).

Suppose first that G is compactly generated and that B' is its maximal compact subgroup. We denote as usual by f the natural projection of G onto G/B' . Since G/B' is of the form $C^p D^q$ its only compact element is zero. Thus if b is a compact element in G then $f(b) = 0$ so that $b \in B'$. On the other hand, it is clear that every element of B' is compact. Thus $B' = B$.

Let now G be any locally compact group. If x and y are elements of B then the multiples of x are contained in some compact set X and the multiples of y in some compact set Y whence it follows that the multiples of the difference $x - y$ are all contained in the compact set $X - Y$. Thus $x - y \in B$ and B is a subgroup of the algebraic group G . It remains to show that B is closed. Let $x \in \overline{B}$ and denote by H a compactly generated open subgroup containing x (see A)). Then $B' = H \cap B$ is the collection of compact elements belonging to H and is therefore a compact subgroup of H by the above case. But also $x \in \overline{B}' = B'$ so that $x \in B$ which shows that B is closed.

We show finally that G/B contains no compact elements other than zero. Denote, as usual, by f the natural projection of G onto G/B , let x^* be any compact element in G/B , and let $x \in x^*$. By A) there exists a compactly generated open subgroup H containing x . Since f is open it induces an open homomorphism of H onto the open subgroup $f(H)$ of the factor group. Thus $f(H)$ is isomorphic with H/B' where $B' = B \cap H$. But H/B' contains no compact elements other than zero and since $x^* \in f(H)$ it follows that $x^* = 0$.

Example 71: A discrete group is compactly generated when, and only when, it is finitely generated (this is valid not only for the commutative case but also for arbitrary groups). Indeed, if V is a neighborhood of zero in G that generates G and has compact closure, then, since G is discrete, V must be a finite set and G is finitely generated. On the other hand if G is generated by a finite set M then, joining to M the zero of G , we obtain a neighborhood V of zero that generates G and that is finite, i.e., compact.

SECTION 40
DUALITY THEORY FOR LOCALLY COMPACT GROUPS

In this section we conclude our study of duality theory by proving the various duality theorems for arbitrary locally compact commutative groups.

The Fundamental Theorem

Theorem 52: Let G be a locally compact group, let X be its character group, and let G' be the character group of X . Then the natural homomorphism ω of G into G' (see Definition 37) is an isomorphism onto. By virtue of this isomorphism the groups G and G' may be identified so that G may be viewed as the character group of X ; if this is done then the character of X determined by an element $x \in G$ is defined by the formula $x(\xi) = \xi(x)$, $\xi \in X$.

Proof: Let H be a compactly generated open subgroup of G (see Section 39, A)) and let $\Phi = (X, H)$, $H' = (G', \Phi)$. By Theorem 37 Φ is the character group of the discrete group G/H and is therefore compact. Moreover, it was shown in C) Section 35 that H' is the second character group of H and that the homomorphism induced on H by ω is the natural homomorphism of H into H' . Also by Theorem 51, H resolves into the direct sum of a compact group and an elementary group, and it follows that the natural homomorphism ω of H into H' is an isomorphism onto (see Theorems 38 and 39 and Section 36, H)). But now $H' = W(\Phi, \Lambda_1)$; indeed, every element $x' \in G'$ satisfying the condition $x'(\Phi) \subset \Lambda_1$ also satisfies the condition $x'(\Phi) = 0$ (see Section 34, A)) and therefore belongs to H' . Thus H' is an open subgroup of G' , whence it follows that the natural homomorphism ω of G into G' is open.

All that remains to show is that ω is onto, and this will be done if we can show that for an arbitrary pair of elements $a \in G$, $b' \in G'$ there always exists a compactly generated open subgroup $H \subset G$ such that $a \in H$, $b' \in H'$. To this end let W be a neighborhood of zero in X such that $b'(W) \subset \Lambda_1$ and let U_1 be a symmetric neighborhood of zero in G having compact closure \bar{U}_1 . We denote by H_1 the subgroup generated by U_1 and define $\Phi_1 = (X, H_1)$. By Theorem 37 Φ_1 is the character group of the discrete group G/H_1 . Hence, according to I) Section 36, there exists in G/H_1 a finitely generated subgroup H_2^* such that $\Phi_2 = (\Phi_1, H_2^*) \subset W$. Clearly $\Phi_2 = (X, H_2)$ where H_2 denotes the inverse image of H_2^* under the natural projection of G onto G/H_1 . Let now x_1^*, \dots, x_n^* generate H_2^* , choose an element x_i in each of the cosets x_i^* , $i = 1, \dots, n$, and let H be any compactly generated subgroup containing

U_1 and the elements a, x_1, \dots, x_n . Then $H_2 \subset H$ so that $\Phi = (X, H) \subset \Phi_2 \subset W$. Thus $b'(\Phi) \subset b'(W) \subset \Lambda_1$ and consequently $b'(\Phi) = \{0\}$ (see Section 34, A)). Thus $b' \in H'$ while $a \in H$ by construction.

The Theorem on the Duality of Annihilators

A) For every element $a \neq 0$ of a locally compact group G there exists a character α of G such that $\alpha(a) \neq 0$.

As has been noted before, this is substantially the assertion that the natural homomorphism of G onto its second character group is one-to-one. That it is a consequence of the fundamental duality theorem may be seen as follows. Since a is a non-zero character of the character group X there exists an element $\alpha \in X$ such that $a(\alpha) \neq 0$. But then $\alpha(a) = a(\alpha) \neq 0$.

Theorem 53: Let X be the character group of G , let H be a subgroup of G , and let $\Phi = (X, H)$, $H' = (G, \Phi)$ (the annihilator (G, Φ) is defined inasmuch as G is the character group of X). Then $H' = H$.

Proof: It is clear that $H \subset H'$. Thus if $H \neq H'$ then there exists an element $a \in H'$ not belonging to H . By Theorem 37, Φ is the character group of G/H and, since the projection a^* of a on G/H is distinct from zero there exists a character $\alpha \in \Phi$ such that $\alpha(a^*) \neq 0$. But $\alpha(a^*) = \alpha(a)$ and consequently $\alpha(a) \neq 0$, thus contradicting the assumption $a \in H' = (G, \Phi)$.

The Character Group of a Subgroup

The following theorem complements Theorem 37 and is an immediate consequence of the latter and the fundamental duality theorem.

Theorem 54: Let X be the character group of a group G , let H be a subgroup of G , and let $\Phi = (X, H)$. If $\xi^* \in X/\Phi$ then the characters ξ belonging to the coset ξ^* all agree on H so that ξ^* may be regarded as a mapping of the subgroup H according to the formula $\xi^*(x) = \xi(x)$ where $\xi \in \xi^*$, $x \in H$. The mapping thus defined on H is a character; moreover, in this sense, X/Φ is precisely the character group of H .

Proof: We regard G as the character group of X so that $H = (G, \Phi)$ (see Theorem 53) and H is the character group of X/Φ (see Theorem 37), the connection between the element x regarded

as a character of X/Φ the same element x regarded as a character of X being given by the equation $x(\xi^*) = x(\xi)$. But then, regarding X/Φ is the character group of H , we may reformulate the latter equation as $\xi^*(x) = \xi(x)$, and the result follows.

On the Extension of Characters

Theorem 55: Let H be a subgroup of a group G , let a be any element of G not belonging to H , and let β be a character of H . Then there exists a character α of G that coincides with β on H and satisfies the condition $\alpha(a) \neq 0$.

Proof: Let X be the character group of G and let $\Phi = (X, H)$. According to Theorem 54 X/Φ is the character group of H . Consequently there exists an element γ^* of X/Φ which, considered as a character of H , coincides with β . Let $\gamma \in \gamma^*$. Then γ coincides with β on H . If also $\gamma(a) \neq 0$ we have but to let $\alpha = \gamma$. On the other hand, if $\gamma(a) = 0$ then we proceed as follows: the projection a^* of a on the factor group G/H is distinct from zero so there exists a character δ of G/H , $\delta \in \Phi$, such that $\delta(a^*) \neq 0$. But then $\delta(a) \neq 0$ and we define $\alpha = \gamma + \delta$.

On Adjoint Homomorphisms

Theorem 56. Let X_1 and X_2 be the character groups of groups G_1 and G_2 , let f be a homomorphism of G_1 into G_2 and let φ be the adjoint homomorphism of X_2 into X_1 (see Section 35, B)). Then f is also the adjoint of φ . If f is an open homomorphism of G_1 onto a subgroup of G_2 then φ is also an open homomorphism of X_2 onto a subgroup of X_1 . Moreover, if this is the case and if H_1 denotes the kernel of f and $H_2 = f(G_1)$ its range, then the kernel Φ_2 of the adjoint φ is the annihilator $\Phi_2 = (X_2, H_2)$ while the range $\Phi_1 = \varphi(X_2)$ is the annihilator $\Phi_1 = (X_1, H_1)$.

Proof: We regard G_1 and G_2 as the character groups of X_1 and X_2 . Accordingly, the relation $\varphi(\xi_2)x_1 = \xi_2 f(x_1)$, $x_1 \in G_1$, $\xi_2 \in X_2$, that defines the adjoint homomorphism φ may be reformulated as $f(x_1)\xi_2 = x_1\varphi(\xi_2)$. But this says that f is the homomorphism adjoint to φ . In other words, the homomorphisms f and φ are mutually adjoint.

The fact that the kernel of φ is given by $\Phi_2 = (X_2, H_2)$ has already been proved (see Section 35, B)). We show next that $\varphi(X_2) \subset (X_1, H_1)$. Indeed, let $\xi_2 \in X_2$, $x_1 \in H_1$. Then $\varphi(\xi_2)x_1 = \xi_2 f(x_1) = \xi_2 0 = 0$, so that $\varphi(\xi_2) \in (X_1, H_1)$, i.e., $\varphi(X_2) \subset (X_1, H_1)$.

Denote now by f^* the isomorphism of G_1/H_1 onto H_2 associated with the open homomorphism f , and denote similarly by φ^* the isomorphism of the algebraic group X_2/Φ_2 onto $\varphi(X_2) \subset (X_1, H_1)$ associated with φ . According to Theorems 37 and 54, the character group of G_1/H_1 is (X_1, H_1) while the character group of H_2 is X_2/Φ_2 . Moreover, φ^* , considered as a mapping of X_2/Φ_2 into (X_1, H_1) , is the adjoint of f^* . But then, since f^* is an isomorphism onto, its adjoint must be an isomorphism of the topological group X_2/Φ_2 onto the topological group (X_1, H_1) (see Section 35, B)). Thus φ^* is an open mapping onto (X_1, H_1) , whence it follows at once that φ is an open mapping onto the same subgroup.

The Weight of the Character Group

Theorem 57: Let X be the character group of a group G . Then the topological spaces X and G have the same weight.

Proof: If G has finite weight then G is itself finite and X and G are isomorphic (see Section 36, G)). On the other hand, if the weight of G is infinite then the result is an immediate consequence of proposition B) Section 34 and the fundamental duality theorem.

Example 72: A natural question to ask is how it comes about that the group K plays such a special role in duality theory. The following proposition answers this question.

Let Q be any locally compact commutative group. Denote by \bar{K} the naturally defined group of all homomorphisms of K into Q and denote also by $\bar{\bar{K}}$ the group of all homomorphisms of \bar{K} into Q . It turns out that if K and \bar{K} are isomorphic then the group Q must be isomorphic with K . Thus if K were replaced by any other group the fundamental duality theorem could no longer hold.

If \bar{K} contained only zero the same would be true of $\bar{\bar{K}}$, contrary to the assumption that K and \bar{K} are isomorphic. Thus there exists a non-zero homomorphism α of K into Q which carries K onto some subgroup K' of Q . Since $\alpha \neq 0$ it follows that K' and K are isomorphic (although α need not be an isomorphism). Thus Q contains a subgroup K' isomorphic with K .

Denote by P largest compact subgroup of the component of zero in Q (see Example 69). Then $K' \subset P$. We shall show that in fact K' is a direct summand in P .

Let G be the character group of P and let $H = (G, K')$. Then G/H is the character group of K' and is accordingly a free cyclic

group. Let z be any element of G projecting onto a generator of G/H and denote by Z the free cyclic subgroup of G generated by z . It is readily verified that G resolves into the direct sum of the subgroups Z and H . Let $L' = (P, Z)$. Then P resolves into the dual direct sum of the subgroups K' and L' .

Now every homomorphism β of K into Q carries K into P , $\beta(K) \subset P$, and since P is the direct sum of the subgroups K' and L' it follows that K also resolves into the direct sum of subgroups A and B where A consists of all homomorphisms of K into K' and B consists of the homomorphisms of K into L' . The group A is a free cyclic group; the nature of B is of no interest to us.

Since \bar{K} is the direct sum of the subgroups A and B it follows that the group \bar{K} of homomorphisms of \bar{K} into Q is likewise the direct sum of subgroups C and D , isomorphic respectively with the groups of homomorphisms of A and B into Q . Moreover, since A is a free cyclic group the group of homomorphisms of A into Q is clearly isomorphic with Q itself. Thus C and Q are isomorphic. But, by hypothesis, \bar{K} is isomorphic with K whence it follows that Q is isomorphic with some subgroup of K . Since the only subgroups of K are K itself and the finite cyclic groups it follows then that Q is either isomorphic with K or must be finite. But the latter is impossible inasmuch as, has already been seen, Q contains an isomorphic copy of K .

The proposition just proved shows conclusively that K is the one and only group able to play the role assigned to it. The main point is that K has the special property that all of its factor groups are either trivial or isomorphic with K itself. The same property is possessed by the cyclic groups of prime order but they, being finite, cannot be used in the construction of a theory of characters on topological groups.

Example 73: Let X be the character group of G and let B be the subgroup of G consisting of all compact elements (see Example 70). Then (X, B) is precisely the component of zero in X (this generalizes Theorem 46).

Proof: Let $a \in G$, $a \neq 0$. If a is a compact element then X is disconnected. Indeed, the compact element a is contained in some compact subgroup H . Let $\Phi = (X, H)$. Then X/Φ is the character group of H , and since H is compact X/Φ is discrete. But since $a \neq 0$ the group X/Φ cannot be trivial whence it follows that X is disconnected. On the other hand, if a is not compact then X cannot be totally disconnected. Indeed, suppose the contrary. Let W be a neighborhood of zero in X such that $a(W) \subset \Lambda_1$ and let Φ be an open subgroup of X contained in W (see Theorem 16).

Then $a(\Phi) = 0$ (see Section 34, A)) whence we have $a \in H = (G, \Phi)$. But by construction X/Φ is discrete so that its character group H is compact. Thus the element a is compact contrary to hypothesis.

Now let X' be the component of zero in X . Since X/X' is totally disconnected its character group (G, X') can contain only compact elements; $(G, X') \subset B$. But also X' is connected so that $G/(G, X')$ can contain no compact element other than zero, and it follows that $(G, X') \supset B$. Thus $B = (G, X')$ and $X' = (X, B)$.

Example 74: Let X be the character group of G , let X' and G' denote the components of zero in X and G , and let Δ and B denote the subgroups of X and G respectively composed of all compact elements (see Example 70). Then $G' + B$ is open and is therefore a subgroup of G . Consequently, $X' \cap \Delta = (X, G' + B)$ (see Example 73 and Section 37, B)); similarly $X' + \Delta = (X, G' \cap B)$. The subgroup $G' \cap B$ is the maximal compact subgroup of G' so that G' resolves into the direct sum of $G' \cap B$ and a subgroup A of the form D^r (see Example 69). Similary X' resolves into the direct sum of the subgroup $X' \cap \Delta$ and a subgroup Γ of the form D^s . Moreover, G resolves into the direct sum of the subgroups A and (G, Γ) , the latter group having the compact group $G' \cap B$ as its component of zero. Similaly X is the direct sum of the subgroups Γ and (X, A) . Finally $s = r$.

We begin by showing that $G' + B$ is an open subgroup. Let H be a compactly generated open subgroup in G . Then H resolves into the direct sum of subgroups N , F and B' where N is of the form C^p , F of the form D^q , while $B' = H \cap B$ is the maximal compact subgroup of H (see Example 69). Since C^p is discrete $F + B'$ is open in H and therefore open in G . Hence $F + B$ is an open set in G and since $F \subset G'$ it follows that $G' + B$ is also open. Thus $G' + B$ is an open subgroup.

Moreover, $X' \cap \Delta$ is the largest compact subgroup of X' so that $\Gamma \cap \Delta$ contains only zero. Since $(G, \Gamma) + G'$ contains the open set $B + G'$ it follows that $(G, \Gamma) + G'$ is an open subgroup of G , and since $\Gamma \cap \Delta = \{0\}$ we have $(G, \Gamma) + G' = G$. Next, since $(G, \Gamma) \supset (G, X') = B \supset G' \cap B$, we have $G = G' + (G, \Gamma) = A + G' \cap B + (G, \Gamma) = A + (G, \Gamma)$. Similarly $X = \Gamma + (X, A)$ and from this last relation it follows that $(G, \Gamma) \cap A = \{0\}$. Thus, summarizing, we have $(G, \Gamma) + A = G$, $(G, \Gamma) \cap A = \{0\}$ which says that the algebraic group G resolves into the direct sum of the subgroups (G, Γ) and A . The topological conditions for resolution into direct sum are also satisfied. Finally, the character group of A is isomorphic with $X/(X, A)$, i.e., with Γ . Thus $s = r$.

Example 75: Let G be a locally compact locally connected commutative group and let G' be the component of zero in G . Then G' is an open subgroup of G . Indeed, the natural projection of G onto G/G' is open and continuous so that G/G' is locally connected (see Section 15, H)), but it is also totally disconnected (see Section 22, C)), and must therefore be discrete. Thus G' is open in G . Now G' resolves into the direct sum of its maximal compact subgroup B and a subgroup A of the form D^s (see Example 69). Since G' is locally connected so is the factor group G'/A (see Section 15, H)) whence it follows that B , being isomorphic with G'/A , is also locally connected. Suppose now that G is separable; then B is separable also and accordingly resolves into the direct sum of a finite or countable number of subgroups isomorphic with K (see Theorem 49). Thus in the separable case G' is of the form $K^r D^s$, where r is finite or countably infinite while s is finite. Suppose now in addition that G is finite dimensional (see Definition 21). Then G' is of the form $K^r D^s$, where both r and s are finite. In this case G is locally isomorphic with D^{r+s} so that in a sufficiently small neighborhood of zero it is possible to introduce coordinates in such a way that the addition of elements corresponds to the addition of their coordinates. Thus a separable, locally compact, locally connected, commutative, topological group of finite dimension is a Lie group (see Definition 39).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

7

THE CONCEPT OF A LIE GROUP

Till now in the investigation of topological groups we have imposed on them only requirements of a quite general character formulated in terms of abstract algebra and abstract topology. The concept of a Lie group, on the other hand, contains in its very definition the requirement of the analyticity, or at the very least, the differentiability of certain functions, viz., the functions determining the operation of group multiplication (see Definition 39). In consequence of this it is possible in investigating Lie groups to make extensive use of the apparatus of analysis, in particular of the theory of differential equations, and this, in turn, makes possible a very deep structural analysis. The analytic apparatus permits the reduction of the study of Lie groups to certain quite delicate but elementary questions of an algebraic character (see Chapter 10), these questions being, in essence, certain special problems in the theory of matrices. Only after this reduction is made does the deep and detailed theory of Lie groups proper commence (see Chapter 11). However, these are not the questions with which we shall be concerned in the present chapter.

In theories of relatively ancient origin it is not customary for the question of the differentiability or analyticity of the functions under investigation to receive much attention. All functions that turn up in the course of the investigation are simply assumed to be differentiable or analytic according to need. In this, however, there is an essential defect. It is one thing to demand that certain functions, appearing in the definition of an object, be differentiable; it is an altogether different thing to assume, from the beginning, the differentiability of all functions which might be met with in the investigation of that object. The very nature of these functions is not known in advance and it is *a priori* possible that the investigation

of a perfectly natural question might lead to the appearance of non-differentiable functions. Exactly for this reason the classical theory of Lie groups left matters in a not entirely satisfactory state. Let us assume, for instance, that we are investigating a certain Lie group. We have no reason to suppose *a priori* that all of its subgroups are also Lie groups, but we nevertheless find it necessary to consider arbitrary subgroups. The situation is exactly analogous as regards factor groups; and suppose we find it necessary to consider automorphisms of the Lie group. Can they be expressed by means of differentiable functions? It is with the solution of these preliminary questions that the present chapter is concerned. Starting from the assumption of the differentiability or analyticity of certain functions, we shall show that other functions that turn up in a natural manner in the process of investigation are likewise differentiable, or analytic, respectively. The distinction made here, i. e., the distinction between differentiability and analyticity, will be maintained throughout the chapter. Later it will turn out that it is, in fact, possible in the study of Lie groups to limit oneself to the mere assumption of differentiability, inasmuch as one can then reduce all problems to the study of analytic functions without restricting the class of objects investigated. Here, however, it will be necessary for us to conduct a twofold investigation, one based on the assumption of differentiability, the other upon the assumption of analyticity, since the reduction to analytic functions lies outside the scope of the present chapter. Were we, at this time, to limit ourselves to the differentiable case alone, the results of the following chapter would remain incomplete.

The results of the present chapter are for the most part intended to give a preparation for the material of Chapter 8. In that chapter the theory of compact topological groups will, in large measure, be reduced to the study of Lie groups. There also we shall give a definition of a compact Lie group formulated in abstract terms, without resort to the concept of differentiability.

If, in making his acquaintance with Lie groups, the reader desires to limit himself to the classical formulation of problems and does not wish to get into the questions referred to above, it is not necessary for him to read this chapter in its entirety. It will suffice to read Sections 41, 42; moreover, he can skip Theorem 60.

In the classical theory a Lie group was understood to be a local group in which a differentiable coordinate system was given (see Definition 39) and by a property of the group was understood a property of the system of equations (3), Section 41, that remained invariant under differentiable transformations of coordinates (see Section 41, A)). A subgroup was understood to be a subgroup

determined by the relations (20), Section 44; in other words, Theorem 62 was turned into a definition. Similarly a homomorphism was understood to be given by equations (26), Section 44, so that Theorem 63 was also turned into a definition.

Because of the large number of computations we shall encounter in the present chapter, as well as in Chapters 10, 11, I shall in these chapters employ tensor notation, without, however, assuming the reader to be familiar with tensor analysis. The main point is that in indicating sums we dispense with the symbol \sum . The standard conventions are as follows: Indices are written not only as subscripts but also as superscripts and a monomial in which one and the same index, for instance i , appears twice, once as a subscript and once as a superscript, indicates the sum as the index i takes on all of its possible values. If not one but several indices are repeated in a monomial, that monomial is to be understood as a multiple sum. For instance a^b indicates the sum $\sum_{i=1}^r a_i b^i$, while $c_{ij}{}^i a^j$ indicates the double sum $\sum_i \sum_j c_{ij}{}^i a^j$. The placing of the indices follows a definite scheme; moving indices up or down is not permissible. In particular, the coordinates of points and the components of vectors are indicated by letters with superscripts, the letter chosen being always the same as the letter used to designate the point or vector itself. Thus the coordinates of x are denoted by x^1, \dots, x^r . We shall not write the superscripts in parentheses as is sometimes done to distinguish them from powers. Rather, to indicate the power of a letter we shall write that letter itself in parentheses. Thus $(a)^n$ will designate the n th power of the letter a . In any case, powers will play but a small role in the sequel. Finally, we continue to denote by δ_j^i that number equal to 1 for $i = j$ and equal to 0 for $i \neq j$.

SECTION 41. LIE GROUPS

The classical theory of Lie groups is concerned for the most part with the study of local groups. Therefore we here select as the fundamental concept that of a local Lie group and base upon it our definition of a global Lie group.

A) If G is a local group (see Section 23, D)) we shall say that a coordinate system is defined in G if there is given a homeomorphism φ of some neighborhood U of the identity element of G onto an open set V of a Euclidean space S under which the identity is carried into the origin of S . In this way to each $x \in U$ there

corresponds a system of real numbers

$$x^1, \dots, x^r, \quad (1)$$

comprising the coordinates of the point $\varphi(x) \in S$. We shall also refer to these numbers as the coordinates of the point $x \in U$. In particular, the coordinates of the identity element of the group are all equal to zero. Moreover, each r -tuple (1), in which the numbers are sufficiently small in absolute value, corresponds to a definite point $x \in U$ having this r -tuple for its coordinates. The number r is the dimension of the local group G (see Section 23, N) and Section 16). Let W be a neighborhood of the identity $e \in G$ sufficiently small so that for each pair x, y of elements of W the product xy is defined and belongs to U . Then we have

$$xy = z = f(x, y). \quad (2)$$

Since x, y , and z all belong to U , they possess coordinates and in coordinate form the relations (2) may be written

$$z^i = f^i(x, y) = f^i(x^1, \dots, x^r; y^1, \dots, y^r), \quad (3)$$

where the functions f^i appearing on the right are continuous single valued functions defined for all values of the arguments that are sufficiently small in absolute value. Moreover, since $xe = x$ and $ey = y$ we have

$$f^i(x^1, \dots, x^r; 0, \dots, 0) = x^i,$$

$$f^i(0, \dots, 0; y^1, \dots, y^r) = y^i. \quad (4)$$

The coordinates (1) defined in the local group G are said to be differentiable if the functions (3) are three times continuously differentiable, and are said to be analytic if the functions (3) are analytic. As an immediate consequence of (4) we have

$$\frac{\partial f^i}{\partial x^j} = \frac{\partial f^i}{\partial y^j} = \delta_j^i \text{ for } x = y = e. \quad (5)$$

From (5) it follows that in some neighborhood of e equations (3) may be solved for the coordinates x^1, \dots, x^r of the element $x = zy^{-1}$; consequently these coordinates are also three times continuously differentiable or analytic functions, respectively, of the coordinates of y and z . And the same is true with respect to $y = x^{-1}z$.

Definition 39: A local group G is a local Lie group if it is possible to introduce differentiable coordinates in G . A topological group G is a Lie group if it is separable and if it is a local Lie

group considered as a local group.

It is obvious that every local Lie group is locally compact (see Section 23, N)). Observe that, in view of separability, a countably compact Lie group is automatically compact, so that the concepts of compactness and countable compactness coincide for Lie groups.

In the tenth chapter it will be shown that it is possible to introduce analytic coordinates into every local Lie group but in this chapter we must distinguish between analytic Lie groups and differentiable Lie groups. An important problem in the general theory of topological groups is the so-called fifth problem of Hilbert: If G possesses a coordinate system (see A)) does it necessarily possess a differentiable coordinate system? The solution of the problem will be given in this book only for the compact and the commutative cases (see Theorem 70 and Example 75). For the general solution of the problem see [15, 36].

The entire study of Lie groups is based upon the use of the differentiable coordinates with which they come equipped. Indeed, the immediate object of investigation is not the structure of the group itself but rather the structure of the system of equations (3) expressing the law of multiplication in the group. But in making this study care must be exercised to admit only those properties of the system of equations which do not depend upon the choice of the coordinates and accordingly express genuine properties of the group itself. Along with any given system D of differentiable coordinates in the group we may consider the entirety $[D]$ of all coordinate systems obtainable from D by means of differentiable transformations of coordinates (see B)). Later (see Section 43) it will be shown that the collection $[D]$ contains all the differentiable coordinate systems which it is possible to introduce into the group. In this way the task of studying the structure of a Lie group is seen to coincide with that of seeking out the invariants of systems of equations (3) with respect to differentiable transformations of coordinates—a manner of posing the problem that is in full accord with the classical point of view. In the classical theory of Lie groups one supposed given a definite differentiable coordinate system D and admitted into consideration only those coordinate systems of the collection $[D]$. The question of the existence of other coordinate systems not belonging to $[D]$ was simply left unasked.

B) Let G be a local Lie group and let D be a differentiable coordinate system in G . The coordinates of an arbitrary point x in the system D we denote as usual by x^i . Let

$$\varphi^i(x) = \varphi^i(x^1, \dots, x^r), \quad i = 1, \dots, r, \quad (6)$$

be a system of three times continuously differentiable functions such that

$$\varphi^i(e) = \varphi^i(0, \dots, 0) = 0. \quad (7)$$

Let

$$p_j^i = \frac{\partial \varphi^i(e)}{\partial x^j} \quad (8)$$

and suppose that the determinant of the matrix $\|p_j^i\|$ is not equal to zero. Then the system of equations

$$x'^i = \varphi^i(x^1, \dots, x^r), \quad i = 1, \dots, r, \quad (9)$$

may be viewed as introducing into G a new system of coordinates D' ; indeed as the new coordinates of the point x we may simply use the numbers x'^i . It is obvious that the coordinate system D' is differentiable and that it is even analytic if the original system D and the transformation (9) are analytic. The change from D to D' is a differentiable [analytic] transformation of coordinates. The inverse change from D' back to D is then also a differentiable or an analytic transformation of coordinates, respectively.

C) Let G be a local Lie group and let D be a differentiable coordinate system in G . By an arc x in G we shall mean a continuous mapping x of some interval $|t| \leq \alpha (\alpha > 0)$ into G satisfying the condition $x(0) = e$. The arc x is said to possess a tangent in the coordinate system D if the derivatives

$$\frac{dx^i(0)}{dt} = a^i. \quad (10)$$

exist. The numbers a^i may be regarded as the components of a vector a called the tangent vector to x . (Observe that we refer here only to the tangent vector at the point $t = 0$; as we shall have no occasion in the future to concern ourselves with tangent vectors at any other points, we shall consistently omit the phrase "at $t = 0$.") If we change from the given coordinate system D to a new coordinate system D' by means of a differentiable transformation of coordinates (9) then in the new coordinate system the vector a receives new coordinates a'^i expressed in terms of the old by

$$a'^i = p_j^i a^j$$

(see (8)). In this manner we associate with each local Lie group a certain vector space R composed of all those vectors tangent to differentiable arcs in G . The connection between G and R is initially established with the aid of a certain coordinate system D and thus appears to depend on D , but to every transformation (9) of coordinates in G there corresponds the transformation (11) of coordinates in R and the connection between G and R thus turns out to be invariant with respect to differentiable transformations of coordinates.

D) If G and G' are two differentiable [analytic] local Lie groups then so is their direct product H .

Indeed let D and D' be differentiable [analytic] coordinate systems of G and G' respectively. If x^1, \dots, x^r are the coordinates of a point $x \in G$ while x'^1, \dots, x'^s are the coordinates of a point $x' \in G'$ then as coordinates of the pair $(x, x') \in H$ we simply take the $(r+s)$ -tuple $x^1, \dots, x^r, x'^1, \dots, x'^s$. If multiplication in G and G' , is expressed in terms of coordinates by the relations

$$z^i = f^i(x^1, \dots, x^r; y^1, \dots, y^r), \quad (12)$$

$$z'^j = f'^j(x'^1, \dots, x'^s; y'^1, \dots, y'^s), \quad (13)$$

then multiplication in H is expressed by the relations (12) and (13) taken together.

E) In every Lie group G there exists, by definition, a coordinate system D for which the law of multiplication is written with the help of three times continuously differentiable functions (see (3)). The corresponding coordinates are called differentiable. The functions (6) which effect the transformation (9) from D to D' were assumed to be three times continuously differentiable so that D' would also be differentiable in the formulated sense.

Were the function two times continuously differentiable, then the coordinates D' obtained from (9) would not be differentiable in this sense because the law of multiplication in D' is expressed through two times continuously differentiable functions. But such two times continuously differentiable coordinates could be used for certain purposes. For instance, the definition C) of a tangent to the curve $x = x(t)$ has meaning even when this curve is expressed in two times differentiable coordinates."

Example 76: Let G be the topological group of all non-singular real $n \times n$ matrices. We shall show that G is an analytic Lie group. To this end we introduce coordinates in G as follows: an arbitrary matrix $x \in G$ may be expressed in the form

$$e + \|x_j^i\|, \quad (14)$$

where e denotes the identity matrix; we define the coordinates of x to be the entries of the matrix $\|x_j^i\|$. In this way we obtain a mapping φ of the entire group G onto a domain of the Euclidean space S of dimension n^2 which carries the identity matrix into the origin of S . Relations (3) assume the following algebraic form:

$$z_j^i = x_j^i + y_j^i + x_k^i y_j^k. \quad (15)$$

Thus G is an analytic Lie group. Analogously the non-singular complex $n \times n$ matrices form an analytic Lie group of dimension $2n^2$.

SECTION 42. ONE-PARAMETER SUBGROUPS

In the study of Lie groups a very important role is played by one-parameter subgroups (see Section 23, M)). These subgroups are connected

with the Lie group in an invariant manner, i.e., they do not depend upon the choice of coordinates, and permit the introduction into the group of natural coordinate systems.

A) Let G be a local Lie group and let D be a two times differentiable coordinate system in G (see Section 41, E)). If g is a one-parameter subgroup of G then g is said to be differentiable in the coordinate system D if the arc g possesses a tangent vector in that coordinate system (see Section 41, C), E)). The tangent vector is then called the direction vector of g .

We turn now to the question of the existence and uniqueness of a one-parameter subgroup with prescribed direction vector a . In order more conveniently to formulate the relevant theorem we introduce the auxiliary functions

$$\begin{aligned} u_j^i(x) &= u_j^i(x^1, \dots, x^r) \\ &= \frac{\partial}{\partial y^j} f^i(x^1, \dots, x^r; 0, \dots, 0) \end{aligned} \quad (1)$$

(see Section 41, (3)).

Theorem 58: let G be a local Lie group and let D be a two times differentiable coordinate system in G . Then any one-parameter subgroup g possessing direction vector a satisfies the system of differential equations

$$\frac{dg^i(t)}{dt} = u_j^i(g(t))a^j \quad (2)$$

with initial conditions

$$g^i(0) = 0. \quad (3)$$

Conversely, any solution of the initial value problem (2, 3) determines a one-parameter subgroup g possessing direction vector a . In view of the existence and uniqueness of the solution of the initial value problem, it follows that there exists in G a unique one-parameter subgroup $g = g(a, t)$ with direction vector a . Moreover, it follows from (2) that the functions $g^i(a, t) = g^i(a^1, \dots, a^r, t)$ are two times continuously differentiable (analytic) in all arguments in a sufficiently small neighbourhood of the zero if D is differentiable (analytic).

Proof: If g is a one-parameter subgroup with direction vector a then the initial condition (3) is satisfied since $g(0) = e$. Thus in order to show that the coordinates $g^i(t)$ of the element $g(t)$ satisfy (2, 3) it suffices to compute the derivative

$$\lim_{s \rightarrow 0} \frac{g^i(t+s) - g^i(t)}{s} = (g^i)'(t). \quad (4)$$

From the relation $g(t+s) = g(t)g(s)$ and from (3) and (4), Section 41, we obtain

$$g^i(t+s) = f^i(g(t), g(s)) = g^i(t) + u_j^i(g(t))g^j(s) + \epsilon^i s,$$

where $\epsilon^i \rightarrow 0$ as $s \rightarrow 0$. But then

$$\frac{g^i(t+s) - g^i(t)}{s} = u_j^i(g(t)) \frac{g^j(s)}{s} + \epsilon^i,$$

and it follows that the derivative $(g^i)'(t)$ exists and that the functions g^i satisfy (2).

We now assume that the functions g^i satisfy (2) and the initial conditions (3) and show that the point $g(t)$ with coordinates $g^i(t)$ describes a one-parameter subgroup having direction vector a .

Observe that the latter assertion, namely that $\frac{dg^i(o)}{dt} = a^i$, is an

immediate consequence of (5), Section 41, so that all that is necessary is to establish that g is a one-parameter subgroup.

Let

$$g^*(t, u) = g(t)g(u), \quad (5)$$

and denote by $g^{*i}(t, u)$ the coordinates of $g^*(t, u)$. We estimate the difference

$$g^{*i}(t, u) - g^i(t+u) = \epsilon_1^i u, \quad (6)$$

showing that ϵ_1^i tends to zero along with u . On the one hand

$$g^{*i}(t, u) = f^i(g(t), g(u)),$$

whence we obtain

$$g^{*i}(t, u) = g^i(t) + u_j^i(g(t))a^j u + \epsilon_2^i u, \quad (7)$$

where $\epsilon_2^i \rightarrow 0$ along with u . On the other hand, from (2) we have

$$g^i(t+u) = g^i(t) + u_j^i(g(t))a^j u + \epsilon_3^i u, \quad (8)$$

where $\epsilon_3^i \rightarrow 0$ along with u . But from (7) and (8) it follows that $\epsilon_1^i \rightarrow 0$ along with u .

Next we show that the functions $g^{*i}(s, t)$ satisfy the initial value problem

$$\frac{\partial g^{*i}(s, t)}{\partial t} = u_j^i(g^*(s, t))a^j \quad (9)$$

$$g^{*i}(s, 0) = g^i(s). \quad (10)$$

Since (10) is an immediate consequence of the definition (5), it remains only to compute $\frac{\partial g^{*i}(s, t)}{\partial t}$. Now

$$g^{*i}(s, t + u) = f^i(g(s), g(t + u)).$$

and from this, taking (6) into account, it follows that

$$g^{*i}(s, t + u) = f^i(g(s), g^*(t, u)) + \epsilon_4^i u$$

where $\epsilon_4^i \rightarrow 0$ as $u \rightarrow 0$. But then also

$$g^{*i}(s, t + u) = f^i(g^*(s, t), g(u)) + \epsilon_4^i u$$

since multiplication is associative in G . Finally, making use (1), we may rewrite this last equation as

$$g^{*i}(s, t + u) = g^*(s, t) + u_j^i(g^*(s, t))a^j u + \epsilon_5^i u, \quad (11)$$

where $\epsilon_5^i \rightarrow 0$ as $u \rightarrow 0$, and (9) follows immediately.

On the other hand, the initial value problem (9, 10) is also satisfied by the functions $g^i(s + t)$. Indeed

$$\frac{\partial g^i(s + t)}{\partial t} = u_j^i(g(s + t))a^j, \quad (12)$$

$$g^i(s + 0) = g^i(s), \quad (13)$$

since (12) and (2) are in fact the same equation.

Thus $g^{*i}(s, t)$ and $g^i(s + t)$, considered as functions of the argument t , satisfy one and the same initial value problem. By the uniqueness of solutions of ordinary differential equations it follows that $g^*(s, t) = g(s + t)$ or, in other words, that $g(s)g(t) = g(s + t)$ (see (5)). Thus g is a one-parameter subgroup and that the functions $g^i(a, t)$ are differentiable (analytic) follows from the theory of ordinary differentiable equations. This completes the proof of Theorem 58.

B) Let G be a local Lie group and let D be a two times differentiable coordinate system defined in a neighborhood U of the identity element of G . A neighborhood $V \subset U$ is said to be a star-shaped neighborhood if, along with each point (x^1, \dots, x^r) in V , the point (tx^1, \dots, tx^r) is also in V for all $|t| \leq 1$. A coordinate system D defined in a star-shaped neighborhood U is said to be a canonical coordinate system of the first kind if every system of equations $x^i = a^i t$ determines a one-parameter subgroup, defined for all those values of t for which the point $(a^1 t, \dots, a^r t)$ belongs to U . Note that a linear transformation of coordinates carries a canonical coordinate system of the first kind into another canonical coordinate system of the first kind.

C) Let G be a local Lie group and let D be a canonical coordinate system of the first kind defined in a neighborhood U . Then every one parameter subgroup $g = g(t)$ which is differentiable in the coordinate system D , and satisfies the condition $g(t) \in U$ for all $|t| \leq \alpha$, must possess a coordinate expression of the form

$$g^i(t) = a^i t \text{ for all } |t| \leq \alpha \quad (14)$$

where a^i are the components of the direction vector a of the subgroup g .

To prove this assertion we introduce the functions $h^i(t) = a^i t$. According to B) these relations define a one-parameter subgroup h for all values of the argument t for which they make sense, and since U is a star-shaped neighborhood, the set of all such values of t forms an open interval $|t| < \beta$. Now the one-parameter subgroups g and h have the same direction vector and therefore coincide for sufficiently small values of t by Theorem 58. But then they must coincide for all values of t for which they are both defined; thus it suffices to show $\alpha < \beta$. Suppose the contrary. Then $a^i \beta = g^i(\beta)$ so that $(a^1 \beta, \dots, a^r \beta) \in U$ and the equations $h^i(t) = a^i t$ are defined for $t = \beta$. But this contradicts the definition of β .

Theorem 59: Let D be a differentiable [analytic] coordinate system in a local Lie group G . Then there exists a canonical coordinate system of the first kind D' such that the coordinate transformation from D to D' is two times differentiable [analytic] and, moreover, such that the matrix $\|p_j^i\|$ corresponding to the coordinate transformation from D to D' (see Section 41, B)) is the identity matrix.

Proof: Let g be a one-parameter subgroup that is a differentiable in the coordinate system D and has direction vector a . In order to make clear the dependence of g on a we write

$$g(t) = g(a, t). \quad (15)$$

or, in coordinate form

$$g^i(t) = g^i(a, t) = g^i(a^1, \dots, a^r; t). \quad (16)$$

Consider now the function $g(\alpha t)$ where α is a real number. Considered as a function of the parameter t , this is also a one-parameter subgroup since

$$g(\alpha s)g(\alpha t) = g(\alpha s + \alpha t) = g(\alpha(s + t)).$$

Moreover, the direction vector of $g(\alpha t)$ is αa . Indeed

$$\frac{dg^i(\alpha t)}{dt} = \frac{dg^i(\alpha t)}{d(\alpha t)} \cdot \alpha = \alpha a^i \quad \text{at } t = 0.$$

Since, by Theorem 58, there is only one one-parameter subgroup in G with direction vector αa it follows that

$$g(a, \alpha t) = g(\alpha a, t). \quad (17)$$

or, in coordinate form,

$$g^i(a^1, \dots, a^r; \alpha t) = g^i(\alpha a^1, \dots, \alpha a^r; t) \quad (18)$$

Now the functions (16) are solutions of the intial value problem (2, 3) and are therefore two times continuously differentiable [analytic] in all their arguments for $|t| \leq \epsilon$, $|a^i| \leq \epsilon$, where ϵ denotes some sufficiently small positive number. But then it follows from (18) that

$$g^i(a^1, \dots, a^r; t) = g^i\left(\frac{a^1 t}{\epsilon}, \dots, \frac{a^r t}{\epsilon}; \epsilon\right),$$

so that the functions g^i are defined for all values of their arguments satisfying the conditions $|a^i t| \leq \epsilon^2$, and in particular, for $t = 1$ and $|a^i| \leq \epsilon^2$. Accordingly, the functions

$$h^i(a) = h^i(a^1, \dots, a^r) = g^i(a^1, \dots, a^r; 1) \quad (19)$$

are defined in a neighborhood of the origin $(0, \dots, 0)$. Moreover

$$h^i(0, \dots, 0) = 0 \quad (20)$$

since

$$h^i(0a^1, \dots, 0a^r) = g^i(a^1, \dots, a^r; 0) = 0. \quad (21)$$

We next compute the derivatives of these functions at the origin.

Since in computing $\frac{\partial}{\partial a^j} h^i(0, \dots, 0)$ we start with all arguments

except a^j equal to zero, we may as well assume in advance that a has the special form a' where a' denotes the vector all of whose coordinates are equal to 0 with the exception of the j -th coordinate which has the value 1, so that $\frac{\partial}{\partial a^j} h^i(0, \dots, 0) = \frac{d}{dt} h^i(a't)|_0$.

Now according to (19) and (18) we have $h^i(a't) = g^i(a', t)$ so that $\frac{d}{dt} h^i(a't) = \frac{d}{dt} g^i(a', t)$ and, by definition, the derivative

$\frac{d}{dt} g^i(a', 0)$ is just the i -th coordinate of the direction vector a' of

the subgroup $g(a', t)$. Thus, taking into account the special choice of a' , it follows that

$$\frac{\partial}{\partial a^j} h^i(0, \dots, 0) = \delta_j^i. \quad (22)$$

For the purpose of introducing new coordinates in G we now consider the system of equations

$$x^i = h^i(x'^1, \dots, x'^r) \quad (23)$$

in the unknowns x'^k . In the first place, (20) shows that these equations have solution $x'^k = 0$ for $x^i = 0$. In the second place, (22) shows that the Jacobian of the system is one at the origin. Hence, by the implicit function theorem, the system (23) possesses unique continuous solutions in a neighborhood of the origin,

and therefore (see Section 41, B)) defines a transformation of coordinates assigning new two times differentiable coordinates x'^k to the point x whose coordinates are x^i in the original coordinate system D. We denote the new system of coordinates thus obtained by D' .

Consider now in G the arc g^* defined in the coordinate system D' by the linear equations

$$g^{*i}(t) = a^i t. \quad (24)$$

In order to compute the coordinates of this arc in the old coordinate system D we substitute $a^k t$ for x'^k in (23), obtaining

$$x^i = h^i(a^1 t, \dots, a^r t) = g^i(a^1, \dots, a^r; t)$$

(see (19) and (18)). But this implies that the arc g^* is a one-parameter subgroup. Thus every arc defined in the coordinate system D' by equations of the form (24) is a one-parameter subgroup, and D' is a canonical coordinate system of the first kind.

Finally, since the functions (16) are two times continuously differentiable [analytic], it follows that the functions (19) possess the same property so the transformation of coordinates from D' to D is twice continuously differentiable [analytic] and Theorem 59 is proved.

Our next result shows that every one-parameter subgroup is differentiable in an arbitrary differentiable coordinate system. This constitutes the first major step in the direction of proving that certain functions not assumed a priori to be differentiable do, in fact, turn out to be differentiable after all.

Theorem 60: If D is an arbitrary differentiable coordinate system in a local Lie group G, and if g is an arbitrary one-parameter subgroup, then g is differentiable in D (see A)).

Proof: Since by Theorem 59 we may introduce in G a canonical coordinate system of the first kind by means of a two times differentiable coordinate transformation. We can assume that the coordinate system D is substituted by a canonical coordinate system of the first kind D' .

Let U denote the (star-shaped) neighborhood of the identity $e \in G$ in which D' is defined and let V denote another star-shaped neighborhood of e so small that the product of an arbitrary pair of elements in V is defined and lies in U (see Section 23, E)). Let α be a positive number so small that $g(t) \in V$ for all $|t| \leq \alpha$. We denote by $g^i(t)$ the coordinates of the point $g(t)$ in the coordinate system D' (for $|t| \leq \alpha$). For each positive integer n, denote by a_n

the vector with components $a_n^i = \frac{n}{\alpha} g^i(\frac{\alpha}{n})$ and let g_n denote the one-parameter subgroup with direction vector a_n . Since D' is a canonical

coordinate system of the first kind, g_n is defined by the equations

$$g_n^i(t) = a_n^i t \quad (25)$$

for all values of the argument t such that the point $(a_n^1 t, \dots, a_n^n t)$ E lies in U. We shall show that the latter condition is satisfied for all $|t| \leq \alpha$.

Now $g_n(\frac{\alpha}{n}) = g(\frac{\alpha}{n})$ and $g(\frac{\alpha}{n}) \in V$; hence for $|t| \leq \frac{\alpha}{n}$ the point $(a_n^1 t, \dots, a_n^n t)$ is in V so that (25) defines a one-parameter subgroup g_n lying (for $|t| \leq \frac{\alpha}{n}$) in the neighborhood V. Let m be a positive integer, $m < n$, and suppose that for all $|t| \leq \frac{m}{n} \alpha$ equations (25) define a one-parameter subgroup g_n lying (for $|t| \leq \frac{m}{n} \alpha$) in V and that $g_n(\frac{m}{n} \alpha) = g(\frac{m}{n} \alpha)$. Let $\frac{m}{n} \alpha < t \leq \frac{m+1}{n} \alpha$ so that $t = \frac{m}{n} \alpha + \theta$ where $0 < \theta \leq \frac{\alpha}{n}$. Then $g_n(\frac{m}{n} \alpha)$ and $g_n(\theta)$ belong to V so their product is defined and belongs to U. Accordingly we may define $g_n(t) = g_n(\frac{m}{n} \alpha) g_n(\theta)$ and $g_n(-t) = g(t)^{-1}$.

Thus the function g_n is extended onto the enlarged interval $|t| \leq \frac{m+1}{n} \alpha$ and, as may be readily verified, defines a one-parameter subgroup belonging to U. But then (see C)) equations (25) remain valid for $t \leq \frac{m+1}{n} \alpha$. Since $g_n(\frac{m}{n} \alpha) = g(\frac{m}{n} \alpha)$ and $g_n(\frac{\alpha}{n}) = g(\frac{\alpha}{n})$ it follows that $g_n(\frac{m+1}{n} \alpha) = g(\frac{m+1}{n} \alpha)$ and since $g(\frac{m+1}{n} \alpha) \in V$, we have also $g_n(\frac{m+1}{n} \alpha) \in V$. Finally, since V is a star-shaped neighborhood it follows that $g_n(t) \in V$ for all $|t| \leq \frac{(m+1)}{n} \alpha$.

Thus, by induction, we see that equations (25) define a one-parameter subgroup g_n lying in V for all $|t| \leq \alpha$ and satisfying the conditions

$$g_n\left(\frac{m}{n} \alpha\right) = g\left(\frac{m}{n} \alpha\right), \quad m = 0, 1, \dots, n. \quad (26)$$

In particular, letting $m = n$, we find that $a_n^i \alpha = g^i(\alpha)$ so that the vector a_n is, in fact, independent of n. But then the one-parameter subgroup g_n is also independent of n so that we may write, say, $g_n = g^*$, $n = 1, 2, \dots$, whereupon (26) assumes the form

$$g^*\left(\frac{m}{n} \alpha\right) = g\left(\frac{m}{n} \alpha\right), \quad (27)$$

where m and n denote arbitrary positive integers such that $m \leq n$. But then, since g and g^* are both continuous functions, it follows at once that $g = g^*$. Thus g is differentiable and Theorem 60 is proved.

Example 77. Let R denote the topological ring of all real [complex] square matrices of order n , the identity matrix being denoted, as usual, by e . For $x \in R$ we define the matrix $\exp(x)$ by

$$\exp(x) = e + x + \frac{1}{2!} x^2 + \frac{1}{3!} x^3 + \dots \quad (28)$$

It is easy to see that this series is everywhere convergent. Moreover, if x and y are two commuting matrices, then, as is readily verified,

$$\exp(x + y) = \exp(x) \exp(y). \quad (29)$$

In particular $\exp(x) \exp(-x) = e$ so that the determinant of $\exp(x)$ is always different from zero.

Now, the implicit function theorem may be applied to (28) to show that $\exp(x)$ defines a homeomorphic analytic mapping of some neighborhood V_ε of the zero matrix onto a neighborhood W_ε of the identity e of the group G of non-singular matrices. Thus every matrix $w \in W_\varepsilon$ may be written uniquely in the form $w = \exp(x)$, $x \in V_\varepsilon$. The mapping inverse to \exp we denote by the symbol \log so that $x = \log w$.

Thus we may use the entries x_j^i of the matrix x as coordinates of $w = \exp(x)$. (In the complex case the coordinates of w are the real and imaginary parts of x_j^i .) It turns out that these coordinates are canonical coordinates of the first kind. Indeed let $a \in R$ and let s and t be real numbers. Then $\exp(ta)$ is non-singular and therefore belongs to G . Also, since sa and ta commute, we have

$$\exp((s+t)a) = \exp(sa)\exp(ta).$$

Thus, for fixed matrix a , $\exp(ta)$ describes a one-parameter subgroup which, in the coordinates we have just introduced in G , is defined by the equations $x_j^i = ia_j^i$, i.e., x_j^i are in fact canonical coordinates of the first kind.

SECTION 43. THE INVARIANCE THEOREM

In this section it will be shown that any two differentiable coordinate systems in the same Lie group G are connected by a differentiable transformation. The significance of this result has already been discussed in Section 41. It provides the basis for

the coordinate study of Lie groups. In fact, in studying the group operation by means of coordinates we are really studying properties of the system of equations (3) Section 41 and if we are to obtain properties of the group itself we must seek out those properties of the system (3) which remain invariant under coordinate transformations. Theorem 61, proved below, says that it suffices to consider differentiable coordinate transformations.

To facilitate the proof of Theorem 61 we introduce the concept of a canonical coordinate system of the second kind.

A) Let G be a local Lie group and let D be differentiable [analytic] coordinate system in G . We shall say that the one-parameter subgroups g_1, \dots, g_s are linearly independent in the coordinate system D if their direction vectors, as computed in D , are linearly independent. Let r be the number of coordinates in D and select in G a system of r linearly independent one-parameter subgroups

$$g_1, \dots, g_r. \quad (1)$$

Then we define

$$g(t^1, \dots, t^r) = g_1(t^1)g_2(t^2) \dots g_r(t^r). \quad (2)$$

It turns out that there exists a positive number γ small enough so that for $|t^k| < \gamma$, $k = 1, \dots, r$, the product (2) is defined; the points thus obtained fill a certain neighborhood W_γ of the identity in G , each of the points of W_γ being represented in the form (2) in one and only one way for $|t^k| < \gamma$ and, finally, the transition from the given coordinate system D to the coordinate system D^* with coordinates t^1, \dots, t^r thus defined in the neighborhood W_γ is differentiable [analytic]. The coordinate system D^* is called a canonical system of the second kind.

In proving A) we employ the usual notation: $g_k^i(t)$ are the coordinates of the point $g_k(t)$, $g^i(t^1, \dots, t^r)$ the coordinates of $g(t^1, \dots, t^r)$, and finally a_k^i the coordinates of the direction vector a_k of the group g_k all coordinates computed in the system D . The transition from D^* to D is given by the relations

$$x^i = g^i(t^1, \dots, t^r), \quad (3)$$

where x^i are the coordinates of a point x in the system D while t^k are the coordinates of the same point in D^* . In order to prove A) it suffices to show that (3) satisfies the conditions of the definition B) Section 41.

That the system (3) is differentiable [analytic] follows immediately from Theorem 58. Moreover, since $g_k(0) = e$ we have

$g(0, \dots, 0) = e$ and consequently $g^i(0, \dots, 0) = 0$. It remains to compute the derivatives $\frac{\partial}{\partial t^k} g^i(t^1, \dots, t^r)$ at the origin. In carrying out this computation we assign the value zero to all the arguments except t^k . Consequently:

$$\frac{\partial}{\partial t^k} g^i(t^1, \dots, t^r) = \frac{d}{dt} g_k^i(t) = a_k^i \quad \text{for } t^k = t = 0.$$

Thus the Jacobian of (3) is equal to the determinant of the matrix $\|a_k^i\|$, which does not vanish because of the linear independence of the subgroups (1). It follows that the system of equations (3) is solvable in a sufficiently small neighborhood of the identity, and A) is proved.

Before turning to Theorem 61 we make a pair of preparatory remarks.

B) Let G be a local Lie group, let D and D' be two differentiable coordinate systems in G and denote by R and R' the vector spaces associated with G by means of the coordinate systems (see Section 41, C)). Let g be a one-parameter subgroup in G and denote by a and a' , respectively, the direction vectors of g in the coordinate systems D and D' (see Theorem 60), $a \in R$, $a' \in R'$. Then the one-to-one mapping $a \rightleftharpoons a'$ thus obtained between the spaces R and R' is both ways continuous. Consequently we may in a natural manner topologize the collection of all one-parameter subgroups of G with a topology independent of coordinate systems, two subgroups being accounted close together if their direction vectors are close together in some differentiable coordinate system.

By Theorem 59 it is no loss of generality to suppose the coordinate systems D and D' to be (two times differentiable) canonical of the first kind. In order to demonstrate the continuity of the mapping $a \rightarrow a'$ in the vicinity of some vector a , select a positive number τ small enough so that the coordinates $a^i\tau$ and $a'^i\tau$ of the point $g(\tau)$ are defined in both coordinate systems D and D' (see Section 42, B)). It is then at once clear that a small change in a gives rise to a small change in the point $g(\tau)$, which in turn gives rise to a small change in its coordinates $a'^i\tau$, i.e., to a small change in a' . In other words, the mapping $a \rightarrow a'$ is continuous. The continuity of the mapping $a' \rightarrow a$ is proved exactly the same way.

C) Let $f(z^1, \dots, z^k)$ be a function of the variables z^1, \dots, z^k defined in a star-shaped domain U (see Section 42, B)). Then f is said to be homogeneous if for every system of constants c^1, \dots, c^k , the function $f(c^1t, \dots, c^kt)$ of the parameter t , defined for all those values of t for which the point (c^1t, \dots, c^kt) belongs to U , is a linear function of t , i.e.,

$$f(c^1 t, \dots, c^k t) = ct \quad (4)$$

where c does not depend on t . It turns out that a homogeneous function $g(z^1, \dots, z^k)$ that is differentiable is automatically linear:

$$f(z^1, \dots, z^k) = p_1 z^1 + \dots + p_k z^k,$$

where p_1, \dots, p_k are constants.

Indeed, let $(c^1, \dots, c^k) \in U$. Then (4) holds for $|t| \leq 1$ and, for $t = 1$, reads:

$$f(c^1, \dots, c^k) = c. \quad (5)$$

But also, differentiating (4) with respect to t at $t = 0$, we obtain

$$c = \sum_{i=1}^k \frac{\partial}{\partial z^i} f(0, \dots, 0) c^i. \quad (6)$$

Taken together, relations (5) and (6) show that $f(z^1, \dots, z^k)$ is a linear function.

Theorem 61. Let D and D' be two differentiable [analytic] coordinate systems in the same local Lie group G . Denote by x^1, \dots, x^r and x'^1, \dots, x'^s the coordinates of a point x in the systems D and D' respectively. Then $s = r$ and we have

$$x'^i = \varphi^i(x^1, \dots, x^r), \quad i = 1, \dots, r, \quad (7)$$

where φ^i is a three times continuously differentiable [analytic] function and the functional determinant $\left| \frac{\partial \varphi^i}{\partial x^j} \right|$ does not vanish at $x^1 = \dots = x^r = 0$. If D and D' are both canonical coordinate systems of the first kind then the functions (7) are linear:

$$x'^j = \sum_{i=1}^r p_i^j x^i, \quad j = 1, \dots, r.$$

Observe that $r = s$ is a consequence of the invariance of dimension of a local group (see Section 23, N) and Section 16); however, the following proof makes no use of dimension theory.

Proof: We may suppose $r \leq s$. Select, as in A), a system of one-parameter subgroups

$$g_1, \dots, g_r, \quad (8)$$

that are linearly independent in the coordinate system D . That these subgroups possess direction vectors in D' follows from Theorem 60; however it is not a priori clear that they are linearly independent in D' and we overcome this little difficulty by replacing the system (8) by another system obtained from it by making small

changes in the subgroups (see B)). Since $s \geq r$ it is easily seen that by making arbitrarily small changes in the subgroups we can arrange for their linear independence in D' , while, as is clear, if these modifications are small enough the linear independence of the system of subgroups in the coordinate system D will not be disturbed. Thus it is no loss of generality to suppose that the subgroups (8) are linearly independent in both D and D' . If $s > r$, we adjoin to (8) new one-parameter subgroups g_{r+1}, \dots, g_s so that the new system

$$g_1, \dots, g_r, g_{r+1}, \dots, g_s \quad (9)$$

is linearly independent in D' . Finally we use (8) and (9) to construct canonical coordinate systems D^* and D'^* of the second kind.

Let U and U' denote the neighborhoods in which the coordinate systems D^* and D'^* are defined and let t be a positive number small enough so that $g_{r+1}(t) \in U \cap U'$. Then the coordinates of $g_{r+1}(t)$ in D'^* are the numbers $t'^1 = 0, \dots, t'^r = 0, t'^{r+1} = t, t'^{r+2} = 0, \dots, t'^s = 0$. Let t^1, \dots, t^r denote the coordinates of $g_{r+1}(t)$ in D^* . Then

$$\begin{aligned} g_1(t^1)g_2(t^2)\dots g_r(t^r)g_{r+1}(0)\dots g_s(0) &= g_1(0)g_2(0)\dots g_{r+1}(t) \\ &\dots g_s(0). \end{aligned}$$

Viewing this equation in the coordinate system D'^* , we conclude that $t = 0$ which is a contradiction. Hence $s = r$ and consequently $D^* = D'^*$. Since by A) the transitions from D to D^* and from D' to D'^* are both differentiable [analytic], the same is true of the transition from D to D' .

Finally if both D and D' are canonical coordinate systems of the first kind then the functions (7) are homogeneous (see C)) as may be seen by taking for x^1, \dots, x^r the coordinates of a point that traces out a one-parameter subgroup. But then they must be linear, and Theorem 61 is proved.

Theorem 61 yields the following important corollary.

D) Let φ be a local isomorphism of a local Lie group G onto a local Lie group G' and let D and D' be differentiable [analytic] coordinate systems in G and G' , respectively. Denote by x^1, \dots, x^r the coordinates in D of a point $x \in G$ and by x'^1, \dots, x'^s the coordinates in D' of the image $x' = \varphi(x)$. Thus

$$x'^j = \varphi^j(x^1, \dots, x^r), \quad j = 1, \dots, s. \quad (10)$$

Then $s = r$, the functions φ^j are three times continuously differentiable

[analytic], and the functional determinant $\left| \frac{\partial \varphi^j}{\partial x^i} \right|$ does not vanish at $x^1 = \dots = x^r = 0$. In particular, every local automorphism φ of a local Lie group G is defined in D by means of a system (10) of three times continuously differentiable [analytic] functions with non-vanishing functional determinant. Thus, for example, this is true of the inner automorphisms $\varphi_a(x) = a^{-1}x a$ where a denotes a fixed element of G . If the coordinate systems D and D' are canonical of the first kind then the functions φ^i are linear.

In order to prove the assertion it suffices to use the mapping φ to import into G a new coordinate system D'' in which the coordinates of a point $x \in G$ are just the coordinates of $\varphi(x) \in G'$ in the system D' , and then apply Theorem 61 to D and D'' .

Example 78: Let G be a commutative Lie group and define in G a canonical coordinate system of the second kind. Let $g(t^1, \dots, t^r)$ denote the point with coordinates t^i . Then, as is not hard to see, the multiplication of two group elements is given by the formula

$$g(s^1, \dots, s^r)g(t^1, \dots, t^r) = g(s^1 + t^1, \dots, s^r + t^r).$$

It follows that any commutative Lie group is locally isomorphic with a vector group.

SECTION 44. SUBGROUP AND FACTOR GROUP

In this section it will be shown that every subgroup H of a local Lie group G is itself a local Lie group differentiable or analytic, depending on G . Similarly, it will be shown that every factor group G^* of a local Lie group is itself a local Lie group and the natural projection of G onto G^* is given by differentiable functions. Thus it will be shown that in studying subgroups and factor groups there is no loss of generality in sticking to differentiable functions.

Lemma. Let H be a subgroup of a local Lie group G . Then there exists in G a canonical coordinate system D^* of the second kind defined in a neighborhood W_γ (see Section 43, A)) such that the intersection $M_\gamma = W_\gamma \cap H$ consists of precisely those points $x \in W_\gamma$ whose coordinates (t^1, \dots, t^r) satisfy the conditions

$$t^1 = \dots = t^{r-s} = 0, \quad (1)$$

(the number s being determined by the subgroup H) and such that, for

arbitrary elements $v_1, v_2 \in M_\gamma$, the products $v_1^{-1} v_2$ and $v_1 v_2$ are defined and belong to H .

Proof: Let D' be a canonical coordinate system of the first kind in G defined, say, in an open set V . The coordinates of a point $x \in V$ in D' will be denoted x^1, \dots, x^r . Let U_α , $\alpha > 0$, denote the set of those points x for which

$$x^1 x^1 + \dots + x^r x^r < \alpha^2. \quad (2)$$

There exists a positive number β small enough so that: 1) for arbitrary numbers y^1, \dots, y^r satisfying the inequality $y^1 y^1 + \dots + y^r y^r \leq \beta^2$ there exists a point $y \in V$ having coordinates y^i ; 2) the product of any $r+1$ elements of \bar{U}_β is defined, and if these elements belong to H so must their product (see Section 23, E)); 3) the set $\bar{U}_\beta \cap H$ is closed in \bar{U}_β . By making a similarity transformation of coordinates we may, and do, arrange things so that $\beta = 1$, and we write $U_\beta = U$.

Let now $b \in U \cap H$ and let b^i be the coordinates of b in D' . We write $\sqrt{b^1 b^1 \dots b^r b^r} = \rho$ and show that if m is a positive integer such that $m\rho < 1$ then the element $(b)^m$ has coordinates mb^i and belongs to H :

$$(b)^m \in H \text{ for } m \rho < 1. \quad (3)$$

To this end, consider the one-parameter subgroup g whose direction vector has the coordinates b^i . Then $g^i(t) = b^i t$, $|t| \leq \frac{1}{\rho}$ (see Section 42, B); in particular, $b = g(1) \in U \cap H$. We show by induction that the powers $(b)^2, \dots, (b)^m$ are defined and all belong to $U \cap H$. Let $p < m$ and suppose the power $(b)^p$ is defined and belongs to $U \cap H$. Then the product $(b)^p b = (b)^{p+1}$ is defined and belongs to H . Moreover since $p+1 < \frac{1}{\rho}$ it also follows that $g(p+1)$ is defined and belongs to U . But, since g is a one-parameter subgroup, we have $g(p+1) = (b)^{p+1}$ and consequently $(b)^{p+1} \in U \cap H$. Thus (3) is proved.

Let now

$$g_1, \dots, g_k, \quad k \geq 0, \quad (4)$$

be a system of one-parameter subgroups whose direction vectors $a_j = (a_j^1, \dots, a_j^r)$, $j = 1, \dots, k$, constitute an orthonormal system, i.e., satisfy the condition

$$\sum_{i=1}^r a_p^i a_q^i = \delta_{pq}. \quad (5)$$

Since the vectors a_j are unit vectors it follows that the subgroups g_j are defined and belong to U for $|t| \leq 1$. Suppose now also that $g_j(t) \in H$ for all $|t| \leq 1$, $j = 1, \dots, k$, and denote by H_k the collection of all elements of the form

$$g(t^1, \dots, t^k) = g_1(t^1)g_2(t^2) \dots g_k(t^k), \quad |t^j| \leq 1, \quad j = 1, \dots, k. \quad (6)$$

For $k = 0$ we define $H_0 = \{e\}$.) We shall show that there exist just two possibilities: a) the set H_k contains some neighborhood of the identity in the subgroup H ; b) there exists a one-parameter subgroup g_{k+1} with unit direction vector a_{k+1} orthogonal to all the vectors a_1, \dots, a_k such that $g_{k+1}(t) \in H$, $|t| \leq 1$.

Denote by L_k the set of elements $x \in U$, the coordinates x^1, \dots, x^r of which satisfy the linear equations

$$\sum_{i=1}^r a_j^i x^i = 0, \quad j = 1, \dots, k. \quad (7)$$

(For $k = 0$ we simply let $L_0 = U$.) Denote also by

$$g(t^1, \dots, t^k; x) \quad (8)$$

the element $g(t^1, \dots, t^k)x^{-1}$ where $x \in U$. The set of all elements of the form (8), for fixed x and for $|t^j| \leq 1$, $j = 1, \dots, k$ is $H_k x^{-1}$. Let us consider the intersection of the sets L_k and $H_k x^{-1}$ for x close to e . Denote by $g^i(t^1, \dots, t^k; x)$ the coordinates of (8). Then the intersection of L_k with $H_k x^{-1}$ is obtained by solving the system of equations

$$\sum_{i=1}^r a_j^i g^i(t^1, \dots, t^k; x) = 0, \quad j = 1, \dots, k. \quad (9)$$

with respect to the parameters t^1, \dots, t^k . Clearly for $x = e$ this system has the solution $t^p = 0$, $p = 1, \dots, k$. Let us compute the Jacobian of the system at this point. We have

$$\frac{\partial}{\partial t^j} g^i(t^1, \dots, t^k; x) = \frac{d}{dt} g_j^i(t) = a_j^i \text{ for } t = 0, \quad (10)$$

and consequently

$$\frac{\partial}{\partial t^j} \sum_{i=1}^r a_j^i g^i(t^1, \dots, t^k; x) = \sum_{i=1}^r a_j^i a_j^i = \delta_{hj}$$

(see (10) and (5)). Thus for x sufficiently close to e the system (9) possesses a unique solution close to the origin and depending continuously on x . But this says that for x sufficiently close to e the sets L_k and $H_k x^{-1}$ have a unique point of intersection $\varphi(x)$ depending continuously on x and satisfying $\varphi(e) = e$. Suppose now that a) does not hold. Then there exists a sequence

$$b_1, \dots, b_n, \dots \quad (11)$$

in the set $H \setminus H_k$ that converges to e . Let $c_n = \varphi(b_n)$. Since $\varphi(x)$ is continuous and $\varphi(e) = e$, the sequence

$$c_1, \dots, c_n, \dots \quad (12)$$

also converges to e . Since $\varphi(x) \in L_k$ this sequence lies in L_k . But it also lies in H . Indeed $c_n \in H_k b_n^{-1} \subset H$ since $b_n^{-1} \in U$. Note also the important fact that no element of (12) can equal e , for if $c_n = e$ we would have $e \in H_k b_n^{-1}$ and hence $b_n \in H_k$, which is contrary to hypothesis. Thus, altogether,

$$c_n \in L_k, \quad c_n \in H, \quad c_n \neq e, \quad \lim_{n \rightarrow \infty} c_n = e. \quad (13)$$

We denote now by

$$c_n^i \quad (14)$$

the coordinates of c_n and let

$$\rho_n = \sqrt{c_n^1 c_n^1 + \dots + c_n^r c_n^r}. \quad (15)$$

The point with coordinates

$$\frac{1}{\rho_n} c_n^i = a_n^i \quad (16)$$

we denote by a_n^i . Then a_n^i lies in the intersection of \bar{L}_k with the boundary of U and consequently the sequence

$$a_1^i, \dots, a_n^i, \dots, \quad (17)$$

has a limit point a also lying in the intersection of \bar{L}_k with the boundary of U . Let a_{k+1}^i be the coordinates of a in the coordinate system D' . Then since $a \in \bar{L}_k$ these coordinates satisfy the system of equations (7). Moreover,

$$a_{k+1}^1 a_{k+1}^1 + \dots + a_{k+1}^r a_{k+1}^r = 1,$$

since a is in the boundary of U . Consider the one-parameter subgroup g_{k+1} having direction vector a_{k+1} . The vector a_{k+1} is a unit

vector and is orthogonal to the vectors a_1, \dots, a_k . We shall complete the proof by showing that $g_{k+1}(t) \in H$, $|t| \leq 1$. The point $c_n \in H$ has coordinates $\rho_n a_n^{i_n}$ (see (16)) and it follows (see (3)) that the point $(c_n)^m$ is in H and has coordinates $m\rho_n a_n^{i_n}$ provided $m\rho_n < 1$. Let $0 < t \leq 1$. Since a is a limit point of the sequence (17) while $\lim \rho_n = 0$ (see (13)) it follows that for any given positive ϵ there exist positive integers n and m such that $m\rho_n < 1$ and $|ta_{k+1}^i - m\rho_n a_n^{i_n}| < \epsilon$, $i = 1, \dots, r$. Thus $g_{k+1}(t)$ is a limit point of the set of points of the form $(c_n)^m \in \bar{U} \cap H$, and since $\bar{U} \cap H$ is a compact we have $g_{k+1}(t) \in H$.

Thus condition a) must hold if b) fails, and using this inductive construction, we may enlarge the system (4), beginning with $k = 0$ and proceeding step by step until we arrive at a system

$$g_1, \dots, g_s, \quad (18)$$

for which a) is satisfied. The direction vectors a_1, \dots, a_s of the system (18) are linearly independent since they are orthogonal (5). Finally, if $s < r$ we may enlarge (18) to a complete linearly independent system

$$h_1, \dots, h_{r-s}, g_1, \dots, g_s. \quad (19)$$

Then, according to A) Section 43, the system (19) may be used to introduce in G a canonical coordinate system D^* of the second kind defined in some neighborhood W_γ . Since the subsystem (18) satisfies condition a), there exists a neighborhood Γ of the identity in H such that $\Gamma \subset H_s$. For sufficiently small γ we have then $W_\gamma \cap H \subset \Gamma \subset H_s$ and, for the canonical coordinate system D^* restricted to such a neighborhood W_γ , the conditions of the lemma are satisfied.

Theorem 62: Let H be a subgroup of a local Lie group G . Then H is also a local Lie group and is analytic if G is. Moreover, let D and E be differentiable [analytic] coordinate systems in G and H , let x^1, \dots, x^r and y^1, \dots, y^s be the coordinates of the same point $x \in H$ in the two systems D and E respectively, and let

$$x^i = \psi^i(y^1, \dots, y^s), \quad i = 1, \dots, r. \quad (20)$$

Then the functions ψ^i are three times continuously differentiable [analytic] and the functional matrix $\left\| \frac{\partial \psi^i}{\partial y^j} \right\|$ has rank s . In particular, it follows that $s \leq r$. Finally, if D and E are canonical coordinate systems of the first kind then the functions (20) are linear:

$$x^i = \sum_{j=1}^s p_j^i y^j, \quad i = 1, \dots, r. \quad (20')$$

Proof: Let D^* be the canonical coordinate system of the second kind constructed in the preceding lemma, so that D^* is defined in an open set W_γ possessing the property that the intersection $M_\gamma = W_\gamma \cap H$ is given in D^* by the equations

$$t^1 = \dots = t^{r-s} = 0. \quad (21)$$

Note that if G is analytic then D^* is an analytic coordinate system (see Section 43, A)). Let the group multiplication be defined in D^* by the functions

$$z^i = f^i(x^1, \dots, x^r; y^1, \dots, y^r), \quad i = 1, \dots, r \quad (22)$$

(see Section 41 (3)). Then the functions f^i are defined and three times continuously differentiable [analytic] for all sufficiently small values of their arguments. We now introduce in H a coordinate system E^* by taking as the coordinates of a point $x = (0, \dots, 0, x^{r-s+1}, \dots, x^r) \in M_\gamma$ the numbers x^{r-s+1}, \dots, x^r . Then in the coordinate system E^* the equations for the group multiplication of elements of the subgroup H have the form

$$\begin{aligned} z^i &= f^i(0, \dots, 0, x^{r-s+1}, \dots, x^r; 0, \dots, 0, y^{r-s+1}, \dots, y^r), \\ i &= r - s + 1, \dots, r. \end{aligned}$$

But this shows that H is a local Lie group and that H is analytic if G is. Moreover, in the coordinate systems D^* and E^* relations (20) assume the simple form

$$x^1 = \dots = x^{r-s} = 0, \quad x^i = y^i, \quad i = r - s + 1, \dots, r. \quad (23)$$

whence it follows by Theorem 61 that for arbitrary differentiable [analytic] coordinate systems D and E the function ψ^i are three times continuously differentiable [analytic] and that the rank of the matrix $\left\| \frac{\partial \psi^i}{\partial y^j} \right\|$ is always equal to s .

Finally, suppose D and E are canonical coordinate systems of the first kind and substitute for y^1, \dots, y^s in the right members of (20) the coordinates $b^1 t, \dots, b^s t$ of a point $g(t)$ that traces out a one-parameter subgroup. The variables x^1, \dots, x^r are then the coordinates in the system D of the same point $g(t)$ and must have the form $a^1 t, \dots, a^r t$. Thus the functions ψ^i are homogeneous and therefore linear (see Section 43, C)).

A) Let G be a local Lie group, let H be a subgroup, and denote by D^* the canonical coordinate system of the second kind constructed in the above lemma. We turn now to the consideration of the subset L_γ of the neighborhood W_γ defined by the equations $t^{n+1} = \dots = t^r = 0$ where $n = r - s$. Each element of L_γ has coordinates

$$t^1, \dots, t^n, 0, \dots, 0; |t^i| < \gamma,$$

and the numbers t^1, \dots, t^n may be taken as the coordinates of this element in a new system B^* defined in L_γ . Every $w \in W_\gamma$ can be written uniquely in the form $w = uv$ where $u \in L_\gamma$, $v \in M_\gamma$. Choose ϵ so small that $W_\epsilon W_\epsilon^{-1} W_\epsilon \subset W_\gamma$. Then for every element $w \in W_\epsilon$ we have $W_\epsilon \cap wH = uM_\epsilon$ where the element $u \in L_\epsilon$ is uniquely determined by w . Thus every left coset $W_\epsilon \cap wH$, $w \in W_\epsilon$, of the subgroup H meets L_ϵ in exactly one point u . The coordinates in B^* of this element u may be taken as the coordinates of the corresponding coset wH , thus defining a coordinate system C^* in an open set K_ϵ of the space G/H (See Section 23, J)) consisting of all of the cosets that meet W_ϵ .

In order to prove the various assertions here made let g_1, \dots, g_r be the one-parameter subgroups employed in constructing the coordinate system D^* (see Section 43, A)). Then every element $w \in W_\gamma$ may be written uniquely in the form

$$w = g_1(t^1) g_2(t^2) \dots g_r(t^r), |t^i| < \gamma. \quad (24)$$

Let $u = g_1(t^1) g_2(t^2) \dots g_n(t^n)$, $v = g_{n+1}(t^{n+1}) g_{n+2}(t^{n+2}) \dots g_r(t^r)$. Then

$$w = uv, \quad u \in L_\gamma, \quad v \in M_\gamma, \quad (25)$$

and since the expression (24) is unique, the factorization (25) is unique also. Let now $w \in W_\epsilon$. By (25) we have $w = uv$, $u \in L_\epsilon$, $v \in M_\epsilon$. Consider the intersection $W_\epsilon \cap wH$. If $h \in H$ satisfies the condition $wh \in W_\epsilon$ then $h \in W_\epsilon^{-1} W_\epsilon$ and $vh \in W_\epsilon W_\epsilon^{-1} W_\epsilon \subset W_\gamma$ so that $vh \in M_\gamma$. But then, since $u(vh) \in W_\epsilon$ it follows that $vh \in M_\epsilon$. Thus $wh = u(vh) \in uM_\epsilon$, and we have $W_\epsilon \cap wH \subset uM_\epsilon$. In order to verify the reverse inclusion let $v' \in M_\epsilon$. Cancelling u in the equation $uv' = wh$ we obtain $v' = vh$, and since both v and v' belong to M_ϵ it follows that the product $v'^{-1} v'$ is defined and belongs to H (see the lemma). Thus $h = v'^{-1} v' \in H$ satisfies the equation $uv' = wh \in wH$ so that $uM_\epsilon \subset W_\epsilon \cap wH$ and the equation $uM_\epsilon = W_\epsilon \cap wH$ is proved. Finally the uniqueness of the element u defined by this relation follows from the uniqueness of the factorization (25), and proposition A) follows.

Theorem 63: Let G be a local Lie group, let F be a factor group, and let χ denote the natural projection of G onto F . Then F is also a local Lie group and is analytic if G is. Moreover, let D and C be differentiable [analytic] coordinate systems in G and F , respectively, let y^1, \dots, y^r be the coordinates of a point $y \in G$ in the system D , let x^1, \dots, x^n be the coordinates of the projection $\chi(y)$ in the system C , and let

$$x^i = \chi^i(y^1, \dots, y^r), \quad i = 1, \dots, n. \quad (26)$$

Then the functions χ^i are three times continuously differentiable [analytic] and the functional matrix $\left\| \frac{\partial \chi^i}{\partial y^j} \right\|$ has rank n . In particular, we have $n \leq r$. Finally, if the coordinate systems D and C are canonical coordinate systems of the first kind, then the functions (26) are linear:

$$x^i = \sum_{j=1}^n q_j^i y^j, \quad i = 1, \dots, n. \quad (26')$$

Proof: Let H be the kernel of the projection χ , let D^* be a canonical coordinate system of the second kind as described in the lemma and let the equations of group multiplication have the following form in D^* :

$$z^i = f^i(x^1, \dots, x^n; y^1, \dots, y^r), \quad i = 1, \dots, r. \quad (27)$$

The functions f^i are three times continuously differentiable [analytic] (see Section 43, A)). We introduce in the factor group F the coordinate system C^* described in A) by taking as coordinates of the coset uH , $u \in L_\varepsilon$, the coordinates of u in the system B^* . Let x and y be two elements of L_ε close enough to the identity so that $z = xy \in W_\varepsilon$. Let the coordinates of x and y in B^* be x^1, \dots, x^n and y^1, \dots, y^n and let the coordinates of z in D^* be z^1, \dots, z^r . If x^*, y^*, z^* are the cosets containing x, y, z respectively then the coordinates of x^*, y^*, z^* in the coordinate system C^* are just $x^1, \dots, x^n; y^1, \dots, y^n; z^1, \dots, z^n$. Thus

$$z^i = f^i(x^1, \dots, x^n, 0, \dots, 0; y^1, \dots, y^n, 0, \dots, 0), \\ i = 1, \dots, n.$$

But this shows that the multiplication of elements in the factor group F is defined by three times continuously differentiable [analytic] functions in the coordinate system C^* so that F is a local Lie group which is analytic if G is analytic.

Now if y^1, \dots, y^r are the coordinates of an element $y \in G$ in the coordinate system D^* while x^1, \dots, x^n are the coordinates of the projection $\chi(y)$ in the coordinate system C^* then we have

simply

$$x^i = y^i, \quad i = 1, \dots, n. \quad (28)$$

Thus in the coordinate systems D^* , C^* the functions χ^i assume a particularly simple form and in this case the assertion of the theorem is obviously satisfied. But from this and from Theorem 61 it follows that the assertions made in the theorem regarding the functions χ^i are satisfied for arbitrary differentiable [analytic] coordinate systems D , C .

Finally, suppose D and C are canonical coordinate systems of the first kind. Substituting for the variables y^1, \dots, y^r in relations (26) the coordinates $b^1 t, \dots, b^r t$ of an element $g(t)$ that traces out a one-parameter subgroup we obtain for the variables x^1, \dots, x^n expressions of the form $a^1 t, \dots, a^n t$, since the element $\chi(g(t))$ also traces out a one-parameter subgroup. But then, as before, it follows from proposition C) Section 43 that the functions χ^i are linear.

Taken together, Theorems 61, 62, and 63 show that from now on we need consider only differentiable functions in studying Lie groups.

We mention here a particularly important corollary of Theorem 62.

B) It was shown in Example 76 that the topological group G of all non-singular square complex matrices of order n is an analytic Lie group. Hence, according to Theorem 62, all of the subgroups of G are also analytic Lie groups.

Example 79: Let G be the group of all real non-singular square matrices of order n , and denote by H the subgroup of all orthogonal matrices. Denote also by F the multiplicative group of non-zero real numbers and by χ the homomorphism of G onto F that associates with each matrix $w \in G$ its determinant. The kernel N of χ consists of all matrices with determinant 1. As canonical coordinates of the first kind for the matrix w we may take the elements x_j^i of the matrix $x = \log w$ (see Example 77) while as canonical coordinates of a number $v \in F$ we may, as is easily seen, take the number $y = \log v$ (these canonical coordinates in G and F are, of course, defined only in suitably small neighborhoods of the identity). We show that, in these coordinate systems, the subgroup H is defined by the linear equations

$$x_j^i + x_i^j = 0, \quad i, j = 1, \dots, n, \quad (29)$$

(see Theorem 62, (20')); note that here i, j do not denote indices

of summation) and that x is defined by the relations

$$y = \text{Tr}(x) = x_i^i \quad (30)$$

(see Theorem 63, (26')) so that N is defined by the equation

$$\text{Tr}(x) = 0. \quad (31)$$

Indeed, denoting by u^* the transpose of the matrix u , we have

$$(\exp(x))^* = \exp(x^*) \quad (32)$$

(see Section 42, (28)). Suppose now that x satisfies (29), i.e., that x is a skew-symmetric matrix; then $x^* = -x$ and from (32) we obtain

$$(\exp(x))^* = \exp(x^*) = \exp(-x) = (\exp(x))^{-1} \quad (33)$$

In other words, if x is skew-symmetric then $\exp(x)$ is orthogonal (see Example 3). Conversely, if $w \in W_\epsilon$ is an orthogonal matrix then

$$x^* = (\log(w))^* = \log(w^*) = \log(w^{-1}) = -\log(w) = -x,$$

i.e., x is skew-symmetric. Accordingly, in the vicinity of the identity, the subgroup H is defined by (29).

We consider next the homomorphism x . A matrix u is said to be triangular if its entries u_{ij} satisfy the condition $u_{ij} = 0$ for $i < j$. It is well known that for any square matrix x there exists a non-singular matrix t (in general, t has complex entries) such that txt^{-1} is triangular. Now for the transformed matrix txt^{-1} , it follows immediately from (28) Section 42 that

$$\exp(txt^{-1}) = t(\exp(x)t^{-1}).$$

Moreover, as is easily verified, both the trace and the determinant of txt^{-1} are the same as those of x . But then it follows that

$$\text{Det}(\exp(x)) = e^{\text{Tr}(x)} \quad (34)$$

(here e denotes the basis of the system of natural logarithms and not the identity matrix). Indeed, for a triangular matrix x this relation is an immediate consequence of (28) Section 42, while, as we have just seen, an arbitrary matrix x may be transformed into triangular form without changing either member of equation (34). But, now, (30) is an immediate consequence of (34).

SECTION 45. LIE GROUPS AND ANALYTIC MANIFOLDS

The coordinate method makes it possible to determine the location of a point in a space by giving a system of numbers—its coordinates; conversely, it makes it possible to interpret a system of numbers as a point in the space. Thus the coordinate method opens up the possibility of the application of algebra and analysis to geometry, as well as the possibility of interpreting geometrically objects that are not geometrical, and in this lies its importance in mathematics. Now, in Euclidean spaces the coordinate method may be employed without any complications, for in this case there is a one-to-one correspondence between the points of the space and their coordinates; but in other spaces things are not so simple. Geographical coordinates on the surface of the earth, for instance, are more complicated: longitude varies only from 0° to 360° (moreover, 0° and 360° are to be identified), latitude varies only from -90° to $+90^\circ$, while at the poles the longitude is not defined at all. Thus geographical coordinates do not yield a one-to-one correspondence between the points of the earth's surface and number pairs, and this not because latitude and longitude are an unfortunate choice for a coordinate system but, rather, because it is impossible to define a completely perfect coordinate system on a sphere. In general, unless a given space is homeomorphic with some Euclidean space it will not be possible to define in it a single coordinate system that is as perfect as that available in Euclidean space. On the other hand, geometry itself, as well as other branches of mathematics and natural science (algebra, mechanics, etc.), lead us to the study of spaces that are not homeomorphic with Euclidean space. For these more general spaces it is just as desirable to employ the coordinate method, but it is not possible to introduce a single coordinate system that is satisfactory for the entire space. Consequently, one is led to the use of local coordinates i. e., coordinate systems that are only defined in parts of the space. In those parts of the space where two local coordinate systems overlap they are connected with one another by means of transformations, and on these transformations various conditions may be imposed according to circumstances; sometimes they are required to be continuously differentiable to some specified order, sometimes they are required to be analytic. According to the various requirements imposed upon the transformations connecting different local coordinate systems there arise different mathematical concepts: differentiable manifolds and analytic manifolds. In this section we give a precise definition of these concepts and show that the space of a Lie group,

as well as any space on which a Lie group acts as a transitive transformation group, are in a natural way analytic manifolds

A) A separable Hausdorff space is said to be an r -dimensional topological manifold if every point of the space has a neighborhood that is homeomorphic with some open set in r -dimensional Euclidean space. Obviously a topological manifold is locally compact and locally connected (see Definition 19 and Section 15, H)). A compact topological manifold is ordinarily said to be closed.

B) Let U be a topological space that admits a homeomorphism φ onto an open set of r -dimensional Euclidean space E^r and suppose a Cartesian coordinate system has been fixed in E^r . Taking the coordinates of the point $\varphi(x) \in E^r$ as the coordinates of the point $x \in U$ we define in U a coordinate system D . If D and D' are two coordinate systems defined in U in this manner then the coordinates x^1, \dots, x^r of the point $x \in U$ in the system D and the coordinates x'^1, \dots, x'^r of the same point x in the system D' are connected by relations of the form

$$x'^i = g^i(x^1, \dots, x^r), \quad i = 1, \dots, r, \quad (1)$$

$$x^i = g^i(x'^1, \dots, x'^r), \quad i = 1, \dots, r, \quad (2)$$

where g^i and g^i are continuous functions. If g^i and g^i are also differentiable then the functional determinants $|\frac{\partial g'^i}{\partial x^j}|$ and $|\frac{\partial g^i}{\partial x'^j}|$ are different from zero since their product is equal to one. Let m denote either a fixed positive integer or ∞ . From the implicit function theorem it follows that if the function g^i are m times continuously differentiable [analytic] and the functional determinant $|\frac{\partial g^i}{\partial x^j}|$ is different from zero at every point $x \in U$ then the functions g^i are m times continuously differentiable [analytic]. If g^i and g^i are m times continuously differentiable [analytic] then D and D' will be said to belong to the same differentiability type of class m [analyticity type]. If a certain differentiability type of class m [analyticity type] of coordinate systems has been distinguished on U then we shall say of U itself that it is a differentiable coordinate space of class m [analytic coordinate space]. In order to distinguish on U a differentiability [analyticity] type it suffices to designate one coordinate system belonging to that type. If U is a differentiable coordinate space of class m [analytic coordinate space] then by a coordinate system on U will always be understood a coordinate system belonging to the distinguished type. Let U be a differentiable

coordinate space of class m [analytic coordinate space] and let φ be one of the mappings of U into Euclidean space defining a coordinate system on U . If W is an open subset of U then φ likewise defines a coordinate system on W so that W itself becomes a differentiable coordinate space of class m [analytic coordinate space]. Such a coordinate space we shall call a part of the coordinate space U .

Definition 40: Let M be a topological manifold of dimension r . Then an open covering Σ of M is differentiable of class m [analytic] if every one of the covering sets is a differentiable coordinate space of class m [analytic coordinate space] and if, moreover, the intersection $W = U \cap V$ of any two covering sets (provided W is not empty) is the same differentiable [analytic] coordinate space whether viewed as a part of U or as a part of V . The latter requirement amounts to saying that the differentiability [analyticity] type induced on W by U coincides with that induced on W by V . Two differentiable open coverings of class m [analytic open coverings] Σ, Σ' of the manifold M are said to belong to the same differentiability type [analyticity type] if the covering $\Sigma \cup \Sigma'$ is also differentiable of class m [analytic]. Finally, we shall say that a differentiable structure of class m [analytic structure] is defined on the topological manifold M if a definite differentiability type of class m [analyticity type] of coverings has been distinguished on it. A topological manifold equipped with a differentiable structure of class m [analytic structure] is a differentiable manifold of class m [analytic manifold].

If M is a differentiable [analytic] manifold then, unless the contrary is specified, all differentiable [analytic] open coverings of M will be assumed to belong to the distinguished differentiability [analyticity] type. Let M be a differentiable [analytic] manifold, let Σ be a differentiable covering of M , let U be any one of the covering sets belonging to Σ , and let D be one of the coordinate systems defined on U . Then D is said to be a local coordinate system in M . If D' is any other local coordinate system in M defined, say, on the open set U' and if x^1, \dots, x^r and x'^1, \dots, x'^r are the coordinates in the systems D and D' , respectively, of the same point $x \in U \cap U'$ then

$$x'^i = h'^i(x^1, \dots, x^r), \quad i = 1, \dots, r, \quad (3)$$

$$x^i = h^i(x'^1, \dots, x'^r), \quad i = 1, \dots, r, \quad (4)$$

where the functions h'^i and h^i are m times continuously differentiable [analytic].

Definition 41: Let P and Q be differentiable manifolds of class m [analytic manifolds] of dimensions r and s , let φ be a continuous mapping of P into Q and let $x_0 \in P$. Let also D be a local coordinate system in P defined in some neighborhood of x_0 , let E be a local coordinate system in Q defined in some neighborhood of the point $y = \varphi(x_0)$, and let x be any point of P sufficiently close to x_0 so that the coordinates x^1, \dots, x^r of the point x are defined in the coordinate system D and the coordinates y^1, \dots, y^s of $y = \varphi(x)$ are defined in E . Then we define the functions

$$y^j = \varphi^j(x^1, \dots, x^r), \quad j = 1, \dots, s. \quad (5)$$

The mapping φ is said to be differentiable [analytic] at x_0 if the functions φ^j are m times continuously differentiable [analytic] in the vicinity of x_0 . The mapping φ is differentiable [analytic] if it is differentiable [analytic] at every point $x_0 \in P$. Finally φ is a differentiable [analytic] homeomorphism if it is a homeomorphism and if the mappings φ and φ^{-1} are both differentiable [analytic].

C) Let M_1 and M_2 be two differentiable manifolds of class m [analytic manifolds] of dimension r_1 and r_2 , and let Σ_1 and Σ_2 be differentiable [analytic] open coverings of the manifolds M_1 and M_2 respectively. Let $P = M_1 \times M_2$ be the product of M_1 and M_2 . If D_1 is a coordinate system defined in a covering set $U_1 \in \Sigma_1$ and D_2 a coordinate system defined in covering set $U_2 \in \Sigma_2$ and if the coordinates of a point $x_1 \in U_1$ in the system D_1 are $x_1^1, \dots, x_1^{r_1}$ while the coordinates of a point $x_2 \in U_2$ in the system D_2 are $x_2^1, \dots, x_2^{r_2}$ then, in the neighborhood $U_1 \times U_2$, we define a coordinate system D by taking as the coordinates of a point $(x_1, x_2) \in U_1 \times U_2$ the numbers $x_1^1, \dots, x_1^{r_1}, x_2^1, \dots, x_2^{r_2}$. It is easy to verify that with this choice of coordinates the covering Σ of the manifold P consisting of the open sets $U_1 \times U_2$, $U_1 \in \Sigma_1$, $U_2 \in \Sigma_2$, is differentiable of class m [analytic] and consequently determines a differentiable structure of class m [analytic structure] on the product manifold P . The differentiable [analytic] manifold P thus obtained is called the product of the differentiable [analytic] manifolds M_1 and M_2 . Let φ be a function of two variables $x_1 \in M_1$, $x_2 \in M_2$, that takes its values in Q where Q is also a differentiable manifold of class m [analytic manifold]. Then φ is said to be differentiable [analytic] if it is a differentiable [analytic] mapping of the product manifold P into Q .

The following Theorems 64, 65, 66 are proved here only for analytic Lie groups, but proofs may be given in exactly the same fashion for differentiable Lie groups, the analytic manifolds and

analytic functions being replaced throughout by differentiable manifolds and functions differentiable of class 3. By considering only analytic Lie groups we do not, in fact, lose any generality inasmuch as, according to the results of Chapter 10, it is possible to introduce analytic coordinates in any Lie group.

Theorem 64: An analytic Lie group G is a topological manifold. Moreover, there exists one and only one analytic structure on G with respect to which the function $\varphi(x, y) = xy^{-1}$ is analytic.

Proof: Let D be a fixed analytic coordinate system defined on a neighborhood U of the identity $e \in G$ and let V be a neighborhood of the identity so small that for any three elements x_1, x_2, x_3 belonging to V the product $x_1 x_2^{-1} x_3$ is defined and belongs to U . In each neighborhood aV , $a \in G$, we introduce a coordinate system aD by taking as the coordinates of the point $ax \in aV$ the coordinates of the point x in V . We shall show that with this choice of coordinate systems the covering Σ consisting of the open sets aV , $a \in G$, becomes an analytic covering of G . Indeed, suppose aV and bV intersect. Because of the symmetry of the situation it suffices to show that the coordinates, in the system D , of an element $y \in V$ defined by the equation $ax = by$, $x \in V$, are given by analytic functions of the coordinates of x in the system D . But now $b^{-1}a = yx^{-1} \in VV^{-1}$ and it follows that the element $b^{-1}a$ has coordinates in the system D , and since $y = b^{-1}ax$ the coordinates of y are expressible as analytic functions in the coordinates of $b^{-1}a$ and x . Thus the coordinate systems here introduced define an analytic structure on G .

We must also show that the function φ is analytic with respect to this analytic structure. Let $x_0 \in G$, $y_0 \in G$, $z_0 = x_0 y_0^{-1}$, and let x, y be two elements close to e . Our task comes down to showing that the coordinates in the system D of the point z defined by the equation $z_0 z = x_0 x (y_0 y)^{-1}$ are expressible as analytic functions in the coordinates of the points x and y in the same system. But $z = y_0 (xy^{-1}) y_0^{-1}$ and the coordinates of $y_0 (xy^{-1}) y_0^{-1}$ are analytic functions in the coordinates of xy^{-1} (see Section 43, D)), while the coordinates of xy^{-1} are analytic functions in the coordinates of x and y (see Section 41, A)). Thus the desired analyticity of φ is proved.

For the sake of brevity let us refer to the analytic structure defined by the covering Σ as the first and suppose there exists a second analytic structure with respect to which φ is analytic. From the analyticity of φ it follows that the mapping $x \rightarrow x^{-1}$ is an analytic homeomorphism, and from this and the properties of φ it follows, in turn, that the function $f(x, y) = xy$ is also analytic. Finally, it

follows from this that the mapping $x \rightarrow ax$ is an analytic homeomorphism. Now let D' be any local coordinate system belonging to the second analytic structure and having its origin at e . Since f is analytic, it follows from Theorem 61 that the coordinate systems D and D' are connected by an analytic transformation in the vicinity of e . Let $a \in G$ and let A be a local coordinate system belonging to the second analytic structure and defined in some neighborhood of a . Starting from the system D' we construct a system aD' (in a neighborhood of a) exactly as aD was constructed from D . Since the mapping $x \rightarrow ax$ is an analytic homeomorphism it follows that A and aD' are connected in a neighborhood of a by an analytic transformation. Moreover, since D and D' are already known to be so connected, it follows that the coordinate systems aD and aD' are also connected in a neighborhood of a by an analytic transformation. But then aD and A are connected by an analytic transformation in a neighborhood of a , and since the point a is arbitrary it follows that the first and second analytic structures coincide. Thus Theorem 64 is proved.

The following result does not bear directly upon the theory of analytic manifolds and could equally well have been proved in Section 44, as a companion to Theorem 63. Its appearance at this point in the discussion is owing to the fact that the sole use to be made of it is in the proof of Theorem 66.

Theorem 65: Let G be an analytic local Lie group, let H be a subgroup, and let G/H be the space of left cosets (see Section 23, J)). Let also D be an analytic coordinate system in G and let C be a coordinate system defined in G/H and having its origin at the point H . If $x \in G$ and $\Xi \in G/H$ are sufficiently close to e and H , respectively, so that the coordinates x^1, \dots, x^r of x in the system D and the coordinates ξ^1, \dots, ξ^n and η^1, \dots, η^n of the elements Ξ and $H = x\Xi$ are defined in the system C , let

$$\begin{aligned} \eta^i &= \varphi^i(\Xi; x) = \varphi^i(\xi^1, \dots, \xi^n; x) = \varphi^i(\xi^1, \dots, \xi^n; x^1, \dots, x^r), \\ i &= 1, \dots, n. \end{aligned} \quad (6)$$

Then there exist in G/H coordinate systems C with respect to which the functions φ^i are analytic; for example, the system C^* constructed in proposition A) Section 44 had this property. Moreover, any two coordinate systems C having this property are connected by an analytic coordinate transformation.

Note that analyticity of the functions φ^i is not affected by changing from one analytic coordinate system D in G to another (see Theorem 61).

Proof: The first part of the proof is a simple matter of verification. Let D^* and C^* be the coordinate systems in G and G/H , respectively, that were constructed in A) Section 44. Group multiplication is expressed in coordinate form in the system D^* by analytic functions f^1, \dots, f^r (see Section 41, (3) and Section 43, A)). Let x^1, \dots, x^r be the coordinates of an element x in the system D^* , let $\Xi = xH$, $\xi \in L_\epsilon$, and let $\xi^1, \dots, \xi^n, 0, \dots, 0$ be the coordinates of ξ in D^* . Then ξ^1, \dots, ξ^n are the coordinates of Ξ in C^* . Let $\eta = x\xi$ and let η^1, \dots, η^r be the coordinates of η in D^* ; then η^1, \dots, η^n are the coordinates of $H = x\Xi = x\xi H$ in C^* . Thus

$$\begin{aligned} \eta^i &= f^i(x^1, \dots, x^r; \xi^1, \dots, \xi^n, 0, \dots, 0), \\ i &= 1, \dots, r. \end{aligned} \quad (7)$$

But then, in our special choice of coordinate systems D and C ($D = D^*$, $C = C^*$), we have

$$\begin{aligned} \varphi^i(\xi^1, \dots, \xi^n; x^1, \dots, x^r) \\ = f^i(x^1, \dots, x^r; \xi^1, \dots, \xi^n, 0, \dots, 0), \quad i = 1, \dots, n, \end{aligned}$$

which shows that the functions φ^i are analytic.

We turn now to the proof of the second part of the theorem. In order to simplify things as much as possible we retain the notation already established: the coordinate systems D^* and C^* introduced above will be fixed throughout the balance of the proof; the coordinates of a point $x \in G$ in D^* will be denoted by x^1, \dots, x^r ; the coordinates of a point $\Xi \in G/H$ in C^* will be denoted by ξ^1, \dots, ξ^n ; and the functions $\varphi^1, \dots, \varphi^n$ will define the coordinate expressions (6) of the mapping $(\Xi; x) \rightarrow x\Xi$ in the vicinity of the point $(H; e)$. Now, let C' be an arbitrary coordinate system in G/H defined in a neighborhood of H and having its origin at H . By reducing ϵ if necessary we may, and do, arrange things so that C^* and C' are defined in the same open subset U of G/H . Let ξ'^1, \dots, ξ'^n be the coordinates in C' of the point Ξ whose coordinates in C^* are ξ^1, \dots, ξ^n , and let the coordinate expressions of the mapping $(\Xi; x) \rightarrow x\Xi$ be given by the functions $\varphi'^1, \dots, \varphi'^n$ in the coordinate systems D^* , C' so that relations (6) assume the form

$$\begin{aligned} \eta'^i &= \varphi'^i(\Xi; x) = \varphi'^i(\xi'^1, \dots, \xi'^n; x) \\ &= \varphi'^i(\xi'^1, \dots, \xi'^n; x^1, \dots, x^r), \quad i = 1, \dots, n, \end{aligned} \quad (8)$$

in terms of the new coordinates. Finally, let

$$\xi'^i = \psi^i(\Xi) = \psi^i(\xi^1, \dots, \xi^n), \quad i = 1, \dots, n, \quad (9)$$

be the coordinate expressions of the change of coordinates from C^* to C' . In accordance with the hypotheses of the theorem, we assume the functions $\varphi^{*1}, \dots, \varphi^{*n}$ to be analytic; our task is to prove that the coordinate transformation defined by ψ^1, \dots, ψ^n is analytic also. To this end it suffices to show that the functions ψ^i are analytic and that the functional determinant $\left| \frac{\partial \psi^i}{\partial \xi^j} \right|$ does not vanish at the origin (see B)).

The first part of the proof is, once more, simple enough. Indeed, for each $\Xi \in U$ let ξ be the element of G whose coordinates in D^* are $\xi^1, \dots, \xi^n, 0, \dots, 0$, so that $\Xi = \xi H$. Then, since the origin of C' is the point $H \in G/H$, we obtain from (8):

$$\xi^{*i} = \varphi^{*i}(0, \dots, 0; \xi^1, \dots, \xi^n, 0, \dots, 0)$$

and consequently

$$\begin{aligned} \psi^i(\xi^1, \dots, \xi^n) &= \varphi^{*i}(0, \dots, 0; \xi^1, \dots, \xi^n, 0, \dots, 0), \\ i &= 1, \dots, n. \end{aligned} \quad (10)$$

Thus the functions ψ^1, \dots, ψ^n are analytic.

It remains to verify that the functional determinant $\left| \frac{\partial \psi^i}{\partial \xi^j} \right|$ does not vanish at $\xi^1 = \dots = \xi^n = 0$. Let H_0 denote a fixed but arbitrary point of U and choose $x_0 \in L_\epsilon$ such that $H_0 = x_0 H$. Since the coordinate expressions (in either C' or C^*) for the mapping $\Xi \rightarrow H = x_0 \Xi$ are given by functions that are, by hypothesis, defined and analytic in some neighborhood of the origin H , it follows, in particular, that the mapping is continuous in a neighborhood of H . Similarly, the mapping $H \rightarrow \Xi = x_0^{-1} H$ is defined and continuous in some neighborhood of H_0 . But the composition of these two mappings is the identity mapping, and it follows that the functional determinant of the mapping $\Xi \rightarrow x_0 \Xi$ (computed either in C' or C^*) is different from zero at $\Xi = H$. In other words

$$\left| \frac{\partial \varphi^{*i}(\xi^1, \dots, \xi^n; x_0)}{\partial \xi^j} \neq 0 \right| \quad (11)$$

and

$$\left| \frac{\partial \varphi^i(\xi^1, \dots, \xi^n; x_0)}{\partial \xi^j} \neq 0 \right| \quad (12)$$

at the origin H . But then by the implicit function theorem there exist neighborhoods V and V' of H and H_0 in G/H such that V and V' are both contained in U and such that V is mapped homeomorphically

onto V' by the mapping $\Xi \rightarrow H = x_0 \cdot \Xi$. (The inverse homeomorphism is, of course, the mapping $H \rightarrow \Xi = x_0^{-1} \cdot H$.)

Now from what has been shown it follows that the coordinate transformation

$$\eta^i = \psi^i(\eta^1, \dots, \eta^n)$$

defined by the functions ψ^i in the neighborhood V' can be factored. Indeed, we have

$$\begin{aligned}\eta^i &= \varphi^{i1}(\xi^1, \dots, \xi^n; x_0) \\ \xi^i &= \psi^i(\xi^1, \dots, \xi^n) \\ \xi^i &= \varphi^i(\eta^1, \dots, \eta^n; x_0^{-1})\end{aligned}\tag{13}$$

where all functions are analytic. But then the functional determinant

$$\left| \frac{\partial \psi^i(H_0)}{\partial \xi^j} \right|$$

of the functions ψ^i computed at the point H_0 can also be factored:

$$\left| \frac{\partial \psi^i(H_0)}{\partial \xi^j} \right| = \left| \frac{\partial \varphi^{i1}(H; x_0)}{\partial \xi^j} \right| \cdot \left| \frac{\partial \psi^i(H)}{\partial \xi^j} \right| \cdot \left| \frac{\partial \varphi^i(H_0; x_0^{-1})}{\partial \xi^j} \right|,$$

where $\left| \frac{\partial \psi^i(H)}{\partial \xi^j} \right|$ denotes the value of the functional determinant at the origin H . Since the point H_0 was arbitrary, we have shown

that if $\left| \frac{\partial \psi^i}{\partial \xi^j} \right|$ vanishes at H it must vanish identically on U . Thus there exists a number $\delta > 0$ such that

$$\left| \frac{\partial \psi^i(\xi^1, \dots, \xi^n)}{\partial \xi^j} \right| = 0 \text{ for all } |\xi^j| < \delta, \tag{14}$$

$i = 1, \dots, n.$

The proof will be completed by showing that this leads to a contradiction.

A classical theorem in analysis asserts that under condition (14) the functions ψ^1, \dots, ψ^n are dependent. More precisely; if (14) holds then in an arbitrary neighborhood of the origin of the coordinate system there exists a point $\Xi_0 = (\xi_0^1, \dots, \xi_0^n)$, in some neighborhood W of which one of the functions ψ^i , say ψ^1 , may be expressed in terms of the other functions. Thus we have in W

$$\psi^1 = \Psi(\psi^2, \dots, \psi^n) \tag{15}$$

where Ψ is a single valued continuous function of its arguments. But this is impossible as may be seen as follows. Let $\xi_0^{i^1}, \dots, \xi_0^{i^n}$ be the coordinates of Ξ_0 in the coordinate system C' and let Ξ_1 be a point belonging to W whose coordinates $\xi_1^{i^1}, \dots, \xi_1^{i^n}$ in the same coordinate system satisfy the conditions

$$\xi_1^{i^1} \neq \xi_0^{i^1}, \quad \xi_1^{i^2} = \xi_0^{i^2}, \dots, \quad \xi_1^{i^n} = \xi_0^{i^n}. \quad (16)$$

Finally let $\xi_1^{i^1}, \dots, \xi_1^{i^n}$ be the coordinates of the same point Ξ_1 in the coordinate system C^* so that

$$\xi_1^{i^i} = \psi^i(\xi_1^{i^1}, \dots, \xi_1^{i^n}), \quad i = 1, \dots, n. \quad (17)$$

Comparing now (15), (16) and (17) we see that $\xi_1^{i^1} = \xi_0^{i^1}$ which contradicts (16).

Theorem 66: Let G be a (global) analytic Lie group that acts as a continuous transitive transformation group on a locally compact separable Hausdorff space Γ (see Definition 31). Then Γ is a topological manifold and there exists a unique analytic structure on Γ with respect to which the function $\sigma(x, \xi) = x^*(\xi)$, $x \in G$, $\xi \in \Gamma$, is analytic.

Proof: According to Theorem 20 the pair G, Γ is similar to the pair $G, G/H$ where H denotes the stabilizer subgroup. Thus it suffices to prove the theorem for the latter pair. In neighborhoods W_ϵ and K_ϵ of the identity $e \in G$ and of the point $H \in G/H$ respectively, we introduce the coordinate systems D^* and C^* constructed in proposition A), Section 44. Let $\Xi_0 = aH$. In the neighborhood $a^*(K_\epsilon)$ of the point Ξ_0 we define a coordinate system aC^* by taking as the coordinates of the point $a\Xi$, $\Xi \in K_\epsilon$, the coordinates of Ξ in the system C^* . In other words, if the element $a \Xi$ is written in the form $a \xi H$ with $\xi \in L_\epsilon$, then the coordinates of $a\Xi$ in the system of aC^* are the first n coordinates of ξ in D^* . We shall show that, with this definition of coordinates, the covering Σ consisting of the coordinate neighborhoods $a^*(K_\epsilon)$, $a \in G$, is an analytic covering.

Suppose first that a and b are elements of G such that $aH = bH = \Xi_0$, so that in the vicinity of Ξ_0 we have the two coordinate systems aC^* , bC^* . We show that these coordinate systems are connected by an analytic coordinate transformation in some neighborhood of Ξ_0 . From the symmetry of the situation it is easily seen that it suffices to prove the following: if $\xi \in L_\epsilon$ is sufficiently close to e then the coordinates in the system B^* of the element $\eta \in L_\epsilon$ defined by the equation $b\eta H = a\xi H$ may be expressed in terms of the coordinates in B^* of the element ξ by means of analytic functions. Now if $a\xi H = b\eta H$ then $a\xi = b\eta h$, where $h \in H$, and for fixed a and b the elements η and h are both single valued

and continuous functions of ξ . Let $h = h_0$ for $\xi = e$; then for ξ close to e the element h has the form vh_0 where $v \in M_\xi$. Thus we have $\eta v = b^{-1} a \xi h_0^{-1}$, or, since $h_0 = b^{-1} a$, $\eta v = h_0 \xi h_0^{-1}$. But now by D) Section 43 the coordinates in D^* of $h_0 \xi h_0^{-1}$ are analytic functions of ξ while the coordinates of η in the system B^* are, by definition, just the first n coordinates of $\eta v = h_0 \xi h_0^{-1}$.

Let now c_1, c_2 be any two elements of G for which the neighborhoods $c_1^*(K_\xi)$ and $c_2^*(K_\xi)$ meet, and let aH be an element belonging to their intersection. We must show that in some neighborhood of aH the systems $c_1 C^*$, $c_2 C^*$ are connected by an analytic transformation. Let ξ_i be an element of L such that $c_i \xi_i H = aH$, $i = 1, 2$, and let $b_i = c_i \xi_i$. Then it follows from Theorem 65 that in some neighborhood of aH the coordinate systems $c_i C^*$ and $b_i C^*$ are connected by an analytic transformation. On the other hand, as was just shown above the coordinate systems $b_i C^*$ and $a C^*$ are also connected by an analytic transformation in the vicinity of aH . Thus Σ is an analytic covering of the manifold G/H .

We show next that with respect to the analytic structure thus defined on G/H the function σ is analytic. Let $x_0 \in G$, let $\Xi_0 = aH \in G/H$ and let $H_0 = x_0 \Xi_0$. Moreover let $x \in G$ and $\xi \in L_\xi$ be sufficiently close to the identity. The coordinates of $x_0 x$ in the system $x_0 D^*$ (see the proof of Theorem 64) are just the coordinates of x in D^* ; the coordinates of $a \xi H$ in a C^* are just the coordinates of ξ in the coordinate system B^* . We define an element $\eta \in L$ by means of the relation

$$x_0 a \eta H = x_0 x a \xi H. \quad (18)$$

Then the coordinates of η in B^* are also the coordinates of $x_0 a \eta H$ in the system $(x_0 a) C^*$. Thus the result will follow if we show that the coordinates of η in B^* are analytic functions in the coordinates of the elements x and ξ . But now from (18) we have

$$\eta H = a^{-1} x a \xi H, \quad (19)$$

and it follows from Theorem 65 that the coordinates of η are analytic functions in the coordinates of $a^{-1} x a$ and ξ . But by D) Section 43 the coordinates of $a^{-1} x a$ are analytic functions in those of x . Thus the analyticity of σ is proved.

Let us, once again, refer to the analytic structure defined on G/H by the covering Σ as the first and suppose that there is also defined on G/H a second analytic structure with respect to which σ is analytic. Let C' be a local coordinate system with origin H belonging to the second analytic structure. Then by Theorem 65 the systems C^* and C' are connected in the neighborhood of H by an analytic transformation. Note also that the analyticity of σ

implies that the mapping $\Xi \rightarrow a\Xi$ is an analytic homeomorphism of G/H onto itself. Let $\Xi_0 = aH$ be an arbitrary element of G/H and let A be a local coordinate system belonging to the second analytic structure and defined in some neighborhood of Ξ_0 . Starting from C' we define a coordinate system aC' in exactly the same way as the coordinates system aC^* was defined above in terms of C^* . Because of the relation between C^* and C' the coordinate systems aC^* and aC' are connected in a neighborhood of Ξ_0 by an analytic coordinate transformation. Moreover, from the fact that the mapping $\Xi \rightarrow a\Xi$ is an analytic homemorphism with respect to the second analytic structure it follows that aC' and A are also connected in a neighborhood of Ξ_0 by an analytic transformation. But then the same is true of the systems aC^* and A , and since Ξ_0 is an arbitrary point in G/H it follows that the second analytic structure coincides with the first.

Example 80: Let R^{n+1} denote Euclidean space of dimension $n + 1$ equipped with a fixed Cartesian coordinate system. The equation $(x^1)^2 + (x^2)^2 + \dots + (x^{n+1})^2 = 1$ defines in R^{n+1} a sphere S^n of dimension n . Denote by G the group of all orthogonal matrices of order $n + 1$ having determinant $+1$. Then each element $g \in G$ determines in the given coordinate system a rotation g^* of the space R^{n+1} about the origin of the coordinate system. By virtue of the correspondence $g \rightarrow g^*$ the group G becomes an effective continuous transformation group acting on R^{n+1} . The subset S^n is carried onto itself by the transformations of the group G and G is easily seen to be transitive on S^n .

We construct on S^n the analytic structure introduced in Theorem 66. Denote by U_i the open set in S^n consisting of all points (x^1, \dots, x^{n+1}) satisfying the condition $x_i > 0$ and by U_i' the open set of those points satisfying the condition $x_i < 0$. The collection Σ of open sets $U_1 U_1', \dots, U_{n+1} U_{n+1}'$ forms a covering of S^n . In each of these sets we define a coordinate system by projecting U_i and U_i' orthogonally onto the coordinate plane $x_i = 0$, i.e., by taking as the coordinates of a point (x^1, \dots, x^{n+1}) in U_i or U_i' the system of numbers $x^1, \dots, x^{i-1}, x^{i+1}, \dots, x^{n+1}$. It is seen at once that these projections map U_i and U_i' homeomorphically on the interior of the unit ball in the coordinate space $x_i = 0$. It is also readily verified that the covering Σ thus obtained is analytic and that the transformations of the group are analytic with respect to the analytic structure thus defined on S^n .

The covering Σ contains $2(n + 1)$ sets, and if even one of these sets is removed from Σ we no longer have a covering. It is possible, however, to construct an analytic covering Σ^* of the manifold

S^n defining upon S^n the same analytic structure as the covering Σ and consisting of two open sets. Let $p = (1, 0, \dots, 0)$ and $p' = (-1, 0, \dots, 0)$. Projecting the set $U = S^n \setminus p$ from the point p onto the coordinate plane $x_1 = 0$ we obtain a homeomorphism of U onto the entire plane $x_1 = 0$. In exactly the same fashion the open set $U' = S^n \setminus p'$ may be projected onto the plane $x_1 = 0$ from the point p' . The covering Σ^* consisting of the two sets U and U' with the prescribed coordinate systems is an analytic covering of the same type as the covering Σ .

8

THE STRUCTURE OF COMPACT GROUPS

In the present chapter we investigate the structure of finite dimensional compact groups and the structure of compact transformation groups acting on finite dimensional spaces. The root idea of the analysis is a fundamental connection between compact groups and Lie groups (Theorem 67): every neighborhood of the identity in a compact group contains a normal subgroup, the factor group modulo which is a Lie group. From this theorem, which is a direct consequence of the theory of linear representations (Chapter 5), it follows [43] that an arbitrary separable compact group can be represented as the limit, in a certain sense, of a sequence of Lie groups. In the case of compact groups that do not possess a countable topological base the analogous result cannot be obtained using ordinary infinite sequences and it becomes necessary to introduce either partially ordered systems of Lie groups, as is done by Weil [56], or transfinite sequences of compact groups, which is the course followed here.

The fundamental result of the chapter as far as compact groups are concerned is the theorem (due to me in the separable case) which asserts that a compact locally connected group of finite dimension is a Lie group (see Theorem 70). This theorem shows that among all compact groups the compact Lie groups are singled out by conditions of a general topological character. In particular, it contains von Neumann's positive solution [37] of Hilbert's fifth problem (see Section 41) in the compact case.

The fundamental result of the chapter as far as transformation groups are concerned is the theorem of Montgomery and Zippin [35] which asserts that an effective compact transformation group that acts transitively on a locally connected finite dimensional space is a Lie group (see Theorem 74). As an immediate consequence

of this we obtain the corollary that every effective compact transformation group that acts transitively on a topological manifold is a Lie group.

All the results of the chapter could be extended without difficulty to locally compact groups if there existed for the latter a theory of linear representations analogous with that developed in the fifth chapter for compact groups. The absence of such a theory renders locally compact groups inaccessible to the existing methods of analysis.

Throughout the chapter the term Lie group will be understood to mean analytic Lie group.

SECTION 46 CONVERGENT SERIES OF COMPACT GROUPS

The main business of the present section is the proof of Theorem 67, which shows that in a certain sense an arbitrary compact group can be approximated to any desired degree of accuracy by means of Lie groups. We also introduce the concept of a Lie series (see Definition 42) consisting of a transfinite sequence of compact groups. The groups of the series are not required to be Lie groups themselves, but it is asked that each group of the sequence should be the homomorphic image of the next under a homomorphism whose kernel is a Lie group. It turns out that this weaker requirement is adequate to permit the desired use of Lie groups in analyzing compact groups. Since a transfinite sequence of indices may always be extended to a longer sequence by adjoining one new term, there is no real need to introduce in our discussions the concept of the limit of a transfinite sequence of groups; instead of that we could always speak of the last term of a transfinite series, and it is in these terms that Theorem 68 is formulated. Nevertheless, the concept of the limit of a transfinite sequence is introduced for the sake of completeness, though it will be employed only in the construction of examples.

Remark: The proof of Theorem 67 rests essentially on a result borrowed from the theory of linear representations. However, this result, namely, that for every element a / e in a compact group G there exists a linear representation f_a of G such that $f_a(a)$ is not the identity matrix, involves only a relatively insignificant part of that theory. Accordingly, only a portion of Chapter 5 is essential as background for the present chapter. It suffices to be familiar with Sections 28, 29, 30, the definition of a linear representation, the concept of a uniformly complete system of

functions (see Section 33, A)), as well as with a part of the proof of Theorem 32 and a slight modification of the proof of Theorem 33. From the proof of Theorem 32 all that is needed is the completeness of the system Δ'' consisting of all functions appearing as matrix entries in all possible linear representations of G . The modification of the proof of Theorem 33 consists in replacing the system of irreducible representations by the system of all representations, and accordingly replacing Δ by Δ'' . Note, in particular, that in this curtailed program for a theory of linear representations there is no need even to introduce the concept of an irreducible representation.

A) Let G be a compact group, let N_1, \dots, N_k be normal subgroups of G and suppose that the factor groups G/N_i , $i = 1, \dots, k$ are all Lie groups. Let $N = N_1 \cap \dots \cap N_k$. Then G/N is also a Lie group.

It suffices to prove the proposition for $k = 2$. Denote by f_i the natural projection of G onto the Lie group $G/N_i = G_i$, $i = 1, 2$, and by G^* the direct product of G_1 and G_2 . With every element $x \in G$ we associate the element $f(x) \in G^*$ where $f(x) = (f_1(x), f_2(x))$. Clearly f is a homomorphism of G into G^* with kernel $N = N_1 \cap N_2$. Since G^* is a Lie group and G is compact it follows that f is an open homomorphism of G onto the Lie group $f(G) \subset G^*$ (see Theorem 62). Thus G/N is a Lie group.

Theorem 67: Let G be a compact group. Then every neighborhood of the identity in G contains a normal subgroup N such that the factor group G/N is an (analytic) Lie group.

Proof: By Theorem 33, if $a \in G$, $a \neq e$, then there exists a linear representation f_a of G such that $f_a(a)$ is not the identity matrix. The mapping f_a is a homomorphism of G onto a compact group of matrices and is, therefore, an open homomorphism of G onto an analytic Lie group (see Theorem 62 and Example 76). Let N_a denote the kernel of f_a . In this way, with every $a \in G$, $a \neq e$, we associate a normal subgroup N_a such that a / N_a and such that the factor group G/N_a is a Lie group.

Now let U be an arbitrary neighborhood of the identity element of G . Since N_a is closed and a / N_a there exists a neighborhood V_a of a which does not meet N_a , and the open sets V_a , $a \in G \setminus U$, form a covering of the compact set $G \setminus U$. Let V_{a_1}, \dots, V_{a_k} be a finite covering selected from this covering and let $N = N_{a_1} \cap \dots \cap N_{a_k}$. Clearly $N \subset U$, and by A) the factor group G/N is an analytic Lie group.

Definition 42: Suppose given a transfinite sequence G_1, G_2, \dots of compact groups, indexed by the transfinite numbers α , $1 \leq \alpha < \theta$, where θ denotes an arbitrary fixed transfinite number. Suppose also that with each pair of transfinite numbers $1 \leq \alpha < \beta < \theta$ there is associated a homomorphism φ_α^β of G_β onto G_α . Let K_α^β denote the kernel of φ_α^β . Then the sequence G_1, G_2, \dots with homomorphisms φ_α^β will be called a convergent series of length θ if the following conditions are satisfied:

- a) For $1 \leq \alpha < \beta < \gamma < \theta$ we have $\varphi_\alpha^\beta \circ \varphi_\beta^\gamma = \varphi_\alpha^\gamma$.
- b) If $\delta < \theta$ is a limit number then the intersection of the normal subgroups K_α^δ , $\alpha < \delta$, contains only the identity element of G_δ .
- c) A convergent series will be called a Lie series if the following condition is also satisfied:
c) The group G_1 and all of the subgroups $K_{\alpha+1}^\alpha$, $\alpha + 1 < \theta$ are Lie groups.

Theorem 68: Let G be a compact group and let φ be a homomorphism of G onto a Lie group G_1 . Then there exists a Lie series $G_1, G_2, \dots, G_\theta = G$, of length $\theta + 1$, beginning with G_1 and ending with the given group G , and satisfying the condition $\varphi = \varphi_1^\theta$. If the weight of G is t then θ may be taken to be the least transfinite number having cardinality t . In particular, if G is separable then θ may be taken to be ω (the first infinite transfinite number). In this event the sequence G_1, G_2, \dots of groups preceding G_ω is an ordinary infinite sequence and all the groups of the sequence are Lie groups.

Proof: Choose any complete system of neighborhoods of the identity in G and enumerate it in a transfinite sequence $\Gamma_0, \Gamma_1, \Gamma_2, \dots$ using the transfinite numbers less than some number θ . We suppose that $\Gamma_0 = G$. Clearly we may also suppose that θ is the least transfinite number having cardinality t . By Theorem 67 each neighborhood Γ_α contains a subgroup N_α such that the factor group G/N_α is a Lie group. For N_0 we may and do choose the kernel of the given homomorphism φ . For $1 \leq \beta < \theta$ we define K_β^θ to be the intersection of the normal subgroups N_α , $\alpha < \beta$. Let $G_\beta = G/K_\beta^\theta$; $G_\theta = G$. Observe that if $\theta = \omega$ the intersections formed in constructing the groups K_β^θ are finite so that the groups G_β , $\beta < \omega$, are Lie groups by proposition A). For φ_β^θ we take the natural projection of G_θ onto G_β . Finally if $1 \leq \beta < \gamma < \theta$ then $K_\beta^\gamma \subset K_\beta^\theta$, and there exists a unique homomorphism φ_β^γ of G_γ onto G_β satisfying the condition

$$\varphi_\beta^\gamma \circ \varphi_\gamma^\theta = \varphi_\beta^\theta. \quad (1)$$

The kernel $K_\theta^\beta / K_\theta^\gamma$ of φ_θ^γ we denote by K_γ^β . If $1 \leq \alpha < \beta < \gamma < \theta$ then, multiplying both sides of (1) by φ_α^β , we obtain $\varphi_\alpha^\beta \varphi_\beta^\gamma \varphi_\gamma^\theta = \varphi_\alpha^\beta \varphi_\theta^\theta = \varphi_\alpha^\theta = \varphi_\alpha^\gamma \varphi_\gamma^\theta$ and it follows that $\varphi_\alpha^\theta \varphi_\beta^\gamma = \varphi_\alpha^\gamma$. Thus for the system of homomorphisms φ_α^θ , $\alpha < \beta < \theta + 1$, condition a) of Definition 42 is satisfied.

We now show that condition b) is also satisfied. To this end suppose first that γ is a limit number such that $\gamma < \theta$. Then K_γ^β is the intersection of the normal subgroups K_θ^β , $\beta < \gamma$, and it follows that in G_γ the intersection of the subgroups $K_\theta^\beta = K_\theta^\beta / K_\theta^\gamma$, $\beta < \gamma$, contains only the identity, which is what we wish to show. On the other hand, for $\gamma = \theta$ the desired relation holds for a different reason; indeed the intersection of the normal subgroups K_θ^α , $\alpha < \theta$, is contained in the intersection of the neighborhoods $\Gamma_0, \Gamma_1, \Gamma_2, \dots$. Thus we have shown that the sequence $G_1, G_2, \dots, G_\theta$, with homomorphisms φ_α^θ , is a convergent series.

Since G_1 is a Lie group by hypothesis it remains only to show that each of the kernels $K_{\alpha+1}^\alpha$ is a Lie group. Since $K_\theta^{\alpha+1} = K_\theta^\alpha / N_\alpha$ it follows that under the natural projection of G_θ onto the Lie group G_θ / N_α the subgroup K_θ^α is carried onto a subgroup isomorphic with $K_\theta^{\alpha+1} / K_\theta^{\alpha+1}$. Thus $K_{\alpha+1}^\alpha$ is isomorphic with a subgroup of a Lie group and is therefore itself a Lie group.

The following definition will be employed in the sequel only in the construction of examples. Moreover, propositions B) and C) will find no application at all and are presented here only for the sake of completeness.

Definition 43: Let the sequence G_1, G_2, \dots , with homomorphisms φ_α^θ , be a convergent series of length θ . Then a similarly indexed transfinite sequence $x = (x_1, x_2, \dots)$ of elements will be called a fundamental sequence if for every $1 \leq \alpha < \theta$ we have $x_\alpha \in G_\alpha$ and $\varphi_\alpha^\theta x_\beta = x_\alpha$. Denote by G the collection of all fundamental sequences. The product $z = xy$ of two elements $x = (x_1, x_2, \dots)$ and $y = (y_1, y_2, \dots)$ of G is defined to be $z = (z_1, z_2, \dots)$ where $z_\alpha = x_\alpha y_\alpha$, $\alpha < \theta$. Clearly $z \in G$. Moreover, with this definition G becomes a group. We also define a topology in G . Let $\alpha < \theta$ and let U_α be a fixed neighborhood in G_α . We denote by $[U_\alpha]$ the set of all elements $x \in G$ satisfying the condition $x_\alpha \in U_\alpha$. The collection of all sets of the form $[U_\alpha]$, $\alpha < \theta$, forms a complete system of neighborhoods for a topology in G . With these definitions of multiplication and topology G becomes a compact topological group, called the limit of the convergent series G_1, G_2, \dots , with homomorphisms φ_α^θ .

That G is a group is easily seen. Indeed, it is a subgroup

of the full algebraic direct product of the groups G_α , $\alpha < \theta$ (see Definition 10). We must show that G is also a topological space. Note first of all that if U_α is any neighborhood in G_α and if U_β denotes its inverse image under φ_α^β then

$$[U_\alpha] = [U_\beta]. \quad (2)$$

Let $a = (a_1, a_2, \dots)$ and $b = (b_1, b_2, \dots)$ be any two distinct elements of G . Since $a \neq b$ there exists an index $\alpha < \theta$ such that $a_\alpha \neq b_\alpha$ and consequently in G_α there exists a neighborhood U_α of the element a_α that does not contain b_α . But then $[U_\alpha]$ is a neighborhood in G containing a and not containing b . Next, let $[U_\alpha]$ and $[V_\beta]$, $\alpha \leq \beta$, be any two neighborhoods of $a = (a_1, a_2, \dots)$. If $\alpha < \beta$ there exists a neighborhood U_β in G_β such that $[U_\alpha] = [U_\beta]$ (see (2)). But then U_β and V_β are neighborhoods of a_β in G_β and consequently there exists a neighborhood W_β of a_β such that $W_\beta \subset U_\beta \cap V_\beta$. Clearly $[W_\beta] \subset [U_\alpha] \cap [V_\beta]$. Thus the conditions of Theorem 3 are satisfied and the collection of sets $[U_\alpha]$ is a base for a unique topology turning G into a topological space.

We show next that G is a topological group. Let a and b be elements of G as above; then $ab^{-1} = c = (c_1, c_2, \dots)$ where $c_\alpha = a_\alpha b_\alpha^{-1}$. Let $[W_\gamma]$ be an arbitrary neighborhood of c . Since W_γ is a neighborhood of $c_\gamma = a_\gamma b_\gamma^{-1}$ in G_γ , it follows that there exist neighborhoods U_γ and V_γ of a_γ and b_γ such that $U_\gamma V_\gamma^{-1} \subset W_\gamma$. But then $[U_\gamma] [V_\gamma]^{-1} \subset [W_\gamma]$. Thus G is a topological group.

Finally we show that G is compact. Let G^* denote the direct product of the compact groups G_α , $\alpha < \theta$ (see Definition 29). The elements u^* of G^* are the transfinite sequences (u_1, u_2, \dots) that satisfy the condition $u_\alpha \in G_\alpha$, $\alpha < \theta$, so that G is just the subset of G^* defined by the conditions $\varphi_\alpha^\beta u_\beta = u_\alpha$, $\alpha < \beta < \theta$. The continuity of the homomorphisms φ_α^β implies that G is a closed set in the compact space G^* . The proof will be completed by showing that the topology on G , as defined above, coincides with the topology induced on it by G^* . Let U_{α_i} be a neighborhood in G_{α_i} , $i = 1, \dots, k$. Then a typical neighborhood U^* in G^* consists of all elements $u^* = (u_1, u_2, \dots)$ satisfying the conditions $u_{\alpha_i} \in U_{\alpha_i}$, $i = 1, \dots, k$. Let $a = (a_1, a_2, \dots) \in U^* \cap G$. We must show that there is a neighborhood $[V_\alpha]$ of a in G such that $[V_\alpha] \subset U^*$. The index α we take to be the largest of the numbers $\alpha_1, \dots, \alpha_k$ and for each i we choose a neighborhood U_{α^i} in G_α such that $[U_{\alpha_i}] = [U_{\alpha^i}]$ (see (2)). Since the neighborhoods U_{α^i} , $i = 1, \dots, k$, all contain a_α it follows that there is a neighborhood V_α of a_α contained in the intersection $U_{\alpha^1} \cap \dots \cap U_{\alpha^k}$. But then $a \in [V_\alpha] \subset U^*$. On the other hand, let $[W_\alpha]$ be an arbitrary neighborhood of a in the space

G. If W^* is defined to consist of the elements $u^* = (u_1, u_2, \dots)$ satisfying the condition $u_\alpha \in W_\alpha$ then clearly $[W_\alpha] = W^* \cap G$. Thus the two topologies on G coincide and the result is established.

B) Let the sequence G_1, G_2, \dots , with homomorphisms φ_α^β , constitute a convergent series of length θ , and let G be the limit of the series. Define $G_\theta = G$, and let φ_α^θ denote the mapping that associates with each element $x_\theta = (x_1, x_2, \dots, x_\alpha, \dots) \in G_\theta$ the element $x_\alpha \in G_\alpha$: $\varphi_\alpha^\theta(x_\theta) = x_\alpha$. Then φ_α^θ is a homomorphism of G_θ onto G_α and the extended sequence $G_1, G_2, \dots, G_\theta$ with homomorphisms φ_α^β , $1 \leq \alpha < \beta < \theta + 1$, is a convergent series of length $\theta + 1$.

That φ_α^θ is a homomorphism of the topological group G into the topological group G_α , and that the conditions $\varphi_\alpha^\beta \varphi_\beta^\gamma = \varphi_\alpha^\gamma$ are satisfied for $\alpha < \beta < \gamma < \theta + 1$ may readily be verified. Moreover, it is easily seen that the intersection of the subgroups K_θ^α , $\alpha < \theta$, contains only the identity e_θ of the group G_θ , for if $x_\theta \in K_\theta^\alpha$ for all $\alpha < \theta$, then $\varphi_\alpha^\theta(x_\theta) = e_\alpha$ so that $x_\theta = (e_1, e_2, \dots) = e_\theta$. Thus it remains only to verify that φ_α^θ is onto. Let x_α be any element of G_α . We must construct an element x_θ of G_θ of the form $x_\theta = (x_1, x_2, \dots, x_\alpha, \dots)$. For the lower order indices $\beta < \alpha$ it is clear we must have $x_\beta = \varphi_\beta^\alpha(x_\alpha)$. For higher indices we define x_β by transfinite induction. Let $\alpha < \beta < \theta$ and suppose elements $x_1, x_2, \dots, x_\alpha, \dots$, already defined in such a way that the conditions $x_\delta \in G_\delta$ and $\varphi_\gamma^\delta(x_\delta) = x_\gamma$ are satisfied for all $\gamma < \delta < \beta$. If β has an immediate predecessor $\beta - 1$, then for x_β we take any element of G_β satisfying the condition $\varphi_{\beta-1}^\beta(x_\beta) = x_{\beta-1}$; such an element exists since $\varphi_{\beta-1}^\beta(G_\beta) = G_{\beta-1}$. On the other hand, if β is a limit number, denote by X_β the inverse image of the element x_γ , $\gamma < \beta$, under the mapping φ_γ^β . The sets $X_\beta^1, X_\beta^2, \dots$ are compact and form a decreasing transfinite sequence; consequently their intersection is not empty and we may take any element belonging to the intersection for x_β . In this way we obtain an element x_θ of G_θ satisfying the condition $\varphi_\alpha^\theta(x_\theta) = x_\alpha$, and the proof is complete.

Taken together, the following proposition C) and Theorem 68 say that every compact group is the limit of a Lie series.

C) Let $G_1, G_2, \dots, G_\theta$ with homomorphisms φ_α^β , $1 \leq \alpha < \beta \leq \theta$, constitute a convergent series of length $\theta + 1$, where θ is a transfinite limit number, and denote by G the limit of the convergent series G_1, G_2, \dots with homomorphisms φ_α^β , $1 \leq \alpha < \beta < \theta$, obtained from the preceding series by discarding its last term. For fixed $x_\theta \in G_\theta$ and for each $\alpha < \theta$ let $x_\alpha = \varphi_\alpha^\theta(x_\theta)$. Then

$x = (x_1, \dots, x_\alpha, \dots) \in G$. Let φ^θ denote the mapping $x_\theta \rightarrow x$ of G_θ into G thus defined. Then φ^θ is an isomorphism between these two topological groups.

It is immediately apparent that φ^θ is a homomorphism of the topological group G_θ into the topological group G . Moreover, the kernel of φ^θ is trivial by condition b) of Definition 42. To see, finally, that φ^θ is onto, let $x = (x_1, x_2, \dots) \in G$ and, for each $\alpha < \theta$, let X_θ^α denote the inverse image of x_α under the mapping φ_α^θ . The sets $X_\theta^{-1}, X_\theta^{-2}, \dots$ form a decreasing transfinite sequence of compact sets and consequently contain a common element x_θ . For this element we clearly have $\varphi_\alpha^\theta(x_\theta) = x$.

Example 81: Let G_1, G_2, \dots be an ordinary infinite sequence of compact groups and for each i let φ_i be a homomorphism of G_{i+1} onto G_i . If i and j are positive integers, $i < j$, we define $\varphi_i^j = \varphi_i \varphi_{i+1} \dots \varphi_{j-1}$. Then the sequence G_1, G_2, \dots with homomorphisms φ_i^j , $1 \leq i < j \leq \omega$, clearly forms a convergent series of length ω , and consequently defines a limit group G . We shall say that the sequence G_1, G_2, \dots with homomorphisms $\varphi_1, \varphi_2, \dots$ converges to G . According to B) the group G may be adjoined to the sequence G_1, G_2, \dots so as to form a convergent series $G_1, G_2, \dots, G = G$ with homomorphisms φ_α^β , $1 \leq \alpha < \beta \leq \omega$, of length $\omega + 1$. From Definition 43 it follows that if all of the groups G_1, G_2, \dots are separable then the limit group G is also separable. Thus, by Theorem 68 and Proposition C), it follows that every separable compact group G is, in this sense, the limit of a sequence G_1, G_2, \dots of Lie groups.

Now if all of the groups G_1, G_2, \dots are finite the limit group $G = G_\omega$ is 0-dimensional. Indeed, since each φ_α^ω is a homomorphism of G_ω onto a finite group the kernels K_ω^α are open, and since the intersection of all the kernels K_ω^α , $\alpha < \omega$, contains only the identity of G_ω , it follows that for an arbitrary neighborhood U of the identity in G_ω there exists an index α such that $K_\omega^\alpha \subset U$. But this shows that G is 0-dimensional (see Section 23, E) and Section 16, F)). It may easily be shown that the topological space G is either finite or homeomorphic with the Cantor set. Conversely, it follows at once from the proof of Theorem 68 that every separable 0-dimensional compact group is the limit of a sequence of finite groups.

Suppose next that $G_i = K$, $i = 1, 2, \dots$, where $K = D/N$ denotes, as usual, the factor group of the real numbers modulo the integers. We define a homomorphism φ_i of G_{i+1} onto G_i by writing $\varphi_i(x) = s_i x$, where s_i denotes any fixed positive integer. It is easily seen that the kernel K_ω^{-1} of the homomorphism φ_i^ω of the limit group G_ω onto G_1 is itself the limit of the sequence $K_2^{-1}, K_3^{-1}, \dots$

with homomorphisms $\varphi_2, \varphi_3, \dots$. Since each K_i^{-1} is finite (its order is $s_1 s_2 \dots s_{i-1}$) it follows that K_ω^{-1} is 0-dimensional. Let L be a connected neighborhood of 0 in G_1 that does not coincide with the whole group. Clearly L is an interval. The inverse image V of L under the homomorphism φ_1^{-1} is then homeomorphic with the product of the interval L and the 0-dimensional space K_ω^{-1} . As will be shown in Theorem 69, this structural feature is shared by all finite dimensional compact groups.

SECTION 47

FINITE DIMENSIONAL COMPACT GROUPS

In this Section it will be proved that a finite dimensional compact group resolves, locally, into the direct product of a local Lie group and a (global) 0-dimensional subgroup (see Theorem 69). From this it follows that, in the presence of local connectedness, a finite dimensional compact group must actually be a Lie group. The most important tool in the investigation is Lemma 2, which asserts that if φ is a homomorphism of a compact group G onto a Lie group G^* and if g^* is any one-parameter subgroup of G^* then G possesses a one-parameter subgroup g satisfying the condition $\varphi(g(t)) = g^*(t)$. Theorem 68 and the concept of a Lie series are used only in the proof of this lemma and do not appear elsewhere in the section.

In this and the following section the dimension of a compact space R will be denoted by $\dim R$.

A) Let L and M be local Lie groups, let χ be a local homomorphism of M onto L , and let g be a one-parameter subgroup of L . Then there exists a one-parameter subgroup h of M and a positive number ϵ such that for $|t| < \epsilon$ we have $g(t) = \chi(h(t))$.

In order to prove the assertion we introduce canonical coordinate systems of the first kind in both L and M . It follows from Theorem 63 that the mapping χ is expressed in these coordinates in the form

$$x^i = \sum_{j=1}^r q_j^i y^j, \quad i = 1, \dots, n, \quad (1)$$

where the rank of the matrix $\|q_j^i\|$ is n . Let a^1, \dots, a^n be the components of the direction vector of g in the chosen coordinate

system. The system of equations $a^i = \sum_{j=1}^r q_j^i b^j$, $i = 1, \dots, n$,

may be solved with respect to the unknowns b^1, \dots, b^r , and it follows from (1) that the one-parameter subgroup h with direction vector $b = (b^1, \dots, b^r)$ satisfies the condition $g(t) = \chi(h(t))$.

Lemma 1: Let G and H be compact groups, let φ be a homomorphism of H onto G with kernel K , where K is a Lie group, and let g be a one-parameter subgroup of G with domain of definition $|t| < \delta$. Then there exists in H a one-parameter subgroup h satisfying the condition $g(t) = \varphi(h(t))$ for all $|t| < \delta$.

Proof: Denote by L the set of all elements $g(t)$, $|t| < \delta$. We may suppose that g is not constantly equal to the identity. It follows that g induces an isomorphism of a part of the local group $|t| < \delta$ onto a part of L and hence that L is a local Lie group with respect to the group operation in G . Clearly the set $M = \varphi^{-1}(L)$ is also a local group with respect to the group operation in H . We shall show that M is a local Lie group, but first let us see that this fact will, when established, suffice to prove the lemma. By A) there exists a positive number ε and a one-parameter subgroup h in M such that $g(t) = \varphi(h(t))$ for $|t| < \varepsilon$. Since h is also a one-parameter subgroup in H its domain of definition can be extended in one and only one way so as to include all values of the parameter t . But, then, we must have $g(t) = \varphi(h(t))$ for all $|t| < \delta$.

It remains to show that M is a local Lie group. To this end we introduce the concept of a sufficiently small neighborhood. Let P be a local group and let W be a neighborhood of the identity $e \in P$. Then W will be said to be sufficiently small if for every $x \in W$, $x \neq e$, there exists a power x^r of x which is defined in P but does not belong to W . Not all groups possess sufficiently small neighborhoods; the important thing for present purposes is that local Lie groups do. Indeed, if P is a local Lie group we may introduce a canonical coordinate system of the first kind, defined on a star-shaped domain W' . Let W be a neighborhood of e such that \bar{W} is compact and small enough so that the product of any two elements of W is defined and belongs to W' . It is easy to verify that any such neighborhood W satisfies the above criterion and is therefore sufficiently small. Observe that this implies that in a local Lie group there is a base at e consisting of sufficiently small neighborhoods.

Now let U be a neighborhood of the identity in G such that $U \cap L$ is a sufficiently small neighborhood in the local Lie group L , and let V be a neighborhood of the identity in H such that $\varphi(V) \subset U$ and such that $K \cap V$ is a sufficiently small neighborhood of the identity in the Lie group K . By Theorem 67 there exists a normal subgroup N of H contained in V such that H/N is a Lie group. We

shall show that $N \cap M$ contains only the identity of H . Indeed $\varphi(N \cap M) \subset U \subset L$, and since $U \cap L$ is a sufficiently small neighborhood it follows that the set $\varphi(N \cap M)$ contains only the identity. Thus $N \cap M \subset K$ and consequently $N \cap M \subset V \cap K$. Since $K \subset M$ and $V \cap K$ is a sufficiently small neighborhood, it follows that $N \cap M$ contains only the identity. But then the natural projection of H onto the Lie group H/N maps a part of the local group M isomorphically onto a local subgroup of H/N whence it follows that M itself is a local Lie group (see Theorem 62). †

Lemma 2: Let G be a compact group, let φ be a homomorphism of G onto a Lie group G^* , and let g^* be a one-parameter subgroup of G^* with domain of definition $|t| < \delta$. Then there exists a one-parameter subgroup g of G satisfying the condition $\varphi(g(t)) = g^*(t)$ for all $|t| < \delta$.

Proof: According to Theorem 68 there exists a Lie series $G_1 = G^*$, $G_2, \dots, G_\theta = G$ with homomorphisms φ_α^β such that $\varphi_1^\theta = \varphi$. We define $g_1 = g^*$ and suppose that for all transfinite numbers α , $\alpha < \gamma \leq \theta$, one-parameter subgroups g_α of G , each having domain of definition $|t| < \delta$, have already been constructed such that $\varphi_\alpha^\beta(g_\beta(t)) = g_\alpha(t)$, for all $|t| < \delta$ and all $1 \leq \alpha < \beta < \gamma$. If γ possesses a predecessor $\gamma - 1$ then by Lemma 1 there exists in G_γ a one-parameter subgroup g_γ such that $\varphi_{\gamma-1}^\gamma(g_\gamma(t)) = g_{\gamma-1}(t)$, $|t| < \delta$. But then for arbitrary $\alpha < \beta \leq \gamma$ we have $\varphi_\alpha^\beta(g_\beta(t)) = g_\alpha(t)$, $|t| < \delta$. On the other hand, if γ is a limit number let $X_\gamma^\alpha(t)$ denote the inverse image of $g_\alpha(t) \in G_\alpha$ under the homomorphism φ_α^γ . The sets $X_\gamma^{-1}(t)$, $X_\gamma^2(t), \dots$ form a decreasing transfinite sequence of compact sets and consequently have non-empty intersection. Moreover, the intersection can contain only one element since the intersection of the subgroups K_γ^α contains only the identity. Denote this element by $g_\gamma(t)$. It is clear that for $\alpha < \beta \leq \gamma$ we have $\varphi_\alpha^\beta(g_\beta(t)) = g_\alpha(t)$, $|t| < \delta$. We shall complete the transfinite induction by showing that g_γ is a one-parameter subgroup of G_γ with domain of definition $|t| < \delta$. Let t_1 and t_2 be real numbers such that $|t_1| < \delta$, $|t_2| < \delta$, $|t_1 + t_2| < \delta$. Then $\varphi_\alpha^\gamma(g_\gamma(t_1)g_\gamma(t_2)) = g_\alpha(t_1)g_\alpha(t_2) = g_\alpha(t_1 + t_2)$. Thus $g_\gamma(t_1)g_\gamma(t_2) \in X_\gamma(t_1 + t_2)$ for arbitrary $\alpha < \gamma$, and consequently $g_\gamma(t_1)g_\gamma(t_2) = g_\gamma(t_1 + t_2)$. Next let U_γ denote an arbitrary neighborhood of

† That the natural projection is locally homeomorphic on M follows from the fact that M is locally compact, which, in turn, follows from the local compactness of L . See footnote, p. 139. Trans.

the identity in G_γ , let V_γ be a neighborhood of the identity such that $V_\gamma^{-2} \subset U_\gamma$, and finally let $V_\alpha = \varphi_\alpha^\gamma(V_\gamma)$. Since the intersection of the subgroups $K_\gamma^{-\alpha}$, $\alpha < \gamma$, contains only the identity, it follows that for some $\beta < \gamma$ we have $K_\gamma^{-\beta} \subset V_\gamma$. From this and from $\varphi_\beta^\gamma(V_\gamma) = V_\beta$ it follows that the inverse image W_γ of the open set V_β under φ_β^γ is contained in U_γ . If now $\epsilon > 0$ is sufficiently small so that for $|t| < \epsilon$ we have $g_\beta(t) \in V_\beta$ then for the same values of t we have likewise $g_\gamma(t) \in W_\gamma \subset U_\gamma$. This shows that g_γ is a continuous local homomorphism and consequently a one-parameter subgroup of G_γ .

As the last step in this transfinite construction we obtain a one-parameter subgroup $g = g_\theta$ of $G = G_\theta$ satisfying the condition $\varphi_1^\theta(g^\theta(t)) = g_1(t)$, $|t| < \delta$. Thus Lemma 2 is proved.

In the present paragraph proposition B) will be employed only in the special case $H = \{e\}$; however, the general case will be needed in the following paragraph in the study of transformation groups.

B) Let G be a compact group, let H be a subgroup and let $\Gamma = G/H$ denote the space of left cosets. Let $r = \dim \Gamma$ be the dimension of this space (the case $r = \infty$ is not excluded), and finally let s be a non-negative integer such that $s \leq r$. Then there exists a neighborhood U of the identity in G such that if N is any normal subgroup of G contained in U then the left coset space $\Gamma^* = G/NH$ has dimension greater than or equal to s . In particular, if r is finite we may take $s = r$ in which case $\dim \Gamma^* \geq \dim \Gamma$.

Proof: Let N be an arbitrary normal subgroup of G and let Γ^* denote the left coset space $\Gamma^* = G/NH$. With each $X \in \Gamma$ we associate the element $X^* = N X \in \Gamma^*$ and we denote the continuous mapping of Γ onto Γ^* thus defined by f ; $X^* = f(X)$. According to E) Section 16 there exists a finite open covering $\Omega' = \{W_1', \dots, W_k'\}$ of Γ such that, if f is subordinate to that covering, then the dimension of Γ^* is at least s . The proof will be completed by constructing a neighborhood U such that f is subordinate to Ω' whenever $N \subset U$.

Let G denote the natural projection of G onto G/H and let $W_j = g^{-1}(W_j')$. The open sets W_1, \dots, W_k cover G . For each $x \in G$ select j such that $x \in W_j$ and then a neighborhood V_x of the identity in G such that $xV_x^{-2} \subset W_j$. The open sets xV_x , $x \in G$, also cover G . Select from this a finite covering $x_1V_{x_1}, \dots, x_hV_{x_h}$ and denote by U the intersection $V_{x_1} \cap \dots \cap V_{x_h}$. Suppose now that $N \subset U$ and let $A^* = aNH$, $a \in G$, be any element of Γ^* . The set $f^{-1}(A^*)$ is the union of all left cosets of the form a_nH , $n \in N$. There exist i such that $a \in x_iV_{x_i}$ and j such that $x_iV_{x_i}^{-2} \subset W_j$, and with this choice of i and j we have

$$a \cdot H \subset x_i V_{x_i} \cdot NH \subset x_i V_{x_i}^{-2} H \subset W_j H \subset W_j ;$$

i.e., $a \cdot H \in W_j'$. Thus $f^{-1}(A^*) \subset W_j'$ so that f is subordinate to Ω' and the proposition is proved.

Theorem 69: A compact group G of finite dimension r resolves locally into the direct product of an r -dimensional local Lie group L and a (global) 0-dimensional normal subgroup N . More precisely: there exists a subset L , homeomorphic with an open r -dimensional cube, and a 0-dimensional normal subgroup N , such that the following conditions are satisfied: a) every element $l \in L$ commutes with every element $n \in N$; b) the set $V = LN$ is a neighborhood of the identity in G ; c) every element $v \in V$ possesses a unique expression of the form $v = ln$, $l \in L$, $n \in N$, the elements l and n thus defined being continuous functions of v ; d) if l_1 and l_2 are two elements of L such that $l_1 l_2 \in V$ then $l_1 l_2 \in L$ so that L is a local group with respect to the product defined in G ; e) the local group L is a local Lie group. From this it follows immediately that G/N is a Lie group. It turns out that N may be taken to be any 0-dimensional normal subgroup of G with the property that G/N is a Lie group.

Proof: Let φ be a homomorphism of G onto an arbitrary Lie group G^* and let δ be the dimension of G^* . Select in G^* a maximal linearly independent system g_1^*, \dots, g_s^* of one-parameter subgroups and let ∞ be a positive number sufficiently small so that for $|t^i| < \delta$, $i = 1, \dots, s$, the numbers t^1, t^2, \dots, t^s may serve as coordinates of the point $g_1^*(t^1)g_2^*(t^2) \dots g_s^*(t^s)$ (see Section 43, A)). Denote by L_δ^* the set of all such points, $|t^i| < \delta$, $i = 1, \dots, s$. Then L_δ^* is homeomorphic with an open s -dimensional cube. By Lemma 2 there exist in G one-parameter subgroups g_i with domain of definition $|t| < \delta$ satisfying the condition $\varphi(g_i(t)) = g_i^*(t)$, $|t| < \delta$, $i = 1, \dots, s$. Denote by L_δ the set of points of the form $g_1(t^1)g_2(t^2) \dots g_s(t^s)$, $|t^i| < \delta$, $i = 1, \dots, s$. Associating with each point $x^* = g_1^*(t^1) \dots g_s^*(t^s) \in L_\delta^*$ the point $f(x^*) = x = g_1(t^1) \dots g_s(t^s) \in L_\delta$, we obtain a mapping f of L_δ^* onto L_δ which is clearly continuous; but then since $\varphi(f(x^*)) = x^*$ and φ is also continuous, the two mappings f and φ are mutually inverse homomorphisms between L_δ^* and L_δ . Thus G contains a set L_δ homeomorphic with an s -dimensional cube. It follows, in particular, that $r \geq s$ and we have shown that if φ is any homomorphism of G onto a Lie group then

$$\dim(\varphi(G)) \leq \dim(G) . \quad (2)$$

Now denote by N the kernel of φ and let U be a neighborhood of the identity in G such that for any normal subgroup K contained in U we have

$$\dim(G/K) \geq \dim(G), \quad (3)$$

and also such that for any normal subgroup N_1 of N contained in $N \cap U$ we have

$$\dim(N/N_1) \geq \dim(N). \quad (4)$$

(The existence of such a neighborhood U is assured by B)). Next select a normal subgroup K of G such that $K \subset U$ and such that G/K is a Lie group (see Theorem 67). Let $N_1 = N \cap K$. Then G/N_1 and N/N_1 are both Lie groups (see Section 46, A)). Let φ_1 denote the natural projection of G onto G/N_1 . According to (3) and (4) we have

$$\dim(\varphi_1(G)) \geq \dim(G), \quad (5)$$

$$\dim(\varphi_1(N)) \geq \dim(N). \quad (6)$$

Since $\varphi_1(G)$ and $\varphi_1(N)$ are both Lie groups it follows from (2), (5), (6) that

$$\dim(\varphi_1(G)) = \dim(G), \quad (7)$$

$$\dim(\varphi_1(N)) = \dim(N). \quad (8)$$

Moreover, since $\varphi_1(G)$ is a Lie group and $\varphi(G) = \varphi_1(G)/\varphi_1(N)$ it follows from Theorem 63 that

$$\dim(\varphi_1(G)) = \dim(\varphi(G)) + \dim(\varphi_1(N)). \quad (9)$$

Finally, from (7), (8), (9) we obtain

$$\dim(G) = \dim(\varphi(G)) + \dim(N). \quad (10)$$

Here N denotes the kernel of φ , and (10) holds for any homomorphism of a finite dimensional compact group G onto a Lie group. In particular, applying (10) to φ_1 we obtain

$$\dim(G) = \dim(\varphi_1(G)) + \dim(N_1), \quad (11)$$

which, together with (7), implies $\dim(N_1) = 0$. Thus G possesses

a 0-dimensional normal subgroup yielding a factor group that is a Lie group.

We now define $V_\delta = \varphi^{-1}(L^*)$. Let $v \in V_\delta$ and let $l = f(\varphi(v))$; then $l \in L_\delta$. Since $\varphi(l) = \varphi(v)$ the elements l and v belong to the same coset of N and consequently $v = ln$ where $n \in N$. This resolution of v is unique since if $v = ln$, $l \in L_\delta$, $n \in N$ then $l = f(\varphi(v))$. Denote by L_γ^* , $0 < \gamma < \delta$, the collection of elements $x^* \in L_\delta^*$ for which $|t^i| < \gamma$, $i = 1, \dots, s$ and let $L_\gamma = f(L_\gamma^*)$ and $V_\gamma = \varphi^{-1}(L_\gamma^*)$. Then $\bar{V}_\gamma = \varphi^{-1}(L_\gamma^*)$. To each point (l, n) of the product $L_\gamma \times N$ we associate the point $ln \in L_\gamma N$. Since this mapping is continuous and one-to-one and the space $\bar{L}_\gamma \times N$ is compact, it follows that the mapping $(l, n) \rightarrow ln$ is a homeomorphism for arbitrary $\gamma < \delta$. From this it follows in particular that the relation $v = ln$ defines $l \in L_\delta$, $n \in N$, as continuous functions of the element v , $v \in V_\delta$.

Suppose now that $\dim(N) = 0$. (That there exist 0-dimensional normal subgroups of G yielding Lie factor groups has already been shown.) In this case we have $s = r$ by (10) so that L_γ is homeomorphic with an open r -dimensional cube. We shall show that if $\dim(N) = 0$ then the elements $l \in L_\delta$ and $n \in N$ commute with one another. Let n be a fixed element of N . With each $l \in L_\delta$ we associate the element $\psi(l) = l^{-1}nl$. Since the mapping ψ of L_δ into N is continuous it follows that $\psi(L_\delta)$ is connected while N , being 0-dimensional, is totally disconnected. Thus $\psi(L_\delta) = n$. In other words $ln = nl$ for each $l \in L_\delta$. Next choose γ such that $L_\gamma^{*2} \subset L_\delta^*$ and let l_1 and l_2 be two elements of L_γ . Then, as has already been shown, $l_1 l_2 = ln$ where l and n are single valued continuous functions of l_1 and l_2 and the function $n = n(l_1, l_2)$ yields a continuous mapping of $L_\gamma \times L_\gamma$ into N . Since $L_\gamma \times L_\gamma$ is connected the function $n(l_1, l_2)$ must be constant. Since $n(e, e) = e$ we have $n(l_1, l_2) = e$ for arbitrary $l_1, l_2 \in L_\gamma$ and it follows that $l_1 l_2 \in L_\delta$. In particular, if $l_1 l_2 \in V_\gamma$ then $l_1 l_2 \in V_\gamma \cap L_\delta = L_\gamma$. Thus L_γ is a local group, and since the mapping φ of this group onto the local Lie group L_γ^* is homomorphic and homeomorphic it follows that L_γ is a local Lie group.

Now let $L = L_\gamma$. Then the 0-dimensional normal subgroup N and L , which is homeomorphic with an open r -dimensional cube, satisfy conditions a) – e) formulated in the theorem. Moreover, in the course of the proof it has been seen that N may be taken to be any 0-dimensional normal subgroup of G whose factor group is a Lie group. Thus Theorem 69 is proved.

Theorem 70: A locally connected compact finite dimensional group is a Lie group.

Proof: Let G be a locally connected compact group of finite dimension. By Theorem 69 there exists a neighborhood V of the identity in G that is homeomorphic with the product of an open cube L and a 0-dimensional normal subgroup N . From the local connectedness of G it follows that V is a locally connected space. But since N is 0-dimensional and compact the space $L \times N$ can be locally connected only if N consists of a finite number of points. Thus L is itself a neighborhood of the identity in G , and since L is a local Lie group it follows that G is a Lie group.

Theorem 71: If the space of a compact group is a topological manifold (see Section 45) then the group is a Lie group.

Proof: A topological manifold is finite dimensional and locally connected.

Example 82: Let G be a compact connected group of finite dimension r and let Z be any 0-dimensional normal subgroup. We shall show that Z is necessarily a central subgroup of G . Simultaneously it will be seen that there exists a one-to-one homomorphism ψ of a connected r -dimensional Lie group L into G such that $\psi(L)$ is everywhere dense in G .

Let N_1 be a 0-dimensional normal subgroup of G such that G/N_1 is a Lie group. Since $Z/(Z \cap N_1)$ is isomorphic with a subgroup of the Lie group G/N_1 it follows that $Z/(Z \cap N_1)$ is a finite group (see (10)). Since ZN_1/N_1 is isomorphic with $Z/(Z \cap N_1)$, this group is finite too. Hence $N = ZN_1$ is also 0-dimensional and consequently may be used in place of N_1 . Now let $L \subset G$ be a local Lie group of dimension r such that the neighborhood $V = LN$ resolves into the direct product of L and the normal subgroup N (see Theorem 69). Let U_1 be a connected symmetric neighborhood of the identity in L and let $U_1, U_2, \dots, U_n, \dots$ be a decreasing sequence of neighborhoods in L forming a base at the identity. We define $L = U_1 \cup U_1^2 \cup \dots \cup U_1^m \cup \dots$. Clearly L is a subgroup of the algebraic group G . We introduce a topology in L by taking, as a complete system of neighborhoods of the identity, the sequence $U_1, U_2, \dots, U_n, \dots$ (see Theorem 9). The topological group L thus defined is connected and has, as one of its neighborhoods of the identity, the set U_1 with the topology induced therein by G . Since U_1 is a local Lie group it follows that L is itself a Lie group. Associating with each element x of L the element $\psi(x) = x \in G$ we obtain a one-to-one homomorphism ψ of the Lie group L into G . We next show that L is everywhere dense in G . To this end it suffices to show that for an arbitrary neighborhood W of the identity in G , the set LW coincides with G . Let K be

a normal subgroup of G contained in W such that G/K is a Lie group. Then $N_2 = N \cap K$ is also a normal subgroup and G/N_2 is again a Lie group. Let φ denote the natural projection of G onto G/N_2 . Then $\varphi\psi$ is a homomorphism of \hat{L} into G/N_2 , and since G/N_2 is connected and has the same dimension as L it follows that $\varphi\psi(\hat{L}) = G/N_2$. But then $\hat{L}N_2 = G$ and since $N_2 \subset W$ we have $\hat{L}W = G$.

Since every element of U_1 commutes with every element of N it follows that every element of \hat{L} also commutes with every element of N . Finally, since the closure of \hat{L} is all of G it follows that every element of G commutes with every element of N . Thus N is a central normal subgroup of G and since $Z \subset N$ the subgroup Z is also central.

SECTION 48

TRANSITIVE COMPACT TRANSFORMATION GROUPS ACTING ON FINITE DIMENSIONAL SPACES

The main business of the present section is to show that an effective and transitive compact transformation group acting on a finite dimensional space is itself finite dimensional, and also to study the local structure of the space on which such a group acts. It turns out that every point of the space possesses a neighborhood homeomorphic with the topological product of an open cube and a 0-dimensional subspace. Moreover, it will be shown that if this 0-dimensional space is finite then the transformation group is necessarily a Lie group. In particular, the transformation group is a Lie group if the space on which it acts is locally connected.

A) Let G be a 0-dimensional compact group and let H be a subgroup. Then the left coset space $\Gamma = G/H$ is also 0-dimensional.

Indeed, according to B) Section 47, there exists a neighborhood U of the identity in G such that if N is a normal subgroup of G contained in U then the left coset space $\Gamma^* = G/NH$ has dimension no less than that of Γ . But, by Theorem 17 and F) Section 16, G possesses an open normal subgroup $N \subset U$. Since NH is open along with N it follows that G/NH is finite, and, in particular, 0-dimensional. Thus Γ is 0-dimensional too.

B) Let N be a compact group and let N' be the component of the identity in N . Then for any homomorphism φ defined on N the component of the identity in $\varphi(N)$ is $\varphi(N')$.

Denote by $\varphi(N)'$ the component of the identity in $\varphi(N)$. Since $\varphi(N')$ is a connected group it follows that $\varphi(N') \subset \varphi(N)'$. Suppose $\varphi(N') \neq \varphi(N)'$; then the component of the identity in the factor group $\varphi(N)/\varphi(N')$ is the non-trivial group $\varphi(N)'/\varphi(N')$ so that $\varphi(N)/\varphi(N')$ is not 0-dimensional. On the other hand, $\varphi(N)/\varphi(N')$ is isomorphic with a factor group of the 0-dimensional group N/N' and must therefore be 0-dimensional by A). Thus $\varphi(N') = \varphi(N)'$.

Theorem 72: An effective and transitive compact transformation group G acting on a finite dimensional space Γ is finite dimensional.

Proof: Let H be any stabilizer subgroup of G . Then H contains no normal subgroups of G other than $\{e\}$, while the left coset space G/H is homeomorphic with Γ and therefore finite dimensional. Hence, by proposition B) Section 47, there exists a neighborhood U of the identity in G such that for every normal subgroup N of G contained in U we have

$$\dim(G/NH) \geq \dim(G/H) . \quad (1)$$

We show that if $N \subset U$ and G/N is a Lie group then in fact

$$\dim(G/NH) = \dim(G/H) . \quad (2)$$

Let φ be the natural projection of G onto the Lie group G^* = G/N and let $H^* = \varphi(H)$. Clearly G/NH and G^*/H^* are homeomorphic. For the Lie group G^* and subgroup H^* we select a system of one-parameter subgroups $g_1^*, \dots, g_n^*, \dots, g_r^*$ such that for the domain of definition W_ε , $|t| < \varepsilon$, $i = 1, \dots, r$, the set $M_\varepsilon = W_\varepsilon \cap H^*$ is defined by the relations $t^1 = \dots = t_n = 0$ (see Section 44, A)). Here n is the dimension of G^*/H^* . Denote by Λ_ε^* the set of all elements of the form $g_1^*(t^1) \dots g_n^*(t^n)$, $|t^i| < \varepsilon$, $i = 1, \dots, n$. Then every coset X^* of H^* in G^* meets Δ_ε^* in at most one point. For each $i = 1, \dots, n$ let g_i be a one-parameter subgroup of G with domain of definition $|t| < \varepsilon$ such that $\varphi(g_i(t)) = g_i^*(t)$ for $|t| < \varepsilon$ (see Section 47, Lemma 2). With each point $x^* = g_1^*(t^1) \dots g_n^*(t^n) \in \Lambda_\varepsilon^*$ we associate the point $x = f(x^*) = g_1(t^1) \dots g_n(t^n)$, and write $\Lambda_\varepsilon = f(\Lambda_\varepsilon^*)$. Clearly $\varphi(f(x^*)) = x^*$ so that f is a homeomorphism of Λ_ε^* onto Λ_ε , the inverse homeomorphism being given by the projection φ . If now x is any point of Λ_ε then the coset xH meets Λ_ε only in the point x . Indeed, if there existed a point distinct from x and common to the sets xH and Λ_ε then, since φ is a one-to-one mapping of Λ_ε onto Λ_ε^* , there would be at least two points in the intersection of the coset

$\varphi(x)H^*$ with Λ_ε^* , which is impossible. It follows that the collection of cosets of the form xH , $x \in \Lambda_\varepsilon$, is homeomorphic with the open cube Λ_ε^* of dimension n , and consequently that $\dim(G^*/H^*) \leq \dim(G/H)$. But from this and (1) we obtain (2), since G/NH and G^*/H^* are homeomorphic. Moreover, since $G^* = \varphi(G)$ and $H^* = \varphi(H)$ are both Lie groups, equation (2) may equally well be written in the form

$$\dim(\varphi(G)) - \dim(\varphi(H)) = \dim(\Gamma). \quad (3)$$

Observe that this relation was derived solely from the hypotheses that the kernel of φ is contained in U and that $\varphi(G)$ is a Lie group.

Now fix any one normal subgroup $N \subset U$ such that G/N is a Lie group. (That such subgroups exist was proved in Theorem 67.) We show that the dimension of N is necessarily zero. Let $P = N \cap H$, let V be any neighborhood of the identity in G , and let $K \subset V$ be a normal subgroup of G such that G/K is a Lie group. If $N_1 = N \cap K$ then G/N_1 is also a Lie group (see Section 46, A)). Let φ_1 be the natural projection of G onto G/N_1 . Since $N_1 \subset U$ equation (3) holds, so that

$$\dim(\varphi_1(G)) - \dim(\varphi_1(H)) = \dim(\Gamma). \quad (4)$$

Subtracting (3) from (4) we obtain

$$\dim(\varphi_1(G)) - \dim(\varphi(G)) = \dim(\varphi_1(H)) - \dim(\varphi(H)). \quad (5)$$

Since $\varphi_1(G)$ is a Lie group and $\varphi(G) = \varphi_1(G)/\varphi_1(N)$ we have also

$$\dim(\varphi_1(G)) - \dim(\varphi(G)) = \dim(\varphi_1(N)).$$

Similarly

$$\dim(\varphi_1(H)) - \dim(\varphi(H)) = \dim(\varphi_1(P)).$$

Hence, taking (5) into account, we obtain

$$\dim(\varphi_1(N)) = \dim(\varphi_1(P)).$$

Since the Lie groups $\varphi_1(N)$ and $\varphi_1(P)$ have the same dimension and $\varphi_1(P) \subset \varphi_1(N)$ it follows that the components $\varphi_1(N)', \varphi_1(P)'$ of the identity in these two groups must coincide. Let N' and P' denote the components of the identity in N and P . Since $\varphi_1(N') = \varphi_1(N)'$

(see B)) the inverse image of $\varphi_1(N)'$ under φ_1 is $N'N_1$. Similarly, the inverse image of $\varphi_1(P)'$ under φ_1 is $P'N_1$. Thus, since $\varphi_1(N)' = \varphi_1(P)'$ we have $N'N_1 = P'N_1$, whence it follows that $N' \subset P'V$ and $P' \subset N'V$. Since these relations hold for arbitrary V it follows that $N' = P'$. But now N' is the component of the identity in the normal subgroup N so that N' is itself a normal subgroup of G . Thus $N' = P'$ is a normal subgroup of G contained in H so that N' can contain only the identity. In other words N is totally disconnected, and therefore of dimension zero.

It is now a simple matter to show that the dimension of G is finite. Indeed, suppose the contrary and let s be a positive integer greater than $\dim(G/N)$. By proposition B) Section 47 the neighborhood V may be selected so that $\dim(G/N_1) \geq s$. But since G/N_1 is a Lie group we have $\dim(G/N_1) = \dim(G/N) + \dim(N/N_1)$ which is impossible since $\dim(N/N_1) = 0$ (see A)).

Theorem 73: Let G be an effective and transitive compact transformation group acting on a finite dimensional space Γ . Then every point $\alpha \in \Gamma$ possesses a neighborhood Π homeomorphic with the product $\Lambda \times \Theta$ of an open cube Λ and a compact 0-dimensional space Θ which itself admits the action of a transitive compact 0-dimensional transformation group. In the event that Θ consists only a finite number of points, G is a Lie group.

Proof: Let H be the stabilizer subgroup of G leaving fixed the point α . Since there exists a homeomorphism of the left coset space G/H onto Γ that carries the coset H onto α , it suffices to show that the conditions of the theorem are satisfied by some neighborhood of H in the space G/H . By Theorem 72, G has finite dimension, say r . Consequently some neighborhood V of the identity in G resolves into the product of a local Lie group L and a 0-dimensional normal subgroup N (see Theorem 69). Let $P = N \cap H$. Since the natural projection of G onto G/N carries H onto a subgroup of the Lie group G/N which is isomorphic with H/P it follows that H/P is also a Lie group. Moreover, the subgroup P is 0-dimensional since it is contained in the 0-dimensional group N . Thus by Theorem 69 there exists a neighborhood W of the identity in H that resolves into the product of a local Lie group M and the normal subgroup P . Clearly we may assume $W \subset V$. But then, since M is connected and N is 0-dimensional, it follows that $M \subset L$ and consequently that M is a local subgroup of the local Lie group L . Let D^* be a canonical coordinate system of the second kind in L with domain of definition L_ε , $|t^i| < \varepsilon$, $i = 1, \dots, r$, constructed in such a way that the set $M_\varepsilon = L_\varepsilon \cap M$ is defined by the relations $t^1 = \dots = t_n = 0$ (see Section 44, A)). Denote by

Λ_ε is the subset of L_ε defined by the relations $t^{n+1} = \dots = t^r = 0$. Then $L_\varepsilon N$ is a neighborhood of the identity in G , every element of which may be written uniquely in the form $\lambda m n$, where $\lambda \in \Lambda_\varepsilon$, $m \in M$, $n \in N$. Similarly, $M \in P$ is a neighborhood of the identity in H , every element of which may be written uniquely in the form $m p$, where $m \in M_\varepsilon$, $p \in P$. Moreover, if $\lambda_1 m_1 n_1$ and $\lambda_2 m_2 n_2$ are two elements of $L_\varepsilon N$ belonging to one and the same coset of H then, for sufficiently small ε , we have $\lambda_2 m_2 n_2 = \lambda_1 m_1 n_1 m p$ where $m \in M$, $p \in P$. Thus $\lambda_1 m_1 n_1$ and $\lambda_2 m_2 n_2$ belong to the same coset of H when and only when $\lambda_1 = \lambda_2$ and n_1 and n_2 belong to the same coset of P in N . From this it follows immediately that the neighborhood Π of H in G/H consisting of those left cosets that meet $L_\varepsilon N$ is homeomorphic with the product of the open cube Λ_ε and the space N/P .

Since N/P is 0-dimensional (see A) the first part of the theorem is proved. Suppose next that N/P is finite. We must show that in this event G is a Lie group. Since N/P is discrete the subgroup P is open in N and consequently there exists in G a neighborhood U of the identity such that $U \cap N = P \cap U$. Let $K \subset U$ be a normal subgroup of G such that G/K is a Lie group (see Theorem 67). It follows that $N/(N \cap K)$ is also a Lie group and, since this group is 0-dimensional by A), the set $N \cap K$ must be open in N . On the other hand, since $K \subset U$ and $N \cap U = P \cap U$, it follows that $N \cap K = P \cap K$. Thus $N \cap K$, which is normal in G , is included in H and therefore can contain only the identity. It follows that N is discrete and therefore finite. But then L_ε is itself a neighborhood of the identity in G , and since L_ε is a local Lie group by construction it follows that G is a Lie group.

Theorem 74: An effective and transitive compact transformation group G acting on a locally connected finite dimensional space Γ is necessarily a Lie group.

Proof: By Theorem 73 there is a neighborhood Π of the point $\alpha \in \Gamma$ homeomorphic with the product of an open cube Λ and a compact 0-dimensional space Θ . Either Θ is finite or it contains a limit point. But the latter possibility is incompatible with the 0-dimensionality of Θ and the local connectedness of Π . Thus Θ must be finite and G is a Lie group.

Theorem 75: An effective and transitive compact transformation group acting on a manifold is a Lie group.

Proof: A manifold is finite dimensional and locally connected.

Example 83: Let G be an effective and transitive compact transformation group acting on a space Γ homeomorphic with the n -dimensional sphere. The question arises whether there exists a homeomorphism of Γ onto the unit sphere S^n in Euclidean $(n+1)$ -dimensional space which carries G onto some group of motions of S^n . According to Theorem 75, G is a Lie group and the problem is thus reduced to a question in the theory of Lie groups. As far as I know the question still remains unsolved.

Example 84: Let G be an effective, transitive, compact connected transformation group acting on a finite dimensional space Γ . Then in any event the stabilizer subgroups are Lie groups. Indeed G is finite dimensional by Theorem 72 and consequently contain a 0-dimensional normal subgroup N such that G/N is a Lie group (see Theorem 69). From the connectedness of G it follows (see Example 82) that N is central and consequently the intersection of N with a stabilizer subgroup H can contain only the identity. Thus the natural projection of G onto the Lie group G/N maps H isomorphically onto a subgroup of a Lie group, whence it follows that H itself is a Lie group.

9

LOCALLY ISOMORPHIC GROUPS

The central aim of the present chapter is the detailed analysis of the connections in the large between groups that are locally isomorphic. The importance of this problem may be seen in the case of Lie groups. The theory of Lie groups is directed almost entirely to the analysis of their local structure and results in the reduction of this local study to the investigation of Lie algebras (see Chapter 10), the latter being purely algebraic objects. The global study of Lie groups, on the other hand, requires topological methods and, in particular, the illumination of the relations between locally isomorphic groups. This question has already been touched on briefly (see Theorem 18). In this chapter considerably deeper results will be obtained for a class of groups which is narrower but still broad enough to contain all connected Lie groups. For every group G of this class there will be constructed a group \tilde{G} such that every group locally isomorphic with G is isomorphic (globally) with a factor group \tilde{G}/N where N is a discrete (and therefore central, see Theorem 15) normal subgroup of \tilde{G} . The group \tilde{G} is called the universal covering of G . It is also the universal covering of every group locally isomorphic with G , and is uniquely determined by a class of mutually locally isomorphic groups.

In essence this result reduces the investigation of an entire class of locally isomorphic groups to the investigation of a single group—the universal covering belonging to that class. It does not by any means, however reduce the global investigation of a group to the study of its local properties.

The construction of the universal covering employs topological apparatus: the fundamental group and the idea of a covering space. Since these concepts, which go back to the Poincaré, are of great interest and importance in their own right, I shall devote more

attention to them than would be absolutely necessary for the theory of topological groups.

The results of this chapter, as they bear on the theory of topological groups, are due formally to Schreier [48, 49], who was the first to formulate them explicitly, but the ideas were known before Schreier's work, having been employed, for example, in the works of H. Weyl [57].

SECTION 49. THE FUNDAMENTAL GROUP

The fundamental group of a topological space is one of its most important topological invariants, reflecting, as it does, topological properties of the space that are of basic interest. It is in general, not commutative. In this paragraph we define the fundamental group and distinguish that class of topological spaces for which the construction of the fundamental group and of covering spaces is most natural, namely, the arc wise connected, locally arc-wise connected, and locally simply connected spaces.

A) By a path f in a topological space R is meant a continuous function f of the real parameter t , $0 \leq t \leq 1$, associating with each number t , $0 \leq t \leq 1$, a point $f(t) \in R$. The point $f(0)$ is the initial point of f , $f(1)$ is its terminal point, and f is said to join $f(1)$ to $f(0)$ in R . The points $f(0)$ and $f(1)$ are the end points of f . A path f is called a null path if the function $f(t)$ is constant. The path f^{-1} inverse to a given path f is defined to be the function $f(1 - t)$ of the parameter t . If two paths f and g are so related that the terminal point of the first coincides with the initial point of the second, $f(1) = g(0)$, then we define the product $h = fg$ of the paths f and g as follows: $h(t) = f(2t)$ for $0 \leq t \leq 1/2$; $h(t) = g(2t - 1)$ for $1/2 \leq t \leq 1$. A path whose end points coincide is said to be a closed path about the common end point.

It should not be supposed that the collection of paths in a topological space constitutes a group. In the first place, the product is not always defined and even when it is defined it is not associative. Moreover, the product of a path f with its inverse f^{-1} is not, in general, a null path, and the product of a path f with a null path is not, in general, the same as f . For these reasons and others the paths themselves will not interest us much. From our point of view the important objects are the classes of equivalent or homotopic paths. From among these classes we shall pick out a collection that does form a group, and it is this group that is known as the fundamental group.

B) Two paths f and g in a space R are said to be homotopic or equivalent, in symbols: $f \sim g$, if there exists a continuous deformation carrying f into g which does not move the end points. A more precise definition of this concept is as follows: the paths f and g are equivalent if there exists a continuous function $\varphi(s, t)$ of the pair of real parameters s and t , $0 \leq t \leq 1$, $0 \leq s \leq 1$, such that $\varphi(0, t) = f(t)$, $\varphi(1, t) = g(t)$, $\varphi(s, 0) = f(0) = g(0)$, $\varphi(s, 1) = f(1) = g(1)$. Defining $\varphi_s(t) = \varphi(s, t)$ we obtain a path φ_s that depends continuously on the parameter s ; we shall say that the continuously varying path φ_s constitutes a deformation carrying f into g . A closed path f is said to be null-homotopic or equivalent to 0, $f \sim 0$, if it is homotopic to a null path.

It is easily verified that the concept of equivalence of paths here introduced is reflexive: $f \sim f$; symmetric: if $f \sim g$, then $g \sim f$ and transitive: if $f \sim g$ and $g \sim h$, then $f \sim h$. The collection of paths equivalent with a path f will be denoted by $\{f\}$. It is also readily verified that if $f \sim f'$ and $g \sim g'$ and if the product $f \cdot g$ is defined then so is the product $f' \cdot g'$ and

$$fg \sim f'g';$$

moreover,

$$f^{-1} \sim f'^{-1}.$$

C) If f is any path and if e and e' are null paths such that $e(1) = f(0)$, $f(1) = e'(0)$ then

$$ef \sim f, \quad (1)$$

$$e'f \sim f. \quad (2)$$

if f , g , h are paths such that $f(1) = g(0)$, $g(1) = h(0)$, then

$$(fg)h \sim f(gh). \quad (3)$$

Finally, for any path f we have

$$ff^{-1} \sim 0, \quad (4)$$

$$f^{-1}f \sim 0. \quad (5)$$

To facilitate the proof of these facts we begin by making a general remark. Let k be any path, let I denote the number segment, $0 \leq t \leq 1$, and let χ be a continuous mapping of I into itself such that $\chi(0) = 0$. Then $k\chi$, defined by $k\chi(t) = k(\chi(t))$ is a path beginning at the point $k(0)$. If $\chi(1) = 1$ then

$$k\chi \sim k; \quad (6)$$

while if $\chi(1) = 0$ then

$$k\chi \sim 0. \quad (7)$$

Indeed $\varphi(s, t) = k(st + (1 - s)\chi(t))$ defines a deformation of $k\chi$ into k if $\chi(1) = 1$, while $\varphi(s, t) = k((1 - s)\chi(t))$ defines a deformation of $k\chi$ into a null path if $\chi(1) = 0$.

In order to prove (1) we define χ as follows: the segment $[0, 1/2]$ is carried into 0, while the segment $[1/2, 1]$ is mapped linearly onto $[0, 1]$. The $f\chi = e f$ and (1) follows from (6). An analogous choice for χ likewise serves to prove (2).

To prove (3) we let $k = f(gh)$ and define χ as follows: the segment $[0, 1/4]$ is mapped linearly onto $[0, 1/2]$, the segment $[1/4, 1/2]$ is translated onto $[1/2, 3/4]$, and the segment $[1/2, 1]$ is mapped linearly onto $[3/4, 1]$. Then $k\chi = (fg)h$ and (3) follows from (6).

Finally, for the mapping χ of I into itself that carries the segment $[0, 1/2]$ linearly onto $[0, 1]$ and $[1/2, 1]$ linearly onto $[1, 0]$, we have $f\chi = ff^{-1}$ so that (4) follows from (7). Since (5) is just (4) applied to the inverse path f^{-1} , this completes the verification of all parts of C).

D) A topological space R is said to be arcwise connected if any two of its points may be joined by a path in R . R is locally arcwise connected if for every neighborhood U of an arbitrary point $p \in R$ there exists a neighborhood $V \subset U$ of the same point such that p may be joined to any point of V by a path in U . Finally, R is locally simply connected if for every neighborhood U of an arbitrary point $p \in R$ there exists a neighborhood $V \subset U$ of the same point such that every closed path in V about p is null-homotopic in U . If R is locally arcwise connected then there exists a topological base consisting entirely of arcwise connected neighborhoods.

Indeed, let a be any point and U any neighborhood of a . Denote by W the set of all points that can be joined to a by paths in U . Clearly W is arcwise connected and contained in U . We shall show that it is also open. Let $p \in W$. Then since R is locally arcwise connected there exists a neighborhood V of p such that $V \subset U$ and such that every point $x \in V$ can be joined to p by a path lying in U . But the product of such a path with any path in U that joins p to a is a path lying in U and joining x to a . Consequently $x \in W$, i. e., $V \subset W$. Thus W is open.

Definition 44: Let R be an arcwise connected topological space and let p be any one fixed point in R . Denote by P the collection of closed paths about p . The set P is partitioned into equivalence classes by the equivalence relation between paths introduced in B).

This set of equivalence classes of paths we denote by $\pi^1(R, p) = \pi^1(R) = \pi^1$, and we turn it in to a group by defining in it a product as follows: let $\{a\}$ and $\{b\}$ be any two elements of π^1 . Then the product of a and b is defined since both paths have their end points at p . Let $c = ab$. According to B) the equivalence class $\{c\}$ is determined by the classes $\{a\}$ and $\{b\}$ and does not depend on the choice of the particular paths a and b . Consequently we may and do define the product of $\{a\}$ and $\{b\}$ by writing $\{a\}\{b\} = \{c\}$. The group π^1 thus obtained is, up to isomorphism, independent of the choice of the point p , is a topological invariant of the space R , and is called the fundamental group of R . If $\pi^1(R)$ is trivial, then R is said to be simply connected.

It is easy to verify that the product here defined in π^1 satisfies the conditions of Definition 1. Associativity holds by virtue of (3); the identity element of π^1 is the equivalence class consisting of the null-homotopic paths in P (see (1), (2)); finally, for any element $\{a\}$ of π^1 we have $\{a\}^{-1} = \{a^{-1}\}$ (see B) and (4), (5)).

It remains to verify that the fundamental group does not depend on the point p . Let p' be any other point of R and let $\pi'^1 = \pi^1(R, p')$. We must show that π^1 and π'^1 are isomorphic. Let f be an arbitrary but fixed path in R joining p to p' ; such a path exists since R is arcwise connected by hypothesis. For each element $\{a\}$ of π^1 we write $a' = f a f^{-1}$. According to B) the class $\{a'\}$ is uniquely determined by $\{a\}$, i. e., does not depend on the particular choice of the path a (subject, of course, to the condition that f remain fixed). Accordingly, we define $\{a'\} = \varphi(\{a\})$. We shall show that φ is an isomorphism of π^1 onto π'^1 . In the first place, to see that φ is one-to-one, consider the path $f^{-1} a' f$. Clearly $f^{-1} a' f = f^{-1} f a f^{-1} f$ is homotopic with a so that the class $\{a\}$ is in its turn uniquely determined by $\{a'\}$. Since the roles of the groups π^1 and π'^1 may be interchanged in this argument it follows that φ is a one-to-one mapping of π^1 onto π'^1 . Similarly it may be shown that φ preserves the group operations. Indeed, let $\{a\}$ and $\{b\}$ be elements of π^1 and let $a' = f a f^{-1}$, $b' = f b f^{-1}$, $c = ab$. From c) and B) it follows that $a'b'$ and $f c f^{-1}$ are equivalent which says that $\varphi(\{a\}\{b\}) = \varphi(\{a\})\varphi(\{b\})$. Thus φ is an isomorphism.

It should be noted that the construction of the isomorphism φ depends on the choice of the path f and is not uniquely determined by the points p and p' . In particular if p and p' coincide the above construction may be carried out using for f any closed path about p . The isomorphism thus obtained is then an automorphism of π^1 and is, indeed, an inner automorphism as may readily be verified (see Section 3, B)).

E) Let φ be a continuous mapping of an arcwise connected space S into an arcwise connected space R , and let $p \in R$, $q \in S$, $\varphi(q) = p$. Then φ carries each closed path g about q in S into a closed path $\varphi(g) = f$ about p in R , the defining relation for $f = \varphi(g)$ being

$$f(t) = \varphi(g(t)).$$

Clearly this mapping of paths preserves both the relation of equivalence and the operation of multiplication. Thus φ induces a homomorphism of $\pi^1(S, q)$ into $\pi^1(R, p)$ which we denote by φ .

F) Let R and S be arcwise connected topological spaces and let T denote their product. Then T is likewise arcwise connected and its fundamental group is isomorphic with the direct product of the fundamental groups of R and S . In particular, the product of two simply connected spaces is itself simply connected.

To prove this we select base points $p \in R$, $q \in S$ in the spaces R and S and use (p, q) as the base point in T . If f is a path in R with initial point p and g a path in S with initial point q then the function $(f(t), g(t))$ defines a path in T which we may denote by (f, g) . The path (f, g) has initial point (p, q) and terminal point $(f(1), g(1))$. Since R and S are arcwise connected the terminal points of the paths f and g may be chosen arbitrarily so that the terminal point of the path (f, g) may also be chosen arbitrarily. Thus T is arcwise connected.

Conversely, it may readily be verified that any path h in T with initial point (p, q) may be written in the form of a pair (f, g) . Moreover, it is not difficult to see that $(f', g') \sim (f, g)$ when and only when $f' \sim f$ and $g' \sim g$, and that (f, g) is a closed path if and only if f and g are both closed. Finally, for closed paths f , g , f' , g' the product $(f, g)(f', g')$ is identical with the path (ff', gg') . Thus we see that every element of the fundamental group of T may be written uniquely in the form of a pair of elements belonging to the fundamental groups of the spaces R and S , respectively, and this is in such a way that the requirements of Definition A) Section 5 are satisfied. In other words, the fundamental group of T is isomorphic with the direct product of the fundamental groups of R and S .

G) Let G be a topological group. For any path f in G and any $a \in G$ we denote by af and fa the paths traced out by the points $af(t)$ and $f(t)a$ respectively. Then for any two paths f and g in G with initial point e we have

$$f(f(1)g) \sim g(f \cdot g(1)). \quad (8)$$

From this it follows in particular that the fundamental group of an arcwise connected group G is necessarily commutative. Indeed, if f and g are both closed paths about e then (8) reduces to

$$fg \sim gf,$$

In order to prove (8), consider the function $\varphi(s, t) = f(s)g(t)$ of the two variables $s, t; 0 \leq s \leq 1, 0 \leq t \leq 1$. Clearly φ is a continuous mapping of the square $0 \leq s \leq 1, 0 \leq t \leq 1$ into G . For convenience we name the vertices of the square, writing $a = (0, 0)$, $b = (1, 0)$, $c = (1, 1)$, $d = (0, 1)$. Clearly the paths given by the broken lines abc and adc are homotopic in the square. On the other hand, abc is carried by φ into the path $f(f(1)g)$ while adc is carried into $g(fg(1))$. Thus (8) is proved.

Example 85: We shall show that the fundamental group of a Euclidean space of any dimension is trivial, and that the fundamental group of a sphere of any dimension greater than one is likewise trivial.

Let E denote a Euclidean vector space. With each vector $x \in E$ we associate the vector $\varphi_s(x) = (1 - s)x$, $0 \leq s \leq 1$. The mapping φ_s of E into itself thus defined provides a continuous deformation of E into the origin. Applying the deformation φ_s to any closed path f about the origin, we see that any such path is null-homotopic and consequently that the fundamental group of E is trivial.

Suppose now that E is of dimension $n + 1$ and denote by S the n -dimensional unit sphere in E defined by the equation $(x, x) = 1$. Let $p \in S$ and let ψ denote the stereographic projection of $S \setminus p$ from the point p onto the plane $E' \subset E$ defined by the equation $(p, x) = 0$, i. e., the mapping

$$\psi(x) = \frac{1}{1 - (p, x)} \cdot x - \frac{(p, x)}{1 - (p, x)} \cdot p.$$

It is easily verified that ψ is a homeomorphism of $S \setminus p$ onto E' . Since every closed path in E' is null-homotopic the same is true of the closed paths in $S \setminus p$. But now if $n \geq 2$ then any closed path in S about some point other than p is easily seen to be equivalent with a path not passing through p , i. e., to a path in $S \setminus p$. Thus for $n \geq 2$ the fundamental groups of the sphere $S = S^n$ is also trivial.

SECTION 50. COVERING SPACES

Covering spaces play an essential role in various branches of mathematics. Thus the Riemann surface of a multiple valued

analytic function is just a covering surface of the domain of the function, except for the adjunction of poles and branch points of finite order. On this Riemann surface the multiple valued function becomes single valued. Now the same wish to uniformize multiple valued functions leads to the construction of covering spaces in certain other cases too. In the theory of topological groups the notion of a covering space leads to the construction of the universal covering group. In this section the purely topological theory of covering spaces will be developed.

Definition 45: A continuous mapping ω of a topological space R^* onto a topological space R is said to be a covering map, or a projection, and R^* is called a covering (space) of R , if every point $a \in R$ has a neighborhood U such that the inverse image $\omega^{-1}(U)$ is the union of a finite or infinite collection of pairwise disjoint open sets, each of which is mapped homeomorphically onto U by ω . A neighborhood U having this property will, in the sequel, be said to be properly covered and each of the open sets $V \subset R^*$ homeomorphic with U under ω will be called a proper covering of U . Two covering mappings ω_1 and ω_2 of two covering spaces R_1^* and R_2^* onto the same space R are equivalent if there exists a homomorphism φ of R_1^* onto R_2^* such that $\omega_2 \varphi = \omega_1$.

We shall obtain a complete description of the arcwise connected coverings of arcwise connected, locally arcwise connected, and locally simply connected spaces.

A) Let ω be a projection of a covering space R^* onto a space R , let U be a properly covered neighborhood in R , and let V be any proper covering of U in R^* . Let also f be a continuous mapping of an arbitrary connected space S into R^* such that $\omega f(S) \subset U$ and such that the intersection $f(S) \cap V$ is not empty. Then $f(S) \subset V$.

Indeed, the connected set $f(S)$ is contained in $\omega^{-1}(U)$ and consequently cannot meet both the open sets V and $\omega^{-1}(U) \setminus V$.

B) Let ω be a projection of a covering space R^* onto R and let f be a path in R . We shall say that a path f^* in R^* covers f if $wf^*(t) = f(t)$, $0 \leq t \leq 1$. For any path f in R and any fixed point a^* in R^* such that $\omega(a^*) = a = f(0)$ there exists in R^* one and only one path f^* that covers f and has initial point a^* . Moreover, if f is subjected to a continuous deformation that leaves fixed the initial point a , then f^* also undergoes a continuous deformation leaving fixed the initial point a^* . (This deformation of f^* is called the covering deformation or covering homotopy.) Finally, if the terminal point of f remains fixed throughout the deformation then

the same is true of the covering deformation.

Proof: Let f_s be a family of paths depending continuously on the parameter s and having fixed initial point $a \in R$. If I denotes the number segment $[0, 1]$ and if we define $f(s, t) = f_s(t)$ then $f(s, t)$ is a continuous mapping of $Q = I \times I$ into R . From the compactness of the square Q it follows there exists a positive number ε such that for every point $(s_0, t_0) \in Q$ there exists a properly covered neighborhood $U(s_0, t_0)$ of the point $f(s_0, t_0)$ containing all of the points $f(s, t)$ for $(s, t) \in S_\varepsilon(s_0, t_0) = Q \cap Q_\varepsilon(s_0, t_0)$ where $Q_\varepsilon(s_0, t_0)$ denotes the square $|s - s_0| \leq \varepsilon, |t - t_0| \leq \varepsilon$.

We assume without loss of generality that $\varepsilon = \frac{1}{n}$ where n is a positive integer. Let p be an integer, $0 \leq p < n$, and suppose there exists one and only one continuous function $f^*(s, t)$ defined on the rectangle $0 \leq s \leq 1, 0 \leq t \leq p\varepsilon$, and satisfying the conditions

$$f(s, 0) = a^*, \quad \omega f^*(s, t) = f(s, t). \quad (1)$$

We shall extend f^* continuously to the larger rectangle $0 \leq s \leq 1, 0 \leq t \leq (p + 1)\varepsilon$, in such a way that (1) continues to be satisfied, and show that f^* continues to be uniquely determined by (1) for this enlarged set of parameter values. Since the inductive hypothesis is certainly satisfied for $p = 0$, this will prove the existence and uniqueness of a covering deformation. For $0 \leq s \leq 1$, let $V(s, p\varepsilon)$ denote that open set in R^* which properly covers $U(s, p\varepsilon)$ and which contains the point $f^*(s, p\varepsilon)$, and denote by ω_s' the homeomorphism of $U(s, p\varepsilon)$ onto $V(s, p\varepsilon)$ inverse to ω . If $f^*(s, t)$ is any continuous function of the parameter t that is defined and satisfies (1) for $p\varepsilon \leq t \leq (p + 1)\varepsilon$ then it follows from A) that

$$f^*(s, t) = \omega_s' f(s, t), \quad p\varepsilon \leq t \leq (p + 1)\varepsilon. \quad (2)$$

Since s here denotes any point of I , this shows that the enlarged function f^* is unique if it exists. On the other hand, (2) defines a function f^* on the strip $S: 0 \leq s \leq 1, p\varepsilon \leq t \leq (p + 1)\varepsilon$, which does satisfy (1) and which depends continuously on the parameter t for each fixed value of s . Since the function f^* so defined agrees by construction with the given function f^* along the segment $0 \leq s \leq 1, t = p\varepsilon$, it remains only to show that f^* is continuous on S in both variables s and t . To see this, choose two points s, s_0 such that $0 \leq s \leq 1, 0 \leq s_0 \leq 1$, and $|s - s_0| \leq \varepsilon$. Then $f(s, t) \in U(s_0, p\varepsilon)$ for $p\varepsilon \leq t \leq (p + 1)\varepsilon$, so that $\omega_{s_0}' f(s, t)$ defines a continuous solution of (1) on this interval. But then (see (2)) we must have $\omega_{s_0} f(s, t) = f^*(s, t) = \omega_s' f(s, t)$ for $p\varepsilon \leq t \leq (p + 1)\varepsilon$. In other

words $f^*(s, t)$ agrees with the mapping $\omega_{s_0} f(s, t)$ on the rectangle $R_\varepsilon(s_0, p_0)$ and is therefore continuous there. In particular, f^* is continuous in a neighborhood (relative to S) of each point (s_0, t) , and since s_0 is an arbitrary point of I it follows that f^* is continuous on S .

Suppose now that $f(t)$ is a path in R with initial point a . If $f_1^*(t)$ and $f_2^*(t)$ are two paths in R covering f and having the same initial point a^* , then $f_1^*(s, t) = f_1^*(t)$ and $f_2^*(s, t) = f_2^*(t)$ both define continuous solutions of (1) for the trivial deformation $f_s = f$, $0 \leq s \leq 1$, whence it follows from the uniqueness of covering deformations that $f_1^* = f_2^*$. Thus a covering path with initial point a^* is unique if it exists. On the other hand the trivial deformation of f does possess a covering deformation as we have seen. By the uniqueness just established, this covering deformation must also be trivial and yields at once a path f^* which covers f .

Finally, suppose the terminal point of the path f_s remains fixed for all $0 \leq s \leq 1$, i.e., that $f(s, 1)$ is a constant function. Since $f^*(s, 1)$ is continuous for $0 \leq s \leq 1$ it then follows from A) that $f^*(s, 1) \in V(0, 1)$, $0 \leq s \leq 1$, and consequently that the function $f^*(s, 1)$ is also constant. This completes the proof of B).

Recall that two subgroups H_1 and H_2 of a group G are said to be conjugate if there exists an element $g \in G$ such that $H_2 = g^{-1} H_1 g$. This relation is clearly reflexive, symmetric, and transitive, and consequently partitions the collection of all subgroups of G into pairwise disjoint equivalence classes of mutually conjugate subgroups.

Theorem 76: Let ω be a projection of an arcwise connected covering space R^* onto an arcwise connected space R . Let p be a fixed point in R and let p^* be any point of R^* that projects onto p : $\omega(p^*) = p$. Then the homomorphism $\hat{\omega}$ (see Section 49, E)) is an isomorphism of the fundamental group $\pi^1(R^*, p^*)$ onto a subgroup $\rho(\omega, p^*)$ of the fundamental group $\pi^1(R, p)$. Moreover, as p^* runs over the set $\omega^{-1}(p)$, the subgroup $\rho(\omega, p^*)$ runs over exactly one class of conjugate subgroups of $\pi^1(R, p)$ which we denote by $\sigma(\omega)$.

Proof: Let f^* be any closed path in R^* about the point p^* and let $f = \omega f^*$. It follows from B) that if f is null-homotopic in R then f^* is also null-homotopic in R^* . Thus the homomorphism $\hat{\omega}$ is one-to-one and yields an isomorphism onto a subgroup $\rho(\omega, p^*)$.

Now let p_1^* and p_2^* be any pair of points belonging to $\omega^{-1}(p)$, let f_1^* be a closed path about p_1^* , f_2^* a closed path about p_2^* , and let g^* be a path joining p_2^* to p_1^* . We write $\omega f_1^* = f_1$, $\omega f_2^* = f_2$, $\omega g^* = g$; all three of the paths f_1 , f_2 , g are closed paths about p . Since f_1^* and $g^* f_2^* g^{*-1}$ are both closed paths about p_1^* it follows

that their images f_1 and gf_2g^{-1} determine elements $\{f_1\}$ and $\{g\}$ $\{f_2\}$ $\{g\}^{-1}$ of the subgroup $\rho(\omega, p_1^*)$. Similarly both $\{f_2\}$ and $\{g\}^{-1} \{f_1\} \{g\}$ belong to the subgroup $\rho(\omega, p_2^*)$. Since $\{f_1\}$ and $\{f_2\}$ are arbitrary elements of the subgroups $\rho(\omega, p_1^*)$ and $\rho(\omega, p^*)$, respectively, we see that $\{g\} \rho(\omega, p_2^*) \{g\}^{-1} \subset \rho(\omega, p_1^*)$, and also $\{q\} \rho(\omega, p^*) \{q\} \subset \rho(\omega, p_2^*)$. In other words

$$\rho(\omega, p_2^*) = \{g\}^{-1} \rho(\omega, p_1^*) \{g\}. \quad (3)$$

Thus the subgroups $\rho(\omega, p_1^*)$ and $\rho(\omega, p_2^*)$ are conjugate. On the other hand, if we fix a point p_1^* in the set $\omega^{-1}(p)$, choose any element $\{g\}$ of the group $\pi^1(R, p)$, and let g^* be the path with initial point p_1^* that covers g , then the terminal point $g^*(1) = p_2^*$ also belongs to $\omega^{-1}(p)$. But then (3) holds. Thus an arbitrary subgroup of $\pi^1(R, p)$ conjugate with $\rho(\omega, p_1^*)$ is of the form $\rho(\omega, p_2^*)$ where $p_2^* \in \omega^{-1}(p)$ and the collection of subgroups of the form $\rho(\omega, p^*)$, $p^* \in \omega^{-1}(p)$, fills exactly one conjugate class of subgroups.

C) Let ω be a covering mapping of a covering space R^* onto R , let $p \in R$, $p^* \in \omega^{-1}(p)$, and let f_1^* and f_2^* be any two paths in R^* with initial point p^* . Then the terminal points of f_1^* and f_2^* coincide if and only if the terminal points of their images $f_1 = \omega f_1^*$, $f_2 = \omega f_2^*$ coincide and $\{f_1\} \{f_2\}^{-1} \in \rho(\omega, p^*)$. In particular, f_1^* is closed when and only when f_1 is closed and $\{f_1\} \in \rho(\omega, p^*)$.

We begin by considering the special case in which f_1 is closed. In the first place, if f_1^* is closed then we have $\{f_1\} \in \rho(\omega, p^*)$ by definition. On the other hand if $\{f_1\} \in \rho(\omega, p^*)$ then there exists a closed path h^* about p^* whose image $h = \omega h^*$ belongs to the class $\{f_1\}$. Since h and f_1 are homotopic it follows that it is possible to deform h continuously into f_1 without moving the end points, whence it follows from B) that the covering path h^* may be deformed continuously into f_1^* without moving the end points. In particular h^* and f_1^* must have the same end points, and since h^* is a closed path so is f_1^* .

We turn now to the general case. In the first place, if f_1^* and f_2^* have the same terminal point then the same is certainly true of the images f_1 and f_2 . Moreover, $f_1^*(f_2^*)^{-1}$ is closed, whence we have $\{f_1\} \{f_2\}^{-1} \in \rho(\omega, p^*)$. Suppose, on the other hand, that these two conditions are satisfied. The path $f_1 f_2^{-1}$ is covered by $f_1^*(g_2^*)^{-1}$ where $(g_2^*)^{-1}$ denotes the path with initial point $f_1^*(1)$ that covers f_2^{-1} . Since, as we have just seen, $f_1^*(g_2^*)^{-1}$ is closed it follows that $(g_2^*)^{-1}$ must have terminal point p^* . Thus g_2^* and f_2^* both have initial point p^* and cover the same path f_2 . Consequently

$g_2^* = f_2^*$, and in particular $f_2^*(1) = g_2^*(1) = f_1^*(1)$. Thus f_2^* and f_1^* have the same terminal point.

It is an easy consequence of C) that the cardinal number of the set $\omega^{-1}(x)$, $x \in R$, is equal to the index of the subgroup $\rho(\omega, p^*)$ in the fundamental group $\pi^1(R, p)$, where $p \in R$ is any base point and p^* any element of $\omega^{-1}(p)$. Thus this cardinal number is independent of x ; it is called the number of sheets of the covering ω .

Theorem 77: Let ω_1 and ω_2 be two covering mappings of arcwise connected covering spaces R_1^* and R_2^* onto the same arcwise connected and locally arcwise connected space R . Let $p \in R$, $p_1^* \in \omega_1^{-1}(p)$, $p_2^* \in \omega_2^{-1}(p)$, and suppose that $\rho(\omega_1, p_1^*) \subset \rho(\omega_2, p_2^*)$. Then there exists a covering mapping ω of R_1^* onto R_2^* such that $\omega_2 \omega = \omega_1$. In the event that $\rho(\omega_1, p_1^*) = \rho(\omega_2, p_2^*)$ the mapping ω is a homeomorphism. From this it follows, in particular, that two coverings ω_1 and ω_2 are equivalent when and only when $\sigma(\omega_1) = \sigma(\omega_2)$.

Proof: Let x_1^* be an arbitrary point of R_1^* , and let f_1^* be an arbitrary path in R_1^* joining x_1^* to p_1^* . Let also $f = \omega_1 f_1^*$ be the projection of this path on R and let f_2^* be the path in R_2^* that covers f and has initial point p_2^* . Finally, let x_2^* be the terminal point of f_2^* . In this way we associate with each $x_1^* \in R_1^*$ a point $x_2^* \in R_2^*$, the whole construction depending only on the choice of f_1^* . In general, if f_1^* were replaced by some other path joining x_1^* to p_1^* the point x_2^* would be changed; in our case however, we have $\rho(\omega_1, p_1^*) \subset \rho(\omega_2, p_2^*)$, whence it follows by C) that replacing the chosen path f_1^* by any other path with the same end points has no effect on x_2^* . Thus x_2^* is uniquely determined by the point x_1^* and we define $x_2^* = \omega(x_1^*)$. Clearly $\omega_2 \omega = \omega_1$. Moreover, since the construction can be carried through in reverse order, starting from $x_2^* \in R_2^*$, to obtain a point $x_1^* \in R_1^*$ for which $\omega(x_1^*) = x_2^*$, we see that ω is onto. Likewise, employing C) once again, we observe that if $\rho(\omega_1, p_1^*) = \rho(\omega_2, p_2^*)$ then ω must be one-to-one. Since a covering mapping that is one-to-one is necessarily a homeomorphism, the proof of the theorem will be complete once we show that ω is a covering mapping.

Let $x_1^* \in R_1^*$, $x_2^* = \omega(x_1^*)$, $x = \omega_2(x_2^*)$, and let U be an arcwise connected open set in R that contains x and is properly covered by both ω_1 and ω_2 . (Such sets exist and, indeed, constitute a base in R ; see Section 49, D). Denote by $V_i(x_i^*)$, $i = 1, 2$, that open set in R_i^* which properly covers U and contains x_i^* . We shall show that $\omega(V_1(x_1^*)) = V_2(x_2^*) = V_2(\omega(x_1^*))$ and that ω maps $V_1(x_1^*)$ homeomorphically onto $V_2(x_2^*)$. Let paths f_1^* , f , f_2^* be chosen as above, let $y_1^* \in V_1(x_1^*)$ and let g_1^* be a path in $V_1(x_1^*)$

joining y_1^* to x_1^* . Let also $g = \omega_1 g_1^*$ and let g_2^* be the path in R_2^* that covers g and has initial point x_2^* . Clearly g_2^* lies in $V_2(x_2^*)$. But also $f_2^* g_2^*$ covers the path fg . Thus $\omega(y_1^*) \in V_2(x_2^*)$, and it follows that $\omega(V_1(x_1^*)) \subset V_2(x_2^*)$. Moreover, this mapping of $V_1(x_1^*)$ into $V_2(x_2^*)$ is given by $\omega = \omega_2^{-1} \omega_1$ where ω_2^{-1} denotes the well defined homeomorphism of U onto $V_2(x_2^*)$ inverse to ω_2 , whence it follows that ω maps $V_1(x_1^*)$ homeomorphically onto all of $V_2(x_2^*)$.

Suppose now that x_2^* is any point of R_2^* . From what has just been shown it follows that the inverse image $\omega^{-1}(V_2(x_2^*))$ is the union of all the sets $V_1(x_1^*)$, $x_1^* \in \omega^{-1}(x_2^*)$. Thus $V_2(x_2^*)$ is properly covered by ω . Moreover, if follows, in particular, that $\omega^{-1}(V_2(x_2^*))$ is open in R_1^* , and since the special sets $V_2(x_2^*)$ constitute a base in the topological space R_2^* , the argument also serves to show that ω is continuous. Thus the proof of Theorem 77 is complete.

Theorem 77 settles the question of the uniqueness of covering spaces. The following result settles the question of their existence.

Theorem 78: Let R be an arcwise connected, locally arcwise connected, and locally simply connected Hausdorff space. Let $p \in R$ and let ρ be an arbitrarily prescribed subgroup of the fundamental group $\pi^1(R, p)$. Then there exists a covering mapping ω of an arcwise connected covering space R^* onto R such that $\rho(\omega, p^*) = \rho$ for some $p^* \in \omega^{-1}(p)$.

Proof: If f and g are any two paths in R with initial point p then we regard f and g as equivalent modulo ρ if their terminal points coincide and if $\{fg^{-1}\} \in \rho$. It is easily seen that this relation is reflexive, symmetric, and transitive, and consequently partitions the collection of all paths with initial point p into disjoint equivalence classes of pairwise equivalent paths. For the sake of brevity we shall refer to these classes as bundles and we define R^* to consist of the set of all bundles. Associating with each bundle x^* the unique point $\omega(x^*) = x \in R$ which is the common terminal point of the paths belonging to x^* , we obtain a mapping ω of R^* into R . The mapping ω is onto since R is arcwise connected.

We topologize R^* by defining a complete system of neighborhoods. To this end let Σ denote the collection of all arcwise connected open sets U in R with the property that every closed path in U is null-homotopic in R . From the fact that R is both locally arcwise connected and locally simply connected it follows at once that Σ is a base for R (see Section 49, D)). Next, for any $U \in \Sigma$ and any bundle x^* such that $\omega(x^*) \in U$, we define $U^* = \{U, x^*\} \subset R^*$

in the following manner: if $f \in x^*$ and if g is a path in U with initial point x and terminal point $y \in U$, then the bundle y^* containing the path fg belongs to U^* , and only those bundles belong to U^* that may be so obtained. It turns out that y^* is uniquely determined by the point y and the bundle x^* , and does not depend upon the choice of the paths f and g , i.e., ω is one-to-one mapping of U^* onto U . Indeed, if $f' \in x^*$ is some other path belonging to x^* and g' some other path in U joining y to x then $f'g'(fg)^{-1} = f'g'g^{-1}f^{-1}$. But $g'g^{-1}$ is a closed path in U and is therefore null-homotopic in R . Consequently $f'g'(fg)^{-1}$ is homotopic with $f'f^{-1}$. But $\{f'f^{-1}\} \in \rho$ by hypothesis, and it follows that $f'g'$ and fg belong to the same bundle. An immediate verification discloses that

$$\omega(U^*) = U; \quad (4)$$

and, moreover, that

$$\text{if } y^* \in \{U, x^*\} \text{ then } \{U, y^*\} = \{U, x^*\}. \quad (5)$$

Denote now by Σ^* the collection of all sets of the form $\{U, x^*\}$. We shall show that Σ^* satisfies the conditions of Theorem 3, i.e., that Σ^* is a base for a uniquely defined topology on R^* .

Let x^* and y^* be distinct points of R^* . If $\omega(x^*) \neq \omega(y^*)$ then there exist in Σ disjoint neighborhoods U and V of the points $\omega(x^*)$ and $\omega(y^*)$ and we define $U^* = \{U, x^*\}$, $V^* = \{V, y^*\}$. Since the sets $\omega(U^*)$ and U and $\omega(V^*) = V$ are disjoint, it follows that U^* and V^* are also disjoint. If, on the other hand, $\omega(x^*) = \omega(y^*) = x$, let U be any neighborhood of x belonging to Σ and let $U^* = \{U, x^*\}$, $V^* = \{U, y^*\}$. Suppose that U^* and V^* have an element z^* in common. Then $U^* = \{U, z^*\}$, $V^* = \{U, z^*\}$, and since ω is one-to-one on the set $U^* = V^*$ it follows from $\omega(x^*) = \omega(y^*)$ and the fact that x^* and y^* both belong to $U^* = V^*$ that $x^* = y^*$, which is impossible. Thus U^* and V^* must be disjoint.

Let now x^* be any point of R^* . Since every set in Σ^* containing x^* is of the form $\{U, x^*\}$ where $\omega(x^*) \in U$, $U \in \Sigma$, it follows that any two neighborhoods of x^* may be written in the form $\{U, x^*\}$, $\{V, x^*\}$ where U and V are neighborhoods of $\omega(x^*)$. But then there exists a neighborhood $W \in \Sigma$ such that $W \subset U \cap V$ and the set $\{W, x^*\}$ belongs to Σ^* , contains x^* , and satisfies the condition $\{W, x^*\} \subset \{U, x^*\} \cap \{V, x^*\}$. Thus Σ^* defines a topology on R^* .

It is now a simple matter to verify that ω is a covering mapping and R^* a covering space of R . Indeed, let $x \in R$ and let U be any neighborhood of x belonging to Σ . It is clear that $\omega^{-1}(U)$ is just the union of the sets $\{U, x^*\}$, $x^* \in \omega^{-1}(x)$, and these sets, which we have just seen to be disjoint, are open by definition. Moreover, we have already shown that ω maps each set $\{U, x^*\}$ in one-to-one

fashion onto U . Finally, that the mapping of $\{U, x^*\}$ onto U induced by ω is homeomorphic follows immediately from the definition of Σ^* .

We now fix as a base point p^* the bundle containing the null path at p and show that R^* is arcwise connected and that $\rho(\omega, p^*) = \rho$. Let f be any path with initial point p and define $f_s(t) = f(st)$. Then f_s depends continuously on the parameter s and defines a deformation of the path f . Denote by $f^*(s)$ the bundle containing f_s . We shall show that f^* is a path in R^* which covers f and has initial point p^* . Since it is clear that $wf^*(t) = f(t)$ and that $f^*(0) = p^*$, it is only necessary to verify that $f^*(s)$ is a continuous function of s . Let s_0 be any fixed value of the parameter, let U be a neighborhood of $f(s_0)$ belonging to Σ , and let $U^* = \{U, f^*(s_0)\}$. Choose a positive number ϵ sufficiently small so that $f(s) \in U$ for $|s - s_0| < \epsilon$. Clearly each path f_s , $|s - s_0| < \epsilon$, is equivalent with the path obtained by multiplying f_{s_0} on the right by the path described by $f(t)$ as t goes from s_0 to s . But then, according to the definition of $U^* = \{U, f^*(s_0)\}$, we have $f^*(s) \in U^*$, $|s - s_0| < \epsilon$, whence it follows that f^* is continuous.

In order to see that R^* is arcwise connected, let x^* be a point of R^* and let f be any path belonging to the bundle x^* . Then the path f^* just constructed joins x^* to p^* in R^* .

Finally, to verify the relation $\rho(\omega, p^*) = \rho$ it suffices to show that the path f^* covering f is closed when and only when f is closed and $\{f\} \in \rho$ (see C)). But, by construction, f is contained in the bundle $f^*(1)$; consequently the latter bundle contains the null path at p when and only when f is closed and satisfies the condition $\{f\} \in \rho$.

D) A covering mapping $\tilde{\omega}$ of an arcwise connected space \tilde{R} onto an arcwise connected space R is said to be the universal covering mapping, and \tilde{R} is called the universal covering space for R , if R is simply connected. It follows from Theorem 77 that if R is locally arcwise connected, and if ω^* any covering mapping of an arcwise connected covering space R^* onto R , then there exists a covering mapping ω of \tilde{R} onto R^* such that $\omega^*\omega = \tilde{\omega}$. It is for this reason that the covering is said to be universal. It also follows from Theorem 77 that the universal covering is unique up to equivalence. Finally, Theorem 78 implies the existence of a universal covering for an arbitrary arcwise connected, locally arcwise connected, and locally simply connected space R .

The following proposition concerns an interesting group theoretical example of a covering.

E) Let G be an arcwise connected topological group, let D be any discrete subgroup of G , and let $M = G/D$ denote the space of (for the sake of definiteness, say, right) cosets. It is easy to verify that the natural projection ω of G onto M is a covering mapping. It turns out that in this situation the subgroup $\rho(\omega, e)$ of the fundamental group $\pi^1(M, \omega(e))$ is a central normal subgroup and that the factor group $\pi^1(M, \omega(e))/\rho(\omega, e)$ is isomorphic with D . In particular, if G is simply connected then the fundamental group of the coset space M is itself isomorphic with D . A complete description of the group $\pi^1(M, \omega(e))$ in the general case will be given in the following proof.

By a bundle we shall here mean any equivalence class of pairwise homotopic paths having initial point e and terminal point lying in the subgroup D . If $\{f\}$ and $\{g\}$ are two such bundles then it is clear that the bundle $\{f(f(1)g)\}$ depends only on $\{f\}$ and $\{g\}$ and not on the choice of the particular paths f and g ; consequently we may define $\{f\}\{g\} = \{f(f(1)g)\}$. (Here $f(1)g$ denotes, as usual, the path traced out by $f(1)g(t)$ as t varies from 0 to 1; see Section 49, G)). Thus an operation of multiplication is introduced in the collection P of all bundles. Observe that the bundles determined by closed paths at e are precisely the elements of the fundamental group $\pi^1(G, e)$, and that for two such equivalence classes the product just defined is the same as their product considered as elements of the fundamental group.

If $\{f\}$ is any bundle then ωf is a closed path in M about the point $\omega(e)$, and since the equivalence class $\{\omega f\}$ depends only on the bundle $\{f\}$ and not on the path f we may write $\omega(\{f\}) = \{\omega f\}$, thus defining a mapping ω of P into the fundamental group $\pi^1(M, \omega(e))$. It turns out that ω is a one-to-one mapping of P onto the entire fundamental group. Indeed, if f' is an arbitrary closed path in M about the point $\omega(e)$ and f is the path in G covering f' and having initial point e , then $f(1) \in D$ so that $\{f\} \in P$ and since clearly $\omega(\{f\}) = \{f'\}$ we see that ω is onto. On the other hand, if $\{f'\} = \{g'\}$ then the covering paths f and g belong to the same bundle, whence it follows that ω is one-to-one.

Finally, we show that ω preserves the operation of multiplication of bundles. Indeed since $f(1) \in D$ we have $\omega f(1)g = \omega g$ and consequently

$$\omega(\{f\}\{g\}) = \{\omega(f(f(1)g))\} = \{\omega f\}\{\omega g\} = \omega(\{f\})\omega(\{g\}).$$

It follows that P forms a group with respect to the operation of multiplication of bundles and that the group P is mapped isomorphically by ω onto the fundamental group $\pi^1(M, \omega(e))$.

As has already been observed, the fundamental group $\pi^1(G, e)$

$= N$ constitutes a subgroup of P . In order to complete the proof of E) it suffices to show that N is a central subgroup. To this end let f be any closed path about e and let g be a path with initial point e and terminal point lying in D . Since g^{-1} covers the inverse of the path ωg we have $\{g\}^{-1} = \{g(1)^{-1}g^{-1}\}$, and since the product $g(g(1)f)$ has terminal point $g(1)$ it follows that $\{g\}\{f\}\{g\}^{-1} = \{g(g(1)f)g^{-1}\}$. But now, by (8) Section 49, we have

$$g(g(1)f) \sim fg.$$

Thus $\{g\}\{f\}\{g\}^{-1} = \{f\}$, and consequently N belongs to the center of P .[†]

Example 86: We construct the universal covering, and compute the fundamental group, of the n -dimensional torus. Let R be the vector group of dimension n and let e_1, \dots, e_n be a basis in R . Denote by D the discrete subgroup consisting of all integral linear combinations of the vectors e_1, \dots, e_n and let ω be the natural projection of R onto $R/D = T^n$. The space T^n is homeomorphic with an n -dimensional torus for $n \geq 2$ and is a circle for $n = 1$. Clearly ω is the universal covering of T^n . Let $f_i^*(t) = te_i$, $0 \leq t \leq 1$, $i = 1, \dots, n$. Then the path $\omega f_i^* = f_i$ is closed in T^n , and it follows easily from E) that elements $\{f_1\}, \dots, \{f_n\}$ constitute a linearly independent system of generators for the fundamental group $\pi^1(T^n, 0)$. Thus $\pi^1(T^n, 0)$ is a free abelian group of rank n . The group T^n we denote by K . The fundamental group $\pi^1(K, 0)$ is generated by $\{f\}$ where $f(t)$ traverses the circle K once uniformly in the positive direction, starting from 0 and returning to 0, as t varies from zero to one.

Example 87: We construct the universal covering, and compute the fundamental group, of a lemniscate. Take r exemplars of the circle group K (see the preceding example) and denote them by K_1, \dots, K_r ; the elements 0 and $1/2$ in the copy K_i will be denoted by 0_i and q_i respectively. We identify all of the points 0_i , $i = 1, \dots, r$, into a single point p , and denote by L the connected complex resulting from this identification. The complex L is just the circle for $r = 1$, and is homeomorphic with the familiar lemniscate for $r = 2$. Denote by f_i the path defining the generator of the fundamental group of K_i and denote by a_i the generator itself. Since

[†] That P/N is isomorphic with D may be seen as follows: the mapping $\{f\} \rightarrow f(1)$ is a well defined homomorphism of P into D having N for its kernel; it is also onto since G is arcwise connected. Trans.

f_i is a closed path in L about the point p we may regard a_i as an element of $\pi^1(L, p)$. It turns out that $\pi^1(L, p)$ is the free (non-commutative for $r > 1$) group on the independent generators a_1, \dots, a_r . The exact sense of the assertion will be made clear below.

Let n be an arbitrary non-negative integer, let $\alpha(i)$ be any integral valued function of the integral argument $i = 1, 2, \dots, n$, which takes only values $1, 2, \dots, r$, and never takes the same value at two neighboring values of the argument, and let $\beta(i)$ be any integral valued function of the same integral argument which never takes the value zero. Then an expression of the form

$$c = (a_{\alpha(1)})^{\beta(1)} (a_{\alpha(2)})^{\beta(2)} \dots (a_{\alpha(n)})^{\beta(n)}. \quad (6)$$

is called a word in the letters a_1, \dots, a_r . For $n = 0$ we obtain the empty or identical word, which we denote by the symbol 1. It turns out that each element of the group $\pi^1(L, p)$ may be written in the form (6) in one and only one way, and it is this that is meant by saying that $\pi^1(L, p)$ is the free group on the independent generators a_1, \dots, a_r .

We show first that every element of $\pi^1(L, p)$ may be written in the form (6). Denoting by I the segment $[0, 1]$, we observe that a closed path g about p in L is a continuous mapping of I into L that carries the end points into p . Since $K_i \setminus p = U_i$ is an open set in L it follows that $g^{-1}(U_i) = V_i$ is an open set in I that does not contain the end points of I . Hence V_i is a finite or countable union of pairwise disjoint open intervals J_{i1}, J_{i2}, \dots . Since the set $g^{-1}(q)$ is compact it is easily seen that there can be only a finite number of intervals J_{ij} meeting $g^{-1}(q_i)$. Denote by J_i the union of the intervals J_{ij} that do not meet $g^{-1}(q)$. By sliding each point $g(t)$, $t \in J_i$, uniformly to p along the shorter of the two arcs on K_i determined by $g(t)$ and p , we obtain a deformation of g carrying it onto an equivalent path which we continue to denote by g , and for which the number of intervals J_{ij} is finite. But now the mapping g , considered on the segment \bar{J}_{i1} , defines a definite element of the group $\pi^1(K, p)$ which may be written as some power of a , and it follows that an arbitrary element $\{g\} \in \pi^1(L, p)$ may be written in the form (6).

In order to prove that the representation (6) is unique for elements of $\pi^1(L, p)$ we construct the universal covering $\tilde{\omega}$ of the linear complex L , an object of considerable interest in its own right. We begin by cutting L at each of the points q_i , $i = 1, \dots, r$; thus each of the points q_i splits into a pair of points $q_i(+1)$ and $q_i(-1)$, where we agree for the sake of definiteness that $q_i(+1)$ denotes that one of the two points which we come to in moving along K_i in the positive direction starting from p . Let ω' denote the

natural projection of the complex L' thus obtained onto the original lemniscate L . Then ω' is a local homeomorphism in the neighborhood of every point except the points $q_i(\varepsilon)$, $\varepsilon = \pm 1$, $i = 1, \dots, r$, while the points $q_i(-1)$ and $q_i(+1)$ are mapped by ω' onto the same point q_i . We next associate with each word c of the form (6) an exemplar of the complex L' , which we denote by L_c . The natural projection ω' of L_c onto L will be denoted by ω_c . Moreover, the points $q_i(\varepsilon)$ and the point p belonging to the complex L_c will be denoted by $q_{ic}(\varepsilon)$ and p_c , respectively. Let now c be a word of the form (6), let a_i be any one of the generators a_1, \dots, a_r , and let $\varepsilon = \pm 1$. In the event that $i = \alpha(n)$ we suppose that ε has the same sign as $\beta(n)$, and in this case we write:

$$d = d(c, \varepsilon) = (a_{\alpha(1)})^{\beta(1)} \dots (a_{\alpha(n)})^{\beta(n) + \varepsilon}. \quad (7)$$

If, on the other hand, $i \neq \alpha(n)$, then ε may be either ± 1 and we write:

$$d = d(c, \varepsilon) = (a_{\alpha(1)})^{\beta(1)} \dots (a_{\alpha(n)})^{\beta(n)} a_i^\varepsilon. \quad (8)$$

The word defined by (7) or (8), depending on the case, is called an extension of c . Clearly any word may be obtained as the result of a finite sequence of extensions, starting from the identical word, the sequence of extensions employed being uniquely determined by the word finally obtained. If d is an extension of c we identify the point $q_{ic}(\varepsilon)$ in the complex L_c with the point $q_{id}(-\varepsilon)$ in the complex L_d . Let \tilde{L} denote the complex resulting from all such identifications. Then \tilde{L} is arcwise connected, for, as noted, any word may be obtained from the identical word by a sequence of extensions which shows that it is possible to pass continuously from the complex L_1 , associated with the identical word, to any other complex L_c . Moreover, the mapping $\tilde{\omega}$ of \tilde{L} onto L obtained by uniting the projections ω_c is easily seen to be a covering mapping. Now let c be any word of the form (6). We associate with c a path f_c in L which starts at the point p , goes round the circle $K_{\alpha(1)}$ exactly $\beta(1)$ times, then around the circle $K_{\alpha(2)}$ exactly $\beta(2)$ times, and so forth, finally going around the circle $K_{\alpha(n)}$ exactly $\beta(n)$ times. Let \tilde{f}_c be the path in \tilde{L} that covers f_c and has initial point p_1 . Clearly \tilde{f}_c has terminal point p_c . This shows, in the first place, that distinct words necessarily define distinct elements of the fundamental group $\pi^1(L, p)$, and simultaneously, that a closed path about p_1 in \tilde{L} must be projected by $\tilde{\omega}$ onto a path in L homotopic with f_1 , i.e., onto a null-homotopic path. In other words, the fundamental group $\pi^1(\tilde{L}, p_1)$ is trivial, so that $\tilde{\omega}$ is, in fact, the universal covering.

Example 88: We construct the universal covering, and compute the fundamental group, of the generalized projective plane. Let E be a disc of unit radius in the plane and let K be the circle that forms its boundary. We introduce polar coordinates in E , taking as origin the center 0 of the disc and measuring angles from a fixed point p on the boundary K . Then every point $x \in E$ may be written in the form $x = (\rho, \theta)$. We now fix a positive integer $n \geq 2$ and construct a topological space P_n by identifying each boundary point $(1, \theta)$ with the point $(1, \theta + \frac{2\pi}{n})$. (Thus P_2 is homeomorphic with the projective plane.) Let φ denote the natural projection of E onto P_n . The arc I on K consisting of the points $(1, \theta), 0 \leq \theta \leq \frac{2\pi}{n}$, is carried by φ onto a circle K' lying on P_n , and φ induces on the circle K an n -sheeted covering mapping of K onto K' . It is not difficult to verify that the generator a of the fundamental group $\pi^1(K', p')$, where $p' = \varphi(p)$, is in fact a generator of the fundamental group $\pi^1(P_n, p')$ and that $a^n = 1$. In order to show that $\pi^1(P_n, p')$ is exactly the cyclic group of order n we construct the universal covering of P_n . To this end we take n exemplars, E_1, \dots, E_n , of the disc E and identify them along their boundaries by identifying each point $(1, \theta)$ in E_i with the corresponding point $(1, \theta)$ in E_j ; $i, j = 1, \dots, n$. Let \tilde{P}_n denote the topological space thus obtained. It is easy to see that \tilde{P}_n is simply connected. Each point $x \in \tilde{P}_n$ is defined by giving the index i of the disc E_i to which it belongs, and then the coordinates ρ, θ of the point x in E_i : we write $x = (\rho, \theta, i)$. Let $\omega(\rho, \theta, i) = (\rho, \theta + \frac{2\pi i}{n})$, where the right member is to be regarded as a point in P_n . It may be verified that this defines a mapping of \tilde{P}_n onto P_n , and that this mapping is a covering mapping; and since \tilde{P}_n is simply connected the covering thus obtained is, in fact, the universal covering. Finally, since the universal covering is n -sheeted it follows that the order of the fundamental group $\pi^1(P_n)$ is n .

SECTION 51. COVERING GROUPS

In this paragraph it will be shown that an arcwise connected covering space of a topological group is itself, in a natural way, a topological group. In the case of the universal covering space we obtain in this fashion the universal covering group. It follows from Theorem 80 that the universal covering group is unique.

Moreover, Theorem 80 also says that any local homomorphism of a simply connected group may be extended to a homomorphism in the large. This result bears the character of a uniformization theorem, inasmuch as attempts to extend local homomorphisms of non-simply connected groups lead to multiple valued mappings.

Theorem 79: Let ω be a covering mapping of an arcwise connected covering space G^* onto an arcwise connected and locally arcwise connected topological group G . Then it is possible to define in G^* an operation of multiplication in such a way that G^* becomes a topological group and ω a homomorphism of G^* onto G . Clearly the homomorphism ω is open and has discrete kernel.

Proof: As the identity element e^* in G^* we select an arbitrary element of the set $\omega^{-1}(e)$. Let a^* and b^* be any two points of G^* , let f^* and g^* be paths in G^* joining them to e^* and write $a = \omega(a^*)$, $b = \omega(b^*)$, $f = \omega f^*$, $g = \omega g^*$. Finally, construct the path $h = f(ag)$, let h^* be the path in G^* that covers h and has initial point e^* , and denote by c^* the terminal point of h^* . We shall show that c^* depends only on a^* and b^* and not on the choice of the paths f^* and g^* . Suppose f_1^* and g_1^* are two other paths joining a^* and b^* to e^* and write $f_1 = \omega f_1^*$, $g_1 = \omega g_1^*$. If $h_1 = f_1(ag_1)$ and h_1^* denotes the path in G^* that covers h_1 and has initial point e^* we must show that h^* and h_1^* have a common terminal point. According to C) Section 50 it suffices to show $\{h_1 h^{-1}\} \in \rho(\omega, e^*)$. But now

$$h_1 h^{-1} = f_1(ag_1)(ag^{-1})f^{-1} = f_1(a(g_1g^{-1}))f^{-1} \sim (g_1g^{-1})(f_1f^{-1})$$

(see Section 49(8)), and since $\{f_1f^{-1}\} \in \rho(\omega, e^*)$, $\{g_1g^{-1}\} \in \rho(\omega, e^*)$, it follows that

$$\{h_1 h^{-1}\} \in \rho(\omega, e^*).$$

Thus c^* is uniquely determined by a^* and b^* . Accordingly we define

$$c^* = a^*b^*.$$

It is then clear that

$$\omega(a^*b^*) = \omega(a^*)\omega(b^*). \quad (1)$$

The associativity of this product follows from the associativity of multiplication of paths (see Section 49, (3)). Moreover, e^* is an identity element with respect to it. Finally, the element inverse to a^* is the terminal point of the path covering $a^{-1}f^{-1}$. Thus G^* becomes a group and ω becomes a homomorphism.

It remains to verify that the group operations are continuous in G^* . We begin by showing that if f^* and g^* are paths in G^* then

the point $f^*(t)(g^*(t))^{-1}$ depends continuously on the parameter t , i.e., describes a path in G^* . Since any path in G^* may be viewed as a part of some path having initial point e^* it is no loss of generality to suppose that f^* and g^* themselves begin at e^* . Let

$$f = \omega f^*, \quad g = \omega g^*, \quad f_s(t) = f(st), \quad g_s(t) = g(st).$$

By definition $f^*(s)(g^*(s))^{-1}$ is the terminal point of the path h_s^* covering h_s , where $h_s = f_s(f(s)(g(s))^{-1}g_s^{-1})$. From this formula it may be seen that h_s depends continuously on s , whence it follows that the covering path h_s^* likewise depends continuously on s (see Section 50 B)). But then so must its terminal point $f^*(s)(g^*(s))^{-1}$.

Now let a^* and b^* be any two points of G^* . Let $c^* = a^*(b^*)^{-1}$, write $a = \omega(a^*)$, $b = \omega(b^*)$, $c = \omega(c^*)$, and select a neighborhood W^* of c^* that properly covers some neighborhood W of c . We construct neighborhoods U^* , V^* of a^* , b^* , respectively, such that $U^*V^{*-1} \subset W^*$. Since the properly covering neighborhoods W^* constitute a base in G^* this will complete the proof of the theorem. Let U and V be arcwise connected properly covered neighborhoods of a and b , respectively, such that $UV^{-1} \subset W$, and let U^* and V^* be neighborhoods of a^* and b^* that properly cover U and V . If $x^* \in U^*$ there is a path f^* in U^* joining x^* to a^* . Similarly for any point y^* belonging to V^* there is a path g^* in V^* joining y^* to b^* . Then since

$$\omega(f^*(s)(g^*(s))^{-1}) = \omega f^*(s)(\omega g^*(s))^{-1} \in UV^{-1} \subset W$$

and $f^*(0)(g^*(0))^{-1} \in W^*$, and since $f^*(s)(g^*(s))^{-1}$ depends continuously on s , it follows from A) Section 50 that $f^*(s)(g^*(s))^{-1} \in W^*$, $0 \leq s \leq 1$. In particular, $x^*(y^*)^{-1} = f^*(1)(g^*(1))^{-1} \in W^*$. Thus $U^*V^{*-1} \subset W^*$ and the proof of Theorem 79 is complete.

The following theorem is of great importance. It implies, in particular, the uniqueness of the universal covering group.

Theorem 80: Let G and G' be arcwise connected topological groups, and suppose that G is also locally arcwise connected and simply connected. Let f be a local homomorphism of G into G' (see Section 23, K)). Then it is possible to extend f in one and only one way to a homomorphism φ of the entire group G into G' ; i.e., there exists a unique homomorphism φ of G into G' that coincides with f in some neighborhood W of the identity in G . If the local homomorphism f is onto then φ is a homomorphism of G onto G' . If f is open so is φ . If G' is also locally arcwise connected and simply connected, and if f is a local isomorphism, then φ is an isomorphism.

Proof: If φ is any homomorphism of the algebraic group G into the algebraic group G' which is an extension of f in the above sense then φ , being continuous in a neighborhood W of the identity in G , must be continuous everywhere (see Section 20, A)), and is consequently a homomorphism of the topological group G into the topological group G' . If the local homomorphism f is onto and if φ is a homomorphic extension of f then $\varphi(G)$ contains $f(W)$ which in turn contains a neighborhood of the identity in G' , and since G' is arcwise connected, and in particular connected, it follows that φ is onto (see Theorem 14). Again, if the local homomorphism f is open and if φ is a homomorphic extension of f then φ is an open mapping of W into G' and is consequently open everywhere (see Section 20, A) once again). Thus all but the first and last assertions of the theorem are disposed of.

We show next that the homomorphic extension φ is unique if it exists. Indeed, suppose φ and φ' are two homomorphisms, both of which extend f . Let $x \in G$ and let W be a neighborhood of the identity in G on which φ and φ' both coincide with f . Since G is connected it follows from Theorem 14 that x may be written in the form $x = a_1 \dots a_n$ where $a_i \in W$, $i = 1, \dots, n$. But then

$$\varphi(x) = f(a_1) \dots f(a_n), \quad \varphi'(x) = f(a_1) \dots f(a_n)$$

whence it follows that

$$\varphi(x) = \varphi'(x).$$

We turn now to the construction of φ . Let g be an arbitrary path in G with initial point at the identity e . We shall show that there corresponds to g a uniquely determined path g' in G' satisfying the following conditions:

- a) $g'(0) = e'$, where e' denotes the identity element in G' ;
- b) If U denotes that neighborhood of e in G on which the given local homomorphism f is defined, then there exists a positive number ε sufficiently small so that for $|t_1 - t_2| \leq \varepsilon$ we have

$$(g(t_1))^{-1} g(t_2) \in U \text{ and } (g'(t_1))^{-1} g'(t_2) = f((g(t_1))^{-1} g(t_2)).$$

Let us see first that the path g' is unique if it exists. To begin with, the initial point of g' is determined by a). Moreover, if g' is uniquely determined for all $t < \tau$ then it is uniquely determined for $t = \tau$ by continuity. But then $g'(t)$ is also uniquely determined for all t such that $0 \leq t \leq 1$ and $t - \tau < \varepsilon$ since, according to b), $g'(t) = g'(\tau) f((g(\tau))^{-1} g(t))$. Thus g' is uniquely determined for all values of t .

We next show that such a path g' exists. Let V be a neighborhood of e such that $V^{-1}V \subset U$. There exists a positive integer n

sufficiently large so that for $|t_1 - t_2| \leq 1/n$ we have $(g(t_1))^{-1} g(t_2)$ in V . Let $\epsilon = 1/n$, let m be an integer, $0 \leq m < n$, and suppose g' is already defined for all values of t , $0 \leq t \leq m\epsilon$, in such a way that a) and b) are satisfied. We shall show that the domain of definition of g' may then be extended to the larger interval $0 \leq t \leq (m+1)\epsilon$. Since the inductive hypothesis is satisfied for $m=0$ if we simply define $g'(0) = e'$, this will complete the proof of the existence of the desired path g' . Let $0 \leq h \leq \epsilon$. We define $g'(m\epsilon + h)$ by writing

$$g^*(m\epsilon + h) = g'(m\epsilon) f((g(m\epsilon))^{-1} g(m\epsilon + h)). \quad (2)$$

In order to see that b) continues to hold for the extended function $g'(t)$ thus obtained, let h' be any number such that $|h'| \leq \epsilon$. Then

$$g'(m\epsilon + h') = g'(m\epsilon) f((g(m\epsilon))^{-1} g(m\epsilon + h')). \quad (3)$$

Indeed, if h' is positive this follows from (2), while if h' is negative it is a consequence of the inductive hypothesis. But then

$$(g'(m\epsilon + h))^{-1} g'(m\epsilon + h') = f((g(m\epsilon + h))^{-1} g(m\epsilon + h')),$$

which shows that b) is satisfied. Since the validity of a) for the extended function is automatic, the proof is complete.

Now let t_1 and t_2 be two numbers such that $0 \leq t_1 < t_2 \leq 1$, $t_2 - t_1 \leq \epsilon$, and suppose the path g is subjected to a continuous deformation leaving fixed all points except those belonging to the interval $t_1 < t < t_2$. Then the corresponding path g' is changed only on the same parameter interval. Indeed, the above construction shows that, for $0 \leq t \leq t_1$, g' depends only on the behavior of the path g for $0 \leq t \leq t_1$. Moreover, for $t = t_2$, $g'(t)$ is determined by b) and $g'(t_1)$, while, for $t_2 \leq t \leq 1$, the behavior of $g'(t)$ is again completely determined by $g'(t_2)$ and the behavior of g for $t_2 \leq t \leq 1$. Let us call a deformation of g of the sort here described a small deformation. From what has just been said it follows, then, in particular, that if the path g is subjected to any small deformation, the end points of the corresponding path g' remain unchanged. But now it is not hard to see that any deformation of g that leaves its end points fixed may be obtained as the result of a sequence of several small deformations. Thus if g_1 and g_2 are any two homotopic paths in G with the common initial point e then the corresponding paths g'_1 and g'_2 have the same end points.

Now let x be any point of G and let g be a path joining x to e . Then the terminal point x' of the path g' corresponding to g depends only on x and not on the choice of g . Indeed, if h is any other path joining x to e in G then, since G is by hypothesis, simply connected, it follows that h and g are homotopic and hence that h' and g' have

the same terminal point x' . In this way we associate with each $x \in G$ a uniquely determined $x' \in G$, thus defining a mapping φ of G into G' : $x' = \varphi(x)$.

We show next that there exists a neighborhood $W \subset U$ of e on which $\varphi = f$. Let W be an arcwise connected neighborhood of e such that $W^{-1}W \subset U$, let $x \in W$, and let g be a path joining x to e in W . Then the path $g' = fg$ satisfies condition b) of the above construction. Indeed, since $g(t) \in W$ we have $(g(t))^{-1} \in W^{-1}$ and consequently, for any two numbers t_1 and t_2 , $0 \leq t_1, t_2 \leq 1$, $(g(t_1))^{-1}g(t_2) \in W^{-1}W \subset U$. But then

$$\begin{aligned} f((g(t_1))^{-1}g(t_2)) &= f((g(t_1))^{-1})f(g(t_2)) = (f(g(t_1)))^{-1}f(g(t_2)) \\ &= (g'(t_1))^{-1}g'(t_2). \end{aligned}$$

Thus the terminal point of the corresponding path g' is $f(x)$, i.e., $\varphi(x) = f(x)$ for $x \in W$.

We show next that φ is a homomorphism of the algebraic group G into the algebraic group G' . Let a and b be any two elements of G , let g and h be paths in G joining a and b , respectively, to e , and let g' and h' be the corresponding paths in G' . If a' and b' denote the terminal points of g' and h' , then $\varphi(a) = a'$, $\varphi(b) = b'$. It is clear that $m g(ah)$ is a path in G joining ab to e . Similarly, $m' = g'(a'h')$ joins $a'b'$ to e' . Moreover, a direct verification discloses that m' is the path corresponding to m . Thus $\varphi(ab) = a'b' = \varphi(a)\varphi(b)$, i.e., φ is homomorphic.

It remains only to consider the case in which G' is itself locally arcwise connected and simply connected and f is a local isomorphism. In this case, by choosing U sufficiently small, we may arrange for f to possess an inverse mapping f^{-1} which is itself a local isomorphism of G' into G . Since G' satisfies all the hypotheses originally imposed on G , it follows from the portion of the theorem already proved that f^{-1} also possesses a continuous open homomorphic extension ψ mapping G' onto G . The mapping $\psi(\varphi(x)) = \chi(x)$ is then an open homomorphism of G onto itself, and since $\chi(x)$ coincides with the mapping $f^{-1}(f(x)) = x$ in a neighborhood of e , it follows that χ is an extension of the local identity automorphism in G . But then, by the uniqueness of extension, we have $\chi(x) = x$ for all $x \in G$. Since φ and ψ are already known to be onto, this suffices to prove that $\varphi^{-1} = \psi$ and consequently that φ is an isomorphism. Thus all parts of Theorem 80 are proved.

Theorems 78, 79, 80 make possible the following definition.

Definition 46: A topological group will be said to be admissible if it is arcwise connected, locally arcwise connected, and locally

simply connected. Denote by Γ the class of all admissible groups that are locally isomorphic with some one fixed admissible group. From Theorems 78, 79, 80 it follows that in Γ there is one and, up to isomorphism, only one simply connected group. This group is called the universal covering group for all of the groups belonging to Γ . According to Theorem 80 each group in Γ may be obtained from the universal covering group by factoring out some discrete (and, consequently, central, see Theorem 15) normal subgroup.

The following examples are of great theoretical significance. In them we compute the fundamental groups and the centers of the rotation groups of Euclidean spaces. In Section 65 (see Example 108) we shall, using the same methods, compute the fundamental groups and centers of the groups belonging to the remaining two series of classical compact Lie groups.

Example 89: We shall investigate the rotation groups H_3 and H_4 of Euclidean space of dimension three and four. The investigation will be based on the use of quaternions and will disclose, in particular, that the fundamental groups $\pi^1(H_3)$ and $\pi^1(H_4)$ are of order two.

Let K denote the division ring of quaternions (see Section 26), D the field of real numbers, considered as a subfield of K , J the collection of all pure imaginary quaternions, and G the multiplicative group of quaternions of modulus one. The manifold G is homeomorphic with a three dimensional sphere and is therefore simply connected (see Example 85). With each pair x, y of quaternions belonging to G we now associate a linear transformation $\varphi_{x,y}$ of K into itself according to the formula

$$\varphi_{x,y}(u) = xuy^{-1}, \quad u \in K.$$

Since $|xuy^{-1}| = |u|$ it follows that $\varphi_{x,y}$ is a rotation of the Euclidean space K . It turns out that, associating with each element (x, y) of $G \times G$ the rotation $\lambda(x, y) = \varphi_{x,y}$, we obtain a homomorphism λ of $G \times G$ onto the group H_4 of all rotations of the four dimensional space K . The kernel of λ consists of the two elements $(1, 1)$ and $(-1, -1)$. Since $G \times G$ is also simply connected (see Section 49, F)) it follows that the fundamental group $\pi^1(H_4)$ is of order two. Moreover, the transformation $\psi_x = \varphi_{x,x}$ leaves fixed the line D and consequently maps the orthogonal complement J onto itself. Thus ψ_x may be regarded as a rotation of the three dimensional space J , and defining $\mu(x) = \psi_x$, we obtain another homomorphism μ of G onto the group H_3 of all rotations of the three dimensional space J . The kernel of μ coincides with the center of G and consists

of the elements 1 and -1. Thus H_3 has trivial center and its fundamental group is also of order two. Finally, the path f in G joining -1 to 1 and defined by the formula

$$f(t) = \cos \pi t + k \sin \pi t, \quad 0 \leq t \leq 1,$$

is carried by μ into the closed path $g = \mu f$ in H_3 defined by the formula

$$g(t) = \begin{vmatrix} \cos 2\pi t & -\sin 2\pi t & 0 \\ \sin 2\pi t & \cos 2\pi t & 0 \\ 0 & 0 & 1 \end{vmatrix} \quad (4)$$

The element $\{g\}$ of the fundamental group $\pi^1(H_3)$ containing g has order two and generates the group.

In the first place, a simple computation shows that

$$\psi_{x,y} \circ \psi_{x',y'} = \psi_{xx',yy'},$$

so that λ is, in fact, a homomorphism of $G \times G$ into H_4 . From this it follows that μ is also a homomorphism of G into H_3 . We show first that $\mu(G) = H_3$. Let $l = aj + bk$ where $a^2 + b^2 = 1$. Then

$$l^2 = -1, \quad li = -il. \quad (5)$$

Now let $x = \cos \beta + l \sin \beta$. It follows from (5) that

$$\begin{aligned} \psi_x(i) &= (\cos \beta + l \sin \beta)i(\cos \beta - l \sin \beta) = (\cos \beta + l \sin \beta)^2 i \\ &= (\cos 2\beta + l \sin 2\beta)i = i \cos 2\beta + (bj - ak)\sin 2\beta, \end{aligned} \quad (6)$$

whence we see that, by making suitable choices for a, b, β , we may obtain a transformation ψ_x carrying the quaternion i into any element of the set $S^2 = J \cap G$. Moreover, for $a = 0, b = 1$, (6) reduces to

$$\psi_x(i) = i \cos 2\beta + j \sin 2\beta, \quad (7)$$

and since, in this case, x commutes with k it follows that by means of transformations of the form ψ_x we may effect an arbitrary rotation of J about the k -axis. But, now, G is a group and it follows from what has been said that the transformations of the form ψ_x , $x \in G$, suffice to effect an arbitrary rotation of J . Moreover, it is clear from the multiplication table for K that the only elements of G commuting with i are of the form $a + bi$, while the only elements commuting with j are of the form $a + bj$. Thus the center of G consists only of 1 and -1, and the kernel of μ likewise consists of the same two elements. Finally, (4) is an immediate consequence of (7).

Now let φ be any rotation of K , and let $\varphi(1) = z$. Then

$\varphi_{1,z}^{-1}$ φ leaves D fixed and may therefore be written in the form $\varphi_{x,x}$. Thus

$$\varphi = \varphi_{1,z}^{-1} \varphi_{x,x} = \varphi_{x,z^{-1}x},$$

whence it follows that λ is onto. On the other hand, if $\varphi_{x,y}$ is the identity rotation then it leaves in particular, the axis D fixed, so that $x = y$. But then, as has already been shown, $x = \pm 1$. Thus the kernel of λ consists of two elements (1, 1) and (-1, -1).

Example 90: Let G be a Lie group, H a subgroup, and denote by $M = G/H$ the space of (for the sake of definiteness, say, right) cosets. We shall show that if G and H are connected, and if the manifold M is homeomorphic with an r-dimensional sphere, $r > 2$, then the fundamental groups $\pi^1(G)$ and $\pi^1(H)$ are isomorphic:

$$\pi^1(G) \approx \pi^1(H) \quad (8)$$

This comparatively special result will be used later in completing the computation of the fundamental groups of the classical compact Lie groups. In order to prove it we first prove the following preparatory lemma, which may also be employed to elucidate the connection between the fundamental groups of the manifolds G, H, and M in the general case.

Lemma: Let φ be the natural projection of the Lie group G onto the manifold $M = G/H$ of (right) cosets. Let g_t be a continuous deformation of a mapping g_0 of an arbitrary compact space R into M, and let f_0 be a continuous mapping of R into G such that $\varphi f_0 = g_0$. Then there exists a continuous deformation f_t of f_0 such that $\varphi f_t = g_t$, $0 \leq t \leq 1$. (Such a deformation will be said to cover the given deformation g_t .) The deformation f_t also satisfies the condition that if for some $x_0 \in R$, we have $g_t(x_0) = g_0(x_0)$, $0 \leq t \leq 1$, then also $f_t(x_0) = f_0(x_0)$, $0 \leq t \leq 1$.

Proof: Let L be a smooth cross-section in G which meets H in e and is mapped homeomorphically by φ onto a neighborhood of the point $p = \varphi(e) \in M$ (for the construction of such a set, see Section 44, A)). There exists a positive integer n so large that if $|t_1 - t_2| \leq \frac{1}{n}$ and $a \in \varphi^{-1}(g_{t_1}(x))$ then the set L a meets the coset $g_{t_2}(x)$ in a single point. Suppose now that f_t has already been defined for all t , $0 \leq t \leq \frac{p}{n}$. We extend the domain of definition of the deformation to the interval $\frac{p}{n} \leq t \leq \frac{p+1}{n}$ by taking

for $f_t(x)$ the unique point of intersection of the set $L_{f_p}(x)$ with

the coset $g_t(x)$. It is readily verified that the deformation f_t resulting from this inductive construction satisfies all the above requirements.[†]

We turn now to the proof of (8). The line of argument developed here may also be employed to obtain more general results.

Let g be an arbitrary closed path in M about the point $p = \varphi(e)$. We may regard g as a continuous deformation g_t of a mapping of a one point space $R = \{c\}$ into M , writing $g_t(c) = g(t)$. Hence, by the lemma, there exists a path f in G having initial point e and satisfying the condition $\varphi f = g$. The terminal point of f belongs to H and, if H is connected, the path f may be extended through H back to the point e . In this way we obtain in G a closed path f about e which satisfies the condition $\varphi f \sim g$. Thus we see that if both G and H are connected the induced homomorphism φ is onto. Moreover, it follows from the lemma that if g is null-homotopic in M the covering path f may be deformed continuously into a path lying in H . Thus the kernel of φ consists exactly of those equivalence classes of closed paths that possess representatives lying wholly in H . Finally, let f be a closed path about e in H which is null-homotopic in G . Since f is closed it may be regarded as a continuous mapping of a circle S^1 into H . Moreover, since f is null-homotopic in G , it can be extended to a continuous mapping of the disc E^2 having S^1 as its boundary. But now the mapping φf of E^2 into M collapses the entire boundary S^1 into the point p and, if M is (topologically) a sphere of dimension greater than two, then, φf can be continuously deformed into the constant mapping that collapses the entire disc E^2 into the point p without changing the values of φf on the boundary S^1 . The covering deformation of this deformation has, as its end result, a continuous mapping of the disc E^2 into H that still induces the original closed path f on the boundary S^1 . Thus we see that if f is null-homotopic in G it is also null-homotopic in H . Finally, since the fundamental group $\pi^1(M)$ of the sphere M is trivial (see Example 85), it follows from what has been said that G and H have isomorphic fundamental groups.

Example 91: Let H_n denote the group of all rotations of n -dimensional Euclidean space E^n , $n \geq 3$, or, what comes to the same thing, the group of orthogonal matrices of order n having determinant one. It turns out that all of the groups H_n have

[†] A version of the covering homotopy theorem that contains both this lemma and Section 50, B) may be found in [51, Chapter 1]. Trans.

fundamental groups of order two and, consequently, that the universal covering group \tilde{H}_n of H_n is two-sheeted. Moreover, for odd n , the center of H_n is trivial while, for even n , the center consists of the two matrices e and $-e$. Accordingly, for odd n , the center of the universal covering group \tilde{H}_n is a cyclic group of order two while, for even n , the center of \tilde{H}_n is a group of order four. The complete story is as follows: if n is divisible by four then the center of \tilde{H}_n is the direct product of two cyclic groups in order two, while if n is even but not divisible by four then the center of \tilde{H}_n is a cyclic group of order four.

In order to compute the fundamental group of H_n we regard it as a transitive transformation group acting on the unit $(n - 1)$ -dimensional sphere S^{n-1} in the Euclidean space E^n . Let $p \in S_{n-1}$. Then the stable subgroup of H_n corresponding to p (see Section 3, K) is clearly isomorphic with H_{n-1} , and we denote it by H_{n-1} . Thus $H_n/H_{n-1} = S^{n-1}$ and, by Example 90, the fundamental groups of the manifolds H_n and H_{n-1} are isomorphic with one another for $n \geq 4$. Since the fundamental group of H_3 is of order two (see Example 89) it follows that the fundamental groups of all the groups H_n , $n \geq 3$, are of order two.

We show next that a square matrix $z = \|z_{ij}^i\|$ of order n that commutes with all the matrices belonging to H_n is scalar. Indeed, denote by $a = a(p, q)$ the element of H_n , depending on the two integral parameters p and q , $p \neq q$, $1 \leq p, q \leq n$, in which the only non-zero entries are

$$a_i^i = 1, \quad i \neq p, q; \quad a_q^p = -a_p^q = 1.$$

From the commutativity $za = az$ we obtain for the entries of z the relations

$$z_p^p = z_q^q \tag{9}$$

$$z_p^\alpha = z_q^\alpha = 0 \text{ for } \alpha \neq p, q. \tag{10}$$

If now z_β^α is any entry of z off the main diagonal, and if $n \geq 3$, we may choose p and q such that $q = \beta$, $p \neq \alpha$, whence it follows from (10) that $z_\beta^\alpha = 0$. Thus z must be a diagonal matrix, and hence by (9) a scalar matrix. Thus the center of H_n consists of scalar matrices. But, for odd n , the only scalar matrix belonging to H is the identity matrix e while, for even n , there are the two scalar matrices, e and $-e$.

Suppose now that n is even; we shall also compute the center of the universal covering group \tilde{H}_n . Let $\sigma(t)$ be the matrix of order two defining a rotation of the plane through the angle πt :

$$\sigma(t) = \begin{vmatrix} \cos \pi t & -\sin \pi t \\ \sin \pi t & \cos \pi t \end{vmatrix}.$$

We define $f(t)$ to be the diagonal block matrix consisting of $\frac{n}{2}$ blocks, each equal to $\sigma(t)$. Then f is a path in H_n joining $-e$ to e , so that the covering path \tilde{f} in \tilde{H}_n has initial point at the identity and terminal point at a central element u which projects onto $-e$ under the natural homomorphism. From this it follows that if the center of \tilde{H}_n is cyclic of order four then u is of order four, while if the center of \tilde{H}_n is the direct sum of two groups of order two then u is of order two. But now, by the definition of multiplication in the covering group \tilde{H}_n (see the proof of Theorem 79), the element u^2 , is the terminal point of the path covering $f((-e)f)$, which is the path described by $g(t) = f(2t)$. Thus if g is null-homotopic in H_n then u^2 is the identity and u has order two, while if g is not null-homotopic then u^2 must have order two so that u is of order four. Hence it only remains to examine the behavior of g . Consider the diagonal block matrix $h(t^1, \dots, t^n)$ consisting of the diagonal blocks

$\sigma(2t^1), \dots, \sigma(2t^n)$. The function h maps an $\frac{n}{2}$ - dimensional cube into H_n . The diagonal of the cube joining the vertex $(1, 1, \dots, 1)$ to $(0, 0, \dots, 0)$ is carried by h onto the path g , while every edge of the cube is carried onto a closed path which is not null-homotopic (see Example 89, (4) and Example 90) and therefore onto the generator of $\pi^1(H_n)$. Since in a cube of dimension $\frac{n}{2}$ the diagonal is homotopic to a path consisting of $\frac{n}{2}$ edges, we see that g is null-homotopic when and only when $\frac{n}{2}$ is even. Thus the question of the structure of the center of \tilde{H}_n is settled in full.

Example 92: Let G denote the group of quaternions of modulus one (see Section 26, A)) and let H denote the set of quaternion units, i. e., the set of elements $\pm 1, \pm i, \pm j, \pm k$. Clearly H is a non-commutative subgroup of order eight. Hence the coset space G/H is a three dimensional manifold having a non-commutative fundamental group isomorphic with H (see Section 50, E)).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

10

LIE GROUPS AND LIE ALGEBRAS

In the seventh chapter the concept of a Lie group was introduced and the simplest properties of Lie groups were discussed. In this chapter the results of Chapter 7 will be made the basis of a more detailed analysis of Lie groups. With each Lie group we associate a more elementary algebraic object, the Lie algebra, and show that the local analysis of a Lie group can be entirely reduced to the analysis of its Lie algebra. The details of this reduction comprise the principal contents of the chapter though certain related matters will also be considered. The deeper results of Killing [25], Cartan [8] and Weyl [57] will be presented (but only for compact groups) in the following chapter.

It was shown in Chapter 7 that the functions that turn up in the analysis of the structure of a Lie group are differentiable functions of several real variables. Accordingly, we may make full use of the apparatus of differential calculus and the theory of differential equations, and these will in fact be our principal weapons in the present chapter. In view of the number and complexity of the computations to be encountered I shall once more, as in Chapter 7, employ the notational conventions of tensor analysis.

SECTION 52 STRUCTURE CONSTANTS. THE LIE ALGEBRA

We begin by introducing the structure constants of a Lie group. This system of numbers form a tensor, i.e., transforms as do the components of a tensor under a change of coordinates in the group. The Lie algebra is an algebraic object equivalent with the complete system of structure constants and invariant with

respect to change of coordinates. We also establish the fundamental properties of structure constants comprising the content of the third theorem of Lie (see Theorem 81) and the corresponding properties of the Lie algebra.

The basic method of the present paragraph will be the expansion of various functions in Taylor series up to terms of degree two or, sometimes, three. The study of the Taylor coefficients that thus appear will lead us to the structure constants as well as to the relations they satisfy. It would have been possible, to be sure, to conduct the investigation in terms of derivatives, as is customary, but the use of Taylor series seems to me to be more fitting.

A) The remainders of series will not be written out in detail but will rather be indicated by ϵ 's with various indices. In each case the order of vanishing of the remainder ϵ will be specifically stated. If ϵ is a function of the arguments x_1, \dots, x_n then we shall say that ϵ is small of order $q + 1$ with respect to these arguments if ϵ/ρ^q tends to zero with $\rho = \sqrt{[x_1^2 + \dots + x_n^2]}^{1/2}$.

B) Just as in Chapter 7, whenever some letter is used to denote a point or a vector the same letter equipped with appropriate superscripts will denote the coordinates of that point or vector. This convention will be adhered to throughout the chapter and consequently need not be restated each time it is used.

Definition 47: Let G be an r -dimensional local Lie group and let D be a differentiable coordinate system in G (see Definition 39). If x and y are elements of G sufficiently close to the identity e then the product $f = xy = f(x, y)$ is also close to e and the rule of multiplication may be written in coordinate form in terms of the coordinate system D :

$$f^i = f^i(x, y) = f^i(x^1, \dots, x^r; y^1, \dots, y^r). \quad (1)$$

Since the coordinates of e are all 0's we have the special relations

$$f^i(x, e) = f^i(x^1, \dots, x^r; 0, \dots, 0) = x^i, \quad (2)$$

$$f^i(e, y) = f^i(0, \dots, 0; y^1, \dots, y^r) = y^i. \quad (3)$$

Since the function f^i are three times continuously differentiable they can be expanded in Taylor series up to terms of degree three. Moreover, because of (2) and (3), these expansions assume a somewhat special form; indeed it may readily be verified that

$$f^i = x^i + y^i + a_{jk}{}^i x^j y^k + g_{jkl}{}^i x^j x^k y^l + h_{jkl}{}^i x^j y^k y^l + \epsilon_1{}^i, \quad (4)$$

where $\epsilon_1{}^i$ is small of degree four with respect to the coordinates of x and y . The numbers

$$c_{jk}{}^i = a_{jk}{}^i - a_{kj}{}^i \quad (5)$$

are called the structure constants of G in the coordinate system D. The structure constants clearly satisfy

$$c_{jk}{}^i = -c_{kj}{}^i \quad (6)$$

Clearly the structure constants can be determined with the help of two times differentiable coordinates.

Relation (4) shows that any Lie group is, in the first approximation, commutative and isomorphic with a vector group, and that the departure from commutativity first appears in the second degree approximation. It is not difficult to show that even if G is commutative there may exist coordinate systems in which the second degree terms in (4) do not vanish. However, in the case of a commutative group we clearly have $a_{jk}{}^i = a_{kj}{}^i$, so that the structure constants all vanish. This fact constitutes the first hint of the great importance of the structure constants. Later it will be seen that, in fact, they determine the local structure of the group completely; it is this that justifies their name.

We now give an alternative definition of the structure constants which sheds further light on their role.

C) Let x and y be elements of G and consider the commutator $q(x, y)$ (see Section 4, C))

$$q = xyx^{-1}y^{-1} = q(x, y). \quad (7)$$

It turns out that in coordinate form (7) assumes the form

$$q^i = c_{jk}{}^i x^j y^k + \epsilon_2{}^i \quad (8)$$

where $\epsilon_2{}^i$ is small of degree three with respect to the coordinates of x and y . Thus (8) may also be used to define the structure constants and it shows that the constants form a tensor. Note that according to (4), (5) and (8) we have

$$q^i(x, y) = f^i(x, y) - f^i(y, x) + \epsilon_3{}^i \quad (9)$$

where $\epsilon_3{}^i$ is small of degree three.

In order to verify (8) we first use (4) to obtain a second degree approximation to the coordinates of the element z' inverse

to z . A straightforward computation shows that if $zz' = e$ then

$$z'^i = -z^i + a_{jk}{}^i z^j z^k + \epsilon_4{}^i \quad (10)$$

Now letting $z^* = xy$ and $z = yx$, we have $q = z^* z'$, and consequently, employing (4) once again along with (5) and (10), we obtain

$$\begin{aligned} q^i &= (x^i + y^i + a_{jk}{}^i x^j y^k) + (-x^i - y^i - a_{kj}{}^i x^j y^k \\ &\quad + a_{jk}{}^i (x^j + y^j)(x^k + y^k)) - a_{jk}{}^i (x^j + y^j)(x^k + y^k) + \epsilon_2{}^i \\ &= c_{jk}{}^i x^j y^k + \epsilon_2{}^i. \end{aligned}$$

Thus (8) is verified.

Theorem 81: The structure constants of any Lie group G satisfy the following relations:

$$c_{ij}{}^p = -c_{ji}{}^p, \quad (11)$$

$$c_{is}{}^p c_{jk}{}^s + c_{js}{}^p c_{ki}{}^s + c_{ks}{}^p c_{ij}{}^s = 0. \quad (12)$$

(Identity (12), sometimes known as the Jacobi identity, is intimately connected with the associativity of G . This is proved with the help of three times differentiable coordinates.)

Proof: Relation (11) has already been proved (see (6)). In order to prove (12) it suffices to express in coordinate form the associative law for multiplication in G . We let

$$u = yz, \quad v = xy, \quad w = xu, \quad w' = vz$$

and write out the coordinate expression of the equation $w = w'$. Employing (4), and carrying out all computations to terms of the third degree, we obtain

$$\begin{aligned} w^p &= x^p + (y^p + z^p + a_{jk}{}^p y^j z^k + g_{ijk}{}^p y^i y^j z^k + h_{ijk}{}^p y^i z^j z^k) \\ &\quad + a_{is}{}^p x^i (y^s + z^s + a_{jk}{}^s y^j z^k) + g_{ijk}{}^p x^i x^j (y^k + z^k) \\ &\quad + h_{ijk}{}^p x^i (y^j + z^j) (y^k + z^k) + \epsilon_5{}^p, \\ w'^p &= (x^p + y^p + a_{ij}{}^p x^i y^j + g_{ijk}{}^p x^i x^j y^k + h_{ijk}{}^p x^i y^j y^k) + z^p \\ &\quad + a_{sk}{}^p (x^s + y^s + a_{ij}{}^s x^i y^j) z^k + g_{ijk}{}^p (x^i + y^i) (x^j + y^j) z^k \\ &\quad + h_{ijk}{}^p (x^i + y^i) z^j z^k + \epsilon_6{}^p, \end{aligned}$$

where ϵ_5^p and ϵ_6^p are small of degree four.

Comparison of the first degree terms in these expressions for w^p and w'^p yields

$$x^p + (y^p + z^p) = (x^p + y^p) + z^p,$$

while comparison of the second degree terms yields

$$a_{jk}^p y^j z^k + a_{is}^p x^i y^s + a_{ls}^p x^i z^s = a_{ij}^p x^i y^j + a_{sk}^p x^s z^k + a_{sk}^p y^s z^k.$$

These equations hold identically, independently of the associativity of the group multiplication.

We turn now to the comparison of terms of degree three, limiting our attention to those terms that actually depend on all three of the points, x , y and z , since the sums of such terms must be equal among themselves. (The remaining terms of degree three turn out to be identically equal anyway, so that the comparison of their coefficients would lead to no new relations.) In this way we obtain

$$\begin{aligned} a_{is}^p x^i a_{jk}^s y^j z^k + h_{ijk}^p x^i (y^j z^k + y^k z^j) &= a_{sk}^p a_{ij}^s x^i y^j z^k \\ &+ g_{ijk}^p (x^i y^j + x^j y^i) z^k, \end{aligned}$$

whence comparison of coefficients leads to

$$a_{is}^p a_{jk}^s - a_{sk}^p a_{ij}^s = -h_{ijk}^p - h_{ikj}^p + g_{ijk}^p + g_{jik}^p. \quad (13)$$

Now permuting the subscripts i , j , k gives rise to five other identities of the same form as (13). If each of these six identities is multiplied by $+1$ or -1 , according as the permutation that produces it is even or odd, and the six are then added together, the relation thus obtained has zero for its right member and, for its left member, a sum of twelve terms. On the other hand, if we replace each structure constant in (12) by its expression (5), we also obtain a relation having a sum of twelve terms for its left member and zero for its right member. Finally, from the general character of the terms involved it is not hard to see that these two equations coincide. Thus (12) is a consequence of (13) and (5), and the proof of Theorem 81 is complete.

We turn now to the construction of the Lie algebra.

Definition 48: Let R be an r -dimensional vector space over a field K (in the sequel K will always be either the field of real numbers or the field of complex numbers) in which there is defined

a law of composition for vectors, so that to each pair of vectors a and b there corresponds a vector $c = [a, b]$, called the commutator or bracket product of a and b , in such a way that the following conditions are satisfied:

$$[\alpha a + \alpha' a', b] = \alpha[a, b] + \alpha'[a', b] \quad (14)$$

and $[a, b] + [b, a] = 0 \quad (15)$

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0. \quad (16)$$

(Here α, α' denote elements of K . Relation (16) will be referred to in the sequel as the Jacobi identity.) A vector space R in which such a bracket product is defined is a Lie algebra over K . (If K is the field of real numbers then R is a real Lie algebra; if K is the field of complex numbers then R is a complex Lie algebra. The Lie algebra of a Lie group (see Theorem 82) is always real and we shall refer to it simply as the Lie algebra.) If $[a, b] = 0$ for every pair of vectors $a, b \in R$ then R is said to be commutative.

From the linearity (14) and property (15) it follows that commutators may be expressed in terms of a coordinate system in the form

$$c^i = [a, b]^i = {}^*c_{jk}{}^i a^j b^k. \quad (17)$$

The scalars ${}^*c_{jk}{}^i$ are called the structure constants of R in the given coordinate system. From (15) and (16) it follows that the structure constants satisfy the following identities:

$${}^*c_{jk}{}^i = - {}^*c_{kj}{}^i, \quad (18)$$

$${}^*c_{is}{}^p {}^*c_{jk}{}^s + {}^*c_{js}{}^p {}^*c_{ki}{}^s + {}^*c_{ks}{}^p {}^*c_{ij}{}^s = 0. \quad (19)$$

On the other hand, straightforward computation shows that if R is a vector space over K , and if ${}^*c_{jk}{}^i$ is a system of scalars satisfying (18) and (19), then (17) may be used to define a bracket product in R which turns it into a Lie algebra. Thus the study of systems of structure constants ${}^*c_{jk}{}^i$ satisfying (18) and (19) is equivalent with the study of Lie algebras.

Theorem 82: Let G be an r -dimensional local Lie group. By C) Section 41 there corresponds to each differentiable arc in G a tangent vector a and the correspondence thus established associates with G an r -dimensional vector space R . Let a and b be any two vectors in R , let $x(t)$ and $y(t)$ be arcs having a and

b respectively, as their tangent vectors, and let

$$q(t) = x(t) y(t) (x(t))^{-1} (y(t))^{-1}. \quad (20)$$

Then $q(t)$ is again an arc in G . We introduce on q a new parameter s by writing $t = \sqrt{s}$. The arc $q(\sqrt{s})$ thus obtained is defined for non-negative values of the parameter s and has a tangent vector c which depends only on the vectors a and b . We define the commutator $[a, b]$ by writing $[a, b] = c$. The bracket product thus defined in R satisfies conditions (14), (15), and (16) so that R is turned into a Lie algebra. The (real) Lie algebra R thus obtained is called the Lie algebra of the Lie group G : $G \rightarrow R$. The structure constants of G and those of R coincide in corresponding coordinate systems (see Definitions 47 and 48).

Proof: We have but to fix a coordinate system in G and compute the coordinates of the vector c . Because of the choice of the pa-

rameter s it is easily seen that $c = \lim_{t \rightarrow 0} \frac{q^i(t)}{t^2}$. But then, substi-
tuting from (8), we obtain

$$c^i = \lim_{t \rightarrow 0} \frac{1}{t^2} (c_{jk}^i x^j(t) y^k(t) + \epsilon_7^i(t)) = c_{jk}^i a^j b^k$$

since the remainder $\epsilon_7^i(t)$ is small of degree three with respect to t . Thus

$$c^i = [a, b]^i = c_{jk}^i a^j b^k.$$

In other words, the structure constants of the bracket product defined in R coincide with those of the Lie group G . Since the structure constants of G are known to satisfy (11), (12) it follows, as has been observed, that the bracket product in R satisfies (14), (15) and (16), and R is a Lie algebra. Thus the theorem is proved. (That the vector c is uniquely determined by a and b is clear from the fact that its coordinates are expressible in terms of the coordinates of a and b and the structure constants.)

D) For the purpose of computing commutators the following characterization is frequently preferable. Let

$$q^i(x, y) = q^i(x^1, \dots, x^r; y^1, \dots, y^r)$$

denote the sum of the terms of order two in the expansion of the

difference $f^i(x, y) - f^i(y, x)$ (see (1)). Then $c = [a, b]$ has the coordinate expression

$$c^i = \dot{q}^i(a^1, \dots, a^r; b^1, \dots, b^r). \quad (21)$$

The validity of this assertion is an immediate consequence of (9).

The significance of the Lie algebra lies in the fact that to each (real) Lie algebra there corresponds a uniquely determined local Lie group. It is to the proof of this fundamental result that the following sections are devoted. The question of whether an arbitrary real Lie algebra is the Lie algebra of a global Lie group is more difficult, but it too possesses an affirmative answer. In this latter case, of course, there is no question of the uniqueness of the corresponding group. One and the same Lie algebra R may belong to several non-isomorphic global groups, but these groups must all be locally isomorphic and the question of how they are related to one another is answered by the results of Chapter 9.

Example 93: Let R be a three-dimensional vector space in which the usual vector product is defined, and let $[a, b]$ denote the product of the vectors a and b . If we take $[a, b]$ as the commutator of a and b then, according to the familiar rules of vector calculus, the conditions of Definition 48 are all satisfied and R becomes a Lie algebra.

We shall show that R is in fact the Lie algebra of the group G of quaternions of modulus one. Since G is locally isomorphic with the group H_3 of rotations of a three dimensional Euclidean space it follows that R is also the Lie algebra of H_3 (see Example 89).

If $x \in G$ is sufficiently close to 1 we may write

$$x = 1 + \frac{x'}{\sqrt{2}} + \epsilon,$$

where x' is a pure imaginary quaternion, the components of which we take as the coordinates of x , while ϵ is a real quaternion, small of degree two with respect to the components of x' . According to D) we may compute the commutator of two quaternions x and y , both of which are sufficiently close to 1, by computing $xy - yx$ and then discarding all terms that are small of degree three. But now

$$\begin{aligned} xy - yx &= (1 + \frac{x'}{\sqrt{2}} + \epsilon_1)(1 + \frac{y'}{\sqrt{2}} + \epsilon_2) \\ &\quad - (1 + \frac{y'}{\sqrt{2}} + \epsilon_2)(1 + \frac{x'}{\sqrt{2}} + \epsilon_1) = \frac{x'y' - y'x'}{2} + \epsilon_3 \\ &= \frac{-(x', y') + [x', y'] + (y', x') - [y', x']}{2} + \epsilon_3 = [x', y'] + \epsilon_3, \end{aligned}$$

where (x', y') and $[x', y']$ denote, respectively, the scalar and vector products in the space of J of pure imaginary quaternions (see Example 47).

SECTION 53

SUBALGEBRA. FACTOR ALGEBRA. HOMOMORPHISM

In the preceding section there was associated with each Lie group G its Lie algebra R . Here we introduce the algebraic concepts corresponding to those of subgroup, normal subgroup, factor group, and homomorphism of the group G .

A) Let R be a Lie algebra over a field K . A subset S of R is said to be a subalgebra of R if the following two conditions are satisfied: a) S is a subspace of R , i.e., along with every pair of vectors a and b in S the vector $\alpha a + \beta b$ also belongs to S where α and β denote arbitrary elements of K ; b) if a and b are vectors belonging to S then the commutator $[a, b]$ also belongs to S . Clearly any one-dimensional subspace is a subalgebra. A subalgebra S of a Lie algebra R is said to be an ideal if c) $[a, b] \in S$ for all $a \in R$, $b \in S$. R is said to be simple if it has no ideals other than R and $\{0\}$. An ideal S is central if d) $[a, b] = 0$ for all $a \in R$, $b \in S$. The set of all elements $b \in R$ such that $[a, b] = 0$ for every $a \in R$ is clearly the maximal central ideal in R and will be called its center.

The terminology just introduced is justified by the following:

Theorem 83: Let G be a local Lie group, let R be its Lie algebra, and let H be an arbitrary subgroup of G . Denote by S the set of all vectors that are tangent to arcs lying in H . Then S is a subalgebra of R and is also the Lie algebra of H . We shall say that S corresponds to H : $H \rightarrow S$. If H is a normal subgroup then S is an ideal. If H is a central normal subgroup then S is a central ideal.

Proof: According to Theorem 62, H is a differentiable submanifold of the manifold G ; thus S is a subspace of R and condition a) of definition A) is satisfied. It remains to verify condition b). Let $a, b \in S$, and let $x(t)$ and $y(t)$ be arcs in H having a and b as their tangent vectors. In order to obtain $c = [a, b]$ we consider the arc $q(t) = x(t)y(t)(x(t))^{-1}(y(t))^{-1}$. This arc clearly lies in H since H is a subgroup. But then the arc $q(\sqrt{s})$ is also in H and consequently c , being the tangent vector of $q(\sqrt{s})$, belongs to S so that $[a, b] \in S$.

We suppose next that H is a normal subgroup and verify condition c) of the above definition. Let $a \in R$, $b \in S$. Let $x(t)$ be an arbitrary arc in G with tangent vector a and let $y(t)$ be an arc in H with tangent vector b . Since H is normal the arc $x(t)y(t)(x(t))^{-1}$ belongs to H whence it follows that $q(t) = x(t)y(t)(x(t))^{-1}(y(t))^{-1}$ also belongs to H . Consequently $q(\sqrt{s})$ is in H and its tangent vector $c = [a, b]$ belongs to S .

Finally we observe that if H is a central normal subgroup then the arc $q(t)$ is identically equal to e in some neighborhood of $t = 0$ so that in this case the tangent vector c is the zero vector.

B) Let R be a Lie algebra over a field K and let S be an ideal in R . We partition the vector group R into cosets modulo the subgroup S and observe that the collection R^* of cosets thus obtained forms a vector space over K . It is also possible to define a bracket product in R^* in a natural way. Indeed, let A and B be cosets, let $a \in A$, $b \in B$, and write $c = [a, b]$. We shall show that the coset C containing c depends only on A and B and not on the choice of a and b . To see this let $a' \in A$ be any other element of A and let $c' = [a', b]$. Then $c' - c = [a' - b] - [a, b] = [a' - a, b] \in S$ since S is an ideal. Thus $c' \in C$. Because of the skew-symmetry of commutators, this suffices to verify the desired independence. Accordingly, we define $[A, B] = C$. Since conditions (14), (15), (16), Section 52 hold in R they continue to hold in R^* . Consequently R^* is a Lie algebra over K ; it will be called the factor algebra of R modulo the ideal S , and will be denoted by $R^* = R/S$.

C) Let R and R' be two Lie algebras over the same field K and let g be a mapping of R into R' . Then g is a homomorphism if the following conditions are satisfied:

a) g is a linear transformation, i.e., for arbitrary scalars $\alpha, \beta \in K$ we have:

$$g(\alpha a + \beta b) = \alpha g(a) + \beta g(b) \text{ for } a, b \in R;$$

$$b) g([a, b]) = [g(a), g(b)] \text{ for } a, b \in R.$$

The set S of those elements of R carried into zero by g is its kernel. The homomorphism is said to be an isomorphism if it is one-to-one and onto. If there exists an isomorphism of one Lie algebra onto another then the algebras are said to be isomorphic. An isomorphism of a Lie algebra onto itself is an automorphism.

D) Let R and R' be Lie algebras over the same field K , let

g be a homomorphism of R onto R' and let S be the kernel of G . Then S is an ideal in R and the factor algebra R/S is isomorphic with R' under the homomorphism naturally associated with g .

That S is a subspace is a consequence of the fact that g is a linear transformation. Let $a \in R$, $b \in S$. Then

$$g([a, b]) = [g(a), g(b)] = [g(a), 0] = 0.$$

Thus $[a, b] \in S$, i.e., S is an ideal in R .

Now let a' be an arbitrary element of R' and denote by A the set of all elements in R mapped into a' by g . Since g is a homomorphism of the vector group R onto the vector group R' it follows that A is a coset of S so that the homomorphism naturally associated with g gives a one-to-one mapping of R/S onto R' . The proof that this mapping is an isomorphism is trivial.

The following theorem serves to justify the terminology just introduced.

Theorem 84: Let G and G' be local Lie groups and let f be a local homomorphism of G into G' . Denote by R and R' the Lie algebras of G and G' , respectively, let $a \in R$, and let $x(t)$ be an arc in G having tangent vector a . Then $f(x(t))$ is an arc in G' , the tangent vector of which we denote by a' . It turns out that a' is uniquely determined by a , i.e., does not depend on the choice of the arc $x(t)$ (assuming of course that its tangent vector is a) so that we may define $a' = g(a)$. The mapping g thus obtained is a homomorphism R into R' . Thus with every homomorphism f of G into G' there is associated in a natural way a homomorphism g of R into R' . We shall say that g corresponds to f : $f \rightarrow g$. If f is onto then so is g . Denote by N the kernel of f and by S the kernel of g . Then the ideal S corresponds to the subgroup N , $N \rightarrow S$. Accordingly, if f is an isomorphism then g is an isomorphism too.

Proof: Since $f(G)$ is a subgroup of G'^* it is no loss of generality to assume that f is a homomorphism of G onto the entire group $G' = f(G)$. By virtue of Theorem 63 the mapping f has a coordinate expression in terms of differentiable functions. From this it follows readily that g is well defined and is, moreover, a linear transformation of R onto R' . Let now $x(t)$ and $y(t)$ be arcs in G , let a and b be their tangent vectors, and define

* See footnote, p. 139. Trans.

$$q(t) = x(t)y(t)(x(t))^{-1}(y(t))^{-1}.$$

Then $c = [a, b]$ is the tangent vector of the arc $q(\sqrt{s})$ (see Theorem 82), while $a' = g(a)$ and $b' = g(b)$ are the tangent vectors of the arcs $x'(t) = f(x(t))$ and $y'(t) = f(y(t))$. In order to obtain the commutator $c' = [a', b']$ we introduce the arc

$$q'(t) = x'(t)y'(t)(x'(t))^{-1}(y'(t))^{-1}.$$

Since f is homomorphic we have $q'(\sqrt{s}) = f(q(\sqrt{s}))$. Thus $g(c) = c'$, and it follows that g is a homomorphism.

Denote by S' the ideal in R corresponding to the subgroup N (see Theorem 83). Since every arc lying in N is carried by f into the point e' we clearly have $S' \subset S$. But then $S' = S$ since, considered as subspaces, S and S' have the same dimension. Thus the proof of Theorem 84 is complete.

E) Let G, G', G'' be local Lie groups, let R, R', R'' be their Lie algebras, and suppose given local homomorphisms f' and f'' of G into G' and of G' into G'' , respectively. Denote also by g' and g'' the corresponding homomorphisms of the Lie algebras: $f' \rightarrow g', f'' \rightarrow g''$. Then the homomorphism corresponding to the product $f = f''f'$ is the product $g = g''g'$.

The proof follows from the very definition of the correspondence given in Theorem 84. If $x(t)$ is an arc in G with tangent vector a then $f'(x(t))$ has tangent vector $g'(a)$ and consequently $f''(f'(x(t)))$ has tangent vector $g''(g'(a))$. In other words $f(x(t))$ has the tangent vector $g(a)$ so that $f \rightarrow g$.

F) A Lie algebra R is said to resolve into the direct sum of two of its subalgebras S and T if the linear space R resolves into the direct sum of the subspaces S and T , and if, moreover, both S and T are ideals in R . Thus, if R resolves into the direct sum of the subalgebras S and T then every element $x \in R$ may be written uniquely in the form $x = y + z$ where $y \in S$, $z \in T$, and if $b \in S$, $c \in T$ then $[a, c] = 0$. This shows how to reconstitute the original algebra in R , given the subalgebras S and T . We simply define the direct sum R of two given Lie algebras S and T to be the collection of all pairs (y, z) , $y \in S$, $z \in T$, with the linear operations in R defined as in the direct sum of the vector spaces S and T , and the bracket product defined by the formula $[(y_1, z_1), (y_2, z_2)] = ([y_1, y_2], [z_1, z_2])$. If the local Lie group G resolves into the direct product of two normal subgroups H and K and if $G \rightarrow R$, $H \rightarrow S$, $K \rightarrow T$, then the Lie algebra R resolves into the direct

sum of the subalgebras S and T. The verification of this connection between direct products of local Lie groups and direct sums of their corresponding Lie algebras is automatic. Moreover, the definitions and the theorem extend immediately to an arbitrary finite number of direct factors, and direct summands, respectively.

Theorems 83, and 84 and Proposition F) show that to every concept or relation bearing on Lie groups there corresponds, in a natural and unique fashion, a concept or relation bearing on the associated Lie algebras. In the following paragraphs we turn attention to the more difficult problem of going in the reverse direction, from Lie algebra to Lie group.

Example 94: We continue the investigation begun in Example 93. It is not difficult to show that the Lie algebra R of Example 93 possesses no subalgebras other than the one-dimensional subalgebras, while every one-dimensional subspace of R is, of course, a subalgebra. Suppose, in fact, that R possessed a two-dimensional subalgebra S. Then S would contain two linearly independent vectors a and b , whence it would follow that $c = [a, b]$, being the vector product of a and b , would have to be distinct from 0 and perpendicular to the plane S. But then of course $c \in S$. In exactly the same fashion one verifies easily that R is simple.

SECTION 54

LINEAR GROUPS. AUTOMORPHISMS OF LIE ALGEBRAS

In the preceding paragraph it was shown that an automorphism of the Lie algebra corresponds to each automorphism of a Lie group. We here undertake a detailed investigation of the automorphisms of a Lie algebra. In the first place, we shall examine the automorphism group of a Lie algebra; this group turns out to be a Lie group in its own right, and we construct its Lie algebra. Moreover, we shall examine the adjoint group of a Lie algebra, i.e., the group corresponding to the group of inner automorphisms of the Lie group, and construct the Lie algebra of the adjoint group. In both cases the analysis begins with the description of the corresponding Lie algebras. Inasmuch as automorphisms of Lie algebras are, in particular, linear automorphisms, we first investigate linear Lie groups. The contents of the present paragraph are intended primarily for use in Chapter 11; the only parts needed in the present chapter are propositions B) and F).

Linear Lie groups or, what comes to the same thing, Lie groups of linear transformations, play an important role in the

theory of Lie groups generally. The Lie algebra of a linear Lie group is itself composed of linear transformations and is called a linear Lie algebra. We begin with the definition of a linear Lie algebra since this much of the theory makes sense over an arbitrary field.

A) Let A be a vector space over a field K and let R be any set of linear transformations of A into itself that contains, along with each pair of transformations a and b , both the transformation $ab - ba$, and all linear combinations $\alpha a + \beta b$ where α, β denote arbitrary elements of K . Then R is automatically a vector space over K . We define a bracket product in R by writing

$$[a, b] = ab - ba . \quad (1)$$

With this definition R becomes a Lie algebra. Such a Lie algebra is called a linear Lie algebra.

Conditions (14) and (15) of Section 52 are clearly satisfied by the bracket product thus defined in R and it suffices to verify the Jacobi identity (16). Let a, b, c be any three transformations belonging to R . Then

$$[a, [b, c]] = a[b, c] - [b, c]a = abc - acb - bca + cba .$$

Permuting a, b, c cyclically in this expression, we obtain two other similar expressions; and the sum of these three identities is easily seen to be (16).

B) Let A be a real or complex vector space, and let G be any set of linear automorphisms of A which, with respect to the natural topology constitutes a local Lie group of linear transformations. Such a local Lie group G is said to be linear. Let $x(t)$ be an arc in G which passes through the identity matrix e at $t = 0$: $x(0) = e$. Since the set of linear transformations of A into itself forms a real vector space, it makes sense to define the derivative of the linear transformation valued function $x(t)$ at $t = 0$:

$$a = \lim_{t \rightarrow 0} \frac{x(t) - x(0)}{t} . \quad (2)$$

This derivative, assuming it exists, is again a linear transformation on A ; we shall say that it is tangent to $x(t)$. It turns out that the set of all linear transformations on A that are tangent

to arcs lying in G constitutes a real linear Lie algebra R in the sense of A) and, moreover, that this algebra is, in a natural way, isomorphic with the Lie algebra of G . Indeed, the arc $x(t)$ possesses a tangent a when and only when it possesses a tangent vector a' when considered as an arc in the local group G (see Section 41, C)) and the correspondence $a = a'$, which does not depend on the choice of $x(t)$, yields the desired natural isomorphism. In view of this we may regard the linear Lie algebra R as the Lie algebra of G . Moreover, if $x(t)$ is a one-parameter subgroup of G having the tangent transformation a , then $x(t)$ satisfies the differential equation

$$\frac{dx(t)}{dt} = ax(t) . \quad (3)$$

From this it follows, in particular, that a local linear Lie group G is uniquely determined by its Lie algebra R . More precisely, if two local linear Lie groups G_1 and G_2 of linear automorphisms of the vector space A have the same linear Lie algebra R , then they coincide in some neighborhood of the identity matrix.

In order to prove B) we first coordinatize the topological group G^* of all linear automorphisms of A (see Example 76). Select a basis in A and write the matrix corresponding to a given transformation $x \in G^*$ in the form $\|\delta_j^i + x_j^i\|$. If A is real we take as coordinates of x the entries x_j^i ; if, on the other hand, A is complex then we take as coordinates of x the real and imaginary parts of the entries x_j^i . In this coordinate system the product $z = xy$ assumes the coordinate form

$$z_j^i = (\delta_\alpha^i + x_\alpha^i)(\delta_j^\alpha + y_j^\alpha) - \delta_j^i = x_j^i + y_j^i + x_\alpha^i y_j^\alpha . \quad (4)$$

Thus G^* is an analytic Lie group. If $x(t)$ is an arc in G^* , and if $x_j^i = x_j^i(t)$ is its coordinate expression, then the coordinates a_j^i of the vector a tangent to $x(t)$ are, by definition (see Section 41, C)), given by the formula

$$a_j^i = \frac{dx_j^i(0)}{dt} . \quad (5)$$

But (5) is just the matrix form of (2). Thus the Lie algebra R^* of G^* consists of the set of all linear transformations of A into itself. In order to compute the bracket product we employ Section 52, D)). Let $z^* = yx$. Then

$$z_j^{*i} = y_j^i + x_j^i + y_\alpha^i x_j^\alpha . \quad (6)$$

Subtracting (6) from (4) we obtain

$$q_j^i = z_j^i - z_j^{*i} = x_\alpha^i y_j - y_\alpha^i x_j^\alpha$$

whence, returning once more to the notation of linear transformations, we have

$$[a, b] = ab - ba . \quad (7)$$

In other words, the Lie algebra R^* of the full linear group G^* is the linear Lie algebra consisting of the set of all linear transformations A into itself. But then if G is a local subgroup of G^* the collection of all transformations tangent to arcs in G constitutes the Lie algebra R of G and is a subalgebra of R^* (see Theorem 83). Finally if $x(t)$ is a one-parameter subgroup of G with direction vector (transformation) a then

$$x(s+t) = x(s)x(t) ;$$

whence, differentiating with respect to s and evaluating at $s = 0$, we obtain (3).

We turn now to the consideration of certain linear Lie groups of automorphisms of a Lie algebra; once again we commence our analysis with the corresponding Lie algebras.

C) Let R be a Lie algebra over an arbitrary field K . We denote by R_A the collection of those linear transformations a of the vector space R into itself which satisfy the condition

$$a([u, v]) = [a(u), v] + [u, a(v)] ; \quad u \in R, \quad v \in R . \quad (8)$$

Clearly, if a and b belong to R_A then so does $\alpha a + \beta b$ where α, β denote elements of K . It turns out that the commutator $[a, b] = ab - ba$ also belongs to R_A so that R_A is a linear Lie algebra over K . The algebra R_A is called the algebra of differentiations of R .

We must show that $c = ab - ba \in R_A$. Applying the transformation b to (8) we obtain

$$ba([u, v]) = [ba(u), v] + [a(u), b(v)] + [b(u), a(v)] + [u, ba(v)] . \quad (9)$$

Analogously

$$ab([u, v]) = [ab(u), v] + [b(u), a(v)] + [a(u), b(v)] + [u, ab(v)]. \quad (10)$$

But then, subtracting (9) from (10) one obtains

$$c([u, v]) = [c(u), v] + [u, c(v)].$$

D) Let R be a real Lie algebra and denote by G_A the group of all automorphisms of R . It is clear that G_A is a subgroup of the group of all linear automorphisms of the vector space R , and hence that G_A is a linear Lie group (see B)). It turns out that the Lie algebra of G_A is precisely the algebra R_A of derivations of R .

In order to prove D) it suffices to show that a one-parameter subgroup $x(t) = x_t$ of linear automorphisms of the linear space R belongs to G_A when and only when the direction transformation a of the subgroup satisfies (8). Suppose first that $x_t \in G_A$. Then

$$x_t([u, v]) = [x_t(u), x_t(v)] \quad (11)$$

and, differentiating this relation at $t = 0$, we obtain (8). Suppose, on the other hand, that a satisfies (8). Let $u(t) = x_t(u)$, $v(t) = x_t(v)$, and let $w(t) = [u(t), v(t)] - x_t([u, v])$. Employing (3) and (8) we obtain the following relation:

$$\begin{aligned} \frac{dw(t)}{dt} &= [a(u(t)), v(t)] + [u(t), a(v(t))] - ax_t([u, v]) = \\ &= [a(u(t)), v(t)] + [u(t), a(v(t))] - a([u(t), v(t)]) \\ &\quad + a([u(t), v(t)]) - ax_t([u, v]) = a[u(t), v(t)] - ax_t([u, v]) \\ &= a(w(t)), \end{aligned}$$

Thus if a satisfies (8) then $w(t)$ satisfies

$$\frac{dw(t)}{dt} = a(w(t)). \quad (12)$$

But this says that the coordinates of $w(t)$ satisfy a system of linear differential equations with constant coefficients and since $w(0) = 0$ it follows that $w(t) = 0$. Thus $x_t \in G$.

E) Let R be a Lie algebra over an arbitrary field K . With each element $a \in R$ we associate a linear transformation p_a of the linear space R into itself by writing

$$p_a(u) = [a, u], \quad u \in R. \quad (13)$$

The set P of all linear transformations of the form p_a , $a \in R$, is a linear Lie algebra and an ideal in the Lie algebra R_A of all derivations. The algebra P is called the adjoint algebra of R or the algebra of inner derivations. The mapping g defined by $g(a) = p_a$ is a homomorphism of R onto P . Clearly the kernel of g is just the center of R . Finally, if $q \in R_A$, $a \in R$, and if φ is an arbitrary automorphism of R then

$$p_{q(a)} = [q, p_a], \quad (14)$$

$$p_{\varphi(a)} = \varphi p_a \varphi^{-1}. \quad (15)$$

The proof of the first part of E) consists of a straightforward computation based on the Jacobi identity (16) Section 52. In the first place

$$\begin{aligned} p_a([u, v]) &= [a, [u, v]] = [[a, u], v] + [u, [a, v]] \\ &= [p_a(u), v] + [u, p_a(v)]. \end{aligned}$$

Thus $p_a \in R_A$. Similarly, if a, b denote any two elements of R , then

$$\begin{aligned} p_{[a,b]}(u) &= [[a, b], u] = [a, [b, u]] - [b, [a, u]] \\ &= p_a p_b(u) - p_b p_a(u) = [p_a, p_b](u). \end{aligned}$$

Thus P is a linear Lie algebra and g is a homomorphism of R onto P .

In order to show that P is an ideal in R_A it suffices to verify (14). Let $r = [q, p_a]$. Then $r = qp_a - p_a q$ and, applying r to an arbitrary vector $u \in R$, we obtain (see (8)):

$$\begin{aligned} r(u) &= q([a, u]) - [a, q(u)] = [q(a), u] + [a, q(u)] \\ &\quad - [a, q(u)] = p_{q(a)}(u). \end{aligned}$$

Thus (14) holds.

It remains only to verify (15). Since φ is an automorphism of R we have

$$[\varphi(a), \varphi(u)] = \varphi([a, u]),$$

or, in other words,

$$p_{\varphi(a)}(\varphi(u)) = \varphi p_a(u).$$

Since this holds for every vector $u \in R$ we obtain $p_{\varphi(a)} \circ \varphi = \varphi \circ p_a$, or, equivalently, $p_{\varphi(a)} = \varphi p_a \varphi^{-1}$.

F) Let G be a local Lie group and let R be its Lie algebra. With each element $x \in G$ we associate the inner automorphism φ_x defined by

$$\varphi_x(z) = zxz^{-1}, \quad z \in G. \quad (16)$$

By Theorem 84 there corresponds to φ_x an automorphism l_x of the Lie algebra R . The mapping f defined by $f(x) = l_x$ is a homomorphism of G onto a locally linear Lie group L of automorphisms of R . This group L is called the adjoint group of G (or of R). The kernel of f is clearly the center of G . It turns out that the Lie algebra of the adjoint group L is precisely the adjoint algebra P of the Lie algebra R , and that the Lie algebra homomorphism corresponding to f is the homomorphism $a \rightarrow p_a$ (see E)).

The proof of F) consists in the explicit computation of the homomorphism g corresponding to f .† Let $a, u \in R$, $p = g(a)$. Then p is defined by the formula

$$p(u) = \frac{d}{ds} l_{x(s)}(u),$$

where $x(s)$ denotes an arc in G with direction vector a . (Here

† The argument would seem to require a prior verification of the continuity of f . Let $u \in R$, $x \in G$ and let $z(t)$ be a continuously differentiable arc with tangent vector u . If g^1, \dots, g^n denote the coordinates of $xz(t)x^{-1} = \varphi_x(z(t))$ then each g^i is a continuously differentiable function of x^1, \dots, x^n and t so that

$\frac{\partial g^i}{\partial t}|_{t=0}$ is a continuous function of x . But these derivatives are

the coordinates of $l_x(u)$. Thus $l_x(u) \rightarrow l_{x_0}(u)$ in R as $x \rightarrow x_0$ in G , and since this holds for every $u \in R$ it follows that f is continuous.

This also shows that L is, in fact, a local subgroup of the group of linear automorphisms of R ; see footnote, p. 139. Trans.

and below derivatives are understood to be taken at the origin.) But $l_{x(s)}(u)$ is the direction vector of $x(s)z(t)x(s)^{-1}$, considered as an arc with parameter t , where $z(t)$ denotes an arc with direction vector u . Thus in coordinate form

$$(p(u))^i = \frac{d}{ds} \left(\frac{d}{dt} (x(s)z(t)(x(s))^{-1})^i \right). \quad (17)$$

But now, assuming, as we may, that both $x(s)$ and $z(t)$ are sufficiently smooth, and employing Section 52, (4) and (8), we obtain

$$\begin{aligned} (x(s)z(t)(x(s))^{-1})^i &= [(x(s)z(t)(x(s))^{-1}(z(t))^{-1})z(t)]^i \\ &= c_{jk}{}^i x^j(s) z^k(t) + z^i(t) + \varepsilon, \end{aligned}$$

where ε is small of degree three with respect to s, t . Thus the differentiations indicated in (17) yield

$$(p(u))^i = c_{jk}{}^i a^j u^k = [a, u]^i,$$

which shows that $p(u) = [a, u] = p_a(u)$, and the proof is complete.

On the basis of the results already obtained we formulate the following uniqueness theorem, a more general version of which will be proved later (see Theorem 89).

G) If two local Lie groups G_1 and G_2 have the same Lie algebra R , and if R has no center, then G_1 and G_2 are locally isomorphic with one another. Moreover, there exists one and only one isomorphism between G_1 and G_2 to which corresponds the identity automorphism of R .

Since R has trivial center the same is true (locally) of the groups G_1 and G_2 (see Theorem 83). Thus the homomorphism f_i of G_i onto the adjoint group L_i , $i = 1, 2$, may be assumed to be an isomorphism. Moreover, since the Lie group L_i is uniquely determined (as a linear group, see B)) by its Lie algebra, and since the Lie algebra of L_i is just the adjoint algebra P of R , it follows that L_1 and L_2 coincide. But then $f_1^{-1}f_2$ is an isomorphism of G_2 onto G_1 to which corresponds the identity transformation of R onto itself. That there can be no other isomorphism of G_2 onto G_1 possessing this property may be seen as follows. A non-identical automorphism of G_1 is expressed, in a canonical coordinate system of the first kind, in the form of a non-identical linear automorphism; consequently, to a non-identical automorphism of G_1 there corresponds a non-identical automorphism of R .

Example 95: Let G^* denote the group of all linear automorphisms of an n -dimensional real or complex vector space A and let R^* be the linear Lie algebra of G^* . As has already been noted, the group G^* may be viewed as the group of all non-singular real or complex square matrices of order n , which we write in the form $\|\delta_j^i + x_j^i\|$. The Lie algebra R^* is then the algebra of all real or complex square matrices of order n . We single out two interesting subgroups of G^* and determine which subalgebras of R^* correspond to them. (It is instructive to compare this example with Example 79.)

Denote first by G the subgroup of G^* consisting of the unimodular transformations or, what comes to the same thing, the group of matrices with determinant +1. Since the determinant of $\|\delta_j^i + x_j^i\|$ is easily seen to be of the form $1 + x_i^i + \epsilon$, where ϵ is small of degree two with respect to the coordinates x_j^i , it follows that x belongs to G if and only if

$$x_i^i + \epsilon = 0. \quad (18)$$

But then, taking in G an arbitrary arc $x(t)$, i.e., supposing that $x_j^i = x_j^i(t)$, and differentiating (18), we obtain

$$a_i^i = 0. \quad (19)$$

Since the dimension of G and the dimension of the algebra consisting of the matrices that satisfy (19) are equal to one another, it follows that the subalgebra R corresponding to G consists precisely of the linear transformations with trace zero. Since G is a normal subgroup of G^* it follows that R is an ideal in R^* .

Next let H denote the subgroup of G^* consisting of all orthogonal matrices $\|\delta_j^i + x_j^i\|$. The condition of orthogonality has the form

$$x_j^i + x_i^j + \epsilon' = 0 \quad (20)$$

where ϵ' is also small of degree two with respect to the coordinates x_j^i . (Here i and j do not denote indices of summation.) Once again, taking in H an arc $x(t)$, i.e., assuming that $x_j^i = x_j^i(t)$, and differentiating (20), we obtain

$$a_j^i + a_i^j = 0. \quad (21)$$

Thus the subalgebra S corresponding to H consists exclusively of skew-symmetric matrices, and from a consideration of dimension

it follows as before that S consists precisely of all skew-symmetric matrices.

SECTION 55 INTEGRABILITY CONDITIONS

In the process of reconstructing a Lie group from its structure constants we shall require an elementary result from the theory of partial differential equations. We here state this result without proof and derive those corollaries that will be needed in the sequel.

Consider the system of differential equations

$$\frac{\partial f^i}{\partial x^j} = \varphi_j^i(f^1, \dots, f^n; x^1, \dots, x^r) = \varphi_j^i(f, x), \\ i = 1, \dots, n; \quad j = 1, \dots, r, \quad (1)$$

where f denotes a point with coordinates f^1, \dots, f^n ; x a point with coordinates x^1, \dots, x^r , and the functions $\varphi_j^i(f, x)$ are defined and have continuous first order partial derivatives in all arguments (analytic) for $f \in U$, $x \in V$, where U and V are open sets in the respective coordinate spaces. By a solution of (1) is meant a function $f(x)$ or, in coordinate form, a system of functions

$$f^i(x) = f^i(x^1, \dots, x^r), \quad i = 1, \dots, n,$$

satisfying (1) identically in the independent variables x^1, \dots, x^r on some portion of the set V . The problem we wish to investigate is that of finding a solution of (1) that satisfies a specified initial condition

$$f(x_0) = f_0, \quad (2)$$

where $x_0 \in V$, $f_0 \in U$. By a solution of the initial value problem (1, 2) is meant a function $f(x)$ that satisfies (2) and is defined and satisfies (1) identically in some neighborhood of x_0 . The main result in this context is the following theorem.

Theorem 85: A necessary condition in order that the initial value problem (1, 2) should possess a solution for arbitrary initial values $x_0 \in V$, $f_0 \in U$, is that the conditions

$$\begin{aligned} \frac{\partial \varphi_k^i(f, x)}{\partial f^\alpha} \varphi_j^\alpha(f, x) + \frac{\partial \varphi_k^i(f, x)}{\partial x^j} - \frac{\partial \varphi_j^i(f, x)}{\partial f^\alpha} \varphi_k^\alpha(f, x) \\ - \frac{\partial \varphi_j^i(f, x)}{\partial x^k} = 0 \end{aligned} \quad (3)$$

(known as the integrability conditions for the system (1)) should hold identically for $x \in V$, $f \in U$. Conversely, if (3) does hold for all $x \in V$, $f \in U$, then for arbitrary initial values $x_0 \in V$, $f_0 \in U$, there exists one and only one solution $f(x)$. In any event, and independently of the integrability conditions, it is impossible for (1) to have more than one solution satisfying a given initial condition.

We express explicitly the dependence of the solution $f(x)$ on the initial condition by writing $f(x) = f(x, f_0, x_0)$. Let \bar{U}' and \bar{V}' be open sets with compact closures \bar{U}' and \bar{V}' such that $\bar{U}' \subset U$, $\bar{V}' \subset V$. Then there exists a positive number ϵ so small that for all $f_0 \in \bar{U}'$, $x_0 \in \bar{V}'$ and $|x^i - x_0^i| < \epsilon$, $i = 1, \dots, r$, the solution $f(x, f_0, x_0)$ exists and has continuous second order partial derivatives in x^1, \dots, x^r , continuous first order partial derivatives in x_0^1, \dots, x_0^r and in f_0^1, \dots, f_0^r , and is analytic in all arguments if the right-hand sides of (1) are analytic.

I give here only the proof of the necessity of the condition. For a proof of sufficiency see [53].

Suppose $f(x)$ is a solution of the initial value problem (1, 2). Substituting $f(x)$ into (1), and differentiating the resulting identity, we obtain

$$\begin{aligned} \frac{\partial^2 f^i}{\partial x^j \partial x^k} = \frac{\partial \varphi_j^i(f, x)}{\partial f^\alpha} \cdot \frac{\partial f^\alpha}{\partial x^k} + \frac{\partial \varphi_j^i(f, x)}{\partial x^k} = \frac{\partial \varphi_j^i(f, x)}{\partial f^\alpha} \varphi_k^\alpha(f, x) \\ + \frac{\partial \varphi_j^i(f, x)}{\partial x^k}. \end{aligned} \quad (4)$$

But then, since $\frac{\partial^2 f^i}{\partial x^j \partial x^k} = \frac{\partial^2 f^i}{\partial x^k \partial x^j}$, it follows that (3) is satisfied for $f = f(x)$, and, in particular, for $x = x_0$, $f = f_0$. Thus if the initial values may be prescribed arbitrarily subject only to $x_0 \in V$, $f_0 \in U$, it follows that (3) must hold identically for $x \in U$, $f \in U$, and the necessity of (3) is verified.

† This last assertion contains a slight inaccuracy; simple examples show that one needs to exclude those derivatives involving three differentiations with respect to the coordinates of (f^0, x^0) . Trans.

The systems of differential equations that appear in the study of Lie groups do not present themselves explicitly in the form (1). Accordingly, we obtain a form of the integrability conditions better suited to the applications we shall need to make a Theorem 85.

A) Consider the system of differential equations

$$v_k^i(f) \frac{\partial f^k}{\partial x^j} = v_j^i(x), i = 1, \dots, r; j = 1, \dots, r, \quad (5)$$

where the functions $v_j^i(z) = v_j^i(z^1, \dots, z^r)$ are defined and have continuous first order partial derivatives in all arguments on some open set U and are such that the determinant of the matrix $\|v_j^i(z)\|$ does not vanish on U . The system (5) may easily be reduced to the form (1), and the integrability conditions for it have the form

$$\frac{\partial v_k^i(z)}{\partial z^j} - \frac{\partial v_j^i(z)}{\partial z^k} = \tilde{c}_{\alpha\beta}^i v_j^\alpha(z) v_k^\beta(z), \quad (6)$$

where \tilde{c}_{jk}^i are certain constants (depending on the system (5)). Note that (5) can be written in the following symmetric form:

$$v_j^i(f) df^j = v_j^i(x) dx^j, \quad i = 1, \dots, r, \quad (7)$$

where df^j denotes the total differential of the function $f^j(x)$ and dx^j the differential of the independent variable x^j .

In order to derive (6) we introduce the matrix $\|u_j^i(z)\|$ inverse to $\|v_j^i(z)\|$ which exists since $\|v_j^i(z)\|$ is, by hypothesis, non-singular throughout U . We have then

$$u^i(z) v_j(z) = v^i(z) u_j(z) = \delta_j^i, \quad (8)$$

where $\|\delta_j^i\|$ denotes the identity matrix. Differentiating (8), we obtain

$$v_\alpha^i(z) \frac{\partial u_j^\alpha(z)}{\partial z^k} + \frac{\partial v_\alpha^i(z)}{\partial z^k} u_j^\alpha(z) = 0 \quad (9)$$

Multiplying (5) by $u_i^p(f)$ and summing over i we obtain (after changing the names of the indices)

$$\frac{\partial f^i}{\partial x^j} = u_\beta^i(f) v_j^\beta(x). \quad (10)$$

This system is in form (1) so that Theorem 85 is applicable, and for it the integrability conditions read

$$\begin{aligned} & \frac{\partial u_\beta^i(f)}{\partial f^\alpha} u_\gamma^\alpha(f) v_j^\gamma(x) v_k^\beta(x) + u_\beta^i(f) \frac{\partial v_k^\beta(x)}{\partial x^j} \\ & - \frac{\partial u_\beta^i(f)}{\partial f^\alpha} u_\gamma^\alpha(f) v_k^\gamma(x) v_j^\beta(x) - u_\beta^i(f) \frac{\partial v_j^\beta(x)}{\partial x^k} = 0. \end{aligned} \quad (11)$$

Now, multiplying (11) by $v_i^p(f)$, summing over i , and employing (9) and (8), we obtain

$$\begin{aligned} & -\frac{\partial v_i^p(f)}{\partial f^\alpha} u_\beta^i(f) u_\gamma^\alpha(f) v_j^\gamma(x) v_k^\beta(x) + \frac{\partial v_k^p(x)}{\partial x^j} \\ & + \frac{\partial v_i^p(f)}{\partial f^\alpha} u_\beta^i(f) u_\gamma^\alpha(f) v_k^\gamma(x) v_j^\beta(x) - \frac{\partial v_j^p(x)}{\partial x^k} = 0. \end{aligned}$$

Next, multiplying by $u_s^j(x) u_t^k(x)$ and summing over both j and k , we obtain

$$\begin{aligned} & \left(\frac{\partial v_\beta^p(x)}{\partial x^\alpha} - \frac{\partial v_\alpha^p(x)}{\partial x^\beta} \right) u_s^\alpha(x) u_t^\beta(x) \\ & = \left(\frac{\partial v_\beta^p(f)}{\partial f^\alpha} - \frac{\partial v_\alpha^p(f)}{\partial f^\beta} \right) u_s^\alpha(f) u_t^\beta(f). \end{aligned} \quad (12)$$

But in this expression the variables x and f are separated and it follows that if (12) is to hold identically the two sides of the equation must both be identically equal to the same constant. Thus we obtain

$$\left(\frac{\partial v_\beta^i(z)}{\partial z^\alpha} - \frac{\partial v_\alpha^i(z)}{\partial z^\beta} \right) u_s^\alpha(z) u_t^\beta(z) = \tilde{c}_{s t}^i.$$

Finally, multiplying by $v_j^s(z) v_k^t(z)$ and summing over s and t , we obtain (6). Similarly, going in the reverse direction we may obtain (11) from (6). Thus (6) expresses the integrability conditions for the original system (5).

SECTION 56

THE CONSTRUCTION OF A LIE GROUP FROM ITS STRUCTURE CONSTANTS

We here give a construction of a local Lie group having

prescribed structure constants, thus proving the converse of the third theorem of Lie. The construction will be given in terms of coordinates, which amounts to saying that we shall construct the functions $f^i(x, y)$ expressing the coordinates of the product $f = xy = f(x, y)$ in terms of the coordinates of x and y . Since there exist coordinate transformations which change the functions f^i but do not change the structure constants, it goes without saying that the structure constants by themselves do not suffice to determine the functions f^i . Consequently it will be necessary to select, in some fashion, a special coordinate system; say, for example, canonical coordinates of the first or second kind. It is, in fact, possible to carry out the construction in either kind of canonical coordinate system. We here employ canonical coordinates of the first kind.

The construction is carried out in two steps. The first step consists of the introduction of certain auxiliary functions which serve to determine uniquely the functions $f^i(x, y)$ and which are, in their turn, uniquely determined by them (first theorem of Lie—converse and direct). The auxiliary functions satisfy a system of differential equations involving the structure constants, and the relations expressed in these equations (see (8)) constitute the content of the second theorem of Lie. The second step in the construction consists in the integration of these equations (converse of the second theorem of Lie), and it is at this point that it becomes necessary to employ canonical coordinates, since it is only in such a special coordinate system that the auxiliary functions are uniquely determined by the structure constants.

A) Let G be a local Lie group and D be some two times differentiable coordinate system in G , and let

$$f = xy = f(x, y), \quad (1)$$

or, in terms of the coordinate system D ,

$$f^i = f^i(x, y) = f^i(x^1, \dots, x^r; y^1, \dots, y^r). \quad (2)$$

We here introduce the auxiliary functions. To this end denote by $x + \delta x$ the element with coordinates $x^i \pm \delta x^i$, $i = 1, \dots, r$, where x^i , $i = 1, \dots, r$, are the coordinates of a fixed element x , while

$$\delta x^i, i = 1, \dots, r, \quad (3)$$

denote increments in those coordinates. We write $p = (x + \delta x)x^{-1}$ and expand the coordinates of p in Taylor series in the increments (3).

Then

$$p^i = v_j^i(x) \delta x^j + \epsilon_1^i, \quad (4)$$

where ϵ_1^i is small of degree two with respect to the increments (3), while $v_j^i(x) = v_j^i(x^1, \dots, x^r)$ are well defined functions of x . These functions satisfy

$$v_j^i(e) = \delta_j^i, \quad (5)$$

where $\|\delta_j^i\|$ denotes, as usual, the identity matrix, and e is the identity of G . Moreover,

$$v_k^i(f) \frac{\partial f^k}{\partial x^j} = v_j^i(x). \quad (6)$$

Thus $f(x, y)$, considered as a function of x (y held constant), satisfies the system of differential equations (6) along with the obvious initial condition

$$f(e, y) = y. \quad (7)$$

The auxiliary functions $v_j^i(x)$ satisfy the system of equations:

$$\frac{\partial v_k^i(x)}{\partial x^j} - \frac{\partial v_j^i(x)}{\partial x^k} = c_{jk}^i v_j(x) v_k(x), \quad (8)$$

where c_{jk}^i are the structure constants of G . Equations (8) are precisely the integrability conditions for (6) (see Section 55, A)). Finally, we observe that in terms of the auxiliary functions $v_j^i(x)$ it is possible to give a particularly simple form to the equations of a one-parameter subgroup. Indeed, if $x(t)$ is the one-parameter subgroup of G with direction vector a then

$$a^i = v_j^i(x(t)) \frac{dx^j(t)}{dt} \quad (9)$$

In proving A) the important things are, clearly, to verify (6), (8), and (9), since (5) is obviously satisfied. In order to establish (6) we displace the element x in (1) by a small increment; then the coordinates of f are also displaced so that

$$f + \delta f = (x + \delta x)y.$$

From this and from (1) we obtain

$$(f + \delta f)f^{-1} = (x + \delta x)y(xy)^{-1} = (x + \delta x)x^{-1}.$$

Next, writing this equation in coordinate form and employing (4) we obtain

$$v_k^i(f)\delta f^k = v_j^i(x)\delta x^j + \epsilon_2^i, \quad (10)$$

where ϵ_2^i is small of degree two with respect to the increments (3). Next we expand the functions δf^k in Taylor series in the increments (3), obtaining

$$\delta f^k = \frac{\partial f^k}{\partial x^i} \delta x^i + \epsilon_3^k, \quad (11)$$

where ϵ_3^k is also small of degree two. But then, substituting (11) into (10), we have

$$v_k^i(f) \frac{\partial f^k}{\partial x^j} \delta x^j = v_j^i(x) \delta x^j + \epsilon_4^i$$

whence (6) follows by a comparison of coefficients.

In order to verify (8) we remark that if x_0 and f_0 are any two elements sufficiently close to the identity then there exists an element y_0 such that $f_0 = x_0 y_0$. In other words, (6) possesses a solution for arbitrary initial values x_0 and f_0 sufficiently close to e , and consequently, by virtue of Theorem 85, the integrability conditions must be satisfied for (6).

Thus, according to A), Section 55, we have

$$\frac{\partial v_k^i(x)}{\partial x^j} - \frac{\partial v_j^i(x)}{\partial x^k} = \tilde{c}_{\alpha\beta}^i v_j^\alpha(x) v_k^\beta(x), \quad (12)$$

where \tilde{c}_{jk}^i denote certain constants, and our task reduces to showing that these constants are the structure constants of G . Now for $x = e$, (6) reduces to

$$v_\alpha^i(y) \frac{\partial f^\alpha(e, y)}{\partial x^j} = \delta_j^i.$$

Differentiating this relation we obtain

$$\frac{\partial v_\alpha^i(y)}{\partial y^k} \cdot \frac{\partial f^\alpha(e, y)}{\partial x^j} + v_\alpha^i(y) \frac{\partial^2 f^\alpha(e, y)}{\partial x^j \partial y^k} = 0$$

which, at $y = e$, reduces to

$$\frac{\partial v_j^i(e)}{\partial y^k} + \frac{\partial^2 f^i(e, e)}{\partial x^j \partial y^k} = 0. \quad (13)$$

But from this and from (4), Section 52, it follows that $\frac{\partial v_j^i(e)}{\partial y^k} = -a_{jk}^i$.

Thus at $x = e$ (12) assumes the form

$$a_{jk}^i - a_{kj}^i = \tilde{c}_{jk}^i,$$

i.e., the coefficients \tilde{c}_{jk}^i appearing in (12) are precisely the structure constants of G .

Finally we verify (9). To this end let the parameter t change by a small increment δt . Then

$$x(t + \delta t)(x(t))^{-1} = x(\delta t);$$

in other words,

$$x^i(\delta t) = v_j^i(x(t))(x^j(t + \delta t) - x^j(t) + \epsilon_5^i).$$

But then, dividing by δt and taking the limit as $\delta t \rightarrow 0$, we obtain (9). Thus all parts of proposition A) are verified.

The following theorem is the converse of A).

Theorem 86: Let U be an open set in r -dimensional Euclidean space containing the origin e , and suppose defined in U a system of analytic functions

$$\hat{v}_j^i(x) = \hat{v}_j^i(x^1, \dots, x^r),$$

such that the matrix $\|\hat{v}_j^i(x)\|$ remains non-singular throughout U and such that the following conditions are satisfied:

$$\hat{v}_j^i(e) = \delta_j^i, \quad (14)$$

$$\frac{\partial \hat{v}_k^i(x)}{\partial x^j} - \frac{\partial \hat{v}_j^i(x)}{\partial x^k} = \hat{c}_{\alpha\beta}^i \hat{v}_j^\alpha(x) \hat{v}_k^\beta(x), \quad (15)$$

where \hat{c}_{jk}^i denote constants. Since (15) is the integrability condition for the system of equations

$$\hat{v}_k^i(f) \frac{\partial f^k}{\partial x^j} = \hat{v}_j^i(x) \quad (16)$$

it follows from Theorem 85 that there exists a neighborhood G of the origin e sufficiently small so that for $x_0, f_0 \in G$, there exists an analytic solution $f = f(x, f_0, x_0)$ of (16) defined for all $x \in G$ and satisfying the initial condition $f(x_0, f_0, x_0) = f_0$. Let $f(x, y) = f(x, y, e)$. Then

$$f(e, y) = y. \quad (17)$$

We employ the function f to define a product in G , writing

$$f = xy = f(x, y). \quad (18)$$

With respect to this law of multiplication G becomes a local lie group with identity e . Moreover, the auxiliary functions $v_j^i(x)$ for the Group (see A)) coincide with the given functions $\hat{v}_j^i(x)$, and the structure constants c_{jk}^i of G coincide with the constants \hat{c}_{jk}^i :

$$v_j^i(x) = \hat{v}_j^i(x), \quad (19)$$

$$c_{jk}^i = \hat{c}_{jk}^i. \quad (20)$$

Proof: We first verify the associativity of the product defined in the statement of the theorem. In the first place, according to (17) we have $f(e, e) = e$, and since f is continuous we may select a neighborhood V of e sufficiently small so that for $x, y \in V$ we have $f(x, y) \in G$. Let x, y, z be elements of V such that $u = f(x, y)$ and $v = f(y, z)$ also belong to V and let $w = f(u, z)$, $w^* = f(x, v)$. We shall show that $w = w^*$.

We regard y and z as fixed and x as a variable. Then according to the definition of f , the function $w^*(x)$ is a solution of (16) satisfying the initial condition $w^*(e) = v$. Since a solution of (16) is uniquely determined by a set of initial conditions (see Theorem 85) and since $w(e) = v$ it suffices to show that $w(x)$ is also a solution of (16). To this end we introduce the matrix $\|\hat{u}_j^i(x)\|$ inverse to $\|\hat{v}_j^i(x)\|$ and rewrite (16) in the form

$$\frac{\partial f}{\partial x^j} = \hat{u}_k^i(f) \hat{v}_j^k(x). \quad (21)$$

By the chain rule,

$$\frac{\partial w^i}{\partial x^j} = \frac{\partial w^i}{\partial u^\alpha} \frac{\partial u^\alpha}{\partial x^j} = \hat{u}_k^i(w) \hat{v}_\alpha^k(u) \hat{u}_1^\alpha(u) \hat{v}_j^1(x) = \hat{u}_k^i(w) \hat{v}_j^k(x).$$

Thus $w(x)$ is a solution of (21), and associativity is verified. Moreover, in view of the associativity of the product, it follows from (17) that e is the identity of G .

It remains to show that inverses exist in G , i.e., that it is possible to solve

$$f^i(x, y) = 0 \quad (22)$$

with respect to x . Now for $y = e$, (22) has solution $x = e$, while (14) and (16) imply that the Jacobian of (22) is equal to one for $x = y = e$. Thus (22) has unique solution x for all y sufficiently close to e , i.e., there is a neighborhood of e in G consisting of invertible elements.

From what has already been shown it follows that G is a local Lie group and hence (see A)) that $f(x, y)$ satisfies (6). Since f also satisfied (16) it follows that $v_j^i(z) = \hat{v}_j^i(z)$. Indeed, (6) and (16) with $x = e$ show that the functions $v_j^i(z)$ and $\hat{v}_j^i(z)$ are uniquely determined by $f(x, y)$ (see (5) and (14)). Finally, it is an immediate consequence of (19) that the coefficients in (8) and (15) also coincide, i.e., $c_{jk}^i = \hat{c}_{jk}^i$.

This completes the first step in the construction of a Lie group. We turn now to the second step. Here the problem consists in the solution of (8), i.e., in finding the auxiliary functions $v_j^i(x)$ when the structure constants are given. The very form of (8) shows that the solution of this problem, even in the presence of the initial condition (5), is not uniquely determined. As has already been observed, it is necessary to specialize the choice of coordinate system; in this way the functions $v_j^i(x)$ will be subjected to further conditions which will permit a unique solution of the problem. As special coordinates in this connection we employ a canonical coordinate system of the first kind (see Section 42, B) and Theorem 59).

The problem of solving (8) in a canonical coordinate system will be reduced to the integration of a system of ordinary differential equations. The method employed here is one that occurs fairly frequently; rather than attempting to solve for the functions v_j^i directly in the whole neighborhood of the identity we first determine them along an arc, in this case along a one-parameter subgroup. Indeed if $g(t)$ is a given one-parameter subgroup then, in a canonical coordinate system of the first kind, we have $g^i(t) = a^i t$, and the functions $v_j^i(g(t))$ are functions of the single parameter t along the subgroup $g(t)$. It turns out that the functions $t v_j^i(g(t))$, considered as functions of t , satisfy a system of ordinary linear

differential equations with constant coefficients. Accordingly, their existence is assured by an elementary existence theorem and, as we shall see, this serves to solve the problem completely.

We begin by observing a characteristic property of canonical coordinate systems of the first kind.

B) Let D be a two times differentiable coordinate system in a local Lie group G . Then a necessary and sufficient condition that D should be canonical of the first kind is that the auxiliary functions $v_j^i(x)$, as computed in the system D , should satisfy the equations

$$v_j^i(x)x^j = x^i. \quad (23)$$

Indeed, suppose D is a canonical coordinate system of the first kind and let $g(t)$ be a one-parameter subgroup in G having direction vector a . Then $g^i(t) = a^i t$ and, employing (9), we obtain

$$v_j^i(at)a^j = a^i. \quad (24)$$

But for $a = x$, $t = 1$, this reduces to (23).

Suppose, on the other hand, that (23) is satisfied and let $g(t)$ be the one-parameter subgroup with direction vector a . Then using (9) once again we obtain

$$v_j^i(g(t)) \frac{dg^j(t)}{dt} = a^i. \quad (25)$$

But now, by (23), this equation is also satisfied by $g^i(t) = a^i t$ and we conclude that $g^i(t) = a^i t$ by virtue of the uniqueness of solutions of (25). Thus D is a canonical coordinate system of the first kind.

C) Let G be a local Lie group and let D be an arbitrary but fixed two times differentiable coordinate system of the first kind in G . Let $v_j^i(x) = v_j^i(x^1, \dots, x^r)$ be the auxiliary functions expressed in the system D and let

$$w_j^i(t) = w_j^i(t, a) = tv_j^i(a^1t, \dots, a^rt) = tv_j^i(at), \quad (26)$$

where a is a fixed vector and $a t$ denotes the element with coordinates $a^i t$. Then the following relations hold:

$$v_j^i(x) = w_j^i(1, x), \quad (27)$$

$$w_j^i(0, a) = 0, \quad (28)$$

$$\frac{dw_j^i(t)}{dt} = \delta_j^i + c_{\alpha\beta}^j a^\alpha w_j^\beta(t). \quad (29)$$

In particular, the functions $w_j^i(t, a)$, considered as functions of the parameter t , are solutions of the initial value problem (29, 28) and are therefore analytic to all arguments, while the auxiliary functions may be recaptured at once from the functions w_j^i via (27). Thus the verification of these relations will serve to show that, in a canonical coordinate system of the first kind, the auxiliary functions v_j^i are uniquely determined by the structure constants c_{jk}^i and are analytic functions. Thus, the canonical coordinate system of the first kind, which by Theorem 59 is known only to be two times differentiable, is indeed analytic as well (see Theorem 86).

The validity of (27) and (28) is clear from the definition so it is only necessary to prove (29). To this end we first differentiate (23), obtaining

$$x^k \frac{\partial v_k^i(x)}{\partial x^j} + v_j^i(x) = \delta_j^i. \quad (30)$$

Next, multiplying (8) by x^k and summing over k , we have

$$\begin{aligned} \frac{\partial v_k^i(x)}{\partial x^j} x^k - \frac{\partial v_j^i(x)}{\partial x^k} x^k &= c_{\alpha\beta}^i v_j^\alpha(x) v_k^\beta(x) x^k \\ &= -c_{\alpha\beta}^i x^\alpha v_j^\beta(x) \end{aligned} \quad (31)$$

(here we use (23) and the skew-symmetry of the structure constants, see Section 52, ()). From (30) and (31) it follows that

$$\frac{\partial v_j^i(x)}{\partial x^k} x^k + v_j^i(x) = \delta_j^i + c_{\alpha\beta}^i x^\alpha v_j^\beta(x)$$

whence, evaluating at $x = a t$, we obtain

$$\frac{\partial v_j^i(a t)}{\partial x^k} ta^k + v_j^i(a t) = \delta_j^i + c_{\alpha\beta}^i a^\alpha v_j^\beta(a t). \quad (32)$$

But the left member of this equation is precisely the derivative of $w_j^i(t, a)$ with respect to t . Thus (32) may be rewritten in the form (29), and proposition C) is established.

The following theorem is the converse of C).

Theorem 87: Let \hat{c}_{jk}^i be a system of constants satisfying the conditions

$$\hat{c}_{jk}^i = -\hat{c}_{kj}^i, \quad (33)$$

$$\overset{*}{c}_{is}{}^p \overset{*}{c}_{jk}{}^s + \overset{*}{c}_{js}{}^p \overset{*}{c}_{ki}{}^s + \overset{*}{c}_{ks}{}^p \overset{*}{c}_{ij}{}^s = 0. \quad (34)$$

Consider the system of ordinary differential equations

$$\frac{d\overset{*}{w}_j{}^i}{dt} = \delta_j{}^i + \overset{*}{c}_{\alpha\beta}{}^i a \overset{*}{w}_j{}^\beta, \quad (35)$$

where a denotes an arbitrary constant vector and $\overset{*}{w}_j{}^i$ denote unknown functions of a parameter t . Since the system (35) is linear and has constant coefficients its solutions are defined and analytic for all t and a . Let $\overset{*}{w}_j{}^i(t)$, $a >$ denote the solution of (35) satisfying the initial condition

$$\overset{*}{w}_j{}^i(0, a) = 0 \quad (36)$$

and define

$$\overset{*}{v}_j{}^i(x) = \overset{*}{w}_j{}^i(1, x). \quad (37)$$

Then the functions $\overset{*}{v}_j{}^i(x)$ satisfy relations (14) and (15), where e denotes the origin of the coordinate system. Moreover, the equations

$$\overset{*}{v}_j{}^i(x)x^j = x^i \quad (38)$$

are satisfied.

Proof: It is clear that for $a = e$ the initial value problem (35, 36) is satisfied by the functions $\overset{*}{w}_j{}^i(t) = \delta_j{}^i t$ so that, according to (37), $\overset{*}{v}_j{}^i(e) = \delta_j{}^i$, and (14) is verified. The remaining relations (15) and (38) will be proved by two more applications of the same device. In order to make clear the line of argument we begin with the simpler of the two, viz., (38).

Let

$$h^i(t) = \overset{*}{w}_j{}^i(t, a)a^j - ta^i. \quad (39)$$

We shall show that $h^i(t) = 0$ identically in t . In particular, $h^i(1) = 0$, which is precisely (38). In order to verify the desired identity we begin by observing that

$$h^i(0) = 0. \quad (40)$$

Next we compute the derivative $h^i(t)$. Since the skew-symmetry (33) implies that $c_{\alpha\beta}{}^i a^\alpha a^\beta = 0$ we have, according to (35),

$$\begin{aligned}\frac{dh^i(t)}{dt} &= (\delta_j^i + \overset{*}{c}_{\alpha\beta}^j a^\alpha \overset{*}{w}_j^\beta(t, a)) a^j - a^i = \overset{*}{c}_{\alpha\beta}^j a^\alpha \overset{*}{w}_j^\beta(t, a) a^j \\ &= \overset{*}{c}_{\alpha\beta}^j a^\alpha (\overset{*}{w}_j^\beta(t, a) a^j - t a^\beta).\end{aligned}$$

In other words, the functions $h^i(t)$ satisfy the system of homogeneous linear equations

$$\frac{dh^i}{dt} = \overset{*}{c}_{\alpha j}^i a^\alpha h^j. \quad (41)$$

But now, one solution of (41) satisfying the trivial initial condition $h^i(0) = 0$ is the trivial solution $h^i(t) = 0$, and since a solution of (41) is uniquely determined by its initial condition we conclude that $h^i(t) = 0$ for all t , whence (38) follows.

In order to apply the same device to the proof of (15) we define the functions

$$h_{jk}^i(t) = \frac{\partial \overset{*}{w}_k^i(t, a)}{\partial a^j} - \frac{\partial \overset{*}{w}_j^i(t, a)}{\partial a^k} - \overset{*}{c}_{\alpha\beta}^i \overset{*}{w}_j^\alpha(t, a) \overset{*}{w}_k^\beta(t, a). \quad (42)$$

Since (15) is just the equation $h_{jk}^i(1) = 0$ it suffices, once again, to show that $h_{jk}^i(t) = 0$ identically.

Since $\overset{*}{w}_j^i(0, a) = 0$ it is clear that $\frac{\partial \overset{*}{w}_j^i(0, a)}{\partial a^k} = 0$. Thus the functions h_{jk}^i satisfy the trivial initial condition

$$h_{jk}^i(0) = 0. \quad (43)$$

As before, the proof will be completed by showing that the functions $h_{jk}^i(t)$ satisfy a system of homogeneous linear equations. To begin with, differentiating (35) with respect to a^i yields

$$\frac{\partial^2 \overset{*}{w}_k^i(t, a)}{\partial t \partial a^i} = \overset{*}{c}_{j\beta}^i \overset{*}{w}_k^\beta(t, a) + \overset{*}{c}_{\alpha\beta}^i a^\alpha \frac{\partial \overset{*}{w}_k^\beta(t, a)}{\partial a^j}. \quad (44)$$

But then taking (35) into account once again, we obtain

$$\begin{aligned}\frac{dh_{jk}^i}{dt} &= \overset{*}{c}_{j\beta}^i \overset{*}{w}_k^\beta + \overset{*}{c}_{\alpha\beta}^i a^\alpha \frac{\partial \overset{*}{w}_k^\beta}{\partial a^j} - \overset{*}{c}_{k\beta}^i \overset{*}{w}_j^\beta - \overset{*}{c}_{\alpha\beta}^i a^\alpha \frac{\partial \overset{*}{w}_j^\beta}{\partial a^k} \\ &\quad - \overset{*}{c}_{\alpha\beta}^i (\delta_j^\alpha + \overset{*}{c}_{\gamma\delta}^\alpha a^\gamma \overset{*}{w}_j^\delta) \overset{*}{w}_k^\beta - \overset{*}{c}_{\alpha\beta}^i \overset{*}{w}_j^\alpha (\delta_k^\beta + \overset{*}{c}_{\gamma\delta}^\beta a^\gamma \overset{*}{w}_k^\delta).\end{aligned}$$

Of the eight terms in this sum, four cancel in pairs because of

the skew-symmetry (33), while two others may be combined using (34). Making these simplifications, and relabeling the dummy indices appropriately, we obtain

$$\frac{dh_{jk}^i}{dt} = c_{\alpha\beta}^i a^\alpha \left(\frac{\partial \overset{*}{w}_{k\beta}}{\partial a^j} - \frac{\partial \overset{*}{w}_{j\beta}}{\partial a^k} - \overset{*}{c}_{\gamma\delta}^{\beta} \overset{*}{w}_j^\gamma \overset{*}{w}_k^\delta \right) = \overset{*}{c}_{\alpha\beta}^i a^\alpha h_{jk}^\beta,$$

which says that the functions $h_{jk}^i(t)$ satisfy

$$\frac{dh}{dt} = \overset{*}{c}_{\alpha\beta} a^\alpha h^\beta. \quad (45)$$

Since the trivial initial condition (43) is also satisfied, (15) now follows, as before from $h_{jk}^i = 0$. Thus the proof of Theorem 87 is complete.

Both steps in the program of the construction of a local Lie group from its structure constants have now been completed. We here summarize the entire process in the form of a single theorem.

Theorem 88: Let c_{jk}^i be any system of constants satisfying relations (11) and (12), Section 52. Consider the system of equations

$$\frac{dw_j^i}{dt} = \delta_j^i + c_{\alpha\beta}^i a^\alpha w_j^\beta, \quad (46)$$

where a denotes a constant vector and w_j^i denote unknown functions of the parameter t . Let $w_j^i(t, a)$ denote the solution of (46) satisfying the initial condition

$$w_j^i(0, a) = 0 \quad (47)$$

and define

$$v_j^i(x) = w_j^i(1, x). \quad (48)$$

Since (46) is a system of linear equations with constant coefficients its solutions are defined and analytic for arbitrary a and for all values of t ; consequently the functions $v_j^i(x)$ are defined and analytic for all values of x , i.e., on all of Euclidean space. Consider next the system of partial differential equations

$$v_k^i(f) \frac{\partial f^k}{\partial x^j} = v_j^i(x). \quad (49)$$

The integrability condition is satisfied for this system and since,

at the origin e , the matrix $\|v_j^i(x)\|$ reduces to the identity matrix, it follows that there exists a neighborhood G of the origin e sufficiently small so that for every $y \in G$ there exists a solution $f(x, y)$ of (49) defined for all $x \in G$, $y \in G$ and satisfying the initial condition

$$f(e, y) = y. \quad (50)$$

Defining the product of two points x and y in G to be

$$xy = f(x, y) \quad (51)$$

turns G into a local Lie group. Moreover the Euclidean coordinates in G constitute a canonical coordinate system of the first kind and the structure constants of G in this coordinate system coincide with the given constants c_{jk}^i . Finally, if G^* is an arbitrary local Lie group whose structure constants coincide with the given constants c_{jk}^i in some canonical coordinate system of the first kind then the function $f^*(x, y)$ defining the product in G^* coincides, in its coordinate form, with the function $f(x, y)$ obtained above.

The various parts of Theorem 88 have already been proved in Propositions A), B), C) and Theorems 86 and 87. Thus the existence and uniqueness of a local Lie group having a given set of structure constants is demonstrated. It is important to note that the function $f(x, y)$ here obtained is analytic since the systems of equations that must be integrated are all analytic. Thus any Lie group admits an analytic coordinate system.

It remains to formulate this result in terms of the Lie algebra.

Theorem 89: If R is any real Lie algebra then there exists a local Lie group G whose Lie algebra is isomorphic with R . Moreover, if G and G' are local Lie groups with Lie algebras R and R' , and if g is an isomorphism of R onto R' , then there exists one and, up to equivalence, only one local isomorphism h of G onto G' to which the given isomorphism g corresponds.

Proof: In order to construct the desired group G we have but to introduce a coordinate system in R . Since the structure constants of R in this coordinate system satisfy (11) and (12) Section 52, they may, according to Theorem 88, be used to construct a local Lie group G . But then the Lie algebra of G is clearly isomorphic with R .

To prove the rest of the theorem, let R and R' be isomorphic Lie algebras under an isomorphism g , and select coordinate systems in R and R' that correspond to one another under g , so that

the structure constants of the algebras are the same in these coordinate systems. Then, selecting in G and G' , respectively, canonical coordinate systems of the first kind, we obtain in these coordinate systems functions $f(x, y)$ and $f'(x, y)$ defining the multiplication in the given groups, and these functions must coincide since the structure constants do (see Theorem 88). Thus, associating with each point $x \in G$ that point $x' \in G'$ which has the same coordinates as x , we obtain the desired isomorphism h . The uniqueness of h follows from the fact that an automorphism of G' assumes the form of a linear transformation in a canonical coordinate system of the first kind (see Section 43, D)) so that a non-identical automorphism of G' gives rise to a non-identical automorphism of its Lie algebra R' .

Theorem 89 shows that the analysis of a local Lie group reduces completely to the analysis of its Lie algebra.

It should be observed that the line of argument followed here in constructing the Lie group possessing a given Lie algebra is primarily of theoretical interest. In practice it is ordinarily easier to find the desired group in some indirect fashion, and then to employ Theorem 89 as a uniqueness theorem. As an example of this procedure we mention the following result.

D) Every r -dimensional commutative Lie group is locally isomorphic with an r -dimensional vector group, i.e., with the additive group of an r -dimensional vector space.

Example 96: We analyze the structure of two-dimensional Lie groups. Let R be a two-dimensional real Lie algebra and let p and q be linearly independent vectors in R . Writing $[p, q] = r$ we see at once that, for arbitrary vectors $a, b \in R$, we have $[a, b] = \alpha r$ where α is a real number. We distinguish the two cases $r = 0$ and $r \neq 0$. If $r = 0$ then the commutator of any pair of vectors in R vanishes, and R is commutative. On the other hand, if $r \neq 0$ then there exists a vector t such that $[r, t] = r$ and, as a basis in R , we choose r and t . Then the structure constants are $c_{12}^1 = 1$, $c_{12}^2 = 0$. Thus there are but two non-isomorphic two dimensional Lie algebras. If R is commutative the corresponding Lie group G is also commutative. If R is non-commutative a corresponding Lie group G is defined by the following relations:

$$f^1 = x^1 + y^1 e^{-x^2}, \quad f^2 = x^2 + y^2.$$

Observe that the set of elements in G for which the second coordinate vanishes forms a normal subgroup. The ideal in the

Lie algebra R corresponding to this subgroup is the one-dimensional ideal generated by r.

Example 97: It is now a simple matter to give a complete classification of connected commutative global Lie groups. It turns out that any such group G resolves into the direct product of subgroups, each isomorphic either with D or with K where, as usual, D denotes the additive topological group of real numbers, and K the factor group of D by the subgroup of integers. If G is compact the factors isomorphic with D must be absent.

Indeed, let H be a vector space of the same dimension as G. Since G and H are locally isomorphic (see D)) the simply connected group H is the universal covering of G and G is isomorphic with a factor group H/N where N is a discrete subgroup of H. Let e_1, \dots, e_s denote the system of generators for N constructed in Example 33. Then e_1, \dots, e_s are linearly independent and may be extended to a basis of H by adjoining vectors e_{s+1}, \dots, e_n . Thus H/N resolves into the direct sum of s copies of K and n-s copies of D.

SECTION 57

THE CONSTRUCTION OF SUBGROUPS AND HOMOMORPHISMS

It was seen in the preceding section that the correspondence defined in Section 52 between Lie groups and Lie algebras is one-to-one. We here establish the analogous facts regarding the correspondences (see Section 53) between subgroups and subalgebras, factor groups and residue class algebras, respectively. It should be noted that all of the results of the present paragraph are all of local character.

Theorem 90: Let G be a local Lie group, let R be its Lie algebra, and let S be a subalgebra of R. Then there exists one and, up to equivalence, only one subgroup H of G (see Section 23, I)) whose corresponding subalgebra (see Theorem 83) is S. We shall say that H and S correspond to one another $H = S$.

Proof: Let r and s denote the dimensions of the spaces R and S, respectively. We select a coordinate system in R such that a vector a belongs to S when and only when its coordinates satisfy the relations:

$$a^{s+1} = 0, \dots, a^r = 0, \quad (1)$$

and introduce in G the corresponding canonical coordinate system of the first kind. (These coordinate systems will be kept fixed throughout the course of the proof.) Then a subgroup H of G is defined by a system of linear equations (see Theorem 62), and if the subalgebra corresponding to H is to be S then the defining equations must be

$$x^{s+1} = 0, \dots, x^r = 0, \quad (2)$$

i.e., a point x will belong to H when and only when its coordinates satisfy (2). Thus the desired subgroup is unique if it exists.

It remains to prove that the set H defined by (2) is, in fact, a subgroup of G . Since H is obviously closed it suffices to show that if $x, y \in H$ then $xy \in H$ and $x^{-1} \in H$. This will be established by following the program outlined in Theorem 88.

Let c_{jk}^i be the structure constants of G or, equivalently, of R . Since (1) defines a subalgebra it follows that the structure constants satisfy the following conditions:

$$\text{if } i > s, \quad j \leq s, \quad k \leq s, \quad \text{then } c_{jk}^i = 0. \quad (3)$$

In order to avoid the necessity of stating repeatedly what range of values we ascribe to various indices, we adopt the following convention: an index will be equipped with a single prime ('') if its range is $1, \dots, s$, and with two primes ('') if its range is $s + 1, \dots, r$. Thus, using this convention, (3) may be written more succinctly as

$$c_{j'k'}^{i''} = 0. \quad (4)$$

Similarly points belonging to H and vectors belonging to S will be denoted by letters with primes.

The first step in the program is to solve the system of equations (46), Section 56, in the case $a = a' \in S$. We begin by separating (46) into two independent systems:

$$\frac{dw_j{}^i}{dt} = \delta_{j''}{}^i + c_{\alpha\beta}{}^i a^\alpha w_{j''}{}^\beta, \quad (5)$$

$$\frac{dw_{j''}{}^i}{dt} = \delta_{j''}{}^i + c_{\alpha\beta}{}^i a^{\alpha'} w_{j''}{}^\beta, \quad (6)$$

and introducing the auxiliary system

$$\frac{dw_j^{*,i}}{dt} = \delta_{j,i} + c_{\alpha,\beta}^{*,i} a^\alpha w_\beta^*. \quad (7)$$

Because of (4) it is easily seen that if $w_j^{*,i}$ is a solution of (7) then

$$w_j^{*,i} = w_j^{*,i}, \quad (8)$$

$$w_j^{*,i} = 0 \quad (9)$$

defines a solution of (5), so that, by uniqueness, we have

$$w_j^{*,i}(t, a) = 0 \quad (10)$$

and therefore

$$v_j^{*,i}(x) = 0 \quad (11)$$

Observe that the functions $v_j^{*,i}(x)$ obtained from (8) are themselves the auxiliary functions of the Lie group whose Lie algebra is S . Indeed, we have $v_j^{*,i}(x) = w_j^{*,i}(1, x)$ where the functions $w_j^{*,i}(t, a)$ are obtained by integrating (7), in which the coefficients $c_{j,\alpha}^{*,i}$ are precisely the structure constants of S .

We now turn our attention to the system of equations (49), Section 56. It is required to show that $f(x, y) \in H$, or, what comes to the same thing, $f^{i''}(x, y) = 0$. Since for fixed y the function $f(x, y)$ depends only the variables x^i , $i = 1, \dots, s$, it suffices to solve the subsystem

$$v_k^i(f) \frac{\partial f^k}{\partial x^i} = v_j^i(x) \quad (12)$$

with initial condition $f(e, y) = y$. Observe that (12) may be reduced to the form (1), Section 55, so that, integrable or not, it can possess no more than one solution satisfying the initial condition. In order to solve (12) we introduce the auxiliary system

$$v_k^{*,i}(f^*) \frac{\partial f^{*,k}}{\partial x^i} = v_j^{*,i}(x) \quad (13)$$

with initial condition $f^{*,i}(e, y) = y^i$. This system is integrable since the functions $v_j^{*,i}(z)$ appearing in it are, as noted above, the auxiliary functions of a Lie group. But then, taking (11) into account, it is easily seen that (12) is satisfied by the functions $f^i(x, y) = f^{*,i}(x, y)$, $f^{i''}(x, y) = 0$ and, because of the uniqueness of the solution of (12) we conclude that $f^{i''}(x, y) = 0$. Thus $x'y' = f' \in H$.

Finally, in order to prove $(x')^{-1} \in H$ it suffices to observe

that, in a canonical coordinate system of the first kind, the element x^{-1} has coordinates $-x^i$, $i = 1, \dots, r$ as may readily be verified by consideration of one-parameter subgroups. Thus $(x')^{-1} = z' \in H$ and Theorem 90 is proved.

A) Let G be a local Lie group and fix in G a canonical coordinate system of the first kind. Then the inner automorphism $\varphi_x, x \in G$, defined by $\varphi_x(z) = zxz^{-1}$, is given in coordinate form by a matrix $\|l_j^i(x)\|$:

$$(\varphi_x(z))^i = l_j^i(x)z^j. \quad (14)$$

It turns out that, along the one-parameter subgroup $x^i = a^i t$ determined by an arbitrary direction vector a the matrix $\|l_j^i(ta)\|$ satisfies the homogeneous differential equation

$$\frac{d l_j^i(ta)}{dt} = c_{\alpha\beta}^i a^\alpha l_j^\beta(ta) \quad (15)$$

and the obvious initial condition

$$l_j^i(0a) = \delta_j^i. \quad (16)$$

Indeed, (15) is just another form of a relation obtained in Section 54. The matrix $\|l_j^i(x)\|$ also defines the automorphism l_x of the Lie algebra R corresponding to φ_x and it follows from Section 54, F), that the direction vector of the one-parameter subgroup l_{ta} is the transformation p_a . But then, by Section 54, B), the subgroup l_{ta} satisfies the differential equation

$$\frac{d}{dt} l_{ta} = p_a l_{ta} \quad (17)$$

and (15) is just the coordinate expression of this equation.

Theorem 91: Let G be a local Lie group, let H be a subgroup, let R be the Lie algebra of G and suppose that S is the subalgebra corresponding to H , $H \rightarrow S$ (see Theorem 83). If S is an ideal in R then H is a normal subgroup. If S is a central ideal then H is a central normal subgroup. Finally, if S is the center of R then H is the center of G .

Proof: We continue to use the notational conventions introduced in the proof of Theorem 90. Thus r and s will denote the dimensions of G and H , respectively, and we suppose given in G a canonical

coordinate system of the first kind in which H is defined by

$$x^{s+1} = 0, \dots, x^r = 0. \quad (18)$$

so that, in the corresponding coordinate system in R , the subalgebra S is determined by

$$a^{s+1} = 0, \dots, a^r = 0. \quad (19)$$

Similarly, we continue to denote by an index with one prime ('') one ranging over the values $1, \dots, s$, and by an index with two primes (''') one ranging over the values $s+1, \dots, r$. Finally, elements of H will be denoted by letters equipped with primes.

Our problem is to determine how the inner automorphisms of G act on the elements of H . To this end it suffices to compute the matrix $\|l_j^i(x)\|$.

Now because of the special choice of coordinate system in G and because S is an ideal, the structure constants c_{jk}^i satisfy the relations

$$c_{jk}^{i'''} = 0. \quad (20)$$

Thus if we split the system (15) into the two independent systems

$$\frac{d l_j^i(ta)}{dt} = c_{\alpha\beta}^i a^\alpha l_j^{\beta'}(ta), \quad (21)$$

$$\frac{d l_j^i(ta)}{dt} = c_{\alpha\beta}^i a^\alpha l_j^{\beta''}(ta) \quad (22)$$

and first solve the auxiliary system

$$\frac{d l_j^i(ta)}{dt} = c_{\alpha\beta}^i a^\alpha l_j^{*\beta'}(ta), \quad (23)$$

it is easy to see that (21) is satisfied by the functions $l_j^{*\beta'}(ta) = l_j^{*\beta''}(ta)$, $l_j^{*\beta''}(ta) = 0$. But from this it follows that

$$l_j^{*\beta''}(x) = 0 \quad (24)$$

and consequently that $\varphi_x(z') \in H$ (see (14)), i.e., H is normal.

Suppose now that S is a central ideal. Then (20) is replaced by the stronger condition $c_{jk}^i = 0$ so that (21) has the solution $l_j^i(ta) = \delta_j^i$ (recall the initial condition (16)), and consequently

$$l_{j,i}(x) = \delta_{j,i} . \quad (25)$$

But from this it follows that $\varphi_x(z') = z'$, i.e., that H is a central subgroup.

Finally, suppose S is the center of R . Denote by H_0 the center of G and let $H_0 \rightarrow S_0$. Then $H \subset H_0$ and consequently $S \subset S_0$. But S_0 is a central ideal (see Theorem 83) so that $S_0 \subset S$. Thus $S_0 = S$ and consequently $H_0 = H$.

We turn now to the consideration of homomorphisms.

Theorem 92: Let G and G' be local Lie groups, let R and R' be their Lie algebras, and let h be a homomorphism of R onto R' . Then there exists one and, up to equivalence, only one local homomorphism f of G onto G' such that $f \rightarrow h$. We shall say that f and h correspond to one another: $f \rightleftharpoons h$.

Proof: Let S denote the kernel of h . By Theorems 90 and 91, the ideal S corresponds to a normal subgroup N of G , $N \rightarrow S$. Let $G^* = G/N$ and denote by f^* the natural projection of G onto G^* . Let R^* denote the Lie algebra of G^* and let h^* be the homomorphism of R onto R^* corresponding to f^* . The kernel of h^* is also S since N is the kernel of f^* and $N \rightarrow S$ (see Theorem 84).

Let A denote an arbitrary residue class modulo S . Then h^* carries A onto an element $a^* \in R^*$, while h carries A onto another element $a' \in R'$. Letting $a' = h'(a^*)$ we obtain a mapping h' which is easily seen to be an isomorphism of R^* onto R' satisfying the condition

$$h(a) = h'(h^*(a)) , \quad (26)$$

for every $a \in R$. But then by Theorem 89 there exists a uniquely determined isomorphism f' of G^* onto G' such that $f' \rightarrow h'$. Let

$$f(x) = f'(f^*(x)) . \quad (27)$$

Since $f^* \rightarrow h^*$ and $f' \rightarrow h'$, we have (see Section 53, E))

$$f \rightarrow h . \quad (28)$$

Finally, if there existed two distinct homomorphisms f and f'' , both satisfying (28), then they would have the same kernel and we would obtain from them a non-identical automorphism of G' corresponding to the identity automorphism of the Lie algebra R' , thus contradicting Theorem 89.

The following examples show that the constructions of the present paragraph are, in fact, essentially of a local nature.

Example 98: Let T^2 denote the two-dimensional torus, i.e., the group of pairs (x^1, x^2) of real numbers determined up to an additive integer (see Example 86). Clearly T^2 is a global Lie group. Let R^2 denote its Lie algebra and consider in T^2 the local one-parameter subgroup $x(t)$ defined by the relations $x^1(t) = a^1 t$, $x^2(t) = a^2 t$, where the ratio a^1/a^2 is irrational. To the local subgroup $\{x(t)\} = H$ there corresponds a subalgebra S of R^2 , but there exists no global subgroup of T^2 corresponding to S . For suppose H^* to be such a subgroup. Since H^* is uniquely determined by S it follows that H^* and H coincide in some neighborhood of the identity. Hence, being a global subgroup, H^* must contain all elements $x(t)$, $x^1(t) = a^1 t$, $x^2(t) = a^2 t$, $-\infty < t < +\infty$. But this implies that H^* is everywhere dense in T^2 (see, in this connection, Example 36) and since H^* is closed we arrive at the contradiction $H^* = T^2$.

It is to be observed that T^2 is not simply connected and that if the above constructions had been carried out in the universal covering group T^2 no difficulties would have been encountered (once again, see Example 36). However, the following example shows that even in the case of simply connected global Lie groups there does not exist a one-to-one correspondence between global subgroups and subalgebras of the Lie algebra.

Example 99: Let G be the multiplicative group of quaternions of modulus one and let R be its Lie algebra. Denote by H the one dimensional subgroup of G consisting of quaternions of the form $\cos 2\pi x + i \sin 2\pi x$. The product $G \times G$ contains the toroidal subgroup $H \times H$, the elements $(\cos 2\pi x^1 + i \sin 2\pi x^1, \cos 2\pi x^2 + i \sin 2\pi x^2)$ of which are determined by a pair of real parameters x^1, x^2 , each defined up to an additive integer. Let $x^l = a^l t$, $l = 1, 2$, be the equations of a one-parameter subgroup $H \times H$ given in terms of these parameters, and suppose once again that the ratio a^1/a^2 is irrational. As was observed in the preceding example, the global group $x(t)$ fills an everywhere dense set on the torus $H \times H$. On the other hand, if we consider $x(t)$ on a bounded set of values of the parameter t we obtain a one-dimensional local subgroup H' in $H \times H \subset G \times G$. Let S' denote the corresponding subalgebra of the Lie algebra $R + R$. Clearly S' corresponds to no global subgroup of the simply connected Lie group $G \times G$.

SECTION 58

SOLVABLE AND SEMI-SIMPLE LIE ALGEBRAS

The results of the preceding sections reduce the entire study of local Lie groups to the study of real Lie algebras. The central tool in the deeper investigation of the latter is the adjoint algebra (see Section 54, E)). To each element a of a Lie algebra R there corresponds the linear transformation p_a of the vector space R into itself defined by $p_a(x) = [a, x]$, and the study of the dependence of the eigenvalues and eigenvectors of p_a on the vector a constitutes the fundamental method of analysis of the structure of the algebra. Since these eigenvalues are, in general, complex it becomes necessary to extend the real vector space R to a complex space $[R]$. Thus, we are led unavoidably to the theory of complex Lie algebras. To every real Lie algebra R there corresponds, in a unique fashion, a complex algebra $[R]$ called its complexification. The original real algebra R will be called a real form of the algebra $[R]$. In this connection it is essential to note that non-isomorphic real Lie algebras may possess isomorphic complexifications and, consequently, that a complex Lie algebra may possess several distinct real forms. Moreover, it is not clear a priori whether every complex Lie algebra even has a real form, i.e., is isomorphic with the complexification of some real algebra.

A central problem in the theory of Lie algebras is to give, if possible, a complete classification. As a first step in this direction one distinguishes two broad classes of Lie algebras possessing, to a considerable extent, diametrically opposite properties. These are, on the one hand, the solvable algebras and, on the other hand, the semi-simple algebras. The former are those that can be built up step-wise out of commutative Lie algebras; the latter are less closely related to commutative algebras. It turns out that an arbitrary Lie algebra is made up of a solvable part and a semi-simple part, in the sense that it contains a solvable ideal, the algebra of residues modulo which is semi-simple. In this rather weak sense, the study of an arbitrary Lie algebra reduces to the study of a solvable algebra and a semi-simple algebra. At first glance it would seem that the solvable algebras are more elementary than the semi-simple ones, but this is not so; in any event there is, at the present time, no prospect of giving a complete classification of solvable algebras, while the semi-simple Lie algebras have been completely classified. This classification, which is due to Killing, constitutes perhaps the most interesting and significant result of the theory.

The concepts of solvability and semi-simplicity extend to Lie

algebras over an arbitrary field and it is easy to show that a real algebra R and its complexification $[R]$ are simultaneously solvable or not, semi-simple or not. The results of Killing bear on complex semi-simple Lie algebras. It turns out that any such algebra resolves into the direct sum of simple non-commutative algebras and the complex, non-commutative simple algebras are completely classified. These fall into four infinite series

$$A_n, \quad n \geq 1; \quad B_n, \quad n \geq 2; \quad C_n, \quad n \geq 3; \quad D_n, \quad n \geq 4,$$

along with five exceptional algebras

$$G_2, \quad F_4, \quad E_6, \quad E_7, \quad E_8.$$

This result in itself says nothing, however, concerning the classification of Lie groups since for that purpose one needs a classification of real Lie algebras. The transition from the classification of complex semi-simple algebras to a classification of real semi-simple algebras presents as much difficulty as did the original classification in the complex case. It is shown that every complex semi-simple algebra possesses real forms, that the number of distinct real forms is finite, and these forms are all found (Cartan [9]; see also [14]). Now among the real forms of any one complex semi-simple algebra there is one and only one that corresponds to a compact Lie group so that a one-to-one correspondence exists between complex semi-simple Lie algebras and those real semi-simple Lie algebras that belong to compact groups. Thus the problem of classifying compact semi-simple Lie groups is of approximately the same degree of difficulty as the problem of classifying complex semi-simple Lie algebras. The further problem of classifying all real semi-simple Lie algebras turns out to be very difficult and will not be considered in this book. Since our interest is primarily in real Lie algebras (for these are the algebras corresponding to Lie groups) and not complex Lie algebras, which we regard only as a tool in the study of the real case, we shall content ourselves with the classification of those real semi-simple algebras corresponding to compact Lie groups. Such algebras will be called compact Lie algebras. The classification will be given in the next chapter. We here set forth the definitions of solvable and semi-simple Lie algebras, and establish the simplest relations between real algebras and their complexifications.

A) Let R be a Lie algebra over an arbitrary field K and let

S be a subalgebra and T an ideal in R . Then the algebras $(S + T)/T$ and $S/(S \cap T)$ are isomorphic.

Indeed, let φ be the natural projection of $S + T$ onto $(S + T)/T$. Then the homomorphism induced on S by φ maps S onto $(S + T)/T$ and has kernel $S \cap T$. Thus A) follows from Section 53, D).

Definition 49. A Lie algebra R over an arbitrary field K is said to be solvable if there exists in R a non-increasing sequence of subalgebras

$$R_0 = R, \quad R_1, \dots, R_{n-1}, \quad R_n = \{0\}, \quad (1)$$

such that, for $i = 0, \dots, n-1$, R_{i+1} is an ideal in R_i and the residue class algebra R_i/R_{i+1} is commutative. A Lie algebra is semi-simple if it possesses no solvable ideals other than the trivial ideal $\{0\}$.

Note that a one-dimensional algebra, while simple, is not semi-simple, but rather solvable. On the other hand, a simple Lie algebra of dimension greater than one is non-commutative and semi-simple.

B) Let R be a Lie algebra over an arbitrary field K . If R is solvable then all subalgebras and factor algebras of R are also solvable. Moreover, if R possesses a solvable ideal S such that the residue class algebra R/S is solvable then R itself is solvable.

Suppose first that R is solvable. Let (1) be a sequence of subalgebras such that R_i/R_{i+1} is commutative, $i = 0, \dots, n-1$, and let S be a subalgebra. Then $S_i = S \cap R_i$ defines a non-increasing sequence of subalgebras of S , and since

$$S_{i+1} = S_i \cap R_{i+1}, \quad S_i + R_{i+1} \subset R_i,$$

it follows by A) that

$$(S_i + R_{i+1})/R_{i+1} \approx S_i/(S_i \cap R_{i+1}) = S_i/S_{i+1},$$

so that $S_i/S_{i+1} \approx (S_i + R_{i+1})/R_{i+1} \subset R_i/R_{i+1}$ is also commutative. Thus S is solvable.

Similarly, for any ideal S in R let φ denote the natural projection of R onto the residue class algebra $R^* = R/S$ and define

$$\varphi(R_i) = R_i^*.$$

Then

$$\begin{aligned} R_i^*/R_{i+1} &= (R_i + S)/(R_{i+1} + S) = (R_i + R_{i+1} + S)/R_{i+1} + S \\ &\approx R_i/(R_i \cap (R_{i+1} + S)) = R_i/(R_{i+1} + R_i \cap S) \\ &\approx (R_i/R_{i+1})/(R_{i+1} + R_i \cap S)/R_{i+1}. \end{aligned}$$

Thus R_i^*/R_{i+1} is isomorphic with a factor algebra of the commutative algebra R_i/R_{i+1} and is therefore itself commutative. But then R/S is solvable.

Suppose finally that S is an ideal in R and that S and R/S are both solvable. Then there exists a sequence $R_0^* = R/S, R_1^*, \dots, R_m^* = \{0\}$ of subalgebras of R/S , and similarly a sequence of subalgebras $S_0 = S, S_1, \dots, S_n = \{0\}$ of subalgebras of S , such that in both sequences the successive residue class algebras are all commutative. Define now $R_i = \varphi^{-1}(R_i^*)$, $i = 1, \dots, m$ where φ denotes the natural projection of R onto R/S . Then, as is easily seen, the sequence

$$R_0 = R, R_1, \dots, R_m = S_0, R_{m+1} = S_1, \dots, R_{m+n} = \{0\}$$

establishes the solvability of R .

Theorem 93: Let R be a Lie algebra over an arbitrary field K . Then R possesses a solvable ideal S with the property that every solvable ideal of R is contained in S . The ideal S is called the maximal solvable ideal. The residue class algebra R/S is semi-simple.

Proof: Note first that if S and T are solvable ideals in R then the sum $S + T$ is also solvable. Indeed $(S + T)/T$ and $S/(S \cap T)$ are isomorphic by A), and $S/(S \cap T)$ is solvable by B). Thus $(S + T)/T$ and T are both solvable ideals, whence it follows, using B) once again, that $S + T$ is itself solvable.

Now let S be any solvable ideal that is maximal in the set of all solvable ideals, i.e., a solvable ideal not properly contained in any larger solvable ideal. (That such an ideal exists follows from the finite dimensionality of R .) According to the above remark, if T is any solvable ideal then $S + T$ is solvable and consequently $T \subset S$. Thus a maximal solvable ideal S contains every solvable ideal and is uniquely determined.

In order to see that R/S is semi-simple let φ denote the natural projection of R onto $R^* = R/S$ and let Q^* be a solvable ideal in R^* . Then $Q = \varphi^{-1}(Q^*)$ is an ideal in R containing S , and since Q/S

and S are solvable it follows that Q is solvable. But then $Q = S$ and $Q^* = \{0\}$.

Theorem 93 shows that, in a very weak sense, the study of an arbitrary Lie algebra may be reduced to the study of solvable and semi-simple algebras. The following theorem, stated here without proof (see [29], [58]), presents a substantial improvement over Theorem 93 in those cases in which we are interested.

Theorem 94: Let R be a Lie algebra over a field K with characteristic zero and let S be the maximal solvable ideal in R . Then there exists in R a semi-simple subalgebra T such that $S \cap T = \{0\}$ and $T + S = R$.

If T were an ideal then R would resolve into the direct sum of the semi-simple algebra T and the solvable algebra S . However, this is, in general, not the case; the manner in which R is composed of S and T is more complicated than a simple direct sum. In particular, R is not uniquely determined by S and T . Nevertheless, Theorem 94 does make it possible in some cases to reduce the study of R to the study of S and T individually, as we shall see in connection with the construction of a global Lie group from its Lie algebra.

We turn now to the study of the relations between real and complex Lie algebras.

C) If R is a real vector space we denote by $[R]$ the collection of all expressions of the form $z = x + iy$ where $x, y \in R$ and i denotes the complex unit $i = \sqrt{-1}$. Addition is defined in $[R]$ by

$$z_1 + z_2 = (x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2) ,$$

while multiplication by the complex number $\gamma = \alpha + i\beta$ is defined by

$$\gamma z = \gamma(x + iy) = (\alpha x - \beta y) + i(\alpha y + \beta x) .$$

It is clear that these definitions turn $[R]$ into a complex vector space. This space is called the complexification of the real space R . The complex conjugate \bar{z} of the vector $z = x + iy$ is defined to be $\bar{z} = x - iy$.

If R is a Lie algebra then we also define a bracket product in the complex space $[R]$ by writing

$$[\mathbf{z}_1, \mathbf{z}_2] = [\mathbf{x}_1 + i\mathbf{y}_1, \mathbf{x}_2 + i\mathbf{y}_2]$$

$$= [\mathbf{x}_1, \mathbf{x}_2] - [\mathbf{y}_1, \mathbf{y}_2] + i[\mathbf{x}_1, \mathbf{y}_2] + i[\mathbf{y}_1, \mathbf{x}_2].$$

Clearly the product thus defined is linear (see Section 52, (14)); it also satisfies conditions (15) and (16), Section 52, so that $[R]$ becomes a complex Lie algebra. This algebra is called the complexification of the real Lie algebra R . Observe that $[R]$ and R have the same dimension. Moreover, it is readily verified that if S is an ideal in R then $[S]$ is an ideal in $[R]$ and

$$[R/S] \approx [R]/[S].$$

Thus if R is solvable then so is $[R]$.

The only part of the above assertion that requires proof is the fact that $[R]$ is a Lie algebra. Let e_1, \dots, e_r be a basis for R and let

$$[e_j, e_k] = c_{jk}^{-1} e_1. \quad (2)$$

Then the numbers c_{jk}^{-1} , being the structure constants of a Lie algebra, satisfy (18) and (19), Section 52. But e_1, \dots, e_r is also a basis in $[R]$ and the commutator of e_j and e_k in the complex algebra $[R]$ has the same coordinate expression (2). Thus, as we have seen, the bracket product defined in $[R]$ satisfies (15) and (16), Section 52.

D) If R is a complex Lie algebra then the elements of R admit, in particular, multiplication by real numbers. Consequently R may also be viewed as a real Lie algebra. We denote this real algebra by (R) . The sets R and (R) coincide, and so, of course, do the bracket products defined in them. But while the elements of R may be multiplied by complex numbers those of (R) may be multiplied only by real numbers. Thus it is possible for a subset of $R = (R)$ to be a subalgebra of the real algebra (R) but not a subalgebra of R . If e_1, \dots, e_r is a basis in R then $e_1, ie_1, \dots, e_r, ie_r$ forms a basis in (R) . Moreover it is easily seen that if S is an ideal in R then (S) is an ideal in (R) and

$$(R/S) = (R)/(S).$$

Thus if R is solvable then so is (R) .

E) Let R be a real Lie algebra, let $[R]$ be its complexification,

and let $([R])$ be the Lie algebra, obtained by regarding $[R]$ as a real algebra. We employ the operation $z \rightarrow \bar{z}$ of complex conjugation in $[R]$ to define a mapping $\psi(z) = \bar{z}$. Then ψ is an automorphism of $([R])$ but not an automorphism of $[R]$. Clearly ψ is involutory, i.e., ψ^2 is the identity automorphism. Observe that the original Lie algebra R is a subalgebra of $([R])$ and that R consists exactly of those elements $z \in ([R])$ satisfying the condition $\psi(z) = z$.

F) Let R be a real Lie algebra and let S denote its maximal solvable ideal. Then $[S]$ is the maximal solvable ideal in $[R]$. Thus R and $[R]$ are simultaneously solvable or not, semi-simple or not.

In order to prove F), let T denote the maximal solvable ideal in $[R]$. Clearly \bar{T} is also a solvable ideal in $[R]$ so that by maximality we have $T = \bar{T}$. Thus along with every vector z the ideal T contains the conjugate \bar{z} , and consequently both of the real vectors $z + \bar{z}$ and $i(z - \bar{z})$. Thus $T = [S']$ where S' is an ideal in R . Since T is solvable it follows that (T) is solvable, and hence that S' , being a subalgebra of (T) , is solvable too. Thus, by the maximality of S , we have $S' \subset S$ while, from the solvability of $[S]$, it follows that $[S] \subset [S'] = T$. But then $[S] = [S']$, i.e., $T = [S]$.

As has already been observed, complex Lie algebras are viewed, for purposes of the present treatment, simply as a means of studying real Lie algebras. It is possible, however, to give to the concept of a complex Lie algebra an independent significance by introducing the notion of a complex Lie group. This concept is outlined briefly in G) and H) below but will not be employed elsewhere in the book.

G) If G' is a local group with identity e then we shall say that a complex coordinate system is given in G' if there is given a homeomorphism f of G onto some neighborhood of the origin 0 in a complex vector space A , such that $f(e) = 0$. As the complex coordinates of a point $x \in G'$ we then take the complex coordinates of the vector $f(x)$ (it is understood that a coordinate system has been fixed once for all in A). A local group G' equipped with a complex coordinate system is said to be a complex local Lie group if the group multiplication is expressed in a complex coordinate system by means of analytic functions of the complex variables. A local isomorphism g of one complex local Lie group G_1' onto another G_2' is said to be an isomorphism between the complex Lie groups if its expression in terms of complex coordinates is given by analytic functions of the complex variables. Thus in a complex

local Lie group the complex coordinates are not to be thought of as fixed but rather as defined only up to an analytic transformation. The subgroups and normal subgroups of a complex local Lie group G' are defined to be those subgroups and normal subgroups of the local group G' that are defined by means of analytic relations on the analytic coordinates, and similarly as regards homomorphisms. Let G' be a complex local Lie group and let $x(t)$ be an arc which, in a complex coordinate system, is defined by the relations $x^i = x^i(t)$; here t denotes a real parameter and $x(0) = e$. Then the components of the tangent vector a to the arc $x(t)$ are defined by

$a^i = \frac{d}{dt} x^i(0)$. In this way there is associated with G' a complex vector space R called the tangent space to G' at e . Just as in Section 52 we may introduce in R a bracket product turning R into a complex Lie algebra. Moreover, all of the constructions of Sections 56-57 go through in the complex case. In particular, for a given complex Lie algebra there always exists a complex local Lie group of which it is the Lie algebra. Note that a complex local Lie group G' may always be viewed as a real local Lie group of double the dimension, which group we may conveniently denote by (G') . If R denotes the complex Lie algebra of G' then (R) is the Lie algebra of (G') . Finally, if G is a global topological group and if there exists in some neighborhood of the identity in G a complex coordinate system with respect to which that neighborhood is a complex local Lie group then G itself is said to be a global complex Lie group.

Just as a real Lie algebra R possesses a complexification $[R]$ so also does a real Lie group G' possess a complexification $[G']$.

H) Let G' be a real local Lie group. Then, as we have seen, G' always admits an analytic coordinate system, i.e., a coordinate system in which the group multiplication $z^i = f^i(x, y) = f^i(x^i, \dots, x^r, y^1, \dots, y^r)$ is given by analytic functions. Moreover, such a coordinate system is clearly unique up to analytic coordinate transformations. Since the functions f^i are analytic we may allow the independent variables to take not only real but also complex values, and once this is done we have a law of multiplication for a complex local Lie group $[G']$ which it is natural to call the complexification of the original group G' . If R is the Lie algebra of G' then $[R]$ is the Lie algebra of $[G']$.

Suppose now that the complex local Lie group $[G']$ is a neighborhood of the identity in some connected and simply connected global complex Lie group which we denote by $[G]$. Then the involutory automorphism ψ of the Lie algebra $([R])$ (see E)) corresponds

to an involutory automorphism φ' of the local Lie group ($[G']$) and according to Theorem 80 φ' possesses a unique extension to an involutory automorphism φ of the simply connected global group $[G]$. Let G denote the set of elements $x \in [G]$ such that $\varphi(x) = x$. Then, as is easily seen, G is a Lie group having Lie algebra R , and it is natural to regard $[G]$ as the complexification of the real global group G . The essential difficulty with this construction is that the global group G cannot be regarded as a global lie group given in advance, since it is defined by means of $[G]$. The question under what conditions a real Lie group G can be imbedded in a complex Lie group has been considered by A.I. Mal'tsev who has shown, in particular, that a simple real Lie group with infinite center cannot be so imbedded.

Example 100: Let R^n be an n -dimensional real vector space and denote by G_k^n the group of all linear automorphisms of R^n that leave invariant a non-degenerate quadratic form $\psi_k(x)$ having $n-k$ positive squares and k negative squares in its canonical form. It is not difficult to verify that G_k^n is a real Lie group. On the other hand, it is quite evident that the complexifications of the groups G_k^n ; $k = 0, 1, \dots, n$ are all isomorphic with one another since, in the complex domain, the distinction between the quadratic forms $\psi_k(x)$, $k = 0, 1, \dots, n$, disappears. In the real domain the groups G_k^n and G_1^n are locally isomorphic when and only when $k = 1$ or $k + 1 = n$, in which case they are in fact isomorphic in the large. Obviously the group G_0^n is not locally isomorphic with any of the groups G_k^n , $0 < k < n$, since the universal covering group of G_0^n is compact (see Example 91) while the groups G_k^n , $0 < k < n$, are not compact.

It is worth noting that G_2^4 is its real form is simple, while, as we have seen (see Example 89), G_0^4 resolves locally into a direct product. Thus the complexification of the simple real group G_2^4 is not simple.

We consider the group G_1^3 in more detail. Let G^* denote the component of the identity in this group. Then G^* consists of the linear transformations in G_1^3 that have positive determinant. Let P denote the collection of lines through the origin in R^3 . Then P forms a projective plane and the equation $\psi_1(x) = 0$ defines a real conic section V in the plane P . Thus to every element of G^* there corresponds a projective transformation of P leaving the conic V invariant. Consequently, G^* is isomorphic with the group of projective transformations of P leaving the curve V invariant. As is well known, the latter group is isomorphic with the group of motions of a non-Euclidean plane, and also with the group of fractional linear transformations.

We observe that, up to local isomorphism, there exist but two three-dimensional simple Lie groups: G_0^3 and G_1^3 , and that the first of these is compact while the second is not. The complexifications of G_0^3 and G_1^3 are locally isomorphic.

SECTION 59

THE CONSTRUCTION OF A GLOBAL LIE GROUP

We here give a construction of a global Lie group having prescribed Lie algebra. The construction rests, to be sure, on Theorem 94, which is not proved in the present book, but, inasmuch as Theorem 94 is of strictly local character, the ideas involved in the construction are of interest anyway. In the event that the Lie algebra is either solvable or has trivial center the construction is independent of Theorem 94.

Let it be noted in advance that some of the following proofs have been so stated as to involve slight inaccuracies. These inaccuracies stem from the fact that in a local group the operation of multiplication is not defined for every pair of elements. As a consequence of this, certain of the constructions introduced below make no sense in the originally given local group and are defined only on some sufficiently small part thereof (see Section 23, G)). If in each such instance I had set forth in detail how to select the appropriate part, and introduced a new symbol to stand for it, the result would have been to obscure the ideas and burden the text with inessential minutiae. In the interests of avoiding pedantry, therefore, I have from time to time permitted myself to speak of the entire local group, when what is really intended is only a suitably chosen part of it.

A) If a local Lie group G' has trivial center than a sufficiently small part of G' can be imbedded in a global Lie group G .

In order to prove this assertion we introduce the adjoint group L' (see Section 54, F)). Since G' has trivial center it follows that the mapping f of G' onto L' acts isomorphically on a suitably chosen part of G' . Let

$$U_1, \dots, U_i, \dots \quad (1)$$

be a complete system of neighborhoods of the identity in L' , and denote by L the set of all finite products of matrices belonging to L' . Clearly L is algebraically a group with respect to matrix multiplication. Moreover, it is easily verified that (1) satisfies

the conditions of Theorem 9 in the algebraic group L' and consequently turns L' into a topological group containing L' as a neighborhood of the identity. Thus L' is imbedded in the global group L and, since G' and L' are locally isomorphic, proposition A) follows.

Lemma: Let G' be a local Lie group and suppose that G' contains a normal subgroup N' and a subgroup H' such that every element $g' \in G'$ can be written in one and only one way in the form $g' = n'h'$ where $n' \in N'$, $h' \in H'$. Suppose, moreover, that N' and H' can be imbedded in global groups N and H , respectively, where both N and H are connected and simply connected. Let G denote the product of the topological spaces N and H . Then it is possible to define in G an operation of multiplication in such a way that G becomes a topological group and such that the mapping χ that associates with each element $g' = n'h' \in G'$ the pair $(n', h') \in G$ is a homomorphism of the local Lie group G' onto a neighborhood of the identity in G which acts isomorphically on a suitably chosen part of G' . Thus G is a connected, simply connected, global Lie group containing a part of G' as a neighborhood of the identity.

Proof: Consider the inner automorphism $\varphi_g^!$ of G' defined by $\varphi_g^!(x) = g'xg'^{-1}$. Since N' is normal $\varphi_g^!$ induces an automorphism of N' which by Theorem 80 possesses a unique extension to an automorphism $\varphi_{g^!}$ of the global group N . In particular, every element $h' \in H'$ defines in this fashion an automorphism $\varphi_{h^!}$.

Denote by L' the set of automorphisms of N of the form $\varphi_{h^!}$, $h' \in H'$, and by K' the set of elements $k' \in H'$ with the property that $\varphi_{k^!}$ is the identity automorphism. The mapping ψ' that associates with each $h' \in H'$ the automorphism $\varphi_{h^!}$ is (algebraically) a homomorphism of H' onto L' and it follows that K' is a normal subgroup of H' . The factor group H'/K' is a local Lie group (see Theorem 63) and is algebraically isomorphic with L' . We employ this algebraic isomorphism to import a topology into L' . Thus L' itself becomes a local Lie group and the mapping ψ' is turned into an open local homomorphism of H' onto L' . Let

$$W_1, \dots, W_n, \dots \quad (2)$$

be a complete system of neighborhoods of the identity in L' and denote by L the set of all finite products of automorphisms belonging to L' . Then L is algebraically a group and, as is easily verified, (2) satisfies the conditions of Theorem 9 so that there exists a unique topology with respect to which L is a topological group having (2) as a complete system of neighborhoods of the

identity. Thus L is turned into a connected global Lie group containing L' as a neighborhood of the identity, and ψ' becomes an open local homomorphism of H onto L . Hence we may use Theorem 80 once again to extend ψ' to a homomorphism ψ of the global group H onto L . In this way there is associated with each $h \in H$ a well defined automorphism $\varphi_h = \psi(h)$ of N .

We now define the product of two pairs (n_1, h_1) and (n_2, h_2) by writing

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2). \quad (3)$$

It is not difficult to show that this definition turns the product G into a topological group.

In the first place, associativity of multiplication is verified by the following computation:

$$\begin{aligned} ((n_1, h_1)(n_2, h_2))(n_3, h_3) &= (n_1 \varphi_{h_1}(n_2), h_1 h_2)(n_3, h_3) \\ &= (n_1 \varphi_{h_1}(n_2) \varphi_{h_1 h_2}(n_3), h_1 h_2 h_3), \\ (n_1, h_1)((n_2, h_2)(n_3, h_3)) &= (n_1, h_1)(n_2 \varphi_{h_2}(n_3), h_2 h_3) = \\ &= (n_1 \varphi_{h_1}(n_2) \varphi_{h_1 h_2}(n_3), h_1 h_2 h_3). \end{aligned}$$

The identity element of G is the pair (e_n, e_h) where e_n and e_h are the identities of N and H respectively. Finally, the pair inverse to (n, h) is easily seen to be $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Indeed

$$(n, h)(\varphi_{h^{-1}}(n^{-1}), h^{-1}) = (n \varphi_{h h^{-1}}(n^{-1}), h h^{-1}) = (e_n, e_h).$$

Thus G is a group.

The essential step in showing that G is a topological group is to verify that $\varphi_h(n) \in N$ depends continuously on both $n \in N$ and $h \in H$. Let U and V be neighborhoods of the identity in N' and H' such that $VUV^{-1} \subset N'$. Then for $n \in U$, $h \in V$ we have $\varphi_h(n) = hn h^{-1}$ so that $\varphi_h(n)$ is clearly continuous in both variables on this set. Next let $h \in V$ and let n denote an arbitrary but fixed element of N . Since N is connected we have $n = n_1 \dots n_k$ where $n_i \in U$, $i = 1, \dots, k$ (see Theorem 14) so that

$$\varphi_h(n) = \varphi_h(n_1) \dots \varphi_h(n_k).$$

Since each $\varphi_h(n_i)$ is a continuous function of h and since multiplication is continuous in N it follows that $\varphi_h(n)$ is also a continuous function of h . Moreover, if $h \in V$ and n is a variable element of N we may write $n = n^*n'$ where n^* is fixed while $n' \in U$. Then

$\varphi_h(n) = \varphi_h(n^*)\varphi_h(n')$, whence it follows that $\varphi_h(n)$ depends continuously on both h and n for $h \in V$, $n \in N$. Finally, if $h \in H$ and $n \in N$ we may write $h = h^*h'$ where h^* is fixed while $h' \in V$. Then $\varphi_h(n) = \varphi_{h^*}(\varphi_{h'}(n))$ and since $\varphi_{h'}(n)$ depends continuously on both variables h' and n while $\varphi_{h^*}(n)$ is a continuous function of n it follows that $\varphi_h(n)$ is a continuous function of both h and n .

It is now a simple matter to see that products and inverses are continuous in G . Indeed, from what has been said it follows that $n_1\varphi_{h_1}(n_2)$ is a continuous function of n_1 , h_1 and n_2 , and since h_1h_2 is certainly a continuous function of h_1 and h_2 it follows that the product (3) is a continuous function on $G \times G$. Similarly, the element $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$ inverse to (n, h) depends continuously on (n, h) . Thus G is a topological group.

It remains to show that the mapping χ is isomorphic on a suitably chosen part of the local group G' . Let $g_1 = n_1h_1$ and $g_2 = n_2h_2$ be two elements of G' . Then

$$g_1g_2 = n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = (n_1\varphi_{h_1}(n_2))(h_1h_2).$$

On the other hand, according to (3), the product in G of the pairs (n_1, h_1) , (n_2, h_2) is the pair $(n_1\varphi_{h_1}(n_2), h_1h_2)$. This shows that χ is homomorphic, and since it is clear that χ is homeomorphism the proof of the lemma is complete.

We first apply the lemma to construct a global Lie group having a given solvable Lie algebra.

Theorem 95. Let R be a solvable real Lie algebra. Then there exists a connected, simply connected, global Lie group G whose Lie algebra is isomorphic with R . G is homeomorphic with Euclidean space, i.e., admits a global Cartesian coordinate system x^1, \dots, x^r . Moreover, among all such Cartesian coordinate systems there exists one with the following properties:
 1) multiplication is expressed in it by means of analytic functions defined on the entire group G ; 2) if $g_i(t)$ denotes the point with all coordinates zero except the i -th, whose value is t , then $g_i(t)$ is a one-parameter subgroup of G and t^1, \dots, t^r are the coordinates of the point $g_1(t^1)\dots g_r(t^r)$. Finally, if H_i denotes the collection of all points of the form $g_1(t^1) \dots g_i(t^i)$ then H_i is a subgroup of G and a normal subgroup of H_{i+1} .

Proof: Using the solvability of R it is not difficult to construct an increasing sequence of subalgebras

$$S_1, \dots, S_r = R,$$

where each S_i is of dimension i and is an ideal in S_{i+1} . Let G' be the local Lie group with Lie algebra R and let H'_i be the subgroup of G' corresponding to S_i (see Theorems 89 and 90). The theorem is certainly valid for the one-dimensional algebra S_1 . Suppose it holds for S_i , and select in H'_{i+1} a one-parameter subgroup $\{g'_{i+1}(t)\} = K'_{i+1}$ not lying in H'_i . Then $H'_i K'_{i+1} = H'_{i+1}$ while the intersection $H'_i \cap K'_{i+1}$ contains only the identity. Moreover, H'_i is a normal subgroup of H'_{i+1} since S_i is an ideal in S_{i+1} (see Theorem 91). Thus we may apply the above lemma; the global group H_i exists by the inductive hypothesis, while K'_{i+1} , being a one-parameter group, may also be imbedded in a global one-parameter group $K_{i+1} = \{g_{i+1}(t)\}$. The elements of the global group H_{i+1} are represented as pairs $(h_i, g_{i+1}(t))$ where $h_i \in H_i$, the inductive step is taken, and Theorem 95 follows. As for the analyticity of multiplication, this follows immediately from the fact that every automorphism of H_i generated by an element $g_{i+1}(t)$ has analytic expression in coordinate form.

Theorem 96: For any real Lie algebra R there exists a global Lie group G having R for its Lie algebra. (The proof uses Theorem 94 which we here assume without proof.)

Proof: Let G' be the local Lie group having Lie algebra R (see Theorem 89). According to Theorem 94, R contains a maximal solvable ideal S and a semi-simple subalgebra T such that $S \cap T = \{0\}$ and $S + T = R$. Let N' and H' be the subgroups of G' corresponding to S and T , respectively (see Theorem 90). Then N' is normal in G , while $N' \cap H' = \{e\}$ and $N'H' = G'$. Since N' has the solvable algebra S for its Lie algebra, it follows from Theorem 95 that N' may be imbedded in a connected, simply connected, global group N . Since H' has the semi-simple Lie algebra T it follows, in particular, that H' has trivial center, and consequently H' may also be imbedded in a connected, global group H^* (see A)). But then the universal covering group $\tilde{H}^* = H$ is a connected and simply connected Lie group which contains H' as a local group. Thus, we are once again, in a position to apply the above lemma, and the theorem follows.

Theorem 97: Let G be a connected, simply connected, global Lie group and let N' be a local normal subgroup of G . Then a suitably chosen part of N' is contained, as a neighborhood of the identity, in a global normal subgroup of G . (The analogous assertion for local subgroups H' which are not normal is false; see Example 99.)

Proof: Let G' be a neighborhood of the identity in G sufficiently small so that N' is a normal subgroup of the local group G' . The factor group $G'/N' = H'$ is a local Lie group and, according to Theorem 96, may be imbedded in a connected, simply connected, global Lie group K . The natural projection f' of G' onto K' is then an open local homomorphism of G onto K and, since G is simply connected, may be extended to a homomorphism f of the entire group G onto K (see Theorem 80). Let N denote the kernel of f . It is not difficult to verify that N is an extension of a part of the local group N' .

It is clear that Theorem 97 need not hold if G is not simply connected (see Example 98). The normal subgroup N constructed in the proof of Theorem 97 was shown by A. I. Mal'cev [32] to be simply connected. That N is connected follows easily from the assumed simple connectedness of K .

Example 101. The methods employed in proving the lemma of the present paragraph may also be used to construct examples of Lie groups.

Let N be an r -dimensional Euclidean space considered as an additive vector group, and let H denote the group of all rotations of N . Then with each element $x \in H$ there is associated a rotation φ_x of N and φ_x is an automorphism of N considered as a vector group. We construct a group G , consisting of the pairs of the form (n, h) , $n \in N$, $h \in H$, with multiplication defined by

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2).$$

It is not difficult to verify that G is a Lie group containing N as a normal subgroup and H as a subgroup. If R is the Lie algebra of G and $N \rightarrow S$, $H \rightarrow T$ then, for $r \geq 3$, S is the maximal solvable ideal of R and T is a semi-simple subalgebra (see Theorem 94).

The same technique may be used to show that an arbitrary Lie group N can be imbedded in a larger group G in such a way that every automorphism of N is induced by an inner automorphism of G .

SECTION 60

LOCAL LIE GROUPS OF TRANSFORMATIONS

As has already been noted, Lie groups first made their appearance in the guise of groups of continuous transformations; indeed, the first and second theorems of Lie were stated and proved by Sophus Lie with reference to transformation groups,

and the formulations of these theorems in Section 56 are quite different from the original versions. For the sake of completeness I here present the first and second theorems of Lie (see (7) and (8)), as well as the converses (see Theorem 98), in a form that is close to the original.

In a local investigation, and the classical theory was local in nature, the functions studied are ordinarily not defined for all values of the variables under consideration, but in each case on one or another open set. Consequently, an accurate statement of results would require a series of provisos indicating in every case the domain of definition of the functions involved. We here omit these provisos in view of the fact that it is not difficult to determine in each case on precisely what small domain one or another function is defined.

Definition 50: Let G be an r -dimensional local Lie group and let Γ be an open set in an n -dimensional Euclidean space A . We suppose that to each element $x \in G$ there corresponds a homomorphism φ_x of Γ onto an open set in A in such a way that φ_x depends continuously on x . If $\xi \in \Gamma$ is mapped by φ_x into $\eta \in A$ we write

$$\eta = \varphi_x(\xi) = \varphi(\xi, x) . \quad (1)$$

Under these circumstances we shall say that G is a local Lie group of transformations acting on Γ provided the following conditions are satisfied:

a) The mapping associated with the identity e of G is the identity mapping

$$\varphi_e(\xi) = \xi$$

of Γ onto itself and, moreover,

$$\varphi_x(\varphi_y(\xi)) = \varphi_{xy}(\xi) , \quad (3)$$

i.e., the product of the transformations corresponds to the product of the group elements.

b) The transformations φ_x and φ_y coincide when and only when $x = y$. Another way of formulating this requirement is to demand that φ_x should be the identity map only in the event that x is the identity of G .

c) In coordinate form $\varphi(\xi, x)$ is a (sufficiently many times) continuously differentiable function of the coordinates of ξ and x .

We remark that in terms of coordinates (1) assumes the form
 $\eta^i = \varphi_x^i(\xi) = \varphi^i(\xi, x) = \varphi^i(\xi^1, \dots, \xi^n, x^1, \dots, x^r),$
 $i = 1, \dots, n.$ (4)

A) Let G be a group of transformations acting on the domain Γ and let $x(t)$ be an arc in G with direction vector a . Then for fixed ξ the point $\varphi(\xi, x(t))$ describes an arc on the manifold Γ . The tangent vector to this arc at $t = 0$ is independent of $x(t)$ and is uniquely determined by a ; we denote it by $\psi(\xi, a)$. In coordinate form

$$\psi^i(\xi, a) = \lambda_a^i(\xi) a^\alpha = \lambda_a^i(\xi^1, \dots, \xi^n) a^\alpha, \quad (5)$$

where

$$\lambda_j^i(\xi) = \frac{\partial \varphi^i(\xi, x)}{\partial x^j} \quad \text{at } x = e \quad (6)$$

(see (4)). The function $\eta = \varphi(\xi, x)$, considered as a function of x with ξ held fixed, satisfies the system of differential equations:

$$\frac{\partial \eta^i}{\partial x^j} = \lambda_a^i(\eta) v_j^\alpha(x), \quad (7)$$

where $v_j^\alpha(x)$ are the auxiliary functions of G (see Section 56, A)). Finally, the integrability conditions for (7) may be written in the form

$$\frac{\partial \lambda_j^i(\eta)}{\partial \eta^\alpha} \lambda_k^\alpha(\eta) - \frac{\partial \lambda_k^i(\eta)}{\partial \eta^\alpha} \lambda_j^\alpha(\eta) = c_{jk}^\beta \lambda_\beta^i(\eta), \quad (8)$$

where c_{jk}^β are the structure constants of G .

Proof: Differentiating (4) with respect to t along the arc $x = x(t)$ we obtain

$$\frac{d\varphi^i(\xi, x)}{dt} = \frac{\partial \varphi^i(\xi, x)}{\partial x^\alpha} \frac{dx^\alpha}{dt}.$$

But then evaluation at $t = 0$ yields (5). In order to verify (7) we introduce, as in Section 56 (see Section 56, A)), the element $p = (x + \delta x)x^{-1}$. From (1) and (3) we have

$$\varphi(\xi, x + \delta x) = \varphi(\eta, p)$$

whence (7) follows by passing from finite increments to the derivative.

Finally the integrability conditions for (7) as set forth in Theorem 85 read:

$$\begin{aligned} \frac{\partial \lambda_\alpha^i(\eta)}{\partial \eta^\gamma} v_j^\alpha(x) \lambda_\beta^\gamma(\eta) v_k^\beta(x) - \frac{\partial \lambda_\beta^i(\eta)}{\partial \eta^\gamma} v_k^\beta(x) \lambda_\alpha^\gamma(\eta) v_j^\alpha(x) \\ + \lambda_\delta^i(\eta) \left(\frac{\partial v_j^\delta(x)}{\partial x^k} - \frac{\partial v_k^\delta(x)}{\partial x^j} \right) = 0. \end{aligned}$$

Employing (8), Section 56, we rewrite this condition as:

$$\left(\frac{\partial \lambda_\alpha^i(\eta)}{\partial \eta^\gamma} \lambda_\beta^\gamma(\eta) - \frac{\partial \lambda_\beta^i(\eta)}{\partial \eta^\gamma} \lambda_\alpha^\gamma(\eta) - \lambda_\delta^i(\eta) c_{\alpha\beta}^\delta \right) v_j^\alpha(x) v_k^\beta(x) = 0. \quad (9)$$

But now, since the matrix $\|v_j^\alpha(x)\|$ is non-singular, (8) and (9) are equivalent.

B) Let G be a local Lie group of continuous transformations acting on an open set Γ , and let R be the Lie algebra of G . In A) we associated with each vector $a \in R$ a vector field $\psi(\xi, a)$ defined on Γ . Let P denote the family of vector fields $\psi(\xi, a)$. From (5) it follows that if α and β are real numbers then

$$\psi(\xi, \alpha a + \beta b) = \alpha \psi(\xi, a) + \beta \psi(\xi, b). \quad (10)$$

Accordingly, for any pair of vector fields $\lambda, \mu \in P$ the vector field $\alpha \lambda + \beta \mu$ also belongs to P , i.e., P is a real vector space. We also define in P the commutator of the vector fields $\lambda = \lambda(\xi)$ and $\mu = \mu(\xi)$, by writing

$$[\lambda(\xi, \mu(\xi))]^i = \frac{\partial \lambda^i(\xi)}{\partial \xi^\gamma} \mu^\gamma(\xi) - \frac{\partial \mu^i(\xi)}{\partial \xi^\gamma} \lambda^\gamma(\xi). \quad (11)$$

It turns out that in terms of this definition the following relation holds:

$$[\psi(\xi, a), \psi(\xi, b)] = \psi(\xi, [a, b]). \quad (12)$$

In particular, if $\lambda, \mu \in P$ then $[\lambda, \mu] \in P$. Moreover, (10) and (12) together show that the mapping ψ that associates with each vector $a \in R$ the corresponding vector field $\psi(\xi, a) \in P$ preserves both linear operations and the bracket product. But then the bracket product defined in P must satisfy the requirements of Definition

48, i.e., P is a Lie algebra and ψ is a homomorphism of R onto P . Finally, it turns out that ψ is not only homomorphic but is, in fact, an isomorphism. The Lie algebra P will be called a Lie algebra of transformations on Γ .

As has already been noted, (10) is an immediate consequence of (5). In order to prove (12), multiply both members of (8) by $a_j b^k$ and sum over j and k . That the resulting relation is precisely (12) may be seen by referring once more to (5).

It only remains to prove that ψ is an isomorphism, and to this end it suffices to show that the dimension of P , considered as a vector space, is equal to the dimension r of R . Denote by $\lambda_k(\xi)$ the vector field with components $\lambda_k^1(\xi), \dots, \lambda_k^n(\xi)$. According to (5) the vector fields

$$\lambda_k(\xi), \quad k = 1, \dots, r, \quad (13)$$

form a system of generators in P . Thus it suffices to show that the vector fields (13) are linearly independent, i.e., that a linear combination of them with constant coefficients is the zero vector field only when the coefficients vanish.

Consider now an arbitrary vector $a \in R$ and let $x(t)$ be a one-parameter subgroup in G having direction vector a . Substituting $x(t)$ for x in (7), multiplying by $\frac{dx^j(t)}{dt}$, and summing over j , we obtain (see Section 56, (9))

$$\frac{d\eta^i}{dt} = \lambda_a^i(\eta) v_j^\alpha(x(t)) \frac{dx^j(t)}{dt} = \lambda_a^i(\eta) a^\alpha. \quad (14)$$

Let a^1, \dots, a^r be any system of scalars such that $a^k \lambda_k(\xi) = 0$. Then, taking for a in (14) the vector with components a^k , we have

$$\frac{d\eta^i}{dt} \equiv 0$$

so that $\eta = \varphi(\xi, x(t))$ is independent of t and consequently $\eta = \varphi(\xi, x(t)) = \xi$ for all t . Since this holds for every $\xi \in \Gamma$ it follows that $x(t)$ acts as the identity transformation on Γ . But then, by Definition 50 (b), $x(t) = e$ and consequently $a = 0$. Thus the vector fields (13) are linearly independent, and the proof of B) is complete.

The following theorem constitutes the converse of both A) and B).

Theorem 98: Let Γ be an open set in n -dimensional Euclidean

space and suppose given an r -dimensional real linear space P of vector fields defined on Γ . The linearity of P means that along with any pair of vector fields $\lambda(\xi) \in P$ and $\mu(\xi) \in P$ the vector field $\alpha\lambda(\xi) + \beta\mu(\xi)$ also belongs to P , where α and β denote arbitrary real numbers. Moreover, let the commutator of a pair of vector fields belonging to P be defined by

$$[\lambda(\xi), \mu(\xi)]^i = \frac{\partial \lambda^i(\xi)}{\partial \xi^\gamma} \mu^\gamma(\xi) - \frac{\partial \mu^i(\xi)}{\partial \xi^\gamma} \lambda^\gamma(\xi), \quad (15)$$

and suppose that, along with every pair of vector fields λ and μ , P also contains the vector field $[\lambda, \mu]$. If these conditions are satisfied we say that P is a Lie algebra of transformations on Γ . Then there exists one and only one local Lie group G of continuous transformations acting on Γ (in the sense of A)) and possessing the property that the corresponding Lie algebra of transformations (in the sense of B)) coincides with the given algebra P .

Proof: Observe first of all that if λ, μ, ν are any three vector fields then

$$[\lambda, \mu] + [\mu, \lambda] = 0, \quad (16)$$

$$[\lambda, [\mu, \nu]] + [\mu, [\nu, \lambda]] + [\nu, [\lambda, \mu]] = 0. \quad (17)$$

In both cases the verification consists of a direct calculation based on Definition (15).

Now select in P a linearly independent system of vector fields $\lambda_k(\xi)$, $k = 1, \dots, r$; that such a system exists and forms a basis in P follows from the assumption that P has dimension r . Then we have

$$[\lambda_j(\xi), \lambda_k(\xi)] = c_{jk}^\gamma \lambda_\gamma(\xi), \quad (18)$$

where, because of (16) and (17), the coefficients c_{jk}^i satisfy the characteristic identities for a system of structure constants (see Section 52, (11), (12)). Hence, according to Theorem 88, there exists a local Lie group G having the structure constants c_{jk}^i . Let $v_j^i(x)$ denote the auxiliary functions of G and consider the system of equations

$$\frac{\partial \eta^i}{\partial x^j} = \lambda_\alpha^i(y) v_j^\alpha(x). \quad (19)$$

This system is of exactly the same form as the system (7)

considered in A), where it was shown that the integrability conditions are given by (8). But (18) is just another way of writing (8). Thus the system (19) is integrable. Denote by $\varphi(\xi, x)$ the solution of (19) satisfying the initial condition

$$\varphi(\xi, e) = \xi \quad (20)$$

In this way we associate with each $x \in G$ a transformation φ_x of the manifold Γ which carries the point $\xi \in \Gamma$ into the point $\eta = \varphi_x(\xi) = \varphi(\xi, x) \in \Gamma$. We shall show that conditions a) and b) of Definition 50 are satisfied.

Let x and y be elements of G and let

$$f = xy, \quad \eta = \varphi(\xi, y), \quad \xi^* = \varphi(\eta, x), \quad \zeta = \varphi(\xi, f).$$

In order to verify a) we must show that $\xi^* = \zeta$. The verification will be carried out as usual, by showing that ξ^* and ζ , considered as functions of x , with y held constant, satisfy one and the same system of differential equations as well as the same initial condition, namely $\xi^* = \zeta = \eta$ for $x = e$.

According to (19) we have

$$\frac{\partial \xi^{*i}}{\partial x_j} = \lambda_\alpha^i(\xi^*) v_j^\alpha(x). \quad (21)$$

Let $\|u_j^i(x)\|$ be the matrix inverse to $\|v_j^\alpha(x)\|$. Then (6), Section 56, assumes the form

$$\frac{\partial f^\alpha}{\partial x_j} = u_\beta^\alpha(f) v_j^\beta(x), \quad (22)$$

whence it follows that

$$\frac{\partial \xi^i}{\partial x_j} = \frac{\partial \xi^i}{\partial f^\alpha} \frac{\partial f^\alpha}{\partial x_j} = \lambda_\gamma^i(\xi) v_\alpha^\gamma(f) u_\beta^\alpha(f) v_j^\beta(x) = \lambda_\alpha^i(\xi) v_j^\alpha(x). \quad (23)$$

But (21) and (23) coincide. Thus $\xi^* = \zeta$, and a) is verified

The proof of b) is by contradiction and consists in reversing the argument employed in B). Suppose b) fails. There then exists a non-trivial normal subgroup N of G consisting of elements corresponding to the identity transformation of Γ . Hence there must also exist a one-parameter subgroup $x(t)$ lying in N and having direction vector $a \neq 0$. Substituting $x(t)$ for x in (9), multiplying by $\frac{dx^i(t)}{dt}$, and summing over j we obtain:

$$\frac{d\eta^i}{dt} = \lambda_{\alpha}^i(\eta) v_{\beta}^{\alpha}(x(t)) \frac{dx^{\beta}(t)}{dt} = \lambda_{\alpha}^i(\eta) a^{\alpha} \quad (24)$$

(see Section 56, (9)). But, now, by hypothesis $\eta(t) = \varphi(\xi, x(t))$ is identically equal to ξ , and consequently the left member of (24) vanishes identically. Thus

$$\lambda_{\alpha}^i(\xi) a^{\alpha} = 0,$$

which contradicts the assumed linear independence of the vector fields $\lambda_k(\xi)$, $k = 1, \dots, r$.

The validity of condition c) is automatic since the function $\varphi(\xi, x)$ was obtained by integrating a system of differential equations.

Clearly the Lie algebra of transformations on Γ belonging to the group G in the sense of A) is precisely the given algebra P . Finally, in order to see that G is unique, we observe that the transformation φ_x is uniquely determined by the initial value problem (19, 20), while the auxiliary functions $v_j^i(x)$ appearing in (19) are, in a canonical coordinate system of the first kind, uniquely determined by the structure constants of the Lie algebra P .

In conclusion we shall take a closer look at transitive local Lie groups of transformations. For such groups it is possible to obtain results analogous to those of Section 24. We here state these results, in somewhat abbreviated form and without proof, in order to draw attention to the essential differences between the local and global theories.

C) Let G be a transitive Lie group of transformations acting on an open set Γ . Transitivity of the local group is here to be understood as follows: for every point $\xi \in \Gamma$ there exists a neighborhood $U \subset \Gamma$ of ξ such that if $\eta \in U$ there exists a transformation φ_x , $x \in G$, satisfying the condition $\varphi_x(\xi) = \eta$. Let α denote a fixed point in Γ and denote by K_{α} the set of all elements $x \in G$ for which $\varphi_x(\alpha) = \alpha$. Then $K_{\alpha} = H$ is a subgroup of the local group G which contains no non-trivial normal subgroup, and each K_{α} is a left coset of H in G . Conversely, if K is any left coset of H in G then all of the transformations φ_x , $x \in K$, carry the point α into one and the same point of Γ . In this way the study of a transitive local Lie group of transformations reduces to the study of a pair G, H , where G is a local Lie group and H a subgroup containing no non-trivial normal subgroup. The study of such a pair G, H is in its turn equivalent with the study of a pair R, S , where R is a real Lie algebra while S is a subalgebra containing no non-trivial ideal. Given any such pair R, S , it is possible to construct

a local pair G, H and thence an open set Γ on which G acts by defining Γ to be the space G/H of left cosets.

It turns out, however, to be impossible in general to imbed the local Lie group G in a global group G^* in such a way that the local subgroup H becomes a part of a global subgroup H^* (see Example 103). Thus there obtains here an even greater difference between the local and global theories than in the case of Lie groups themselves, where for a given Lie algebra it was at least possible to construct a global group.

Example 102: Let G be a local Lie group of linear automorphisms of a vector space Γ . The Lie algebra R of G consists then of all linear transformations of Γ into itself that are tangent to arcs lying in G (see Section 54, B)), i.e., that are defined by the formula

$$a = \frac{d}{dt} \varphi_{x(0)}. \quad (25)$$

In coordinate form the transformation φ_x may be written

$$\eta^j = \varphi_{x^j}(x) \xi^i. \quad (26)$$

Suppose now that $x(t)$ is an arc with tangent vector a . Substituting $x(t)$ for x in (26) and differentiating with respect to t at $t = 0$ we obtain

$$\psi^j(\xi, a) = a_i \xi^i \quad (27)$$

(see A)). Thus to every element $a = \|a_i^j\| \in R$ there corresponds the vector field $\psi(\xi, a)$ defined by

$$\psi(\xi, a) = a(\xi). \quad (28)$$

Example 103: In Example 99 there was constructed a simply connected global Lie group $G \times G$ and a one-dimensional local subgroup H' such that H' was not contained in any one-dimensional global subgroup of $G \times G$. According to Theorem 97 it follows that H' cannot be normal in $G \times G$ and, being one-dimensional, can contain no non-trivial local subgroup. Let G' be any neighborhood of the identity in $G \times G$. Then the pair G', H' determines, as in C), a certain transitive local group of transformations. However, it is impossible to extend this group to a group of transformations in the large, for H' cannot be imbedded in a global one-dimensional subgroup of $G \times G$.

11

THE STRUCTURE OF COMPACT LIE GROUPS

The present chapter is devoted to a very thorough investigation of compact Lie groups and culminates in their complete classification. The first point in the program is to obtain a necessary and sufficient condition in order that a given real Lie algebra R should be the Lie algebra of a compact Lie group. It turns out that the desired criterion consists in the existence on the vector space of the Lie algebra of a scalar product (u, v) which turns it into a Euclidean space and is invariant with respect to the adjoint group (see Section 54, F)). Invariance with respect to the adjoint group amounts to the condition

$$([x, u], v) + (u, [x, v]) = 0; \quad x \in R, \quad u \in R, \quad v \in R. \quad (1)$$

Such a Lie algebra will, throughout the chapter, be called a compact Lie algebra. It will be shown that a compact Lie algebra R resolves into the direct sum of its center R_0 , which coincides with its maximal solvable ideal, and a compact semi-simple algebra R' which, in its turn, resolves into the direct sum of certain uniquely determined compact non-commutative simple algebras R_1, \dots, R_k . This result, whose proof is entirely elementary, reduces the problem of classifying all compact Lie algebras to the problem of classifying the simple compact algebras.

A basic tool in the entire investigation is the introduction, on an arbitrary Lie algebra R , of a uniquely determined scalar product (u, v) . This goes as follows: if u and v are elements of R then (u, v) is defined to be the trace of the linear transformation $-p_u p_v$,

$$(u, v) = -\text{Tr}(p_u p_v), \quad (2)$$

where p_u denotes the inner derivation $p_u(x) = [u, x]$ (see Section 54, E)). An elementary argument shows that a real Lie

algebra R is compact and semi-simple when and only when the scalar product (2) turns R into a Euclidean space, i.e., is positive definite. Since this scalar product is automatically invariant with respect to all the automorphisms of R , it follows that the group G_A of all automorphisms of a compact-semi simple Lie algebra R is a compact Lie group. Now it is a remarkable but elementary fact that the Lie algebra of G_A is isomorphic with the original compact semi-simple algebra R . Thus, without getting outside of the circle of ideas of Section 54, we obtain a straightforward proof of the existence of a global compact Lie group having given compact semi-simple Lie algebra. This is the content of Section 61.

There arises the natural, and also extremely important, question: can a compact Lie algebra be the Lie algebra of a non-compact connected Lie group or, what comes to the same thing, can two connected Lie groups be locally isomorphic if one of them is compact and the other is not? Clearly the answer is yes if the compact algebra R has non-trivial center. It is a deep and important theorem, due to Weyl, that any connected, in particular any simply connected, Lie group \tilde{G} having compact and semi-simple Lie algebra R must be itself compact. Since the center Z of \tilde{G} is finite there exist but a finite number of connected groups locally isomorphic with \tilde{G} . This result of Weyl's will be proved in Section 64 after sufficient information concerning compact semi-simple Lie algebras has been obtained in Sections 62 and 63.

As was already indicated in Section 58, it is customary to obtain the classification of real semi-simple Lie algebras by giving a preliminary classification of complex semi-simple algebras and then determining all the real forms of the latter. In this context it is noteworthy that a complex semi-simple Lie algebra admits one and, up to isomorphism, only one real form which is compact. Now the problem of finding the real forms of all complex semi-simple Lie algebras is very complicated and was solved by Cartan (see [9]) by means of some delicate geometric constructions that find no natural place even in a very thorough treatment of Lie groups. Thus the usual practice in developing the theory of Lie groups is to give only the classification of complex Lie algebras and to omit the discussion of their real forms. However, this contributes nothing to the theory of topological groups, for the classification of complex Lie algebras leads to no classification of groups. Accordingly, I shall here take a diffent course, employing the method of root systems developed by Weyl in his study of complex semi-simple Lie algebras (see [57]). The method

will not be developed in its most general form, however, but only with a view to its application to real compact semi-simple Lie algebras. Under these conditions Weyl's method simplifies somewhat since, thanks to the presence of an invariant positive definite quadratic form on a compact algebra, it suffices to exploit the theory of elementary divisors for skew-symmetric matrices only. In this somewhat abbreviated treatment Weyl's method gains in simplicity and elegance while losing one of its principal features. Thus we obtain a classification of compact semi-simple Lie algebras and thence, directly, a classification of compact Lie groups.

The final classification theorem reads as follows: every compact simple non-commutative Lie algebra is either isomorphic with one of the algebras of four infinite series of classical algebras

$$A_n, n \geq 1; \quad B_n, n \geq 2; \quad C_n, n \geq 3; \quad D_n, n \geq 4, \quad (3)$$

or else with one of five exceptional algebras

$$G_2, F_4, E_6, E_7, E_8. \quad (4)$$

Moreover, no two of the algebras (3), (4) are isomorphic with one another.

This result is originally due to Killing (see [25]). Cartan (see [8]) filled some essential gaps in Killing's proof. As has already been observed, Killing and Cartan both dealt with complex Lie algebras.

One lacuna in the present discussion is the absence of a complete description of the five exceptional algebras, and consequently of a proof of their existence. We construct only the root systems of these algebras, which serves to settle the question of their uniqueness. A detailed description of the exceptional algebras themselves would require a massive amount of computation, while the method of their construction from their root systems is quite clear.

We continued to employ in this chapter the summation conventions of the tensor notation.

SECTION 61. COMPACT LIE ALGEBRAS

A Lie algebra isomorphic with the Lie algebra of a compact Lie group will, in the sequel, be said to be compact. We here establish a necessary and sufficient condition for a given Lie algebra to be compact. In order to formulate this condition, we

first introduce the concept of an invariant quadratic form on a Lie algebra. Let R be a Lie algebra and let $\psi(u, u)$ be a quadratic form defined on the vector space R . Then ψ is said to be invariant if it is invariant with respect to an arbitrary transformation belonging to the adjoint group L (see Section 54, F)), i.e., if for $l \in L$ we have $\psi(l(u), l(u)) = \psi(u, u)$. It will be shown that a Lie algebra is compact when and only when there exists on it an invariant positive definite quadratic form. Because of the existence of such a form, a compact Lie algebra may be resolved into the direct sum of its center R_0 and compact semi-simple algebra R' . The latter resolves, in its turn, into the direct sum of compact non-commutative simple algebras. Thus the problem of classifying compact Lie algebras is reduced to the classification of the compact simple algebras.

In the present section it will also be shown that the group G_A of all automorphisms of a compact semi-simple Lie algebra R has for its Lie algebra the algebra R itself. This automatically settles in the affirmative the question of the existence of a global Lie group having given compact semi-simple Lie algebra. Since a semi-simple Lie algebra has trivial center the uniqueness of the corresponding local group follows from the results of Section 54 (see Section 54, G)). In this way the existence (in the large), as well as the uniqueness, of a Lie group having given compact semi-simple Lie algebra is established without any appeal to the results of Sections 55, 56. Obviously a Lie group may possess a compact Lie algebra without being itself compact; consider, for example, the vector groups, the Lie algebras of which are commutative and therefore compact. This is not the case, however, with compact semi-simple algebras. Indeed, an arbitrary connected Lie group having compact semi-simple Lie algebra must itself be compact. This important result of Weyl's will be proved in Section 64.

The bracket operation $[a, b]$ in a Lie algebra has certain features reminiscent of the familiar operation of vector multiplication. It turns out that every Lie algebra also admits, in a natural way, a scalar product (a, b) , i.e., a symmetric bilinear form. This scalar product is invariant not only with respect to the adjoint group but with respect to all automorphisms of the Lie algebra and plays a very important role. In terms of the scalar product we may formulate (Definition 49) the well-known criteria of Cartan for the semi-simplicity and solvability of a Lie algebra. A Lie algebra is semi-simple when and only when the quadratic form of its scalar product is non-degenerate; a Lie algebra is solvable when and only when $(a, a) = 0$ for every $a \in [R, R]$.

These criteria will be obtained here only for compact Lie algebras, where they follow immediately from Theorem 101, which states that the subspace of degeneracy of the scalar product is precisely the center in the case of a compact Lie algebra, and that in a compact semi-simple algebra the quadratic form of the scalar product is positive definite. This last fact, when applied to the complexification of a compact Lie algebra, leads to a certain simplification of the entire process of classifying the complex simple algebras. These matters will be taken up in Section 62.

A) Let R be a real Lie algebra and let L denote the adjoint group of R (see Section 54, F)). A symmetric bilinear form $\psi(u, v)$, $u, v \in R$, defined on R will be said to be invariant with respect to L or, simply, invariant, if

$$\psi(l(u), l(v)) = \psi(u, v)$$

holds for every $l \in L$. Similarly, the associated quadratic form $\psi(u, u)$ is invariant with respect to the adjoint group or, simply, invariant if

$$\psi(l(u), l(u)) = \psi(u, u)$$

holds for arbitrary $l \in L$. A symmetric bilinear form is uniquely determined by its quadratic form, and conversely, and it follows that the invariance of either of the forms implies the invariance of the other. A bilinear form $\psi(u, v)$ is invariant when and only when the identity

$$\psi([a, u], v) + \psi(u, [a, v]) = 0 \quad (1)$$

holds for arbitrary $a \in R$.

Only the latter assertion requires proof. Let G be the local Lie group corresponding to R , and let $l(t) = l_t$ be a one-parameter subgroup of the local group L having direction vector p_a . From the invariance of $\psi(u, v)$ it follows that

$$\psi(l_t(u), l_t(v)) = \psi(u, v).$$

Differentiating this relation with respect to t at $t = 0$ we obtain $\psi(p_a(u), v) + \psi(u, p_a(v)) = 0$, which is equivalent with (1). Suppose, on the other hand, that (1) holds and consider the function $\psi(l_t(u), l_t(v))$.

By virtue of (3) Section 54 and F) Section 54 we have

$$\frac{d}{dt} l_t(u) = [a, l_t(u)]; \quad \frac{d}{dt} l_t(v) = [a, l_t(v)].$$

$$\text{Thus } \frac{d}{dt} \psi(l_t(u), l_t(v)) = \psi([a, l_t(u)], l_t(v)) \\ + \psi(l_t(u), [a, l_t(v)]) = 0$$

by (1). Consequently, $\psi(l_t(u), l_t(v))$ is independent of t . But then $\psi(u, v)$ is invariant, for there exists a one-paramenter subgroup passing through any point of the local group L .

The following theorem establishes a characteristic property of compact Lie algebras that greatly simplifies their study.

Theorem 99: Every compact Lie algebra admits a positive definite quadratic form invariant with respect to the adjoint group.

Proof: Let G be a compact group having Lie algebra R , and let $\varphi(u, u)$ be any positive definite quadratic form on R . We define $\varphi_x(u, u) = \varphi(l_x(u), l_x(u))$, $x \in G$ (see Section 54, F)). For fixed $x \in G$ the function $\varphi_x(u, u)$, considered as a function of the vector $u \in R$, is a positive definite quadratic form, while for fixed vector $u \neq 0$ the function $\varphi_x(u, u)$, considered as a function of $x \in G$, is easily seen to be a continuous real-valued function on G that takes only positive values. It follows that the function $\psi(u, u)$ defined by

$$\psi(u, u) = \int \varphi_x(u, u) dx$$

(see Section 29) is a positive definite quadratic form. That this form is also invariant with respect to L may be seen as follows. Let $y \in G$. Then

$$\begin{aligned} \psi(l_y(u), l_y(u)) &= \int \varphi(l_{xy}(u), l_{xy}(u)) dx = \int \varphi(l_x(u), l_x(u)) dx \\ &= \psi(u, u). \end{aligned}$$

Thus the proof of Theorem 99 is complete.

B) If R is a real Lie algebra admitting an invariant positive definite quadratic form then every ideal S in R is a direct summand, i. e., there exists in R a complementary ideal T such that $S \cap T = \{0\}$, $S + T = R$.

Proof: Let $\psi(u, u)$ be an invariant positive definite quadratic form on R . For any ideal S we denote by T the orthogonal complement of the subspace S with respect to the metric defined on R by the bilinear form $\psi(u, v)$. In other words, T consists of all vectors $v \in R$ such that $\psi(u, v) = 0$ for every $u \in S$. The relations $S \cap T = \{0\}$, $S + T = R$ are then clear, and it only remains to show that T is an ideal. To this end let $a \in R$, $v \in T$, and let u be an arbitrary element of S . According to (1) we have

$$\psi(u, [a, v]) = -\psi([a, u], v) = 0$$

since $[a, u] \in S$. But this says $[a, v] \in T$ and consequently T is an ideal.

Theorem 100: Let R be any real Lie algebra admitting an invariant positive definite quadratic form. Then R resolves into the direct sum of its center R_0 and a finite number of simple non-commutative algebras R_1, \dots, R_k . This resolution is unique, i.e., the ideals R_0, R_1, \dots, R_k are uniquely determined by R . The center R_0 is the maximal solvable ideal in R .

Proof: Note first that if a bilinear form is invariant on the Lie algebra R then it is also invariant on every subalgebra R' .

According to B), R resolves into the direct sum of its center R_0 and a complementary ideal T . Clearly T has trivial center. Since T also admits an invariant positive definite quadratic form, the results of B) can be applied once more to it. Thus, unless T is already simple, it resolves into the direct sum of two ideals; continuing this process sufficiently often, we obtain a resolution of R into the direct sum of ideals R_0, R_1, \dots, R_k where R_1, \dots, R_k are simple and non-commutative Lie algebras, for if one of the ideals R_i , $i > 0$, were commutative then the ideal $R_0 + R_i$ would be central in R , which is impossible.

In order to verify the uniqueness of this resolution, suppose given a similar resolution of R into the direct sum of ideals R_0, R'_1, \dots, R'_k and let $a \in R'_i$, $i \geq 1$. Since R'_i has trivial center there exists an element $b \in R'_i$ such that $[a, b] \neq 0$. Let now

$$b = b_0 + b_1 + \dots + b_k$$

be the resolution of b along the ideals R_0, R_1, \dots, R_k , so that $b_i \in R_i$, $i \geq 0$. Then $[a, b_0] = 0$ and there exists an index $j \geq 1$ such that $c = [a, b_j] \neq 0$. Since c is contained in both R'_i and R_j it follows that the intersection $R'_i \cap R_j$ is not trivial. But this intersection is also an ideal, and since R'_i and R_j are both simple it follows that $R'_i = R_j$. In other words, every ideal R'_i , $i \geq 1$ coincides with one of the ideals R_j , $j \geq 1$. Similarly, every ideal R_m , $m \geq 1$, coincides with one of the ideals R_n , $n \geq 1$. Thus, the sequence of ideals R'_1, \dots, R'_k is just a reordering of the sequence R_1, \dots, R_k .

Finally, we show that $S = R_0$ where S denotes the maximal solvable ideal in R . In the first place R_0 is solvable whence it follows that $R_0 \subset S$. Suppose $R_0 \neq S$. Then there exists an element $s \in S \setminus R_0$. Since s is not central it must fail to commute with some element of one of the subalgebras R_1, \dots, R_k ; suppose $a \in R_i$, $i \geq 1$, and $c = [s, a] \neq 0$. Then $c \in R_i \cap S$ so that $R_i \cap S \neq \{0\}$, and since R_i is simple we have $R_i \subset S$. But then R_i , being a subalgebra of a solvable algebra, must be solvable. Thus R_i is simultaneously simple and solvable, which can only happen if R_i is one-dimensional and commutative. But this is impossible since, by hypothesis, R_i is not commutative. Thus $R_0 = S$ and Theorem 100 is proved.

We turn now to the construction on an arbitrary Lie algebra

R of the scalar product, a symmetric bilinear form (u, v) , $u \in R$, $v \in R$, that is invariant with respect to all the automorphisms of R . This scalar product plays a major role in the theory of Lie algebras.

Recall that if R is a vector space and p a linear transformation of R into itself, then the trace $\text{Tr}(p)$ is defined by $\text{Tr}(p) = p_a^a$, where $\|p_j^i\|$ is a matrix representing p in some fixed coordinate system. It is readily verified that the trace $\text{Tr}(p)$, while defined in terms of a coordinate system, is in fact independent of that coordinate system and is uniquely determined by p . Moreover, it is easy to see that the trace $\text{Tr}(p_1 p_2)$ of the product of two linear transformations p_1 and p_2 is independent of the order of the product:

$$\text{Tr}(p_1 p_2) = \text{Tr}(p_2 p_1) \quad (2)$$

(see Section 31).

C) The scalar product (a, b) of two elements $a, b \in R$, is defined to be

$$(a, b) = -\text{Tr}(p_a p_b). \quad (3)$$

It is easy to see that, according to this definition, (a, b) is a symmetric bilinear form on R . In terms of a coordinate system we have (see Section 52, (17))

$$(a, b) = -c_{\alpha j}^i c_{\beta i}^j a^\alpha b^\beta. \quad (4)$$

Moreover, it follows from (15) Section 54 that for an arbitrary automorphism of the Lie algebra R we have

$$(\varphi(a), \varphi(b)) = (a, b). \quad (5)$$

In particular, the scalar product is an invariant bilinear form and consequently, for any three elements, a , u and v belonging to R , the following relation holds:

$$([a, u], v) + (u, [a, v]) = 0. \quad (6)$$

D) Let $\psi(u, u)$ be any invariant positive definite quadratic form defined on a real Lie algebra R , and select in R a coordinate system with respect to which

$$\psi(u, u) = u^1 u^1 + \dots + u^r u^r. \quad (7)$$

Let c_{jk}^i be the structure constants of R in this coordinate system. We shall write

$$c_{ijk} = c_{jk}^i \quad (8)$$

It turns out that the structure constants c_{ijk} are skew-symmetric in each pair of indices, i.e.,

$$c_{ijk} = c_{jki} = c_{kij} = -c_{jik} = -c_{kji} = -c_{ikj}. \quad (9)$$

Indeed, writing (6) in coordinate form, we obtain

$$0 = c_{ijk} a^j u^k v^i + c_{ikj} u^i a^j v^k = a^j u^k v^i (c_{ijk} + c_{kji})$$

Thus $c_{ijk} = -c_{kji}$, and from this and the basic skew-symmetry (see Section 52, (18)) of any set of structure constants (9) follows at once.

Theorem 101: Let R be any real Lie algebra admitting an invariant positive definite quadratic form. Then the center of R is precisely the collection R_0 of all elements of R that are orthogonal to R in the sense of the scalar product defined in C). Moreover, if R_0 is trivial then the quadratic form (u, u) of the scalar product is itself an invariant positive definite quadratic form.

Proof: Let $\psi(u, u)$ be an invariant positive definite quadratic form on R and choose a coordinate system with respect to which (7) holds. In terms of these coordinates the quadratic form (a, a) of the scalar product may be written

$$\begin{aligned} (a, a) &= - \sum_{i,j} c_{i\alpha j} c_{j\beta i} a^\alpha a^\beta = \sum_{i,j} (c_{i\alpha j} a^\alpha) (c_{j\beta i} a^\beta) \\ &= \sum_{i,j} (c_{i\alpha j} a^\alpha)^2 \end{aligned} \tag{10}$$

(see (4) and (9)). Since the right member is a sum of squares, it follows that for arbitrary $a \in R_0$ we have

$$c_{i\alpha j} a^\alpha = 0$$

But then $[a, b]^i = c_{\alpha j}^i a^\alpha b^j = (c_{i\alpha j} a^\alpha) b^j = 0$ and consequently $[a, b] = 0$ for every $b \in R$, i.e., a belongs to the center of R . Conversely, if a is central then $p_a = 0$ so that $(a, b) = -\text{Tr}(p_a p_b) = 0$ for arbitrary $b \in R$. Thus R_0 is precisely the center. Moreover, if R_0 is trivial then (10) shows that the quadratic form (a, a) is positive definite.

Theorem 102: Let R be a real Lie algebra on which the quadratic form of the scalar product is positive definite. Then the Lie group G_A of automorphisms of R is compact and its Lie algebra R_A coincides with the adjoint algebra P of R . Since, according to Theorem 101, R has trivial center, R and P are isomorphic. Finally, if G denotes the component of the identity in G_A then neither G nor G_A contains any central element other than e .

We observe that this result is obtained without appealing to the theorem (Theorem 88) which asserts that every real Lie algebra is the Lie algebra of a local group. Thus Theorem 102

provides a straightforward, independent proof of the existence, in the large, of a Lie group having prescribed Lie algebra provided the quadratic form of the scalar product of that algebra is positive definite.

Proof: Denote by G^* the group of all linear automorphisms of the vector space R that leave invariant the scalar product (u, v) defined in C). Since (u, u) is, by hypothesis, a positive definite form, it follows that G^* is isomorphic with the group of orthogonal matrices of order equal to the dimension of R , and consequently that G^* is compact. Since the group G_A of automorphisms of R is a subgroup G^* , it follows that G_A is also compact. In order to see that the Lie algebra R_A of G_A coincides with P , we observe that P is an ideal in R_A (see Section 54, E)) and therefore a direct summand in R_A , since R_A is the Lie algebra of a compact group (see Theorem 99 and B)). Thus R_A resolves into the direct sum of P and a complementary ideal Q . In order to prove $P = R_A$ it suffices to show that Q is trivial. But suppose $q \in Q$. Then $[q, p_a] = 0$ whence, by (14) Section 54, we have $p_{q(a)} = 0$. Thus $q(a)$ belongs to the center of R and since R has trivial center it follows that $q(a) = 0$. Since this holds for arbitrary $a \in R$ we have $q = 0$.

It remains to show that G_A and G have trivial center. Suppose that φ is a central element of either G_A or G , let a be an arbitrary element of R , and let $x(t)$ be an arc in G with tangent vector p_a . Then $\varphi x(t) \varphi^{-1} = x(t)$ and, differentiating this relation with respect to t at $t = 0$, we obtain $\varphi p_a \varphi^{-1} = p_a$ which, by virtue of (15) Section 54, implies $p_{\varphi(a)} = p_a$, i.e., $\varphi(a) = a$. Since a is arbitrary, φ is the identity automorphism. Thus the proof of Theorem 102 is complete.

Theorem 103: A Lie algebra is compact if and only if it admits a positive definite quadratic form which is invariant with respect to the adjoint group.

Proof: The necessity of the condition was proved in Theorem 99. Suppose the Lie algebra R admits an invariant positive definite quadratic form. We must show there exists a compact Lie group whose Lie algebra is isomorphic with R . By Theorem 100, R resolves into the direct sum of its center R_0 and a complementary semi-simple ideal R' . Thus it suffices to show that R_0 and R' individually are isomorphic with the Lie algebras of suitable compact groups G_0 and G' (see Section 53, F)).

Now the commutative part R_0 offers little difficulty; if s is the dimension of R_0 we simply take for G_0 an s -dimensional torus,

i. e., the product of s copies of the additive group of real numbers reduced modulo 1 (see Example 86.) The semi-simple part offers even less difficulty; according to Theorem 102 we may take for G' the group of all automorphisms of R' itself.

As an immediate consequence of Theorems 99, 100, 101 and 103 we obtain the following proposition.

E) A real Lie algebra is both compact and semi-simple when and only when the quadratic form of its scalar product is positive definite.

The following sections are devoted to the further study of compact semi-simple algebras.

As has been noted, Theorem 102 implies the existence of a global Lie group having prescribed compact semi-simple Lie algebra. The following uniqueness theorem for this special case is also obtained without recourse to the results of Section 56.

F) Let R be a compact semi-simple Lie algebra, and let G be the component of the identity in the group G_A of all automorphisms of R . According to Theorem 102, G is a compact Lie group with trivial center whose Lie algebra is isomorphic with given algebra R . If G' is any Lie group whose Lie algebra is isomorphic with R then G' is locally isomorphic with G ; moreover, if G' is a connected global group having trivial center then it is, in fact, isomorphic with G .

Proposition F) is an immediate consequence of G) Section 54, and the results of Chapter 9.

Example 104: Let R denote a three-dimensional Euclidean space. As has already been observed, by taking as the commutator $[a, b]$ of two vectors in R the ordinary vector product, we turn R into a Lie algebra. A simple computation shows that the scalar product (a, b) in this Lie algebra is given in coordinate form by the formula $(a, b) = 2(a^1 b^1 + a^2 b^2 + a^3 b^3)$, i. e., just twice the ordinary scalar product. In particular, the scalar product has positive definite quadratic form, whence it follows that R is semi-simple and compact. According to Theorem 101, R resolves into the direct sum of simple non-commutative algebras and, since a one-dimensional algebra is necessarily commutative, it follows that R itself is simple. Let G_A denote the group of all automorphisms of R . Since an automorphism preserves the scalar product it follows that G_A consists exclusively of orthogonal transformations of the vector space R . Moreover, it is clear that the orthogonal transformations with positive determinant preserve the vector

product, while those with negative determinant do not. Thus G_A is just the group of all rotations of R . From Theorem 102 we obtain once again (see Example 93) the fact that the Lie algebra R_A of the group G_A is isomorphic with R .

SECTION 62

ROOT SYSTEMS OF COMPACT SEMI-SIMPLE LIE ALGEBRAS

In the present section we introduce the concept of a root system, a concrete, geometric invariant of a compact semi-simple Lie algebra R that determines the algebra uniquely up to isomorphism. A general outline of the construction of the root system is as follows. Let $a \in R$ and let p_a be the corresponding element of the adjoint algebra, i.e., the linear transformation $p_a(x) = [a, x]$. Since $[a, a] = 0$ we see that p_a always has zero as an eigenvalue. The multiplicity of the eigenvalue zero depends on a ; the minimal value n of this multiplicity is called the rank of R , and every element $c \in R$ for which p_c has zero as an eigenvalue of multiplicity n is called a regular element of R . In order to construct a root system one fixes a regular element $c \in R$. Then the set S of those $x \in R$ such that $[c, x] = 0$ forms an n -dimensional commutative subalgebra of R , a so-called regular subalgebra. It turns out that all the linear transformations p_s , $s \in S$, possess common eigenvectors and that the eigenvalues of these transformations are pure imaginary linear forms in the vector s . Now S is a Euclidean space with respect to the scalar product defined on R (Section 61, C)), and it follows that a real linear form on S may be written as a scalar product (α, s) where α is a vector in S uniquely attached to the linear form. In particular, the eigenvalues of p_s are of the form $i(\alpha, s)$ where α denotes a uniquely determined vector called a root vector. The collection of all root vectors $\alpha \in S$ forms a root system Σ of R . According to this construction, the root system depends on the choice of a regular element c . It turns out, however, that any two root systems of the same compact semi-simple algebra are isometric with one another. This will be proved in Section 64. Moreover, whenever two compact semi-simple algebras have isometric root systems, the algebras themselves are isomorphic. This will be proved in Section 63.

In the present section we consider only Lie algebras R that are compact and semi-simple, i.e., algebras with the property that the quadratic form of the scalar product is positive definite. This hypothesis is to be understood as being in force even when it is not

expressly stipulated.

Since the eigenvalues of the transformations p_α are pure imaginary, we shall need to employ the complexification [R] of the real vector space R (see Section 58, C)). If φ is a linear form defined on R then φ may be extended to [R] by writing $\varphi(x + iy) = \varphi(x) + i\varphi(y)$. Similarly, if p is a linear transformation of R into itself then p may be extended to [R] by writing $p(x + iy) = p(x) + ip(y)$, and a bilinear form $\psi(x_1, x_2)$ on R may be extended to [R] according to the formula $\psi(x_1 + iy_1, x_2 + iy_2) = \psi(x_1, x_2) - \psi(y_1, y_2) + i\psi(x_1, y_2) + i\psi(y_1, x_2)$. Note that if the quadratic form $\psi(x, x)$ is positive definite on R then the Hermitian extension $\psi(z, \bar{z})$ is positive definite on [R].

We here recall briefly the notions of eigenvalue and eigenvector of a linear transformation. If R is a vector space over an arbitrary field K and p is a linear transformation of R into itself, then an element $\lambda \in K$ is said to be an eigenvalue of p if there exists a vector $x \in R$, $x \neq 0$, such that

$$p(x) = \lambda x. \quad (1)$$

A vector $x \neq 0$ satisfying (1) is an eigenvector of p associated with the eigenvalue λ . If $\|p_j^i\|$ is the matrix representing p with respect to some basis in R then (1) has the coordinate expression

$$p_{\alpha}^{-1}x^\alpha = \lambda x^i. \quad (2)$$

Thus $\lambda \in K$ is an eigenvalue when and only when λ satisfies the equation

$$\chi(\lambda, p) = 0 \quad (3)$$

where $\chi(\lambda, p)$ denotes the characteristic polynomial of p defined by the formula

$$\chi(\lambda, p) = |\lambda \delta_j^i - p_j^i|. \quad (4)$$

A) Let R be a Euclidean space. A linear transformation p of R into itself is said to be skew-symmetric if

$$(p(u), v) + (u, p(v)) = 0; \quad u \in R, v \in R. \quad (5)$$

The eigenvalues of a skew-symmetric transformation are pure imaginary.

Indeed let p be skew-symmetric and let λ be an eigenvalue of p. Then there exists a non-zero vector $z \in [R]$ such that

$$p(z) = \lambda z. \quad (6)$$

But then also

$$p(\bar{z}) = \bar{\lambda} \bar{z}. \quad (7)$$

Forming the scalar product of (6) with \bar{z} , the scalar product of (7) with z , and adding the results we obtain

$$0 = (\lambda + \bar{\lambda})(z, \bar{z}).$$

and since $(z, \bar{z}) \neq 0$ it follows that $\lambda = -\bar{\lambda}$, i.e., λ is pure imaginary.

B) Let Q be a commutative, linear Lie algebra (see Section 54, A)) of skew-symmetric transformations of a Euclidean vector space A into itself and denote by A_0' the collection of all vectors $x \in A$ satisfying the condition $q(x) = 0$ for all $q \in Q$. If φ is a linear form on the vector space Q we write A_φ for the collection of all vectors $x \in [A]$ satisfying the condition $q(x) = \varphi(q)x$ for every $q \in Q$. Clearly A_0' is a subspace of A while A_φ is a subspace of $[A]$. Moreover, it is easy to see that for the linear form 0 we have $A_0 = [A_0']$. If A_φ is non-trivial then φ will be said to be an eigenform of Q , and the space A_φ the eigenspace associated with φ . It turns out that all eigenforms of Q are pure imaginary and that, along with each eigenform φ , the linear form $-\varphi$ is also an eigenform satisfying $A_{-\varphi} = \bar{A}_\varphi$. Finally, $[A]$ is the direct sum of its eigenspaces, i.e., of the subspaces $A_{\varphi_0}, A_{\varphi_1}, \dots, A_{\varphi_k}$, where $\varphi_0, \varphi_1, \dots, \varphi_k$ is a complete list of eigenforms of Q .

Proof: It may easily be verified that if B is a subspace of A invariant with respect to Q , i.e., with respect to all the transformations belonging to Q , then the orthogonal complement of B is also invariant with respect to Q . Let Q' be a subalgebra of Q , let φ' be an eigenform of the algebra Q' , and let $A_{\varphi'}$ denote the eigenspace in $[A]$ corresponding to φ' . We shall show that $A_{\varphi'}$ is, in fact, invariant with respect to Q . Indeed, let $x \in A_{\varphi'}, y = q(x)$, $q \in Q$, and denote by a q' an arbitrary element of Q' . Then

$$q'(y) = q'(q(x)) = qq'(x) = q(\varphi'(q')x) = \varphi'(q')q(x) = \varphi'(q')y.$$

Thus $y \in A_{\varphi'}$, and the invariance of $A_{\varphi'}$ with respect to Q is proved.

We show next that Q possesses at least one eigenform. The proof is by induction on the dimension of Q . In the case of the zero-dimensional algebra the validity of the assertion is clear. Suppose the assertion proved for all commutative algebras of dimension less than that of Q . We may resolve Q into the direct sum of a subalgebra Q' and one-dimensional algebra Q'' with basis vector q'' . By the inductive hypothesis Q' possesses an eigenform φ' . Let $A_{\varphi'}$ be the eigenspace associated with this form. Then

A_φ , is invariant with respect to Q and therefore, in particular, with respect to q'' . Let x be an eigenvector of q'' belonging to A_φ and associated with some eigenvalue λ . Any element $q \in Q$ may be written uniquely as $q = q' + \nu q''$ where $q' \in Q'$ while ν is a real number. Consequently we may define $\varphi(q) = \varphi'(q') + \nu\lambda$. The mapping φ thus defined is a linear form on Q , and since $q(x) = q'(x) + \nu q''(x) = \varphi'(q')x + \nu\lambda x = \varphi(q)x$, we see that φ is, in fact, an eigenform of Q .

That the eigenforms of the algebra Q are all pure imaginary is easily seen. Indeed, if φ is an eigenform and $q \in Q$ then $\varphi(q)$ is an eigenvalue of the skew-symmetric transformation q and is therefore pure imaginary by A). Also, if the non-zero vector $x \in [A]$ satisfies the condition $q(x) = \varphi(q)x$ then \bar{x} clearly satisfies the condition $q(\bar{x}) = -\varphi(q)\bar{x}$, so that $-\varphi$ is an eigenform along with φ and $A_{-\varphi} = \bar{A}_\varphi$.

We show next that $[A]$ resolves into the direct sum of subspace $A_{\varphi_0}, \dots, A_{\varphi_k}$ where $\varphi_0, \dots, \varphi_k$ are eigenforms of Q . The proof is again by induction, this time on the dimension of A . The assertion is clearly valid if A is one-dimensional. Suppose the assertion true for all commutative linear Lie algebras of skew-symmetric transformations on Euclidean spaces of dimension less than that of A . As we have seen, Q possesses at least one eigenform φ_0 . Let A_{φ_0} be the corresponding eigenspace. Then A_{φ_0} and $A_{-\varphi_0}$ are both invariant with respect to Q and consequently the sum $A_{\varphi_0} + A_{-\varphi_0}$ is invariant. Since $A_{-\varphi_0} = \bar{A}_{\varphi_0}$ it follows that $A_{\varphi_0} + A_{-\varphi_0} = [B]$ where B is a subspace of A which is also invariant with respect to Q . Let C denote the orthogonal complement of B in A . Then C is likewise invariant and since C has dimension less than that of A it follows from the inductive hypothesis that $[C]$ resolves into the direct sum of eigenspaces $C_{\psi_1}, \dots, C_{\psi_l}$, where ψ_1, \dots, ψ_l are eigenforms of Q regarded as an algebra on C . It is easily seen that these forms are distinct from φ_0 and $-\varphi_0$, whence it follows that $C_{\psi_1}, \dots, C_{\psi_l}$ are eigenspaces in $[A]$, and that $[A]$ is the direct sum of the spaces $A_{\varphi_0}, A_{-\varphi_0}, C_{\psi_1}, \dots, C_{\psi_l}$.

We complete the proof of B) by showing that if $[A]$ is the direct sum of subspaces $A_{\varphi_0}, \dots, A_{\varphi_k}$, where $\varphi_0, \dots, \varphi_k$ are eigenforms of Q , then the list $\varphi_0, \dots, \varphi_k$ must exhaust the set of all eigenforms of Q . Indeed suppose φ_{k+1} is an eigenform of Q distinct from the forms $\varphi_0, \dots, \varphi_k$. There exists an element $q \in Q$ such that the numbers $\varphi_0(q), \dots, \varphi_{k+1}(q)$ are not all the same. Let x_{k+1} be an eigenvector associated with the form φ_{k+1} .

Then $x_0 + x_1 + \dots + x_{k+1} = 0$ where $x_i \in A_{\varphi_i}$, $i = 0, \dots, k$. Applying the transformation q we obtain

$$\sum_{i=0}^{k+1} \varphi_i(q) x_i = 0.$$

But this, along with $x_0 + x_1 + \dots + x_{k+1} = 0$, yields a non-trivial relation among the vectors x_0, \dots, x_k , which is impossible. Thus the proof of B) is complete.

C) Let q_0 be a skew-symmetric transformation of a Euclidean space A into itself. For any eigenvalue λ_i of q_0 denote by A_{λ_i} the collection of all vectors $x \in [A]$ for which $q_0(x) = \lambda_i x$. Then the dimension of A_{λ_i} is precisely the multiplicity of $\lambda = \lambda_i$ as a root of the characteristic equation $\chi(\lambda, q_0) = 0$.

Indeed, denote by Q the set of all linear transformations of the form νq_0 where ν is a real number. Then $A_{\lambda_i} = A_{\varphi_i}$ where $\varphi_i(q) = \varphi_i(\nu q_0) = \nu \lambda_i$, and it follows from B) that $[A]$ is the direct sum of the subspaces $A_{\lambda_0}, \dots, A_{\lambda_k}$ where $\lambda_0, \dots, \lambda_k$ is the set of all eigenvalues of q_0 . But then, choosing a basis in each of the subspaces A_{λ_i} , and uniting these partial bases, we obtain a basis in $[A]$ with respect to which the matrix of q_0 is diagonal, and it follows at once that $\chi(\lambda, q_0) = (\lambda - \lambda_0)^{n_0} \dots (\lambda - \lambda_k)^{n_k}$ where n_i denotes the dimension of A_{λ_i} .

Theorem 104. Let R be a compact semi-simple Lie algebra, let $a \in R$ and denote by S_a the collection of elements $x \in R$ satisfying the condition $[a, x] = 0$. Then S_a is a non-trivial subalgebra of R , the dimension of which depends on a . The minimum value n of this dimension is called the rank of R . If S_c has dimension n then S_c is said to be a regular subalgebra of R , and c is said to be a regular element. A regular subalgebra is commutative.

Proof: There are two things to settle: that each S_a is a subalgebra, and that if S_c is regular then it is necessarily commutative. The first assertion is a straightforward consequence of the Jacobi identity (see Section 52, (16)); indeed, if $x, y \in S_a$ then

$$[a, [x, y]] = [[a, x], y] + [x, [a, y]] = 0$$

so that $[x, y] \in S_a$.

The second part of the proof is considerably more difficult. We begin by observing that the inner derivations p of R , i.e., the transformations belonging to the adjoint algebra, are all skew-symmetric with respect to the scalar product of R . Indeed, this is just another way of saying that the scalar product is invariant (see Section 61, (6)). If r denotes the dimension of R then it is

easily seen that the characteristic polynomial $\chi(\lambda, p_a)$ of p_a , when computed in terms of any coordinate system in R , is a homogeneous polynomial of degree r in the indeterminants λ, a^1, \dots, a^r where a^1, \dots, a^r are the components of a (see (4)). Thus if $\chi(\lambda, p_a)$ is written as a polynomial in λ then the coefficient of λ^k , which we denote by $\chi_{r-k}(a)$, and which depends upon a but not upon the choice of the coordinate system, is itself a homogeneous polynomial of degree $r - k$ in a^1, \dots, a^r . Moreover, since $p_a(a) = [a, a] = 0$ the characteristic polynomial always has $\lambda = 0$ as a zero at least once, i.e., the constant term $\chi_r(a)$ vanishes identically. Thus we may write

$$\chi(\lambda, p_a) = \lambda^r + \chi_1(a)\lambda^{r-1} + \dots + \chi_{r-n}(a)\lambda^n, \quad n > 0 \quad (8)$$

where $\chi_{r-n}(a)$ does not vanish identically. Now S_a and $[S_a]$ have the same dimension, and the latter subspace is the eigenspace of p_a (on the complexification $[R]$) associated with the eigenvalue zero. Thus it follows from C) that the dimension of S_a is precisely the multiplicity of $\lambda = 0$ as a zero of $\chi(\lambda, p_a)$ and consequently that this dimension takes on its minimum at a vector $a = c$ if and only if

$$\chi_{r-n}(c) \neq 0. \quad (9)$$

In other words, a subalgebra $S = S_c$ is regular if and only if c satisfies (9); we must show that such a subalgebra S is commutative.

Let T denote the orthogonal complement of S in R . Since S is a subalgebra we have $p_s(S) \subset S$ for every $s \in S$ and, from this and the skew-symmetry of p_s , it follows that $p_s(T) \subset T$ also. Thus R resolves orthogonally into the direct sum of the subspaces S and T , each of which is invariant with respect to S . Let p_s' and p_s'' denote the linear transformations induced on S and T , respectively, by p_s . Then we have

$$\chi(\lambda, p_s) = \chi(\lambda, p_s') \chi(\lambda, p_s'') \quad (10)$$

as may be seen by referring p_s to an orthonormal basis in R , the first n vectors of which form a basis in the subspace S .

We show next that

$$\chi(\lambda, p_s') = \lambda^n \quad (11)$$

for every $s \in S$. Note, first of all, that, if s^1, \dots, s^n are the components of s with respect to any coordinate system in S , then $\chi(\lambda, p_s')$ and $\chi(\lambda, p_s'')$ are homogeneous polynomials of degree n and $r - n$, respectively, in the indeterminants λ, s^1, \dots, s^n . In particular, when $\chi(\lambda, p_s')$ and $\chi(\lambda, p_s'')$ are written as polynomials in λ the coefficients are all homogeneous polynomials in

s^1, \dots, s^n . Now S is the subspace consisting of those vectors $x \in R$ such that $p_c(x) = 0$, whence it follows that $c \in S$ and also that

$$\chi(\lambda, p_c') = \lambda^n. \quad (12)$$

From (9), (10), and (12) we see that $\chi(\lambda, p_s'')$ does not have $\lambda = 0$ as a zero. But then, since the coefficients of $\chi(\lambda, p_s'')$ are continuous functions of s , the same must be true for all vectors $b \in S$ sufficiently close to c . Thus, in some neighborhood of c (relative to S) the multiplicity of $\lambda = 0$ as a zero of $\chi(\lambda, p_s')$ is entirely accounted for by the factor $\chi(\lambda, p_s')$ and since this multiplicity can never fall below n , while the degree of $\chi(\lambda, p_s')$ in λ is precisely n , we see that (11) is valid in a neighborhood of c . But the coefficients of $\chi(\lambda, p_s')$ are polynomials in the coordinates of s , and if they vanish on an open set they must vanish identically. Thus (11) holds for all $s \in S$.

It is now a simple matter to complete the proof. Indeed, according to C), (11) implies that the entire subalgebra S is in the null space of p_s for every $s \in S$. Thus if $s, s' \in S$ then $[s, s'] = p_s(s') = 0$, i. e., S is commutative.

Definition 51: Let R be a compact semi-simple Lie algebra, let S be a regular subalgebra of R (see Theorem 104) and denote by Q the collection of all linear transformations on R of the form p_s , $s \in S$. Then Q is a commutative linear Lie algebra of skew-symmetric transformations of R into itself and the results of B) are valid. Among the eigenforms of Q we have the zero form with corresponding eigenspace $[S]$. Let $\varphi_0 = 0, \varphi_1, \dots, \varphi_k$ be a list of all the eigenforms of Q . Since p_s depends linearly on s , these forms are also pure imaginary linear forms on S . Thus for each j there exists a unique vector $\alpha_j \in S$ such that

$$\varphi_j(p_s) = i(\alpha_j, s). \quad (13)$$

The following notation and terminology will be employed: the eigenspace R_{φ_j} will be denoted by R_{α_j} ; the full set of vectors $\alpha_0 = 0, \alpha_1, \dots, \alpha_k$ will be denoted by Δ ; the deleted set $\alpha_1, \dots, \alpha_k$ will be denoted by Σ . The vectors $\alpha_1, \dots, \alpha_k$ are root vectors of R , the collection Σ of root vectors is a root system, and the spaces R_{α_i} , $i = 1, \dots, k$, are root spaces. From B) it follows that, along with each root vector $\alpha \in \Sigma$, the negative vector $-\alpha$ is also a root vector, that

$$R_{-\alpha} = \bar{R}_\alpha, \quad (14)$$

and that the complexification $[R]$ resolves into the direct sum of the subspaces $[S], R_{\alpha_1}, \dots, R_{\alpha_k}$. According to (13) we have

$$[s, x] = i(\alpha_j, s)x; \quad x \in R_{\alpha_j}, \quad s \in S. \quad (15)$$

Moreover, it turns out that if $x \in R_{\alpha_\mu}$, $y \in R_{\alpha_\nu}$; $\mu, \nu = 0, 1, \dots, k$, then

$$[s, y] \in R_{\alpha_\mu + \alpha_\nu}; \quad (16)$$

here it is to be understood that $R_{\alpha_\mu + \alpha_\nu}$ denotes the trivial subspace $\{0\}$ in the event that $\alpha_\mu + \alpha_\nu \notin \Delta$.

The only thing requiring proof is (16). To verify this we note that

$$\begin{aligned} p_s([x, y]) &= [p_s(x), y] + [x, p_s(y)] = i(\alpha_\mu, s)[x, y] \\ &\quad + i(a, s)[x, y] = (\varphi_\mu(p_s) + \varphi_\nu(p_s))[x, y]. \end{aligned}$$

In other words $[x, y] \in R_{\varphi_\mu + \varphi_\nu}$, and (16) follows.

D) Let $x \in R_\alpha$, $y \in R_{-\alpha}$, $\alpha \in \Sigma$; then

$$[x, y] = i(x, y)\alpha. \quad (17)$$

Indeed, by the invariance of the scalar product ((6) Section 61), we have $([x, y], s) + (y, [x, s]) = 0$ or, in other words,

$$([x, y], s) = (y, [s, x]) = i(\alpha, s)(x, y) = (i(x, y)\alpha, s)$$

(see (15)). Since this is valid for all $s \in S$, while, by (16), $[x, y]$ is itself and element of $[S]$, it follows that (17) holds.

Theorem 105. Let R be a compact semi-simple Lie algebra and let Σ be a root system for R . Then, in the notation of Definition 51: a) For each $\alpha \in \Sigma$ the root space R_α is a one-dimensional complex vector space. b) If $\alpha \in \Sigma$ then an integral multiple $j\alpha$ of α belongs to Σ when and only when $j = \pm 1$. c) Let α, β be any two vectors belonging to Σ and consider vectors of the form $\beta + j\alpha$ where j denotes an integer. Define l to be the maximum integer such that all vectors $\beta - j\alpha$ belong to Δ for $j = 0, 1, \dots, l$. Analogously, define m to be the maximum integer such that all vectors $\beta + j\alpha$ belong to Δ for $j = 0, 1, \dots, m$. Then

$$l - m = \frac{2(\alpha, \beta)}{(\alpha, \alpha)}. \quad (18)$$

Moreover, if $(x, \bar{x}) = 1$, $x \in R_\alpha$, $y \in R_\beta$, then

$$[\bar{x}, [x, y]] = -\frac{m(1+1)}{2} (\alpha, \beta) y. \quad (19)$$

d) If α and β are two vectors belonging to Σ such that $\alpha + \beta \in \Sigma$ and if x and y are non-zero vectors belonging to the root spaces R_α , R_β , respectively, then $[x, y]$ is a non-zero vector belonging to $R_{\alpha+\beta}$.

Proof: Before launching into the proof of the theorem, we introduce the following preliminary construction. Let

$$\lambda, \alpha \in \Sigma, u \in R_\lambda, x \in R_\alpha, u \neq 0, (x, \bar{x}) = 1, [x, u] = 0, \quad (20)$$

and form the sequence

$$\begin{aligned} u_0 &= u \in R_\lambda, u_1 = [x, u_0] \in R_{\lambda+\alpha}, \dots, \\ u_j &= [x, u_{j-1}] \in R_{\lambda+j\alpha}, \dots. \end{aligned} \quad (21)$$

We shall show that

$$[\bar{x}, u_j] = (j(\lambda, \alpha) + \frac{j(j-1)}{2} (\alpha, \alpha)) u_{j-1}. \quad (22)$$

The proof is by induction. For $j = 0$ (22) is valid in the sense that the coefficient in the right member is zero while the left member vanishes by hypothesis. Suppose (22) holds for $j = t$ and let $j = t + 1$. Using the skew-symmetry of commutators and the Jacobi identity (Section 52, (15), (16)) we have

$$[\bar{x}, u_{t+1}] = [\bar{x}, [x, u_t]] = -[[x, \bar{x}], u_t] + [x, [\bar{x}, u_t]]. \quad (23)$$

Now $[x, \bar{x}] = i\alpha$ by (17) and (20), while, since $\alpha \in S$, (15) says that $[\alpha, u_t] = i(\lambda + t\alpha, \alpha) u_t$. Thus

$$-[[x, \bar{x}], u_t] = -i[\alpha, u_t] = ((\lambda, \alpha) + t(\alpha, \alpha)) u_t. \quad (24)$$

Moreover, according to (20) and the inductive hypothesis, we have

$$\begin{aligned} [x, [\bar{x}, u_t]] &= t(\lambda, \alpha) + \frac{t(t-1)}{2} (\alpha, \alpha) [x, u_{t-1}] = \\ &= t(\lambda, \alpha) + \frac{t(t-1)}{2} (\alpha, \alpha) u_t. \end{aligned} \quad (25)$$

Finally, from (23), (24), (25) we obtain (22) for the case $j = t + 1$. Thus (22) holds for all j .

Observe that, since u_j belongs to $R_{\lambda+j\alpha}$, and the number of subspaces R_γ , $\gamma \in \Delta$, is finite, there exists an index $g \geq 0$ such that $u_g \neq 0$, $u_{g+1} = 0$. Substituting $j = g + 1$ in (22) we obtain

$$g = -\frac{2(\lambda, \alpha)}{(\alpha, \alpha)}. \quad (26)$$

But then since $g \geq 0$ it follows that

$$(\lambda, \alpha) \leq 0. \quad (27)$$

Proof of a). Suppose, on the contrary, that the dimension of R_α , $\alpha \in \Sigma$, is greater than one, and let u be an arbitrary non-zero vector belonging to R_α . Since $R_{-\alpha} = \bar{R}_\alpha$ it follows that $R_{-\alpha}$ also has dimension greater than one and consequently there exists in $R_{-\alpha}$ a vector $\bar{x} \neq 0$ satisfying the condition $(\bar{x}, u) = 0$ and hence the condition $[\bar{x}, u] = 0$ (see (17)). The vector x may be normalized so as to make $(x, \bar{x}) = 1$, whereupon (20) is satisfied for $\lambda = \alpha$. In particular, according to (27), we have $(\alpha, \alpha) \leq 0$ which is impossible. Thus the dimension of R_α is not greater than one, and since R_α is non-trivial by construction it follows that its dimension is exactly one.

Proof of b). Let t be the largest integer j satisfying $-j\alpha \in \Sigma$. Since $-\alpha \in \Sigma$ we have $t \geq 1$. We shall show that in fact $t = 1$. Let $\lambda = -t\alpha$, let u be a non-zero vector belonging to R_λ , and let $x \in R_\alpha$ be normalized so that $(x, \bar{x}) = 1$. By (16) we have $[\bar{x}, u] \in R_{-(t+1)\alpha} = R_{-(t+1)\alpha}$ and since $-(t+1)\alpha \notin \Delta$ it follows that $[\bar{x}, u] = 0$. Thus (20) is satisfied. Substituting $\lambda = -ta$ in (26) we obtain $= 2t$ so that the vectors u_0, u_1, \dots, u_2 are all distinct from 0. But u_{t+1} belongs to R_α (see (21)) and is therefore proportional to x since R_α is one-dimensional. Thus $u_{t+2} = [\bar{x}, u_{t+1}] = 0$ so that $2t < t + 2$ and consequently $t < 2$, i.e., $t = 1$.

Proof of c). This time let $\lambda = \beta - 1\alpha$, let u be a non-zero vector belonging to R_λ , and let $x \in R_\alpha$ be normalized so that $(x, \bar{x}) = 1$. As before we have $[\bar{x}, u] \in R_{\beta-(1+1)\alpha}$, and $\beta - (1+1)\alpha \notin \Delta$ so that (20) is satisfied. Thus u_0, u_1, \dots, u_g are all distinct from 0, while $u_{g+1} = 0$, and g is given by (26).

Denote now by T the linear span of the spaces

$$R_\lambda = R_{\beta-1\alpha}, \quad R_{\lambda+\alpha}, \quad \dots, \quad R_{\lambda+(1+m)\alpha} = R_{\beta+m\alpha}$$

By (16) we have $p_{\bar{x}}(R_{\lambda+j\alpha}) \subset R_{\lambda+(j-1)\alpha}$, and since $p_{\bar{x}}(R_{\beta-1\alpha}) = 0$ it follows that T is invariant with respect to $p_{\bar{x}}$. Similarly, $p_x(R_{\lambda+j\alpha}) \subset R_{\lambda+(j+1)\alpha}$, while $p_x(R_{\beta+m\alpha}) = 0$, so that T is invariant with respect to p_x . Finally, since $[\bar{x}, \bar{x}] = i\alpha$ (see (17)) it follows from F) Section 54 that T is also invariant with respect to $p_{i\alpha}$. Indeed

$$p_{i\alpha} = p_{[\bar{x}, \bar{x}]} = p_{\bar{x}}p_{\bar{x}} - p_{\bar{x}}p_x. \quad (28)$$

We now compute the trace of $p_{i\alpha}$ on the subspace T . On the one hand

$$\text{Tr}(p_{1\alpha}) = \text{Tr}(p_x p_{\bar{x}}) - \text{Tr}(p_{\bar{x}} p_x) = 0 \quad (29)$$

(see Section 61, (2)). But $\text{Tr}(p_{1\alpha})$ can also be computed directly. Indeed $R_{\lambda+j\alpha}$ is invariant with respect to $p_{1\alpha}$ and for every vector $z \in R_{\lambda+j\alpha}$ we have $p_{1\alpha}(z) = -((\lambda, \alpha) + j(\alpha, \alpha))z$ (see (15)). Thus

$$\begin{aligned} \text{Tr}(p_{1\alpha}) &= - \sum_{j=0}^{1+m} ((\lambda, \alpha) + j(\alpha, \alpha)) = \\ &= - (1+m+1)(\lambda, \alpha) - \frac{(1+m)(1+m+1)}{2} (\alpha, \alpha) \end{aligned} \quad (30)$$

(We here use the fact that $R_{\lambda+j\alpha}$ is one-dimensional for $\lambda + j\alpha \neq 0$. Note that $(\lambda, \alpha) + j(\alpha, \alpha) = 0$ for $\lambda + j\alpha = 0$ so that the dimension of $R_0 = [S]$ is irrelevant.) Hence, equating (29) and (30) we obtain

$$1+m = - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)} \quad (31)$$

and consequently, by (26), $1+m = g$. Thus the vectors u_0, u_1, \dots, u_{1+m} are all distinct from 0. Finally, substituting $\lambda = \beta - 1\alpha$ in (31), we obtain (18).

We turn now to the proof of (19). Since both members of (19) are linear in y , and since R_β is one-dimensional, we may take for y the vector $u_1 \in R_\beta$. According to (22) we have

$$[\bar{x}, [x, u_1]] = [\bar{x}, u_{1+1}] = (1+1)(\lambda, \alpha) + \frac{1(1+1)}{2} (\alpha, \alpha) u_1.$$

Substituting $\lambda = \beta - 1\alpha$ we obtain

$$[\bar{x}, [x, u_1]] = (1+1)(\alpha, \beta) - \frac{1(1+1)}{2} (\alpha, \alpha) u_1.$$

Finally $(\alpha, \beta) = \frac{1}{2}(1-m)(\alpha, \alpha)$ by (18), and making this substitution in the last relation, we obtain

$$[\bar{x}, [x, u_1]] = - \frac{m(1+1)}{2} (\alpha, \alpha) u_1,$$

and (19) follows:

Proof of d). It follows from (19) that if $\alpha + \beta \in \Sigma$ then $[x, y] \neq 0$ for $l \geq 0$ by definition, while $m \geq 1$ since $\alpha + \beta \in \Sigma$, and consequently $\frac{m(1+1)}{2} > 0$.

Example 105: Let R denote a three-dimensional Euclidean space, with the commutator $[a, b]$ of two vectors a and b defined to be their vector product. Then R is a compact simple Lie algebra (see Example 104). If $a \neq 0$ the set S_a of elements commuting

with a consists of the vectors collinear with a and is one-dimensional. Hence R is of rank one and every non-zero element is regular. Let e, f, g be an orthonormal basis in R satisfying

$$[e, f] = g, [f, g] = e, [g, e] = f.$$

Let $S = S_e$. Then (see Section 58, C))

$$[e, f + ig] = -i(f + ig), \quad (32)$$

$$[e, f - ig] = i(f - ig). \quad (33)$$

Recalling that the quadratic form of the scalar product of R is given in terms of the basis e, f, g by $(x, x) = 2(x_1^2 + x_2^2 + x_3^2)$, we conclude from (32) and (33) that the root vectors are $\alpha = -\frac{1}{2}e$ and $-\alpha = +\frac{1}{2}e$, while the corresponding eigenvectors r_α and $r_{-\alpha}$ are given by

$$r_\alpha = f + ig, \quad r_{-\alpha} = f - ig.$$

SECTION 63.

THE CONSTRUCTION OF A COMPACT SEMI-SIMPLE LIE ALGEBRA FROM A ROOT SYSTEM

If A and A' are subsets of Euclidean spaces R and R' , respectively, then a mapping f of A onto A' is said to be a similarity if

$$(f(x), f(y)) = k^2(x, y); \quad x \in A, y \in A,$$

where k is a positive number independent of the vectors x and y . The number k is known as the coefficient of similarity. If $k = 1$ then f is an isometry. The sets A and A' are said to be similar or isometric if there exists a similarity or isometry, respectively, of one onto the other.

The relevance of these concepts stems from the fact that a root system Σ of a compact semi-simple algebra R is a subset of a Euclidean space, namely the regular subalgebra S . In terms of them the results of the present section may be stated as follows. If two compact semi-simple algebras have isometric root systems then the algebras are isomorphic. Moreover, a similarity of one root system onto another is automatically an isometry. Thus, in order that two compact semi-simple Lie algebras should be isomorphic, it is sufficient that they should possess similar root systems. At the conclusion of the section a criterion is given for the

simplicity of an algebra based on the metric structure of a root system.

In this section, as in the last, we consider only compact semi-simple Lie algebras, and this hypothesis is to be understood as being in force even when it is not expressly stipulated.

A) Let S be a regular subalgebra of R , $\Sigma \subset S$ the root system contained in S . Then for any vector $s \in S$ we have

$$(s, s) = \sum_j (\alpha_j, s)^2, \quad (1)$$

where the sum is taken over all vectors $\alpha_j \in \Sigma$. It follows that S is the linear span of Σ .

In order to prove (1) we recall that $[R]$ resolves into the direct sum of spaces $R_0, R_{\alpha_1}, \dots, R_{\alpha_k}$, invariant with respect to all derivations p_s , $s \in S$, where the dimension of each space R_{α_j} , $j = 1, \dots, k$ is unity (see Theorem 105). Since $p_s(p_s(x)) = 0$ for $x \in R_0$, while for $x \in R^{\alpha_j}$ we have $p_s(p_s(x)) = -(\alpha_j, s)^2 x$, it follows from the definition of the scalar product (see (3) Section 61) that

$$(s, s) = -\text{Tr}(p_s p_s) = \sum_{j=1}^k (\alpha_j, s)^2$$

Thus (1) is proved. In order to see that S is the linear span of Σ , consider a vector $s \in S$ orthogonal to all the vectors of Σ . According to (1) we have

$$(s, s) = \sum_j (\alpha_j, s)^2 = 0,$$

whence it follows that $s = 0$.

B) Let Σ' be a system of vectors in a Euclidean space and suppose that Σ' is similar with a root system, so that for some positive number k the system $k \Sigma'$ consisting of vectors of the form $k\alpha'$, $\alpha' \in \Sigma'$, is isometric with a root system. Then the coefficient of similarity k is uniquely determined by Σ' . In particular, a similarity between two root systems is automatically an isometry.

Indeed, select any one fixed vector β' in Σ' , and apply (1) to the system $k \Sigma'$ with $s = k \beta'$. Then

$$(\beta', \beta') = k^2 \sum_{\alpha' \in \Sigma'} (\alpha', \beta')^2. \quad (2)$$

Thus the coefficient of similarity k is uniquely determined.

We turn now to the proof of the fact that the algebra R is uniquely determined, up to isomorphism, by the metric structure of a root system.

C) Let Σ be a root system of R and select in each subspace R_α , $\alpha \in \Sigma$, a non-zero vector r . Since R_α is one-dimensional the single vector r_α forms a basis in R_α . Moreover, since $R_{-\alpha} = \bar{R}_\alpha$, we may and do suppose the basis vectors r_α to be normalized in such a way that the following conditions are satisfied:

$$r_{-\alpha} = \bar{r}_\alpha; \quad (r_\alpha, r_{-\alpha}) = 1. \quad (3)$$

(Note that with this normalization each r_α is uniquely determined up to multiplication by a complex number of modulus one.) If α and β are two vectors in Σ such that $\alpha + \beta \in \Sigma$ then

$$[r_\alpha, r_\beta] = N_{\alpha\beta} r_{\alpha+\beta} \quad (4)$$

where $N_{\alpha\beta}$ is a uniquely determined complex number distinct from zero (see Theorem 105, d)). If any one of the three vectors α , β , $\alpha + \beta$ fails to belong to Σ we agree to write

$$N_{\alpha\beta} = 0 \quad (5)$$

Clearly then, in any case,

$$N_{\beta\alpha} = -N_{\alpha\beta} \quad (6)$$

and

$$N_{-\alpha, -\beta} = \bar{N}_{\alpha\beta}. \quad (7)$$

We now verify two further properties of the coefficients $N_{\alpha\beta}$.

a) If three vectors α , β , γ belonging to Σ form a triangle, i.e., satisfy the condition

$$\alpha + \beta + \gamma = 0$$

then

$$N_{\alpha\beta} = N_{\beta\gamma} = N_{\gamma\alpha}. \quad (8)$$

b) If four vectors α , β , γ , δ belonging to Σ form a quadrilateral, i.e., satisfy the condition

$$\alpha + \beta + \gamma + \delta = 0$$

and if no two of the vectors are negatives of one and other, then

$$N_{\alpha\beta} N_{\gamma\delta} + N_{\alpha\gamma} N_{\delta\beta} + N_{\alpha\delta} N_{\beta\gamma} = 0. \quad (9)$$

Proof of a). By the invariance of the scalar product (Section 61, (6)) we have

$$([r_\alpha, r_\beta], r_\gamma) + (r_\beta, [r_\alpha, r_\gamma]) = 0.$$

Moreover, by (3) and (4)

$$([r_\alpha, r_\beta], r_\gamma) = N_{\alpha\beta}(r_{\alpha+\beta}, r_\gamma) = N_{\alpha\beta}(r_{-\gamma}, r_\gamma) = N_{\alpha\beta}$$

and similarly

$$(r_\beta, [r_\alpha, r_\gamma]) = N_{\alpha\gamma}(r_\beta, r_{\alpha+\gamma}) = N_{\alpha\gamma}(r_\beta, r_{-\beta}) = N_{\alpha\gamma} = -N_{\gamma\alpha}$$

(see (6)). Thus $N_{\alpha\beta} - N_{\gamma\alpha} = 0$, whence (8) follows by symmetry.

Proof of b). By the Jacobi identity ((16) Section 52) we have

$$[r_\alpha, [r_\beta, r_\gamma]] + [r_\beta, [r_\gamma, r_\alpha]] + [r_\gamma, [r_\alpha, r_\beta]] = 0 \quad (10)$$

Now if $\beta + \gamma \in \Sigma$ then, $\alpha, \beta + \gamma, \delta$ form a triangle in Σ so that by

a) we have

$$[r_\alpha, [r_\beta, r_\gamma]] = N_{\beta\gamma}[r_\alpha, r_{\beta+\gamma}] = N_{\beta\gamma}N_{\alpha, \beta+\gamma}r_{\alpha+\beta+\gamma} = N_{\delta\alpha}r_{-\delta}$$

On the other hand, if $\beta + \gamma \notin \Sigma$ then both $[r_\alpha, [r_\beta, r_\gamma]]$ and $N_{\beta\gamma}$ vanish. Thus, in either case,

$$[r_\alpha, [r_\beta, r_\gamma]] = -N_{\alpha\delta}N_{\beta\gamma}r_{-\delta}. \quad (11)$$

Similary

$$\begin{aligned} [r_\beta, [r_\gamma, r_\alpha]] &= -N_{\alpha\gamma}N_{\delta\beta}r_{-\delta}; [r_\gamma, [r_\alpha, r_\beta]] \\ &= -N_{\alpha\beta}N_{\gamma\delta}r_{-\delta} \end{aligned} \quad (12)$$

Finally, adding (11) and (12) and taking account of (10), we obtain (9).

D) For any root system Σ and any two vectors α and β belonging to Σ , let l and m be defined as in Theorem 105, c). Then

$$|N_{\alpha\beta}|^2 = \frac{m(1+1)}{2}(\alpha, \alpha) \quad (13)$$

Indeed, if $\alpha + \beta \notin \Sigma$ then $N_{\alpha\beta} = m = 0$, while if $\alpha + \beta \in \Sigma$ then, employing (19) Section 62 with $\bar{x} = r_{-\alpha}$, $x = r_\alpha$, $y = r_\beta$, we obtain

$$[r_{-\alpha}, [r_\alpha, r_\beta]] = -\frac{m(1+1)}{2}(\alpha, \alpha)r_\beta \quad (14)$$

Since $-\alpha, \alpha + \beta, -\beta$ form a triangle we also have

$$\begin{aligned} [r_{-\alpha}, [r_\alpha, r_\beta]] &= N_{\alpha\beta}[r_{-\alpha}, r_{\alpha+\beta}] = N_{\alpha\beta}N_{-\alpha\alpha+\beta}r_\beta = \\ &= -N_{\alpha\beta}N_{-\alpha}r_{-\beta} \end{aligned} \quad (15)$$

Equating the right members of (14) and (15), and employing (7), we obtain (13).

E) Let $\Sigma \subset S$ be a root system of R . Then every element $x \in [R]$ possesses a unique expression of the form

$$x = s - \sum_{\alpha} \tau_{\alpha} r_{\alpha}, \quad (16)$$

where $s \in [S]$ while τ_{α} , $\alpha \in \Sigma$, is a complex number. In order that x should be real, i.e., should belong to R , it is necessary and sufficient that $x = \bar{x}$ or, equivalently, that the conditions

$$s \in S; \tau^{\alpha} = \tau^{-\alpha}, \alpha \in \Sigma \quad (17)$$

should be satisfied. Since the subalgebra S is commutative the bracket product in $[R]$ is uniquely determined by the relations

$$[s, r_{\alpha}] = i(\alpha, s)r_{\alpha}, \quad (18)$$

$$[r_{\alpha}, r_{-\alpha}] = i\alpha, \quad (19)$$

$$[r_{\alpha}, r_{\beta}] = N_{\alpha\beta} r_{\alpha+\beta}, \alpha + \beta \neq 0 \quad (20)$$

(see Section 62, (15) and (17); the notation is that introduced in C.).

In the further study of Lie algebras we shall frequently have occasion to employ the following scheme for ordering a vector space.

F) Let A be a real vector space with basis e_1, \dots, e_m . We introduce an order relation in A as follows. Let $a \neq 0$ and write $a = a^1 e_1 + \dots + a^m e_m$. Then not all of the coordinates in the sequence a^1, \dots, a^m are zero. If the first non-zero coordinate is positive we shall say that a is positive and write $a > 0$. If a and b are distinct vectors in A we shall also write $a > b$ (or $b < a$) if $a - b > 0$. Thus if a and b are any two distinct elements of A then either $a < b$ or $a > b$. Moreover, inequalities may be added and multiplied by positive numbers according to the usual rules. If A is the regular subalgebra S or, more generally, any space containing S , then the root system $\Sigma \subset S$ automatically becomes an ordered set, and there arises the important concept of a primitive root vector: a root vector is said to be primitive if it is positive but cannot be written as the sum of two positive root vectors. It should be emphasized that the order relation here defined depends on the choice of a basis, and that it is quite possible for a root vector to be primitive with respect to one such ordering and imprimitive with respect to another.

We turn now to the statement and proof of Theorem 106, a result which lies at the basis of the classification of Lie algebras. It is clear that the Lie algebra R is completely determined by S , Σ , and the system of coefficients $N_{\alpha\beta}$. Moreover, S is determined

by Σ and, according to D), the absolute values of the coefficients $N_{\alpha\beta}$ are too. Theorem 106 asserts that everything is determined by the metric structure of Σ alone. The idea on which the proof rests is to utilize an ordering of S , and the freedom of choice remaining in the selection of the basis vectors r_α , to arrange matters so that the coefficients $N_{\alpha\beta}$ are all real and to choose the algebraic signs of the $N_{\alpha\beta}$ according to a definite scheme so that the same choices can be made simultaneously for two isometric root systems.

Theorem 106: If R and R' are Lie algebras possessing isometric root systems Σ , Σ' , respectively, then R and R' are isomorphic. More precisely; if f is any isometry of Σ onto Σ' then f may be extended to an isomorphism of R onto R' . In the course of the proof it will be shown that it is possible to choose the basis vectors r_α , $\alpha \in \Sigma$, in such a way that all the coefficients $N_{\alpha\beta}$ are real (see C)).

Proof: We choose a basis e_1, \dots, e_n in S and use it to order S in the manner described in F). This ordering is understood to be fixed throughout the proof. In particular, Σ is ordered and the set of positive root vectors is partitioned, once for all, into primitive and imprimitive vectors. If ρ is an imprimitive root vector then there exist ordered pairs of positive root vectors λ, μ such that $\lambda + \mu = \rho$. Among such pairs we select the (unique) pair α, β with the property that λ assumes its minimum value at $\lambda = \alpha$, and we define $N_\rho = N$. In this way a non-zero number N_ρ is assigned to each imprimitive positive vector $\rho \in \Sigma$. If λ, μ is a pair of positive root vectors distinct from α, β and satisfying the relations $\lambda + \mu = \alpha + \beta = \rho$ and $\lambda < \mu$ (see Theorem 105, b)) then

$$\alpha < \lambda < \mu < \beta, \quad (21)$$

and, since $\alpha, \beta, -\lambda, -\mu$ form a quadrilateral, we have

$$N_{\alpha\beta} N_{-\lambda, -\mu} + N_{\alpha, -\lambda} N_{-\mu, \beta} + N_{\alpha, -\mu} N_{\beta, -\lambda} = 0,$$

by (9). Using (7) and the definition of $N_\rho = N_{\lambda+\mu}$ this may be written

$$N_{\lambda, \mu} = \frac{\bar{N}_{\alpha, -\lambda} \bar{N}_{\beta, -\mu} - \bar{N}_{\alpha, -\mu} \bar{N}_{\beta, -\lambda}}{\bar{N}_{\lambda+\mu}}$$

If $\lambda - \alpha \in \Sigma$ then $\alpha, -\lambda, \lambda - \alpha$ form a triangle whence, by (8),

$$\bar{N}_{\alpha, -\lambda} = \bar{N} \quad (22)$$

On the other hand, if $\lambda - \alpha \notin \Sigma$ then both members of (22) vanish;

thus (22) holds in any case. Similarly we obtain

$$\bar{N}_{\beta, -\mu} = N_{\mu, \beta-\mu}, \quad \bar{N}_{\alpha, -\mu} = \bar{N}_{\mu-\alpha, \alpha}, \quad \bar{N}_{\beta, -\lambda} = N_{\lambda, \beta-\lambda}.$$

Thus finally,

$$N_{\lambda, \mu} = \frac{\bar{N}_{\lambda-\alpha, \alpha} N_{\mu, \beta-\mu} - \bar{N}_{\mu-\alpha, \alpha} N_{\lambda, \beta-\lambda}}{\bar{N}_{\lambda+\mu}} \quad (23)$$

In this way the coefficient $N_{\lambda, \mu}$ is expressed in terms of $N_{\lambda+\mu}$ and certain of the coefficients $N_{\gamma, \delta}$ where γ and δ are positive root vectors satisfying $\gamma + \delta < \lambda + \mu$. In particular, if $N_{\lambda+\mu}$ and the various $N_{\gamma, \delta}$ appearing in (23) are all real then so is $N_{\lambda, \mu}$.

This reduction may now be repeated. Each of the coefficients $N_{\gamma, \delta}$ appearing (23) may, in turn, be expressed in terms of $N_{\gamma+\delta}$ along with various coefficients $N_{\varepsilon, \zeta}$ where ε and ζ are positive root vectors satisfying $\varepsilon + \zeta < \gamma + \delta$. As the end result of all possible reductions of this sort we obtain an expression for each coefficient $N_{\lambda, \mu}$, $\lambda > 0$, $\mu > 0$, in terms of the numbers N_ρ , $\rho \in \Sigma$, $0 < \rho \leq \lambda + \mu$. Since the numerical coefficients appearing in these expressions are real it follows that if the numbers N_ρ are all real then the same is true of the coefficients $N_{\lambda, \mu}$, $\lambda > 0$, $\mu > 0$.

Now let λ, μ, ν be any three root vectors that form a triangle. It is impossible for the three to be all positive or all negative so there are just two possibilities: either two of the three are positive and the third negative or two are negative and the third positive. Thus, in view of (7) and (8), it follows that all of the coefficients $N_{\lambda, \mu}$ may be expressed in terms of the numbers N_ρ , and that all coefficients $N_{\lambda, \mu}$ are real provided the numbers N_ρ are.

We next show that it is possible to choose basis vectors r_α , $\alpha \in \Sigma$, in such a way that the numbers N_ρ are all real and positive. In view of what has already been said, this suffices to take care of the last assertion of the theorem. We remark parenthetically that, with this normalization, the numbers N_ρ , and hence the coefficients $N_{\lambda, \mu}$ are all uniquely determined by the metric structure of Σ (see (13)). Since $r_{-\alpha} = r_\alpha$ it suffices to choose basis vectors r_α for positive $\alpha \in \Sigma$. The construction is by mathematical induction. Let $\rho \in \Sigma$, $\rho > 0$, and suppose vectors r_α already constructed for $0 < \alpha < \rho$ in such a way that the numbers N_α , $0 < \alpha < \rho$, are positive. If ρ is primitive (note that the least positive root vector is certainly primitive) we may take for r_ρ any vector in R_ρ satisfying $(r_\rho, f_\rho) = 1$. On the other hand, if ρ is imprimitive we select α, β among the pairs λ, μ of positive root vectors satisfying $\lambda + \mu = \rho$ in such a way that λ assumes its minimum at $\lambda = \alpha$, and choose for r_ρ the unique vector in R_ρ satisfying

$(r_\rho, \bar{r}_\rho) = 1$ and

$$[r_\alpha, r_\beta] = N_{\alpha\beta} r_\rho,$$

with positive real coefficient $N_{\alpha\beta} = N_\rho$. Thus the inductive construction is complete.

Suppose now that S' and Σ' are a regular subalgebra and corresponding root system in the algebra R' . The given isometry f of Σ onto Σ' may be extended to an isometry of S onto S' . In S' we use the basis $e_i = f(e_i)$, $i = 1, \dots, n$, to define an order relation, so that f is turned into an order preserving mapping. Next, we use the resulting ordering of Σ' to construct inductively in R' a system of basis vectors $r'_{\alpha'}$, $\alpha' \in \Sigma'$, exactly as was done in R . Next we extend f to the basis vectors r_α by defining $f(r_\alpha) = r'_{f(\alpha)}$. Clearly then

$$N'_{f(\alpha)f(\beta)} = N_{\alpha\beta}$$

The mapping f , which was defined on S , is thus defined on the basis vectors r_α , $\alpha \in \Sigma$; consequently we may use (16) to extend f by linearity to the entire algebra $[R]$. It follows at once from (18) (19), (20) that the mapping thus obtained is an isomorphism of the complex Lie algebra $[R]$ onto $[R']$. Finally we have $f(R) = R'$ by (17), and the proof of the theorem is complete.

G) Suppose R resolves into the direct sum of subalgebras R_1 and R_2 . According to C) and E), Section 61, the summands R_1 and R_2 are themselves compact semi-simple Lie algebras. Let $c_i \in R_i$, $i = 1, 2$, $c = c_1 + c_2$. Then

$$S_c = S_{c_1}^{-1} + S_{c_2}^{-2}, \quad (24)$$

where $S_{c_i}^{-i}$ denotes the subalgebra of R_i commuting with c_i , $i = 1, 2$, (see Theorem 104). Hence, c is a regular element of R when and only when c_i is a regular element of R_i , $i = 1, 2$.

Indeed, let n, n_1, n_2 denote the ranks of R, R_1, R_2 , respectively. The validity of (24) follows at once from

$$[x_1 + x_2, y_1 + y_2] = [x_1, y_1] + [x_2, y_2]; \quad x_i, y_i \in R_i,$$

$$i = 1, 2.$$

Choosing a regular element for c in (24) we see that $n \geq n_1 + n_2$ with $n > n_1 + n_2$ if and only if at least one of the elements $c_i, i \in R$ is irregular. On the other hand, choosing regular elements for both c_1 and c_2 in (24) we see that $n \leq n_1 + n_2$ with $n < n_1 + n_2$

if and only if c is irregular. These facts, taken together, imply that $m = n_1 + n_2$ and that c is regular when and only when both c_1 and c_2 are.

The following proposition gives (in terms of root systems) a criterion for the reducibility of R into a direct sum.

H) We shall say that a system Γ of vectors in a Euclidean space reduces into two subsystems Γ_1 and Γ_2 if $\Gamma = \Gamma_1 \cup \Gamma_2$, where Γ_1 and Γ_2 are non-empty and disjoint, and where every vector belonging to Γ_1 is orthogonal to every vector belonging to Γ_2 . The desired criterion may then be stated as follows: if a root system Σ of the Lie algebra R reduces into two subsystems Σ_1 and Σ_2 then R resolves into a direct sum of subalgebras R_1 and R_2 having root systems Σ_1 and Σ_2 , respectively; conversely, if R is a direct sum of subalgebras R_1 and R_2 then, for a suitable choice of regular subalgebra S , the corresponding root system $\Sigma \subset S$ reduces into root systems Σ_1 and Σ_2 for R_1 and R_2 .

Suppose first that Σ reduces into Σ_1 and Σ_2 . Denote by S_i the linear span of Σ_i , $i = 1, 2$. Then $S = S_1 + S_2$ (see A)). For each root vector $\lambda \in \Sigma$ select an eigenvector r_λ in such a way that $r_{-\lambda} = \bar{r}_\lambda$. Then every element $a \in R$ may be written uniquely in the form

$$a = b_1 + b_2 + \sum_{\lambda \in \Sigma_1} \tau^\lambda r_\lambda + \sum_{\lambda \in \Sigma_2} \tau^\lambda r_\lambda; \quad \tau^{-\lambda} = \tau^\lambda, \quad b_1 \in S_1, \quad b_2 \in S_2.$$

Define

$$a_1 = b_1 + \sum_{\lambda \in \Sigma_1} \tau^\lambda r_\lambda, \quad a_2 = b_2 + \sum_{\lambda \in \Sigma_2} \tau^\lambda r_\lambda.$$

Then $a = a_1 + a_2$ and the vector space R resolves into the direct sum of the subspaces R_1 and R_2 , where R_i denote the collection of all vectors of the form a_i , $i = 1, 2$. Now if $\alpha_1 \in \Sigma_1$, $\alpha_2 \in \Sigma_2$, then $\alpha_1 + \alpha_2$ cannot belong to Σ since $\alpha_1 + \alpha_2$ is not orthogonal to either of the vectors α_1 or α_2 . From this it follows that $[a_1, a_2] = 0$ (see Section 62, (15), (16)), and hence that, R_1 and R_2 are ideals in R . But then, according to G), S_i is a regular subalgebra of R_i whence it follows, by Definition 51, that Σ_i is a root system for R_i , $i = 1, 2$.

Suppose, on the other hand, that R is the direct sum of R_1 and R_2 and let $\Sigma_1 \subset S_1$ and $\Sigma_2 \subset S_2$ be root systems for R_1 and R_2 , respectively. Then $S = S_1 + S_2$ is a regular subalgebra in R and, according to Definition 51, $\Sigma = \Sigma_1 \cup \Sigma_2$ is a root system for R . Moreover, if $x_1, y_1 \in R_1$, $x_2, y_2 \in R_2$ then $(x_1 + x_2, y_1 + y_2) = (x_1, y_1) + (x_2, y_2)$ (see Section 61, C)) so that the vectors of Σ_1 are

orthogonal to the vectors of Σ_2 . Thus H) is proved.

SECTION 64. THE INVARIANCE OF ROOT SYSTEMS

In defining a root system of a compact semi-simple Lie algebra it was necessary to begin by making a preliminary choice of a regular subalgebra (see Definition 51). In the preceding section it was shown that the metric structure of a root system determines the algebra uniquely, but the question remains open whether it is possible to find two non-isometric root systems in the same algebra. In the present section we settle this question in the negative (Theorem 109). Thus the classification of compact semi-simple Lie algebras reduces to the classification of their root systems. The isometry of any two root systems of the same Lie algebra R derives from the fact that any two regular subalgebras of R are mapped onto one another by some automorphism g of R. Since g need not be in the vicinity of the identity mapping, this theorem is not of a local character. In order to construct g we introduce the Lie group G consisting of the component of the identity in the group of all automorphisms of R. Since R is, in a natural way, isomorphic with the Lie algebra P of G (see Theorem 102) it follows that a regular subalgebra S corresponds to a subgroup H of G. We shall show that an arbitrary element of G is mapped into H by some inner automorphism (Theorem 107); from this result Theorem 109 then follows as an easy consequence. Pursuing the same line of inquiry we shall also obtain a proof of the important theorem of Weyl [57] which asserts that the universal covering of G is compact. Thus there exist only a finite number of connected, pairwise non-isomorphic, compact Lie groups having Lie algebra isomorphic with R.

A) Let R be an m-dimensional compact semi-simple Lie algebra of rank n, let P be its adjoint algebra, and let G be the component of the identity in the group of all automorphisms of R. It has already been observed that P is the Lie algebra of G and that the correspondence $a \rightarrow p_a$ is an isomorphism of R onto P (see Theorem 102). Let S be a regular subalgebra of R and denote by Q the corresponding subalgebra of P, i. e., the algebra of all derivations of the form p_s , $s \in S$. Then Q corresponds to a global subgroup H of G. A precise description of H is as follows. Let $\varphi(t, a)$, $a \in R$, denote the one-parameter subgroup of G with direction vector p_a , and define

$$\varphi(a) = \varphi(1, a).$$

Then φ is a homomorphism of the vector group S onto a closed subgroup $H = \varphi(S)$ of G , and Q is the subalgebra corresponding to H . Moreover, the automorphism $h_s = \varphi(s)$, $s \in S$, of the Lie algebra R satisfies, and is determined by, the relations

$$h_s(b) = b, \quad b \in S; \quad h_s(r_\alpha) = e^{i(\alpha, s)} r_\alpha, \quad \alpha \in \Sigma. \quad (1)$$

Proof: It may be verified by straightforward computation that (1) defines, by linear extension, an isomorphism h_s of the real algebra R onto itself. Moreover

$$h_{ts}(b) = b, \quad h_{ts}(r_\alpha) = e^{it(\alpha, s)} r_\alpha. \quad (2)$$

In other words, h_{ts} is a one-parameter subgroup of the group of all linear automorphisms of the vector space R onto itself, the parameter being t . But now, differentiating (2) at $t = 0$, we obtain (see Definition 51)

$$\frac{d}{dt} h_{ts} \Big|_{t=0} = p_s. \quad (3)$$

Thus the direction vector of the subgroup h_{ts} is p_s and consequently, (see Section 54, F)) h_s belongs to G . That φ is a homomorphism follows from the fact that S is commutative (it is also a consequence of (1).) Finally if $\varphi(S) = H$ were not closed then H would be a subgroup of G of dimension greater than n , which is impossible since S is a maximal commutative subalgebra of R .

Later it will be shown (Theorem 107) that every $f \in G$ may be written in the form

$$f = ghg^{-1}; \quad g \in G, \quad h \in H. \quad (4)$$

Since the automorphisms belonging to H have the particularly simple form (1), we may view this result as stating the possibility of reducing every automorphism $f \in G$ to canonical form h . With respect to a basis s_i, r_α ; $i = 1, \dots, n$, $\alpha \in \Sigma$, the matrix corresponding to h has diagonal form. From (1) it is clear that n eigenvalues of h , and consequently also of f , are equal to one, while the remaining eigenvalues are of absolute value one. An automorphism $f \in G$ will be said to be regular if exactly n of its eigenvalues are equal to one. The present section is devoted to the proof of Theorem 107 and to the discussion of its consequences. The first and main step in this direction is the following lemma.

B) Let $a \in R$, $g \in G$ and let U be a spherical neighborhood of radius $\rho > 0$ about the origin in the vector space R . Then

$$g\varphi(a)g^{-1} = \varphi(g(a)), \quad (5)$$

$$g(U) = U \quad (6)$$

where φ denotes the homomorphism defined in A). Moreover, if ρ is chosen sufficiently small, then φ is a homeomorphism of U onto a neighborhood of the identity in G and, in this event,

$$a \in U, b \in U, \quad g\varphi(a)g^{-1} = \varphi(b) \quad (7)$$

implies $b = g(a)$ (8)

and conversely. Finally, given a subgroup K of G there exists a ρ sufficiently small so that

$$\varphi(U) \cap K = \varphi(T \cap U) \quad (9)$$

where T denotes the subalgebra of R corresponding to K .

In order to verify (5) we compute the direction vector of the one-parameter subgroup $g\varphi(ta)g^{-1}$. Differentiating at $t=0$, we obtain

$$\left. \frac{d}{dt} g\varphi(ta)g^{-1} \right|_{t=0} = gp_a g^{-1} = p_{g(a)}$$

(see Section 54, (15)). Thus $g\varphi(ta)g^{-1} = \varphi(tg(a))$ which, at $t=1$, yields (5). Relation (6) is an immediate consequence of the fact that isomorphisms of the Lie algebra R preserve scalar products (see Section 61, (5)), while the fact that, for ρ sufficiently small, φ is a homeomorphism of U onto a neighborhood of the identity in G , and satisfies (9) for arbitrarily prescribed subgroup K , follows from the properties of canonical coordinate systems of the first kind (see Section 42, B) and Theorem 62). Finally, if φ is homeomorphic on U , or even one-to-one, and if (7) holds, then from (5) we obtain $\varphi(g(a)) = \varphi(b)$, and since $g(a) \in U$ (see (6)) it follows that $g(a) = b$.

Lemma. Let the mapping ψ of the group $G \times H$ into G be defined by

$$\psi(g, h) = ghg^{-1}; \quad g \in G, h \in H. \quad (10)$$

Then ψ is an analytic mapping of the manifold $G \times H$ into the manifold G . Since the dimension of G is m the rank of the functional matrix of ψ can nowhere exceed m . The rank is equal to m at a point $(g, h) \in G \times H$ when and only when h or, what comes to the same thing, $f = ghg^{-1} = \psi(g, h)$, is regular. Moreover, the set \mathfrak{S} of these irregular elements $f \in G$ that can be written in the form $f = \psi(g, h)$ is the union of a finite number of sets, each of which is the image under an analytic mapping of a compact analytic manifold of dimension $m - 3$.

Proof: The relation $f = ghg^{-1}$ may be rewritten in the form

$$fg = gh. \quad (11)$$

Let (g_*, h_*) be a fixed element of $G \times H$ and let

$$f_* g_* = g_* h_*. \quad (12)$$

We introduce the translation $(g, h) \rightarrow (y, z)$ of $G \times H$ defined by

$$(g, h) = (g_* y, h_* z), \quad (13)$$

as well as the translation $f \rightarrow x$ of G defined by

$$f = f_* x. \quad (14)$$

Since both of these transformations are smooth and possess smooth inverses they may be viewed as introducing new variables x, y, z in place of the variables f, g, h . In terms of these new variables (11) assumes the form

$$f_* x g_* y = g_* y h_* z$$

or, what comes to the same thing (see (12)),

$$(f_* g_*)^{-1} f_* x g_* y = (g_* h_*)^{-1} g_* y h_* z.$$

Thus we have

$$g_*^{-1} x g_* y = h_*^{-1} y h_* z. \quad (15)$$

This last relation defines a mapping $\psi((y, z) \rightarrow x)$ of $G \times H$ into G that takes (e, e) into e and has the property that the rank of its functional matrix at (e, e) is equal to the rank of the functional matrix of ψ at (g_*, h_*) .

In order to compute the rank of ψ at (e, e) we linearize it, obtaining a linear transformation ψ^* of the space $P + Q$ tangent to $G \times H$ at (e, e) into the space P tangent to G at e . The rank of the functional matrix of ψ at (e, e) is just the dimension of the range $\psi^*(P + Q)$. Next, in order to compute the action of the linear transformation ψ^* , we select in $G \times H$ an arbitrary arc $(y(t), z(t))$ passing through (e, e) at $t = 0$ and having direction vector (p_b, p_c) , where $b \in R, c \in S$. Let p_a denote the direction vector of the corresponding arc $\psi(y(t), z(t)) = x(t)$. According to (15), $x(t)$ is defined by the equation

$$g_*^{-1} x(t) g_* y(t) = h_*^{-1} y(t) h_* z(t).$$

Differentiating with respect to t at $t = 0$ we obtain

$$g_*^{-1} p_a g_* + p_b = h_*^{-1} p_b h_* + p_c.$$

But then by (15) Section 54 we have

$$g_*^{-1}(a) + b' h_*^{-1}(b) + c,$$

or, equivalently,

$$a = g_*(h_*^{-1}(b) - b + c). \quad (16)$$

Now g_* is an automorphism of R , while the mapping $u \rightarrow p_u$ is an isomorphism of R onto P which carries S onto Q . Thus in place of ψ^* , which maps $P + Q$ into P , we may equally well consider the mapping of $R + S$ into R defined by

$$\omega(b, c) = h_*^{-1}(b) - b + c; \quad b \in R, \quad c \in S. \quad (17)$$

Finally it follows from (1) that the dimension of $\omega(R + S)$ is less than m when and only when h_* satisfies

$$h_*(r_\alpha) = r_\alpha, \quad (18)$$

for at least one vector $\alpha \in \Sigma$, i.e., when h_* is irregular. Thus the first part of the lemma is proved.

Now let $\alpha \in \Sigma$ be a fixed root vector. The set $H^{(\alpha)}$ consisting of the element $h \in H$ satisfying the condition

$$h(r_\alpha) = r_\alpha, \quad (19)$$

is clearly a subgroup of H . Moreover, if $s \in S$ is sufficiently close to the origin then $h = h_s$ belongs to $H^{(\alpha)}$ when and only when $(\alpha, s) = 0$ (see (1)). Thus the dimension of $H^{(\alpha)}$ is $n - 1$. Let $G^{(\alpha)}$ denote the collection of those elements of G that commute with all the elements of $H^{(\alpha)}$. Clearly $G^{(\alpha)}$ is a subgroup of G . Let R^α denote the subalgebra of R corresponding to $G^{(\alpha)}$. It is clear from B) that an element $a \in R$ belongs to $R^{(\alpha)}$ when and only when $h(a) = a$ for every $h \in H^{(\alpha)}$, and this relation is satisfied by elements a of the form

$$a = s + \tau r_\alpha + \bar{\tau} r_{-\alpha}, \quad s \in S, \quad (20)$$

and only by such elements. Thus the dimension of $G^{(\alpha)}$ is $n + 2$, and the dimension of the space $G/G^{(\alpha)}$ of left cosets is $m - (n + 2)$. If now g_1 and g_2 are two elements of G belonging to the same left coset $\hat{g} \in G/G^{(\alpha)}$ and if $h \in H^{(\alpha)}$, then $g_1 h g_1^{-1} = g_2 h g_2^{-1}$. Thus we may define

$$\psi(\hat{g}, h) = \psi(g_1, h); \quad g_1 \in g, \quad h \in H_\alpha.$$

In other words ψ may be regarded as defined on the direct product $(G/G^{(\alpha)}) \times H^{(\alpha)}$ whose dimension is $m - (n + 2) + n - 1 = m - 3$. Finally for every irregular $h \in H$ there exists a root vector α for which $h \in H^{(\alpha)}$, so that the set \mathfrak{S} defined in the lemma is the union of the analytic images of the manifolds $(G/G^{(\alpha)}) \times H^{(\alpha)}$, $\alpha \in \Sigma$,

and the lemma is proved.

The following propositions C), D), E), which we shall need in the proof of Theorem 107, are elementary facts pertaining to the theory of differentiable manifolds (see Section 45).

C) Let ψ be a smooth mapping of an 1-dimensional manifold L into an m -dimensional manifold M , where $l < m$, and let F be a compact subset of L . Then $\psi(F)$ is nowhere dense in M .

Proof: Let $a \in F$, $b = \psi(a)$. Let V_b be a coordinate neighborhood of b in M and let U_a be a coordinate neighborhood of a in L such that $\psi(U_a) \subset V_b$. Select neighborhoods U_{a1} and U_{a2} of a such that $\bar{U}_{a1} \subset U_a$, $\bar{U}_{a2} \subset U_{a1}$ and such that \bar{U}_{a1} is compact. The sets U_{a2} , $a \in F$, cover F and from this covering we may select a finite covering. Thus it suffices to prove that for any point $a \in F$ the set $\psi(\bar{U}_{a2})$ is nowhere dense in V_b . Since U_a and V_b are both coordinate neighborhoods it is no loss of generality to suppose that U_a is an open subset of 1-dimensional Euclidean space E^1 and that ψ is a smooth mapping of U_a into m -dimensional Euclidean space E^m . Our object then is to prove that $\psi(\bar{U}_{a2})$ is nowhere dense in E^m . Since \bar{U}_{a2} and, consequently, the continuous image $\psi(\bar{U}_{a2})$ are compact, this amounts to showing that $\psi(\bar{U}_{a2})$ contains no open subset of E^m .

Since ψ is smooth and \bar{U}_{a1} is compact there exists a positive constant c such that for any two points $x, x' \in \bar{U}_{a1}$ the inequality

$$\rho(\psi(x), \psi(x')) \leq c \rho(x, x') \quad (21)$$

is satisfied. Select an ε -tessellation of the space E^1 , i. e., a decomposition of E^1 into congruent cubes of edge ε , and denote by Ω the collection of all cubes of the tessellation that meet \bar{U}_{a2} . Since U_{a2} is compact, and is therefore contained in a cube of sufficiently large edge, it follows that the number of cubes belonging to Ω

cannot (for sufficiently small ε) exceed $\frac{c_1}{\varepsilon^1}$ where c_1 is a positive constant independent of ε . Let δ denote the distance between the sets $E \setminus U_{a1}$ and \bar{U}_{a2} and let $\varepsilon < \frac{\delta}{\sqrt{1}}$. Then every cube $L_i \in \Omega$ is contained in U_{a1} and hence, by (21), $\psi(L_i)$ is contained in a cube M_i in E^m with edge $c\varepsilon\sqrt{1}$. Thus $\psi(\bar{U}_{a2})$ is contained in a union of cubes M_i , of edge $c\varepsilon\sqrt{1}$ the number of which does not exceed $\frac{c_1}{\varepsilon^1}$. It follows that the measure of $\psi(\bar{U}_{a2})$ is dominated by $c_1 c^m l^{m-2} \varepsilon^{m-1}$. Since ε is arbitrary this implies that $\psi(\bar{U}_{a2})$ contains no open set, and C) follows.

D) Let ψ be a smooth mapping of a compact 1-dimensional manifold L into an m -dimensional manifold M where $1 \leq m - 2$, and let $x(t)$, $0 \leq t \leq 1$, be an arc in M , the end points of which do not belong to $\psi(L)$. Then there exists an arc $x'(t)$ in M , having the same end points as $x(t)$, approximating $x(t)$ arbitrarily closely and passing through no point of $\psi(L)$.

Proof: By a spherical region in the manifold M we shall mean any image of a closed solid sphere in m -dimensional Euclidean space under a smooth homeomorphism. As a first step in the proof we show that if a and b are two points interior to a spherical region $U \subset M$ and not belonging to $\psi(L)$ then a and b can be joined in the interior of U by an arc which is disjoint from $\psi(L)$. Indeed, let c be an interior point of the spherical region U not lying in $\psi(L)$ and let U' be a spherical region concentric with U and of smaller "radius" than that of U but still large enough to contain the points a , b , c in its interior. Let $F = \psi^{-1}(U')$ and let L' be a neighborhood of F in L such that $\psi(L') \subset U$. Since "central projection" from the point c of $\psi(L')$ into the spherical surface of U' defines a smooth mapping on L' , it follows from C) that almost every "ray" emanating from c fails to meet the set $\psi(F)$ inside U' . In particular, if V and W are connected neighborhoods of a and b disjoint from $\psi(F)$ and interior to U' then there exist points $a' \in V$ and $b' \in W$ such that the segments ca' and cb' are disjoint from $\psi(F)$. But then, joining a' to a in V and b' to b in W , we obtain an arc interior to U' that joins b to a and passes through no point of $\psi(L)$.

Since the arc $x(t)$ is compact there exists a positive number $\epsilon = \frac{1}{2n}$ (n a positive integer) sufficiently small so that for every point t_0 , $0 \leq t_0 \leq 1$, there exists a spherical neighborhood U_{t_0} of $x(t_0)$ containing all points $x(t)$ for $|t - t_0| \leq \epsilon$. Let $0 \leq j < n$. Then $x(2j\epsilon)$ belongs simultaneously to the spheres $U_{(2j-1)\epsilon}$ and $U_{(2j+1)\epsilon}$. Select a point $x'(2j\epsilon)$ which is interior to both of these spheres and does not belong to $\psi(L)$, and let $x'(0) = x(0)$, $x'(1) = x(1)$. Joining $x'(2j\epsilon)$ to $x'((2j+2)\epsilon)$ in the neighborhood $U_{(2j+1)\epsilon}$ by means of an arc $x'(t)$, $2j\epsilon \leq t \leq (2j+2)\epsilon$, which passes through no point of the set $\psi(L)$, we obtain an arc $x'(t)$, $0 \leq t \leq 1$, joining $x'(1) = x(1)$ to $x'(0) = x(0)$ and disjoint from $\psi(L)$. The arc $x'(t)$ thus obtained can be made to approximate $x(t)$ as closely as desired by choosing the spheres U_{t_0} sufficiently small.

E) Let ψ be a smooth mapping of a closed manifold N into an m -dimensional manifold M and let $x(t)$, $0 \leq t \leq 1$, be an arc in M . Suppose that at every point $y \in N$ satisfying the condition $\psi(y) = x(t)$,

$0 \leq t \leq 1$, the rank of the functional matrix of ψ is equal to m , and let $y_0 \in N$ be a given point such that $\psi(y_0) = x(0)$. Then there exists in N an arc $y(t)$, $0 \leq t \leq 1$, having initial point y_0 and covering $x(t)$, i.e., satisfying the condition $\psi(y(t)) = x(t)$, $0 \leq t \leq 1$.

Proof: Let $a = x(t_0)$, $\psi(b) = a$, and let x^1, \dots, x^m be local coordinates in M defined in some neighborhood of a and having origin a . Let also y^1, \dots, y^n be local coordinates in N defined in some neighborhood of $b \in N$ and having origin b . Finally let

$$x^i = \psi^i(y^1, \dots, y^n), \quad i = 1, \dots, m$$

be the coordinate representation of ψ in the vicinity of b . Since the rank of $\left\| \frac{\partial \psi^i}{\partial y_j} \right\|$, $i = 1, \dots, m$; $j = 1, \dots, n$ is equal to m

for $y^i = 0$, it follows that the matrix possesses m linearly independent columns. Suppose, for the sake of definiteness, that the first m columns are linearly independent. We introduce a new local coordinate system z^1, \dots, z^n in the vicinity of b by writing

$$z^i = \psi^i(y^1, \dots, y^n), \quad i = 1, \dots, m; \quad z^j = y^j,$$

$$j = m + 1, \dots, n.$$

In this system the coordinate representation of ψ in a sufficiently small neighborhood of b assumes the form

$$x^i = z^i, \quad i = 1, \dots, m,$$

where these relations define ψ for all z^1, \dots, z^n satisfying the condition $|z^j| < \delta$, $j = 1, \dots, n$, for some sufficiently small positive number δ . Let $\epsilon(b, t_0)$ be a positive number sufficiently small so that for $|t - t_0| \leq \epsilon(b, t_0)$ we have $|x^i(t)| < \delta$, where $x^i(t)$ are the coordinates of $x(t)$. We define $z(t) = (z^1(t), \dots, z^n(t))$ for $|t - t_0| \leq \epsilon(b, t_0)$ by writing $z^i(t) = x^i(t)$, $i = 1, \dots, m$; $z^j = 0$, $j = m + 1, \dots, n$. Thus we obtain an arc $z(t)$ which covers $x(t)$ on the interval $|t - t_0| \leq \epsilon(b, t_0)$ and which satisfies the condition $y(t_0) = b$. Since the collection of pairs (b, t_0) satisfying the condition $\psi(b) = x(t_0)$ is compact, there exists a positive number ϵ independent of b and t_0 and small enough so that for an arbitrary pair (b, t_0) satisfying $\psi(b) = x(t_0)$ there exists an arc $z(t)$, defined on the interval $|t - t_0| \leq \epsilon$ which covers $x(t)$ on that interval and satisfies the condition $z(t_0) = b$. If we now break the segment $[0, 1]$ into subintervals of length $\frac{1}{n} \leq \epsilon$ and construct $z(t)$ on each subinterval, beginning at y_0 , we obtain an arc having the desired properties.

Theorem 107: Every element $f \in G$ may be written in the form

$$f = ghg^{-1}; \quad g \in G, \quad h \in H.$$

(The notation here is that introduced in A.)

Proof: An equivalent assertion is that ψ maps $G \times H$ onto G . Since $\psi(G \times H)$ is closed in G (for G is compact, see Theorem 102) it suffices to prove that it is everywhere dense in G . Thus it is enough to show that

$$G \setminus \psi(G \times H) \subset \psi(G \times H) \quad (22)$$

since, as we know from the lemma and proposition C), the set $\psi(G \times H)$ is nowhere dense in G .

Let h_* be a fixed regular element belonging to H and let f be an arbitrary element of $G \setminus \psi(G \times H)$. Since h_* and f do not belong to $\psi(G \times H)$ it follows from the lemma and D) that there exists an arc $f(t)$ in $G \setminus \psi(G \times H)$ joining f to h_* . Hence, according to E), there also exists an arc $(g(t), h(t))$ in $G \times H$ beginning at (e, h_*) and covering $f(t)$, i.e., satisfying the condition

$$\psi(g(t), h(t)) = f(t).$$

But then, letting $t = 1$, we obtain

$$\psi(g, h) = f.$$

and the theorem follows.

Theorem 108: Every element $a \in R$ may be written in the form

$$a = g(b, \quad g \in G, \quad b \in S. \quad (23)$$

(Here again the notation is that introduced in A).)

Proof: Choose a spherical neighborhood U of the origin in R sufficiently small so that the conditions of proposition B) are satisfied for $K = H$. For given vector a and for sufficiently small positive ε we have $\varepsilon a \in U$. But then, according to Theorem 107, $\varphi(\varepsilon a)$ may be written in the form

$$\varphi(\varepsilon a) = ghg^{-1}, \quad g \in G, \quad h \in H,$$

and since $h = g^{-1} \varphi(\varepsilon a) g \in \varphi(U)$ it follows that $h = \varphi(\varepsilon b)$, $b \in S$. Thus

$$\varphi(\varepsilon a) = g\varphi(\varepsilon b)g^{-1},$$

whence, from B), we have $\varepsilon a = g(\varepsilon b)$ or, cancelling ε , $a = g(b)$.

Theorem 109: For any two regular subalgebras S and S' of the

same Lie algebra R there exists an automorphism $g \in G$ (see A)) such that

$$S' = g(S). \quad (24)$$

From this it follows that the root systems Σ and Σ' belonging to S and S' are likewise connected by the relation

$$\Sigma' = g(\Sigma). \quad (25)$$

In particular, the metric structure of a root system is an invariant of the algebra.

Proof: Let c and c' be regular elements in R giving rise to the regular subalgebras S and S' , respectively (see Theorem 104). By Theorem 108 we have $c' = g(c'')$, $g \in G$, $c'' \in S$. Moreover, since g is an automorphism, c'' is also regular. Let S'' denote the regular subalgebra determined by c'' . Since S'' consists of all elements commuting with c'' it follows that S'' contains S . But S and S'' have the same dimension so they must coincide. On the other hand, from $c' = g(c'')$ it follows that $S' = g(S'')$. Thus (24) is proved.

In order to verify (25) let $\alpha \in \Sigma$. For arbitrary $s \in S$ we have

$$[s, r_\alpha] = i(\alpha, s)r_\alpha.$$

But then, applying the automorphism g , we obtain

$$[s', g(r_\alpha)] = i(g(\alpha), s')g(r_\alpha)$$

for arbitrary $s' \in S'$. Thus $g(\alpha) \in \Sigma'$ (see Definition 51), i.e., $g(\Sigma) \subset \Sigma'$. Similarly, $g^{-1}(\Sigma') \subset \Sigma$, and the result follows.

Theorem 110: The universal covering group \tilde{G} of G (see A)) is compact.

Proof: The argument is somewhat indirect. We already know (see Definition 46) that $G = \tilde{G}/D$ where D is a discrete central subgroup of \tilde{G} which (Section 50, E)) is isomorphic with the fundamental group of G . Now \tilde{G} is compact if and only if D is finite (see Section 19, I)). The theorem will be proved by showing $\pi^1(G)$ to be finite.

Let U be a spherical neighborhood of the origin in R sufficiently small so that the conditions of B) are satisfied for $K = H$, and let h_* be an arbitrary but fixed regular point in $\varphi(U) \cap H = \varphi(S \cap U)$. If $f = f(t)$, $0 \leq t \leq 1$, is a closed path in G about h_* which passes through no point of the set Ξ of irregular elements, then there exists a path $(g, h) = (g(t), h(t))$ which is covering path for f with respect to ψ (see the lemma). The path h is then also free of irregular points. As the first step in the proof we show that if h is

closed then f is null-homotopic in G .

Suppose then that $h = h(t)$ is a closed path. Since $f(0) = h_* \in \varphi(U)$ it follows from B) that $h(0) = \varphi(s_*)$, $s_* \in S \cap U$. Moreover, φ is a covering mapping of S onto H (see Section 50, E)) and consequently there exists in S a path $s = s(t)$ with initial point s_* which is a covering path for h with respect to φ . We show first that s is also closed. Indeed, suppose $s(1) - s(0) \neq 0$. Then there exists a root vector $\alpha \in \Sigma$ such that $(\alpha, s(1) - s(0)) \neq 0$, and since $\varphi(s(1)) = \varphi(s(0))$, we must have $(\alpha, s(1) - s(0)) = 2k\pi$ where $k \neq 0$. Since $(\alpha, s(t))$ is a continuous function of t , there is at least one value of t for which $(\alpha, s(t))$ is itself a multiple of 2π . But, for such a t , $h(t) = \varphi(s(t)) = h_{s(t)}$ is irregular, which is impossible. Thus s is closed. Now the path s is certainly null-homotopic in S . Let $s_\tau = s_\tau(t)$ be a deformation carrying $s_0 = s$ into the null path at s_* . Then $f_\tau(t) = g(t) \varphi(s_\tau(t)) (g(t))^{-1}$ is a deformation carrying the path $f_0 = f$ into the path $f_1(t) = g(t) \varphi(s_*)(g(t))^{-1}$.

We note next that, since f and h are both closed paths, we have $g(0)h(0)(g(0))^{-1} = g(1)h(1)(g(1))^{-1} = g(1)h(0)(g(1))^{-1}$, i.e., $h(0) = h(1) = \varphi(s_*)$ commutes with $(g(0))^{-1}g(1)$. But then, according to B), $(g(0))^{-1}g(1)$ commutes with every element of the one-parameter subgroup $\varphi(ts_*)$. Thus we have

$$g(0)\varphi((1-\tau)s_*)(g(0))^{-1} = g(1)\varphi((1-\tau)s_*)(g(1))^{-1} = \chi(\tau) \quad (26)$$

Let now

$$f'_\tau(t) = g(t) \varphi((1-\tau)s_*)(g(t))^{-1} (\chi(\tau)^{-1}\chi(0)). \quad (27)$$

Then, f'_τ is a deformation carrying the path $f_0' = f_1$ into the null path at h_* . Thus $f \sim f_1 \sim 0$ and we see that if h is closed then f is null-homotopic.

Consider now the fundamental group $\pi^1 = \pi^1(G, h_*)$ with base point h_* . From D) and the local simple connectedness of G it follows that each path class belonging to π^1 contains a path disjoint from Ξ . In each path class we select one such path f and use E) to construct for it a fixed covering path $(g_f, h_f) = (g_f(t), h_f(t))$ having initial point (e, h_*) . If f_1 and f_2 are two such representative paths then the path products $g_{f_1}^{-1}g_{f_2}$ and $h_{f_1}^{-1}h_{f_2}$ may be formed in G and H respectively. The path $(g_{f_1}^{-1}g_{f_2}, h_{f_1}^{-1}h_{f_2})$ covers $f_1^{-1}f_2$ and, from what has just been proved, it follows that if $h_{f_1}^{-1}h_{f_2}$ is closed, i.e., if $h_{f_1}(1) = h_{f_2}(1)$, then $f_1^{-1}f_2 \sim 0$ and consequently $f_1 \sim f_2$. Equivalently, if $f_1 \sim f_2$ then $h_{f_1}(1) \neq h_{f_2}(1)$. Thus the association $\{f\} \rightarrow h_f(1)$ maps π^1 into H in a one-to-one fashion. Moreover, each element $h_f(1)$ is a conjugate of h_* ; indeed, $\psi(g_f(1), h_f(1)) = g_f(1)h_f(1)(g_f(1))^{-1} = h_*$. The proof will be completed by showing that there exist only a finite number

of elements of H that are conjugate to h_* .

In order to see this, we recall that the elements of H are all linear transformations on R having the vectors r_α , $\alpha \in \Sigma$, as eigenvectors. Thus if $h \in H$ then $h(r_\alpha) = \varepsilon_\alpha r_\alpha$, $\alpha \in \Sigma$, and h is uniquely determined by the assignment $\alpha \rightarrow \varepsilon_\alpha$ of its eigenvalues. But if h is conjugate to h_* its eigenvalues must coincide with those of h_* , and since only a finite number of assignments $\alpha \rightarrow \varepsilon_\alpha$ are possible when the numbers ε_α are restricted to run over the set of eigenvalues of h_* , the finiteness of the set of conjugates of h_* belonging to H is established, and the proof of the theorem is complete.

From Theorem 110 it follows that there exist only a finite number of connected Lie groups having Lie algebra R . Indeed, every such group is of the form \tilde{G}/N where N is a discrete central subgroup of \tilde{G} . But \tilde{G} is compact and has no continuous center (for any group with Lie algebra R has locally trivial center; see Theorem 91). Hence the center Z of \tilde{G} is a finite group and possesses only a finite number of distinct subgroups N . The particular group G introduced in A) has trivial center and is therefore isomorphic with \tilde{G}/Z so that Z is isomorphic with the fundamental group of G . In the following example we elucidate the structure of those connected Lie groups with non-trivial center having prescribed compact Lie algebra.

Example 106: Let R^* be a compact Lie algebra. According to Theorem 100, R^* resolves into the direct sum of its center C and a semi-simple compact subalgebra R . Let p denote the dimension of C . Let G be the component of the identity in the group of all automorphisms of R and let \tilde{G} be the universal covering group of G . According to Theorem 110, the center Z of \tilde{G} is finite, say of order r . We may now describe the most general connected Lie group having Lie algebra R^* . Let K denote, as usual, the additive group of real numbers reduced modulo 1, and denote by X its cyclic subgroup of order r , i.e., the subgroup generated by $\frac{1}{r}$.

Take $q \leq p$ exemplars K_1, \dots, K_q of K and construct the direct product F of the groups $\tilde{G}, K_1, \dots, K_q$, and an additive vector group B of dimension $p - q$. If X_i denotes the cyclic subgroup of K_i corresponding to the subgroup $X \subset K$, then the set of these elements in F whose orders divide r is the finite central subgroup $Y = X_1 X_2 \dots X_q Z$, and the most general connected Lie group having Lie algebra R^* is of the form F/U where U denotes an arbitrary subgroup of Y . In particular, there exist, up to isomorphism, only a finite number of such groups.

Proof: We regard the additive vector group C as a Lie group. The group $C \times \tilde{G}$ is then a simply connected Lie group having

Lie algebra R^* and center $C \times Z$, so that every connected Lie group with algebra R^* is on the form $(C \times \tilde{G})/N$ where N is a discrete subgroup of $C \times Z$. Form the intersection $N' = C \cap N$ (here C is regarded as a subgroup of $C \times G$: $C = C \times e$). Then N' is a discrete subgroup of C and, choosing a basis e_1, \dots, e_p in C in such a way that e_1, \dots, e_q is also a basis for N' (see Example 33), we see that $(C \times G)/N'$ may, in an obvious way, be identified with F . Moreover, if $n \in N$ then $n^r \in N'$, and it follows that, under this identification, N/N' is identified with a subgroup U of Y . Thus

$$(C \times \tilde{G})/N \approx F/U$$

and the result follows.

Example 107: Theorem 110 permits a deeper analysis of the structure of finite dimensional compact groups. By way of an example of its application we here prove the following result.

The most general compact connected finite dimensional group G may be obtained as follows: take a simply connected compact semi-simple Lie group L' and a compact connected finite dimensional commutative group H , form the direct product $L' \times H$, and factor out a finite central subgroup having only the identity element in common with H .

This proposition shows that all of the set theoretic complexity of such a group is "concentrated" in a commutative group, viz., in its center.

Proof: Let G be a compact connected finite dimensional group, and let L and N be, respectively, a local Lie group and zero-dimensional normal subgroup, such that G is locally the direct product of L and N (see Theorem 69). Forming the set of finite products of elements of L , we construct, as before (see Example 82) a homomorphism ψ of a connected global Lie group \hat{L} into G in such a way that \hat{L} contains L as a neighborhood of the identity and such that $\psi(\hat{L})$ is dense in G . We suppose \hat{L} to be simply connected (if it isn't we may replace it by its universal covering). Since G/N is compact the group L is locally isomorphic with a compact Lie group. Therefore \hat{L} resolves into the direct product of a vector group L_0 and a simply connected compact semi-simple group L' (see Example 106). Let $H = \psi(L_0)$; then H is a connected central subgroup of G . To each $(x, y) \in L' \times H$ we now assign the element $\varphi(x, y) = \psi(x)y \in G$. Since $\psi(\hat{L})$ is everywhere dense in G it follows that $\varphi(L' \times H) = G$ so that φ is a homomorphism of $L' \times H$ onto G . Since φ is the identity mapping on the factor H , while the center of L' is finite, it follows that the kernel

of φ is a finite group having only the identity element in common with H .

SECTION 65

THE CLASSICAL LIE ALGEBRAS AND THEIR ROOT SYSTEMS

This section is devoted to the classical compact Lie groups. We introduce the groups themselves and compute the Lie algebra and root system of each. It is customary to designate as classical four infinite series, A_n , B_n , C_n , $n \geq 1$; D_n , $n \geq 2$, of linear or matrix groups. Here A_n denotes the group of unimodular unitary matrices of order $n+1$; B_n the group of orthogonal matrices of order $2n+1$; C_n the group of symplectic matrices of order $2n$ or, what comes to the same thing, the group of unitary matrices of order $2n$ leaving invariant a fixed non-degenerate skew-symmetric bilinear form; D_n the group of orthogonal matrices of order $2n$. With the exception of D_2 these groups are simple and of rank n . Moreover, with a finite number of exceptions they are (locally) pairwise non-isomorphic.

A) Let E^r be a Euclidean space of dimension r , i.e., a real vector space of dimension r in which an ordinary real scalar product (u, v) is defined. We denote by \mathfrak{H}_r the collection of all linear automorphisms of E^r that preserve the scalar product, i.e., those linear automorphisms x of E^r satisfying

$$(x(u), x(v)) = (u, v). \quad (1)$$

Clearly \mathfrak{H}_r is a compact Lie group. The Lie algebra H_r of \mathfrak{H}_r consists of all those linear transformations a of E^r into itself satisfying the condition

$$(a(u), v) + (u, a(v)) = 0. \quad (2)$$

If we introduce an orthonormal basis in E^r then to each element $x \in \mathfrak{H}_r$ there corresponds an orthogonal matrix $\|x_k^j\|$ of order r , and conversely to each orthogonal matrix $\|x_k^j\|$ of order r there corresponds an element $x \in \mathfrak{H}_r$ (see Example 3). In this sense we may identify \mathfrak{H}_r with the group of orthogonal matrices of order r ; $x = \|x_k^j\|$. If this identification is made then H_r is identified with the linear Lie algebra (see Section 54, A)) of skew-symmetric matrices $a = \|a_k^j\|$ of order r , i.e., the matrices satisfying the condition

$$a^* + a = 0 \quad (3)$$

or, equivalently,

$$a_k^j + a_j^k = 0; \quad j, k = 1, \dots, r, \quad (4)$$

(j, k are not indices of summation). The complexification [H_r] is then the linear Lie algebra of skew-symmetric complex matrices of order r , i.e., those complex matrices $a = \|a_{kj}\|$ satisfying condition (3) or (4). As will be seen in the sequel, it is convenient to split the series of algebras H_r into two series: $r = 3, 5, 7, \dots$ and $r = 4, 6, 8, \dots$. Accordingly, we introduce the notation

$$\mathfrak{B}_n = \mathfrak{H}_{2n+1}, \quad B_n = H_{2n+1}, \quad n = 1, 2, \dots,$$

$$\mathfrak{D}_n = \mathfrak{H}_{2n}, \quad D_n = H_{2n}, \quad n = 2, 3, \dots.$$

Of the assertions made in proposition A) the only one requiring proof is that H_r consists of the transformations satisfying (2). To see this, let x_t be a one-parameter subgroup of the group of all linear automorphisms of E^r and let a be its direction transformation (see Section 54, B)). If x_t lies in \mathfrak{H}_r , then

$$(x_t(u), x_t(v)) = (u, v).$$

Differentiating this relation with respect to t at $t = 0$ we obtain (2). Suppose, on the other hand, that a satisfies (2); then (using Section 54, B) once again) we obtain

$$\frac{d}{dt} (x_t(u), x_t(v)) = (ax_t(u), x_t(v)) + (x_t(u), ax_t(v)) = 0,$$

whence it follows that $((x_t(t), x_t(v)) = (u, v)$. Thus the Lie algebra of \mathfrak{H}_r consists precisely of those transformations of E^r satisfying (2).

B) Let U^{n+1} be a unitary space of dimension $n+1$, i.e., a complex vector space of dimension $n+1$ in which a Hermitian scalar product (u, v) is defined. (A Hermitian scalar product is a complex valued function (u, v) of two vector variables u, v which is linear as a function of u , conjugate linear as a function of v , satisfies the identity $(\bar{u}, v) = (v, u)$, and is such that $(u, u) > 0$ for $u \neq 0$.)

Denote by \mathfrak{A}_n the group of all linear automorphisms of U^{n+1} which preserve the scalar product and have determinant +1, i.e., the collection of linear automorphisms x of U^{n+1} satisfying the conditions

$$(x(u), x(v)) = (u, v), \quad (5)$$

$$\det x = 1. \quad (6)$$

Clearly \mathfrak{M}_n is a compact Lie group. The Lie algebra A_n of \mathfrak{M}_n consists of all those linear transformations a of U^{n+1} into itself which satisfy the conditions

$$(a(u), v) + (u, a(v)) = 0, \quad (7)$$

$$\text{Tr}(a) = 0, \quad (8)$$

where, as always, $\text{Tr}(a)$ denotes the trace of a (see Section 31). If an orthonormal basis is selected in U^{n+1} then to each element $x \in \mathfrak{M}_n$ there corresponds a unimodular unitary matrix $\|x_k^j\|$ of order $n+1$, and conversely every unimodular unitary matrix $\|x_k^j\|$ of order $n+1$ determines an element $x \in \mathfrak{M}_n$. In this sense we may identify \mathfrak{M}_n with the group of unimodular unitary matrices of order $n+1$: $x = \|x_k^j\|$. If this identification is made then A_n is identified with the linear Lie algebra of complex matrices $a = \|a_k^j\|$ of order $n+1$ satisfying the conditions

$$\bar{a}^* + a = 0, \quad (9)$$

$$\text{Tr}(a) = 0, \quad (10)$$

or, equivalently,

$$\bar{a}_j^k + a_k^j = 0; \quad j, k = 1, \dots, n+1 \quad (11)$$

$$\sum_{j=1}^{n+1} a_j^j = 0, \quad (12)$$

(j, k are not indices of summation in (11)). The elements of A_n are thus written as complex matrices; nevertheless A_n is to be regarded as a real Lie algebra since it is the Lie algebra of an ordinary compact Lie group in which we may introduce real coordinates. The multiplication of an element of A_n by a real number is the ordinary multiplication of a complex matrix by a scalar; the addition of elements of A_n is the ordinary addition of complex matrices; the commutator is that defined in (1) Section 54. The complexification $[A_n]$ may be identified with the linear Lie algebra of complex matrices c of order $n+1$ satisfying the single condition

$$\text{Tr}(c) = 0, \quad (13)$$

but with complex conjugation in $[A_n]$, regarded as the complexification of A_n , given by

$$c \rightarrow -\bar{c}^*. \quad (14)$$

We show first that A_n consists of all those transformations a satisfying (7) and (8). Denote by \mathfrak{L}_{n+1} the (real) Lie group of all linear automorphisms of the complex vector space U^{n+1} . The Lie algebra L_{n+1} of \mathfrak{L}_{n+1} clearly consists of all linear transformations

of U^{n+1} into itself, considered as a real Lie algebra, and the fact that the subalgebra of L_{n+1} defined by (7) is the subalgebra corresponding to the subgroup of \mathfrak{L}_{n+1} defined by (5) may be proved exactly as in A). Denote by \mathfrak{L}^1_{n+1} the subgroup of \mathfrak{L}_{n+1} defined by (6) and by L^1_{n+1} the subalgebra of L_{n+1} defined by (8). It suffices to show that L^1_{n+1} is the subalgebra corresponding to \mathfrak{L}^1_{n+1} .

Let $x(t) = \|x_k^j(t)\|$ be a one-parameter subgroup of \mathfrak{L}_{n+1} and let $a = \|a_k^j\|$ be its direction transformation. Direct computation discloses that

$$\frac{d}{dt} \det \|x_k^j(t)\| \quad t=0 = \sum_{j=1}^{n+1} a_j^j.$$

In particular, if $x(t)$ belongs to \mathfrak{L}^1_{n+1} then $a \in L^1_{n+1}$. But then, since the dimension of \mathfrak{L}^1_{n+1} is one less than that of \mathfrak{L}_{n+1} , while the dimension of L^1_{n+1} is likewise one less than that of L_{n+1} , it follows that L^1_{n+1} corresponds to \mathfrak{L}^1_{n+1} .

It remains to show that the complexification of A_n may be identified with the complex algebra L_{n+1}^1 , but with complex conjugation in $[A_n]$ given by (14) rather than by $c \rightarrow \bar{c}$. By C) Section 58, every element $c \in [A_n]$ may be written as a formal sum

$$c = a + bi, \quad a \in A_n, \quad b \in A_n, \quad (15)$$

the element d conjugate to c being then given by the formal sum

$$d = a - bi. \quad (16)$$

Now if we interpret the operations of addition and multiplication by i in (15) as the ordinary operations on complex matrices then c belongs to L_{n+1}^1 . The proof will be completed by showing that the mapping of $[A_n]$ into L_{n+1}^1 thus obtained is one-to-one and onto. Indeed, let $c \in L_{n+1}^1$ and define

$$a = \frac{c - \bar{c}^*}{2}; \quad b = \frac{c - \bar{c}^*}{2i}; \quad (17)$$

Then (15) holds, while a and b satisfy (9) and (10). On the other hand, if (15) holds then a and b are given by (17). Finally, substituting in (16) the expressions for a and b given in (17), we obtain

$$d = -\bar{c}^*$$

Thus the proof of B) is complete.

In order to facilitate the ensuing computations, it will frequently be convenient to dissect a matrix of even order into a block matrix, the entries of which are matrices of order two. More precisely, if $x = \|y_k^j\|$, is a matrix of order $2n$, we shall write

$$x_q^p = \begin{vmatrix} y_{2q-1}^{2p-1} & y_{2q}^{2p-1} \\ y_{2q-1}^{2p} & y_{2q}^{2p} \end{vmatrix} = \begin{vmatrix} x_{q1}^{p1} & x_{q2}^{p1} \\ x_{q1}^{p2} & x_{q2}^{p2} \end{vmatrix}$$

and

$$x = \|x_q^p\|; p, q = 1, \dots, n. \quad (18)$$

In connection with this notation, it will likewise be convenient to make a special arrangement as regards the components of a vector u in a space of dimension $2n$. We shall write

$$u = (u^1, \dots, u^n) \text{ where } u^p = (u^{p1}, u^{p2}). \quad (19)$$

A simple computation shows that, in terms of this notation, the linear transformation $v = x(u)$ corresponding to x may be written in coordinate form as

$$v^p * = \sum_q x_q^p u^{q*} \quad (20)$$

where the expressions in (19) are regarded as row matrices and $x_q^p u^{q*}$ denotes a matrix product. (Recall that in order to obtain the coordinate expression for $v = x(u)$ as a matrix product it is necessary to write the components of the vectors as column matrices (see Section 31, (2)); hence the transpositions appearing in (20) and below.) Similarly, the bilinear form $x(u, v)$ determined by x has the coordinate expression

$$x(u, v) = uxv^* = \sum_{p,q} u^p x_q^p v^{q*} \quad (21)$$

and if $x = \|x_q^p\|$ and $x' = \|x'_q^p\|$ are two matrices of order $2n$, written as in (18), then

$$xx' = \|z_q^p\|, \text{ where } z_q^p = \sum_{\alpha=1}^n x^p x'^{\alpha}_q,$$

where $x^p x'^{\alpha}_q$ denotes the ordinary product of matrices of order two.

C) Let U^{2n} be a unitary space of dimension $2n$ equipped with a fixed orthonormal basis, and consider the bilinear form $f(u, v)$ defined, according to (21), by the matrix $f = \|f_q^p\|$ with entries

$$f_q^p = \delta_q^p \sigma; \quad p, q = 1, \dots, n, \quad \text{where } \sigma = \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix} \quad (22)$$

and δ_q^p is, as usual, defined to be 1 for $p = q$ and 0 otherwise. (Thus f is a diagonal block matrix with σ repeated n times down the diagonal.) We denote by \mathfrak{A}_n the collection of all linear

automorphisms x of U^{2^n} that preserve the bilinear form $f(u, v)$, i.e., satisfy the condition

$$f(x(u), x(v)) = f(u, v). \quad (23)$$

Let $\mathfrak{G}_n = \mathfrak{A}_n \oplus \mathfrak{A}_{2n-1}$ (see B). Then \mathfrak{G}_n is a compact Lie group. The Lie algebra K_n of the group \mathfrak{G}_n consists of all linear transformations a of U^{2^n} into itself satisfying the condition

$$f(a(u), v) + f(u, a(v)) = 0. \quad (24)$$

If a , regarded as a matrix, is written as in (18): $a = \|a_{pq}^p\|$; $p, q = 1, \dots, n$, then (24) is equivalent with either of the conditions

$$a_p{}^q * = \sigma a_q{}^p \sigma \text{ or } a_p{}^q = \sigma a_p{}^q * \sigma; p, q = 1, \dots, n \quad (25)$$

For the diagonal blocks $a_p{}^p$, (25) is equivalent with

$$\text{Tr}(a_p{}^p) = 0. \quad (26)$$

(As for the rest, the blocks $a_p{}^q$, $q < p$, are determined by the blocks $a_q{}^p$, which may be prescribed arbitrarily.) From (26) it follows that $\text{Tr}(a) = 0$. Consequently the Lie algebra C_n of \mathfrak{G}_n consists of all those linear transformations a of U^{2^n} into itself satisfying (25) and

$$\bar{a}^* + a = 0. \quad (27)$$

(See (9); as has been seen (10) is a consequence of (25).) The complexification $[C_n]$ may be identified with the algebra K_n , but with complex conjugation given in $[C_n]$ by

$$c \rightarrow -\bar{c}^*. \quad (28)$$

Proof of C). The fact that K_n consists of the transformations a satisfying (24) may be proved exactly as in A). In matrix notation (24) may be written

$$fa + a^*f = 0 \quad (29)$$

which, in view of (22) is easily seen to be equivalent with

$$\sigma a_q{}^p + a_q{}^p * \sigma = 0. \quad (30)$$

Finally, since $\sigma^{-1} = -\sigma$, (25) follows from (30). Moreover, for $p = q$, (25) yields $a_{p1}{}^{p1} = -a_{p2}{}^{p2}$, i.e., (26), while $a_{p2}{}^{p1}$ and $a_{p1}{}^{p2}$ remain arbitrary.

Each element $c \in [C_n]$ may be written as a formal sum

$$c = a + bi; \quad a \in C_n, \quad b \in C_n. \quad (31)$$

If, as in the proof of B), we suppose the formal operations in (31)

given their ordinary significance then, since $a \in C_n$, $b \in C_n$, we have $c \in K_n$. On the other hand, if $c \in K_n$ then the elements a and b defined by

$$a = \frac{c - \bar{c}^*}{2}, \quad b = \frac{c + \bar{c}^*}{2i},$$

satisfy (27) and therefore belong to C_n . Thus we may identify $[C_n]$ with K_n , and (28) follows as in B).

Theorem 111: All of the algebras A_n , B_n , C_n , D_n , with the exception of D_1 , are compact semi-simple Lie algebras of rank n , so that each contains an n -dimensional regular subalgebra S^n . In order to describe the root system $\Sigma(A_n)$ of A_n we suppose the subspace S^n imbedded in an $(n+1)$ -dimensional Euclidean space E^{n+1} . Then it is possible to select an orthogonal basis e_1, \dots, e_{n+1} in E^{n+1} , the elements of which are all of the same length, such that the root system $\Sigma(A_n)$ is given by

$$\Sigma(A_n) = \{e_j - e_k, j \neq k; j, k = 1, \dots, n+1\}, \quad (32)$$

As for the algebras B_n , C_n , D_n , it is possible, in each case, to select an orthogonal basis e_1, \dots, e_n in S^n , the elements of which are all of the same length, such that the respective root systems are given by

$$\Sigma(B_n) = \{\pm e_j, j = 1, \dots, n; \pm e_j \pm e_k, j < k; j, k = 1, \dots, n\}, \quad (33)$$

$$\Sigma(C_n) = \{\pm 2e_j, j = 1, \dots, n; \pm e_j \pm e_k, j < k; j, k = 1, \dots, n\}, \quad (34)$$

$$\Sigma(D_n) = \{\pm e_j \pm e_k, j < k; j, k = 1, \dots, n\}. \quad (35)$$

We note that in the case of the algebra A_n the regular subalgebra S^n is the subspace of E^{n+1} determined by the equation

$$s^1 + s^2 + \dots + s^{n+1} = 0 \quad (36)$$

in terms of the special basis referred to above.

Before launching into the proof of Theorem 111, we establish the following general criterion.

D) Let R be a compact Lie algebra, let S be a commutative subalgebra, and let $\Sigma' = \{\varphi_1, \dots, \varphi_k\}$ be a finite system of pure imaginary, non-zero, pairwise distinct, linear forms defined on S . Suppose the following conditions are satisfied: a) For each vector $s \neq 0$ in S there exists a linear form $\varphi_j \in \Sigma'$ such that $\varphi_j(s) \neq 0$. b) To each form $\varphi_j \in \Sigma'$ there corresponds a vector $r_j \neq 0$ belonging to the complexification $[R]$ such that $[s, r_j] = \varphi_j(s)r_j$ for all $s \in S$. c) The subspace S and the vectors r_j , $j = 1, \dots, k$, span $[R]$ as a complex vector space. Then R is semi-simple, S

is a regular subalgebra and, finally, if for each φ_j we select the vector a_j defined by the condition $i(a_j, s) = \varphi_j(s)$, $s \in S$, the resulting system of vectors a_1, \dots, a_k is a root system for R .

Proof: Since none of the forms φ_j , $\varphi_1 - \varphi_m$ is identically zero, the set on which any one vanishes is nowhere dense. Therefore there exists a vector $c \in S$ such that the numbers $\varphi_j(c)$, $j = 1, \dots, k$, are all distinct and different from zero. We choose any one such vector c and keep it fixed for the rest of the proof.

By c) every vector $a \in [R]$ can be written in the form

$$a = b + \sum_{j=1}^k \tau^j r_j, \quad b \in [S]. \quad (37)$$

Suppose that a commutes with c : $[c, a] = 0$ or, equivalently, $p_c(a) = 0$. Raising p_c to the power m , we have $(p_c)^m(a) = 0$, $m = 1, \dots, k$, and therefore, according to b),

$$0 = (p_c)^m(a) = \sum_{j=1}^k (\varphi_j(c))^m \tau^j r_j, \quad m = 1, \dots, k. \quad (38)$$

But, by virtue of the choice of the vector c , the determinant $|(\varphi_j(c))|^m$ is non-zero. Thus we must have $\tau^j = 0$, $j = 1, \dots, k$.

From this computation we easily derive several consequences:

(i) S is the commutant of c in R , i.e.,

$$a \in R \text{ and } [c, a] = 0 \text{ imply } a \in S. \quad (39)$$

Indeed, writing a as in (37) we have $a = b \in [S] \cap R = S$.

(ii) The vectors r_j , $j = 1, \dots, k$, are linearly independent modulo $[S]$, i.e., $[R]$ is the direct sum of $[S]$ and the one-dimensional complex subspaces R_j spanned by the vectors r_j . Indeed, if τ^1, \dots, τ^k satisfy $\sum_j \tau^j r_j = -b \in [S]$ then we have $a = 0$ in (37) and consequently $\tau^1 = \dots = \tau^k = 0$.

(iii) The center of R is trivial. Indeed, if a is a central element in R then $a \in S$ by (39) so that $0 = [a, r_j] = \varphi_j(a)r_j$, $j = 1, \dots, k$. But then $\varphi_j(a) = 0$, $j = 1, \dots, k$, and $a = 0$ because of a).

Now R is compact by hypothesis. Hence (iii) implies that R is also semi-simple (see Theorems 99 and 100). Write Q for the algebra of derivations p_s , $s \in S$, and define forms φ_j on Q by writing $\varphi_j(p_s) = \varphi_j(s)$. Then $\varphi_1, \dots, \varphi_k$ are eigenforms of Q by b) and since, by (ii), the expression (37) is unique, it follows from the way c was chosen that if $[c, a] = \varphi_j(c)a$ then $a \in R_j$, i.e., R_j is the eigenspace of φ_j . Moreover, the eigenspace of the zero form $\varphi = 0$ is $[S]$. Thus (ii) implies that Σ' is a complete list of non-zero eigenforms (see Section 62, B)), and the conditions of

Definition 51 are all satisfied. Hence the proof will be complete if we show that S is a regular subalgebra of R .

To verify the regularity of S we invoke Theorem 108: if S' denotes any regular subalgebra then there exists an element $c' \in S'$ and an automorphism g of R such that $g(c') = c$. Thus there exists a regular subalgebra $S'' = g(S')$ containing c . Since S'' is commutative it follows from (39) that $S'' \subset S$. But S'' is also a maximal commutative subalgebra. Hence $S = S''$ and the proof of D) is complete.

The proof of Theorem 111 consists of an explicit construction for each of the algebras A_n , B_n , C_n , D_n , of a commutative subalgebra S^n and a system of linear forms satisfying the conditions of proposition D).

Proof of Theorem 111. A_n) Let s^1, \dots, s^{n+1} be an arbitrary system of real numbers satisfying

$$s^1 + \dots + s^{n+1} = 0. \quad (40)$$

With this system we associate the matrix $s = \|s_k^j\|$, $j, k = 1, \dots, n+1$, where

$$s_k^j = i s^j \delta_k^j \quad (41)$$

The matrix s is a pure imaginary diagonal matrix of order $n+1$; it satisfies the conditions $\bar{s}^* + s = 0$ and $\text{Tr}(s) = 0$ (see (40)), and therefore belongs to A_n (see (9), (10)). The collection of all such matrices forms an n -dimensional commutative subalgebra S^n of A_n , and we turn to the construction of a system of linear forms and corresponding eigenmatrices in A_n satisfying the conditions of D).

Consider the matrix $r = r(p, q) = \|r_k^j\|$ defined for each pair of integers $p \neq q$; $p, q = 1, \dots, n+1$, by the formula

$$r_k^j = \delta_p^j \delta_q^k, \quad j, k = 1, \dots, n+1 \quad (42)$$

The sole non-zero entry of $r(p, q)$ is $r_q^p = 1$. Since $p \neq q$ we have $\text{Tr}(r) = 0$ so that $r \in [A_n]$. Let $t = \|t_k^j\|$ denote the commutator $[s, r] = sr - rs$. Then

$$\begin{aligned} t_k^j &= \sum_{\alpha} i s^j \delta_{\alpha}^j \delta_{p^{\alpha}} \delta_{q^{\alpha}} - \sum_{\alpha} i \delta_p^j \delta_{q^{\alpha}} s^{\alpha} \delta_k^{\alpha} \\ &= i s^j \delta_p^j \delta_q^k - i s^q \delta_p^j \delta_k^q = i(s^p - s^q) r_k^j. \end{aligned}$$

In other words,

$$[s, r(p, q)] = i(s^p - s^q) r(p, q) \quad (43)$$

Now $i(s^p - s^q)$ is a pure imaginary linear form on S^n , and if we denote by Σ' the system of all such forms, $p \neq q$, then, as is easily seen, the conditions of D) are all satisfied for Σ' and $S = S^n$. Indeed, a) is clear, b) is verified in (43), and c) holds because of (13).

It remains to construct the orthogonal basis referred to in the statement of the theorem. To this end we compute the scalar product (s, s) of a vector $s \in S^n$ with itself. By definition (see C) Section 61) we have $(s, s) = -\text{Tr}(p_s p_s)$ and since each number $i(s^p - s^q)$ is an eigenvalue of p_s , and the numbers $i(s^p - s^q)$ exhaust the collection of non-zero eigenvalues, we have

$$\begin{aligned} (s, s) &= -\text{Tr}(p_s p_s) = -\sum_{p,q=1}^{n+1} i^2 (s^p - s^q)^2 = (2n+2) \sum_{p=1}^{n+1} (s^p)^2 \\ &\quad - 2 \sum_{p,q=1}^{n+1} s^p s^q = 2n \sum_{p=1}^{n+1} (s^p)^2 - 4 \sum_{p < q} s^p s^q = \\ &= (2n+2) \sum_{p=1}^{n+1} (s^p)^2 - 2 \left(\sum_{p=1}^{n+1} s^p \right)^2 = (2n+2) \sum_{p=1}^{n+1} (s^p)^2, \end{aligned}$$

(see (40)). We may regard s^1, \dots, s^{n+1} as the coordinates of s with respect to a basis f_1, \dots, f_{n+1} in a Euclidean space E^{n+1} in which the scalar product of a vector with itself is given by the formula

$$(s, s) = (2n+2) \sum_{p=1}^{n+1} (s^p)^2.$$

Then S^n is given as a subspace of E^{n+1} by (40). The basis f_1, \dots, f_{n+1} is orthogonal and its elements are all of length $\sqrt{2n+2}$. Clearly the vector

$$\alpha(p, q) = \frac{1}{2n+2} f_p - \frac{1}{2n+2} f_q$$

satisfies the condition $(\alpha(p, q), s) = s^p - s^q$. Thus, letting $e_p = \frac{1}{2n+2} f_p$, we obtain a basis e_1, \dots, e_{n+1} in E^{n+1} satisfying the conditions stated in the theorem.

C_n) The matrices of $[C_n]$ will be written, as in (18), as block matrices with entries of order two. Let

$$\tau = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix}. \quad (44)$$

With each sequence s^1, \dots, s^n of real numbers we associate a matrix $s = \|s_k^j\|$, $j, k = 1, \dots, n$, where

$$s_k^j = i s^j \delta_k^j \tau \quad (45)$$

Then s is a diagonal matrix of order $2n$ satisfying (26) and (27), and therefore belongs to C_n . The collection of all such matrices constitutes an n -dimensional commutative subalgebra S^n of C_n , and we turn to the construction of a system of linear forms and corresponding eigenmatrices satisfying the conditions of D).

Consider the two-by-one matrices

$$p(\epsilon) = \begin{vmatrix} 1 + \epsilon \\ 1 - \epsilon \end{vmatrix}, \quad \epsilon = \pm 1.$$

It is easily verified that

$$\tau p(\epsilon) = \epsilon p(\epsilon) \quad (46)$$

so that $p(+1)$ and $p(-1)$ are eigenvectors of τ written as column matrices. Transposing (46) we obtain

$$p^*(\epsilon) \tau = \epsilon p^*(\epsilon). \quad (47)$$

Now the product $\rho(\delta) p^*(\epsilon)$; $\delta = \pm 1$, $\epsilon = \pm 1$, is a square matrix of order two depending on the parameters δ, ϵ . Moreover, according to (46) and (47) we have

$$s^p \tau \rho(\delta) p^*(\epsilon) - s^q \rho(\delta) p^*(\epsilon) \tau = (\delta s^p - \epsilon s^q) \rho(\delta) p^*(\epsilon). \quad (48)$$

Note also that $(\delta) \rho^*(-\delta)$ satisfies the condition

$$\text{Tr}(\rho(\delta) \rho^*(-\delta)) = 0. \quad (49)$$

We now define matrices $r = r(p, q, \delta, \epsilon) = \|r_k^j\|$ depending on the integral parameters p, q, δ, ϵ ; $p \leq q$, $p, q = 1, \dots, n$; $\delta = \pm 1$, $\epsilon = \pm 1$, and satisfying the condition $\delta = -\epsilon$ when $p = q$. In the notation (18) the matrix r is given by

$$r_k^j = \delta_p^j \delta_q^k \rho(\delta) \rho^*(\epsilon) + \delta_q^j \delta_p^k \sigma \rho(\epsilon) \rho^*(\delta) \sigma, \quad p < q, \quad (50)$$

$$r_k^j = \delta_p^j \delta_p^k \rho(\delta) \rho^*(-\delta), \quad p = q, \quad (51)$$

where σ denotes the matrix (22). For $p < q$ the matrix $r(p, q, \delta, \epsilon)$ has but two non-zero entries, viz., $r_q^p = \rho(\delta) \rho^*(\epsilon)$ and $r_p^q = \sigma \rho(\epsilon) \rho^*(\delta) \sigma$, and therefore belongs to $[C_n]$. On the other hand $r(p, p, \delta, -\delta)$ has but one non-zero entry, viz., $r_p^p = \rho(\delta) \rho^*(-\delta)$, and likewise belongs to $[C_n]$ because of (49). From (45) and (48) it follows by direct computation that

$$[s, r(p, q, \delta, \epsilon)] = i(\delta s^p - \epsilon s^q) r(p, q, \delta, \epsilon), \quad p < q, \quad (52)$$

$$[s, r(p, p, \delta, -\delta)] = 2i\delta s^p r(p, p, \delta, -\delta). \quad (53)$$

Once again, it may be verified that for the system Σ' of linear forms $i(\delta s^p - \varepsilon s^q)$, $p < q$; and $2i\delta s^p$, with the corresponding eigenmatrices $r(p, q, \delta, \varepsilon)$, $p < q$; $r(p, p, \delta, -\delta)$, the conditions of D) are all satisfied. Moreover, just as in the case of the algebra A_n , it is easily seen that

$$(s, s) = \nu \sum_{p=1}^n (s^p)^2, \quad (54)$$

where ν is a number depending only on n . From this and D) the validity of (34) follows at once.

D_n) Here again we employ the notation (18) to write an arbitrary matrix $a \in [D_n]$ in the form $a = \|a_k^j\|$; $j, k = 1, \dots, n$, where each a_k^j is a matrix of order two, so that condition (3), which defines $[D_n]$, assumes the form

$$a_j^k * + a_j^k = 0. \quad (55)$$

This shows that the entries a_k^j , $j < k$, may be chosen arbitrarily, while the entries a_k^j , $j > k$, are then uniquely determined; the entries a_j^j must be skew-symmetric, of course. This time we associate with each system s^1, \dots, s^n of real numbers the matrix $s = \|s_k^j\|$; $j, k = 1, \dots, n$, where, in terms of (18),

$$s_k^j = s^j \delta_k^j \sigma \quad (56)$$

(see (22)). Then s is a real skew-symmetric matrix of order $2n$ and therefore belongs to D_n . Once again the collection of such matrices constitutes an n -dimensional commutative subalgebra S^n of D_n , and we turn to the construction of a system of linear forms and corresponding eigenmatrices satisfying the conditions of D).

This time consider the two-by-one matrices

$$\pi(\varepsilon) = \begin{vmatrix} 1 \\ i\varepsilon \end{vmatrix}, \quad \varepsilon = \pm 1. \quad (57)$$

It is easily verified that

$$\sigma \pi(\varepsilon) = i\varepsilon \pi(\varepsilon). \quad (58)$$

so that $\pi(+1)$ and $\pi(-1)$ are eigenvectors of σ written as column matrices. Transposing (58), we obtain

$$\pi^*(\varepsilon) \sigma = -i\varepsilon \pi^*(\varepsilon). \quad (59)$$

The product $\pi(\delta) \pi^*(\varepsilon)$, $\delta = \pm 1$, $\varepsilon = \pm 1$ is then a square matrix of order two depending on the parameters δ, ε , which, by (57) and (58), satisfies

$$s^p \sigma \pi(\delta) \pi^*(\varepsilon) - s^q \pi(\delta) \pi^*(\varepsilon) \sigma = i(\delta s^p + \varepsilon s^q) \pi(\delta) \pi^*(\varepsilon). \quad (60)$$

Once again we define matrices $r = r(p, q, \delta, \epsilon) = \|r_{k^j}\|$, depending on the integral parameters p, q, δ, ϵ ; $p < q$; $p, q = 1, \dots, n$; $\delta = \pm 1, \epsilon = \pm 1$. In the notation (18):

$$r_{k^j} = \delta_p^{j^1} \delta_p^{j^2} \pi(\delta) \pi^*(\epsilon) - \delta_q^{j^1} \delta_p^{j^2} \pi(\epsilon) \pi^*(\delta), \quad p < q. \quad (61)$$

Here r has the two non-zero entries $r_q^p = \pi(\delta) \pi^*(\epsilon)$ and $r_p^q = -\pi(\epsilon) \pi^*(\delta)$, so that r satisfies (55) and consequently belongs to $[D_n]$. From (56) and (60) it follows by direct computation that

$$[s, r(p, q, \delta, \epsilon)] = i(\delta s^p + \epsilon s^q) r(p, q, \delta, \epsilon), \quad p < q. \quad (62)$$

As before it may be verified without difficulty that for the system Σ' of linear forms $i(\delta s^p + \epsilon s^q)$, $p < q$; $p, q = 1, \dots, n$; $\delta = \pm 1, \epsilon = \pm 1$, with corresponding eigenmatrices $r(p, q, \delta, \epsilon)$, $p < q$, the conditions of D) are all satisfied, and that

$$(s, s) = \mu \sum_{p=1}^n (s^p)^2,$$

where μ is a number depending only on n . From this and D) the validity of (35) follows at once.

B_n) A skew-symmetric matrix b of order $2n + 1$ may be dissected in the following fashion:

$$b = \begin{vmatrix} a & -u^* \\ u & 0 \end{vmatrix}$$

where a is a skew-symmetric matrix of order $2n$ and u is a row matrix of length $2n$. In particular, b is determined by its submatrix a and the row u , and we write $b = \{a, u\}$. It will be convenient to identify the matrix a with the larger matrix $\{a, 0\}$ obtained from it by bordering it with 0's. In this way D_n and its regular subalgebra S^n constructed above (see D_n) become, respectively, a subalgebra and a commutative subalgebra of B_n . Moreover, the eigenmatrices $r(p, q, \delta, \epsilon)$, $p < q$, constructed for $[D_n]$ are turned into eigenmatrices of $[B_n]$. However, the complex linear span of S^n and the matrices $r(p, q, \delta, \epsilon)$ is $[D_n] \neq [B_n]$, so the system Σ' of linear forms constructed in D_n must be enlarged in order to take care of B_n . To this end we introduce row matrices $u = u(p, \delta)$, depending on the integral parameters $p = 1, \dots, n$; $\delta = \pm 1$, by writing, in the notation (19),

$$u^j = \delta_p^j \pi^*(\delta) \quad (63)$$

where π denotes the matrix (57). Bordering the zero matrix with the row $u(p, \delta)$ we obtain the matrix $r(p, \delta) = \{0, u(p, \delta)\} \in [B_n]$, for which (see 56), (58)) we have

$$[s, r(p, \delta)] = i\delta s^p r(p, \delta). \quad (64)$$

Since every element of $[B_n]$ of the form $\{0, u\}$ may be written as a complex linear combination of the eigenmatrices $r(p, \delta)$, $p = 1, \dots, n$; $\delta = \pm 1$, the conditions of proposition D) are, once again, easily verified for the system of eigenforms $i(\epsilon s^p + \delta s^q)$, $p < q$, and $i\delta s^p$; $p, q = 1, \dots, n$; $\delta, \epsilon = \pm 1$, and the validity of (33) follows exactly as before. Thus the proof of Theorem 111 is complete.

E) The dimensions of the algebras A_n, B_n, C_n, D_n are, respectively, $n^2 + 2n, 2n^2 + n, 2n^2 + n, 2n^2 - n$.

Since the dimension of each algebra is n plus the number of vectors in its root system (see Section 63, E)) this is an immediate consequence of Theorem 111.

Theorem 112: The algebras A_n, B_n, C_n , $n \geq 1$, and D_n , $n \geq 3$, are all simple. The algebras A_1, B_1 , and C_1 are mutually isomorphic, as are the pairs B_2 and C_2 and A_3 and D_3 . Aside from these exceptions the classical algebras are pairwise non-isomorphic. Thus a complete catalog of pairwise non-isomorphic classical Lie algebras is given by the following series:

$$A_n, n \geq 1; B_n, n \geq 2; C_n, n \geq 3; D_n, n \geq 4.$$

The algebra D_2 resolves into the direct sum of two copies of A_1 .

Proof: Since the rank of an algebra is an invariant it is clear that no two algebras A_n, B_n, C_n, D_n with different subscripts can be isomorphic. Moreover, the dimension is also invariant so an isomorphism between A_n and B_n or between A_n and C_n is impossible unless $n^2 + 2n = 2n^2 + n$, i.e., unless $n = 1$ (see E)). Similarly, A_n and D_n can be isomorphic only when $n^2 + 2n = 2n^2 - n$, i.e., when $n = 3$. Finally, an isomorphism between B_n and D_n or between C_n and D_n is never possible since $2n^2 + n = 2n^2 - n$ implies $n = 0$.

In order to see that B_n and C_n are not isomorphic for $n > 2$ we observe that the root systems of these algebras contain vectors of only two different lengths and that $\Sigma(B_n)$ contains exactly $2n$ vectors of the shorter length while $\Sigma(C_n)$ contains $2n^2 - 2n > 2n$ such vectors when $n > 2$. Thus the root systems of B_n and C_n are not isometric for $n > 2$, whence it follows that the algebras themselves are not isomorphic (see Theorem 109).

The root systems $\Sigma(A_1), \Sigma(B_1), \Sigma(C_1)$ all consist of two mutually opposed vectors and are therefore similar. Thus, according to Section 63, B) and Theorem 106, A_1, B_1 and C_1 are all

isomorphic with the vector-product algebra of Example 93 (see also Example 105).

The root systems $\Sigma(B_2)$ and $\Sigma(C_2)$ have the form

$$\Sigma(B_2) = \{\pm e_1; \pm e_2; \pm e_1 \pm e_2\},$$

$$\Sigma(C_2) = \{\pm 2e'_1; \pm 2e'_2; \pm e'_1 \pm e'_2\}.$$

Thus the linear transformation defined by

$$e_1 \rightarrow e'_1 + e'_2,$$

$$e_2 \rightarrow e'_1 - e'_2,$$

carries $\Sigma(B_2)$ onto $\Sigma(C_2)$ and, since this is a similarity, B_2 and C_2 are isomorphic.

The root systems $\Sigma(A_3)$ and $\Sigma(D_3)$ have the form

$$\Sigma(A_3) = \{e'_j - e'_k, j \neq k; j, k = 1, \dots, 4\},$$

$$\Sigma(D_3) = \{\pm e_j \pm e_k, j < k = 2, 3\}.$$

Thus, in this case, the linear transformation defined by

$$e_1 \rightarrow \frac{e'_1 + e'_2 - e'_3 - e'_4}{2}$$

$$e_2 \rightarrow \frac{e'_1 - e'_2 + e'_3 - e'_4}{2}$$

$$e_3 \rightarrow \frac{e'_1 - e'_2 - e'_3 + e'_4}{2}$$

carries $\Sigma(D_3)$ onto $\Sigma(A_3)$ and, since this transformation is actually an isometry, A_3 and D_3 are isomorphic.

Thus all questions concerning the existence of isomorphisms between the various classical algebras are settled. It remains to establish their simplicity.

We employ H) Section 63. Suppose first that $\Sigma(A_n)$ reduces into subsystems Σ_1 and Σ_2 . Say, for the sake of definiteness, $e_1 - e_2 \in \Sigma_1$, $e_j - e_k \in \Sigma_2$. Since $e_1 - e_2$ is orthogonal to $e_j - e_k$ both j and k are distinct from 1 and 2. But then $e_1 - e_j$ can belong to neither Σ_1 nor Σ_2 since it is not orthogonal to either of $e_1 - e_2$, $e_j - e_k$. Thus $\Sigma(A_n)$ is irreducible, and A_n is simple. Now each of the root systems $\Sigma(B_{n+1})$, $\Sigma(C_{n+1})$, $\Sigma(D_{n+1})$ contains a copy of $\Sigma(A_n)$ as a subsystem (see (32), (33), (34), (35)). Hence if any one of these systems reduced into subsystems Σ_1 and Σ_2 then $\Sigma(A_n)$ would have to be entirely contained in one of the two, say in Σ_1 . Thus Σ_2 would consist of vectors orthogonal to

$\Sigma(A_n) \subset \Sigma_1$, i.e., vectors of the form $\lambda(e_1 + \dots + e_n)$. But this condition is satisfied only in the case of $\Sigma(D_2)$. Hence A_n, B_n, C_n ; $n \geq 1$ and $D_n, n \geq 3$, are all simple. Finally, it is clear that $\Sigma(D_2)$ splits into two subsystems, each similar to $\Sigma(A_1)$. Thus the proof of Theorem 112 is complete.

In Example 91 there was begun a catalog of the centers and the fundamental groups of the classical compact Lie groups. The compilation will be completed below in Example 108. We here summarize under one heading the results of these investigations.

F) Let $G(R)$ denote the (unique) connected, simply connected Lie group having compact semi-simple Lie algebra R . Then for the classical Lie algebras we have:

- a) The center of $G(A_n)$ is a cyclic group of order $n+1$;
- b) The center of $G(B_n)$ is a cyclic group of order two;
- c) The center of $G(C_n)$ is a cyclic group of order two;
- d) The center of $G(D_n)$, $n \geq 2$, is a group of order four; for even n it is the direct sum of two cyclic groups of order two, while for odd n it is cyclic.

Since $G(R)$ is also an invariant of R (see Theorem 80), proposition F) opens up the possibility of distinguishing between most pairs of classical algebras without any appeal to their root systems. This line of argument fails, however, in the case of $G(B_n)$ and $G(C_n)$, which have the same dimension and the same center, and the proof that B_n and C_n are not isomorphic rests essentially on Theorem 109 and the concepts of Section 64. This essential part of the classification theorem is frequently omitted (see for example [13]).

Example 108: We here show that \mathfrak{A}_n and \mathfrak{C}_n are connected and simply connected (i.e., that $\mathfrak{A}_n = G(A_n)$, $\mathfrak{C}_n = G(C_n)$ in the notation of F)) and that the center of \mathfrak{A}_n is a cyclic group of order

$n+1$ generated by $(\cos \frac{2\pi}{n+1} + i \sin \frac{2\pi}{n+1})e$, where e denotes the identity matrix, while the center of \mathfrak{C}_n consists of just the two elements e and $-e$.

We first note that \mathfrak{A}_1 and \mathfrak{C}_1 coincide and are isomorphic with the group of quaternions of modulus one (see Section 26, A)). Indeed, for $n=1$ conditions (23) reduces to (6) so $\mathfrak{A}_1 = \mathfrak{C}_1$. Let

$$z = \begin{vmatrix} z_1^1 & z_2^1 \\ z_1^2 & z_2^2 \end{vmatrix}$$

be a complex matrix of order two; the conditions for z to belong

to \mathfrak{A}_1 are

$$\begin{aligned} z_1^1 \bar{z}_1^1 + z_2^1 \bar{z}_2^1 &= 1, & z_1^2 \bar{z}_1^2 + z_2^2 \bar{z}_2^2 &= 1, \\ z_1^1 \bar{z}_1^2 + z_2^1 \bar{z}_2^2 &= 0, & z_1^1 z_2^2 - z_1^2 z_2^1 &= 1. \end{aligned} \tag{65}$$

Letting $x = z_1^1$, $y = z_2^1$, we learn from (65) that $z_1^2 = -\bar{y}$, $z_2^2 = \bar{x}$. Thus a matrix z belonging to \mathfrak{A}_1 is of the form

$$z = \begin{vmatrix} x & y \\ -\bar{y} & \bar{x} \end{vmatrix}, \quad x\bar{x} + y\bar{y} = 1.$$

With each such matrix z we associate the quaternion $\varphi(z) = x + yj$. Then φ is a homeomorphism of \mathfrak{A}_1 onto the group of quaternions of modulus one. It may readily be verified that φ is also an isomorphism.

We regard \mathfrak{A}_n as a group of linear automorphisms of a unitary space U^{n+1} . Since the Hermitian form (x, x) is invariant under \mathfrak{A}_n the set S^{2n+1} of points x satisfying the condition $(x, x) = 1$ is also invariant under the action of \mathfrak{A}_n . If we regard the complex space U^{n+1} as a real space of double the dimension, then S^{2n+1} is just the unit sphere of dimension $2n+1$ in this space. Similarly, if we regard \mathfrak{C}_n as a group of linear automorphisms of the unitary space U^{2n} , then this group leaves invariant the unit sphere S^{4n-1} of dimension $4n-1$. We shall show that \mathfrak{C}_n acts transitively on S^{4n-1} with stabilizer subgroup \mathfrak{C}'_{n-1} isomorphic with \mathfrak{C}_{n-1} . Let p denote the first vector in the basis for U^{2n} with respect to which f has the form (22). It is easily verified that a transformation $u \in \mathfrak{C}_n$ that leaves the vector p fixed also leaves fixed the second vector in the basis and hence the stabilizer subgroup leaving p fixed is isomorphic with \mathfrak{C}_{n-1} . Denote now by M the set of all points into which p is carried by transformations belonging to \mathfrak{C}_n . Then \mathfrak{C}_n acts as a transitive transformation group on the manifold M , the dimension of which must therefore be equal to the difference between the dimensions of \mathfrak{C}_n and \mathfrak{C}_{n-1} , i.e., to $4n-1$. Since M is a submanifold of the sphere S^{4n-1} whose dimension is also $4n-1$, it follows that $M = S^{4n-1}$, i.e., that \mathfrak{C}_n acts transitively on S^{4n-1} . Hence the manifold $\mathfrak{C}_n/\mathfrak{C}'_{n-1}$ is homeomorphic with S^{4n-1} . In exactly the same way it may be shown that the manifold $\mathfrak{A}_n/\mathfrak{A}'_{n-1}$ is homeomorphic with S^{2n+1} . From this it follows immediately that if the groups \mathfrak{A}_{n-1} and \mathfrak{C}_{n-1} are connected then so are \mathfrak{A}_n and \mathfrak{C}_n and, since \mathfrak{A}_1 and \mathfrak{C}_1 have been seen to be connected, it follows by induction that all of the groups \mathfrak{A}_n , \mathfrak{C}_n are connected. Moreover, from the results of Example 90 it follows

that the fundamental groups of the manifolds \mathfrak{A}_n , \mathfrak{C}_n are all isomorphic with the fundamental group of a three-dimensional sphere, i.e., are trivial. In other words, these groups are also simply connected.

Since the linear groups \mathfrak{A}_n and \mathfrak{C}_n act transitively on the unit sphere they constitute irreducible sets of linear transformations and the center of each must therefore consist of scalar matrices only (see Section 31, E)). From this it follows easily that the centers of \mathfrak{A}_n and \mathfrak{C}_n have the state form.

SECTION 66 THE CLASSIFICATION OF COMPACT SIMPLE LIE ALGEBRAS

In this section we complete the proof of the theorem, first announced in Section 58, that an arbitrary compact simple Lie algebra is isomorphic either with one of the algebras

$$A_n, n \geq 1; \quad B_n, n \geq 2; \quad C_n, n \geq 3; \quad D_n, n \geq 4$$

constructed in the preceding paragraph, or else with one of five exceptional algebras

$$G_2, F_4, E_6, E_7, E_8,$$

the existence of which, however, will not be proved in this book. According to the results of the preceding sections, the classification of simple Lie algebras reduces to the classification of their root systems, and it is to the latter problem that the present section is addressed. By its very definition a root system is the root system of some Lie algebra, while, in order to obtain a complete classification, we need an abstract characterization of a root system. Thus we are lead to the introduction of the auxiliary concept of a σ -system, a collection of vectors possessing certain characteristic properties of root systems. As it happens, every irreducible σ -system is, in fact, similar with the root system of some compact simple Lie algebra, but that will not be proved here for the five σ -systems corresponding to the five exceptional algebras, since these algebras will not be constructed. The classification of σ -systems follows the usual method.

A) Let Γ be a system of non-zero vectors in a Euclidean space possessing the property that for every pair of vectors λ and μ belonging to Γ the ratio $\frac{2(\lambda, \mu)}{(\lambda, \lambda)}$ is an integer. Denote by φ the angle between the two non-collinear vectors α and β belonging to Γ and suppose, for the sake of definiteness, that $(\alpha, \alpha) \leq (\beta, \beta)$. Then

we have

$$\cos \varphi = \frac{\epsilon}{2} \sqrt{r}, \quad \epsilon = \pm 1, \quad r = 0, 1, 2, 3, \quad (1)$$

$$\text{if } r \neq 0 \text{ then } \frac{(\beta, \beta)}{(\alpha, \alpha)} = r, \quad (2)$$

$$\text{if } r \neq 0 \text{ then } \frac{2(\alpha, \beta)}{(\alpha, \alpha)} = \epsilon r; \quad \frac{2(\alpha, \beta)}{(\beta, \beta)} = \epsilon, \quad (3)$$

$$\text{if } r = 0 \text{ then } \frac{2(\alpha, \beta)}{(\alpha, \alpha)} = \frac{2(\alpha, \beta)}{(\beta, \beta)} = 0. \quad (4)$$

The lengths of α and β are unrelated for $r = 0$.

Indeed let

$$p = \frac{2(\alpha, \beta)}{(\alpha, \alpha)} \quad q = \frac{2(\alpha, \beta)}{(\beta, \beta)} \quad (5)$$

Then

$$\cos^2 \varphi = \frac{(\alpha, \beta)^2}{(\alpha, \alpha)(\beta, \beta)} = \frac{pq}{4} \quad (6)$$

But now $|p| \geq |q|$, since $(\alpha, \alpha) \leq (\beta, \beta)$ by hypothesis, so that the only possibilities for p and q are as follows:

$$\begin{aligned} p &= 0, q = 0; \quad p = \pm 1, q = \pm 1; \\ p &= \pm 2, q = \pm 1; \quad p = \pm 3, q = \pm 1. \end{aligned} \quad (7)$$

(Observe that $pq = 4$ is excluded by the non-collinearity of α and β .) Moreover, if $(\alpha, \beta) \neq 0$ we may divide the equations (5) by one another, obtaining

$$\frac{(\beta, \beta)}{(\alpha, \alpha)} = \frac{p}{q} \quad (8)$$

The validity of A) now follows immediately from (5), (6) (7) and (8).

B) A system Γ of non-zero vectors in a Euclidean space will be called a σ -system if the following two conditions are satisfied:

a) If $\lambda \in \Gamma$ and if r is an integer then $r\lambda \in \Gamma$ when and only when $r = \pm 1$.

b) For any two non-collinear vectors λ and μ belonging to Γ , if $l \geq 0$ and $m \geq 0$ denote the largest integers with the property that all of the vectors $\mu - j\lambda$ belong to Γ for $j = l, l-1, \dots, 1, 0, -1, \dots, -m$, then

$$l-m = \frac{2(\lambda, \mu)}{(\lambda, \lambda)} \quad (9)$$

It follows from Theorem 105 that a root system of a compact semi-simple Lie algebra is a σ -system.[†]

Theorem 113. In any σ -system Γ it is possible to select a linearly independent subsystem $B = \{\beta_1, \dots, \beta_n\}$, such that the following two conditions are satisfied:

- 1) If α and β are distinct vectors belonging to B then

$$(\alpha, \beta) \leq 0. \quad (10)$$

- 2) Every vector $\lambda \in \Gamma$ may be written (uniquely) in the form

$$\lambda = \varepsilon (a^1 \beta_1 + \dots + a^n \beta_n), \quad (11)$$

where $\varepsilon = \pm 1$ while a^1, \dots, a_n are non-negative integers. Moreover the given σ -system Γ is uniquely determined by any such subsystem B in the sense that the metric properties of B determined which linear forms (11) yield vectors belonging to Γ .

Proof. By hypothesis Γ is contained in a Euclidean space S . Fix a basis in S and use it to define an order relation as in Section 63, F). We first observe that any set x_1, \dots, x_m of positive vectors in S satisfying the condition

$$(x_j, x_k) \leq 0, \quad j \neq k, \quad (12)$$

is automatically linearly independent.

Indeed, suppose x_1, \dots, x_m satisfy the stated condition and are linearly dependent. Let y_1, \dots, y_n be a minimal linearly dependent subsystem. Then there exist coefficients b^1, \dots, b^n , all distinct from zero, such that

$$b^1 y_1 + \dots + b^n y_n = 0 \quad (13)$$

Among these coefficients there must appear both positive and negative numbers since the vectors y_1, \dots, y_n are all positive by hypothesis. Denote by u the sum of the terms in (13) having positive coefficients and by $-v$ the sum of the terms having negative coefficients so that (13) assumes the form $u = -v$ where u and v are both positive. Then $(u, u) = (u, v)$. But $(u, u) > 0$ while $(u, v) \leq 0$ by (12), and we have arrived at a contradiction.

A positive vector belonging to Γ will be said to be primitive if it cannot be expressed as the sum of two positive vectors belonging to Γ . Denote by $B = \{\beta_1, \dots, \beta_n\}$ the collection of all primitive

[†] Clearly a) needs to be required for all scalars r and not just for integers, and it is in this form that the definition will be used in the sequel. It is easily seen that Theorem 105 also implies this stronger condition. Trans.

vectors belonging to Γ . We shall show that B satisfies the conditions of the theorem. From what has just been proved it will then follow that B is linearly independent.

Proof of 1). Suppose on the contrary that $(\beta_i, \beta_j) > 0$. Then $\beta_i - \beta_j \in \Gamma$ by condition b) of B), and of the two vectors $\beta_i - \beta_j$ and $\beta_j - \beta_i$, both of which belong to Γ , one must be positive and the other negative. Suppose, for the sake of definiteness, $\beta_i - \beta_j = \gamma > 0$. Then $\beta_i = \beta_j + \gamma$, which is impossible since β_i was assumed to be primitive.

Proof of 2). First let λ be a positive vector belonging to Γ . If λ is primitive we have $\lambda = \beta_i$ for some $i = 1, \dots, n$ and 2) holds. On the other hand, if λ is not primitive then $\lambda = \alpha + \beta$ where α and β are both positive vectors belonging to Γ . If α and β are primitive then 2) holds; if not then α or β or both may, in turn, be written as a sum of positive vectors belonging to Γ . Continuing this process as long as possible, we arrive at an expression for λ of the form (11) with $\varepsilon = +1$. Finally, if λ is a negative then $-\lambda$ is positive and we obtain an expression for λ of the form (11) with $\varepsilon = -1$.

Thus an arbitrary σ -system Γ contains a linearly independent subsystem B satisfying conditions 1) and 2), and the proof of the first part of the theorem is complete.

We turn now to the second part of the theorem. Let Γ be a σ system and let $B = \{\beta_1, \dots, \beta_n\}$ be an arbitrary linearly independent subsystem of Γ satisfying 1) and 2). We must show that it is possible to recover Γ from the metric structure of B . Let S denote the linear span of B . Then $\Gamma \subset S$ by 2). Moreover, B is a basis for S and may be used to define an ordering as in Section 63, F). We suppose S to be so ordered. Then a vector expressed as in (11) is positive for $\varepsilon = +1$ and negative for $\varepsilon = -1$, and since Γ is determined by its positive vectors we may, and shall, confine attention to those linear forms (11) with $\varepsilon = +1$. For such a form we define the height to be the sum $a^1 + \dots + a^n$ of its coefficients. The only form with height zero yields the zero vector which does not belong to Γ . On the other hand, the forms of height one yield the vectors β_1, \dots, β_n , all of which belong to Γ . Let Γ_a , $a = 1, 2, \dots$, denote the set of positive vectors belonging to Γ and given by expressions (11) with height a . Then, as just noted, $\Gamma_1 (= B)$ is certainly determined by B . The proof will be completed by induction.

Suppose Γ_a , $1 \leq a \leq b$, has already been constructed, and let $\gamma \in \Gamma_{b+1}$. Then $\{\beta_1, \dots, \beta_n, \gamma\}$ is a linearly dependent set of positive vectors (see 2)) and, according to the criterion established above (see (12)), there exists a vector $\beta_i \in B$ such that (γ, β_i)

> 0 . But then $\alpha = \gamma - \beta_1 \in \Gamma$ by condition b) of B) and comparing the expressions (11) for α and γ , we find $\alpha \in \Gamma_b$. Thus every vector $\gamma \in \Gamma_{b+1}$ may be written in the form $\gamma = \alpha + \beta$, $\alpha \in \Gamma_b$, $\beta \in B$, and we need only give a criterion determining whether or not the sum $\gamma = \alpha + \beta$ belongs to Γ when $\alpha \in \Gamma_b$, $\beta \in B$.

If $\alpha = \beta$ then $\gamma \notin \Gamma$ by condition a) of B). Hence we suppose $\alpha \neq \beta$. Consider vectors of the form $\alpha - j\beta$, $j = 1, 2, \dots$. If $\alpha - j\beta$ belongs to Γ then it must belong to the already constructed set Γ_{b-j} . Thus the number 1 (see B)) can be determined for the pair β, α . But then, from 1 and the ratio $p = \frac{2(\beta, \alpha)}{(\beta, \beta)}$, we can also determine $m = 1 - p$; and in terms of m the desired criterion may readily be stated. Indeed, if $m > 0$ then $\gamma \in \Gamma_{b+1}$, while if $m = 0$ then $\gamma \notin \Gamma_{b+1}$. Thus the sets $\Gamma_a, a = 1, 2, \dots$ are reconstructed recursively from the metric structure of B. Finally, $\Gamma_+ = \Gamma_1 \cup \Gamma_2 \cup \dots$ is the set of positive elements of Γ , so that $\Gamma = \Gamma_+ \cup (-\Gamma_+)$.

C) Let Γ be a σ -system and let B be any linearly independent subsystem of Γ satisfying conditions 1) and 2) of Theorem 113. Then Γ is reducible (see Section 63, H) when and only when B is.

One way is easy enough; if Γ reduces into subsystems Γ' and Γ'' then B reduces into $B \cap \Gamma'$ and $B \cap \Gamma''$. Suppose on the other hand that B reduces into subsystems B' and B'' . Employing the notation introduced in the proof of Theorem 113, write Γ_a' and Γ_a'' for the collections of vectors belonging to Γ_a and lying in the linear span of B' and B'' , respectively. We assume that Γ_a reduces into Γ_a' and Γ_a'' (this is correct for $a = 1$ by hypothesis) and show that Γ_{a+1} also reduces into Γ_{a+1}' and Γ_{a+1}'' . Indeed, let $\gamma \in \Gamma_{a+1}$. Then $\gamma = \alpha + \beta$, $\alpha \in \Gamma_a$, $\beta \in B$. By the inductive hypothesis α belongs to one of the subsystems Γ_a' , Γ_a'' , say $\alpha \in \Gamma_a'$. Suppose $\beta \in B''$. Then $\alpha - \beta \notin \Gamma$, since the expression of this vector in terms of B involves both positive and negative coefficients. But also $p = \frac{2(\beta, \alpha)}{(\beta, \beta)} = 0$ and it follows (see condition b) of B)) that $\gamma = \alpha + \beta \notin \Gamma$, a contradiction. Thus we must have $\beta \in B'$ and consequently $\gamma \in \Gamma_{a+1}'$. Letting $\Gamma_+' = \Gamma_1' \cup \Gamma_2' \cup \dots$, $\Gamma_+'' = \Gamma_1'' \cup \Gamma_2'' \cup \dots$, we see that Γ_+ reduces into Γ_+' and Γ_+'' , and it follows that Γ itself is reducible.

Theorem 113 and proposition C) are the motivation for the following definition.

D) A linearly independent system $B = \{\beta_1, \dots, \beta_n\}$ of vectors in a Euclidean space will be said to be a π -system if it is irreducible, i. e., does not split into orthogonal subsystems, and if, for an

arbitrary pair of distinct vectors α and β belonging to B , the ratio $\frac{2(\alpha, \beta)}{(\alpha, \alpha)}$ is a non-positive integer. The number of vectors in a π -system will be called its rank.

We shall use the following scheme to represent a π -system $B = \{\beta_1, \dots, \beta_n\}$ graphically as a connected linear complex L : The vertices $(\beta_1), \dots, (\beta_n)$ of the complex L will be in one-to-one correspondence with the vectors in B , and two distinct vertices (β_i) and (β_j) will be joined in L by r edges (or, as we shall say, by an r -fold edge) if the cosine of the angle made by β_i and β_j is $-\frac{1}{2} \sqrt{r}$, $r = 0, 1, 2, 3$, (see(1)). That the complex L thus defined is connected follows from the fact that B is irreducible. In this schematic representation of π -system only the angles between the various vectors are taken into account and not their lengths, so that the representing complex L yields only an incomplete description of its π -system

The following proposition is readily verified (see Theorems 111 and 112).

E) The root systems

$$\Sigma(A_n), n \geq 1; \quad \Sigma(B_n), n \geq 2; \quad (14)$$

$$\Sigma(C_n), n \geq 3; \quad \Sigma(D_n), n \geq 4 \quad (15)$$

(See Section 65, (32) - (35)) are irreducible σ -systems. Respective π -subsystems satisfying conditions 1) and 2) of Theorem 113 are given by

$$\pi(A_n) = \{e_2 - e_1, e_3 - e_2, \dots, e_{n+1} - e_n\}, \quad (16)$$

$$\pi(B_n) = \{e_1, e_2 - e_1, e_3 - e_2, \dots, e_n - e_{n-1}\}, \quad (17)$$

$$\pi(C_n) = \{2e_1, e_2 - e_1, e_3 - e_2, \dots, e_n - e_{n-1}\}, \quad (18)$$

$$\pi(D_n) = \{e_1 + e_2, e_2 - e_1, e_3 - e_2, \dots, e_n - e_{n-1}\}. \quad (19)$$

The associated linear complexes are shown in Figure 4.

$$L(A_n) \quad \bullet - \bullet - \bullet - \cdots - \bullet - \bullet \quad (20)$$

$$L(B_n) \quad \bullet - \bullet - \bullet - \cdots - \bullet - \bullet \quad (21)$$

$$L(C_n) \quad \bullet - \bullet - \bullet - \cdots - \bullet - \bullet \quad (22)$$

$$L(D_n) \quad \begin{array}{c} \bullet \\ | \\ \bullet \end{array} - \bullet - \bullet - \cdots - \bullet - \bullet \quad (23)$$

Fig. 4

F) Besides the four infinite series of classical Lie algebras

there exist five exceptional Lie algebras: G_2 , F_4 , E_6 , E_7 , E_8 , a description of which will not be given in this book. The root systems and π -systems

$$\pi(G_2), \pi(F_4), \pi(E_6), \pi(E_7), \pi(E_8) \quad (24)$$

of these algebras will be described below in G). The associated linear complexes are shown in Figure 5.

$$L(G_2) \quad \text{---} \quad (25)$$

$$L(F_4) \quad \text{---} \text{---} \quad (26)$$

$$L(E_6) \quad \text{---} \text{---} \text{---} \quad (27)$$

$$L(E_7) \quad \text{---} \text{---} \text{---} \text{---} \quad (28)$$

$$L(E_8) \quad \text{---} \text{---} \text{---} \text{---} \text{---} \quad (29)$$

Fig. 5

Theorem 114: Every compact simple Lie algebra is isomorphic with one of the algebras

$$A_n, n \geq 1; B_n, n \geq 2; C_n, n \geq 3; D_n, n \geq 4, \quad (30)$$

$$G_2, F_4, E_6, E_7, E_8. \quad (31)$$

Proof: Since a Lie algebra is uniquely determined by its root system (see Theorem 106) and the root system is, in turn, uniquely determined by a π -subsystem satisfying the conditions of Theorem 113, it suffices to show that an arbitrary π -system is similar to one of the systems (16)–(19), (24). We first show that the linear complex L associated with a π -system B must be one of the complexes (20)–(23), (25)–(29).

The complex L determines the angles between the various pairs of vectors in B and therefore determines a configuration, unique up to isometry, consisting of n linearly independent directions in an n -dimensional Euclidean space. We shall show that such a configuration of directions can only exist when L is one of the complexes listed above. The argument rests on the following considerations.

Let L denote an arbitrary connected linear complex, with vertices enumerated in some order, and let r_{ij} ($= r_{ji}$) denote the number of edges in L joining the i -th vertex to the j -th. If L is a complex representing some π -system $B = \{\beta_1, \dots, \beta_n\}$ then r_{ij} ($= 0, 1, 2, 3$) determines the angle φ_{ij} made by β_i and β_j according to the formula $\cos \varphi_{ij} = -\frac{1}{2} \sqrt{r_{ij}}$. Thus $(\gamma_i, \gamma_j) = -\frac{1}{2} \sqrt{r_{ij}}$ where γ_i

denotes the unit vector in the direction of β_1 and it follows that for any system c^1, \dots, c^n of non-negative real numbers, not all of which are zero, we have

$$0 < (\gamma, \gamma) = (c^1)^2 + \dots + (c^n)^2 - \sum_{i < j} c^i c^j \sqrt{r_{ij}} \quad (32)$$

where γ denotes the vector

$$\gamma = c^1 \gamma_1 + \dots + c^n \gamma_n.$$

Thus if it is possible to find a sequence c^1, \dots, c^n of non-negative real numbers, not all zero, such that

$$(c^1)^2 + \dots + (c^n)^2 - \sum_{i < j} c^i c^j \sqrt{r_{ij}} \leq 0, \quad (33)$$

then no system of directions $\gamma_1, \dots, \gamma_n$ corresponds to L , and L does not represent a π -system.

Next, let L' be a subcomplex of L . Suppose for the sake of definiteness that L' contains the first m vertices of L and does not contain the others (reenumerate if necessary), and write r'_{ij} , $i, j = 1, \dots, m$, for the number of edges in L' joining the i -th vertex to the j -th. Then

$$r'_{ij} \leq r_{ij}, \quad i, j = 1, \dots, m,$$

and therefore

$$\begin{aligned} (c^1)^2 + \dots + (c^m)^2 - \sum_{i < j} c^i c^j \sqrt{r_{ij}} &\leq (c^1)^2 + \dots + (c^m)^2 \\ &- \sum_{i < j} c^i c^j \sqrt{r'_{ij}} \end{aligned}$$

for non-negative c^1, \dots, c^m . Thus if there exists a system of non-negative numbers c^1, \dots, c^m , not all zero, such that for L'

$$(c^1)^2 + \dots + (c^m)^2 - \sum_{i < j} c^i c^j \sqrt{r'_{ij}} \leq 0, \quad (34)$$

then, letting $c^{m+1} = \dots = c^n = 0$, we also satisfy (33).

Now for each of the nine following complexes (see Fig. 6) inequality (33) is satisfied for suitable coefficients c^1, \dots, c^n . An appropriate choice is indicated in each diagram according to the following scheme: under each vertex there appears the square $(c^1)^2$ of the coefficient to be assigned to that vertex, while above each edge appears the corresponding product $-c^i c^j \sqrt{r_{ij}}$. Thus none of the complexes (35)–(43) can be contained in a complex L that represents a π -system. Note that in (36), (37), (38) and (40) the number of vertices may be any of the numbers appearing to the right

of the diagram. The fact that the number of vertices may take different values is indicated by broken lines.

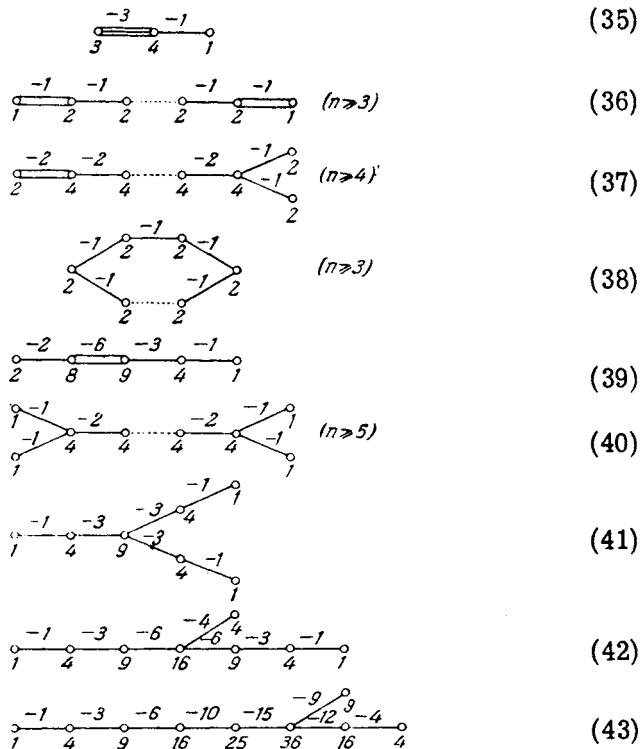


Fig. 6

Suppose now that L is the complex of a π -system B . If L contains a triple edge then it contains no other edge (see (35)) and is therefore of the form $L(G_2)$. If L contains a double edge then it contains only one double edge (see (36)), has no branch point (see (37)), and contains no cycle (see (38)). It follows that if both ends of the double edge are also vertices of single edges then L is of the form $L(F_4)$ (see (39)), while, if single edges adjoin the double edge at only one end, then L is of the form $L(B_n)$.

If L contains only single edges then it contains only one branch point (see (40), $n > 5$), contains no vertex at which more than three edges meet (see (40) $n = 5$), and contains no cycle (see (38)).

In the event that L contains no branch points at all it is of the form $L(A_n)$. If it contains a branch point then at least one of the branches issuing from this point consists of only one edge (see (41)). If two of the branches issuing from the branch point consist of single edges then L is of the form $L(D_n)$. Finally, if there are two branches consisting of more than one edge, issuing from the branch point, then L must coincide with one of the complexes $L(E_6)$, $L(E_7)$ or $L(E_8)$ (see (42), (43)).

It remains only to show that there exists no more than one π -system B yielding each of the complexes (20)–(23), (25)–(29). The existence problem has already been settled in the affirmative for the complexes (20)–(23) (see E); for the complexes (25)–(29) it will be settled in G). In order to prove uniqueness we observe that if the vertices (β_i) and (β_j) are joined in L by r edges, $r > 0$, then the lengths of β_i and β_j satisfy the relation

$$\frac{(\beta_i, \beta_i)}{(\beta_j, \beta_j)} = r^{\pm 1}$$

(see A)). In particular, if $r = 1$ we have $(\beta_i, \beta_i) = (\beta_j, \beta_j)$. Thus if L contains only single edges then all of the vectors β_1, \dots, β_n are of the same length, since L is connected, so that in this case B is determined up to similarity by L .

It remains to consider the four admissible complexes containing multiple edges. In $L(G_2)$ there are only two vertices and these are symmetrically situated so that it is of no consequence which of the two vectors of $\pi(G_2)$ we regard as longer than the other, and the π -system represented by $L(G_2)$ is unique up to similarity. Similarly, $L(F_4)$ contains a double edge, but the ends of the double edge are symmetrically situated and there is but the one π -system $\pi(F_4)$ giving rise to $L(F_4)$. Finally, we consider $L(B_n) = L(C_n)$. Let the vertices of the double edge be (β_1) , (β_2) . If $n = 2$ these vertices are symmetrically situated and it is of no consequence which of the vectors we regard as the longer (recall that $\Sigma(B_2)$ and $\Sigma(C_2)$ are similar). If $n > 2$ then, regarding β_1 as the shorter of the two, we obtain the π -system $\pi(B_n)$, while, regarding β_1 as the longer of the two, we obtain $\pi(C_n)$. Thus the proof of Theorem 114 is complete.

G) Let e_1, e_2, \dots be an orthonormal basis in a Euclidean space and let $e^{(r)}$ denote the sum $e^{(r)} = e_1 + e_2 + \dots + e_r$. Then the root systems of the five exceptional algebras are given, up to similarity, by the formulas:

$$\Sigma(G_2) = \{e_i - e_j; \pm(e^{(3)} - 3e_i); i, j = 1, 2, 3\}, \quad (44)$$

$$\Sigma(F_4) = \{\pm e_i; \pm e_i \pm e_j; \frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4);$$

$$i, j = 1, 2, 3, 4\}, \quad (45)$$

$$\Sigma(E_6) = e_i - e_j; \pm e_7 \sqrt{2}; \pm \left(e_7 \frac{\sqrt{2}}{2} + \frac{1}{2} e^{(6)} - e_i - e_j - e_k\right);$$

$$i, j, k = 1, \dots, 6\}, \quad (46)$$

$$\Sigma(E_7) = \{e_i - e_j; \frac{1}{2} e^{(8)} - e_i - e_j - e_k - e_m\};$$

$$i, j, k, m = 1, \dots, 8\}, \quad (47)$$

$$\Sigma(E_8) = \{\pm e_i \pm e_j; \pm \left(\frac{1}{2} e^{(8)} - e_i\right); \pm \left(\frac{1}{2} e^{(8)} - e_i - e_j - e_k\right)\};$$

$$i, j, k = 1, \dots, 8\}. \quad (48)$$

In each case the literal indices are understood to be pairwise distinct. Respective π -systems are given by the formulas

$$\pi(G_2) = \{e_2 - e_1; e^{(3)} - 3e_2\}, \quad (49)$$

$$\pi(F_4) = \{e_3 - e_2; e_2 - e_1; e_1; \frac{e_4 - e_1 - e_2 - e_3}{2}\}, \quad (50)$$

$$\pi(E_6) = \{e_2 - e_1; e_3 - e_2; e_4 - e_3; e_5 - e_4; e_6 - e_5; \\ (e_7 \frac{\sqrt{2}}{2} + \frac{1}{2} e^{(6)} - e_4 - e_5 - e_6)\}, \quad (51)$$

$$\pi(E_7) = \{e_2 - e_1; e_3 - e_2; e_4 - e_3; e_5 - e_4; e_6 - e_5; e_7 - e_6;$$

$$\frac{1}{2} e^{(8)} - e_4 - e_5 - e_6 - e_7\}, \quad (52)$$

$$\pi(E_8) = \{e_1 + e_2; e_2 - e_1; e_3 - e_2; e_4 - e_3; e_5 - e_4; e_6 - e_5; \\ e_7 - e_6; e_8 - \frac{1}{2} e^{(8)}\}. \quad (53)$$

The dimensions of these algebras are 14, 52, 78, 133, and 248, respectively. No two of the algebras G_2 , F_4 , E_6 , E_7 , E_8 are isomorphic with one another, and none is isomorphic with any of the

classical algebras.

The fact that (44)–(48) are σ -systems and that (49)–(53) are π -subsystems may be verified by direct calculation. Similarly the stated dimensions may be verified by counting the vectors in the given systems since the dimension of each algebra is equal its rank plus the number of vectors in a root system. That no two of the exceptional algebras are isomorphic follows from the fact that they have different ranks.

Now the classical algebras of rank n having largest dimension are B_n and C_n with dimension $2n^2 + n$. For $n = 2, 4, 6, 7, 8$ (the ranks of the exceptional algebras) these dimensions are 10, 36, 78, 105, and 136, respectively. Comparing these numbers with the dimensions of the exceptional algebras, we see that the only possibility not excluded is that E_6 might be isomorphic with one of the algebras B_6 , C_6 . Such is not the case, however, for $\Sigma(E_6)$ consists of vectors of one length only, while both root systems $\Sigma(B_6)$ and $\Sigma(C_6)$ contain vectors of two different lengths.

Thus G) is proved. The only question remaining open is that of the existence of algebras having (44)–(48) for root systems.

Example 109: We sketch here a line of argument leading to the construction of the five exceptional algebras. The carrying out of the construction in detail would involve a formidable amount of computation.

Let Σ' denote an irreducible σ -system (see B)). By applying a similarity transformation to Σ' we may arrange matters so that at least one vector β' belonging to a similar system Σ satisfies (2) Section 63 with $k = 1$. Calculation then shows that every vector $\beta' \in \Sigma$ satisfies (2) Section 63 with $k = 1$. Next the construction employed in the proof of Theorem 106 may be carried out for Σ to determine a system of real coefficients $N_{\alpha\beta}$. Further computation verifies that, for the coefficients $N_{\alpha\beta}$ thus obtained, relations (8), (9) Section 63 are valid. Once this has been ascertained, it is a simple matter, using (18)–(20) Section 63, to define a Lie algebra having root system Σ .

Applying this procedure to each of the σ -systems (44) – (48), one may show the existence of the five exceptional Lie algebras.

Example 110: The definition of a σ -system (see B)) contains a condition, viz., b), which is rather difficult to verify. We here formulate two apparently weaker conditions a') and b') which, taken together, are equivalent with a) and b) of definition B).

In order to give geometric significance to the condition b') formulated below we observe the following fact: If α is a non-zero vector in a Euclidean space S then the mapping

$$x \rightarrow x - \frac{2(\alpha, x)}{(\alpha, \alpha)} \alpha \quad (54)$$

is the reflection of S in the plane $(\alpha, x) = 0$.

We now show that a system Γ of non-zero vectors in a Euclidean space is a σ -system if and only if the following two conditions are satisfied: a') if $\lambda \in \Gamma$ then $2\lambda \in \Gamma$. b') If $\lambda, \mu \in \Gamma$ then the ratio $\frac{2(\lambda, \mu)}{(\lambda, \lambda)}$ is an integer and

$$\mu^{-2} \frac{(\lambda, \mu)}{(\lambda, \lambda)} \lambda \in \Gamma \quad (55)$$

so that Γ is symmetric with respect to every plane $(\lambda, x) = 0$, $\lambda \in \Gamma$ (see (54)).

Since a') and b') are obviously satisfied by any σ -system, it suffices to show that if Γ satisfies a') and b') then it also satisfies a) and b) of definition B). For $\lambda = \mu = \alpha$ condition b') yields:

$$\text{if } \alpha \in \Gamma \text{ then } -\alpha \in \Gamma. \quad (56)$$

Thus in order to verify a) it suffices to show that if $\alpha \in \Gamma$, $r \alpha \in \Gamma$ then $|r| = 1$. We may suppose that $|r| \geq 1$. But then, since the ratio $\frac{2(\alpha, r\alpha)}{(r\alpha, r\alpha)} = \frac{2}{r}$ is an integer by b'), we have $|r| = 1, 2$, and since $|r| \alpha \in \Gamma$ by (56), the case $|r| = 2$ is excluded by a'). Thus $r = \pm 1$.

Now let α and β be any two non-collinear vectors belonging to Γ and let

$$p = \frac{2(\alpha, \beta)}{(\alpha, \alpha)} ; \quad q = \frac{2(\alpha, \beta)}{(\beta, \beta)}. \quad (57)$$

We shall show that

$$\text{if } p > 0 \text{ then } \beta - j\alpha \in \Gamma, \quad j = 1, \dots, p. \quad (58)$$

Observe that, replacing α by $-\alpha$ in (58), we obtain also

$$\text{if } p < 0 \text{ then } \beta + j\alpha \in \Gamma, \quad j = 1, \dots, |p|. \quad (59)$$

According to b') we have

$$\beta - p\alpha \in \Gamma. \quad (60)$$

Thus if $p = 1$ there is nothing to prove. On the other hand, if $p > 1$ there exist but two possible cases:

$$p = 2, \quad q = 1; \quad p = 3, \quad q = 1 \quad (61)$$

(see A)) so that when $p \geq 2$ we have $q = 1$ and consequently, by (55) with $\lambda = \beta$, $\mu = \alpha$,

$$\alpha - \beta \in \Gamma. \quad (62)$$

But then by (56)

$$\beta - \alpha \in \Gamma. \quad (63)$$

Thus if $p = 2$ then (58) follows from (63) and (60). Finally, if $p = 3$ then, by (55) with $\mu = \beta - \alpha$, $\lambda = \alpha$, we have

$$\beta - 2\alpha \in \Gamma. \quad (64)$$

Thus (58) holds in all cases.

We may now verify b). Since

$$\frac{2(\alpha, \beta - j\alpha)}{(\alpha, \alpha)} = p - 2j, \quad (65)$$

and since $\beta - l\alpha \in \Gamma$ while $\beta - (l+1)\alpha \notin \Gamma$, it follows from (58) that

$$p - 2l \leq 0, \quad (66)$$

whence by (59) we have

$$\beta - l\alpha + j\alpha \in \Gamma, \quad j = 0, \dots, 2l - p,$$

and consequently

$$m \geq l - p. \quad (67)$$

Analogously, since $\beta + m\alpha \in \Gamma$ while $\beta + (m+1)\alpha \notin \Gamma$ it follows from (59) that

$$p + 2m \geq 0.$$

whence by (58) we have

$$\beta + m\alpha - j\alpha \in \Gamma, \quad j = 0, \dots, p + 2m$$

and consequently

$$l \geq m + p. \quad (68)$$

Finally from (67) and (68) we obtain $p = l - m$. Thus b) is verified and the proof is complete.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

REFERENCES

1. Ado, I., On the representation of finite continuous groups by means of linear substitutions (Russian), Izv. Fiz. Mat. Obs. Kazan, 7 (1934/5) 3-43.
2. Aleksandrov (Alexandroff), P. S., On the concept of space in topology (Russian), Uspehi Mat. Nauk, 2, 1 (17) (1947), 5-57.
3. Alexandroff, P. S. and H. Hopf, Topologie, Bd. I, Berlin, 1935.
4. Arens, R. F., A topology for spaces of transformations, Ann. Math., 47(1946), 480-495.
5. Birkhoff, G., Lie groups simply isomorphic with no linear group, Bull. Amer. Math. Soc., 42(1936), 883-888.
6. Bochner, S. and J. von Neumann, Almost periodic functions in groups, II, Trans. Amer. Math. Soc., 37 (1935), 21-50.
7. Bourbaki, N., Topologie générale, Chap. I-II, Paris, 1940.
8. Cartan, E., Sur la structure des groupes de transformations finis et continus, Thèse, Paris, 1894.
9. _____, Groupes simples clos et ouverts et géometrie riemannienne, J. Math. Pures et Appl., 8(1929), 1-33.
10. _____, La théorie des groupes finis et continus et l'Analysis Situs, Mém. Sci. Math., Fasc. XLII, Paris, 1930.
11. van Dantzig, D., Zur topologischen Algebra I, Math. Ann., 107 (1932), 587-626.
12. _____, Zur topologischen Algebra II, Comp. Math., 2 (1935), 201-223.
13. Dynkin, E. B., Structure of semi-simple Lie algebras (Russian), Uspehi Mat. Nauk, 2(1947), 59-127.
14. Gantmacher, F., On the classification of real simple Lie groups, Mat. Sbornik, 5(47), No. 2 (1939), 217-250.

15. Gleason, A. M., Groups without small subgroups, *Ann. Math.*, 56(1952), 193-212.
16. Haar, A., Der Massbegriff in der Theorie der kontinuierlichen Gruppen, *Ann. Math.*, 34(1933), 147-169.
17. Hall, M., The theory of groups, New York, 1959.
18. Hansdorff, F., Set theory, New York, 1957.
19. Jacobson, N., Totally disconnected locally compact rings, *Amer. J. Math.*, 58(1936), 433-449.
20. van Kampen, E., Locally compact abelian groups, *Proc. Nat. Acad. Sci., U.S.A.*, 20, No. 7(1934), 434-436.
21. _____, Locally bicompact abelian groups and their character groups, *Ann. Math.*, 36(1935), 448-463.
22. _____, Note on a theorem of Pontrjagin, *Amer. J. Math.*, 58(1936), 177-180.
23. Kaplansky, I., Topological methods in valuation theory, *Duke J. Math.*, 14(1947), 527-541.
24. Kelley, J. L., General topology, New York, 1955.
25. Killing, W., Die Zusammensetzung der stetigen endlichen Transformationsgruppen. I, *Math. Ann.*, 31(1888), 252-290; II, *ibid.*, 33(1889), 1-48; III, *ibid.*, 34(1889), 57-122; IV, *ibid.*, 36(1890), 161-189.
26. Kolmogoroff (Kolmogorov) A., Zur Begründung der projektiven Geometrie, *Ann. Math.*, 33(1932), 175-176.
27. Kowalski, H. J., Zur topologischen Kennzeichnung von Körpern, *Math. Nachr.* 9(1953), 261-320.
28. Kuroš, A. G., The theory of groups, New York, 1955.
29. Levi, E., Sulla struttura dei gruppi finiti e continui, *Atti. Acad. Torino*, 40 (1905), 3-17.
30. Lie, S. and F. Engel, Theorie der Transformations-gruppen, 1, 2, 3, Leipzig, 1883-1893.
31. Malcev (Mal'cev), A. I., Sur les groupes topologiques locaux et complets, *Dokl. Adad. Nauk SSSR*, 32, No. 9(1941), 606-608.
32. _____, On the simple connectedness of invariant subgroups of Lie groups, *Dokl. Akad. Nauk SSSR*, 34, No. 1 (1942), 10-13.
33. Markoff (Markov), A. A., Über endlich-dimensionale Vektorräume, *Ann. Math.*, 36(1935), 464-506.
34. _____, On free topological groups (Russian), *Izv. Akad. Nauk SSSR, Ser. Mat.*, 9, No. 1(1945), 3-64.
35. Montgomery, D. and L. Zippin, Topological transformation groups. I, *Ann. Math.*, 41(1940), 778-791.
36. _____, Small subgroups of finite dimensional groups, *Ann. Math.*, 56(1952), 213-247.
37. von Neumann, J., Die Einführung analytischer Parameter

- in topologischen Gruppen, Ann. Math., 34(1933), 170-190.
38. _____, Zum Haarschen Mass in topologischen Gruppen, Comp. Math., 7(1934), 106-114.
39. _____, Almost periodic functions in a group. I, Trans. Amer. Math. Soc., 36(1934), 445-492.
40. Otobe, Y., On locally compact fields, Jap. J. Math., 19 (1945), 189-202.
41. Peter, F., and H. Weyl. Die Vollständigkeit der primitiven Darstellungen einer geschlossenen kontinuierlichen Gruppe, Math. Ann., 97(1927), 737-755.
42. Pontryagin, L., Über stetige algebraische Körper, Ann. Math., 33(1932), 163-174.
43. _____, Sur les groupes topologiques compacts et le cinquième problème de M Hilbert, Comptes Rendus, Paris, 198(1934), 238-240.
44. _____, Sur les groupes abéliens continus, Comptes Rendus, Paris, 198(1934), 328-330.
45. _____, The theory of topological commutative groups, Ann. Math., 35(1934), 361-388.
46. _____, Linear representations of compact topological groups, Mat. Sbornik, N. S. 1(43), No. 3(1936), 267-271.
47. _____, Foundations of combinatorial topology, Rochester, 1952.
48. Schreier, O., Abstrakte kontinuierliche Gruppen, Hamburg. Abh. Math. Sem., 4(1925), 15-32.
49. _____, Die Verwandtschaft stetiger Gruppen im grossen, Hamburg, Abh. Math. Sem., 5(1926), 233-244.
50. Shafarevich, I., On the normalizability of topological fields, Dokl. Akad. Nauk SSSR, 40(1943), 133-135.
51. Steenrod, N., The topology of fibre bundles, Princeton, 1951.
52. Tychonoff (Tihonov), A. N., Über einen Metrisationssatz von P. Urysohn, Math. Ann., 95(1925), 139-142.
53. de la Vallée Poussin, Ch. J., Cour d'analyse infinitesimale, Louvain, 1903-06; American ed., New York, 1946.
54. van der Waerden, B., Modern algebra, New York, 1949.
55. _____, Die klassification der einfachen Lieschen Gruppen, Math. Zeit., 37(1933), 446-462.
56. Weil, A., l'Intégration dans les groupes topologiques et ses applications, Paris, 1940.
57. Weyl, H., Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen, I, Math. Zeit., 23(1925), 271-309; II, III, ibid., 24(1925), 328-395.
58. Whitehead, T. H. C., On the decomposition of an infinitesimal group, Proc. Cambridge Phil. Soc., 32(1936), 229-237.

DISTRIBUTION OF THE LITERATURE BY CHAPTERS

Notations: 18.

Chap 1: 17, 28, 54	Chap. 6: 20, 21, 28, 33, 44, 45, 56
Chap. 2: 2, 3, 7, 24, 47, 52	Chap. 7: 15, 36, 37, 43, 44
Chap. 3: 4, 31, 33, 34	Chap. 8: 22, 35, 43
Chap. 4: 11, 12, 19, 23, 26, 27, 40, 42, 50	Chap. 9: 48, 49, 51, 57
Chap. 5: 5, 6, 16, 38, 39, 41, 46, 56	Chap. 10: 1, 10, 29, 30, 32, 53, 58 Chap. 11: 8, 9, 13, 14, 25, 55, 57

INDEX

- Abelian group (see also Commutative group), 2, 17, 27ff., 235ff., 300, 361
additive notation in, 2, 27, 38, 43
coordinates in, 36
finitely generated, 27ff.
free, 28, 361
linear independence in, 27
rank of, 34ff., 259
system of generators for, 27ff., 415
torsion-free, 258ff.
- Abscissa, 65
- Adequate system of linear representations, 185
- Addition, definition of, 46
- Additive group:
of a ring, 39, 41
of a vector space, 43
- Additive notation, 2, 27, 38, 43
- Additivity of rank, 38
- Adherent point, 52, 79
- Adjoint algebra of a Lie algebra, 394-5, 422, 453ff., 460, 476
group, of a Lie algebra, 445ff
of a Lie group, 389, 395-6, 431, 445ff.
homomorphism, 242, 264, 275
- Admissible topological group, 369
topology, 144
- Admission:
of continuous closure, 158, 164
of division, 260
- Aleksandrov (Alexandroff), P. S., 70
- Algebra, adjoint (see Adjoint algebra)
of derivations, 392ff., 496
exceptional, 447, 506, 512, 515
of inner derivations (see Adjoint algebra)
Lie (see Lie algebra)
of matrices of order n , 397
- Algebraic group, 96, 432
ring, 154
- Algebraically closed field, 218
- Almost periodic functions, 233
- Analytic coordinate space, 311
— — — system, 284, 413, 429
— — — transformation, 286, 429
covering, 319ff.
function, 314, 413, 428ff.
homeomorphism, 313ff., 321
Lie group, 285, 308, 313
manifold, 310, 312, 478
mapping, 313, 478
structure, 312, 314, 321
- Analyticity, 281ff.
of a homeomorphism, 313
of a mapping, 313
type, 311, 322
of an open covering, 312
- Angle of rotation, 18
- Annihilator, 235, 242ff.
- Approximation of irrational numbers, 257
- Arc, differentiable, 286, 382, 482ff.
- Arcwise connected space, 346, 348ff.
- Associativity, 1, 38, 47, 49, 349, 380, 406, 433
- Automorphism:
of a group, 10
inner (see Inner automorphism)
involutory, 428, 430
irregular, 478, 480, 485ff
of a Lie algebra, 386, 389, 428, 446ff., 476ff
linear (see Linear automorphism)
local, 300
non-identical, 414
regular (see Regular automorphism)
of a topological group, 112, 152
group, 10;
of a Lie algebra, 389, 393, 448, 453, 476
- Auxiliary functions, 402ff., 417, 441ff.
- Axiomatic definition of a projective geometry, 46

- Axioms of a group, 1
 of incidence, 44
 of projective geometry, 44
 of separation, 65ff.
- Axis of abscissas, 65
- Base, 54
 equivalent, 57, 65
 of induced topology, 64
 at a point, 55, 172
 of spheres, 59
- Basis, orthogonal, 495, 498
 orthonormal, 202, 461, 489ff
 of a vector space, 43, 460
- Bessel's inequality, 202
- Bilinear form, 457, 493-4
 Hermitian, 219
 invariant, 451
 skew-symmetric, 489
- Binomial series, 83
- Block matrix, 492, 498
- Both ways continuous mapping, 61, 65, 82
- Bracket product, 382-3, 390, 426ff., 439, 448
- Bundle of paths, 357, 360
- Bunjakovskii's inequality, 203
- Canonical coordinate system:
 of the first kind, 290, 295, 304ff., 331, 396, 402, 407-8, 413, 416ff., 443, 478
 of the second kind, 296, 300ff., 402 form:
 of an automorphism of a Lie algebra, 477
 of an integral matrix, 29
 of a quadratic form, 430
- Cantor set, 128
- Cardinal number, 7, 54, 71-2, 81, 85, 356
 infinite, 71, 81
- Cardinality:
 of a set (see Cardinal number)
 of a character group, 254
- Cartan, E., 377, 423, 446-8
- Cartesian coordinate system, 18, 58, 117, 127, 143, 159, 321
 global, 434
- Cauchy Criterion, 188
- Cauchy's inequality, 202
- Center:
 of the classical compact Lie groups, 504
 of a division ring, 42
 of the full linear group, 18
- of a group, 16
 of a Lie algebra, 385, 396, 418, 431, 445ff., 453, 487
 of a Lie group, 430, 435, 488, 506
 of perspectivity, 45
 of a topological group, 130, 488
 trivial, 487
- Central element:
 of a group, 16
 of a Lie group, 453
 ideal:
 of a Lie algebra, 451
 maximal, 385
 normal subgroup, 16, 130, 338, 360, 370, 385
 connected, 488
 subfield, 42
- Character:
 of a group, 237 ff
 of a linear representation, 221ff.
 group, 235 ff.
- Characteristic, 41, 171
 equation, 460
 polynomial, 457, 461
- Class:
 of conjugate subgroups, 354
 of a differentiable coordinate space, 311
 of a differentiable manifold, 312
 of a differentiable open covering, 312
 of a differentiable structure, 312
 of a differentiability type, 311
- Classical compact Lie groups, 370, 489
 centers of, 504
 fundamental groups of, 504
 Lie algebras, 447, 502ff., 511, 517
- Classification:
 of compact Lie algebras, 445, 448
 of compact Lie groups, 423, 445, 447
 of compact semi-simple Lie algebras, 423, 447, 476
 of compact simple Lie algebras, 445, 447-8
 of complex Lie algebras, 423, 446, 449
 of Lie algebras, 422, 471
 of Lie groups, 415, 423
 of real Lie algebras, 423, 446
 of root systems, 476, 506
 of σ -systems, 506
 of semi-simple Lie algebras, 422-3, 446-7, 476
 of simple Lie algebras, 423, 445, 447ff., 506

- of solvable Lie algebras, 422
- Closed manifold, 311, 482
 - path, 346, 485-6
 - set, 52, 63, 86
 - subgroup, 477
- Closed-open set, 87
- Closure, 51-2
 - in Euclidean space, 59
- Coefficient of similarity, 467-8
- Collinear vectors, 467
- Commutative group (see also Abelian group) 300, 379, 415
 - compact connected finite dimensional, 488
 - Lie algebra, 382, 414, 422, 448, 454, 460ff
 - linear, 458-9, 462
 - ring, 39
 - subalgebra, 456, 495ff.
- Commutativity, 1, 47, 379
- Commutator:
 - of group elements, 16
 - in a Lie algebra, 382ff., 414, 427, 455
 - in a Lie group, 379ff
 - of matrices, 497
 - skew-symmetry of, 464
 - of vectors, 466
 - of vector fields, 439, 441
- Commutator subgroup, 16
 - of the full linear group, 18
- Commuting elements, 16, 486
- Compact element of a locally compact group, 272
 - Hausdorff space, 73, 89
 - of dimension zero, 92
 - Lie algebra, 423, 445ff., 487, 495
 - complexification of, 449
 - semi-simple (see Compact semi-simple Lie algebra)
 - simple, 445, 447-8, 466, 506, 512
 - simple non-commutative, 447-8
 - group, 423, 445ff., 453, 455, 476, 489, 491, 494
 - classical, 489
 - semi-simple, 423
 - simply connected, 488
 - metric space, 119
 - real form, 446
 - semi-simple Lie algebra, 445ff., 455ff., 463ff., 467ff., 476., 495
 - rank of, 456, 460, 467
 - real, 447
 - root vector of, 462
 - root space of, 462-3
- root system of, 462-3
 - subalgebra, 487
 - set, 70, 481-2
 - space, 70, 75, 79, 81, 85
 - product of, 78
 - topological group, 82
 - finite dimensional connected commutative, 488
 - transformation group, 339ff.
- Compactly generated group, 116, 264ff.
- Compactness, 70, 75, 79, 81, 85
 - countable, 74, 285
 - local, 70
 - of a space of cosets, 109
 - of a subgroup, 109
 - of a subset of a topological group, 145
- Compact-open set, 88
 - subgroup, 131
- Complete limit point, 70
 - orthogonal system of functions, 251
 - regularity, 66, 81, 105
 - system of neighborhoods, 54, 77
 - of the identity in a topological group, 99ff., 134, 431-2
 - of a point, 55
 - of Urysohn functions, 84, 213
- Completely reducible system of matrices, 219
 - regular space, 66, 81
- Completeness, 201
 - uniform, 225
- Complex, 361ff
 - connected linear, 511-2
 - conjugate:
 - element, 491-2, 494
 - vector, 426, 428
 - coordinate system, 428
 - Lie algebra, 382, 422-3, 426ff., 447, 474
 - semi-simple, 423, 446
 - simple, 449
 - group, 428ff
 - global, 429
 - local, 428
 - linear span, 501
 - matrix, 491
 - numbers, 153
 - semi-simple Lie algebra, 423, 446
 - simple Lie algebra, 449
 - vector space, 426ff., 490-1, 495
- Complexification, 490ff., 494
 - of a real Lie algebra, 422-3, 427ff., 462, 495

- of a real compact Lie algebra, 449
- of a real Lie group, 429ff
- of a real simple Lie group, 430
- of a real vector space, 426, 457,
 - 461
- Component of the identity, 129, 339ff.,
 - 430, 453-5, 476, 487
 - in a compact group, 258
 - in a locally compact abelian group, 277
 - , of a point, 86, 93
 - of a topological space, 87
- Conic section, 430
- Conjugate group element, 486-7
 - quaternion, 159
 - subgroup, 354
- Connected central subgroup, 488
 - global group, 455
 - (global) Lie group, 435, 446, 448, 487-8, 505
 - commutative, 415
 - compact finite dimensional, 488
 - locally compact, 116
 - simply connected, 504
 - with non-trivial center, 487
 - linear complex, 511
 - neighborhood of zero, 261
 - set, 86
 - topological group, 129ff., 367, 433
 - — — space, 86ff.
- Continuity:
 - at a point, 62
 - of a complex valued function, 199
 - of a mapping, 61
- Continuous center of a Lie group, 487
 - closure, 158, 176
 - division ring, 153, 158
 - function, 65ff
 - on a topological group, 186
 - of two variables, 82ff.
 - kernel, 82
 - mapping, 60
 - real valued function, 65
 - transformation group, 319, 436ff.
- Continuously differentiable function, 437
- Convergent sequence, 58, 155
 - series, of compact groups, 326
 - of polynomials, 83
- Coordinate method, 310
 - neighborhood, 481
 - space, analytic, 311
 - differentiable, 311
 - system, 310, 383
- analytic, 413, 429
- canonical (see Canonical coordinate system)
- Cartesian, 117, 321
 - complex, 428
 - in a coordinate space, 311
 - differentiable, 387
 - Euclidean, 413
 - local, 312
 - in a local group, 283
 - in a vector space, 452
 - — transformation, analytic, 286, 429
 - differentiable, 285-6, 296
- Coordinates:
 - in an abelian group of finite rank, 36
 - Cartesian, 18, 58
 - local, 279, 310, 483
 - in a vector space, 43
- Coset, 7
 - in a local group, 140, 306
 - space of, 102ff.
- Countable base, 54
 - for D, 65
 - compactness, 74
 - covering, 69, 74
 - everywhere dense set, 75
 - number of coordinates, 85
 - set, 85
 - weight, 54
- Countably compact:
 - Lie group, 285
 - metric space, 75
 - separable space, 75
 - topological group, 127
 - space, 85, 172
 - infinite cardinal number, 85
- Covering:
 - analytic, 319, 321
 - countable, 74
 - finite, 70ff., 88ff
 - proper, 352
 - universal (see Universal covering)
 - arc, 483-4
 - deformation, 352, 372
 - group, 364ff
 - universal, 430, 435, 487
 - homotopy, 352, 372
 - theorem, 373
 - mapping, 352, 486
 - path, 352ff., 485-6
 - space, 345-6, 351ff.
- Cross section, 372
- Cube:
 - in Euclidean space, 481
 - n-dimensional, 259
- Cyclic group, 6, 26, 32ff., 246, 364, 504
 - finite, 33
 - free, 35, 38

- permutation, 4
- subgroup, 27, 32ff., 487
 - generated by an element, 6, 265
- Defining system of neighborhoods, 57
- Definition of a topology:
 - by means of a metric, 59
 - by means of neighborhoods, 57
- Deformation, 347, 486
 - covering, 352, 372
 - small, 368
- Degenerate kernel, 82
- Degree:
 - of a linear representation, 220
 - of a polynomial, 461
- Dependent functions, 318
- Derivation, 392ff
 - algebra of, 392ff., 496
 - inner, 445, 460
- Desargue's Theorem, 45
- Determinant, 16, 397, 400, 430, 496
 - functional, 286, 298ff
 - of a linear transformation, 430, 490
- Diagonal block matrix, 375, 493
 - form, 477
 - matrix, 374, 460, 499
 - pure imaginary, 497
- Difference of sets, xi
- Differentiable arc (see Arc)
 - coordinate space, 311
 - — — system, 284, 378
 - — — transformation, 285-6, 296
 - function, 281ff., 293ff., 300
 - homeomorphism, 313
 - Lie group, 285
 - of class m, 312
 - mapping, 313
 - one-parameter subgroup, 288, 293
 - open covering, 312
 - structure, 312
- Differentiability, 281ff
 - of a function of two variables, 313
 - of a homeomorphism, 313
 - of a mapping, 313
 - type:
 - of class m, 311
 - of an open covering, 312
- Differential equation, 391-3, 398, 402ff., 410ff., 442-3
- Dimension:
 - of a compact abelian group, 259
 - of a compact group, 331
 - of a compact simple Lie algebra, 516
- of a Lie algebra, 458, 485, 487, 492, 502
 - of a Lie group, 397, 415, 478, 480, 492
- of a local group, 142
 - of a local Lie group, 284, 298
 - of a manifold, 480
 - of a topological space, 88ff
 - of a vector space, 43, 415, 440, 459ff.
- Direct factorization (see also Resolution and Direct resolution):
 - of a group, 19, 24, 415
 - of a Lie group, 388, 488
 - of a local group, 141, 388, 430, 488
 - orthogonal, 461
 - of a topological group, 121, 124
 - product, 350
 - of compact groups, 328
 - full, 328
 - of groups, 18ff., 22, 76
 - of Lie groups, 487
 - of local groups, 141
 - of local Lie groups, 388
 - of manifolds, 480
 - of topological groups, 120, 123ff., 488
 - resolution, of Euclidean space, 461
 - of a Lie algebra, 388, 423, 426, 448, 451ff., 474, 487, 502
 - of a local group, 141
 - of a vector group, 458-9, 462, 468, 475
 - sum, of abelian groups, 27
 - dual, 255
 - full, 263
 - of Lie algebras, 388, 475
 - of vector spaces, 496
- Direction transformation, 490, 492
 - vector:
 - of an arc, 479
 - of a one-parameter subgroup, 288, 418, 442, 449, 476ff.
- Disconnected topological space, 86
- Discontinuity, 65
- Discontinuous mapping, 65
- Discrete group, 98, 235, 251ff.
 - subgroup, 360, 370, 415, 488
 - central normal, 485, 487
 - normal, 134ff., 345
 - space, 53
- Distance, 59
- Distinguished pair of neighborhoods, 81, 84

- Distributivity, 38, 49
 Division ring, 39
 continuous, 153, 158
 of quaternions, 158f., 169
 topological, 153ff.
 Divisor, of a group, 6
 of zero, 40
 Domain of existence of a one-parameter subgroup, 142
 Double integral, 199ff.
 Dual direct sums, 255
 Duality, 235ff
 of annihilators, 252, 274
 of closed and open sets, 52
 Duality theory, for compact and discrete groups, 251ff
 for locally compact abelian groups, 273ff.
 Dyadic fraction, 67
 Dynkin, E. B., 504, 506
- ϵ -net, 75
 ϵ -tessellation, 481
 Edge, 511ff
 multiple, 511, 515
 Effective transformation group, 13, 144
 Eigenform:
 of a linear Lie algebra, 458-9, 462, 496, 502
 pure imaginary, 459
 Eigenfunction of an integral equation, 204
 Eigenmatrix, 497, 499ff.
 Eigenspace:
 of an eigenform, 458-9, 462, 496
 of an eigenvalue, 204
 of a linear transformation, 461
 Eigenvalue, 422
 of an integral equation, 204
 of a linear transformation, 456ff., 461, 477, 487, 498
 multiplicity of 456, 460-1
 pure imaginary, 457
 of a skew-symmetric transformation, 460
 Eigenvector, 422
 associated with a root vector, 467, 475
 of a linear transformation, 456-7, 459, 467, 499-500
 Elementary divisor, 447
 group, 246, 250
 operations on a matrix, 29
 Empty word, 362
 End point, 346ff., 482
 Equicontinuity (see Uniform equicontinuity)
- Equivalence:
 of bases, 57
 class, 6, 40, 347ff.
 of coverings, 356
 of covering mappings, 352
 of fundamental sequences, 156
 of linear representations, 220
 of local homomorphisms, 141
 of local isomorphisms, 138
 of local subgroups, 139
 of paths, 357
 relation, 6, 40, 118
 Equivalent bases, 65
 linear representations, 220
 paths, 346ff.
 Euclidean space, 58, 60, 89, 143, 151, 159, 201, 259, 283, 310, 321, 344, 351, 370, 405, 412-3, 434ff., 445-6, 455ff., 460, 466ff., 475, 481, 489, 495, 506ff
 fundamental group of, 351
 topology of, 59
 Everywhere dense set, 53, 86, 484, 488
 countable, 75
 Exceptional Lie algebra, 447, 506, 512, 515-7
 Exponential notation in a group, 3, 5
 Extension:
 of a bilinear form, 457
 of a character, 253, 275
 of a linear form or transformation, 457
 of a word, 363
 Factor algebra, 385, 386, 387
 Factor group, 8
 of a local group, 140
 of a topological group, 104
 Field, 39
 of characteristic zero, 426
 of p-adic numbers, 153, 158, 163ff., 171, 179
 of power series, 158, 163
 of rational functions, 42
 topological, 154
 Fifth problem of Hilbert, 285, 323
 Finite central normal subgroup, 487-8
 completely regular space, 81
 covering, 70ff., 74, 88ff
 of a compact Hausdorff space, 89
 cyclic group, 33
 dimensional compact connected commutative group, 488
 — — — group, 488
 — — — vector space, 43
 ϵ -net, 75
 group, 1, 7, 32, 485, 487-8

- intersection property, 70, 79, 145-6
- number of direct summands, 451
 - of factors, 76
 - of sets, 478
- order, element of, 3, 27, 36
 - group of, 32
- product of normal subgroups, 22
- rank, 34
- set, 1, 27, 53, 58
- system of generators, 28, 32, 34-5
- weight, 81
- First axiom of countability, 155ff.
 - theorem of Lie, 402, 436-7
- Formal power series, 164
- Fourier coefficients, 203
- Free abelian group, 28, 361
 - cyclic group, 6, 35, 38, 276-7
 - element, 3, 258
 - group, 362ff.
- Frobenius, F., 158, 160
- Full direct product, 22, 328
 - sum, 263
 - group of permutations, 4
 - linear groups, 5, 101, 112, 151, 215, 287, 295, 308, 391-2, 397
 - center of, 18
 - commutator subgroup of, 18
- Function, continuous, 65ff., 186
 - differentiable, 281ff., 293, 296ff
 - of two variables, 82ff
- Urysohn, 84
- Functional determinant, 286, 298, 300, 311, 317
- matrix, 304
- rank of, 483
- Fundamental duality theorem, 251, 273
 - group, 345ff., 349ff., 485-6
 - of the classical compact Lie groups, 504
 - of Euclidean space, 351
 - of the generalized projective plane, 364
 - of a manifold, 506
 - of a product, 350
 - of a sphere, 351, 505
 - of a topological group, 351
 - sequence, 156, 327
 - system of eigenfunctions, 204
- Generalized projective plane, 365
- Generating system, 4, 116
- Geometric invariant, 456
- Global group, 283ff.
 - Lie group, 319, 421, 431ff., 444, 448
- compact, 446
- complex, 429
- connected, 448
 - simply connected, 429
- normal subgroup, 435
- one-dimensional subgroup, 444
- study of Lie groups, 345
- subgroup, 476
 - of a Lie group, 421
- Grabar, L., 118
- Group, abelian (see Abelian group)
 - abstract, 1
 - adjoint (see Adjoint group)
 - algebraic, 432
 - of automorphisms (see Automorphism group)
 - center of, 16, 374-5, 504ff
 - compactly generated, 116, 264ff
 - of continuous transformations (see Transformation group)
 - covering (see Covering group)
 - cyclic, 6, 246, 364
 - elementary, 246, 250
 - factor, 8
 - finite, 1, 6, 488-9
 - finite dimensional (see Finite dimensional group)
 - of fractional linear transformations, 430
 - free, 362ff
 - free abelian, 28, 361
 - full linear (see Full linear group)
 - fundamental (see Fundamental group)
 - infinite, 1
 - of isometric transformations, 151
 - Lie (see Lie group)
 - linear, 489
 - of linear automorphisms, 477, 490, 505
 - local, 136, 428, 450
 - of matrices, 185ff., 397 (see also Unimodular group)
 - of motions, 15, 18, 344, 430
 - orthogonal, 9
 - of orthogonal matrices, 151, 373, 397, 454, 489
 - of permutations, 4
 - of projective transformations, 430
 - quasi-cyclic, 241
 - of quaternions of modulus one, 370ff., 384, 421, 504-5
 - of real numbers, 132, 143
 - of rotations, 15, 370ff., 384, 436, 456
 - simple, 9

- solvable, 17
 of symplectic matrices, 489
 topological (see Topological group)
 torsion, 258ff
 torsion free, 258ff
 of transformations (see Transformation group)
 of translations, 15
 of unimodular transformations, 397
 of unimodular unitary matrices,
 489, 491
 universal covering (see Universal covering group)
 vector (see Vector group)
 axioms, 1
 order, 1
 Haar, A., 186
 Hausdorff space, 66, 73, 78, 86
 Height of a linear form, 509
 Hereditary property, 69
 Hermitian bilinear form, 219-20
 quadratic form, 457, 505
 scalar product, 490
 Hilbert parallelopiped, 85
 space, 60, 85
 Hilbert's fifth problem, 285, 323
 Homeomorphism, 60, 73, 437, 478,
 505
 differentiable, 313
 smooth, 482
 Homogeneity:
 of a coset space, 104
 of a topological group, 97
 Homogeneous function of several variables, 297, 305
 polynomial, 461
 Homomorphic mapping:
 of groups, 10
 of rings, 39
 Homomorphism:
 adjoint, 264, 275
 analytic, 313ff., 321
 of groups, 10, 488
 of Lie algebras, 386ff., 420, 440
 of Lie groups, 429, 477
 local, 140, 365ff., 432
 natural, 236, 240
 naturally associated with a homomorphism, 387
 of rings, 39
 of topological groups, 112
 of topological rings, 154
 Homotopic paths, 346ff.
 Homotopy, covering, 352, 372
 Ideal, 39
 of a Lie algebra (see Lie algebra ideal)
 of a topological ring, 154
 Identical intersection schemes, 89
 word, 362
 Identity element, 1, 433, 488-9
 mapping, 3, 64
 matrix, 504
 Implicit function theorem, 292, 295,
 311, 317
 Imprimitive root vector, 472-3
 Incidence axioms, 44
 relation, 44
 Indeterminant, 42, 181
 Index, 7, 356
 Induced topology, 63-4
 Induction, transfinite, 244
 Infinite cardinal number, 71, 81
 center, 430
 cyclic group, 6, 248
 dimensional Hilbert space, 60
 topological space, 89
 group, 1
 order, 3, 35
 rank, 34
 sequence, 85
 set, 27, 53, 58, 70-1
 weight, 81
 Initial point, 346ff.
 value problem, 288, 398, 443
 Inner automorphism, 10, 349, 395,
 418, 432, 436
 of a Lie algebra, 476
 local, 300
 derivation, 445, 460
 Integers, 101
 Integrability conditions, 398ff., 403ff.,
 412, 438ff.
 Integral:
 double, 199
 invariant, 186, 192ff
 iterated, 200
 of a matrix valued function, 222
 equation, 82
 on a group, 201ff.
 matrix, 29
 Intersection, of ideals, 451
 of sets, xi
 scheme, 89-90
 Interval, 65, 70
 Invariant, 485
 geometric, 456
 of a Lie algebra, 502, 504
 of a linear transformation, 215
 topological, 346, 349
 bilinear form, 449, 451

- function on a group, 229
- integral, 186, 192ff.
- measure, 186
- quadratic form, 447ff., 454
- positive definite, 450ff.
- scalar product, 460
- subgroup, 8
- subspace, 458ff., 468
- Inverse, 1
 - of a mapping, xii
 - of a quaternion, 159
 - matrix, 5, 400, 406, 442
 - path, 346
- Involutory automorphism, 428, 430
- Irreducible group, 36
 - representation, 325
 - root system, 503
 - σ -system, 517
 - system:
 - of linear transformations, 216, 506
 - of matrices, 216
 - of vectors, 510-11
- Irregular automorphism, 478ff., 485-6
- Isometric root systems, 456, 472, 476
 - sets, 467
 - transformation, 150
- Isometry, 467-8, 472, 474, 503, 512
- Isomorphic groups, 9
 - Lie algebras, 447, 456, 472, 503
 - groups, 487
 - mapping, 9, 112
 - rings, 40
- Isomorphism:
 - of complex local Lie groups, 428
 - of groups, 9
 - of Lie algebras, 386ff., 413, 480
 - of Lie groups, 505
 - local, 133, 138, 279, 299, 300, 488
 - naturally associated with a homomorphism, 11
 - of projective geometries, 44
 - of rings, 40
 - of topological groups, 112
 - of topological rings, 155
- Iterated integral, 200
- Jacobi identity, 380, 382, 390, 394, 460, 464, 470
- Jacobian, 292, 297, 302, 407
- K, 237, 276ff., 415, 487
- k-dimensional plane, 44
- van Kampen, E., 236
- Kernel:
 - degenerate, 82
 - of a homomorphism, 11, 39, 154, 386, 394, 420, 436, 488
- of ineffectiveness, 13, 144
- of an integral equation, 204
- of a local homomorphism, 140
- Killing, W., 377, 422, 447
- Kolmogorov (Kolmogoroff), A. N., 110, 170
- Kowalski, H., 170
- Kuroš, A., 263
- l -dimensional manifold, 481-2
- Left coset, 7, 480
 - ideal, 39
 - mean on a compact group, 196ff.
- Lemma of Urysohn, 67
- Lemniscate, 361ff
 - universal covering of, 362
- Lie, Sophus, 378, 402, 436
- Lie algebra, 345ff., 377, 381ff., 413ff.
 - adjoint algebra of (see Adjoint algebra)
 - adjoint group of, 445ff
 - algebra of derivations of, 392ff., 496
 - algebra of inner derivations of, 394
 - automorphism of, 386, 389, 428, 446ff., 476ff.
 - automorphism group of, 389, 448, 453ff
 - center of (see Center)
 - central ideal of, 451
 - classical, 447, 502ff., 511, 517
 - commutative, 382, 414, 422, 448, 454, 458ff
 - compact (see Compact Lie algebra)
 - complex (see Complex Lie algebra)
 - dimension of, 458
 - direct resolution of (see Direct resolution)
 - exceptional, 423, 447, 506, 512ff
 - homomorphism of, 386ff., 395, 420, 440
 - inner derivation of, 460
 - isomorphic, 456, 472
 - isomorphism of, 386ff., 413, 480
 - of a Lie group, 382ff., 453, 488ff
 - linear, 390ff., 397, 489ff
 - non-commutative, 414, 445, 451, 455
 - one-dimensional, 424, 435, 451, 455
 - rank of, 456, 460, 467
 - real (see Real Lie algebra)
 - regular automorphism of, 456, 460, 467
 - regular subalgebra of, 460ff., 476
 - semi-simple, 422ff., 446, 448, 454-5, 495

- simple, 385ff., 423-4, 445, 451, 455, 502, 504
- solvable, 422ff., 427ff., 448, 451
- subalgebra of (see Subalgebra)
- of transformations, 440ff
- two-dimensional, 414
- of vector fields, 440ff
- vector space of, 445
 - ideal, 385ff., 414, 450, 475
 - central, 451
 - maximal central, 385
 - maximal solvable, 451
 - group, 185, 279, 281ff., 377ff., 436, 476
 - adjoint algebra of, 389, 395-6, 431, 445ff
 - analytic, 285, 308, 313-4
 - classical compact, 370, 489
 - compact (see Compact Lie group)
 - complex, 428ff
 - connected, 435, 446, 448, 504-5
 - dimension of, 478
 - direct factorization of, 388
 - global, 319, 421, 426, 431ff., 444, 448
 - linear, 389ff., 393, 489, 506
 - local, 432, 444, 488
 - local isomorphism of, 430-1
 - rank of, 489
 - real, 429-30, 491
 - simple, 489
 - simply connected, 432, 434-5, 444, 446, 487-8, 504-5
 - two-dimensional, 414
 - series, 324, 326
- Limit of a convergent series of groups, 327
 - number, 269, 271
 - point, 51-2, 70, 74, 85
 - complete, 70
- Line of a projective geometry, 44
- Linear automorphism:
 - of a Lie algebra, 389ff., 393
 - of a vector space, 214, 397, 430, 444, 454, 477, 489-90, 491, 494
 - complex, 512, 514
 - form, 457-8, 497, 499ff., 508
 - pure imaginary, 456, 458, 462, 495, 498
 - real, 456
 - independence:
 - in an abelian group, 27
 - in a projective geometry, 44
 - in a vector space, 43
 - Lie algebra, 390ff., 397, 489ff.
- commutative, 458-9, 462
- group, 389ff., 393, 489, 506
- local, 390ff
- representation, 185ff., 219ff., 324
 - character of, 221
 - degree of, 220
 - equivalence of, 220
 - splitting of, 221
 - unitary, 220
 - span, 475, 501, 509-10
 - complex, 501
 - of a set of vectors, 468
 - of subspaces, 465
 - subspace, 44
 - transformation, 214, 389, 393, 422, 444, 457, 479, 487, 494ff
- characteristic equation of, 460
- characteristic polynomial of, 457, 461
 - eigenvalue of, 456ff., 461
 - eigenspace of, 461
 - null space of, 462
 - with positive determinant, 430
 - skew-symmetric, 457 ff
 - trace of, 445, 452, 465
 - tangent to an arc, 390
 - with trace zero, 397
 - unimodular, 397
 - unitary, 218
- Linearly dependent system, 259
 - independent directions, 512
 - numbers, 257
 - one-parameter subgroups, 296, 299
 - system of vectors, 508ff.
- Local automorphism, 300
 - compactness, 70
 - of a subgroup, 109
 - of a coset space, 109
 - coordinate system, 312
 - coordinates, 310, 483
 - coset space, 139
 - group, 136ff., 282ff., 428, 450, 453
 - dimension of, 142
 - direct factorization, 141
 - direct product, 141
 - factor group of, 140
 - homomorphism of, 140, 365ff
 - of linear automorphisms, 444
 - local isomorphism of, 138
 - locally compact, 142
 - normal subgroup of, 139, 435
 - part of, 138, 431ff

- subgroup of, 139
 - homomorphism, 140, 365ff., 387, 432
 - isomorphism, 267, 279, 299-300, 488
 - of Lie groups, 431
 - of local groups, 138
 - of topological groups, 133, 143
 - Lie group, 283-4, 406, 413, 422, 432, 437, 444, 488
 - complex, 428
 - corresponding to a Lie algebra, 449
 - linear, 390ff.
 - of transformations, 436ff
 - transitive, 433-4
 - normal subgroup, 139, 435
 - one-dimensional subgroup, 444
 - property, 136
 - resolution into direct product, 430
 - simple connectedness, 486
 - subgroup, 139, 395, 435
 - corresponding to a sub-algebra, 385
 - normal, 435
 - one-dimensional, 444
 - Locally arcwise connected space, 346, 348
 - compact local group, 142
 - space, 70, 80
 - topological group, 115
 - connected compact group, 337
 - space, 88
 - topological group, 260
 - countably compact space, 75
 - topological group, 116
 - isomorphic Lie groups, 384, 396, 415, 430, 446, 455
 - local groups, 138
 - topological groups, 133, 345ff.
 - simply connected space, 346, 348
 - m-dimensional manifold, 481
 - Mal'cev, A., 430, 436
 - Manifold, 343, 478, 505
 - analytic, 478, 310, 312
 - closed, 482
 - compact, 478
 - differentiable, 300, 310, 312, 481
 - dimension of, 480
 - product of, 480
 - topological, 311, 314, 319, 338
 - Mapping, xi
 - analytic, 478
 - both ways continuous, 61, 65, 82
 - continuous, 61-2
 - covering, 352, 486
 - discontinuous, 65
 - homomorphic, 10, 39
 - homeomorphic, 60
 - identity, 3, 64
 - inverse, xii
 - isomorphic, 112
 - one-to-one, xii, 340, 386, 478, 486, 492
 - open, 62, 88
 - order preserving, 474
 - smooth, 481-2
 - Markov, A. A., 110
 - Matrix:
 - diagonal, 374, 460
 - diagonal block, 375
 - even order, 492
 - functional, 483
 - integral, 29
 - inverse, 5, 400, 406
 - of a linear transformation, 452
 - non-singular, 4, 397, 405, 439
 - orthogonal (see Orthogonal)
 - scalar, 374
 - skew-symmetric, 309, 398, 447
 - transposed, 9
 - triangular, 309
 - unit, 5
 - unitary, 218
 - groups, 185ff., 489
 - product, 4, 431, 493
 - Maximal collection of sets, 79, 145-6
 - commutative subalgebra, 477, 497
 - connected set, 86
 - normal divisor, 14
 - solvable ideal, 425ff., 435-6, 445, 451
 - system of linearly independent elements, 34
 - Mean value of a function, 196
 - Measure, in Euclidean space, 481
 - invariant, 186
 - Metric, 59
 - space, 59, 75
 - compact, 119
 - of continuous functions, 191
 - normal, 69
 - Metrizable space, 59
 - Metrization theorem of Urysohn, 85
 - Minimal closed set, 54
 - normal subgroup, 21
 - subfield, 42
 - subgroup, 21
 - Montgomery, D., 323

- Motion:
- of a metric space, 150
 - of the plane, 15, 18
- Multiple edges, 515
- Multiplication:
- in a group, 1
 - of polynomials, 42
 - in a synthetic projective geometry, 48
- Multiplicative collection of sets, 79, 87, 250
- Multiplicity:
- of an eigenvalue, 204, 456, 460
 - of a system of sets, 88ff.
 - of a zero, 462
- n-dimensional Euclidean cube, 89
- space, 57, 143, 151, 259, 437, 440, 512
 - regular subalgebra, 495
 - torus, 361
 - vector space, 397, 430
- n-sheeted covering of the circle, 364
- Napier's constant, 214
- Natural coordinate system, 288
- homomorphism of a group into its second character group, 236, 240
 - isomorphism associated with a homomorphism, 11, 40, 113, 155
 - projection:
 - of a group, 12
 - of a ring, 39, 155
 - of a topological group, 113
 - onto a coset space, 103
 - topology:
 - on Euclidean space, 59, 65
 - on the line, 65, 117
- Negative, 2
- Neighborhood, 54
- coordinate, 481
 - principal, 176
- properly covered, 352, 366
- properly covering, 366
- relative, 462
- spherical, 477, 484-5
- star-shaped, 290
- sufficiently small, 332
- von Neumann, J., 186, 192, 323
- Newton's formula, 181
- Non-collinear vectors, 506-7, 518
- Non-commutative Lie algebra, 414
- compact simple, 447-8
 - simple, 445, 451, 455
- Non-conjugate elements, 231
- Non-Desarguan geometry, 46
- Non-Euclidean plane, 430
- Non-identical automorphism, 414
- Non-isomorphic subgroups, 35
- Non-singular matrix, 4, 397, 400, 405, 439
- Norm, in a Euclidean space, 202
- of a quaternion, 159
- Normal subgroup, 8, 414, 434, 442
- of a complex local Lie group, 429
 - generated by a set, 21
 - of a Lie group, 414
 - local, 139, 435
 - of a local group, 139
 - of a local Lie group, 432
 - of a topological group, 101
 - 0-dimensional, 488
 - space, 66ff., 73, 87
- Normalized element, 202
- Notation of tensor analysis, 377, 447
- Nowhere dense set, 481, 484, 496
- Null-homotopic path, 347ff., 354, 357, 486
- Null path, 346, 359, 486
- space, 462
- Number, cardinal (see Cardinal number)
- complex, 153
 - ordinal, 71, 72, 79
 - real, 153
 - of sheets of a covering, 356
- One-dimensional complex vector space, 463, 465
- ideal, 414
 - Lie algebra, 424, 435, 451, 455
 - subalgebra, 389
 - subgroup, 421, 444
 - subspace, 389, 466ff.
- One-parameter subgroup, 142, 264, 287ff., 331, 403, 407, 418, 421, 435, 440ff., 476ff., 486, 490, 492
- differentiable, 288, 293
 - direction vector of, 288, 449-50
 - linear independence of, 296, 299
- One-to-one correspondence, 423, 511
- mapping, xii, 340, 386, 478, 486, 492
- Open covering, analytic, 312
- differentiable, 312
 - homomorphism, 112, 115
 - mapping, 62, 88
 - set, 52, 63, 405, 437, 462, 481
 - subgroup, 132, 242, 244
- Order:
- of a group, 1
 - of a group element, 3

- of smallness, 378
- preserving mapping, 474
- relation, 471ff., 508-9
- Ordinal number, 71-2, 79
- Orthogonal basis, 495, 498
 - Cartesian coordinate system, 159
 - complement, 450, 458-9, 461
 - elements, 202, 475, 503
 - group, 9, 151, 397
 - matrix, 9, 151, 218, 228, 309, 321, 373, 397, 454, 489
 - pair of groups, 254
 - resolution, 461
 - transformation, 455
- Orthogonalization, 202
- Orthonormal basis, 202, 461, 467, 489ff., 515
 - system
 - of functions, 213-4
 - of vectors, 202, 301
- Oscillation of a function, 191
- π -system, 510ff.
- π -sybsystem, 511-2, 517
- p-adic numbers, 153, 158, 163ff., 171, 179
- Pair of groups, 254
- Part, of a coordinate space, 312
 - of a local group, 138, 431ff.
- Partition of a group into cosets, 7
- Pascal's theorem, 49
- Path, 346
 - closed, 346
 - covering, 352ff.
 - equivalent, 346ff.
 - homotopic, 346ff.
 - inverse, 346
 - null, 346
 - class, 486
- Permutation, 4
- Perspectivity, 45
 - center of, 45
- Peter-Weyl Theorem, 225
- Plane, 15
 - generalized projective, 364
 - non-Euclidean, 430
 - projective, 430
 - in a projective geometry, 44
- Poincaré, H., 345
- Point, adherent, 52
 - of discontinuity, 65
 - limit, 51-2, 74, 85
 - in a projective geometry, 44
 - of a topological space, 52
- Polynomial, degree of, 461
- homogeneous, 461
- over a field, 42
- Positive definite Hermitian form, 21.
 - 20
 - quadratic form, 447ff., 454ff.
 - scalar product, 446
 - root vector, 472-3
 - vector, 471, 508ff.
- Possession of a tangent, 286
- Prime characteristic, 41
 - subfield, 42
- Primitive root vector, 447, 471ff.
 - vector, 508-9
- Principal neighborhood, 176
- Product:
 - of analytic manifolds, 313
 - bracket, 382-3, 390, 426ff., 439, 448
 - of compact spaces, 78
 - of differentiable manifolds, 313
 - direct, 18, 22, 76
 - of elements, 1, 38
 - of groups, 18, 22, 76
 - of Hausdorff spaces, 78
 - of homomorphisms, 388
 - matrix, 4, 431, 493
 - of motions, 15
 - of paths, 346
 - of path classes, 349
 - of polynomials, 42
 - of quotients, 41
 - scalar (see Scalar product)
 - of subgroups, 21-2
 - of subsets, 5
 - of topological spaces, 76ff.
 - of transformations, 3, 452
 - vector, 384, 389, 448, 455, 466, 503
- Projection, 352
 - natural, 12, 103, 360
 - onto a factor, 77
 - stereographic, 351
- Projective geometry, 44, 183
 - continuous, 184
 - isomorphism of, 44
 - synthetic, 45
 - plane, 430
 - generalized, 364
 - transformation, 430
- Proper covering, 352
- Properly covered neighborhood, 352, 366
 - covering neighborhood, 366
- Property:
 - finite intersection, 70

- hereditary, 69
- L, 260ff.
- Pure imaginary diagonal matrix, 497
 - eigenform, 459
 - eigenvalue, 457
 - linear form, 456ff., 462, 495, 498
 - quaternion, 159, 169, 370, 384-5
- Quadratic form, 430
 - Hermitian, 457
 - invariant, 447ff., 450ff
 - of a kernel, 205
 - non-degenerate, 430, 448
 - positive definite, 447ff., 450ff., 456-7
 - of a scalar product, 448, 456, 467
 - of a symmetric bilinear form, 449
- Quadrilateral, 469
- Quasi-cyclic group, 241
- Quaternions, 153, 158ff., 169, 370ff., 384, 421, 504-5
 - pure imaginary, 159, 169, 370, 384-5
 - real, 384
- Quaternion units, 159, 161
- Quotient field, 40
- r-dimensional commutative Lie group, 414
 - Euclidean space, 260, 311, 405, 436
 - local Lie group, 437
 - sphere, 372
 - vector group, 98, 110, 267, 414
 - space, 382, 414, 441
- r-fold edge, 511
- Rank:
 - of an abelian group, 34, 259
 - of a compact Lie algebra, 456, 460, 467, 474ff., 495, 502, 517
 - of a functional matrix, 478-9, 483
 - of a Lie group, 489
 - of a matrix, 304
 - of a π -system, 511
- Rational function, 42
- Real compact semi-simple Lie algebra, 447
 - form of a complex Lie algebra, 422, 430, 446
 - Lie algebra, 382, 422-3, 426ff., 443ff., 449ff., 453, 455, 477, 491-2
 - group, 429-30, 491
 - linear form, 456
- numbers, 153
- quaternion, 384
- scalar product, 489
- semi-simple Lie algebra, 423
- simple Lie group with infinite center, 430
- vector space, 426, 439, 471, 489
- Reducibility (of a Lie algebra), 475
- Reducible system:
 - of linear transformations, 216
 - of matrices, 216
 - of vectors, 510
- Reduction of a system of vectors, 475, 503, 510
- Refinement:
 - of a collection of sets, 89
 - of a covering, 92
- Reflection in a plane, 518
- Reflexivity, 7, 347
- Regular automorphism, 456, 460, 467, 474-5, 477-8, 485
 - space, 66, 97
 - subalgebra, 456, 460ff., 467-8, 471, 474ff., 484-5, 495ff., 501
- Regularity of a coset space, 104
- Representation (see Linear representation)
- Residue class, 39, 420
 - algebra of a Lie algebra, 386, 415, 424ff.
- Resolution, direct (see Direct factorization/resolution)
- Riemann surface, 351
- Right coset, 7
 - ideal, 39
 - mean on a compact group, 194
- Ring, 38
 - algebraic, 154
 - division (see Division ring)
 - isomorphism of, 40
 - of polynomials, 42
 - of residue classes, 39, 155
 - topological, 154
- Root space of a compact semi-simple Lie algebra, 462-3
 - system, 446-7, 456, 462-3, 467ff., 474ff., 485, 489, 495-6, 502ff., 511-2, 515, 517
 - isometric, 456, 472, 476
 - irreducible, 503
 - non-isometric, 476
 - similar, 515
 - vector, 456, 462, 467, 475, 480
- imprimitive, 471ff
- positive, 472-3
- primitive, 471ff

- Rotation:
 angle of, 18
 of Euclidean space, 321, 384, 436
 of the plane, 15
- Rotation group, 370ff.
- σ -system, 506ff., 517-8
 irreducible, 506
- s-dimensional torus, 454
- Scalar matrix, 374, 506
 — product, 169, 201, 385, 445ff., 456
 Hermitian, 490
 invariant, 460
 on a Lie algebra, 452ff., 460, 468-9, 478, 498
 positive definite, 446
 quadratic form of, 456, 467
 real, 489
 subspace of degeneracy of, 449
- Schreier, O., 346
- Second theorem of Lie, 402, 436-7
- Semi-simple ideal, 454
 — Lie algebra, 422ff., 435, 448, 454-5, 495
 compact (see Compact semi-simple Lie algebra)
 complex, 423, 446
 real, 423
 — Lie group, 488
 — subalgebra, 436
 compact, 487
- Separable group, 116, 118
 — locally connected compact abelian group, 262
 — space, 54, 69, 75
- Separation axioms, 65ff.
- Sequence convergent, 155
 fundamental, 156
 transfinite, 26
 uniformly convergent, 188
- Series, binomial, 83
 of compact (Lie) groups, 326
 of polynomials, 83
- Set, xi
 closed, 63, 86
 closed-open, 87
 compact, 70, 481
 compact-open, 88
 connected, 86
 equality of, xi
 everywhere dense, 5, 86, 484, 488
 of generators, 4
 nowhere dense, 481, 484
 open, 63, 405, 437
 well ordered, 54
- Sheet of a covering, 356, 374
- Shur, I., 216
- Shur's lemma, 214, 216, 222
- Similar root systems, 467, 502, 504, 515
 sets, 467
- Similarity, 467, 503, 517
 coefficient of, 467-8
 of matrices, 215
 of transformation groups, 13, 148
- Simple group, 9
 — Lie algebra, 385, 389, 423ff., 445, 455, 502, 504
 compact, 445, 447-8, 466, 506, 512
 complex, 449
 non-commutative, 451, 455
 — group, 430, 489
 — real with infinite center, 430
 topological group, 104
- Simplicity of a Lie algebra, 468, 503
- Simply connected group, 415, 421
 — Lie group, 421, 429, 432, 434ff., 444, 446, 487-8, 505
 compact semi-simple, 488
 — space, 349
- Singular matrix, 4
- Skew-symmetric bilinear form, 489
 — linear transformation, 457-8, 460ff.
 — matrix, 309, 397, 447, 489, 500-1
 complex, 490
- Skew-symmetry:
 of commutators, 464
 of structure constants, 409ff., 452-3
- Small deformation, 368
- Smooth cross-section, 372
 — homeomorphism, 482
 — mapping, 481-2
- Solvability of the group of motions of the plane, 18
- Solvable group, 17
 — ideal, 422, 424
 — maximal, 425ff., 435, 451
 — Lie algebra, 422ff., 427-8, 434, 448, 451
- Space:
 compact, 70, 75, 79, 81, 85
 compact Hausdorff, 73
 completely regular, 66, 81
 countably compact, 74, 85
 — metric, 74, 5
 covering, 345-6, 351ff
 Euclidean (see Euclidean space)

- Hausdorff, 66, 73, 86
 Hilbert, 85
 of infinite sequences, 85
 locally compact, 70, 80
 locally countably compact, 75
 metric, 69, 75, 150
 normal, 66, 73, 87
 regular, 66
 separable, 75
 unitary, 201, 218
 universal covering, 359
 — of cosets, 103, 148, 372, 444, 480
 compact, 109
 homogeneity of, 104
 local, 139
 locally compact, 109
 modulo a compact subgroup, 109
- Sphere**, 372
 in Euclidean space, 59, 321
 in a metric space, 59
 unit, 344, 351
- Spherical neighborhood**, 477, 484-5
 region, 482
- Splitting of a reducible representation**, 221
- Stabilizer subgroup**, 14, 319, 340, 342, 344, 374, 505
- Star-shaped domain**, 297
 neighborhood, 290
- Stereographic projection**, 351
- Structure constants**, 377ff., 414, 416, 427, 441ff., 452
 of a Lie algebra, 382
 of a Lie group, 377ff., 401ff.
- Subalgebra of a Lie algebra**, 385, 397, 424ff., 434, 443, 451, 456ff.
 commutative, 456, 495, 497ff.
 compact semi-simple, 487
 corresponding to subgroup, 385ff., 397, 415, 418, 476ff., 480, 492
 dimension of, 460
 one-dimensional, 389
 regular, 456, 460ff., 467-8, 471, 474ff., 484-5, 495
 semi-simple, 436
- Subcomplex**, 513
- Subdivision ring**, 40
- Subfield**, 40
 central, 42
 prime, 42
- Subgroup**, 6, 63
 admitting division, 260
 central normal, 16, 338, 360, 385
 closed, 477
 commutator, 16
 of compact elements, 277
- of a complex local Lie group, 429
 corresponding to a subalgebra, 421, 435
 cyclic, 487
 discrete, 134, 360, 370, 415, 488
 — central, 485
 — normal, 345, 370
 generated by a set, 21, 36
 global, 421, 444
 index of, 7
 invariant, 8
 of a Lie group, 480
 local, 435, 444
 of a local group, 139
 of a local Lie group, 432
 normal, 8, 414, 429, 434
 one-dimensional, 421
 one-parameter (see One-parameter subgroup)
 open, 242, 244
 stabilizer (see Stabilizer)
 of a topological group, 101, 109
 toroidal, 421
 torsion, 258
 zero-dimensional, 335ff.
- Submatrix**, 501
- Subspace**:
 of degeneracy, 449
 invariant, 458-9, 461, 468
 one-dimensional, 389
 topological, 63, 70
 of a vector space, 44, 385
- Sufficiently small neighborhood**, 332
- Sum**:
 of group elements, 2
 direct (see Direct sum)
 of quotients, 41
- Šura-Bura, M. R.**, 87
- Symmetric bilinear form**, 448, 452
 invariant, 449
 — neighborhood of the identity, 116, 134
- Symmetry**, 7, 347
- Symplectic matrix**, 489
- Synthetic definition of a projective geometry**, 45
- System**:
 of differential equations, 393, 402ff., 412, 442-3
 of generators, 27, 116, 415, 440
 — finite, 28, 32, 34ff
 orthonormal, 202
- Tangent linear transformation**, 390, 444
 — space, 429, 479
 — vector, 286, 444, 454

- Taylor coefficients, 378ff.
 — series, 378ff., 402, 404
- Tensor, 377
 — analysis, 283, 377
 — notation, 283, 447
- Terminal point, 346, 350ff.
- Theorem of Frobenius, 158, 160
 — of Lie:
 — first, 402, 436-7
 — second, 402, 436-7
 — third, 378, 402
 — of Tihonov, 78
- Theory of partial differential equations, 398
- Third Theorem of Lie, 378, 402
- Three-dimensional Euclidean space, 455, 466
 — simple Lie group, 431
 — sphere, 505
 — vector space, 384
- Tihonov (Tychonoff), A. N., 69, 76, 78, 81
- Topological division ring, 153ff
 — admitting continuous closure, 176
 — principal neighborhood of, 176
 — field, 154
- Topological group, 95ff
 — admissible, 369
 — algebraic group of, 96
 — automorphism of, 112, 152
 — center of, 130
 — central normal subgroup of, 130
 — compact, 82
 — compactly generated, 116
 — complete regularity of, 105
 — complete system of neighborhoods
 in, 99ff., 134
 — connected, 129ff., 367, 433
 — countably compact, 127
 — direct product of, 120, 123
 — direct factorization of (see Direct factorization)
 — discrete, 98
 — factor group of, 104
 — finite dimensional, 367, 488
 — full linear (see Full linear group)
 — homomorphism of, 112
 — of integers, 101
 — isomorphism of, 112
 — local isomorphism of, 133, 143
 — local properties of, 136
 — locally countably compact, 116
 — separable, 118
 — simple, 104
 — simply connected, 415, 421
 — totally disconnected, 87, 129ff.
- Topological invariant, 346, 349
 — manifold, 311, 314, 319, 338
 — closed, 311
 — mapping, 60
 — property, 60
 — ring, 154
 — space, 51ff
 — arcwise connected, 346, 348
 — base for, 54
 — compact, 70, 79, 81, 85
 — complete system of neighborhoods
 in, 54
 — completely regular, 81
 — connected, 86
 — countably compact, 85, 172
 — definition of by means of neighborhoods, 57
 — discrete, 53
 — homeomorphism of, 60
 — locally arcwise connected, 346, 348
 — locally compact, 80
 — locally connected, 88
 — locally simply connected, 346, 348
 — metrizable, 59
 — normal, 66, 73, 87
 — product of, 76ff
 — regular, 97
 — separable, 54, 69
 — simply connected, 349
 — totally disconnected, 87, 92
 — weight of, 54
 — zero-dimensional, 92
- Topology:
 — induced, 63-4
 — natural, 59, 65
- Toroidal subgroup, 421
- Torsion group, 258ff.
 — subgroup, 258
- Torsion-free group, 258ff.
- Torus:
 — n-dimensional, 361
 — two-dimensional, 421
- Total differential, 400
- Totally disconnected compact abelian group, 258
 — — — group, 87, 129, 131ff.
 — — — space, 87, 92
- Trace:
 — of a linear transformation, 397,
 445, 452, 465, 491
 — of a matrix, 215, 309
- Transcendental element, 42
- Transfinite construction, 27
 — induction, 75, 244
 — number, 26-7
 — ordinal, 71

- Transfinite sequence, 26, 71-2, 79, 269, 323-4
- Transformation:
- fractional linear, 430
 - linear (see Linear transformation)
 - of a matrix, 215
 - projective, 430
 - group, 13, 95, 436ff
 - compact, 339ff
 - continuous, 319
 - similarity of, 13
 - topological, 143ff
 - transitive, 319
- Transitive local Lie group of transformations, 443-4
- transformation group, 13, 144, 319, 505
 - acting on a sphere, 506
- Transitivity:
- of a relation, 7
 - of a transformation group, 3, 13, 347
- Translation
- Transposed matrix, 9, 216
- Triangle, 469-70, 472-3
- in a projective geometry, 45
 - inequality, 59
- Triangular matrix, 309
- Trivial center, 487
- linear representation, 185
- Two-dimensional Lie algebra, 414
- Lie group, 414
 - subalgebra, 389
 - torus, 421
- Two-sided ideal, 39
- Tychonoff (see Tihonov, A. N.)
- Unbounded division, 35, 37
- Uniform approximation by polynomials, 83-4
- completeness, 225
 - continuity, 187ff.
 - convergence, 188
 - equicontinuity, 188
- Uniformization, 365
- Uniformly bounded system of functions, 188
- complete system of functions, 324
 - convergent sequence, 188
 - series, 83
- Unimodular group, 397
- transformation, 397
 - unitary matrix, 489, 491
- Union, xi, 478
- Unit matrix, 5
- sphere, 151, 344, 351, 374
- of dimension three, 159
- Unit vector, 513
- Unitary group, 219
- linear representation, 220
 - matrix, 218, 489
 - unimodular, 489, 491
 - space, 201, 218, 490, 493, 505
 - transformation, 218
- Universal covering, 345, 361, 476, 488
- of the generalized projective plane, 364
 - of a lemniscate, 362
 - mapping, 359
 - group, 352, 364ff., 415, 421, 430, 435, 485, 487
- Urysohn function, 84
- Urysohn's Lemma, 66-7, 84, 105, 118, 226, 229, 231-2
- Vector, 43
- positive, 471
 - root (see Root vector)
 - tangent, 444
 - field, 439ff.
 - group, 98, 110, 143, 267, 300, 436, 487-8
 - product, 169, 384, 389, 448, 455, 466, 503
- Vector space, 43, 201, 214, 415, 444, 452, 454
- complex, 426, 428-9, 490-1, 495
 - dimension of, 459ff
 - of a Lie algebra, 445, 477
 - real, 426, 430, 439, 471, 489
 - three-dimensional, 384
 - subspace, 44
- Weight:
- of a compact abelian group, 254
 - of dual groups, 239
 - of a topological space, 54, 81, 213, 232
- Weil, A., 236, 323
- Well ordered set, 54
- Weyl, H., 186, 346, 377, 446-8, 476
- Whole numbers (see Integers)
- Winding line, 117, 127, 421
- Word, 362
- empty, 362
 - identical, 362
- Zero:
- of an abelian group, 2
 - characteristic, 41
 - divisor of, 40
- Zero-dimensional compact group, 339

- ____ compact Hausdorff space, 92 Zero-th power, 3, 5
____ normal subgroup, 488 Zippin, L., 323
____ subgroup, 335ff.