Communicated 23 January 1952 by F. Carlson and J. Malmquist

Convexity and norm in topological groups

By Hans Rådström

With 2 figures in the text

§ 1. Introduction and preliminaries

1.1. This work originated in a simple observation on the behaviour of sets of points in the euclidean plane when a certain operation of taking powers is performed on them. Let A and B be two sets in the plane. We define $A+B$ to be the set of all points which can be expressed in the form $a+b$ where $a \varepsilon A$, $b \varepsilon B$ and $a+b$ is the usual vectorial addition of points. The expression $A+A+\ldots A$ will be denoted by A^n if the repeated sum contains n terms, and we shall call A^n the n:th power of A. The reason for choosing the symbol A^n instead of nA is that for real λ the symbol λA has already a universally accepted meaning.

The observation mentioned above may be formulated as follows: The higher the power is, the higher is the degree of convexity. (At present we shall make no attempt to give this statement a precise meaning.) An inspection of Fig. 1 and 2 may make the meaning of this vague statement more clear.

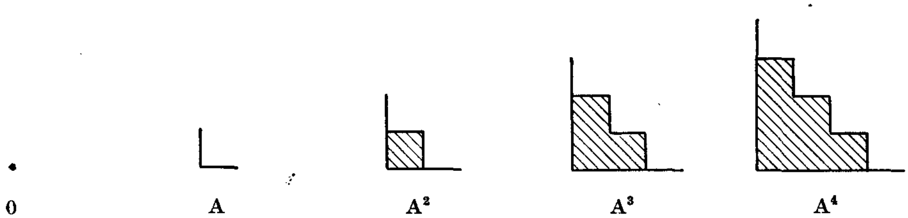

Fig. 1.

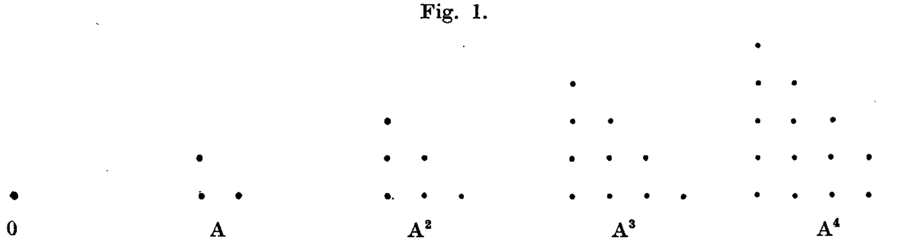

Fig. 2.

In the example of figure 1, it is clear that the sets $\frac{1}{n} A^n$ fill up more and more of the convex hull of A as n increases. In fact, for sufficiently large n any given interior point of the convex hull of A will be an element of $\frac{1}{n} A^n$. The corresponding statement is not true for the example given in figure 2 but it is clear that any point of the convex hull of A in this case also is the limit as $n \to \infty$ of points belonging to $\frac{1}{n} A^n$. In fact, we shall see later that the convex hull of A in a certain sense, to be defined in section 1.4, is the limit of the sets $\frac{1}{n} A^n$.

1.2. These examples seem to suggest that high powers of small sets are in some sense almost convex. Paragraph 3 will be devoted to giving these notions a precise meaning. As a result we obtain a characterization of compact convex sets in a euclidean space in terms of the operation of taking powers. The usual definition of convexity involves the use of the operation of multiplication with scalars. The characterization of compact convex sets which we obtain in § 3 does not involve this operation but only the addition. This fact is important, since it indicates the possibility of defining convexity in arbitrary topological groups with the aid of an analogue for groups of the characterization produced for sets in a euclidean space.

When one tries to work out such a program, it turns out that it is practical not to study the analogues of convex sets directly, but rather the analogues of a certain type of families of convex sets, namely those families which consist of all sets of the type λK, where K is a given convex set and λ a non-negative real number. In an arbitrary group the analogous concept is a family A_λ of subsets depending on a non-negative real number λ and satisfying: $A_{\lambda_1+\lambda_2} = A_{\lambda_1} A_{\lambda_2}$. (We use multiplicative notation so that AB denotes the analogue of $A+B$.) It is a well known fact that if K is a convex set in euclidean space and $\lambda_1 \lambda_2 \geq 0$ then $(\lambda_1 + \lambda_2) K = \lambda_1 K + \lambda_2 K$. If certain further conditions of a topological nature are satisfied by such a family of sets A_λ, we call this family (or rather the mapping $\lambda \to A_\lambda$) a one-parameter semigroup of subsets of the group. In particular, if the group is a euclidean space with addition as group operation, we see from the characterization of compact convex sets mentioned above that a one-parameter semigroup of compact sets is of the form $A_\lambda = \lambda K$ where K is convex.

GLEASON (6) has used the concept of a one-parameter semigroup of subsets of a group to establish the existence of an arc in any locally compact group which is not totally disconnected. Some of his results are important for the present investigation and will therefore be summarized in the proper place (see section 2.8).

We give now a short summary of the contents of the present paper. Paragraph 2 is devoted to the definition of one-parameter semigroups and to the deduction of some consequences of this definition. After the discussion of one-parameter semigroups in euclidean space in § 3, we turn to Lie groups in § 4. The main result (theorem 4.12) states that any one-parameter semigroup in a

Lie group has an infinitesimal generator which is a convex set. Here of course the term "infinitesimal generator" has to be given a precise meaning (definition 4.12).

Paragraph 5 is devoted to the introduction of the concept of a normed group. A metric on a group is a norm if it is left invariant and if the spheres S_δ of radius δ around the identity of the group constitute a one-parameter semigroup. It turns out that a normed group is metrically convex in the sense of MENGER (**9**). From this result it follows that a locally compact normed group is separable, metric, connected and locally connected. It seems to be a very plausible conjecture that for locally compact groups these conditions are also sufficient in order that it be possible to remetrize the group so as to make it a normed group. In § 6 we collect some theorems on normability in this sense and prove the conjecture for commutative and essentially also for compact groups.

1.3. As a continuity axiom for topological groups we postulate continuity of x^{-1} and of xy simultaneously in both variables.

As a continuity axiom for linear spaces we postulate that the space be a topological group if addition is used as group operation. We shall say that the group thus defined is the additive group of the linear space or that the linear space is a group under addition. We also require that multiplication with scalars be continuous in both variables simultaneously.

In general, we shall use multiplicative notation for groups. Exceptions will be pointed out whenever they occur. The identity will be denoted by e in multiplicative notation (with indices if necessary) and in additive notation by 0.

Let A and B be two subsets of a group. By AB we mean the set of all products ab where $a \varepsilon A$ and $b \varepsilon B$. This is an associative operation. It is commutative if the group is commutative. Repeated multiplication of a set A with itself is denoted by A^n. We have

$$A\left(\bigcup_\alpha B_\alpha\right) = \bigcup_\alpha (A B_\alpha) \tag{1}$$

$$A\left(\bigcap_\alpha B_\alpha\right) \subset \bigcap_\alpha (A B_\alpha). \tag{2}$$

In particular, if B_α is a fundamental system of neighborhoods of e, then the left side of (2) is A and the right side is the closure $\bar{A}$ of A. Multiplication is monotone:

$$A_1 \supset B_1 \text{ and } A_2 \subset B_2 \text{ imply } A_1 A_2 \subset B_1 B_2. \tag{3}$$

If A contains e then $B \subset AB$ and $B \subset BA$.

From the definition of A^n it is obvious that

$$A^n A^m = A^{n+m}. \tag{4}$$

We shall let A^0 be defined as $\{e\}$ and for positive n we put A^{-n} = the set of all inverses of elements in A^n. Then (4) is valid for $mn \geqq 0$ but not in general for n and m of different signs.

If at least one of the sets A and B is compact and the other closed then AB is closed. If both are compact then AB is compact (see WEIL **12,** p. 16).

We have

$$\bar{A}\bar{B} \subset \overline{AB}. \tag{5}$$

Proof: Each of the following three conditions:

$x \varepsilon U A$ for all neighborhoods U of e

$x \varepsilon A V$ » » » V » e

$x \varepsilon U A V$ » » » U and V of e

is equivalent to $x \varepsilon \bar{A}$. Let $ab \ \varepsilon \bar{A}\bar{B}$. Then for all U and V we have ab $\varepsilon (UA)(BV)$. Thus $ab \ \varepsilon U(AB)V$ which shows that $ab \ \varepsilon \overline{AB}$.

We denote the set with the elements $a, b, \ldots$ by $\{a, b, \ldots\}$. The set of all those x which have a certain property P is denoted by $\{x \mid P\}$.

If a is a point we shall write aB or Ba instead of $\{a\} B$ or $B \{a\}$ respectively.

1.4. In order to make it possible to define one-parameter semigroups of subsets of a group in a concise form, we need a method to topologize the set of all closed subsets of the group. One such method is the well known method of HAUSDORFF (**7,** p. 143), which applies to arbitrary metric spaces. Hausdorffs method is easy to extend to any uniform space. (BOURBAKI, **4,** p. 97, exercise 7.) In the case of a topological group, G, the procedure is the following: Let K denote the set of all closed subsets of G, let N be a neighborhood of the identity in G and let H_0 be an element of K. By $\hat{N}$ we denote the set of all those $H \varepsilon K$ for which the following two inequalities hold: $H_0 \subset NH$ and $H \subset NH_0$. Now let N_a be the elements of a fundamental system of neighborhoods of the identity of G. The corresponding sets $\hat{N}_a$ will then form a fundamental system of neighborhoods of H_0. The topology thus defined will be called "the Hausdorff topology for K". It is easily verified that this topology is unique, i.e. that it is independent of the choice of the fundamental system N_a.

It is well-known that, topologized in this manner, the space K satisfies Hausdorffs separation axiom.

Let H' be a closed subset of G. Then the set K' of all subsets of G which are also subsets of H' is a certain subset of K. It is known that if H' is compact then K' is also compact in the sense defined by the Hausdorff topology for K.

From the method originally used by HAUSDORFF in the metric case it follows that if G is metrizable then K is metrizable. This means that in this case we may describe the topology of K in terms of convergence of sequences. Hausdorffs method applied to groups gives a metric defined on K. We shall call this metric the Hausdorff metric for K. If S_δ denotes the closed sphere of radius δ in a given metric for G then the corresponding Hausdorff metric for K is defined by $d(H_0, H) = \inf \delta$ where δ is a non-negative number such that

$$H_0 \subset S_\delta H$$

and

$$H \subset S_\delta H_0.$$

In the metric case it has advantages to use sequential compactness instead of compactness. Since in this case the two notions are equivalent we have the following proposition. If A is a compact subset of G and A_ν, $\nu = 1, 2, 3 \ldots$ a sequence of closed subsets of A, then A_ν contains a subsequence which is convergent in the sense of Hausdorff topology.

1.5 Since the product AB of two closed sets A and B is not necessarily closed, the function $(A, B) \to AB$ from $K \times K$ into the set of subsets of G is not necessarily into K. Let us therefore consider the function $(A, B) \to \overline{AB}$ from $K \times K$ into K and inquire whether this function is continuous in the sense of the Hausdorff topology for K.

We shall say that a closed subset A of G has property P if to any given neighborhood U_1 of e it is possible to find another, U_2, so that $A U_2 \subset U_1 A$.

We have the following proposition:

If the mapping $(A, B) \to \overline{AB}$ is continuous at the point $(A_0, \{e\})$ then A_0 has property P.

If A_0 has property P and B_0 is arbitrary, then the mapping $(AB) \to \overline{AB}$ is continuous at (A_0, B_0).

Proof: Suppose first that $\overline{AB}$ is continuous at $(A_0, \{e\})$. Then it is continuous in B separately. This means that given a neighborhood U_1 of e there exists another, U_2, such that

$$1.\quad \{e\} \subset U_2 B$$

and

$$2.\quad B \subset U_2 \{e\} = U_2$$

together imply

$$3.\quad A_0 \{e\} \subset U_1 A_0 B$$

and

$$4.\quad A_0 B \subset U_1 A_0 \{e\} = U_1 A_0.$$

In particular the choice $B = U_2$ makes 1. and 2. hold true. Leaving 3. to one side we obtain from 4.:

$$A_0 U_2 \subset U_1 A_0$$

which proves property P.

Conversely, suppose that A_0 has property P. The continuity at (A_0, B_0) is equivalent to the following statement: Given a neighborhood, U, of e there exists another, V, such that if $A, B \varepsilon K$ and satisfy

$$(\alpha)\colon A_0 \subset VA, \qquad (\beta)\colon A \subset VA_0, \qquad (\gamma)\colon B_0 \subset VB, \qquad (\delta)\colon B \subset VB_0,$$

then $A_0 B_0 \subset U AB$ and $AB \subset UA_0 B_0$.

Therefore suppose that U is given. Choose first U_1 with $U_1^4 \subset U$, secondly U_2

such that $A_0 U_2 \subset U_1 A_0$ and then $V \subset U_1 \cap U_2$. Multiplying (α) with (γ) and (β) with (δ) we obtain:

$$A_0 B_0 \subset V A V B \text{ and } A B \subset V A_0 V B_0.$$

Thus the proposition will be proved if we show that $V A V \subset U A$ and $V A_0 V \subset U A_0$. Since $A_0 \subset V A_0$ it is enough to prove the first of these two inequalities for all A which satisfy (α) and (β):

$$V A V \subset V^2 A_0 V \subset U_1^2 A_0 U_2 \subset U_1^3 A_0 \subset U_1^3 V A \subset U_1^4 A \subset U A.$$

This proves the proposition.

1.6. The following example shows that there are groups G containing subsets A which do not have property P.

Let G be the group consisting of all regular two by two matrices, topologized in the natural way. The identity is the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let A be the set of all matrices of the form $\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, $n = 1, 2, 3 \ldots$ Let $U(\varepsilon)$ be the set of those matrices $\begin{pmatrix} 1+a_{11} & a_{12} \\ a_{21} & 1+a_{22} \end{pmatrix}$ for which $|a_{ij}| \leqq \varepsilon$. Then $U(\varepsilon_1) A_0$ consists of all matrices of the type

$$(\alpha) \qquad \begin{pmatrix} n(1+a_{11}) & a_{12} \\ n a_{21} & 1+a_{22} \end{pmatrix} \qquad |a_{ij}| \leqq \varepsilon_1, \; n = 1, 2, 3 \ldots$$

and $A U(\varepsilon_2)$ consists of all matrices of the type

$$(\beta) \qquad \begin{pmatrix} m(1+b_{11}) & m b_{12} \\ b_{21} & 1+b_{22} \end{pmatrix} \qquad |b_{ij}| \leqq \varepsilon_2, \; m = 1, 2, 3 \ldots$$

A comparison between the matrix elements a_{12} and $m b_{12}$ shows that not every matrix of type (β) can be of type (α). Let namely $b_{12} \neq 0$. Then $m b_{12}$ is unbounded as $m \to \infty$. But if the matrix were of type (α) $|m b_{12}|$ would have to be $\leqq \varepsilon_1$. This shows that A does not have property P.

1.7. We remark that the subset of K consisting of those sets which have property P is closed under the operation $\overline{AB}$. Let namely U_1 be given. Then there exist U_2 with $A U_2 \subset U_1 A$ and U_3 with $B U_3 \subset U_2 B$. Thus $U_1 A B \supset A U_2 B \supset A B U_3$. But $U_1 A B \subset U_1 \overline{AB}$ and $A B U_3 \supset \overline{AB} U_4$ if U_4 is chosen sufficiently small, for example so that $U_4^2 \subset U_3$.

If G has the property that given any neighborhood U of e there exists another, V, such that for all $a \varepsilon G$ we have $a V a^{-1} \subset U$, then every subset of G has property P. Conversely, it can be shown that if G is not of the type mentioned, then there exist sets A_0 and B_0 so that $\overline{AB}$ is not continuous at (A_0, B_0). We deduce that if G is abelian, then $\overline{AB}$ is continuous everywhere.

The same conclusion holds if G is compact, since it is well known that every compact set has property P. In an arbitrary group it is therefore also true that $\overline{AB}$ is continuous at (A_0, B_0) if A_0 is compact.

Thus for compact sets A and B we have: AB is compact and is a continuous function in both variables simultaneously.

1.8. We shall need the following proposition later. Let A be a compact set, and let A_ν and m_ν, $\nu = 1, 2, 3 \ldots$ be sequences of compact sets and positive integers respectively such that $A_\nu^m \subset A$ for all $m \leqq m_\nu$. Let r_i, $i = 1, 2, 3 \ldots$ be an enumeration of the rational numbers between 0 and 1. We denote the largest integer $\leqq \gamma$ by $[\gamma]$. Then it is possible to find a sequence of integers n_ν so that each of the following sequences converges to a compact subset of A as $\nu \to \infty$:

$$A_{n_\nu}^{[r_1 m_{n_\nu}]}, \quad A_{n_\nu}^{[r_2 m_{n_\nu}]}, \quad A_{n_\nu}^{[r_3 m_{n_\nu}]}, \ldots$$

Proof: Since $r_i \leqq 1$ we have $[r_i m_\nu] \leqq m_\nu$ and therefore $A_\nu^{[r_i m_\nu]} \subset A$ for all i and ν. By a remark in section 1.4 it follows that there is a sequence $n_\nu^{(1)}$ such that

$$A_{n_\nu^{(1)}}^{[r_1 m_{n_\nu^{(1)}}]}$$

converges. From this sequence we may select a subsequence $n_\nu^{(2)}$ such that

$$A_{n_\nu^{(2)}}^{[r_2 m_{n_\nu^{(2)}}]}$$

converges, and so on. A diagonal procedure now yields a sequence n_ν with the desired properties.

§ 2. One-parameter semigroups

2.1. Definition: *By a one-parameter semigroup of subsets of a topological group G (for short: one-parameter semigroup in G) is meant a mapping ϕ: $\delta \to A_\delta$ of the non-negative reals into the set of subsets of G, satisfying the conditions:*

1. $A_{\delta_1} A_{\delta_2} = A_{\delta_1 + \delta_2}$.

2. *There exists $\alpha > 0$ such that A_δ is closed if $0 \leqq \delta \leqq \alpha$ and such that the restriction of ϕ to the interval $0 \leqq \delta \leqq \alpha$ is continuous in the Hausdorff topology sense.*

Examples:

1. Let a_δ be a one-parameter subgroup of G, i.e. a continuous mapping of the real interval $-\alpha \leqq \delta \leqq \alpha$ into G, which satisfies $a_{\delta_1} a_{\delta_2} = a_{\delta_1+\delta_2}$. Then $A_\delta = \{a_\delta\}$, $B_\delta = \{a_{-\delta}\}$ and $C_\delta = \{a_\lambda \mid 0 \leqq \lambda \leqq \delta\}$ for $0 \leqq \delta \leqq \alpha$ are the restrictions to $0 \leqq \delta \leqq \alpha$ of three one-parameter semigroups in G.

In connection with these examples, we remark that whereas it is common to assume that a one-parameter subgroup is a non-constant mapping, the corresponding assumption is not made in the above definition of one-parameter semigroups in G.

2. Let G be the additive group of a linear space and let K be a closed bounded convex set. Then the mapping ϕ taking δ into δK is a one-parameter semigroup in G.

Proof: (We use additive notation.) It is a well known fact in the theory of convex sets that for $\delta_1\ \delta_2 \geqq 0$ and K convex the distributive law $\delta_1 K + \delta_2 K = (\delta_1 + \delta_2) K$ holds.

The continuity follows from the boundedness of K. Let U be any symmetric neighborhood of 0. Then there is a $\beta(U) > 0$ such that $\delta K \subset U$ for all $\delta \leqq \beta$. Let $\delta_0 \leqq \delta \leqq \delta_0 + \beta(U)$. Thus $\delta K = \delta_0 K + (\delta - \delta_0) K \subset \delta_0 K + U$. It also follows that $\delta_0 K \subset \delta K + U^{-1} = \delta K + U$. Similarly the two inequalities just proved follow if δ lies in the range $\delta_0 \geqq \delta \geqq \delta_0 - \beta(U)$. This establishes continuity.

The necessity of some condition like the boundedness condition is seen from the following counter-example: Let K be the closed convex set in the cartesian xy-plane bounded by the parabola $y^2 = x$. Then δK for $\delta \neq 0$ is bounded by the parabola $y^2 = \delta x$. It is easily verified that this is not a continuous family of sets. In fact, considered as a set of points in the space of all closed subsets of the plane, the family δK is discrete, i.e. all its points are isolated points.

3. Let A be a closed subgroup of G or, more generally, any closed subset of G satisfying $AA = A$. Then the constant mapping $\delta \to A$ for all δ is a one-parameter semigroup in G.

2.2. If A_δ is a one-parameter semigroup we have $A_0 A_0 = A_{0+0} = A_0$. Any set A satisfying $AA \subset A$ is a subsemigroup of G. If moreover A contains the identity then $AA = A$. Is it always true that, conversely, $AA = A$ implies $e \in A$? The answer is no, even if A is supposed to be closed as is seen from the example: G is the group of the rational numbers under addition and with discrete topology. A is the set of all positive rational numbers. — If G is a euclidean space it seems likely that the answer is affirmative for closed sets A but I have not succeeded in proving this. This question is important for the theory of diophantine approximations.

The following remark concerns the case in which A is compact and non-empty and the group G arbitrary. In this case we may even weaken the assumption $AA = A$ to $AA \subset A$ and still obtain not only the result $e \in A$ but even $A^{-1} \subset A$ which shows that A is a subgroup of G.

Proof: Let $a \in A$. Consider the set $S = \{a^n \mid n = 1, 2 \ldots\}$. We have $aS \subset S \subset A$. Thus $a\bar{S} \subset \bar{S} \subset A$. Suppose $e \notin \bar{S}$. Then there is an open neighborhood U of e disjoint from $\bar{S}$. Obviously $\bar{S}$ is contained in the union of the sets $a^n U$. But $\bar{S}$ is compact since it is closed and $\subset A$. Thus $\bar{S}$ is covered by a finite number of sets $a^n U$. Let m be the largest of the exponents n employed, and let $l > m$ and $k \leqq m$. Then $a^l \notin a^k U$ since otherwise $a^{l-k} \in U$ contrary to the assumption. But, therefore, a^l is in no one of the sets covering $\bar{S}$ and so not in $\bar{S}$. Contradiction. Thus $e \in \bar{S}$. Hence $\bar{S}$ is the closure of $T = \{e, a, a^2 \ldots\}$. But $aT = S$. Thus $a\bar{S} = \bar{S}$ or $\bar{S} = a^{-1}\bar{S}$. Since $e \in \bar{S}$ we obtain $a^{-1} e \in \bar{S}$. We have shown not only that A contains e but also that with any $a \in A$ we have $a^{-1} \in A$, which proves that A is a subgroup of G.

This shows that in general there are restrictions on the sets which are possible to use as A_0 for some one-parameter semigroup. The problem of characterizing these sets is difficult even in the euclidean case. We shall therefore concentrate on the simplest case, namely the one in which $A_0 = \{e\}$.

If ϕ is a one-parameter semigroup in a group G and if A is a subset of G satisfying $AA = A$ and commuting with all the sets $\phi(\delta)$, then the mapping $\psi : \delta \to A\phi(\delta)$ is also a one-parameter semigroup in G provided the sets $\psi(\delta)$ are closed and the mapping ψ is continuous for sufficiently small δ. We have $\psi(0) = A\phi(0)$. Conversely, if a given semigroup ψ can be expressed in this way and if $\phi(0) = \{e\}$, we can thus reduce the study of ψ to the study of the simpler case of ϕ. A theorem stating sufficient conditions under which such a reduction is possible is given in section 2.6.

Is this reduction possible for any given one-parameter semigroup? If this were the case then every problem on the structure of one-parameter semigroups ϕ could be transferred to the case when $\phi(0) = \{e\}$. However, this is not so. We shall give two examples, in the first of which the above reduction is possible, whereas it is impossible in the second one.

Example 1. Let in the cartesian xy-plane be given the convex set K defined by $0 \leqq y \leqq 1$, $x \geqq 0$. Put $\psi(\delta) = \delta K$ for $\delta > 0$ and $\psi(0)$ = the non-negative x-axis. Then ψ is a one-parameter semigroup. Put $\phi(\delta) = \delta L$, where L is the segment $0 \leqq y \leqq 1$ on the y-axis. Then $\psi(\delta) = \psi(0) + \phi(\delta)$ (additive notation) and $\phi(0) = \{0\}$.

Example 2. Let K denote the convex set in the xy-plane bounded by the positive x-axis and the graph of the function $y = \dfrac{x}{1+x}$ for $x \geqq 0$. Put $\varphi(\delta) = \delta K$ for $\delta > 0$ and $\psi(0)$ = the non-negative x-axis.

Suppose now that it is possible to find a one-parameter semigroup ϕ with $\phi(0) = 0$ such that $\psi(\delta) = \phi(\delta) + \psi(0)$. We use a fact which will be proved in § 3, namely that $\phi(0) = \{0\}$ implies that $\phi(\delta)$ is a bounded set for every δ, in particular for $\delta = 1$. Therefore there would exist a number γ so that $\phi(1)$ is contained in the strip $0 \leqq x \leqq \gamma$. From the assumption made it follows that $\psi(1) = \phi(1) + \psi(0)$. But $\psi(0)$ contains 0. Thus $\phi(1) \subset \psi(1)$ which shows that $\phi(1)$ is contained in the rectangle, R,:

$$0 \leqq x \leqq \gamma, \quad 0 \leqq y \leqq \frac{\gamma}{1+\gamma}.$$

Hence

$$\psi(1) = \phi(1) + \psi(0) \subset R + \psi(0).$$

But $R + \psi(0)$ is the half strip: $x \geqq 0$, $0 \leqq y \leqq \dfrac{\gamma}{1+\gamma}$. Now this is a contradiction, since $\psi(1)$ contains points whose y-coordinates are arbitrarily close to 1 and $\dfrac{\gamma}{1+\gamma}$ is less than 1.

2.3 Theorem: *If a one-parameter semigroup, $\phi : \delta \to A_\delta$ is a non-constant mapping, then there is a $\beta > 0$ such that the restriction of ϕ to the interval $0 \leqq \delta \leqq \beta$ is a homeomorphism into the space K of closed subsets of G.*

Proof: Let I_λ denote the interval $0 \leqq \delta \leqq \lambda$ and let α be the number mentioned in definition 2.1. We observe that the restriction of ϕ to any interval I_λ with $\lambda > 0$ is a non-constant mapping. Suppose namely that $A_\delta = A =$ const.

for $\delta \varepsilon I_\lambda$. Then $A A = A$ and $A_{2\delta} = A_\delta A_\delta = A A = A$ so that ϕ is constant also on $I_{2\lambda}$. Iterating this we see that ϕ would be constant everywhere, contrary to hypothesis.

We now define a function $\varphi(\delta)$ of the real variable δ, taking real values or the value ∞. If there is no $\varepsilon > 0$ with $A_{\delta+\varepsilon} = A_\delta$, then $\varphi(\delta) = \infty$. In other cases we let $\varphi(\delta)$ be the infimum of those $\varepsilon > 0$ for which $A_{\delta+\varepsilon} = A_\delta$. This function is monotonic non-increasing. Namely, let $\delta_1 \geqq \delta$. If $\varphi(\delta) = \infty$ there is nothing to prove. If $A_{\delta+\varepsilon} = A_\delta$, then $A_{\delta_1+\varepsilon} = A_{\delta_1-\delta} A_{\delta+\varepsilon} = A_{\delta_1-\delta} A_\delta = A_{\delta_1}$, so that $\varphi(\delta_1) \leqq \varphi(\delta)$.

Our next step will be to show that either there exists a $\gamma > 0$ such that $0 < \delta \leqq \gamma$ implies $\delta + \varphi(\delta) > \gamma$, or $\varphi(\delta) = 0$ for all $\delta > 0$. Suppose that the first alternative does not hold. Then given any $\gamma > 0$, there exists a δ in the interval $0 < \delta \leqq \gamma$ for which $\delta + \varphi(\delta) \leqq \gamma$. Now let $\delta_1 > 0$ be given. Thus there exists a δ_2 in the interval $0 < \delta_2 \leqq \delta_1$ for which $\delta_2 + \varphi(\delta_2) \leqq \delta_1$. Iterating this procedure we construct a sequence δ_ν of real numbers satisfying:

$$0 < \delta_{\nu+1} \leqq \delta_\nu \text{ and } \delta_{\nu+1} + \varphi(\delta_{\nu+1}) \leqq \delta_\nu .$$

Since δ_ν is monotonic, non-increasing and positive it has a limit. Thus $\delta_\nu - \delta_{\nu+1} \to 0$. But $\varphi(\delta_{\nu+1}) \leqq \delta_\nu - \delta_{\nu+1}$. On the other hand, by the monotonicity of φ, we have $\varphi(\delta_1) \leqq \varphi(\delta_{\nu+1})$. Since, by definition, φ is non-negative we obtain:

$$0 \leqq \varphi(\delta_1) \leqq \varphi(\delta_{\nu+1}) \leqq \delta_\nu - \delta_{\nu+1} \to 0.$$

Thus

$$\varphi(\delta_1) = 0.$$

Let $A_{\delta+\varepsilon} = A_\delta$ with $\varepsilon > 0$. Then it is easy to see that $A_{\delta+k\varepsilon} = A_\delta$ for $k = 0, 1, 2, 3 \ldots$. Suppose now $\varphi(\delta) = 0$. Then there exist $\varepsilon_n > 0$ with $\varepsilon_n \to 0$ and $A_{\delta+\varepsilon_n} = A_\delta$. Thus $A_{\delta+k\varepsilon_n} = A_\delta$. But the numbers $k\varepsilon_n$ are dense in the non-negative real axis. Let $C(\delta)$ denote the set of those λ for which $A_\lambda = A_\delta$. Since the restriction of ϕ to I_α is continuous, the set $I_\alpha \cap C(\delta)$ is closed. We obtain the result: If $\delta \leqq \alpha$ then ϕ is constant on the interval with endpoints δ and α. This result shows that the alternative: $\varphi(\delta) = 0$ for all $\delta > 0$ is impossible for then ϕ would be constant on I_α contrary to hypothesis.

There remains only the alternative that there exists a γ such that $0 < \delta \leqq \gamma$ implies $\delta + \varphi(\delta) > \gamma$ which shows that it is possible to have both $\delta_1 < \delta_2 \leqq \gamma$ and $A_{\delta_1} = A_{\delta_2}$ only if $\delta_1 = 0$. It is clear that in this case δ_2 has to be equal to γ ($\varphi(\delta)$ is non-increasing). Thus ϕ is certainly one-to-one on every I_{γ_1} with $\gamma_1 < \gamma$.

Therefore choose $\beta < \min(\alpha, \gamma)$. Then the restriction of ϕ to I_β is one-to-one and continuous. Observing that I_β is compact and using a remark in section 1.4, we obtain the desired result.

2.4. Let $\psi: \delta \to A_\delta$ be a continuous mapping of some interval $0 \leqq \delta \leqq \alpha$ with $\alpha > 0$ into the set K of closed subsets of the topological group G. Suppose also that $A_{\delta_1} A_{\delta_2} = A_{\delta_1+\delta_2}$ for $0 \leqq \delta_1$, $0 \leqq \delta_2$ and $\delta_1 + \delta_2 \leqq \alpha$. Then ψ can be extended to a one-parameter semigroup ϕ in G.

Proof: If δ is any non-negative real number put $\phi(\delta) = (A_{\delta/n})^n$ where n is any natural number satisfying $\frac{\delta}{n} \leqq \alpha$. It is necessary to justify this definition by proving that if n_1 and n_2 are two different numbers satisfying this condition then

$$(A_{\delta/n_1})^{n_1} = (A_{\delta/n_2})^{n_2}$$

but this is quite trivial since both sets are equal to

$$(A_{\delta/n_1 n_2})^{n_1 n_2}.$$

(For example:

$$(A_{\delta/n_1 n_2})^{n_1 n_2} = [(A_{\delta/n_1 n_2})^{n_1}]^{n_2} = (A_{\delta/n_2})^{n_2}.)$$

Further it is clear that $\phi(\delta_1 + \delta_2) = \phi(\delta_1)\,\phi(\delta_2)$ since

$$\phi(\delta_1 + \delta_2) = \left(A_{\frac{\delta_1+\delta_2}{n}}\right)^n = (A_{\delta_1/n}\, A_{\delta_2/n})^n = (A_{\delta_1/n})^n\,(A_{\delta_2/n})^n = \phi(\delta_1)\,\phi(\delta_2).$$

$$\left(\text{Observe that if } \frac{\delta_1+\delta_2}{n} \leqq \alpha \text{ then } \frac{\delta_1}{n} \leqq \alpha \text{ and } \frac{\delta_2}{n} \leqq \alpha.\right)$$

This completes the proof.

This proposition shows that a one-parameter semigroup in G is completely determined by its behaviour in an arbitrarily small neighborhood of zero.

2.5. Let L be a given set. If there are two sets M and N with $L = MN$, we shall call M and N (left- and right-)factors of L and the above equality a factorization of L. If $L = MN$ is a factorization of L, then to every $l \varepsilon L$ there can be found an $m \varepsilon M$ and an $n \varepsilon N$ with $l = mn$. If m and n are uniquely determined by l we say that the factorization is a decomposition of L.

If $L = MN$ is a decomposition, then there is an obvious natural one-to-one correspondence between L and the set $M \times N$, namely the correspondence defined by $mn \longleftrightarrow (m, n)$.

The next theorem shows that under certain circumstances, the study of the structure of a one-parameter semigroup may be reduced to the study of semigroups $\delta \to A_\delta$ where $A_0 = \{e\}$. A detailed study of such semigroups in euclidean space and in Lie groups will be carried out in § 3 and § 4 respectively.

2.6. Theorem: *Let $\phi : \delta \to A_\delta$ be a one-parameter semigroup in a topological group G. Suppose that A_0 is a discrete subgroup of G and that to every neighborhood U of the identity there exists a neighborhood V, such that for all $a \varepsilon A_0$ the inequality $aVa^{-1} \subset U$ holds. Then there exists a one-parameter semigroup $\psi : \delta \to B_\delta$, in G with $B_0 = \{e\}$ and such that $A_\delta = A_0 B_\delta = B_\delta A_0$ for all δ. Moreover any element in A_0 commutes with every set B_δ, and there exists a $\gamma > 0$ such that if $\delta \leqq \gamma$ the factorization $A_\delta = A_0 B_\delta$ is a decomposition.*

Proof: Since A_0 is discrete there is a neighborhood of e which contains no other elements of A_0 than e. This neighborhood contains the square of another neighborhood U of e with the properties: U is closed and $U^{-1} = U$. It follows that if $x \neq y$ but both are εA_0, then xU and yU are disjoint and also Ux and Uy are disjoint.

Since ϕ is continuous at zero, there exists a $\gamma > 0$ such that for all $\delta \leqq \gamma$ we have $A_\delta \subset UA_0$. Thus A_δ (for $\delta \leqq \gamma$) is contained in the union of all sets of the type Ux where $x \varepsilon A_0$. Since these sets are pairwise disjoint, the set

A_δ is split up into parts of the form $Ux \cap A_\delta$. We see that these parts are right translates of one single set B_δ, defined (for $\delta \leqq \gamma$) by $B_\delta = U \cap A_\delta$. We have indeed $B_\delta x = Ux \cap A_\delta x$, but since A_0 is a group, $A_\delta x = A_\delta$. The sets B_δ are so far defined only for $\delta \leqq \gamma$. We shall extend the definition to all non-negative values of δ and show that the mapping $\delta \to B_\delta$ is a semigroup satisfying the requirements of the theorem. First we verify that B_δ satisfies the hypothesis of proposition 2.4.

Since U is closed and A_δ is closed, their intersection B_δ is closed. Also the continuity of the mapping $\delta \to B_\delta$ for $0 \leqq \delta < \gamma$ is easy to verify. It remains to prove that for sufficiently small δ_i, we have $B_{\delta_1} B_{\delta_2} = B_{\delta_1+\delta_2}$. Let U_1 be a neighborhood of e with $U_1^2 \subset U$. Since $B_0 = \{e\}$ and the mapping $\delta \to B_\delta$ is continuous at zero there exists a number $\gamma_1 > 0$ such that $B_\delta \subset U_1$ for all $\delta \leqq \gamma_1$. Let $\delta_1 \leqq \gamma_1$ and $\delta_2 \leqq \gamma_1$. Then $B_{\delta_1} \cdot B_{\delta_2} \subset U_1^2 \subset U$. On the other hand $B_{\delta_1} \cdot B_{\delta_2} \subset A_{\delta_1} \cdot A_{\delta_2} = A_{\delta_1+\delta_2}$. Thus $B_{\delta_1} \cdot B_{\delta_2} \subset B_{\delta_1+\delta_2}$ if $\delta_i \leqq \gamma_1$.

The reverse inequality is more difficult. We start by proving that any element of A_0 commutes with every set B_δ. Let V be the neighborhood determined by U according to the hypothesis of the theorem. Since $\delta \to B_\delta$ is continuous at zero there is a number $\gamma_2 > 0$ such that $B_\delta \subset V$ for all $\delta \leqq \gamma_2$. Now let $a \,\varepsilon\, A_0$ and $\delta \leqq \gamma_2$. Then

$$a B_\delta a^{-1} \subset A_0 B_\delta A_0 \subset A_0 A_\delta A_0 = A_\delta .$$

Further

$$a B_\delta a^{-1} \subset a V a^{-1} \subset U.$$

Thus

$$a B_\delta a^{-1} \subset B_\delta .$$

The same argument applied to a^{-1} instead of a gives the reverse inequality and we obtain the desired result $a B_\delta a^{-1} = B_\delta$ (proved for $\delta \leqq \gamma_2$).

Now let $x \,\varepsilon\, B_{\delta_1+\delta_2}$ where $\delta_i \leqq \min\left(\frac{\gamma}{2}, \gamma_1, \gamma_2\right)$. Thus $x \,\varepsilon\, A_{\delta_1+\delta_2} = A_{\delta_1} A_{\delta_2}$. Therefore there exist $y_1 \,\varepsilon\, A_{\delta_1}$ and $y_2 \,\varepsilon\, A_{\delta_2}$ with $x = y_1 y_2$. Since $\delta_1 < \gamma$ there is one $a_1 \,\varepsilon\, A_0$ such that $y_1 \,\varepsilon\, B_{\delta_1} a_1$ and similarly for y_2. Thus $x \,\varepsilon\, B_{\delta_1} a_1 B_{\delta_2} a_2$. But elements of A_0 commute with the sets B_δ if $\delta \leqq \gamma_2$ which means that $x \,\varepsilon\, B_{\delta_1} B_{\delta_2} a_1 a_2 \subset U_1^2 a_1 a_2 \subset U a_1 a_2$. On the other hand $x \,\varepsilon\, B_{\delta_1+\delta_2}$ where $\delta_1 + \delta_2 \leqq \gamma$ so that $x \,\varepsilon\, U$, which shows that $U a_1 a_2$ and Ue are not disjoint and so $a_1 a_2 = e$. Thus $x \,\varepsilon\, B_{\delta_1} B_{\delta_2}$ and this ends the proof of the relation $B_{\delta_1} B_{\delta_2} = B_{\delta_1+\delta_2}$ $\left(\text{proved for } \delta_i \leqq \min\left(\frac{\gamma}{2}, \gamma_1, \gamma_2\right)\right)$.

By the use of proposition 2.4 we are now able to extend the mapping $\delta \to B_\delta$ to the entire non-negative real axis. Only a few details remain to be proved.

We have seen that for $\delta \leqq \gamma$ the set A_δ is the union of mutually disjoint sets $B_\delta x$ where x runs through A_0. This means that given $a \,\varepsilon\, A_\delta$ there is exactly one $x \,\varepsilon\, A_0$ with $a \,\varepsilon\, B_\delta x$. If follows that $A_\delta = B_\delta A_0$ and that this is a decomposition of A_δ (for $\delta \leqq \gamma$).

Next we verify that $a \,\varepsilon\, A_0$ implies $a B_\delta = B_\delta a$ for arbitrary δ. If n is sufficiently large, we know that $a B_{\delta/n} = B_{\delta/n} a$. Thus

$$a\,(B_{\delta/n})^n = B_{\delta/n}\cdot a\,(B_{\delta/n})^{n-1} = \cdots = (B_{\delta/n})^n\,a.$$

We observe finally that this implies $B_\delta A_0 = A_0 B_\delta$ and that we can extend the relation $A_\delta = B_\delta A_0$ to arbitrary δ. This completes the proof.

2.7. Let $\phi:\delta\to A'_\delta$ be a one-parameter semigroup in a group G' and f a homomorphism of another group G onto G'. Put $\psi = f^{-1}\phi$, i.e. for every δ let A_δ be the inverse image under f of A'_δ and put $\psi(\delta) = A_\delta$. Then ψ is a one-parameter semigroup in G.

Proof: We denote by K the kernel of f, i.e. the inverse image of $e'\,\varepsilon\,G'$. K is a closed normal subgroup of G. Let M be any subset of G. Then the inverse image of $f(M)$ is equal to $MK = KM$. This shows that if M is the inverse image of some set $M'\subset G'$ then $M = MK$. — Let M and N be the inverse images of the sets M' and N'. Then MN is the inverse image of $M'N'$.

The last remark proves that the relation $A_{\delta_1}A_{\delta_2} = A_{\delta_1+\delta_2}$ holds. Since all A_δ for $\delta\leqq\alpha$ are inverse images of closed sets they are closed sets too. The continuity remains to be proved. Let U be a given neighborhood of $e\,\varepsilon\,G$. Since f is open the set $U' = f(U)$ is a neighborhood of e'. Thus for a given δ_0 there exists $\varepsilon(U) > 0$ such that if $\delta_0 - \varepsilon(U)\leqq\delta\leqq\delta_0+\varepsilon(U)$ then $A'_\delta\subset U'A'_{\delta_0}$ and $A'_{\delta_0}\subset U'A'_\delta$. Taking the inverse images of both members in the two inequalities and using the remarks made above we obtain: $A_\delta\subset UK\cdot A_{\delta_0}$ and $A_{\delta_0}\subset UK\cdot A_\delta$. But $KA_{\delta_0} = A_{\delta_0}$ and $KA_\delta = A_\delta$. Thus $A_\delta\subset UA_{\delta_0}$ and $A_{\delta_0}\subset UA_\delta$ which proves the continuity at δ_0.

2.8. In the paper (**6**) mentioned in section 1.2 Gleason has considered one-parameter semigrops ϕ of compact sets containing e and with $\phi(0) = \{e\}$. He outlines a proof (l.c. Lemma 4) that non-constant semigroups of this type exist in any locally compact group which is not totally disconnected. From this result he deduces the important consequence that there exists an arc in such a group.

Also several other results obtained by Gleason (l.c.) are of interest in the present connection. Thus it follows from one of the lemmas (l.c. Lemma 1) that if ϕ is a one-parameter semigroup in a locally compact group and $\phi(\delta)$ is a compact set containing e for every δ, then $\phi(\delta)$ is connected for every δ.

Gleason's lemma 3 implies our theorem 2.2 in the special case when the semigroup ϕ has the properties mentioned above. Gleason also mentions the problem to which §§ 5 and 6 of the present work are devoted, namely to find those groups in which the topology can be defined by giving a one-parameter semigroup ϕ such that the sets $\phi(\delta)$ for $\delta > 0$ constitute a fundamental system of neighborhoods of the identity. He states a result which is essentially equivalent to theorem 6.4 of the present paper.

It should be pointed out that those of Gleason's results which have been mentioned here concern semigroups of sets which are linearly ordered by inclusion. In our terminology this corresponds to the assumption that $\phi(\delta)$ contains e for every δ. It might also be worth mentioning that the result on connectedness wich follows from Gleason's lemma 1 is true also in the general case (i.e. assuming only $\phi(0) = \{e\}$ and $\phi(\delta)$ compact).

§ 3. One-parameter semigroups in euclidean space.

3.1. The present paragraph is devoted to a study of one-parameter semigroups $\delta \to A_\delta$ in euclidean space. The problem of determining all such semigroups with $A_0 = \{0\}$ is completely solved (Theorem 3.5).

In this paragraph, we do not assume that any metric at all is defined on the space under consideration. It might therefore be more accurate to use one of the terms "finite-dimensional linear space" or "affine space" instead of "euclidean space." Since a euclidean metric (not intrinsically defined) can be imposed on any finite-dimensional linear space, however, we shall not insist on this point, but continue to use the term "euclidean space."

In this paragraph, when the group G under consideration is a linear space under addition, we shall use additive notation and terminology except for one case: for repeated addition of a set to itself multiplicative notation will be used. Thus, for example, $A+A+A$ is denoted by A^3 whereas $3A$ denotes the set homothetic to A with respect to the origin and enlarged three times.

We have $nA \subset A^n$ and, if A is convex, $nA = A^n$.

Proof: Every element of nA is of the form nx, where $x \varepsilon A$. But

$$n x = x + x + \cdots + x \,\varepsilon\, A^n.$$

On the other hand if A is convex, then any element of A^n is of the form $\sum_{\nu=1}^{n} x_\nu$ where $x_\nu \varepsilon A$. But since A is convex, $\frac{1}{n}\sum_{1}^{n} x_\nu \,\varepsilon\, A$. Thus

$$\sum_{1}^{n} x_\nu \,\varepsilon\, nA.$$

Conversely, if A is closed and for some $n = 2, 3, 4 \ldots$ we have $nA = A^n$ then A is convex. (This holds in any linear space.)

Proof: Let x and y be elements of A. Then $mx + (n-m)y$ is εA^n, $(m = 0, 1, 2 \ldots n)$. Since it is also $\varepsilon\, nA$, the points $\frac{m}{n}x + \left(1 - \frac{m}{n}\right) y$ are εA. If $n \geqq 2$, at least one of these points is different from both x and y, and they all lie on the segment joining these two points. The rest of the argument follows familiar lines.

3.2. If A is any set in a linear space, we denote the convex hull of A by the symbol $H(A)$, that is, the intersection of all convex sets containing A. (This definition does not coincide with that of Bonnesen-Fenchel (**3**, p. 5).) We denote the set of all finite subsets of A by $F(A)$, and the set of all those subsets of A which contain at most $d+1$ points by $F_d(A)$. It is easy to see that $H(A)$ is equal to the union of all sets $H(S)$, where S runs through $F(A)$ or in symbols (this holds in any linear space):

$$H(A) = \bigcup_{S \varepsilon F(A)} H(S).$$

Proof: First observe that the right member is a convex set. To see this let a and b be $\varepsilon \bigcup H(S)$. Then $a \varepsilon$ some $H(S_a)$ and $b \varepsilon H(S_b)$. Thus $H(S_a \cup S_b)$ contains both a and b and therefore contains the segment joining them. This shows that the right member is convex and since it contains A we see that $H(A) \subset \bigcup H(S)$. Secondly, observe that $S \subset A$ implies $H(S) \subset H(A)$ and therefore $\bigcup H(S) \subset H(A)$.

It is well known (Bonnesen–Fenchel (**3**, p. 9)) that if the linear space is of finite dimension d, then $H(S) = \bigcup H(T)$ where S is any compact set (in particular for S finite) and T runs through all sets $\varepsilon F_d(S)$. Together with the previous result, this gives the formula (valid in all linear spaces of dimension d):

$$H(A) = \bigcup_{S \varepsilon F_d(A)} H(S).$$

Besides these more or less well-known facts about the convex hull, we shall need the following facts from the theory of convex sets: The sum of two convex sets is convex, the intersection of any number of convex sets is convex, the union of an increasing sequence of convex sets is convex and λ, $\mu \geqq 0$, A convex, imply $\lambda A + \mu A = (\lambda + \mu) A$.

3.3. After the above preliminaries, we return to the problem of characterizing one-parameter semigroups in euclidean space. Lemma 1 below is the basic result which makes such a characterization possible. This lemma, which has interesting consequences other than those we are presently interested in, contains the solution of the following problem. For a given set A in a euclidean space, is it possible to find another set $B(A)$ so that $A + B(A)$ is convex? Stated in this vague form, the problem has a trivial solution, we can take B equal to the entire space. This shows that some supplementary requirement is necessary to make the problem interesting; we may, for example, require that B be bounded if A is bounded or that B be small in some sense if A is small. Lemma 2 solves the problem in both of these forms.

Lemma 1. *Let A be any set of points in a d-dimensional euclidean space, and let $\alpha \geqq d$. Then $A + \alpha H(A) = (\alpha + 1) H(A)$.*

Proof: We observe that if the equality in question holds for a certain set, then it holds for all translates of that set:

$$A + \alpha H(A) = (\alpha + 1) H(A)$$

implies

$$A + x + \alpha H(A + x) = A + x + \alpha H(A) + \alpha x =$$

$$= (\alpha + 1) H(A) + (\alpha + 1) x = (\alpha + 1) H(A + x).$$

Our first step is to prove the result for a set S containing at most $d + 1$ points. By the above remark, it is enough to prove it under the assumption that one of these points is the origin. Therefore let $S = \{q_0\, q_1 \ldots q_d\}$, where $q_0 = 0$ and the q_ν are not necessarily different. Then $H(S)$ consists of all points which can be written in the form $\sum_{\nu=1}^{d} \lambda_\nu q_\nu$, where $\lambda_\nu \geqq 0$ and $\sum_{\nu=1}^{d} \lambda_\nu \leqq 1$. The set $S+\alpha H(S)$ consists of all points x for which there exist λ_ν satisfying the above conditions and an integer k such that

$$x = q_k + \alpha \sum_{\nu=1}^{d} \lambda_\nu q_\nu . \tag{1}$$

Similarly $x \varepsilon (\alpha+1) H(S)$ implies that there exist $\mu_\nu \geqq 0$ with $\sum_{\nu=1}^{d} \mu_\nu \leqq 1$ and

$$x = (\alpha+1) \sum_{\nu=1}^{d} \mu_\nu q_\nu . \tag{2}$$

Suppose now that $x \varepsilon (\alpha+1) H(S)$, *i.e.*, that x can be expressed in the form (2). There are two cases. Suppose first that $\sum \mu_\nu \leqq \frac{\alpha}{\alpha+1}$. Then $x = \alpha \sum \frac{\alpha+1}{\alpha} \mu_\nu q_\nu$ expresses x in the form (1) with $k=0$ and $\lambda_\nu = \frac{\alpha+1}{\alpha} \mu_\nu$. Suppose then that $\sum \mu_\nu > \frac{\alpha}{\alpha+1}$. This implies $\sum_{\nu=1}^{d} \mu_\nu > \frac{d}{\alpha+1}$. Thus for one value at least of the index ν we must have $\mu_\nu > \frac{1}{\alpha+1}$. Denote that value by k. Then

$$x = (\alpha+1) \sum_{\nu=1}^{d} \mu_\nu q_\nu = q_k + \alpha \sum_{\nu=1}^{d} \lambda_\nu q_\nu ,$$

where $\lambda_k = \frac{(\alpha+1)\mu_k - 1}{\alpha}$ and $\lambda_\nu = \frac{\alpha+1}{\alpha} \mu_\nu$ for $\nu \neq k$. Then $\lambda_\nu \geqq 0$ for all ν and $\sum_{\nu=1}^{d} \lambda_\nu = \frac{\alpha+1}{\alpha} \sum_{\nu=1}^{d} \mu_\nu - \frac{1}{\alpha} \leqq \frac{\alpha+1}{\alpha} - \frac{1}{\alpha} = 1$. We have thus shown that if x can be written in the form (2), then it can be written in the form (1), which means that $(\alpha+1) H(S) \subset S + \alpha H(S)$. Conversely, we clearly have $S + \alpha H(S) \subset H(S) + \alpha H(S) = (\alpha+1) H(S)$. Thus the lemma is proved for S.

Now let A be any set of points of the d-dimensional euclidean space. Then if $S \varepsilon F_d(A)$, we have $A \supset S$ and hence $A + \alpha H(A) \supset S + \alpha H(S) = (\alpha+1) H(S)$. Thus $A + \alpha H(A) \supset \bigcup_{S \varepsilon F_d(A)} (\alpha+1) H(S) = (\alpha+1) H(A)$. Conversely, we have $A + \alpha \cdot H(A) \subset H(A) + \alpha H(A) = (\alpha+1) H(A)$, which proves the lemma.

The following slight generalisation will also be needed.

Lemma 2. *Let A be any set of points in d-dimensional euclidean space, and let $\alpha \geqq d$. Then $A^n + \alpha H(A) = (\alpha+n) H(A)$ $(n = 1, 2, 3 \ldots)$.*

Proof: We apply finite induction to lemma 1:

$$A^{n+1} + \alpha H(A) = A^n + A + \alpha H(A) = A^n + (\alpha+1) H(A) = (n+\alpha+1) H(A).$$

This shows that not only does every bounded set A admit a bounded set B such that $A+B$ is convex but the same B will do for all powers of A.

3.4. Theorem: *Let A and A_ν, $\nu = 1, 2, 3 \ldots$, be closed subsets of a euclidean space and suppose that they satisfy the relations* $\lim_{\nu\to\infty} A_\nu^{n_\nu} = A$ *and* $\lim_{\nu\to\infty} A_\nu = \{0\}$, *where n_ν are positive integers. The limits are taken in the Hausdorff metric for the set of closed subsets of the space. Then A is a convex set.*

Proof: Let d be the dimension of the space. Let U be a convex symmetric neighborhood of the origin. For all sufficiently large ν we have $A \subset A_\nu^{n_\nu} + U$ and $A_\nu^{n_\nu} \subset A + U$. Since $A_\nu \to \{0\}$, we have also $dH(A_\nu) \to \{0\}$, which implies that the set $dH(A_\nu)$ is contained in U for sufficiently large ν. Let a_ν be an element of $dH(A_\nu)$. Since the set $dH(A_\nu) - a_\nu$ contains 0, the set $A + dH(A_\nu) - a_\nu$ contains A. Suppose now that $N(U)$ is a number so large that $A \subset A_\nu^{n_\nu} + U$, $A_\nu^{n_\nu} \subset A + U$ and $dH(A_\nu) \subset U$ for all $\nu \geqq N(U)$. Then, for $\nu \geqq N(U)$, we have

$$A \subset A + dH(A_\nu) - a_\nu \subset A_\nu^{n_\nu} + dH(A_\nu) + U - a_\nu \subset A_\nu^{n_\nu} + U + U + U \subset A + U^4.$$

Write $C_\nu(U)$ for the set $A_\nu^{n_\nu} + dH(A_\nu) + U - a_\nu$. By lemma 2 of the preceding section, $C_\nu(U)$ is convex.

Since $A \subset C_\nu(U) \subset A + U^4$ for all $\nu \geqq N(U)$, we have

$$A \subset C(U) \subset A + U^4,$$

where

$$C(U) = \bigcap_{\nu \geqq N(U)} C_\nu(U).$$

Being the intersection of convex sets, the set $C(U)$ is convex. Now let U run through a fundamental system of neighborhoods of 0. Then U^4 also runs through such a system. Let C be the intersection of the corresponding sets $C(U)$. Thus $A \subset C \subset \bigcap (A + U^4) = \bar{A}$. Since A is closed, we have $A = \bar{A}$ and therefore $A = C$. Since C is defined as the intersection of convex sets, it is itself convex. Thus A is convex.

We remark that the hypothesis of the theorem implies that A is compact. Namely, let U be a compact neighborhood of 0. Then for all sufficiently large ν, the relation $A_\nu \subset U$ holds. Further $A \subset A_\nu^{n_\nu} + U$ for sufficiently large ν. Let μ be a value of ν for which both these inequalities hold. Since A_μ is a closed subset of the compact set U, the set A_μ is compact. Thus $A_\mu^{n_\mu} + U$ is compact and contains A as a closed subset, which shows that A is compact.

We remark also that it follows from the theorem that if A is any closed set to which there exist arbitrarily small closed sets A_ν each having a power $A_\nu^{n_\nu}$ equal to A, then A is a convex set. This gives rise to the following suggestive formulation of a characterization of compact convex sets: We say that the point set A has a square root if there exists a set B with $B^2 = A$. Then a necessary and sufficient condition that a compact set A be convex is that it have an infinite sequence of successive square roots, *i.e.*, that there exist sets A_ν with $A_0 = A$ and $A_{\nu+1}^2 = A_\nu$, $\nu = 0, 1, 2 \ldots$. We omit the proof of this statement.

3.5. The following theorem contains the characterization of one-parameter semigroups ϕ with $\phi(0) = \{0\}$ in euclidean space.

Theorem: *To any one-parameter semigroup ϕ with $\phi(0)=\{0\}$ in euclidean space, there exists a compact convex set A such that $\phi(\delta)=\delta A$. Conversely, if A is a compact convex set in euclidean space, then the mapping ϕ: $\delta\to\delta A$ is a one-parameter semigroup with $\phi(0)=\{0\}$.*

Proof: Let ϕ be given. By the definition of one-parameter semigroups, there exists a real number $\beta>0$ such that $\phi(\delta)$ is closed for $0\leqq\delta\leqq\beta$. Observe that $\phi(\beta)=\left[\phi\left(\frac{\beta}{\nu}\right)\right]^{\nu}$ and that, because of continuity,

$$\phi\left(\frac{\beta}{\nu}\right)\to\{0\}\text{ as }\nu\to\infty.$$

Apply theorem 3.4. This shows that $\phi(\beta)$ is convex, and the remark following the same theorem shows that $\phi(\beta)$ is compact. Since the same argument can be used for any non-negative number $\delta\leqq\beta$, we see that $\phi(\delta)$ is convex and compact for all $\delta\leqq\beta$. By the extension procedure of section 2.4, the same result is shown to hold for all $\delta\geqq 0$. Put $\phi(\delta)=A_\delta$. Thus $A_1=(A_{\frac{1}{n}})^n=n\,A_{\frac{1}{n}}$ (the last equality sign since $A_{\frac{1}{n}}$ is convex). Further

$$m\,A_1=(A_1)^m=n\,(A_{\frac{1}{n}})^m=n\,A_{\frac{m}{n}}\text{ or }A_{\frac{m}{n}}=\frac{m}{n}A_1.$$

Putting $A_1=A$, we see that $A_\delta=\delta A$ for rational δ. The general result follows by continuity. This proves the first part of the theorem.

The second part is easy. (Cf. section 2.1 example 2. The result $\phi(0)=\{0\}$ follows from the fact that A, being compact, is bounded.)

§ 4. One-parameter semigroups in Lie groups

4.1. The results of the preceding paragraph make it possible to characterize those one-parameter semigroups in an arbitrary Lie group for which $\phi(0)=\{e\}$. It will turn out that these semigroups in a certain sense (see definition 4.12) are generated by infinitesimal, compact, convex sets and that, conversely, any compact, convex infinitesimal set generates a one-parameter semigroup ϕ with $\phi(0)=\{e\}$.

We shall need only the following simple fact from the theory of Lie groups: Let there be given a Lie group G. Then there exists a euclidean space g, a neighborhood U of the origin in g and a mapping f of U into G so that

1. f is a homeomorphism of U onto a neighborhood of the identity in G.

2. There exists a neighborhood V of the origin in g such that $[f(V)]^2\subset f(U)$ and such that if $x\,\varepsilon\,V$ and $y\,\varepsilon\,V$ then $f(x)\,f(y)=f(x+y+r(x,y))$ is a continuous mapping of $V\times V$ into g satisfying

$$\|r(x,y)\|\leqq k\|x\|\cdot\|y\|.$$

Here k is a real number and $\|z\|$ denotes the euclidean distance from z to the origin of g. Moreover, V may be assumed to be the closed euclidean sphere of radius one.

Proof: We choose a sufficiently many times differentiable coordinate system (see PONTRJAGIN **11**, p. 181) for a neighborhood of $e \varepsilon G$. Thus to any point in this neighborhood there is assigned an n-tuple of real numbers where n is the dimension of G. We let g be the n-dimensional linear space consisting of all n-tuples of real numbers, U the neighborhood of the origin in g consisting of those n-tuples whose elements are the n coordinates for a point in the above-mentioned neighborhood of $e \varepsilon G$, and we let f be the mapping of U into G taking any n-tuple into the corresponding point of G. Then f is a homeomorphism on U. Let U' be a neighborhood of 0 in g such that $[f(U')]^2 \subset f(U)$. Thus if $x, y \varepsilon U'$, we have $f(x) f(y) \varepsilon f(U)$ so that $f^{-1}(f(x) f(y))$ is defined. From the fact that the coordinate system is differentiable and that $f^{-1}(f(x) f(0)) = x$ and $f^{-1}(f(0) f(y)) = y$, it follows that

$$f^{-1}(f(x) f(y)) = x + y + r(x, y),$$

where $r(x, y)$ is defined on $U' \times U'$ and takes values from g. It follows also that the coordinates $r_i(x, y)$ $(i = 1, 2, \ldots n)$ of $r(x, y)$ are sufficiently many times differentiable. Furthermore, $r_i(x, 0) = r_i(0, y) = 0$. Now let V be a compact neighborhood of 0 with $V \subset U'$ bounded by a second-degree hypersurface. We may then make g a euclidean space by introducing a euclidean metric in which V is the closed unit sphere. We denote the distance from $z \varepsilon g$ to $0 \varepsilon g$ by $\|z\|$.

Now let x and y be two elements of V. Put $s = \|x\|$ and $t = \|y\|$, and let $x_0 = \frac{x}{s}$, $y_0 = \frac{y}{t}$. Thus x_0 and y_0 lie on the boundary of V. Let $\varrho(x, y)$ be any twice continuously differentiable real valued function defined on $V \times V$ satisfying $\varrho(x, 0) = \varrho(0, y) = 0$. We have then

$$\varrho(x, y) = \int_0^t \int_0^s \frac{\partial^2}{\partial \sigma \, \partial \tau} (\varrho(\sigma x_0, \tau y_0)) \, d\sigma \, d\tau.$$

Since the integrand is a continuous function of σ, τ, x_0 and y_0 and V is compact, it follows that there exists a constant k greater than the modulus of the integrand for all relevant values of the variables. We obtain therefore

$$|\varrho(x, y)| \leqq k \int_0^t \int_0^s d\sigma \, d\tau = k s t.$$

Applying this result to the functions $r_i(x, y)$, we obtain $|r_i(x, y)| \leqq k_i \|x\| \|y\|$. Put $k = (\sum_{i=1}^{n} k_i^2)^{\frac{1}{2}}$. Thus $\|r(x, y)\| \leqq k \|x\| \|y\|$, which proves the proposition.

4.2. Most of the arguments in the rest of this paragraph are based on the proposition just proved. Although it will never be necessary in order to carry the arguments through to specialize the mapping f, wo shall nevertheless assume that f is the exponential mapping (see CHEVALLEY **5**, p. 116). This assumption will simplify the proof of lemma 4.7. It corresponds to choosing the coordinates as canonical of the first kind (PONTRJAGIN **11**, p. 187). The space g will therefore be the underlying linear space of the Lie algebra of G. We shall denote also the Lie algebra of G by g (but we shall not have to deal with the commutation operation). The reason for choosing f in this special way is that the exponential mapping is intrinsically defined, which gives intrinsic meaning also to the term "generate" defined below (definition 4.12). The choice of the exponential mapping for f is admissible, since it corresponds to the choice of an analytic system of coordinates which is therefore certainly sufficiently many times differentiable, an assumption made in the above proof.

The natural methods to use when dealing with Lie groups are based on the theory of differential equations. For example, it is possible to obtain the one-parameter subgroups of a Lie group as solutions of certain differential equations. Unfortunately, analogous methods for dealing with problems concerning one-parameter semigroups in a Lie group have not yet come to light. Such methods would have to be based on a new type of differential calculus where the dependent variables are not points in a euclidean space, as in classical calculus, but rather sets of points. It is no doubt possible to construct such a theory which would then be applicable to our present problems. Judging from attempts in this direction which I have undertaken, it seems clear that the concept of convexity will occupy a central position in such a theory. The main theorem (4.12) of this paragraph also supports this view. It may be formulated as follows in terms of a calculus for sets: The differential of a one-parameter semigroup is a convex set.

4.3. Put $\|A\| = \sup_{a \in A} \|a\|$ for any $A \subset g$.

Let A and B be subsets of V, or in other words

$$\|A\| \text{ and } \|B\| \text{ both } \leqq 1.$$

Then

$$f^{-1}(f(A)f(B)) \subset A + B + \delta V \tag{1}$$

$$A + B \subset f^{-1}(f(A)f(B)) + \delta V \tag{2}$$

provided $\delta \geqq k \|A\| \cdot \|B\|$.

Proof: Any element of the left member of (1) can be expressed in the form $f^{-1}(f(x)f(y))$, where x and y are εV. According to section 4.1 we have,

$$f^{-1}(f(x)f(y)) = x + y + r(x, y) \,\varepsilon\, A + B + k \|A\| \cdot \|B\| V,$$

which proves (1). Similarly (2) follows from

$$x + y = f^{-1}(f(x)f(y)) - r(x, y)$$

upon observing that $V = -V$.

4.4. Lemma: *There exists a number* $\alpha > 0$ *and a finite number* h *such that if* $K \subset V$, δ *and* $\varepsilon \leqq \alpha$, *and* m, n *are integers with* $m \leqq n$, *then*

$$f^{-1}\left(\left[f\left(\frac{\delta}{n}K\right)\right]^m\right) \subset \left(\frac{\delta}{n}K\right)^m + k\left(\frac{m}{n}\delta\right)^2 V, \tag{1}$$

$$\left(\frac{\delta}{n}K\right)^m \subset f^{-1}\left(\left[f\left(\frac{\delta}{n}K\right)\right]^m\right) + k\left(\frac{m}{n}\delta\right)^2 V, \tag{2}$$

and

$$f^{-1}\left(\left[f\left(\frac{\delta K + \varepsilon V}{n}\right)\right]^m\right) \subset f^{-1}\left(\left[f\left(\frac{\delta K}{n}\right)\right]^m\right) + \gamma V \tag{3}$$

where (in (3)) the number γ *is defined as* $\varepsilon_1 \dfrac{e^{h(\varepsilon_1+\delta_1)} - 1}{h(\varepsilon_1+\delta_1)}$, $\varepsilon_1 = \dfrac{m}{n}\varepsilon$, $\delta_1 = \dfrac{m}{n}\delta$.

Remark: The pair of formulas (1) and (2) expresses the fact that two of the sets involved have a Hausdorff distance of infinitesimal order two in δ as $\delta \to 0$. Similarly (3) can be put together with another formula (4) in a pair expressing the fact that two sets have a Hausdorff distance $\leqq \gamma$. The formula (4): $f^{-1}\left(\left[f\left(\frac{\delta K}{n}\right)\right]^m\right) \subset f^{-1}\left(\left[f\left(\frac{\delta K + \varepsilon V}{n}\right)\right]^m\right)$ is not incorporated in the lemma since it is trivially true (observe that $\delta K \subset \delta K + \varepsilon V$). The exact expression for γ does not matter in applying (3) as we shall do. We need only the fact that $\gamma \to 0$ as $\varepsilon \to 0$ and δ is kept small.

We note also that the symbol $\left(\frac{\delta}{n}K\right)^m$ is meant to denote an m times repeated sum $\frac{\delta}{n}K + \frac{\delta}{n}K + \dots \frac{\delta}{n}K$, according to the convention of section 3.1.

Proof of (1): By formula (1) of section 4.3, we have

$$f(\sigma_1 K_1)\, f(\sigma_2 K_2) \subset f(\sigma_1 K_1 + \sigma_2 K_2 + k\,\sigma_1 \sigma_2 V),$$

provided that $\sigma_1, \sigma_2 \leqq 1$. Using this, we can establish the formula

$$[f(\sigma K)]^m \subset f((\sigma K)^m + k(\sigma m)^2 V), \tag{a}$$

valid if $\sigma m \leqq \min\left(1, \frac{1}{k}\right)$. We observe that if $\delta \leqq \min\left(1, \frac{1}{k}\right)$ then we obtain (1) for $\sigma = \frac{\delta}{n}$. We prove (a) by induction. It is trivially true for $m = 1$. If (a) is true for the value m, then

$$[f(\sigma K)]^{m+1} = [f(\sigma K)]^m f(\sigma K) \subset f((\sigma K)^m + k(\sigma m)^2 V)\, f(\sigma K),$$

and the above mentioned formula gives

$$[f(\sigma K)]^{m+1} \subset f((\sigma K)^m + k(\sigma m)^2 V + \sigma K + k\sigma(\sigma m + k\sigma^2 m^2) V) =$$
$$= f((\sigma K)^{m+1} + k(\sigma^2 n^2 + \sigma(\sigma m + k\sigma^2 m^2)) V).$$

Since $\sigma m \leqq \sigma(m+1) \leqq \frac{1}{k}$ we have $k\sigma m \leqq 1$ which gives

$$\sigma^2 m^2 + \sigma(\sigma m + k\sigma^2 m^2) \leqq \sigma^2 m^2 + 2\sigma^2 m \leqq \sigma^2 (m+1)^2.$$

This proves (a).

Proof of (2): The proof is similar to that of (1). We first show that if $\sigma m \leqq \min\left(1, \frac{1}{k}\right)$ then

$$(\sigma K)^m \subset f^{-1}([f(\sigma K)]^m) + k(\sigma m)^2 V.$$

This is trivial for $m = 1$. Suppose that it is true for m. Then

$$(\sigma K)^{m+1} = (\sigma K)^m + \sigma K \subset f^{-1}([f(\sigma K)]^m) + k(\sigma m)^2 V + \sigma K.$$

Observe that according to formula (a) in the proof of (1), we have

$$\|f^{-1}([f(\sigma k)]^m)\| \leqq \sigma m + k\sigma^2 m^2.$$

Thus formula (2) of section 4.3 gives

$$(\sigma K)^{m+1} \subset f^{-1}([f(\sigma K)]^m f(\sigma K)) + k\sigma(\sigma m + k\sigma^2 m^2) V + k\sigma^2 m^2 V.$$

The proof now ends exactly as the proof of (1).

Proof of (3): Let $\beta > 0$ be a number so small that for $x_1, x_2, y_1, y_2 \in \beta V$, the expressions $f^{-1}(f(x_1) f(x_2))$, $f^{-1}((f(y_1) f(y_2))$, and $f^{-1}(f(x_1 + y_1) f(x_2 + y_2))$ are defined. We put

$$\varrho(x_1, x_2, y_1, y_2) = f^{-1}(f(x_1 + y_1) f(x_2 + y_2)) - f^{-1}(f(x_1) f(x_2)) - f^{-1}(f(y_1) f(y_2)).$$

The function ϱ obviously satisfies the relations

$$\varrho(0, 0, y_1, y_2) = \varrho(x_1, x_2, 0, 0) = \varrho(0, x_2, 0, y_2) = \varrho(x_1, 0, y_1, 0) = 0.$$

By an argument similar to the one used to obtain an estimate of the function r in section 4.1, we prove the existence of a constant k' such that

$$\|\varrho(x_1, x_2, y_1, y_2)\| \leqq k'(\|x_1\|\|y_2\| + \|x_2\|\|y_1\|).$$

We have also seen (section 4.1) that $f^{-1}(f(y_1) f(y_2)) = y_1 + y_2 + r(y_1 y_2)$ where $\|r(y_1, y_2)\| \leqq k\|y_1\|\|y_2\|$. Combining these results, we obtain the following. If $x_1, x_2, y_1, y_2 \leqq \beta$, then

$$f^{-1}(f(x_1+y_1)\,f(x_2+y_2)) = f^{-1}(f(x_1)\,f(x_2)) + y_1 + y_2 + r(y_1, y_2) + \varrho(x_1, x_2, y_1, y_2),$$

where $\|r\| \leqq k\,\|y_1\|\,\|y_2\|$ and $\|\varrho\| \leqq k'(\|x_1\|\,\|y_2\| + \|x_2\|\,\|y_1\|)$.

Now let K' and K'' be subsets of V and let $\sigma', \sigma'', \tau', \tau''$ be numbers $\leqq \beta$. By using the estimates for r and ϱ, we easily verify (cf. section 4.3) that

$$\text{(b)}\qquad f^{-1}(f(\sigma' K' + \tau' V)\,f(\sigma'' K'' + \tau'' V)) \subset f^{-1}(f(\sigma' K')\,f(\sigma'' K'')) + \\ + [\tau' + \tau'' + k\,\tau'\,\tau'' + k'\,(\sigma'\,\tau'' + \sigma''\,\tau')]\,V.$$

We shall now establish the formula

$$\text{(c)}\qquad f^{-1}([f(\sigma K + \tau V)]^m) \subset f^{-1}([f(\sigma K)]^m) + \tau\,\frac{c^m - 1}{c - 1}\,V,$$

where $c = 1 + k\,\tau + 3\,k'\,\sigma$. This can be done if $m\,\sigma$ and $m\,\tau$ are sufficiently small ($\leqq$ a number α to be determined later). We prove this by induction. The statement is obviously true for $m = 1$. Let it be assumed for m. Then

$$f^{-1}([f(\sigma K + \tau V)]^{m+1}) \subset f^{-1}(f(\sigma' B + \tau' V)\,f(\sigma K + \tau V)),$$

where

$$\sigma' = \sigma\,m + k\,\sigma^2\,m^2 \text{ and } \tau' = \tau\,\frac{c^m - 1}{c - 1} \text{ and } \sigma' B = f^{-1}([f(\sigma K)]^m).$$

From formula (a) of the above proof of (1), it follows that $\|\sigma' B\| \leqq \sigma'$ so that $B \subset V$. We note that (a) is valid if $\sigma\,m \leqq \min\left(1, \frac{1}{k}\right)$. Then $\sigma\,m + k\,\sigma^2\,m^2 \leqq \leqq 2\,\sigma\,m$, so that if $\sigma\,m \leqq \frac{1}{2}\,\beta$, we have $\sigma' \leqq \beta$. It is also clear that if $\tau\,m$ is small, then τ' is small, so that there exists a number $\alpha > 0$ such that if $\sigma\,m$ and $\tau\,m$ are both $\leqq \alpha$, then we can apply (b). We find that

$$f^{-1}([f(\sigma K + \tau V)^{m+1})] \subset f^{-1}([f(\sigma K)]^{m+1}) + (\tau + \tau' + k\,\tau\,\tau' + k'\,(\sigma'\,\tau + \sigma\,\tau'))\,V.$$

The coefficient for V is

$$\tau + \tau\,\frac{c^m - 1}{c - 1} + k\,\tau\,\tau\,\frac{c^m - 1}{c - 1} + k'\,\sigma'\,\tau + k'\,\sigma\,\tau\,\frac{c^m - 1}{c - 1}.$$

We observe that $\sigma'\,\tau \leqq 2\,m\,\sigma\,\tau \leqq 2\,\sigma\,\tau\,\frac{c^m - 1}{c - 1}$. This shows that the coefficient for V is not larger than

$$\tau + \tau\,\frac{c^m - 1}{c - 1}\,(1 + k\,\tau + 3\,k'\,\sigma) = \tau\left(1 + \frac{c^m - 1}{c - 1}\,c\right) = \tau\,\frac{c^{m+1} - 1}{c - 1}.$$

Thus (c) is proved.

Putting $h = \max(k, 3\,k')$ and $\sigma = \frac{\delta}{n}$, $\tau = \frac{\varepsilon}{n}$, and observing that $1 + h\,(\sigma + \tau) \leqq \leqq e^{h(\sigma + \tau)}$, we obtain formula (3).

This proves the lemma.

4.5. Lemma: *Let A_ν and B_ν be two sequences of compact sets in g such that $d(A_\nu, B_\nu) \to 0$, where d denotes the Hausdorff distance (see 1.4). Suppose also that there exists a number β so that $A_\nu \subset \beta V$ and $B_\nu \subset \beta V$ for all $\nu = 1, 2, 3 \ldots$. Let m_ν and n_ν be sequences of integers with $m_\nu \leqq n_\nu$ and $n_\nu \to \infty$ as $\nu \to \infty$. Then either the two sequences of sets in G $\left[f\left(\frac{A_\nu}{n_\nu}\right)\right]^{m_\nu}$ and $\left[f\left(\frac{B_\nu}{n_\nu}\right)\right]^{m_\nu}$ both converge to the same limit or they both diverge.*

Proof: Put $d(A_\nu, B_\nu) = \varepsilon_\nu$. Then we have for all ν: $A_\nu \subset B_\nu + \varepsilon_\nu V$ and $B_\nu \subset A_\nu + \varepsilon_\nu V$, and we know by the hypothesis that $\varepsilon_\nu \to 0$.

Suppose that $\left[f\left(\frac{A_\nu}{n_\nu}\right)\right]^{m_\nu}$ converges to a set $C \subset G$. We assume first that $A_\nu \subset \alpha V$ where α is the number in lemma 4.4. We have

$$\left[f\left(\frac{A_\nu}{n_\nu}\right)\right]^{m_\nu} \subset \left[f\left(\frac{B_\nu + \varepsilon_\nu V}{n_\nu}\right)\right]^{m_\nu} \subset \left[f\left(\frac{A_\nu + 2\,\varepsilon_\nu V}{n_\nu}\right)\right]^{m_\nu}.$$

Since the first expression converges to C, (3) of lemma 4.4 shows that the last expression also tends to C. We see therefore that the expression in the middle tends to C.

Now $C_\nu = \left[f\left(\frac{B_\nu}{n_\nu}\right)\right]^{m_\nu} \subset \left[f\left(\frac{B_\nu + \varepsilon_\nu V}{n_\nu}\right)\right]^{m_\nu}$. Since the right side tends to C, the sets C_ν are contained in an arbitrarily small neighborhood of C for sufficiently large ν, in particular in some compact neighborhood of C. Thus every subsequence of the sequence C_ν contains a convergent subsequence. Let C_{p_ν} be a sequence converging to $D \subset G$. Then again by (3) of lemma 4.4, the sequence $\left[f\left(\frac{B_{p_\nu} + \varepsilon_{p_\nu} V}{n_{p_\nu}}\right)\right]^{m_{p_\nu}}$ converges to D. But this is a subsequence of a sequence converging to C. Therefore $D = C$. We see that every convergent subsequence of C_ν converges to C. This means, however that C_ν converges to C.

In order to prove the lemma, we have left only to show that the restriction $A_\nu \subset \alpha V$ is inessential. Choose the integer p so large that $\frac{\beta}{p} \leqq \alpha$. Put $n'_\nu = \left[\frac{n^\nu}{p}\right]$ and $m'_\nu = \left[\frac{m_\nu}{p}\right]$. Let A'_ν and B'_ν be defined by $\frac{1}{n'_\nu} A'_\nu = \frac{1}{n_\nu} A_\nu$ and correspondingly for B'_ν. Since $A_\nu \subset \beta V$ and $n'_\nu p \leqq n_\nu$ we have $A'_\nu = \frac{n'_\nu}{n_\nu} A_\nu \subset \frac{n'_\nu}{n_\nu} \cdot \beta V \subset \frac{\beta}{p} V \subset \alpha V$ and similarly $B'_\nu \subset \alpha V$.

We assume again that $\left[f\left(\frac{1}{n_\nu} A_\nu\right)\right]^{m_\nu}$ converges to a set $C \subset G$. But $\frac{1}{n'_\nu} \cdot A'_\nu = \frac{1}{n_\nu} A_\nu$. Thus $\left[f\left(\frac{1}{n'_\nu} A'_\nu\right)\right]^{m_\nu} \to C$. Now $m_\nu = p\, m'_\nu + \theta_\nu p$, where $0 \leqq \theta_\nu < 1$. Since $\frac{1}{n'_\nu} A'_\nu$ tends to $\{0\}$, it follows that $\left[f\left(\frac{1}{n'_\nu} A'_\nu\right)\right]^{\theta_\nu p}$ tends to $\{e\}$. Hence

$\left[f\left(\frac{1}{n'_\nu}A'_\nu\right)\right]^{m'_\nu p}$ converges to C. From the result already obtained, it is easy to see that the sequence $\left[f\left(\frac{1}{n'_\nu}B'\right)\right]^{m'_\nu p}$ converges to C. Again using the equality $m_\nu = p\,m'_\nu + \theta_\nu\, p$, we conclude that also $\left[f\left(\frac{1}{n'_\nu}B'_\nu\right)\right]^{m_\nu} = \left[f\left(\frac{1}{n_\nu}B_\nu\right)\right]^{m_\nu}$ converges to C, which proves the lemma.

4.6. We shall now develop two procedures of construction which we shall call "procedure I" and "procedure II." Procedure I applied to any given compact subset K of g produces a one-parameter semigroup ϕ in G satisfying $\phi(0) = \{e\}$. Conversely, given such a semigroup in G, procedure II when applied to this semigroup, gives rise to a compact subset of g. We shall describe procedure I in this section.

Let $K \subset g$ be given. We assume first that K is small enough to be contained in αV, where α is the number given by lemma 4.4. By formula (1) of that lemma, we have, for all m and n satisfying $m \leqq n$ the inclusion

$$\left[f\left(\frac{1}{n}K\right)\right]^m \subset f\left(\left(\frac{1}{n}K\right)^m + k\left(\frac{m}{n}\right)^2 \alpha^2 V\right).$$

Thus $\left[f\left(\frac{1}{n}K\right)\right]^m \subset f(\alpha V + k\alpha^2 V)$. Denote the right member of this inequality by A, and put $A_\nu = f\left(\frac{1}{\nu}K\right)$. This makes it possible to apply proposition 1.8 (with $m_\nu = \nu$). We find that there exists a sequence n_ν of positive integers such that for every rational number r between 0 and 1, the sequence $\left[f\left(\frac{1}{n_\nu}K\right)\right]^{[rn_\nu]}$ converges. We shall denote the mapping $r \to \lim \left[f\left(\frac{1}{n_\nu}K\right)\right]^{[rn_\nu]}$ by ϕ^*.

Using (1) of lemma 4.4 again we obtain an estimate of $\phi^*(r)$:

$$\left[f\left(\frac{1}{n_\nu}K\right)\right]^{[rn_\nu]} \subset \left[f\left(\frac{\alpha}{n_\nu}V\right)\right]^{[rn_\nu]} \subset f\left(\frac{\alpha\,[rn_\nu]}{n_\nu}V + k\left(\frac{\alpha\,[rn_\nu]}{n_\nu}\right)^2 V\right) \subset$$

$$\subset f(\alpha r V + k\alpha^2 r^2 V),$$

so that

$$\text{(a)} \qquad \|f^{-1}\phi^*(r)\| \leqq \alpha r + k\alpha^2 r^2.$$

This shows that $\phi^*(r) \to \{e\}$ as $r \to 0$.

Now let r_1 and r_2 be given rational numbers between 0 and 1 and satisfying $r_1 + r_2 \leqq 1$. Then we have:

$$A_{n_\nu}^{[(r_1+r_2)n_\nu]} = A_{n_\nu}^{[r_1 n_\nu]+[r_2 n_\nu]+\theta_\nu} = A_{n_\nu}^{[r_1 n_\nu]} \cdot A_{n_\nu}^{[r_2 n_\nu]} \cdot A_{n_\nu}^{\theta_\nu},$$

where θ_ν for each ν denotes one of the numbers 0 and 1. A passage to the limit as $\nu \to \infty$ gives

$$\text{(b)} \qquad \phi^*(r_1 + r_2) = \phi^*(r_1)\,\phi^*(r_2).$$

It is now easy to see that uniform continuity of the mapping ϕ^* follows from (a) and (b). Thus ϕ^* can be extended to a mapping defined for all real numbers between 0 and 1. It then follows from proposition 2.4 that this new mapping can be extended to a one-parameter semigroup ϕ in G. It follows from (a) that $\phi(0) = \{e\}$.

We shall also show that the relation $\phi(\delta) = \lim \left[f\left(\frac{1}{n_\nu} K\right)\right]^{[\delta n_\nu]}$ holds for all positive real numbers δ and not only for those which are rational and less than one. From the formula $\left[\phi\left(\frac{\delta}{n}\right)\right]^n = \phi(\delta)$ we see that it is enough to prove this for $\delta \leqq 1$. Let therefore $r_i \to \delta$ as $i \to \infty$, $(i = 1, 2 \ldots)$. We have

$$\phi(\delta) = \lim_{i\to\infty} \lim_{\nu\to\infty} A_{n_\nu}^{[r_i n_\nu]}.$$

With the aid of (a), it is easy to justify an inversion of the order of the limits, which gives the result.

We finally remove the restriction $K \subset \alpha V$ by the following device. Let K be any compact subset of g. Choose the integer p so large that $\frac{1}{p} K \dot{\subset} \alpha V$. Apply the above procedure to the set $\frac{1}{p} K$. This gives a one-parameter semigroup ϕ'. We see also that $\phi(\delta) = (\phi'(\delta))^p$ defines a semigroup ϕ in G and that if n_ν is the sequence for which $\phi'(\delta) = \lim_{\nu\to\infty} \left[f\left(\frac{1}{n_\nu}\frac{1}{p} K\right)\right]^{[\delta n_\nu]}$, then $p n_\nu$ is a sequence for which $\phi(\delta) = \lim \left[f\left(\frac{1}{p n_\nu} K\right)\right]^{[\delta p n_\nu]}$. This requires a proof that the difference between $[\delta p n_\nu]$ and $p[\delta n_\nu]$ is inessential, which is easy (cf the end of the proof of lemma 4.5.)

Summarizing these considerations, we describe procedure I as follows. Given a compact set $K \subset g$, the procedure consists in choosing a sequence n_ν of integers such that

$$\phi(\delta) = \lim \left[f\left(\frac{1}{n_\nu} K\right)\right]^{[\delta n_\nu]}$$

exists for each non-negative δ and such that ϕ is a one-parameter semigroup with $\phi(0) = \{e\}$.

The above results show that such a choice is always possible.

We conclude with the remark that with some easy and inessential changes the above argument can be adapted to show that given any sequence of positive integers tending to infinity, the sequence n_ν can be chosen as a subsequence of the given sequence.

4.7. Before describing procedure II we shall prove a lemma which is useful in the existence proof which will accompany the description of procedure II. The proof of this lemma is the only place in the proof of theorem 4.12 where we use the fact that f is the exponential mapping. We need the fact that if

m is an integer and $x \varepsilon G$ is sufficiently close to e then $\|f^{-1}(x^m)\| = m \|f^{-1}(x)\|$ (see CHEVALLEY 5, p. 116).

Lemma: *Let ϕ be a one-parameter semigroup in G satisfying $\phi(0)=\{e\}$. Then there exist constants β and l so that $f^{-1}\phi(\delta) \subset \delta l V$ for all $\delta \leqq \beta$.*

Proof: Put $\varphi(\delta) = \|f^{-1}\phi(\delta)\|$. If δ is sufficiently small, say $\leqq \beta$, then $\phi(\delta) \subset f(V)$, which shows that $\varphi(\delta)$ is defined for all $\delta \leqq \beta$. Since ϕ is a continuous function of δ, and f^{-1} and $\|\|$ are continuous functions of the sets $\phi(\delta)$ and $f^{-1}\phi(\delta)$ respectively, we see that $\varphi(\delta)$ is continuous. In particular $\varphi(\delta) \to 0$ as $\delta \to 0$.

Now consider a fixed $\delta > 0$ and $\leqq \beta$. Then $\phi\left(\frac{\delta}{m}\right)$ is a compact set. Let x be an element of this set for which $\|f^{-1}(x)\|$ is a maximum. Then $\varphi\left(\frac{\delta}{m}\right) = \|f^{-1}(x)\|$. Thus by the property of f mentioned above, we have $m\varphi\left(\frac{\delta}{m}\right) = m\|f^{-1}(x)\| = \|f^{-1}(x^m)\|$. But $x^m \varepsilon \left[\phi\left(\frac{\delta}{m}\right)\right]^m = \phi(\delta)$. Thus $m\varphi\left(\frac{\delta}{m}\right) \leqq \varphi(\delta)$. This has been established under the assumption $\delta \leqq \beta$. Changing variables, we may also say that if m is any integer and δ any real number such that $\delta m \leqq \beta$, then

$$\varphi(m\delta) \geqq m\varphi(\delta).$$

Now suppose that there exists a sequence $\delta_\nu \to 0$ and a sequence $l_\nu \to \infty$ of real numbers such that $\varphi(\delta_\nu) = \delta_\nu l_\nu$. We observe that the numbers in the interval between 0 and β which can be expressed in the form $m\delta_\nu$ are dense in that interval. We have also $\varphi(m\delta_\nu) \geqq m\delta_\nu l_\nu$. Let (a, b) be any interval contained in the interval $(0, \beta)$. Then if $m\delta_\nu \varepsilon (a, b)$, we have $\varphi(m\delta_\nu) \geqq m\delta_\nu l_\nu \geqq a l_\nu$. But since $l_\nu \to \infty$ we see that the function φ is unbounded on (a, b), which is inconsistent with its continuity.

Thus there exists a number l so that $\varphi(\delta) \leqq \delta l$, which proves the lemma.

4.8. We now proceed to describe procedure II.

Suppose that ϕ with $\phi(0)=\{e\}$ is a one-parameter semigroup in G. We note that then $\phi(\delta)$ is compact for every δ. We shall consider the sets $K_\delta \subset g$ defined by $K_\delta = \lim_{\nu\to\infty} n_\nu f^{-1}\phi\left(\frac{\delta}{n_\nu}\right)$, where n_ν is a sequence of integers such that the limit exists. Our first step will be to prove the existence of such sequences n_ν.

By lemma 4.7, we have, for all $\delta \leqq \beta$ and all n the equality $n f^{-1}\phi\left(\frac{\delta}{n}\right) \subset \delta l V$. By a procedure analogous to the one used in section 4.6, we construct a sequence n_ν such that $K_\delta = \lim n_\nu f^{-1}\phi\left(\frac{\delta}{n_\nu}\right)$ exists for those δ which are rational numbers between 0 and β. Since $K_\delta \subset \delta l V$, we have $K_\delta \to \{0\}$ as $\delta \to 0$. If δ_1 and δ_2 are two non-negative rational numbers with $\delta_1 + \delta_2 \leqq \beta$, we have $K_{\delta_1+\delta_2} = \lim n_\nu f^{-1}\phi\left(\frac{\delta_1+\delta_2}{n_\nu}\right) = \lim n_\nu f^{-1}\left(\phi\left(\frac{\delta_1}{n_\nu}\right)\phi\left(\frac{\delta_2}{n_\nu}\right)\right)$. Using lemma 4.7 again, we see that $\left\| f^{-1}\,\phi\left(\frac{\delta_1}{n_\nu}\right)\right\| \leqq \frac{\delta_1}{n_\nu}\,l$, and similarly $\left\| f^{-1}\,\phi\left(\frac{\delta_2}{n_\nu}\right)\right\| \leqq \frac{\delta_2}{n_\nu}\,l$. Therefore formula (1) of section 4.3 gives

$$K_{\delta_1+\delta_2} \subset \lim n_\nu \left[f^{-1}\,\phi\left(\frac{\delta_1}{n_\nu}\right) + f^{-1}\,\phi\left(\frac{\delta_2}{n_\nu}\right) + k\,\delta_1\,\delta_2\,l^2\,\frac{1}{n_\nu^2}\,V \right] = K_{\delta_1} + K_{\delta_2}.$$

Similarly formula (2) of the same section gives

$$K_{\delta_1} + K_{\delta_2} = \lim n_\nu \left[f^{-1}\,\phi\left(\frac{\delta_1}{n_\nu}\right) + f^{-1}\,\phi\left(\frac{\delta_2}{n_\nu}\right) \right]$$

$$\subset \lim n_\nu \left[f^{-1}\,\phi\left(\frac{\delta_1+\delta_2}{n_\nu}\right) + k\,\delta_1\,\delta_2\,l^2\,\frac{1}{n_\nu^2}\,V \right] = K_{\delta_1+\delta_2}.$$

Thus $K_{\delta_1+\delta_2} = K_{\delta_1} + K_{\delta_2}$.

From these results, it follows that the mapping $\delta \to K_\delta$ is uniformly continuous, so that the mapping can be extended to the entire non-negative real δ-axis. It also follows that the sets K_δ, thus defined for all $\delta \geqq 0$, satisfy $K_\delta = \lim n_\nu\, f^{-1}\,\phi\left(\frac{\delta}{n_\nu}\right)$ for all sufficiently small δ. Indeed let $r_1, r_2, \ldots$ be a sequence of rational numbers tending to δ. For each ν, we have $n_\nu\, f^{-1}\,\phi\left(\frac{\delta}{n_\nu}\right) = \lim\limits_{i\to\infty} n_\nu\, f^{-1}\,\phi\left(\frac{r_i}{n_\nu}\right)$, and the result follows since $\lim\limits_{\nu\to\infty}\lim\limits_{i\to\infty} = \lim\limits_{i\to\infty}\lim\limits_{\nu\to\infty}$.

From the fact that g is a euclidean space and that the mapping $\delta \to K_\delta$ is a one-parameter semigroup in g, we deduce (theorem 3.5) the important fact that there exists a compact *convex* set K such that $K_\delta = \delta\,K$.

Thus procedure II may be described as follows:

Given a one-parameter semigroup ϕ in G with $\phi(0) = \{e\}$, procedure II consists in choosing a sequence n_ν of integers so that $\lim\limits_{\nu\to\infty} n_\nu\, f^{-1}\,\phi\left(\frac{\delta}{n_\nu}\right)$ exists for all non-negative real numbers δ.

The above results show that such a choice is always possible and that the limit is of the form $\delta\,K$, where K is a compact, convex subset of g.

4.9. The last steps to be taken before we can formulate a structure theorem for one-parameter semigroups in Lie groups consist in investigating the results of the successive application of our two procedures. We consider here the case when procedure II is followed by procedure I.

Let ϕ be a given semigroup in G satisfying $\phi(0) = \{e\}$. We suppose that procedure II has been applied to ϕ, so that we have formed a compact convex set K and a sequence n_ν with $\delta\,K = \lim n_\nu\, f^{-1}\,\phi\left(\frac{\delta}{n_\nu}\right)$ for all non-negative δ.

Put $A_\nu = n_\nu\, f^{-1}\,\phi\left(\frac{\delta}{n_\nu}\right)$ and $B_\nu = \delta\,K$ for $\nu = 1, 2, \ldots$. Then we can apply lemma 4.5 with $m_\nu = [\gamma\, n_\nu]$, where γ is a non-negative real number. Since

$$\left[f\left(\frac{A_\nu}{n_\nu}\right)\right]^{[\gamma n_\nu]}=\left[\phi\left(\frac{\delta}{n_\nu}\right)\right]^{[\gamma n_\nu]}=\phi\left(\frac{[\gamma n_\nu]}{n_\nu}\delta\right)$$

is a convergent sequence with limit $\phi(\gamma\delta)$, we see by the lemma that $\left[f\left(\frac{\delta K}{n_\nu}\right)\right]^{[\gamma n_\nu]}$ also converges to $\phi(\gamma\delta)$.

In particular, we obtain for $\delta=1$ the result that if procedure II takes a semigroup ϕ into a set K then this set K again gives us back the semigroup ϕ if procedure I is applied to K *with the same sequence* n_ν as in procedure II. The result also tells us what happens if we start procedure I with δK instead of with K. Instead of ϕ, we then obtain the semigroup which maps γ on $\phi(\delta\gamma)$. This may be expressed by saying that we obtain ϕ with a change of scale.

4.10. We now consider the result of applying the procedures in the order I, II. Starting from a set K we obtain a semigroup ϕ by I. We should expect to get K back by applying II to ϕ. This is not true unless K is convex. In fact, we always get the convex hull of K.

Thus let K be given and suppose that $\phi(\gamma)=\lim_{\nu\to\infty}\left[f\left(\frac{1}{n_\nu}K\right)\right]^{[\gamma n_\nu]}$ for all non-negative γ. Suppose first that $K\subset\alpha V$, where α is the number described in lemma 4.4. By (1) and (2) of that lemma, we have

$$\text{(a)}\qquad f^{-1}\left(\left[f\left(\frac{1}{n_\nu}K\right)\right]^{[\gamma n_\nu]}\right)\subset\left(\frac{1}{n_\nu}K\right)^{[\gamma n_\nu]}+k\left(\frac{[\gamma n_\nu]}{n_\nu}\right)^2 V$$

and

$$\text{(b)}\qquad \left(\frac{1}{n_\nu}K\right)^{[\gamma n_\nu]}\subset f^{-1}\left(\left[f\left(\frac{1}{n_\nu}K\right)\right]^{[\gamma n_\nu]}\right)+k\left(\frac{[\gamma n_\nu]}{n_\nu}\right)^2 V.$$

We shall show first that $\left(\frac{1}{n_\nu}K\right)^{[\gamma n_\nu]}$ tends to $\gamma H(K)$, where $H(K)$ denotes the convex hull of K. We have obviously

$$\left(\frac{1}{n_\nu}K\right)^{[\gamma n_\nu]}\subset\frac{[\gamma n_\nu]}{n_\nu}H(K).$$

We know too that every sequence of sets $\left(\frac{1}{n_\nu}K\right)^{[\gamma n_\nu]}$ contains a convergent subsequence. By theorem 3.4, the limit of every convergent sequence of these sets must be convex. It is also clear that any such limit contains γK. Since the limit of $\frac{[\gamma n_\nu]}{n_\nu}H(K)$ exists and is $\gamma H(K)$, we see that every limit of a convergent sequence of sets $\left(\frac{1}{n_\nu}K\right)^{[\gamma n_\nu]}$ contains γK, is contained in $\gamma H(K)$, and is convex. This shows that every such limit coincides with $\gamma H(K)$, in other words that $\lim_{\nu\to\infty}\left(\frac{1}{n_\nu}K\right)^{[\gamma n_\nu]} = \gamma H(K)$.

Thus we know that every term in (a) or (b) converges as $\nu\to\infty$. In the limit, we obtain

$$f^{-1}\phi(\gamma)\subset\gamma H(K)+k\gamma^2 V \tag{a'}$$

and

$$\gamma H(K)\subset f^{-1}\phi(\gamma)+k\gamma^2 V. \tag{b'}$$

We are now ready to see what the result of applying procedure II will be. A first, and very reassuring fact to observe is that $\lim_{n\to\infty} n f^{-1}\phi\left(\frac{\gamma}{n}\right)$ exists $(n=1, 2, \ldots)$ and is equal to $\gamma H(K)$. This is important since it shows that *it is not necessary to use a subsequence n_ν in order to produce convergence.* The proof is easy. The two formulas (a′) and (b′) give

$$n f^{-1}\phi\left(\frac{\gamma}{n}\right)\subset\gamma H(K)+k\left(\frac{\gamma^2}{n}\right)V$$

and

$$\gamma H(K)\subset n f^{-1}\phi\left(\frac{\gamma}{n}\right)+k\left(\frac{\gamma^2}{n}\right)V.$$

This proves the result.

It is also clear that the limit of $\frac{1}{\delta}f^{-1}\phi(\gamma\delta)$ as $\delta\to 0$ exists where δ is a continuous variable instead of a sequence.

Finally we note that these results are true without the restriction $K\subset\alpha V$. This is easily proved by the use of a device similar to the one used in sections 4.5 and 4.6. We omit the details.

4.11. Let ϕ be a given semigroup in G with $\phi(0)=\{e\}$. By applying procedure II while using a certain sequence n_ν of integers, we obtain a compact convex set K. We know that procedure I and the same sequence of integers will give us back ϕ. Thus ϕ is obtained by an application of procedure I, and we know that II can be applied with any sequence of integers, or even with a continuous passage to the limit. Therefore we have the following proposition. For any semigroup ϕ in G with $\phi(0)=\{e\}$, the limit $\lim_{\delta\to 0}\frac{f^{-1}\phi(\delta)}{\delta}$ exists and is a compact convex set.

Conversely, let K be a given compact set in g. By procedure I using a sequence n_ν, we obtain a semigroup ϕ. Procedure II can now be applied to ϕ with any sequence of integers. It gives us $H(K)$. We know that if we apply procedure I to $H(K)$ with any sequence of integers we get ϕ again. This shows that if K is convex, we could have used the sequence $1, 2, 3\ldots$ in the first place. This is generally true. By the foregoing, it is clear that any convergent sequence of the type $\left[f\left(\frac{1}{n_\nu} K\right)\right]^{[\gamma n_\nu]}$ converges to the same limit as $\left[f\left(\frac{1}{n_\nu} H(K)\right)\right]^{[\gamma n_\nu]}$ so that all convergent sequences have the same limit. On the other hand, it follows from the last remark of section 4.6 that any such sequence contains a convergent subsequence. This shows that every such sequence is convergent. We therefore see that for any given compact set $K \subset g$ the limit $\lim_{n\to\infty}\left[f\left(\frac{1}{n} K\right)\right]^{[\gamma n]}$ exists.

In this case also we can substitute a continuous variable for $\frac{1}{n}$. The proof is easily carried through by lemma 4.5. Thus we have: for any given compact set $K \subset g$ the limit $\lim_{\delta\to 0}[f(\delta K)]^{[\gamma/\delta]}$ exists and is equal to $\phi(\gamma)$, where ϕ is a one-parameter semigroup in G with $\phi(0) = \{e\}$.

4.12. We now summarize the results obtained so far in this paragraph.

Definition: *Given a one-parameter semigroup ϕ in a Lie group G and a subset K of the Lie algebra g of G, we say that K generates ϕ if for every $\gamma \geqq 0$, we have $\phi(\gamma) = \lim_{\delta\to 0}[f(\delta K)]^{[\gamma/\delta]}$, where f denotes the exponential mapping.*

Theorem: *Let G be a Lie group, let g be the corresponding Lie algebra and f be the exponential mapping. Then:*

(1) *every compact subset of g generates a one-parameter semigroup ϕ in G which satisfies $\phi(0) = \{e\}$;*

(2) *every compact subset of g generates the same semigroup as its convex hull;*

(3) *every one-parameter semigroup ϕ in G which satisfies $\phi(0) = \{e\}$ is generated by a unique compact convex set in g;*

(4) *the compact convex set K which generates a given ϕ is determined by*

$$K = \lim_{\delta\to 0}\frac{1}{\delta} f^{-1}\phi(\delta).$$

4.13. If the Lie group is commutative it is known that it is a homomorphic map of a euclidean space. The homomorphism may be considered as the exponential mapping. The kernel of the homomorphism is a discrete subgroup (submodule) of the euclidean space. We obtain

Theorem: *Let G be a commutative Lie group, g the corresponding Lie algebra and f the exponential mapping (or in other words $G = g/N$ where N is the kernel of the homomorphism f). Let the compact convex set $K \subset g$ generate the one-parameter semigroup ϕ in G. Then $\phi(\delta) = f(\delta . K)$.*

Proof: We first apply proposition 2.7. This gives us a one-parameter semigroup ϕ^* in g which satisfies $\phi^*(0) = N$ and $f\phi^* = \phi$. Then we apply theorem

2.6 to ϕ^*, which gives us a one-parameter semigroup ψ in g such that $\phi^*(\delta) = \psi(\delta) + N$ (we use additive notation since g is a linear space) and with $\psi(0) = \{0\}$. Now ve apply theorem 3.5, which tells us that $\psi(\delta) = \delta M$, where M is a compact convex set. Summing up, we obtain

$$\phi(\delta) = f(\delta M + N) = f(\delta M).$$

Using (4) of theorem 4.12, it is now easy to verify that ϕ is generated by M. But since it is also generated by K and both K and M are convex, it follows from (3) of 4.12 that $K = M$. This proves the theorem.

Remark: We have not much general information about the structure of the sets $\phi(\delta)$ defined by a one-parameter semigroup in a Lie group. The theorem just proved shows that at least in the commutative case, these sets are continuous open maps of compact convex sets, and that if sufficiently small they are even homeomorphic to such sets. Although it seems plausible that this is true in general Lie groups also, I have not succeeded in proving or disproving it.

4.14. We conclude this paragraph with a theorem which throws some light on the problem just mentioned. For the validity of this theorem, it is essential that f be the exponential mapping.

Theorem: *Let G be a Lie group and g the corresponding Lie algebra. Let ϕ be a one-parameter semigroup in G which is generated by a compact, convex subset K of g, Then $\phi(\gamma) \supset f(\gamma K)$, where f denotes the exponential mapping.*

Proof: We have the formula $[f(y)]^m = f(my)$. Therefore we see that

$$\left[f\left(\frac{1}{n} K\right)\right]^m \supset f\left(\frac{m}{n} K\right).$$

Indeed, let $x \varepsilon \frac{m}{n} K$. Then $x = my$, where $y \varepsilon \frac{1}{n} K$. Thus

$$f(x) = f(my) = [f(y)]^m \varepsilon \left[f\left(\frac{1}{n} K\right)\right]^m,$$

which proves the inclusion.

From the definition and theorem of section 4.12, we have

$$\phi(\gamma) = \lim_{\delta \to 0} [f(\delta K)]^{[\gamma/\delta]}.$$

In particular, let δ tend to zero through the values $\frac{\gamma}{m}$, where $m = 1, 2, 3 \ldots$. Then $\phi(\gamma) = \lim_{m \to \infty} \left[f\left(\frac{\gamma K}{m}\right)\right]^m$. We can now apply the formula just proved. We see that $\left[f\left(\frac{\gamma K}{m}\right)\right]^m \supset f(\gamma K)$. Thus the passage to the limit gives $\phi(\gamma) \supset f(\gamma K)$, which proves the theorem.

Remark. Theorem 4.13 shows that in the commutative case we have equality instead of inclusion in $\phi(\gamma) \supset f(\gamma K)$.

§ 5. Normed groups

5.1. Definition: *A normed group G is a group on which there is defined a left-invariant metric with the following properties: The metric defines a topology on G such that in this topology G is a topological group. If S_δ denotes the closed sphere of radius δ around the identity of G, then the mapping $\delta \to S_\delta$ is a one-parameter semigroup. — If G is a normed group, the distance from e to $x \varepsilon G$ is called the norm of x and is denoted by $\|x\|$. — A topological group G is said to be normable if it is possible to define its topology by a metric so as to make G a normed group.*

Remark: The term "norm" has been used in connection with groups in several different ways. Some authors use the word to denote the distance from e to an element of the group in any metric group. ARONSZAJN (**1**) requires conditions on the metric which do not coincide with those of the above definition. If the group is a linear space, then the term "norm" has a universally accepted meaning. It seems very likely that in this case our definition is equivalent with the usual one.

Examples:

1. If G is a normed linear space in the usual sense, then it is also a normed group under addition. The proof is made by verifying conditions R 1–5 of the next section. This is easy, and we omit the details. The converse problem, however, seems to be rather difficult. It can be formulated as follows: Let G be a linear space on which is defined a function $\|x\|$ so that G becomes a normed group under addition. Is it true that G is a normed linear space? From theorem 3.5, it follows that the answer is affirmative if G is finite-dimensional. Such a space is therefore a Minkowski space (finite-dimensional Banach space). I do not know the answer to this problem in the general case.

2. Let G be the group of all complex numbers η of unit modulus under multiplication. Putting $\|\eta\| = |\arg \eta|$ where $\arg \eta$ is chosen between $-\pi$ and π, we see that $\|\eta\|$ is a norm for G.

3. Let G be the direct product of a countable number of groups G_i, $i = 1, 2, 3 \ldots$ isomorphic with and normed in the same way as the one of example 2. An $x \varepsilon G$ can be written as $x = (\eta_1, \eta_2, \ldots)$ where $\eta_i \varepsilon G_i$. Then the function $\|x\| = \sup \frac{1}{i} \|\eta_i\|$ is a norm for G. For the proof, which is easy, we refer to the more general formulation in theorem 6.1.

5.2. Let G be a topological group the topology of which is defined by a left-invariant metric. Let $r(x)$ denote the distance from e to x and S_δ the set $\{x \mid r(x) \leqq \delta\}$ (i.e. the closed sphere of radius δ around e). Then the following conditions are satisfied.

R 1. $r(x)$ is defined for all $x \varepsilon G$ and assumes non-negative real values.
R 2. $r(x) = 0$ if and only if $x = e$.
R 3. $r(x) = r(x^{-1})$.
R 4*. $r(xy) \leqq r(x) + r(y)$.

R 5. Let $x \varepsilon G$ and $\delta > 0$. Then there exists $\varepsilon > 0$ with $r(x y x^{-1}) \leqq \delta$ for all y such that $r(y) \leqq \varepsilon$.

Correspondingly, the sets S_δ satisfy the following conditions.

S 1. $\bigcup_{\delta \geqq 0} S_\delta = G$.

S 2. $S_0 = \{e\}$.

S 3. $S_\delta = S_\delta^{-1}$.

S 4*. $S_{\delta_1} S_{\delta_1} \subset S_{\delta_1 + \delta_2}$.

S 5. Given $x \varepsilon G$ and $\delta > 0$, there exists $\varepsilon > 0$ with $x S_\varepsilon x^{-1} \subset S_\delta$.

S 6. $\bigcap_{\delta > \delta_0} S_\delta = S_{\delta_0}$.

The verifications are simple and are omitted.

Suppose now in addition that r is a norm for G. Then S 4* can be sharpened to

S 4. $S_{\delta_1} S_{\delta_2} = S_{\delta_1 + \delta_2}$.

The corresponding condition for r is:

R 4. The condition R 4* and the following condition hold: given $\delta_1 \geqq 0$, $\delta_2 \geqq 0$ and $z \varepsilon G$ with $r(z) = \delta_1 + \delta_2$, there exist x and y with $xy = z$ and $r(x) = \delta_1$ and $r(y) = \delta_2$.

5.3. Conversely, we shall show that each of the sets of conditions R and S suffice to characterize normed groups. More precisely: Let G be a group on which is defined a function $r(x)$ satisfying R 1, 2, 3, 4*, and 5. Then $d(x, y) = r(x^{-1} y)$ is a left-invariant metric on G in terms of which G is a topological group. Moreover, if the condition R 4 is satisfied, then r is a norm for G.

Proof: We define sets S_δ by $S_\delta = \{x \mid r(x) \leqq \delta\}$. It is easy to verify that these sets satisfy S 1, 2, 3, 4*, 5 and 6. It follows from these conditions that the sets S_δ for $\delta > 0$ constitute a fundamental system of neighborhoods of e in a topology for G which makes G a topological group (see axioms G T I–IV of WEIL, **12**, p. 9). It is also trivial to verify that $d(x, y)$ is a left-invariant metric.

Now suppose that condition R 4 also holds. Then S 4 holds. Further, since a metric is always a continuous function in the topology defined by it, the function $r(x)$ is continuous. Since S_δ is defined as the inverse image under $r(x)$ of a closed interval of the real axis the set S_δ is closed. It remains to show that $\delta \to S_\delta$ is a continuous mapping, *i.e.*, that given a neighborhood U of e and a number δ_0, there exists $\varepsilon > 0$ with $S_\delta \subset U S_{\delta_0}$ and $S_{\delta_0} \subset U S_\delta$ for all δ in the interval $\delta_0 - \varepsilon \leqq \delta \leqq \delta_0 + \varepsilon$. Since we lose no generality in assuming that U belongs to a certain fundamental system of neighborhoods of e, we may choose $U = S_\gamma$ for some $\gamma > 0$. By choosing $\varepsilon = \gamma$ we obtain $\delta \leqq \delta_0 + \gamma$ and $\delta_0 \geqq \delta + \gamma$. Since S_δ varies monotonically with δ, these inequalities imply that $S_{\delta_0} \subset S_{\delta + \gamma} = S_\gamma S_\delta = U S_\delta$ and $S_\delta \subset S_{\delta_0 + \gamma} = S_\gamma S_{\delta_0} = U S_{\delta_0}$, which proves continuity. This completes the proof of the proposition.

5.4. The corresponding proposition obtained by starting from conditions S is: Let G be a group in which is defined sets S_δ, where δ is a non-negative parameter. Suppose that the sets S_δ satisfy conditions S 1, 2, 3, 4*, 5 and 6.

Then there exists a function $r(x)$ satisfying R 1, 2, 3, 4* and 5 such that $S_\delta = \{x \mid r(x) \leqq \delta\}$. The sets S_δ for $\delta > 0$ constitute a fundamental system of neighborhoods of G in a topology which makes G a topological group. If, furthermore, condition S 4 is satisfied, then $r(x)$ is a norm for G.

Proof: By S 3 and S 4* we have $S_\delta \supset S_{\delta/2} S_{\delta/2}^{-1}$, and thus $e \varepsilon S_\delta$. Now let $\delta_2 \geqq \delta_1$. Then by S 4* we have $S_{\delta_2} \supset S_{\delta_1} S_{\delta_2 - \delta_1}$. Since $S_{\delta_2-\delta_1}$ contains e, it follows that $S_{\delta_2} \supset S_{\delta_1}$.

Now let $r(x)$ be the infimum of those non-negative numbers for which $x \varepsilon S_\delta$. By S 1, this infimum exists. From S 6 it follows that $x \varepsilon S_{r(x)}$. Let δ be greater than or equal to $r(x)$. Thus $x \varepsilon S_{r(x)} \subset S_\delta$. Conversely, if $x \varepsilon S_\delta$, then by the definition of r we have $r(x) \leqq \delta$. This shows that $S_\delta = \{x \mid r(x) \leqq \delta\}$. It is now easy to verify conditions R 1, 2, 3, 4* and 5.

If we observe that S 4 implies R 4, we can apply the proposition of the preceding section, which completes the proof.

5.5. We have seen in the preceding sections that each of the sets of conditions R and S can be used as an axiom system for normed groups. The theorem of the next section gives still another characterization of normed groups. We need the following preliminaries.

Menger (9) has introduced the notion of a convex metric space. According to his definition, a metric space is convex if for any two different points x and y in the space, there exists a third point z different from x and from y such that z lies between x and y in the sense that equality holds in the triangle inequality for the three points x, z and y: $d(x, z) + d(z, y) = d(x, y)$, where d is the metric. By a slight abuse of language, it has become common to refer to the metric of a convex metric space as a convex metric. This has certain advantages when dealing with several different metrics defined on the same topological space, and we shall therefore adopt this usage. Our definition of a convex metric will, however, be slightly different from that of Menger.

Definition: *A metric $d(x, y)$ on a set M of points will be called convex if the following condition is satisfied: Let $\delta_1 \geqq 0$, $\delta_2 \geqq 0$ and x, y be two points of M, so that $d(x, y) = \delta_1 + \delta_2$. Then there exists $z \varepsilon M$ with $d(x, z) = \delta_1$ and $d(z, y) = \delta_2$.*

It follows from theorems of Menger that if the set M is compact or even complete, considered as a metric space with the metric d, then this definition coincides with that of Menger. It should also be pointed out that if for two given points x and y we determine for each α between 0 and 1 a point $z(\alpha)$ with $d(xz) = \alpha\, d(xy)$ and $d(zy) = (1-\alpha)\, d(xy)$, then the set of these points $z(\alpha)$ does not necessarily form a segment in the sense of Menger (*l.c.*). If d makes M a complete metric space, it is nevertheless true that the points x and y can be joined by a segment consisting of points $z(\alpha)$ depending on α as described above. This follows from one of the theorems of Menger referred to above. From this result, Menger deduces that a complete convex metric space is connected and locally connected.

Our deviation in terminology from that of Menger simplifies the formulation of the following theorem.

5.6. Theorem: *A necessary and sufficient condition that a metric group G be a normed group is that the metric be left-invariant and convex.*

Proof: 1. Suppose that G is normed. The necessity of left invariance lies in the definition of normed groups. The necessity of convexity follows directly from the fact that condition R 4 must be satisfied. In fact, let $d(x, y)$ be the given metric on G. Then $d(x, y) = d(e, x^{-1} y) = r(x^{-1} y)$. Let a and b be given points in G and α a number between 0 and 1. From R 4, we infer the existence of a point c in G such that $r(a^{-1} c) = \alpha\, r(a^{-1} b)$ and $r(c^{-1} b) = (1-\alpha)\, r(a^{-1} b)$. (Observe that $a^{-1} c\, c^{-1} b = a^{-1} b$). This is just the condition for convexity of d.

2. Suppose that the given metric d is left-invariant and convex. From section 5.2 it follows that conditions R 1, 2, 3, 4* and 5 are satisfied. Retracing the argument of the first part of the proof, in the opposite direction, we see that the convexity of d together with R 4* implies R 4. Applying proposition 5.3, we see that G is normed. The theorem is thus proved.

We have seen already in paragraphs 3 and 4 that there are many connections between the theory of convex sets and the theory of one-parameter semigroups of sets. The above theorem establishes another such connection.

5.7. Theorem: *A complete normed group is metric, connected and locally connected.*

Proof: The result follows immediately from theorem 5.6 and the theorem of Menger quoted at the end of section 5.5.

Theorem: *A locally compact normed group is separable, metric, connected and locally connected.*

Proof: Since any normed group is metric and any locally compact group is complete we have only separability left to verify. But this is an immediate consequence of connectedness and local compactness.

According to a conjecture of Menger which was proved in 1949 by BING (**2**) and MOÏSE (**10**), any compact, connected and locally connected, metrizable space can be given a convex metric. This fact suggests the following problem. Is every locally compact, separable, metrizable, connected and locally connected, topological group normable? Paragraph 6 is devoted largely to a partial solution of this problem.

§ 6. Normability theorems

In this paragraph we collect theorems stating various sets of sufficient conditions for a group to be normable. The emphasis is on locally compact groups.

6.1. Theorem: *Let G be a finite direct product of normed groups or a countable direct product of compact normed groups. Then G is normable.*

Proof: Let $G = G_1 \times G_2 \times \cdots \times G_n$, where each G_i is normed. Let $\| \;\|_i$ denote the norm on G_i. If $x = (x_1, x_2 \ldots x_n)$ is an element of G and $x_i \in G_i$, we put $\|x\| = \max\limits_i \|x_i\|_i$. We easily verify conditions R 1, 2, 3, 4* and 5 of section 5.2. In order to verify R 4, let $z = (z_1 \ldots z_n) \in G$ and $\|z\| = \delta_1 + \delta_2$. Thus for some value of i (say for $i = j$) the coordinate z_i of z satisfies $\|z_i\|_i = \delta_1 + \delta_2$. Since condition R 4 holds for G_j, there exist x_j and $y_j \in G_j$ with $x_j\, y_j = z_j$, $\|x_j\|_j = \delta_1$, and $\|y_j\|_j = \delta_2$. For $i \neq j$, we have $\|z_i\|_i \leqq \delta_1 + \delta_2$, and therefore there exist x_i and

y_i with $x_i y_i = z_i$, $\|x_i\|_i \leqq \delta_1$, and $\|y_i\|_i \leqq \delta_2$. Putting $x = (x_1, x_2 \ldots x_n)$ and $y = (y_1, y_2 \ldots y_n)$, we have $xy = z$, $\|x\| = \delta_1$, and $\|y\| = \delta_2$, which shows that condition R 4 holds for G. This proves the first part of the theorem.

Now let G be the direct product of a countable sequence of compact normed groups G_i, $i = 1, 2, 3 \ldots$. Since the group G_i is compact, the norm $\| \;\|_i$ has a maximum on G_i. We may assume that this maximum is equal to 1 by multiplying the norm with a suitable constant. Let $x = (x_1, x_2 \ldots)$ be an element of G. We put $\|x\| = \max\limits_i \frac{1}{i} \|x_i\|_i$. Because the $\| \;\|_i$ are bounded, the maximum exists and is assumed for some value j of the index i. Verification of conditions R 1 … 5 is carried out in the same way as in the previous part of the proof. It is also clear that the norm thus defined gives the correct topology on the group G. This proves the theorem.

6.2. Theorem: *A separable, metrizable, connected, locally connected and commutative locally compact group is normable.*

Proof: This follows directly from the above theorem and a well-known structure theorem for commutative groups which states that a group with the properties given in the hypothesis is the direct product of a finite number of real lines and a finite or countably infinite number of real lines modulo one. Since both the groups used as factors in the product are normable (c.f. examples 1 and 2 of section 5.1) the theorem follows.

This theorem shows that for commutative, locally compact groups the conditions given as necessary for normability in theorem 5.7 are also sufficient.

6.3. Theorem: *Every factor group G/K of a locally compact normed group G with respect to a closed normal subgroup K is normable.*

Proof: Let $\| \;\|$ be the norm given on G and let zK be a coset of K. Put $r(zK) = \min\limits_{u \varepsilon K} \|zu\|$. Because G is locally compact, this minimum value is assumed for some $u \varepsilon K$. Then the function r defined on the set of all cosets of K satisfies conditions R 1 … 5 of section 5.2. Since the truth of this statement is a wellknown fact for conditions R 1, 2, 3, 4* and 5 (which refer to the situation in an arbitrary metric group), we have only to verify condition R 4. Let $z \varepsilon G$ be given with $r(zK) = \delta_1 + \delta_2$, and let u be an element of K for which $\|zu\|$ is minimal. Thus $\|zu\| = \delta_1 + \delta_2$. This implies that x and y exist with $xy = zu$ and $\|x\| = \delta_1$ and $\|y\| = \delta_2$. Thus $r(xK) \leqq \|xe\| = \delta_1$ and $r(yK) \leqq \|ye\| = \delta_2$. Since the triangle inequality ($=$ condition R 4*) holds for r, we also have

$$r(xK) + r(yK) \geqq r(xKyK) = r(zK) = \delta_1 + \delta_2.$$

This shows that $r(xK) = \delta_1$ and $r(yK) = \delta_2$. This proves condition R 4. The function r is therefore a norm. Since it obviously also defines the correct topology for G/K, the theorem is proved.

Remark: There may of course exist other norms on G/K defining the correct topology for this group. We shall call the norm defined by the procedure used in the above proof, the natural norm for G/K.

6.4. Theorem. *Any connected Lie group is normable.*

Proof: Let K be a compact, convex, symmetric neighborhood of the origin in the Lie algebra of the group G. Let K generate (definition 4.12) a one-parameter semigroup ϕ in G. From theorem 4.12, it follows that $\phi(0) = \{e\}$ which means (since a one-parameter semigroup is a continuous mapping) that given any neighborhood U of e, there exists a $\delta > 0$ with $\phi(\delta) \subset U$. From theorem 4.14, we know that if K is chosen sufficiently small, we have $\phi(\delta) \supset f(\delta K)$, where f is the exponential mapping and $0 \leqq \delta \leqq 1$. Since δK for $\delta > 0$ is a neighborhood of the origin in the Lie algebra of G and f is open it follows that $f(\delta K)$ is a neighborhood of e in G and therefore the same is true for $\phi(\delta)$ for $\delta > 0$. This shows that the sets $\phi(\delta)$ for $\delta > 0$ constitute a fundamental system of neighborhoods for the topology of G.

It is easy to see that $\phi(\delta)$ is symmetric for all δ, since K is symmetric. This proves condition S 3 of section 5.2. We know also that S 4 is satisfied, since ϕ is a one-parameter semigroup. S 5 follows from the fact that the sets $\phi(\delta)$, $\delta > 0$, constitute a fundamental system of neighborhoods of e. Since $\phi(\delta)$ contains e for all δ, S 2 holds. It follovs from S 4 that $\phi(\delta)$ increases monotonically with δ. This verifies S 6. Finally S 1 follows from the fact that G is connected. We know already that the system $\phi(\delta)$, $\delta > 0$, defines the correct topology for G. This proves the theorem.

Remark: We could also have proved the theorem with differential geometric methods by introducing a left-invariant infinitesimal riemannian metric on the group. Then it is easy to see that the length of the shortest arc joining two points is a convex metric on the group. The proof given is, however, more in the spirit of the present work and yields also a more general result than the other method. It shows namely that the infinitesimal generator of the spheres in the metric can be chosen to be any symmetric convex set containing 0 in its interior, whereas for a metric deduced from an infinitesimal riemannian metric the corresponding generator has to be an ellipsoid. Of course also this more general statement can be proved by differential geometric methods since the more general metric can be obtained by making the group a Finsler space rather than a riemannian space.

6.5. In view of the result of Bing and Moïse mentioned in section 5.7 it seems very likely that for compact groups the conditions (separability,) metrizability, connectedness and local connectedness should be sufficient to guarantee normability. If this conjecture were true, it should be possible to verify it quite easily with the aid of the known structure theorems for compact groups. However, attempting to carry such verifications through, I have found that certain complications arise, which are due to difficulties in dealing with the property of local connectedness in the general case. The theorem below gives a partial solution of the problem. It follows easily from the results already obtained in this paragraph combined with known results on the structure of compact groups.

Theorem: *Let G be a separable, metrizable, connected and locally connected, compact group. Then G contains a totally disconnected closed central subgroup K such that G/K is normable.*

Proof: Denote the center of G by C. It is known (see VAN KAMPEN (8), in particular theorems 1 and 3) that C contains a totally disconnected closed subgroup K such that G/K is isomorphic to the direct product of C/K with a finite or countably infinite number of simple Lie groups. The factor group C/K is connected, locally connected and abelian. By theorems 6.2 and 6.4 it follows that every factor of the direct product is normable. Thus the theorem follows from theorem 6.1.

Remark: The group K used in the above proof is defined as the centre of that subgroup of G which is generated by the totality of all normal simple Lie subgroups of G.

Corollary: If K is finite, then G is normable.

Proof: Consider the natural homomorphism of G onto G/K and apply proposition 2.7. The result then follows from theorem 2.6.

REFERENCES

1. ARONSZAJN, Caractérisation métrique de l'espace de Hilbert, des espaces vectoriels et de certains groupes métriques. C. R. Paris, 201 (1935), pp. 811—813, 873—875.
2. BING, Partitioning a set, Bull. Amer. Math. Soc. 55 (1949), pp. 1101—1110.
3. BONNESEN-FENCHEL, Konvexe Körper, Berlin 1934.
4. BOURBAKI, Topologie générale, Chap. I, II, Paris 1940.
5. CHEVALLEY, Theory of Lie groups, I, Princeton 1946.
6. GLEASON, Arcs in locally compact groups, Proc. Nat. Acad. Sci. USA. 36 (1950), pp. 663—667.
7. HAUSDORFF, Mengenlehre, Berlin Leipzig 1927.
8. VAN KAMPEN, The structure of a compact connected group, Amer. J. Math. 57 (1935), pp. 301—308.
9. MENGER, Untersuchungen über allgemeine Metrik, I, II, III, Math. Ann. 100 (1928), pp. 75—163.
10. MOÏSE, Grilledecomposition and convexification theorems for compact metric locally connected continua, Bull. Amer. Math. Soc. 55 (1949), pp. 1111—1121.
11. PONTRJAGIN, Topological groups, Princeton 1939.
12. WEIL, L'intégration dans les groupes topologiques et ses applications, Paris 1940.

Tryckt den 27 mars 1952

Uppsala 1952. Almqvist & Wiksells Boktryckeri AB