GENERATING SETS OF ELEMENTS IN COMPACT GROUPS

GILBERT HELMBERG

1. Preliminaries. It is well known that compact topological groups have many properties similar to those of finite groups, which are of course special cases of compact topological groups under the discrete topology. The program of this paper is to characterize sets of elements in a compact topological group which generate a given subgroup and, conversely, to determine properties of the subgroup generated by a given set of elements by an investigation of the properties of this set. Tools for our investigation are the convolution algebra of continuous complex-valued functions on the group and the system of irreducible representations of the group. We shall also formulate the results using those concepts. Our results are straightforward generalizations of known theorems on generating sets of elements in finite groups[1].

From now on G will denote a compact topological group which, as a topological space, is T_1. It follows that G is Hausdorff and, therefore, also normal. Let e denote the identity of G. A subset H of G will be called a subgroup of G if it is an abstract subgroup of G and closed, unless the contrary is specifically stated. Let μ denote the normalized Haar measure on G: $\mu(G) = 1$.

A subgroup H with positive measure $\mu(H) > 0$ is necessarily both open and closed, as are all (left) cosets of H. Thus a compact group G with such a subgroup is disconnected and the quotient-spaces G/H (with respect to left cosets of H) is finite and discrete in the quotient topology. Then $1/\mu(H)$ is the index of H in G. The quotient space of G with respect to left cosets of a subgroup of measure 0 contains infinitely many elements and is again compact, Hausdorff and normal.

Let C denote the field of complex numbers and $C(G)$ the set of all complex-valued continuous functions on G. Defining scalar multiplication and addition in $C(G)$ pointwise as usual, $C(G)$ becomes a Banach-space under the uniform norm: $\|f\| = \sup_{x\in G}\{|f(x)|\}$ $(f \in C(G))$. Defining multiplication in $C(G)$ by convolution,

$$(f * g)(x) = \int_G f(xy^{-1})g(y)dy ,$$

$C(G)$ becomes a Banach algebra. Left and right translations of $f \in C(G)$ by $s \in G$ are defined by ${}_sf(x) = f(sx)$ and $f_s(x) = f(xs)$ respectively. Both ${}_sf$ and f_s are functions in $C(G)$ and every $f \in C(G)$ is both left

[1] See [2].

Received April 28, 1958. Presented at the 65th Annual Meeting of the American Mathematical Society in Cincinnati, Ohio. January 28-30, 1958.

and right uniformly continuous.

DEFINITION 1. The subgroup H of G is said to be generated by a set $M \subset G$ if it is the smallest subgroup of G containing M.

The subgroup generated by M will be denoted by $H(M)$. It is evidently the closure of the set of all finite products of positive and negative powers of elements in M. From a theorem of Numakura[2] about compact semigroups it follows that $H(M)$ is already the closure of the set of all finite products of positive powers of elements of M.

2. Subsets of G and corresponding ideals in $C(G)$. With every non-void subset M of G we shall associate the set $F(M)$ of all functions $f \in C(G)$ invariant under right translation by every element $s \in M$.

$$F(M) = \{f : f \in C(G), f_s = f \text{ for all } s \in M\} .$$

Obviously $F(M)$ is non-void, since it contains the constant functions. It is clearly a linear subspace of $C(G)$, and it contains with every $f \in F(M)$ the function $a * f$ if $a \in C(G)$ since

$$(a * f)_s(x) = (a * f)(xs) = \int_G a(xsy^{-1}) f(y) dy$$
$$= \int_G a(xy^{-1}) f(ys) dy = (a * f)(x) .$$

$F(M)$ is therefore a left ideal in $C(G)$.

It is clear that $M_1 \subset M_2$ implies $F(M_1) \supset F(M_2)$. If $\overline{M}$ is the closure of M in G we have therefore $F(M) \supset F(\overline{M})$.

LEMMA 1. $F(M) = F(\overline{M})$.

Proof. We have to show $F(M) \subset F(\overline{M})$. Assume that there is $f \in F(M)$ such that $f \notin F(\overline{M})$. Then there is $\overline{m} \in \overline{M}$ such that $f_{\overline{m}} \neq f$ and

$$(1) \qquad \| f_{\overline{m}} - f \| > a \text{ for some } a > 0 .$$

Because of the uniform continuity of f, we can choose a neighborhood V of e such that

$$|f(x) - f(y)| < \frac{a}{2} \text{ if } x^{-1}y \in V .$$

The set $\overline{m}V$ is a neighborhood of $\overline{m}$ and contains a point $m \in M$. Then

[2] See [6] p. 102.

$$|f(x\overline{m}) - f(xm)| < \frac{a}{2} \text{ for all } x \in G$$

since $(x\overline{m})^{-1}xm = \overline{m}^{-1}m \in V$. Since $f(x\overline{m}) = f_{\overline{m}}(x)$ and $f(xm) = f(x)$ it follows that $||f_{\overline{m}} - f|| < a/2$ which contradicts our assumption (1). Hence $f_{\overline{m}} = f$ and $f \in F(\overline{M})$ for all $f \in f(M)$ and the Lemma follows.

Now let $f \in F(M)$ and $a \in M, b \in M$. Clearly $f_e = f$. Since $f(xa) = f(x)$ for all $x \in G$, we also have $f(xa^{-1}a) = f(xa^{-1})$ for all $x \in G$ or $f_{a^{-1}} = f$. Moreover $f_{ab}(x) = f_b(xa) = f(xa) = f(x)$ for all $x \in G$. If we denote by $H'(M)$ the abstract (not necessarily closed) subgroup of G generated by M then evidently $F(M) \subset F(H'(M))$. On the other hand, $M \subset H'(M)$ implies $F(M) \supset F(H'(M))$ and therefore $F(M) = F(H'(M))$. Now $H(M)$ is the closure of $H'(M)$ in G, and by Lemma 1 we obtain

LEMMA 2. $F(M) = F(H(M))$.

This result allows us to infer some further properties of the functions of $F(M)$. To simplify the notation, we shall in the rest of this paragraph write H instead of $H(M)$. Let $\{g_r H : r \in R\}$ be the decomposition of G into distinct left cosets of H and G/H be the corresponding quotient space. For $f \in F(H)$ and arbitrary $h \in H$, we have $f(g_r h) = f(g_r)$, so that f is constant on every coset $g_r H$. Conversely every continuous function on G constant on every left coset of H has clearly the property $f_h = f$ for all $h \in H$ and belongs to $F(H)$. Hence $F(M)$ is the set of all continuous functions on G that are constant on left cosets of the subgroup generated by M.

Let us denote by $C(G/H)$ the set of all continuous complex-valued functions on G/H. If we associate with every $f \in F(H)$ the function f' on G/H defined by $f'(g_r H) = f(g_r)$ then $f' \in C(G/H)$ and the mapping $f \to f'$ is a linear one-to-one mapping of $F(H)$ as a linear space onto the linear space $C(G/H)$.[3]

To identify the dimension of $C(G/H)$ as a linear space we have to distinguish two cases.

(a) $\mu(H) > 0$. G/H is finite and discrete. The $i = 1/\mu(H)$ characteristic functions of the points of G/H form a basis in $C(G/H)$. Therefore $F(H)$ is finite-dimensional and closed in the uniform norm in $C(G)$.

(b) $\mu(H) = 0$. G/H is a normal Hausdorff space with infinitely many points. Therefore $C(G/H)$ and $F(H)$ are infinite-dimensional. Let $\overline{F}(H)$ be the closure of $F(H)$ in $C(G)$ and $\bar{f} \in \overline{F}(H)$. Assume $\bar{f}_h \neq \bar{f}$ for some $h \in H$, or

$$(2) \qquad ||\bar{f}_h - \bar{f}|| > a \text{ for some } a > 0 .$$

[3] See [5] p. 110, 111.

There is $f \in F(H)$ such that $||\bar{f} - f|| < a/2$ or

$$|\bar{f}(xh) - f(xh)| < \frac{a}{2} \quad \text{for all } x \in G$$

$$|\bar{f}_h(x) - f(x)| < \frac{a}{2} \quad \text{for all } x \in G$$

$$||\bar{f}_h - f|| < \frac{a}{2}.$$

But then

$$||\bar{f}_h - \bar{f}|| \leqq ||\bar{f}_h - f|| + ||\bar{f} - f|| < a$$

which contradicts (2). Therefore $\bar{f}_h = \bar{f}$ for all $h \in H$ and $\overline{F}(H) \subset F(H)$ which shows that $F(H)$ is again closed in $C(G)$.

The results of our discussion are summed up in

THEOREM 1. *$F(M)$ is a closed left ideal in $C(G)$ consisting exactly of all continuous functions on G which are constant on each left coset of the subgroup $H(M)$. As linear subspace of $C(G)$, $F(M)$ is $1/\mu(H(M))$-dimensional if $\mu(H(M)) > 0$ and infinite-dimensional if $\mu(H(M)) = 0$.*

Analogous statements hold for the set of all continuous functions on G that are invariant under left-translation by every element $m \in M$.

3. Subgroups of G and corresponding ideals in $C(G)$. Let the subset M of G be a subgroup H. We can reverse the correspondence between H and $F(H)$ by observing that H is completely characterized by $F(H)$ as the set of all elements of G which right translate every $f \in F(H)$ into itself. In order to see this we have only to show that for every $m \notin H$ there is $f \in F(H)$ such that $f_m \neq f$. Since $m^{-1} \notin H$ we have $H \neq m^{-1}H$. By the complete regularity of G/H, there is $f' \in C(G/H)$ such that $f'(H) = 1$ and $f'(m^{-1}H) = 0$. Defining $f \in F(H)$ by the relation $f(x) = f'(xH)$ for all $x \in G$, we have $f(m^{-1}) = 0$ and $f_m(m^{-1}) = f(e) = 1$. Hence $f_m \neq f$.

It follows that for two arbitrary subgroups H_1 and H_2 of G $F(H_1) \supset F(H_2)$ implies $H_1 \subset H_2$. The converse is obviously true. We conclude:

LEMMA 3. *If H_1 and H_2 are subgroups of G_1 then $H_1 \subset H_2$ if and only if $F(H_1) \supset F(H_2)$.*

Taking $\{e\}$ and G as subgroups of G we have in particular $F(e) = C(G)$ and $F(G) = \{\alpha 1\}$ i.e., the (left) ideal consisting of all constant functions.

Let now N be a normal subgroup of G, $n \in N$ and $f \in F(N)$. For every $x \in G$ we have ${}_nf(x) = f(nx) = f(xn_1) = f_{n_1}(x) = f(x)$ where $n_1 \in N$.

Therefore every element of $F(N)$ is both left and right invariant under translation by elements of N. For an arbitrary $a \in C(G)$ we then have:

$$(f * a)_n(x) = (f * a)(xn) = \int_G f(xny^{-1})a(y)dy = \int_G f(n_1xy^{-1})a(y)dy$$
$$= (f * a)(x) \qquad \text{for all } x \in G$$

$F(N)$ is then a right ideal and therefore a two sided ideal in $C(G)$.

Suppose now that H is non-normal. Then $gH \neq Hg$ for some $g \in G$. We can assume that there is $h \in H$ such that $hg \notin gH$. (Otherwise there would be $h_1 \in H$ such that $gh_1 \notin Hg$ or $h_1g^{-1} \notin g^{-1}H$, and we could take h_1 and g^{-1} in place of h and g.) Then $hgH \cap gH = 0$. We shall exhibit functions $f \in F(H)$ and $a \in C(G)$ such that $f * a \notin F(H)$. It will follow that $F(H)$ is not a two-sided ideal in $C(G)$. Again we distinguish two cases.

(a) $\mu(H) > 0$. The sets gH and Hg^{-1} are both open and closed. Let f be the characteristic function of gH and a be the characteristic function of Hg^{-1}. Then $f \in F(H)$ and $a \in C(G)$.

Let us now consider $f_1(y) = f(hy^{-1})a(y)$ as a function of y. Plainly f_1 is continuous. If $y \in Hg^{-1}$ then $hy^{-1} \in hgH$ and $f(hy^{-1}) = 0$, since $hgH \cap gH = 0$. Therefore $f_1(y) = 0$ for $y \in Hg^{-1}$. However, for $y \notin Hg^{-1}$, $a(y) = 0$ and again $f_1(y) = 0$. We see that

$$(3) \qquad (f * a)(h) = \int_G f(hy^{-1})a(y)dy = 0 .$$

On the other hand, using the function $f_2(y) = f(y^{-1})a(y)$, we see that $f_2 \in C(G), f_2 \geqq 0$ and $f_2(g^{-1}) = f(g)a(g^{-1}) = 1$. Since the Haar integral is strictly positive on $C(G)$ we conclude that

$$(4) \qquad (f * a)(e) = \int_G f(y^{-1})a(y)dy > 0 .$$

Comparison of (3) and (4) shows that $f * a$ is not constant on H. Therefore it cannot belong to $F(H)$.

(b) $\mu(H) = 0$. Since G/H is Hausdorff and normal, there are disjoint open neighborhoods U_1 and U_2 of gH and hgH respectively. In view of the complete regularity of G/H, we can find $f' \in C(G/H)$ such that $f' \geqq 0, f'(gH) = 1$, and f' vanishes on the (closed) complement of U_1 in G/H, which contains in particular the open neighborhood U_2 of hgH.

Defining $f(x) = f'(xH)$, we obtain a non-negative function $f \in F(H)$ assuming the value 1 on gH and vanishing on an open set U (the preimage of U_2 under the mapping $x \to xH$) containing hg. We now choose a symmetric open neighborhood V of e such that $hgV \subset U$ and a non-negative function $a \in C(G)$ assuming the value 1 at g^{-1} and vanishing

outside the open set Vg^{-1}. This choice again is possible by the complete regularity of G.

We again consider the continuous function $f_1(y) = f(hy^{-1})a(y)$. For $y \in Vg^{-1}$ we have $hy^{-1} \in hgV \subset U$ so that $f(hy^{-1}) = 0$ and $f_1(y) = 0$. On the other hand, $y \notin Vg^{-1}$ implies $a(y) = 0$ and $f_1(y) = 0$. So

$$(3') \qquad (f * a)(h) = \int_G f(hy^{-1})a(y)dy = 0 .$$

Considering $f_2(y) = f(y^{-1})a(y)$, we see that $f_2 \geqq 0, f_2 \in C(G)$ and $f_2(g^{-1}) = f(g)a(g^{-1}) = 1 > 0$. Therefore

$$(4') \qquad (f * a)(e) = \int_G f(y^{-1})a(y)dy > 0 .$$

Comparing (3') and (4'), we see again that $f * a$ is not constant on H and does not belong to $F(H)$.

As a result we obtain

LEMMA 4. *A subgroup H of G is normal if and only if $F(H)$ is a two sided ideal in $C(G)$.*

The correspondence between $F(M)$ and $H(M)$ for arbitrary subsets $M \subset G$ leads yet to another useful result.

LEMMA 5. *Let M_1 and M_2 be any subsets of G. Then $M_2 \subset H(M_1)$ if and only if $F(M_1 \cup M_2) = F(M_1)$.*

Proof. Assume first $M_2 \subset H(M_1)$. Then $H(M_1 \cup M_2) = H(M_1)$ and by Lemma 2, we have

$$F(M_1 \cup M_2) = F(H(M_1 \cup M_2)) = F(H(M_1)) = F(M_1) .$$

Let us now assume that $F(M_1 \cup M_2) = F(M_1)$. It is clear that $F(M_2) \supset F(M_1 \cup M_2)$. Using Lemma 2, we get $F(H(M_2)) \supset F(H(M_1))$ and by Lemma 3 $M_2 \subset H(M_2) \subset H(M_1)$.

Lemma 5 states in particular that an element $m \in G$ can be approximated by finite products of positive powers of elements in M if and only if the set of all function of $C(G)$ which are invariant under right translation by all elements of M is not reduced by joining m to M.

Taking $M_2 = G$, we obtain as a necessary and sufficient condition for the set M_1 to generate G that $F(M_1)$ be the set of all constant functions on G.

Taking for M_1 a subset of a given subgroup $H = M_2$, Lemma 5 states that M_1 generates H if and only if $F(M_1) = F(H)$.

4. Irreducible representations of G. We now list some definitions

and facts concerning representations which we shall have to use in the following.[4]

Let $\{R^{(\lambda)}: \lambda \in \Lambda\}$ be a complete system of inequivalent irreducible unitary continuous representations of G of degrees r_λ respectively. Let $R^{(\lambda)}(s)$ be the matrix associated with the element s in $R^{(\lambda)}$ for a given basis in the corresponding vector space and $R^{(0)}$ the identity representation. Denoting by $u_{ik}^{(\lambda)} \in C(G)$ the coefficient in the ith row and kth column in $R^{(\lambda)}$, we have $u_{ik}^{(\lambda)}(s^{-1}) = \overline{u_{ki}^{(\lambda)}(s)}$ and

$$
\begin{aligned}
&\sum_{k=1}^{r_\lambda} u_{ik}^{(\lambda)}(s)\overline{u_{ik}^{(\lambda)}(s)} = \delta_{ij} \\
&\int_G u_{ij}^{(\lambda)}(x)\overline{u_{pq}^{(\lambda')}(x)}dx = \delta_{\lambda\lambda'}\delta_{ip}\delta_{jq} \cdot \frac{1}{r_\lambda} \qquad (5) \\
&u_{ij}^{(\lambda)} * u_{pq}^{(\lambda')} = \delta_{\lambda\lambda'}\delta_{jp} \cdot \frac{1}{r_\lambda} u_{iq}^{(\lambda)} ,
\end{aligned}
$$

since the $R^{(\lambda)}$ are unitary.

The functions $u_{ij}^{(\lambda)}$ are linearly independent and form a basis for the linear space $R(G)$ of all complex linear combinations

$$
l = \sum_{\lambda=\lambda_1}^{\lambda_n} \sum_{i,k=1}^{r_\lambda} \alpha_{ik}^{(\lambda)} u_{ik}^{(\lambda)} , \qquad \alpha_{ik}^{(\lambda)} \in C . \tag{6}
$$

(5) shows that $R(G)$ is a subalgebra of $C(G)$. The Peter-Weyl theorem says that $R(G)$ is dense in $C(G)$ under the uniform norm. More specifically[5], every $f \in C(G)$ can be uniformly approximated by functions of the form

$$
l = \sum_{\lambda=\lambda_1}^{\lambda_n} \alpha_\lambda \sum_{i=1}^{r_\lambda} (u_{ii}^{(\lambda)} * f) \tag{7}
$$

which belong to $R(G)$ as shown below.

Using the notation $(a, b) = \int_G a(x)\overline{b(x)}dx$ for $a \in C(G), b \in C(G)$ we have, as can be verified easily,

$$
u_{ik}^{(\lambda)} * f = \sum_{j=1}^{r_\lambda} (f, u_{kj}^{(\lambda)}) u_{ij}^{(\lambda)} \in R(G) \tag{8}
$$

$$
f * u_{ik}^{(\lambda)} = \sum_{j=1}^{r_\lambda} (f, u_{ji}^{(\lambda)}) u_{jk}^{(\lambda)} \in R(G) . \tag{9}
$$

From (5) and (8) we can conclude that for fixed λ and i the functions $u_{ik}^{(\lambda)}$ $(k = 1, 2, \cdots, r_\lambda)$ form a basis for a minimal right ideal $R_i^{(\lambda)}$ of $R(G)$

[4] See [5] §§ 39, 40.

[5] See [5] Theorem 39D. As pointed out be Prof. Edwin Hewitt in a lecture, one can choose the approximate identity in the center of $C(G)$ by taking $u(x) = \int_G v(y^{-1}xy)dy$ and having $v \in C(G)$ $(v \geqq 0)$ vanish outside a sufficiently small neighborhood of e.

and $C(G)$. Analogously it follows from (5) and (9) that for fixed λ and k, the functions $u_{ik}^{(\lambda)}$ $(i = 1, 2, \cdots, r_\lambda)$ form a basis for a minimal left ideal $L_k^{(\lambda)}$ of $R(G)$ and $C(G)$. Finally it follows from (5), (8) and (9) that for fixed λ the functions $u_{ik}^{(\lambda)}$ $(i, k = 1, 2, \cdots, r_\lambda)$ form a basis for a minimal two sided ideal $T^{(\lambda)}$ in $R(G)$ and $C(G)$. Each of these ideals is closed because of its finite dimensionality.

Taking $l \in R(G)$ as in (6) we have

$$
\begin{aligned}
u_{ii}^{(\lambda)} * l &= \frac{1}{r_\lambda} \sum_{k=1}^{r_\lambda} \alpha_{ik}^{(\lambda)} u_{ik}^{(\lambda)} \in R_i^{(\lambda)} \\
l * u_{kk}^{(\lambda)} &= \frac{1}{r_\lambda} \sum_{i=1}^{r_\lambda} \alpha_{ik}^{(\lambda)} u_{ik}^{(\lambda)} \in L_k^{(\lambda)} \qquad (10) \\
\left[\sum_{i=1}^{r_\lambda} u_{ii}^{(\lambda)}\right] * l &= \frac{1}{r_\lambda} \sum_{i,k=1}^{r_\lambda} \alpha_{ik}^{(\lambda)} u_{ik}^{(\lambda)} \in T^{(\lambda)}
\end{aligned}
$$

and

$$
\begin{aligned}
l &= \sum_{\lambda=\lambda_1}^{\lambda_r} r_\lambda \sum_{i=1}^{r_\lambda} (u_{ii}^{(\lambda)} * l) = \sum_{\lambda=\lambda_1}^{\lambda_r} r_\lambda \sum_{k=1}^{r_\lambda} (l * u_{kk}^{(\lambda)}) \qquad (11) \\
&= \sum_{\lambda=\lambda_1}^{\lambda_r} r_\lambda \left[\left(\sum_{i=1}^{r_\lambda} u_{ii}^{(\lambda)}\right) * l\right].
\end{aligned}
$$

We see that $R(G)$ is the direct sum of the minimal two sided ideals $T^{(\lambda)}$ which in turn are direct sums of minimal right ideals $R_i^{(\lambda)}$ and, in the same way, of minimal left ideals $L_k^{(\lambda)}$.

$$
\begin{aligned}
R(G) &= \sum_{\lambda \in \Lambda} \oplus T^{(\lambda)} \qquad (12) \\
T^{(\lambda)} &= \sum_{i=1}^{r_\lambda} \oplus R_i^{(\lambda)} = \sum_{k=1}^{r_\lambda} \oplus L_k^{(\lambda)} .
\end{aligned}
$$

$R(G)$ is itself a two sided ideal in $C(G)$ but is not closed unless it coincides with $C(G)$. (This occurs if and only if G is finite).

The numbers $(f, u_{ik}^{(\lambda)})$ appearing in (8) and (9) can be regarded as the Fourier coefficients of the function $f \in C(G)$. For non-zero f there exist only a countable number of non-zero Fourier coefficients (and at least one).

Every element $a = \sum_{k=1}^{r_\lambda} \alpha_k u_{ik}^{(\lambda)} \in R_i^{(\lambda)}$ can be written in vector notation as a scalar product $\mathfrak{u}_i^{(\lambda)}\mathfrak{a}$ where $\mathfrak{u}_i^{(\lambda)}$ stands for the basis vector $(u_{i1}^{(\lambda)}, u_{i2}^{(\lambda)}, \cdots, u_{ir_\lambda}^{(\lambda)})$ and $\mathfrak{a}$ for the coefficient vector $(\alpha_1, \alpha_2, \cdots, \alpha_{r_\lambda})$, written as column vector. By the definition of $u_{ik}^{(\lambda)}$ we obtain under right translation by any $s \in G$

$$
\begin{aligned}
[u_{ik}^{(\lambda)}]_s(x) &= u_{ik}^{(\lambda)}(xs) = \sum_{j=1}^{r_\lambda} u_{ij}^{(\lambda)}(x) u_{jk}^{(\lambda)}(s) \quad \text{or} \qquad (13) \\
\mathfrak{u}_{i_s}^{(\lambda)} &= \mathfrak{u}_i^{(\lambda)} \cdot R^{(\lambda)}(s) .
\end{aligned}
$$

Right translation by s evidently induces a linear transformation in $R_i^{(\lambda)}$ whose matrix with respect to $\mathfrak{u}_i^{(\lambda)}$ as a basis is just $R^{(\lambda)}(s)$, and $R_i^{(\lambda)}$ is invariant under right translation. For any function $a \in R_i^{(\lambda)}$, the effect of the translation is given by the formulas

$$a_s = \mathfrak{u}_{i_s}^{(\lambda)}\mathfrak{a} = \mathfrak{u}_i^{(\lambda)}R^{(\lambda)}(s)\mathfrak{a} = \mathfrak{u}_i^{(\lambda)}\mathfrak{a}_s \tag{14}$$
$$\mathfrak{a}_s = R^{(\lambda)}(s)\mathfrak{a}$$

where $\mathfrak{a}_s$ is the coefficient vector of a_s.

5. Generating sets in G and irreducible representations of G. We investigate for a given subgroup H of G the intersection of $F(H)$ with the ideals of $R(G)$, introduced above. If $f \in F(H)$ and $f \neq 0$, then $(f, u_{ik}^{(\lambda)}) \neq 0$ for some λ, i, k. The function

$$u_{ii}^{(\lambda)} * f = \sum_{j=1}^{r_\lambda} (f, u_{ij}^{(\lambda)})u_{ij}^{(\lambda)}$$

is different from zero, lies in $F(H)$, and by (8) also in $R(G)$ (in fact in $R_i^{(\lambda)}$), therefore in $F'(H) = F(H) \cap R(G)$ (also in $F(H) \cap R_i^{(\lambda)}$). $F'(H)$ is again a left ideal in $C(G)$ since $R(G)$ is a two sided ideal in $C(G)$ and contains all functions of the form $u_{ii}^{(\lambda)} * f$ for a given $f \in F(H)$. From (7), we obtain as an immediate consequence

LEMMA 6. *$F'(H) = F(H) \cap R(G)$ is dense in $F(H)$.*

Let now $f' \in F'(H)$. By (11), f' can be written as a linear combination of functions of the form $u_{ii}^{(\lambda)} * f$ which are by (10) contained in $F(H) \cap R_i^{(\lambda)}$. On the other hand, every linear combination of functions in $F(H) \cap R_i^{(\lambda)}$ is again a function of $F'(H)$. On account of the direct decomposition of $R(G)$ with respect to the minimal right ideals $R_i^{(\lambda)}$, we see that $F'(H)$ is, as a linear space, the direct sum of the linear spaces $F(H) \cap R_i^{(\lambda)}$,

$$F'(H) = \sum_{\lambda \in \Lambda} \oplus \sum_{i=1}^{r_\lambda} \oplus [F(H) \cap R_i^{(\lambda)}] \tag{15}$$

some of which may consist only of zero.

Let now $F(H) \cap R_i^{(\lambda)}$ be non-zero (we have already seen that there must be at least one non-zero $F(H) \cap R_i^{(\lambda)}$) and let $f_i^{(\lambda)} \in F(H) \cap R_i^{(\lambda)}$. We can write $f_i^{(\lambda)}$ as a scalar product of the basis vector $\mathfrak{u}_i^{(\lambda)}$ of $R_i^{(\lambda)}$ and the coefficient vector $\mathfrak{f}^{(\lambda)}$

$$f_i^{(\lambda)} = \mathfrak{u}_i^{(\lambda)}\mathfrak{f}^{(\lambda)} . \tag{16}$$

The function $f_i^{(\lambda)}$ is invariant under right translation by all elements $h \in H$. In view of (14) this means that

$$\mathfrak{f}^{(\lambda)} = R^{(\lambda)}(h)\mathfrak{f}^{(\lambda)} \text{ for all } h \in H \tag{17}$$

i.e., $\mathfrak{f}^{(\lambda)}$ is an eigenvector of $R^{(\lambda)}(h)$ with eigenvalue 1 for all $h \in H$. Conversely, for fixed λ, every eigenvector with eigenvalue 1 common to all $R^{(\lambda)}(h)$ ($h \in H$) determines by (16) a function $f_i^{(\lambda)} \in F(H) \cap R_i^{(\lambda)}$.

Since for a given i, λ linear independence of functions $f_i^{(\lambda)}, g_i^{(\lambda)}$ is equivalent to linear independence of the corresponding coefficient vectors $\mathfrak{f}^{(\lambda)}, \mathfrak{g}^{(\lambda)}$ we see that the dimension of $F(H) \cap R_i^{(\lambda)}$ as a linear space is precisely the number of linearly independent eigenvectors $\mathfrak{f}^{(\lambda)}$ common to all $R^{(\lambda)}(h)$ ($h \in H$) with eigenvalue 1.

DEFINITION 2. For any non-void subset M of G and for any fixed λ, let $d^{(\lambda)}(M)$ denote the maximal number of linearly independent eigenvectors common with eigenvalue 1 to $R^{(\lambda)}(m)$ for all $m \in M$.

The inequalities $0 \leqq d^{(\lambda)}(M) \leqq r_\lambda$ necessarily hold. In the present case, we see that $d^{(\lambda)}(H)$ is the dimension of $F(H) \cap R_i^{(\lambda)}$ for all $i = 1, 2, \cdots, r_\lambda$ since it obviously does not depend on i. Taking $d^{(\lambda)}(H)$ linearly independent functions of $F(H) \cap R_i^{(\lambda)}$ and $r - d^{(\lambda)}(H)$ properly chosen $u_{ik}^{(\lambda)}$ (i, λ fixed) as a basis for $R_i^{(\lambda)}$ amounts to transforming the representation $R^{(\lambda)}$ to an equivalent one, $R'^{(\lambda)} = S^{-1}R^{(\lambda)}S$, in which $R'^{(\lambda)}$ restricted to the elements of H, becomes reducible as representation of H and is found to contain the identity-representation of H exactly $d^{(\lambda)}(H)$ times. Thus $d^{(\lambda)}(H)$ can also be defined an the multiplicity with which the identity representation of H is contained in $R^{(\lambda)}$, restricted to the elements of H and considered as a representation of H.

$F(H) \cap R_i^{(\lambda)}$ has the dimension $d^{(\lambda)}(H)$ for given λ, as we have seen. The subspace $F(H) \cap T^{(\lambda)}$ is the direct sum of all $F(H) \cap R_i^{(\lambda)}$ ($i=1, 2, \cdots, r_\lambda$) and has therefore dimension $r_\lambda d^{(\lambda)}(H)$. If there is only a finite number of non-zero $d^{(\lambda)}(H)$, then there are only a finite number of non-zero $F(H) \cap R_i^{(\lambda)}$ and $F(H) \cap T^{(\lambda)}$. By (15), we see that $F'(H)$ is a linear space of dimension $\sum_{\lambda \in \Lambda} r_\lambda d^{(\lambda)}(H)$ which is finite-dimensional, and therefore $F'(H)$ is closed. But then $F'(H) = F(H)$ by Lemma 6, and $F(H)$ is of finite dimension $\sum_{\lambda \in \Lambda} r_\lambda d^{(\lambda)}(H)$. If infinitely many $d^{(\lambda)}(H)$ are non-zero then $F'(H)$ is an infinite dimensional linear space and the same must be true of $F(H)$. Combining this result with the results of Theorem 1, we obtain:

THEOREM 2. *If $d^{(\lambda)}(H)$ is the multiplicity with which the identity representation of a subgroup H of G is contained in $R^{(\lambda)}$, restricted to the elements of H and considered as a representation of H, then*

$$\sum_{\lambda \in \Lambda} r_\lambda d^{(\lambda)}(H) = \frac{1}{\mu(H)} \qquad \text{if } \mu(H) > 0 .$$

If $\mu(H) = 0$ then the series $\sum_{\lambda \in \Lambda} r_\lambda d^{(\lambda)}(H)$ diverges.

The sum $\sum_{\lambda\in\Lambda} r_\lambda d^{(\lambda)}(H)$ can therefore be considered as giving the "index" of H in G. A subgroup H has measure 0 if and only if $d^{(\lambda)}(H) > 0$ for infinitely many $\lambda \in \Lambda$.

Let N be a normal subgroup of G and $d^{(\lambda)}(N) > 0$ for a certain λ. Then $F(N) \cap R_i^{(\lambda)}$ contains a non-zero function $f = \sum_{k=1}^{r_\lambda} \alpha_k u_{ik}$. Assume that $\alpha_l \neq 0$. The set $F(N)$ is a two sided ideal by Lemma 4, and so is $F'(N) = F(N) \cap R(G)$. Therefore $F'(N)$ contains together with f the function

$$f * u_{lj}^{(\lambda)} = \frac{\alpha_l}{r_\lambda} u_{ij}^{(\lambda)} \text{ for arbitrary } j\,, \qquad 1 \leqq j \leqq r_\lambda\,.$$

This means that $R_i^{(\lambda)} \subset F'(N)$ and $d^{(\lambda)}(N) = r_\lambda$. On the other hand, supposing that for a given subgroup H $d^{(\lambda)}(H)$ assumes only the values 0 or r_λ for all $\lambda \in \Lambda$, we see that $F(H) \cap R_i^{(\lambda)}$ is either zero or $R_i^{(\lambda)}$. Then $F(H) \cap T^{(\lambda)}$ is either zero or $T^{(\lambda)}$ and $F'(H)$ is the direct sum of two sided ideals and itself a two sided ideal in $C(G)$. Its closure $F(H)$ must also be two sided and by Lemma 4, H is normal.

THEOREM 3. *A subgroup H of G is normal if and only if $d^{(\lambda)}(H)$ assumes only the values 0 or r_λ for all $\lambda \in \Lambda$.*[6]

Trivial illustrations of this fact are given by the entire group G ($d^{(0)}(G) = 1$ and $d^{(\lambda)}(G) = 0$ for $\lambda \neq 0$) and by the group consisting of $\{e\}$ only ($d^{(\lambda)}(e) = r_\lambda$ for all $\lambda \in \Lambda$).

We proceed now to characterize the generating properties of an arbitrary subset M of G by means of the representations $R^{(\lambda)}$. Since $M \subset H(M)$, there are by the definition of $d^{(\lambda)}(H(M))$ at least $d^{(\lambda)}(H(M))$ linearly independent functions in $R_i^{(\lambda)}$ that are invariant under right translation by all elements of M and $d^{(\lambda)}(M) \geqq d^{(\lambda)}(H(M))$. Conversely, as seen in the proof of Lemma 2, any such function of $R_i^{(\lambda)}$ is also invariant under right translation by all elements of $H(M)$ and $d^{(\lambda)}(M) \leqq d^{(\lambda)}(H(M))$. Together with the previous result, we now have

LEMMA 7. *If M is an arbitrary subset of G, then $d^{(\lambda)}(M) = d^{(\lambda)}(H(M))$ for all $\lambda \in \Lambda$.*

The main result which we can now prove is

THEOREM 4. *If M_1 and M_2 are arbitrary subsets of G, then $M_2 \subset H(M_1)$ if and only if $d^{(\lambda)}(M_1 \cup M_2) = d^{(\lambda)}(M_1)$ for all $\lambda \in \Lambda$.*

Proof. Let $M_2 \subset H(M_1)$. Then $H(M_1) = H(M_1 \cup M_2)$ and $d^{(\lambda)}(M_1) = d^{(\lambda)}(M_1 \cup M_2)$ for all $\lambda \in \Lambda$ by Lemma 7. On the other hand, the

[6] See also [4] and [1] Theorem 1.

equality $d^{(\lambda)}(M_1) = d^{(\lambda)}(M_1 \cup M_2)$ for all $\lambda \in \Lambda$ implies by Lemma 7 that

$$F(H(M_1)) \cap R_i^{(\lambda)} = F(H(M_1 \cup M_2)) \cap R_i^{(\lambda)} \text{ for all } \lambda \in \Lambda ,$$

$$F(H(M_1)) \cap T^{(\lambda)} = F(H(M_1 \cup M_2)) \cap T^{(\lambda)} \text{ for all } \lambda \in \Lambda ,$$

$$\begin{aligned} F'(H(M_1)) &= F(H(M_1)) \cap R(G) = F(H(M_1 \cup M_2)) \cap R(G) \\ &= F'(H(M_1 \cup M_2)) \text{ (by (15))} , \end{aligned}$$

$$F(H(M_1)) = F(H(M_1 \cup M_2)) \text{ (by Lemma 6) and}$$
$$M_2 \subset H(M_1) \text{ (by Lemmas 2 and 5)} .$$

A number of corollaries are easily obtained. Putting $M_2 = G$ in Theorem 4 and noting that $d^{(\lambda)}(G)$ is positive only for $\lambda = 0$ we obtain

COROLLARY 4.1. *The subset M of G generates G if and only if $d^{(\lambda)}(M) = 0$ for all $\lambda \neq 0$.*

Taking as M_2 a subgroup H and as M_1 a subset M of H, we get

COROLLARY 4.2. *The subset M of the subgroup H of G generates H if and only if $d^{(\lambda)}(M) = d^{(\lambda)}(H)$ for all $\lambda \in \Lambda$.*

Finally, combining the results of Theorem 2, 3 and Lemma 7, we obtain

COROLLARY 4.3. *The subset M of G generates a normal subgroup of G if and only if $d^{(\lambda)}(M)$ assumes only the values 0 and r_λ for all $\lambda \in \Lambda$. If $d^{(\lambda)}(M) > 0$ for only a finite number of $\lambda \in \Lambda$, then M generates a subgroup of measure $1/\sum_{\lambda \in \Lambda} r_\lambda d^{(\lambda)}(M)$; otherwise M generates a subgroup of measure 0.*

6. Finite generating sets in G. The preceding results are in particular valid for finite groups. In that case we are only concerned with the investigation of generating properties of finite sets of elements. Schreier and Ulam[7] have shown that a connected compact metric group G is generated by almost every pair of elements. Since the component of the identity in any compact group G is a connected normal subgroup of finite index in G, it is clear that there are always a finite number of generators for a compact metric group.

For the case of a finite set M, there is a simple way to determine $d^{(\lambda)}(M)$ and to state the conditions of the last theorems and corollaries, based on the following lemma.

LEMMA 8. *Let $B^{(\lambda)}(m_1, \cdots, m_s)$ be the rectangular matrix with r_λ rows and sr_λ columns obtained by joining horizontally the s matrices $R^{(\lambda)}(m_k) - R^{(\lambda)}(e)$ $(k = 1, 2, \cdots, s)$. Let $b^{(\lambda)}(m_1, \cdots, m_s)$ be the rank of*

[7] See [7] and [8].

$B^{(\lambda)}(m_1, \cdots, m_s)$. *Then* $d^{(\lambda)}(\{m_k : k = 1, \cdots, s\}) = r_\lambda - b^{(\lambda)}(m_1, \cdots, m_s)$.

Since this Lemma has been stated by the author in [1] without proof it may be suitable to set down a proof here.

Proof. Let $B^{*(\lambda)}(m_1, \cdots, m_s)$ be the conjugate transpose of $B^{(\lambda)}(m_1, \cdots, m_s)$. Its rank is the same as that of $B^{(\lambda)}(m_1, \cdots, m_s)$. Since $R^{(\lambda)}$ is unitary, $B^{*(\lambda)}(m_1, \cdots, m_s)$ could have been obtained by placing the s matrices $R^{(\lambda)}(m_k^{-1}) - R^{(\lambda)}(e)$ $(k = 1, \cdots, s)$ below each other. Since $d^{(\lambda)}(\{m_k : k = 1, \cdots, s\}) = d^{(\lambda)}(\{m_k^{-1} : k = 1, \cdots, s\})$ we have to show that the rank of $B^{*(\lambda)}(m_1, \cdots, m_s)$ is equal to $r_\lambda - d^{(\lambda)}(\{m_k^{-1} : k = 1, \cdots, s\})$. In order to simplify the notation, we shall from now on omit the index λ and the indication of the group elements when possible.

If we denote by A_s the $rs \times rs$ matrix obtained by placing the non-singular $r \times r$ matrix, A, s times along the principal diagonal in a $rs \times rs$ zero-matrix, then A_s is non-singular and $A_s^{-1}B^*A$ has again rank b. If $\mathfrak{u} = (u_1, \cdots, u_r)$ is the basis of the r-dimensional linear space corresponding to the matrix-representation R, then the transition to a new basis $\mathfrak{u}'$ in which the d first basis vectors are invariant under the transformations corresponding to $m_1^{-1}, \cdots, m_s^{-1}$ is given by the formula $\mathfrak{u}P = \mathfrak{u}'$ where P is a non-singular $r \times r$ matrix. In the new basis these transformations are given by the matrices $P^{-1}R(m_k^{-1})P$. The d first columns in each of these have as their only non-zero elements 1's in the main diagonal. In each of the matrices $P^{-1}(R(m_k^{-1}) - R(e))P$ those columns are therefore zero columns. Placing those s matrices one below the other we obtain, as one can readily see, exactly the matrix $P_s^{-1}B*P$. The rank of this matrix can therefore not exceed $r - d$ and we have $b \leqq r - d$.

Assume that $b < r - d$. Then one of the columns $C'_{d+1}, \cdots, C'_r$ in $P_s^{-1}B^*P$, say C'_c, would be a linear combination of the other ones. By a permutation of the vectors u_{d+1} and u_c in $\mathfrak{u}'$ given by $\mathfrak{u}'Q = \mathfrak{u}''$, where Q is the matrix of the corresponding permutation, we obtain as above a matrix $Q_s^{-1}P_s^{-1}B^*PQ$ with rank b in which the d first columns vanish and the $(d+1)$-th column appears as a linear combination of the remaining ones $C''_{d+1} = \sum_{j=d+2}^{r} \alpha_j C''_j$.

Define R as the matrix obtained from $R(e)$ by replacing in the $(d+1)$-th column the zeros below the principal diagonal by $-\alpha_{d+2}, \cdots, -\alpha_r$ in that order. Passing to a new basis by the formula $\mathfrak{u}''R = \mathfrak{u}'''$, we obtain as above the matrix $R_s^{-1}Q_s^{-1}P_s^{-1}B^*PQR$ in which, as one can see easily, the first $d+1$ columns vanish. But then the first $d+1$ columns in $(PQR)^{-1}R(m_k^{-1})PQR$ have as their only non-zero elements 1's in the main diagonal. This in turn means that the first $d+1$ basis vectors in $\mathfrak{u}'''$ are invariant under the transformations corresponding to all elements $m_k^{-1}(k = 1, \cdots, s)$. But this contradicts our assumption that there are

not more than d linearly independent vectors of that property. So $b = r - d$, and the lemma is proved.

Lemma 8 allows us to determine $d^{(\lambda)}(\{m_1, \cdots, m_s\})$ if the matrices $R^{(\lambda)}(m_k)(k = 1, \cdots, s)$ are given. Applying Lemma 8 to a single element m, we see that $d^{(\lambda)}(\{m\})$ is exactly the multiplicity of the eigenvalue 1 in $R^{(\lambda)}(m)$. If $R^{(\lambda)}(m)$ does not have 1 as an eigenvalue, then $b^{(\lambda)}(m) = r_\lambda$.

Using Lemma 8, we can also reformulate the preceding results. *e.g.* Corollary 4.1 takes the following form: the elements $m_1, \cdots, m_s$ generate G if and only if $b^{(\lambda)}(m_1, \cdots, m_s) = r_\lambda$ for $\lambda \neq 0$. This condition is in particular satisfied if for every $\lambda \neq 0$ there is at least one $m^{(\lambda)}$ among the $m_1 \cdots m_s$ for which $R^{(\lambda)}(m^{(\lambda)})$ does not have 1 as an eigenvalue. In this case, however, we can even say that the products of the form $m_1^{a_1} \cdots m_s^{a_s}$ $(0 \leqq a_k : k = 1, \cdots, s)$ are dense in G and, arranged in a certain order, form a sequence which is equidistributed in G.[8] Similarly we can see that the hypothesis of Corollary 4.2 is satisfied if for every $\lambda \in \Lambda$ there is at least one $m^{(\lambda)}$ such that the multiplicity of the eigenvalue 1 in $R^{(\lambda)}(m^{(\lambda)})$ is exactly $d^{(\lambda)}(H)$, i.e., the multiplicity with which $R^{(\lambda)}$ restricted to H contains the identity-representation of H. Again in this case we can make the stronger statement that the products of the form $m_1^{a_1} \cdots m_s^{a_s}$ $(0 \leqq a_k : k = 1, \cdots, s)$ are dense in H and, arranged in a certain order, form a sequence which is equidistributed in H.

REFERENCES

1. A. H. Clifford, *Representations induced in an invariant subgronp*, Annals of Math., **38** No. 3 (1937), 533-550.

2. G. Helmberg, *Strukturbeziehungen zwischen endlicher Gruppe, Gruppenring und irreduziblen Darstellungen*, Monatshefte fuer Math. Wien, **58** (1954), 241-257.

3. ———, *A theorem on equidistribution in compact groups*, Pacific J. Math., **8** (1958), 227-241.

4. A. Kulakoff, Rec. Math. Soc. Moscow **36** (1929), 129-134.

5. L. Loomis, *An Introduction to Abstract Harmonic Analysis*, van Nostrand, New York, 1953.

6. Katsumi Numakura, *On bicompact semigroups*, Math. Journal of Okayama Univ. **1** (1952), 99-108.

7. T. Schreier and L. Ulam, *Sur le nombre des generateurs d'un groupe topologique compact et connexe*, Fund. Math. **24** (1935), 302-304.

8. ———, *Eine Bemerkung ueber Erzeugende in kompakten Gruppen*, Fund. Math. **25** (1925), 198-199.

TULANE UNIVERSITY

[8] See [3].