Pacific Journal of Mathematics

A THEOREM ON EQUIDISTRIBUTION ON COMPACT GROUPS

GILBERT HELMBERG

Vol. 8, No. 2 April 1958

A THEOREM ON EQUIDISTRIBUTION IN COMPACT GROUPS

GILBERT HELMBERG

1. Preliminaries. Throughout the discussions in the following sections, we shall assume that G is a compact topological group whose space is T_1 with an identity element e and with Haar-measure μ normalized in such a way that $\mu(G)=1$. G has a complete system of inequivalent irreducible unitary representations[1] $R^{(\lambda)}(\lambda \in \Lambda)$ where $R^{(1)}$ is the identity-representation and r_λ is the degree of $R^{(\lambda)}$. $R^{(\lambda)}(e)$ will then denote the identity matrix of degree r_λ.

The concept of equidistribution of a sequence of points was introduced first by H. Weyl [6] for the direct product of circle groups. It has been transferred to compact groups by B. Eckmann [1] and highly generalized by E. Hlawka [4][2]. We shall use it in the following from:

DEFINITION 1. Let[1] $\{x_\nu : \nu \in \omega\}$ be a sequence of elements in G and let, for any closed subset M of G, $N(M)$ be the number of elements in the set $\{x_\nu : x_\nu \in M,\ \nu \leqq N\}$.

The sequence $\{x_\nu : \nu \in \omega\}$ is said to be *equidistributed in* G if

$$\lim_{N\to\infty} \frac{N(M)}{N} = \mu(M) \tag{1}$$

for all closed subsets M of G, whose boundaries have measured 0.

It is easy to see that a sequence which is equidistributed in G is also dense in G. As Eckmann has shown for compact groups with a countable base, and E. Hlawka for compact groups in general, the equidistribution of a sequence in G can be stated by means of the system $\{R^{(\lambda)} : \lambda \in \Lambda\}$ of representations of G.

LEMMA 1. *The sequence* $\{x_\nu : \nu \in \omega\}$ *is equidistributed in* G *if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\nu=1}^{N} R^{(\lambda)}(x_\nu) = 0 \qquad \text{for all } \lambda \neq 1\,. \tag{1'}$$

Using this lemma, Eckmann arrives at the following theorem.

Received May 27, 1957. Presented at the 535th meeting of the Amer. Math. Soc. in Berkeley, Calif., April 20, 1957.

[1] In the following Λ and Λ' always denote any index-set, finite, countable, or uncountable, and ω denotes the set of positive integers $1, 2, \cdots$.

[2] Professor Hlawka has also noted in a letter to me that in order to secure the validity of Theorem 7 in [1] the lemma and footnote preceding it, it is necessary to change the definition of equidistribution into the form given below.

THEOREM 1. *Let g be an element of G such that*

$$|R^{(\lambda)}(g) - R^{(\lambda)}(e)| \neq 0 \qquad \text{for all } \lambda \neq 1 .$$

Then the sequence $\{g^\nu : \nu \in \omega\}$ is equidistributed in G.

It follows immediately that a group containing an element g with the above property is abelian and generated by a single element in the sense that the powers of g are dense in G. A group with the last property is called monothetic.

It is possible to extend this concept of generation of a group by one element to generation by a finite number of elements, that is, to ask for the smallest closed subgroup of G which contains a given finite set of elements of G (i. e., in which the set of all finite products of finite powers of these elements is dense).

DEFINITION 2. The finite set $\{g_k : k=1, 2, \cdots, n\}$ of elements of G is said to *generate the subgroup* H of G, if H is the smallest closed subgroup of G containing all g_k $(k=1, 2, \cdots, n)$.

Our subject in the following discussion will be a generalization of Eckmann's results in two directions indicated by that definition. First we shall try to find equidistributed sequences produced by finite set of elements in not necessarily commutative groups. In fact, the corresponding Theorem 2 will turn out to contain Theorem 1 as a special case. Furthermore we shall extend the definition of equidistribution in G to equidistribution in a subgroup of G.

DEFINITION 3. The sequence $\{x_\nu : \nu \in \omega\}$ of elements of a subgroup H is said to be *equidistributed in* H if it is equidistributed in the topological group H with respect to the relativized topology and with respect to the Haar-measure on the topological group H.

This definition is legitimate since H in the relativized topology is again a compact and T_1. Theorem 3 permits us to find sequences equidistributed in a subgroup of G and contains Theorem 2 as a special case.

In § 4 we compare our results with the results already known for finite groups which can be considered as compact groups in the discrete topology. Finally, we apply our results to abelian groups.

Before taking up this program, we state two rather obvious lemmas which will be helpful for deriving new equidistributed sequence from given ones. Clearly changing a finite number of elements of an equidistributed sequence has no influence on the property of being equidistributed.

LEMMA 2. *If the sequence $\{a_\nu : \nu \in \omega\}$ is equidistributed in G, then the sequence $\{a_\nu^{-1} : \nu \in \omega\}$ is also equidistributed in G.*

Proof. If M is an arbitrary closed subset of G whose boundary has measure 0, then M^{-1} is also closed its boundary has measure 0 and $\mu(M) = \mu(M^{-1})$ because of the fundamental properties of the Haar-measure μ. Let $N'(M)$ be the number of elements in the set $\{a_\nu : a_\nu \in M, r \leqq N\}$ and correspondingly $N''(M)$ the number of elements in $\{a_\nu^{-1} : a_\nu^{-1} \in M, \nu \leqq N\}$. Then $N''(M) = N'(M^{-1})$ and

$$\lim_{N\to\infty} \frac{N'(M^{-1})}{N} = \mu(M^{-1})$$

which holds because of our assumption for $\{a_\nu : \nu \in \omega\}$ is equivalent with

$$\lim_{N\to\infty} \frac{N''(M)}{N} = \mu(M) .$$

Therefore $\{a_\nu^{-1} : \nu \in \omega\}$ is equidistributed in G.

LEMMA 3. *If the sequences* $\{a_\nu : \nu \in \omega\}$ *and* $\{b_\nu : \nu \in \omega\}$ *are equidistributed in* G, *then the sequence* $\{c_\nu : c_{2\nu-1} = a_\nu, c_{2\nu} = b_\nu, \nu \in \omega\}$ *is also equidistributed in* G.

Proof. Define $N'(M)$, $N''(M)$ and $N(M)$ respectively for the sequences $\{a_\nu : \nu \in \omega\}$, $\{b_\nu : \nu \in \omega\}$ and $\{c_\nu : \nu \in \omega\}$ as above. For any positive integer N, let N_1 be the greatest integer in $(N+1)/2$ and let $N_2 = N - N_1$ (N_1 and N_2 are just the numbers of a's and b's among the first N c's). Then

$$\frac{N(M)}{N} = \frac{N_1'(M) + N_2''(M)}{N_1 + N_2} = \frac{N_1'(M)}{N} + \frac{N_2''(M)}{N} .$$

Starting from our assumption about $\{a_\nu : \nu \in \omega\}$ and $\{b_\nu : \nu \in \omega\}$ it is easy to show that

$$\lim_{N\to\infty} \frac{N_1'(M)}{N} = \lim_{N\to\infty} \frac{N_2''(M)}{N} = \frac{\mu(M)}{2}$$

for any closed subset M of G whose boundary has measure 0. But this implies (1) and the equidistribution of $\{c_\nu : \nu \in \omega\}$.

2. Non-commutative groups. A first generalization of Eckmann's Theorem 1 is given by the following.

THEOREM 2. *Let* g_k $(k = 1, 2, \cdots, n)$ *be* n *elements of* G *such that for each* $\lambda \neq 1$ *there is at least one* $g_{\bar{k}}$ *for which*

$$|R^{(\lambda)}(g_{\bar{k}}) - R^{(\lambda)}(e)| \neq 0 .$$

Then the set of elements[3]

$$G' = \{g' : g' = g_1^{i_1} g_2^{i_2} \cdots g_n^{i_n},\ 0 \leqq i_k < \infty,\ k = 1, 2, \cdots, n\}$$

can be arranged in a sequence which is equidistributed in G.

Proof. We shall use Lemma 1. In order to simplify the notation of the proof, let us agree on the following. If A is the matrix (a_{ij}) then $||A||$ shall stand for the matrix $(|a_{ij}|)$, and if B is a matrix (b_{ij}) of the same degree r_λ as A then we shall write $||A|| \leqq ||B||$ for the simultaneous inequalities $|a_{ij}| \leqq |b_{ij}|$ for all i, j with $1 \leqq i, j \leqq r_\lambda$. The symbol $F^{(\lambda)}$ shall stand for the matrix of degree r_λ with the entries $f_{ij} = 1$ for all i, j with $1 \leqq i, j \leqq r_\lambda$. We can regard $||A||$ as matrix-norm for A for which the following relations hold (all matrices are of same degree r_λ).

$$
\begin{aligned}
||kA|| &= |k| \cdot ||A|| && (k \in K = \text{field of complex numbers}) \\
||A+B|| &\leqq ||A|| + ||B|| && \\
||AB|| &\leqq ||A|| \cdot ||B|| && \qquad (2) \\
||A|| \cdot ||B|| &\leqq ||C|| \cdot ||D|| && \text{if } ||A|| \leqq ||C|| \text{ and } ||B|| \leqq ||D|| \\
||A|| &\leqq aF^{(\lambda)} && \text{if } a \geqq \max\{|a_{ij}| : 1 \leqq i, j \leqq r_\lambda\} \\
(F^{(\lambda)})^m &= r_\lambda^{m-1} F^{(\lambda)} &&
\end{aligned}
$$

Furthermore we shall write $\Pi_{l=1}^{m} h_l$ for the ordered product $h_1 h_2, \cdots, h_m$ and $\sum_{j_l \leqq j_l \leqq \bar{j}_l}$ for

$$\sum_{j_1=\underline{j}_1}^{\bar{j}_1} \sum_{j_2=\underline{j}_2}^{\bar{j}_2}, \cdots, \sum_{j_m=\underline{j}_m}^{\bar{j}_m}$$

if it is clear that l goes from 1 to m.

In order to prove the theorem we first arrange the countable set G' in a sequence $\{g'_\nu : \nu \in \omega\}$ as follows, let g'_1 be e ($i_k = 0$ for $k = 1, 2, \cdots, n$); as the next $2^n - 1$ elements we take the products $\Pi_{k=1}^{n} g_k^{i_k}$ with $0 \leqq i_k \leqq 1$ ($k = 1, 2, \cdots, n$) and $\max\{i_k : k = 1, 2, \cdots, n\} = 1$ in any order. Then we take the $3^n - 2^n$ products $\Pi_{k=1}^{n} g_k^{i_k}$ with $0 \leqq i_k \leqq 2$ ($k = 1, 2, \cdots, n$) and $\max\{i_k : k = 1, 2, \cdots, n\} = 2$ in any order and so on.

The sequence so constructed $\{g'_\nu : \nu \in \omega\}$ contains all elements of G' and has the property that the first $(i+1)^n$ elements g'_ν ($\nu = 1, \cdots (i+1)^n$) are precisely all elements $\Pi_{k=1}^{n} g_k^{i_k}$ with $0 \leqq i_k \leqq i$, ($k = 1, 2, \cdots, n$). In order to show the equidistribution of this sequence in G we have to show that

[3] We allow any element of G to occur an arbitrary number of times in the set G' and similar sets formed below.

$$\lim_{N\to\infty}\frac{1}{N}\sum_{\nu=1}^{N}R^{(\lambda)}(g'_\nu)=0 \qquad \text{for all } \lambda\neq 1 \tag{3}$$

Let us assume that for a fixed $\lambda\neq 1$ the element $g_{\bar{k}}$ satisfies the condition

$$|R^{(\lambda)}(g_{\bar{k}})-R^{(\lambda)}(e)|\neq 0 \tag{4}$$

which means exactly that the matrix $R^{(\lambda)}(g_{\bar{k}})$ does not have the eigenvalue 1. For a given N let i be the greatest integer in $N^{1/n}-1$, such that

$$(i+1)^n\leqq N<(i+2)^n\ . \tag{5}$$

Then

$$\frac{1}{N}\sum_{\nu=1}^{N}R^{(\lambda)}(g'_\nu)=\frac{1}{N}\left[\sum_{\nu=1}^{(i+1)^n}R^{(\lambda)}(g'_\nu)+\sum_{\nu=(i+1)^n+1}^{N}R^{(\lambda)}(g'_\nu)\right]$$

where the second term in the square brackets vanishes if $N=(i+1)^n$; with the same qualification we have

$$\begin{aligned}\frac{1}{N}\sum_{\nu=1}^{N}R^{(\lambda)}(g'_\nu)&=\frac{1}{N}\left[\sum_{0\leqq i_k\leqq i}R^{(\lambda)}\Big(\prod_{k=1}^{n}g_k^{i_k}\Big)+\sum_{\nu=(i+1)^n+1}^{N}R^{(\lambda)}(g'_\nu)\right]\\&=\frac{(i+1)^n}{N}\left[\frac{1}{(i+1)^n}\sum_{0\leqq i_k\leqq i}R^{(\lambda)}\Big(\prod_{k=1}^{u}g_k^{i_k}\Big)+\frac{1}{(i+1)^n}\sum_{\nu=(i+1)^n+1}^{N}R^{(\lambda)}(g'_\nu)\right].\end{aligned} \tag{6}$$

Let us now consider separately the terms in the square brackets.

(a) Because of well-known properties of matrices and group-representations we can write

$$\begin{aligned}\frac{1}{(i+1)^n}\sum_{0\leqq i_k\leqq i}R^{(\lambda)}\Big(\prod_{k=1}^{n}g_k^{i_k}\Big)&=\frac{1}{(i+1)^n}\sum_{0\leqq i_k\leqq i}\prod_{k=1}^{n}[R^{(\lambda)}(g_k)]^{i_k}\\&=\prod_{k=1}^{n}\left\{\frac{1}{i+1}\sum_{i_k=0}^{i}[R^{(\lambda)}(g_k)]^{i_k}\right\}\\&=\prod_{k=1}^{\bar{k}-1}\left\{\frac{1}{i+1}\sum_{i_k=0}^{i}[R^{(\lambda)}(g_k)]^{i_k}\right\}\cdot\frac{1}{i+1}\sum_{i_{\bar{k}}=0}^{i}[R^{(\lambda)}(g_{\bar{k}})]^{i_{\bar{k}}}\\&\quad\times\prod_{k=\bar{k}+1}^{n}\left\{\frac{1}{i+1}\sum_{i_k=0}^{n}[R^{(\lambda)}(g_k)]^{i_k}\right\}.\end{aligned} \tag{7}$$

Again the first or last of the three factors vanishes if $k=1$ or $k=n$.

Since $R^{(\lambda)}(e)$ is the identity matrix, the following identity holds.

$$[R^{(\lambda)}(g_{\bar{k}})-R^{(\lambda)}(e)]\sum_{i_{\bar{k}}=0}^{i}[R^{(\lambda)}(g_{\bar{k}})]^{i_{\bar{k}}}=[R^{(\lambda)}(g_{\bar{k}})]^{i+1}-R^{(\lambda)}(e)\ .$$

Because of our assumption (4), we can solve this equation to obtain.

$$\sum_{i_{\bar{k}}=0}^{i} [R^{(\lambda)}(g_{\bar{k}})]^{i_{\bar{k}}} = [R^{(\lambda)}(g_{\bar{k}}) - R^{(\lambda)}(e)]^{-1} \cdot \{[R^{(\lambda)}(g_{\bar{k}})]^{i+1} - R^{(\lambda)}(e)\}$$

Since $R^{(\lambda)}$ is a unitary representation of G, we have for any $g \in G$ and any integral exponent j

$$(8) \qquad \| [R^{(\lambda)}(g)]^j \| = \| R^{(\lambda)}(g^j) \| \leqq F^{(\lambda)} .$$

According to our rules (2), the following inequalities then hold

$$\| [R^{(\lambda)}(g_{\bar{k}})]^{i+1} - R^{(\lambda)}(e) \| \leqq 2F^{(\lambda)} ,$$

$$\| [R^{(\lambda)}(g_{\bar{k}}) - R^{(\lambda)}(e)]^{-1} \| \leqq m_\lambda F^{(\lambda)} ,$$

where m_λ is a positive constant independent of i. This gives an upper bound for the matrix norm of the middle factor in (7)

$$\left\| \frac{1}{i+1} \sum_{i_{\bar{k}}=0}^{i} [R^{(\lambda)}(g_{\bar{k}})]^{i_{\bar{k}}} \right\| \leqq \frac{2m_\lambda}{i+1} [F^{(\lambda)}]^2 = \frac{2m_\lambda r_\lambda}{i+1} F^{(\lambda)} .$$

Furthermore by (8)

$$\left\| \frac{1}{i+1} \sum_{i_k=0}^{i} [R^{(\lambda)}(g_k)]^{i_k} \right\| \leqq \frac{1}{i+1} (i+1) F^{(\lambda)} = F^{(\lambda)} .$$

Replacing each factor in (7) by the stated bound for its matrix-norm, we get

$$(9) \qquad \left\| \frac{1}{(i+1)^n} \sum_{0 \leqq i_k \leqq i} R^{(\lambda)}\left(\prod_{k=1}^{n} g_k^{i_k} \right) \right\| \leqq \prod_{k=1}^{\bar{k}-1} \{F^{(\lambda)}\} \cdot \frac{1}{i+1} \cdot 2m_\lambda r_\lambda F^{(\lambda)} \cdot \prod_{k=\bar{k}+1}^{n} \{F^{(\lambda)}\}$$

$$= \frac{1}{i+1} \cdot 2m_\lambda r_\lambda^n F^{(\lambda)} .$$

(b) Using (5) we get an upper bound for matrix norm of the second term in (6)

$$\left\| \frac{1}{(i+1)^n} \sum_{\nu=(i+1)^n+1}^{N} R^{(\lambda)}(g'_\nu) \right\| \leqq \frac{1}{(i+1)^n} \sum_{\nu=(i+1)^n+1}^{N} \| R^{(\lambda)}(g'_\nu) \|$$

$$\leqq \frac{N-(i+1)^n}{(i+1)^n} F^{(\lambda)} \qquad \text{(by (8))}$$

$$(10) \qquad < \frac{(i+2)^n-(i+1)^n}{(i+1)^n} F^{(\lambda)} \qquad \text{(by (5))}$$

$$= \left[\left(\frac{i+2}{i+1} \right)^n - 1 \right] F^{(\lambda)}$$

$$= \left[\left(1 + \frac{1}{i+1} \right)^n - 1 \right] F^{(\lambda)} .$$

(c) Let now $\varepsilon>0$. Because of (9) we can find a number I_1 such that for all $i\geqq I_1$

$$\left\| \frac{1}{(i+1)^n} \sum_{0\leqq i_k\leqq i} R^{(\lambda)}\left(\prod_{k=1}^{n} g_k^{i_k}\right)\right\| < \frac{\varepsilon}{2}F^{(\lambda)} . \tag{11}$$

Let

$$I_2 = \frac{2-\left(\frac{\varepsilon}{2}+1\right)^{1/n}}{\left(\frac{\varepsilon}{2}+1\right)^{1/n}-1};$$

then for $i\geqq I_2$ we have

$$\left(1+\frac{1}{i+1}\right)^n - 1 \leqq \frac{\varepsilon}{2} \tag{12}$$

Now let $I=\max(I_1, I_2)$ and take $M=(I+2)^n$. Then from (6), (10) and the last two relations (11) and (12) it follows that

$$\left\| \frac{1}{N}\sum_{\nu=1}^{N} R^{(\lambda)}(g'_\nu)\right\| < \frac{(i+1)^n}{N}\left[\frac{\varepsilon}{2}F^{(\lambda)} + \frac{\varepsilon}{2}F^{(\lambda)}\right]$$

$$\leqq \varepsilon F^{(\lambda)} \qquad \text{for all } N\geqq M .$$

This shows the validity of (3) and the application of Lemma 1 completes the proof.

E. Hlawka, [4, §6] has shown that any sequence which is dense in G can be rearranged so as to be a sequence which is equidistributed in G. In view of that fact it should be emphasized that Theorem 2 (as well as any of the following ones) does not merely state that the set G' is dense in G; it states also the existence of a generally valid formula, as shown in the proof, for actually arranging the elements of G' in a sequence which is equidistributed in G.

Theorem 2 implies two more facts which are worth noting. First if we have n elements of G which satisfy the required condition, then we can, before actually producing the set G', arrange them in an entirely arbitrary order without affecting the equidistribution of the corresponding sequence in G. In the non-commutative case we shall therefore in general get different sequences containg different elements of G which are equidistributed in G. Second, we can add an arbitrary finite number of arbitrary elements $g_{n+1}, \cdots, g_m$ to our set of n elements $\{g_k : k=1, 2, \cdots, n\}$ of G. The new set of $m(>n)$ elements of G still satisfies the condition of the theorem and, taken in any order, produces a set which can be arranged so as to be an equidistributed sequence in G.

The first remark together with Lemma 2 and Lemma 3 leads to the following.

COROLLARY 2.1. *If the elements* g_k $(k=1, 2, \cdots, n)$ *satisfy the condition of Theorem* 2, *then the sets*

$$G'' = \{g'' : g'' = g_1^{i_1} g_2^{i_2}, \cdots, g_n^{i_n}, \ -\infty < i_k \leqq 0, \ k = 1, 2, \cdots, n\}$$

and

$$G''' = \{g''' : g''' = g_1^{i_1} g_2^{i_2}, \cdots, g_n^{i_n}, \ -\infty < i_k < +\infty, \ k = 1, 2, \cdots, n\}$$

can be arranged in sequences which are equidistributed in G.

Proof. Let

$$\overline{G} = \{\bar{g} : \bar{g} = g_n^{i_n} g_{n-1}^{i_{n-1}}, \cdots, g_1^{i_1}, \ 0 \leqq i_k < +\infty, \ k = 1, 2, \cdots, n\} \ .$$

Then $\overline{G}$ can be arranged in a sequence equidistributed in G and $G''=\overline{G}^{-1}$. According to Lemma 2, G'' can also be arranged in a sequence which is equidistributed in G.

G''' is the union[3] of G' and $G''-e$ and according to Lemma 3 can be arranged in a sequence equidistributed in G.

COROLLARY 2.2. *If the elements* g_k $(k=1, 2, \cdots, n)$ *satisfy the condition of Theorem* 2, *then* G *is generated by* $\{g_k : k=1, 2, \cdots, n\}$.

Proof. We notice that G' is not an abstract subgroup of G. However, the subgroup H generated by $\{g_k : k=1, 2, \cdots, n\}$ must contain any finite product of finite powers of the g_k's. Therefore, it must contain all elements of the set G'. Since G' is dense in G, we have $H=G$.

3. **Subgroups.** If H is a subgroup of G, then any $R^{(\lambda)}(\lambda \in \Lambda)$ restricted to the elements of H, gives a representation $R^{*(\lambda)}$ of H. Each $R^{*(\lambda)}$ can be completely reduced into a direct sum of irreducible unitary representations of H which, as remarked before, is again a compact group. Let[1] $R'^{(\tau)}(\tau \in \Lambda')$ be the system of inequivalent irreducible unitary representations of H, so obtained. $R'^{(1)}$ again denotes the identity representation of H, obtained e. g. by restricting $R^{(1)}$ to H.

It can be shown without difficulty that $\{R'^{(\tau)} : \tau \in \Lambda'\}$ is a complete system of inequivalent irreducible representations of H. In order to do that we have by the Stone-Weinstrass-theorem to show that the entries of the system $\{R'^{(\tau)} : \tau \in \Lambda'\}$ span a linear space which is an algebra closed under pointwise multiplication and under conjugation and which separates points in H. But all these properties hold for the system $\{R^{(\lambda)} : \lambda \in \Lambda\}$, and from this we have obtained $\{R'^{(\tau)} : \tau \in \Lambda'\}$ only by changing the base in each $R^{(\lambda)}$, restricting it to H and selecting a system of linearly independent entries.

We can apply Theorem 2 to a subgroup H in the following form.

THEOREM 3. *Let H be a subgroup of G and let h_k $(k=1, 2, \cdots, n)$ be elements of H with the property that for each $\lambda \in \Lambda$ there is at least one element $h_{\bar{k}}$ such that the multiplicity of the eigenvalue 1 in $R^{(\lambda)}(h_{\bar{k}})$ is exactly the multiplicity with which the identity-representation $R'^{(1)}$ of H is contained in $R^{*(\lambda)}$.*

Then the set

$$H' = \{h' : h' = h_1^{i_1} h_2^{i_2}, \cdots, h_n^{i_n},\ 0 \leqq i_k < +\infty,\ k = 1, 2, \cdots, n\}$$

can be arranged in a sequence which is equidistributed in H.

Proof. From the above remarks we can conclude that any irreducible representation of H is contained in some $R^{*(\lambda)}$. Suppose that for a certain $\bar{\tau} \neq 1$ and for each $k=1, 2, \cdots, n$ we have

$$| R'^{(\bar{\tau})}(h_k) - R'^{(\bar{\tau})}(e) | = 0 .$$

This implies that $R'^{(\bar{\tau})}(h_k)$ has the eigenvalue 1 for each $k=1, 2, \cdots, n$. The representation $R'^{(\bar{\tau})}$ is contained in some $R^{*(\lambda)}$ which may contain also $R'^{(1)}$ with multiplicity m. But then each $R^{(\lambda)}(h_k)$ $(k=1, 2, \cdots, n)$ would have the eigenvalue 1 at least with multiplicity $m+1$ which contradicts our assumption.

Therefore for each $\tau \neq 1$ there has to be at least one $h_{\bar{k}}$ such that

$$| R'^{(\tau)}(h_{\bar{k}}) - R'^{(\tau)}(e) | \neq 0$$

and the conclusion of Theorem 2 applies to the topological group H.

Again we notice that the order, in which the elements h_k are used to produce the set H' is insignificant. By exactly the same reasoning as in §2, we obtain the following.

COROLLARY 3.1. *If the elements h_k $(k=1, 2, \cdots, n)$ satisfy the condition of Theorem 3, then the sets*

$$H'' = \{h'' : h'' = h_1^{i_1} h_2^{i_2}, \cdots, h_n^{i_n},\ -\infty < i_k \leqq 0,\ k = 1, 2, \cdots, n\}$$

and

$$H''' = \{h''' : h''' = h_1^{i_1} h_2^{i_2}, \cdots, h_n^{i_n},\ -\infty < i_k < +\infty,\ k = 1, 2, \cdots, n\}$$

can be arranged in sequences which are equidistributed in H.

COROLLARY 3.2. *If the elements h_k $(k=1, 2, \cdots, n)$ satisfy the condition of Theorem 3, then H is generated by $\{h_k : k=1, 2, \cdots, n\}$.*

4. Finite groups. Let now G be a not necessarily commutative

finite group of order o, considered as a finite compact group with the discrete topology. The Haar-measure of G is then defined by $\mu(g)=1/o$ for any element $g \in G$.

The theorems stated so far are valid in general and therefore also for finite groups, since G was nowhere required in the definitions, lemmas and proofs to have infinitely many different group elements or inequivalent, irreducible representations. However, it is of not much use to talk about infinite sequences in a finite group. Therefore it seems justified to modity the concept of equidistribution of a sequence to the situation in finite groups in the following way:

DEFINITION 4. Let $\{x_\nu : \nu=1, 2, \cdots, N\}$ be a finite sequence of elements of G and let $N(M)$ be the number of elements in the set $\{x_\nu : x_\nu \in M, \nu \leqq N\}$ for any subset M of G.

The sequence $\{x_\nu : \nu=1, 2, \cdots, N\}$ is said to be *equidistributed in* G if

$$\frac{N(M)}{N} = \mu(M) \tag{13}$$

for all subsets M of G.

The formal translation of Definition 1 to finite groups, however, admits a much less complicated statement of equidistribution of finite sequence in a finite group which in turn reflects the intuitive meaning of equidistribution in infinte groups. In contrast to the infinite case the order of the element in the finite sequence $\{x_\nu : \nu=1, 2, \cdots, N\}$ is completely irrelevant. Instead of talking about a finite sequence of elements of G, we might therefore just as well talk about a finite set of elements of G (which may contain any element of G arbitrarily often). If M contains m elements, then $\mu(M)=m/o$. Especially if $M=\{g\}$ (a single element of G) (13) gives $N(g)=N/o$ for any element $g \in G$ which means that $\{x_\nu : \nu=1, 2, \cdots, N\}$ contains each element of G equally often. Conversely, if the latter is true, then $N(M)=mN/o$ and (13) holds for any subset M of G. So we can give the following better definition.

DEFINITION 4′. The finite set $\{x_\nu : \nu=1, 2, \cdots, N\}$ of elements of G is said to be equidistributed in G if it contains every element of G equally often.

In the same way we modify Definition 3.

DEFINITION 5. The finite set $\{x_\nu : \nu=1, 2, \cdots, N\}$ of elements of a subgroup H is said to be *equidistributed in* H if it contains every element of H equally often.

The theorems obtained so far are then completely transferrable to

the finite case [3 Theorems 8 and 9]. Let now $\{R^{(\lambda)} : \lambda=1, 2, \cdots, l\}$ be a complete system of inequivalent irreducible unitary representations of G and let $R^{(1)}$ again be the identity-representation of G. Furthermore let $o(g)$ be the order of any element $g \in G$. The results are as follows.

THEOREM 4. *Let g_k $(k=1, 2, \cdots, n)$ be n elements of the finite group G such that for each $\lambda \neq 1$ there is at least one $g_{\bar{k}}$ for which*

$$|R^{(\lambda)}(g_{\bar{k}}) - R^{(\lambda)}(e)| \neq 0 .$$

Then the set

$$G' = \{g' : g' = g_1^{i_1} g_2^{i_2}, \cdots, g_n^{i_n},\ 0 \leqq i_k < o(g_k),\ k = 1, 2, \cdots, n\}$$

is equidistributed in G and contains each element $g \in G$ exactly

$$\frac{1}{o} \prod_{k=1}^{n} o(g_k)$$

times.

COROLLARY 4.1. *If the elements g_k $(k=1, 2, \cdots, n)$ satisfy the condition of Theorem 4, then G is generated by $\{g_k : k=1, 2, \cdots, n\}$.*

THEOREM 5. *Let H be a subgroup of order $o(H)$ of the finite group G and let h_k $(k=1, 2, \cdots, n)$ be elements of H with the property that for each $\lambda=1, 2, \cdots, l$ there is at least one element $h_{\bar{k}}$ such that the multiplicity of the eigenvalue 1 in $R^{(\lambda)}(h_{\bar{k}})$ is exactly the multiplicity with which the identity representation $R'^{(1)}$ of H is contained in $R^{*(\lambda)}$.*

Then the set

$$H' = \{h' : h' = h_1^{i_1} h_2^{i_2}, \cdots, h_n^{i_n},\ 0 \leqq i_k < o(h_k),\ k = 1, 2, \cdots, n\}$$

is equidistributed in H and contains each element $h \in H$ exactly $o(H)^{-1} \prod_{k=1}^{n} o(h_k)$ times.

COROLLARY 5.1. *If the elements h_k $(k=1, 2, \cdots, n)$ satisfy the condition of Theorem 5, then H is generated by $\{h_k : k=1, 2, \cdots, n\}$.*

The Corollaries 2.1 and 3.1, transferred to the finite case, coincide with Theorems 4 and 5. There is a last case which might be of interest, where H is a finite discrete subgroup of the infinite compact group G. Take the notation as defined in the corresponding cases. We get the following.

THEOREM 6. *Let H be a finite discrete subgroup of order $o(H)$ of the infinite compact group G and let h_k $(k=1, 2, \cdots, n)$ be elements of*

H with the property that for each $\lambda \in \Lambda$ there is at least one element $h_{\bar{k}}$ such that the multiplicity of the eigenvalue 1 in $R^{(\lambda)}(h_{\bar{k}})$ is exactly the multiplicity with which the identity-representation $R'^{(1)}$ of H is contained in $R^{*(\lambda)}$.

Then the set

$$H' = \{h' : h' = h_1^{i_1} h_2^{i_2}, \cdots, h_n^{i_n},\ 0 \leqq i_k < o(h_k),\ k = 1, 2, \cdots, n\}$$

is equidistributed in H and contains each element $h \in H$ exactly $o(H)^{-1} \prod_{k=1}^{n} o(h_k)$ times.

Proof. By the same reasoning as in the proof of Theorem 3 we assert that each irreducible representation of H is contained in some $R^{(\lambda)}$, restricted to H. Then as there was done with Theorem 2 we apply Theorem 4 to the finite group H.

COROLLARY 6.1. *If the elements h_k $(k=1, 2, \cdots, n)$ satisfy the conditions of Theorem 6, then H is generated by $\{h_k : k=1, 2, \cdots, n\}$.*

It may be remarked that Theorems 4 to 6 can be deduced also from Theorems 2 and 3 without going back to the corresponding condition imposed on the generating elements, by means of the following lemma.

LEMMA 4. *Let g_k $(k=1, 2, \cdots, n)$ be elements of finite order $o(g_k)$ $(k=1, 2, \cdots, n)$ of an arbitrary compact group G.*

Then (i) the finite set

$$\overline{G} = \{\bar{g} : \bar{g} = g_1^{i_1} g_2^{i_2}, \cdots, g_n^{i_n},\ 0 \leqq i_k < o(g_k),\ k = 1, 2, \cdots, n\}$$

is equidistributed in G if and only if (ii) the set

$$G' = \{g' : g' = g_1^{i_1} g_2^{i_2}, \cdots, g_n^{i_n},\ 0 \leqq i_k < +\infty,\ k = 1, 2, \cdots, n\}$$

can be arranged as in the proof of Theorem 2 in a sequence which is equidistributed in G.

Proof. $(i) \rightarrow (ii)$. From (i) it follows immediately that G is finite. Let m be the least common multiple of the numbers $o(g_k)$ $(k=1, 2, \cdots, n)$. If we arrange the elements of G' in a sequence $\{g'_\nu : \nu \in \omega\}$ as in the proof of Theorem 2, then we observe that

$$\{g'_\nu : \nu \leqq (pm)^n\} = \{g' : g' = g_1^{i_1} g_2^{i_2}, \cdots, g_n^{i_n},\ 0 \leqq i_k < pm,\ k = 1, 2, \cdots, n\}$$

(p=positive integer) is just composed of $(pm)^n / \prod_{k=1}^{n} o(g_k)$ times[3] the set $\overline{G}$. So for $N=(pm)^n$ in (1') we get

$$\frac{1}{(pm)^n} \sum_{\nu=1}^{(pm)^n} R^{(\lambda)}(g'_\nu) = \frac{1}{\prod_{k=1}^{n} o(g_k)} \sum_{0 \leqq i_k < o(g_k)} R^{(\lambda)}\left(\prod_{k=1}^{n} g_k^{i_k}\right). \tag{14}$$

If (i) holds it can be shown that the right-side sum in (14) is the 0-matrix for $\lambda \neq 1$. If N is an integer between $(pm)^n$ and $[(p+1)m]^n$ then the left-side term in (1′) can be split up into $(pm)^n/N$ times the left-side term of (14) and $1/N$ times a sum of $N-(pm)^n$ unitary matrices. But

$$\frac{N-(pm)^n}{N} \leqq \frac{[(p+1)m]^n-(pm)^n}{(pm)^n} = \left(1+\frac{1}{p}\right)^n - 1$$

can be made arbitrarily small as in the proof of Theorem 2 and by the method used there we arrive at (1′).

$(ii) \rightarrow (i)$. We first observe that G' contains only finitely many different elements, namely those contained in $\bar{G}$, and G is finite. Again (14) holds. Since (14) gives just the value of the left-side term of (1′) for $N=(pm)^n$ $(p \in \omega)$, we can conclude from the validity of (1′) that

$$\sum_{0 \leqq i_k < o(g_k)} R^{(\lambda)}\left(\prod_{k=1}^{n} g_k^{i_k}\right) = \sum_{\bar{g} \in \bar{G}} R^{(\lambda)}(\bar{g})$$

has to be the 0-matrix for $\lambda \neq 1$. But from this follows (i) by the well-known properties of irreducible representations of a finite group.

5. **Abelian groups.** Let now G be a (finite or infinite) compact abelian group. The irreducible representations are of degree 1 and instead of talking about a complete system of inequivalent irreducible unitary representations $R^{(\lambda)}$ $(\lambda \in \Lambda)$ we may talk about a complete system of inequivalent characters $\chi^{(\lambda)}$ $(\lambda \in \Lambda)$, where $\chi^{(1)}$ denotes the identity-character. As can be seen easily, the conditions of Theorem 2 and 3 take the specially simple form "$\chi^{(\lambda)}(g_{\bar{k}}) \neq 1$ for $\lambda \neq 1$" and "for each λ for which $\chi^{(\lambda)}(h) \neq 1$ for some element $h \in H$ there is at least one element $h_{\bar{k}}$ such that $\chi^{(\lambda)}(h_{\bar{k}}) \neq 1$" respectively. However, here we can make a stronger statement than in the preceding theorems.

THEOREM 7. *Let g_k $(k=1, 2, \cdots, n)$ be elements of the abelian group G. Furthermore, let*

$$G' = \{g' : g' = g_1^{i_1} g_2^{i_2}, \cdots, g_n^{i_n},\ 0 \leqq i_k < +\infty,\ k = 1, 2, \cdots, n\}$$

and let $\{g'_\nu : \nu \in \omega\}$ be the sequence in which the elements of G' have been arranged as in the proof of Theorem 2.

A necessary and sufficient condition for (i) $\{g_k : k=1, 2, \cdots, n\}$ to generate G and (ii) $\{g'_\nu : \nu \in \omega\}$ to be equidistributed in G is that for each $\lambda \neq 1$ there is at least one $g_{\bar{k}}$ such that

$$\chi^{(\lambda)}(g_{\bar{k}}) \neq 1 .$$

Proof. The statement about sufficiency is exactly Theorem 2

together with Corollary 2.2. Let us now assume that $\{g'_\nu : \nu \in \omega\}$ is equidistributed in G. Then $\{g_k : k=1, 2, \cdots, n\}$ generates G. Suppose that for a given $\lambda \neq 1$ we have $\chi^{(\lambda)}(g_k)=1$ for all $k=1, 2, \cdots, n$. Take a fixed element $g \in G$ with $\chi^{(\lambda)}(g) \neq 1$ and an arbitrary small positive number $\varepsilon < |\chi^{(\lambda)}(g)-1|$. Since finite products of finite powers of the elements g_k $(k=1, 2, \cdots, n)$ are dense in G and since $\chi^{(\lambda)}$ is a continuous character on G there has to be an element $g'=g_1^{j_1} g_2^{j_2} \cdots g_n^{j_n}$ such that

$$|\chi^{(\lambda)}(g) - \chi^{(\lambda)}(g')| < \varepsilon .$$

Since $\chi^{(\lambda)}(g')=1$ this implies $|\chi^{(\lambda)}(g)-1|<\varepsilon$. But this contradicts our assumption about ε.

THEOREM 8. *Let h_k $(k=1, 2, \cdots, n)$ be elements of a subgroup H of the abelian group G. Furthermore let*

$$H' = \{h' : h' = h_1^{i_1} h_2^{i_2}, \cdots, h_n^{i_n},\ 0 \leqq i_k < +\infty,\ k = 1, 2, \cdots, n\}$$

and let $\{h'_\nu : \nu \in \omega\}$ be the sequence in which the elements of H' have been arranged as in the proof of Theorem 3.

A necessary and sufficient condition for (i) $\{h_k : k=1, 2, \cdots, n\}$ *to generate H and* (ii) $\{h'_\nu : \nu \in \omega\}$ *to be equidistributed in H is that for each λ for which $\chi^{(\lambda)}(h) \neq 1$ for some element $h \in H$ there is at least on element $h_{\bar{k}}$ such that $\chi^{(\lambda)}(h_{\bar{k}}) \neq 1$.*

Proof. Again the sufficiency of the above condition is stated in Theorem 3 and Corollary 3.2. On the other had, if $\{h'_\nu : \nu \in \omega\}$ is equidistributed in H, then $\{h_k : k=1, 2, \cdots, n\}$ generates H and we can prove our claim exactly as in the proof of the preceding theorem.

Naturally there hold similar statements as Corollaries 2.1 and 3.1. For finite abelian groups we can, by obvious modifications, arrive at conclusions about equidistribution of finite sets as in §4, see [3, Theorems 10 and 11].

If we take as our abelian group G the direct product of p circle groups, the p-dimensional toroidal group, then Theorems 7 and 8 give us well-known theorems of Kronecker [5, p. 83 Theorem 4] and Weyl [6, Theorem 4]. It has been shown by Halmos and Samelson and again by Eckmann (see [1, Theorems 2 and 5] and [2, Theorem II* and Corollary]) that the p-dimensional toroidal group as well as any separable connected compact abelian group is monothetic.

In contrast to the situation in abelian groups the condition of Theorem 2 is not necessary for the existence of an equidistributed sequence of the form $\{g'_\nu : \nu \in \omega\}$ (as constructed there) in a non-commutative group. A simple counter example is given by the tetrahedral group A_4 (the alternating group of 4 variables). Let g_1 and g_2 be two

different elements of order 2 and g_3 an arbitrary element of order 3. If we denote by $R^{(4)}$ the irreducible representation of A_4 of degree 3 it can be easily checked[4] that $|R^{(4)}(g_k)-R^{(4)}(e)|=0$ for $k=1, 2, 3$. However, the set of 12 element $\overline{G}=\{\overline{g} : \overline{g}=g_1^{i_1} g_2^{i_2} g_3^{i_3},\ 0\leqq i_1<2,\ 0\leqq i_2<2,\ 0\leqq i_3<3\}$ is equidistributed in G. By Lemma 4 it follows that the set

$$G' = \{g' : g' = g_1^{i_1} g_2^{i_2} g_3^{i_3},\ 0 \leqq i < \infty,\ k = 1, 2, 3\}$$

can be arranged in a sequence which is equidistributed in G. A counter-example disproving the necessity of the condition of Theorem 3 is given by any group containing A_4 as a subgroup, for example A_4 itself or the symmetric group of 4 variables.

REFERENCES

1. B. Eckmann, *Ueber monothetische Gruppen*, Comm. Math. Helv. **16** (1943/44), 249-263.
2. P. R. Halmos and H. Samelson, *On monothetic groups*, Proc. Nat. Acad. Sci. USA, **28** (1942), 254-258.
3. G. Helmberg, *Strukturbeziehungen zwischen endlicher Gruppe, Gruppenring und irreduziblen Darstellungen*, Monatsh. Math., **58** (1954), 241-257.
4. E. Hlawka, *Zur formalen Theorie der Gleichverteilung in kompakten Gruppen*, Rend. Circ. Mat. Palermo Ser. II. **IV** (1955), 33-47.
5. J. Koksma, *Diophantische Approximationen*, (Berlin 1936).
6. H. Weyl, *Ueber die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. **77** (1916), 313-352.

UNIVERSITY OF WASHINGTON

[4] The characters of g_1, g_2 and g_3 in $R^{(4)}$ are -1, -1 and 0 respectively.

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. L. ROYDEN
Stanford University
Stanford, California

A. L. WHITEMAN
University of Southern California
Los Angeles 7, California

R. A. BEAUMONT
University of Washington
Seattle 5, Washington

E. G. STRAUS
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH
C. E. BURGESS
M. HALL
E. HEWITT
A. HORN
V. GANAPATHY IYER
R. D. JAMES
M. S. KNEBELMAN
L. NACHBIN
I. NIVEN
T. G. OSTROM
M. M. SCHIFFER
G. SZEKERES
F. WOLF
K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
HUGHES AIRCRAFT COMPANY
THE RAMO-WOOLDRIDGE CORPORATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. All other communications to the editors should be addressed to the managing editor, E. G. Straus at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 10, 1-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics
Vol. 8, No. 2 April, 1958