

PROBABILITIES ON A COMPACT GROUP⁽¹⁾

BY

KARL STROMBERG

Let G be an arbitrary compact Hausdorff group. A *probability measure* on G is a non-negative, real-valued, countably additive, regular Borel measure μ on G such that $\mu(G) = 1$. If μ and λ are two probability measures on G then their convolution $\mu * \lambda$ is also a probability measure on G . In fact if X and Y are any two independent random variables on an arbitrary probability space which take their values in G and if μ and λ are their respective distributions, then $\mu * \lambda$ is the distribution of the pointwise product $X \cdot Y$. Thus the arithmetic of G -valued independent random variables is just the arithmetic of probability measures on G . This arithmetic is discussed in §2.

Weak* convergence of probability measures is discussed and several theorems concerning infinite powers and infinite products are proved.

These and other related problems have been studied in one form or another by other authors. Vorob'yov, in [12], has considered the case in which G is a finite commutative group. Hewitt and Zuckerman, in [3], have studied a class of finite commutative semigroups which includes all finite commutative groups. Kakehashi, in [5], has studied the case in which G is the circle group. In [6], Kawada and Ito have obtained several results for compact metrizable groups. In [14], Wendel has identified all idempotent probability measures when G is an arbitrary compact Hausdorff group. More recently Kloss, in [8], and Urbanik, in [11], have obtained further results in the case that G is an arbitrary compact Hausdorff group. These results and their connection with our findings will be described in the sequel.

It is a pleasure to record here the author's indebtedness to Professor Edwin Hewitt for the wealth of valuable advice that he has given during the preparation of this paper.

1. **Preliminaries.** 1.1. For measure-theoretic terms and techniques not explained explicitly in this paper see [1]. For topological and set-theoretic information see [7]. Reference should be made to [13] for the elementary theory of topological groups and the theory of representations of a compact group. The elementary theory of Banach algebras may be found in [9].

1.2. Let G be an arbitrary compact Hausdorff group and $\mathcal{C}(G)$ the Banach space of all continuous complex-valued functions on G . The class of Borel sets in G , denoted \mathfrak{B} , is the smallest σ -algebra of subsets of G that contains each open subset of G . A *probability measure* on G is a non-negative, real-valued,

Presented to the Society, January 21, 1959; received by the editors February 24, 1959.

⁽¹⁾ This research was supported in part by the National Science Foundation and in part by the Office of Naval Research.

countably additive, regular Borel measure μ on G such that $\mu(G) = 1$. The set of all probability measures on G is denoted $\mathcal{P}(G)$.

It is a simple consequence of the Riesz representation theorem [1, pp. 247–248] that the set of all positive linear functionals M on $\mathcal{C}(G)$ such that $M(1) = 1$ is in a biunique correspondence with $\mathcal{P}(G)$ under the mapping $\mu \rightarrow M$, where $M(f) = \int f d\mu$ for each f in $\mathcal{C}(G)$. Thus $\mathcal{P}(G)$ may, and shall, be thought of as the above subset of $\mathcal{C}(G)^*$, the first conjugate space of $\mathcal{C}(G)$. One readily verifies that $\mathcal{P}(G)$ with the weak* topology is compact and convex.

1.3. NOTATION. The following notation will be used throughout this paper. For each set $A \subset G$, $\text{card } A$ denotes the cardinal number of A , A' is the complement of A with respect to G and χ_A is the characteristic function of A .

2. The semigroup $\mathcal{P}(G)$.

2.1. DEFINITION. Let μ and λ be in $\mathcal{P}(G)$. Then the convolution of μ with λ is the unique measure $\mu * \lambda$ in $\mathcal{P}(G)$ such that

$$(1) \quad \int_G f(z) d\mu * \lambda(z) = \int_G \int_G f(xy) d\mu(x) d\lambda(y)$$

for each f in $\mathcal{C}(G)$.

As is known [10],

$$(2) \quad \mu * \lambda(E) = \int_G \mu(Ey^{-1}) d\lambda(y) = \int_G \int_G \chi_E(xy) d\mu(x) d\lambda(y) = \int_G \lambda(x^{-1}E) d\mu(x)$$

for each E in \mathcal{B} .

The set $\mathcal{P}(G)$ with convolution as multiplication is therefore a semigroup which is commutative if G is commutative.

2.2. THE SUPPORT OF A MEASURE. For each μ in $\mathcal{P}(G)$ we define the support of μ , denoted $S(\mu)$, to be the set of all x in G such that each neighborhood of x has positive μ -measure. The following proposition is well known and readily verified.

2.2.1. PROPOSITION. Let $\mu \in \mathcal{P}(G)$. Then

- (i) $S(\mu)$ is a closed subset of G ;
- (ii) $\mu(S(\mu)) = 1$;
- (iii) if A is a closed subset of G such that $\mu(A) = 1$, then $S(\mu) \subset A$.

A proof of the following theorem appears in [14, Lemma 4].

2.2.2. THEOREM. Let $\mu, \lambda \in \mathcal{P}(G)$. Then

$$S(\mu * \lambda) = S(\mu) \cdot S(\lambda).$$

The point support, $P(\mu)$, of a $\mu \in \mathcal{P}(G)$ is $\{x: x \in G, \mu(\{x\}) > 0\}$. Since $\mu(G) = 1 < +\infty$, $P(\mu)$ is a countable set. Moreover it is easily shown that

$$P(\mu * \lambda) = P(\mu) \cdot P(\lambda), \quad \lambda, \mu \in \mathcal{P}(G).$$

2.3. HAAR MEASURES. It is known, see for example [1, pp. 254, 262-263], that if H is any compact Hausdorff group, then there exists a unique measure $\mu_H \in \mathcal{P}(H)$ such that

$$\mu_H(E) = \mu_H(xE) = \mu_H(Ex) = \mu_H(E^{-1})$$

for each Borel set $E \subset H$ and $x \in H$. The measure μ_H is called Haar measure on H . Now if H is any closed, and hence compact, subgroup of G , we shall let ω_H denote the member of $\mathcal{P}(G)$ defined as follows:

$$\omega_H(E) = \mu_H(E \cap H), \quad E \in \mathcal{B}.$$

We shall refer to ω_H as *Haar measure on H* . The letter ω will be used in place of ω_G to denote Haar measure on G .

Wendel has proved [14, Theorem 1] that the measures ω_H are the only idempotents in the semigroup $\mathcal{P}(G)$.

Formula (2) implies that ω is a two-sided zero for $\mathcal{P}(G)$, i.e., if $\mu \in \mathcal{P}(G)$, then

$$\omega * \mu = \mu * \omega = \omega.$$

2.4. THE POINT MASSES. Let $x \in G$. Then the *point mass* at x , denoted ϵ_x , is the member of $\mathcal{P}(G)$ defined as follows:

$$\epsilon_x(E) = \begin{cases} 1 & \text{if } x \in E, \\ 0 & \text{if } x \notin E, \end{cases} \quad E \in \mathcal{B}.$$

The measure ϵ_x corresponds to the multiplicative linear functional $f \rightarrow f(x)$ on $\mathcal{C}(G)$.

The following observations have been made by Wendel [14]:

- (i) if e is the identity in G , then ϵ_e is a two-sided identity for $\mathcal{P}(G)$;
- (ii) $\epsilon_x * \epsilon_y = \epsilon_{xy}$ for all $x, y \in G$;
- (iii) a measure μ in $\mathcal{P}(G)$ has an inverse if and only if $\mu = \epsilon_x$ for some $x \in G$.

2.5. THE CENTER OF $\mathcal{P}(G)$. The *center* of $\mathcal{P}(G)$ is the set of all μ in $\mathcal{P}(G)$ such that $\mu * \lambda = \lambda * \mu$ for each λ in $\mathcal{P}(G)$.

2.5.1. THEOREM. *Let μ be in $\mathcal{P}(G)$. Then the following four propositions are equivalent:*

- (i) μ is in the center of $\mathcal{P}(G)$;
- (ii) $\epsilon_x * \mu = \mu * \epsilon_x$ for $x \in G$;
- (iii) $\mu(Ex) = \mu(xE)$ for $x \in G$ and $E \in \mathcal{B}$;
- (iv) $\mu(xEx^{-1}) = \mu(E)$ for $x \in G$ and $E \in \mathcal{B}$.

Proof. It is obvious that (i) implies (ii) and that (iii) is equivalent to (iv).

Suppose that (ii) is true. Let $x \in G$ and $E \in \mathcal{B}$. Then $\mu(Ex) = \int_G \mu(Ey^{-1})d\epsilon_x^{-1}(y) = \mu * \epsilon_x^{-1} = \epsilon_x^{-1} * \mu = \int_G \mu(y^{-1}E)d\epsilon_x^{-1}(y) = \mu(xE)$. Hence (ii) implies (iii).

Now suppose that (iii) is true. Let λ be in $\mathcal{P}(G)$. Then, for each E in \mathcal{B} ,

we have $\mu * \lambda(E) = \int_G \mu(Ex^{-1})d\lambda(x) = \int_G \mu(x^{-1}E)d\lambda(x) = \lambda * \mu(E)$. Thus (iii) implies (i) and the proof is complete.

2.5.2. COROLLARY. $\mathcal{O}(G)$ is commutative if and only if G is commutative.

The next theorem shows how elements of the center of $\mathcal{O}(G)$ may be constructed.

2.5.3. THEOREM. Let $\mu \in \mathcal{O}(G)$. Define the measure $\tilde{\mu}$ as follows:

$$\tilde{\mu}(E) = \int_G \mu(xEx^{-1})d\omega(x)$$

for $E \in \mathcal{B}$. Then $\tilde{\mu}$ is in the center of $\mathcal{O}(G)$.

Proof. Define the mapping ϕ from $G \times G$ into G by the formula $\phi(x, y) = x^{-1}yx$. Then ϕ is continuous and $\tilde{\mu}(E) = \omega \times \mu(\phi^{-1}(E))$ for each $E \in \mathcal{B}$. Hence [10, Corollary 1] $\tilde{\mu}$ is a regular measure. All other qualifications for membership in $\mathcal{O}(G)$ are obviously satisfied by $\tilde{\mu}$. That $\tilde{\mu}$ is actually in the center of $\mathcal{O}(G)$ now follows from Theorem 2.5.1 (iv) and the translation invariance of ω .

2.5.4. REMARK. The mapping $\mu \rightarrow \tilde{\mu}$ is a mapping of $\mathcal{O}(G)$ onto its center since $\mu = \tilde{\mu}$ if μ is in the center of $\mathcal{O}(G)$.

We now investigate the relationship between $S(\mu)$ and $S(\tilde{\mu})$.

2.5.5. LEMMA. Let $\mu \in \mathcal{O}(G)$ and let U be an open subset of G . Then the function $f: x \rightarrow \mu(xUx^{-1})$ is lower semi-continuous.

Proof. Let α be any real number and set $A = \{x: x \in G, f(x) > \alpha\}$. We must show that A is open. If $A = 0$, there is nothing to prove. Otherwise let $a \in A$. Then $\mu(aUa^{-1}) = f(a) > \alpha$. Since μ is regular there is a compact set $C \subset aUa^{-1}$ such that $\mu(C) > \alpha$. Now there exists an open neighborhood V of the identity e such that $V^{-1}CV \subset aUa^{-1}$. Then, for $y \in V$, we have $C \subset yaUa^{-1}y^{-1}$ and therefore $\mu(yaUa^{-1}y^{-1}) \geq \mu(C) > \alpha$ which implies that $ya \in A$. Thus $Va \subset A$ and A is open completing the proof.

2.5.6. THEOREM. Let $\mu \in \mathcal{O}(G)$ and set $B = \cup \{A: A \text{ is a conjugate class in } G, A \cap S(\mu) \neq 0\}$. Then $S(\mu) = B^-$.

Proof. Let U be any open subset of G such that $\mu(U) > 0$. Define f as in 2.5.5. Then f is lower semi-continuous and $f(e) > 0$ so there exists an open neighborhood V of e such that $f(x) > f(e)/2$ for each $x \in V$. Thus $\tilde{\mu}(U) = \int_G \mu(xUx^{-1})d\omega(x) \geq \int_V \mu(xUx^{-1})d\omega(x) \geq f(e)\omega(V)/2 > 0$. Accordingly $S(\mu) \subset S(\tilde{\mu})$.

Now let A be any conjugate class in G such that $A \cap S(\mu) \neq 0$. Let $a \in A \cap S(\mu)$ and $b \in A$. Then there exists $c \in G$ such that $b = cac^{-1}$. If W is any neighborhood of b , then $\tilde{\mu}(W) = \tilde{\mu}(c^{-1}Wc) > 0$ since $c^{-1}Wc$ is a neighborhood of a and $a \in S(\mu) \subset S(\tilde{\mu})$. Thus $b \in S(\tilde{\mu})$, $A \subset S(\tilde{\mu})$ and $B \subset S(\tilde{\mu})$. Since $S(\tilde{\mu})$ is closed this implies that $B^- \subset S(\tilde{\mu})$. But $1 \geq \tilde{\mu}(B^-) \geq \tilde{\mu}(B)$

$= \int_G \mu(xBx^{-1})d\omega(x) = \int_G \mu(B)d\omega(x) \geq \int_G \mu(S(\mu))d\omega(x) = 1$. Accordingly $\mu(B^-) = 1$ so $S(\mu) \subset B^-$. This completes the proof.

3. Limit theorems in $\mathcal{O}(G)$. 3.1. Throughout this section we will be concerned with convergence in $\mathcal{O}(G)$. This convergence will always be with respect to the weak* topology on $\mathcal{O}(G)$. To be explicit, a net $\{\mu_\alpha: \alpha \in A\}$ in $\mathcal{O}(G)$ is said to converge to a measure $\mu \in \mathcal{O}(G)$ if and only if $\int_G af(x)d\mu_\alpha(x) \rightarrow \int_G af(x)d\mu(x)$ for each $f \in \mathcal{C}(G)$. As pointed out in 1.2, $\mathcal{O}(G)$ is compact in this topology.

3.2. A TRANSFORM ON $\mathcal{O}(G)$. We now define and state some theorems about a certain embedding of $\mathcal{O}(G)$ which can be used in studying convolution on $\mathcal{O}(G)$.

Let $\mathfrak{D}(G)$ be a complete set of mutually inequivalent, irreducible, continuous unitary representations of the compact group G by complex matrices, [13, pp. 72-76]. In particular let D_0 be the identity representation of G , i.e., $D_0(x) = 1$ for each $x \in G$. For each $D \in \mathfrak{D}(G)$, let $n(D)$ denote the degree of the representation D and let \mathfrak{M}_D denote the multiplicative topological semigroup of all complex square matrices of order $n(D)$, where the topology on \mathfrak{M}_D is the product topology obtained by considering \mathfrak{M}_D as the topological product of $[n(D)]^2$ copies of the complex plane. Each $D \in \mathfrak{D}(G)$ can be expressed in terms of its components d_{ij} ($i = 1, \dots, n(D); j = 1, \dots, n(D)$): $D(x) = (d_{ij}(x))_{i,j=1}^{n(D)}$ where each d_{ij} is in $\mathcal{C}(G)$ and $\|d_{ij}\| \leq 1$.

3.2.1. DEFINITION. Let $\mu \in \mathcal{O}(G)$. For each $D \in \mathfrak{D}(G)$ let the characteristic matrix of μ corresponding to D , denoted $\hat{\mu}(D)$, be defined as

$$\begin{aligned} \hat{\mu}(D) &= \int_G D(x)d\mu(x) = \left(\int_G d_{ij}d\mu \right)_{i,j=1}^{n(D)} \\ &= (\hat{\mu}(d_{ij}))_{i,j=1}^{n(D)}. \end{aligned}$$

Notice that $|\hat{\mu}(d_{ij})| \leq 1$ for each $D \in \mathfrak{D}(G)$ and that $\hat{\mu}(D_0) = 1$ for each $\mu \in \mathcal{O}(G)$.

The following two theorems are proved by Kawada and Itô [6]. They consider only the case that G is metrizable, but their proofs, which depend upon the Peter-Weyl theorem [13, pp. 74-76], are valid in the general case considered here.

3.2.2. THEOREM. Let $D \in \mathfrak{D}(G)$. Then the mapping $\mu \rightarrow \hat{\mu}(D)$ is continuous and is a homomorphism of the semigroup $\mathcal{O}(G)$ into the semigroup \mathfrak{M}_D , i.e., this mapping is continuous on the compact Hausdorff space $\mathcal{O}(G)$ and $\hat{\mu} * \lambda(D) = \hat{\mu}(D) \cdot \hat{\lambda}(D)$ for all μ and λ in $\mathcal{O}(G)$.

3.2.3. DEFINITION. Let $\mu \in \mathcal{O}(G)$. Define $\hat{\mu}$ to be that element of $\prod \{ \mathfrak{M}_D: D \in \mathfrak{D}(G) \}$ whose value at D is $\hat{\mu}(D)$ for each $D \in \mathfrak{D}(G)$, i.e., the D th coordinate of $\hat{\mu}$ is the matrix $\hat{\mu}(D)$.

3.2.4. THEOREM. The mapping $\mu \rightarrow \hat{\mu}$ is a homeomorphism of the compact

space $\mathcal{O}(G)$ and an isomorphism of the semigroup $\mathcal{O}(G)$ onto a compact subsemigroup of the topological semigroup $\prod \{ \mathfrak{M}_D : D \in \mathfrak{D}(G) \}$.

Until now we have considered $\mathcal{O}(G)$ in two separate rôles: as a semigroup and as a compact Hausdorff space. In view of Theorem 3.2.4 we can state a corollary which unifies these rôles.

3.2.5. COROLLARY. *The semigroup $\mathcal{O}(G)$ with the weak* topology is a compact semigroup, i.e. the operation of convolution $\mu * \lambda$ is jointly continuous in the variables μ and λ , on $\mathcal{O}(G)$.*

For later use we now compute, as in [6], the characteristic matrices for ω .

3.2.6. LEMMA. *$\hat{\omega}(D_0) = 1$ and $\hat{\omega}(D) = 0$, the $n(D) \times n(D)$ zero matrix, for each $D \in \mathfrak{D}(G)$ such that $D \neq D_0$.*

Proof. First $\hat{\omega}(D_0) = \int_G D_0 d\omega = \int_G 1 d\omega = \omega(G) = 1$. Next let $D \in \mathfrak{D}(G)$ such that $D \neq D_0$. Then the (i, j) th component of $\hat{\omega}(D)$ is $\hat{\omega}(dij) = \int_G d_{ij}(x) d\omega(x) = \int_G d_{ij}(x)(D_0(x)) d\omega(x) = 0$ since the component functions of the members of $\mathfrak{D}(G)$ are orthogonal [13, pp. 73–74].

3.3. INFINITE POWERS. A measure $\lambda \in \mathcal{O}(G)$ is said to be an *infinite power* if there exists a measure $\mu \in \mathcal{O}(G)$ such that $\lim_{n \rightarrow \infty} \mu^n = \lambda$. Since the idempotent measures in $\mathcal{O}(G)$ are exactly the measures ω_H , and since convolution is jointly continuous on $\mathcal{O}(G)$, it follows that a necessary and sufficient condition that a measure $\lambda \in \mathcal{O}(G)$ be an infinite power is that $\lambda = \omega_H$ for some closed subgroup $H \subset G$.

We next develop necessary and sufficient conditions on μ that $\lim_{n \rightarrow \infty} \mu^n$ exists. We begin with four lemmas.

3.3.1. LEMMA. *Let $\mu \in \mathcal{O}(G)$ and let $f \in \mathcal{C}(G)$ be such that $|f(x)| \leq 1$ for each $x \in G$. Suppose that $\int_G f d\mu = e^{i\theta}$ for some real number θ . Set*

$$A = \{ x : x \in G, f(x) = e^{i\theta} \}.$$

Then $S(\mu) \subset A$.

The proof of this lemma is straightforward and is left to the reader.

3.3.2. LEMMA. *Let A be a Banach algebra. For each $a \in A$, let $r(a) = \max \{ |\alpha| : \alpha \in \text{spectrum}(a) \}$ denote the spectral radius of a . Then $\|a^n\| \rightarrow 0$ if and only if $r(a) < 1$.*

Proof. According to [9, p. 75], $r(a) = \lim_{n \rightarrow \infty} \|a^n\|^{1/n}$. Thus if $r(a) < 1$, there is a $t < 1$ such that $\|a^n\|^{1/n} < t$ for all sufficiently large n . Hence $\lim \|a^n\| = \lim t^n = 0$. On the other hand $\|a^n\| \geq r(a^n) = r(a)^n$, [9, pp. 75, 66]. Hence $\|a^n\| \rightarrow 0$ implies $r(a) < 1$.

3.3.3. LEMMA. *Let H be a closed subgroup of G . Suppose that there exists*

an element $x_0 \in G \cap H'$ such that $x_0H = Hx_0$ and the only closed subgroup of G containing x_0H is G itself. Then H is a normal subgroup of G .

Proof. Set $K = \{x: x \in G, xH = Hx\}$. Then

$$K = \bigcap_{h \in H} \{x: x \in G, xhx^{-1} \in H, x^{-1}hx \in H\}.$$

Being the intersection of closed sets, K is a closed set. Moreover K is a subgroup of G containing x_0H , so $K = G$ and the proof is complete.

3.3.4. LEMMA. Let K be a closed subgroup of G . Set

$$\mathcal{Q} = \{\mu: \mu \in \mathcal{P}(G), S(\mu) \subset K\}.$$

Then \mathcal{Q} is a closed subsemigroup of $\mathcal{P}(G)$ which is isomorphic and homeomorphic to $\mathcal{P}(K)$ under the mapping $\mu \rightarrow \mu'$, where $\mu'(E) = \mu(E)$ for each Borel set $E \subset K$.

This lemma is obvious and proof is therefore omitted.

3.3.5. MAIN THEOREM⁽²⁾. Let $\mu \in \mathcal{P}(G)$ and let K denote the smallest closed subgroup of G which contains $S(\mu)$. Then $\lim_{n \rightarrow \infty} \mu^n$ exists if and only if $S(\mu)$ is not contained in any coset of any proper closed normal subgroup of K . Moreover if this limit exists, then it is equal to ω_K .

Proof. In view of Lemma 3.3.4 it suffices to consider only the case that $K = G$. We therefore suppose $K = G$.

We first prove the sufficiency of the condition. Assume that it is false that $\lim_{n \rightarrow \infty} \mu^n = \omega$. Then, according to 3.2.4 and 3.2.6, there exists $D \in \mathcal{D}(G)$ such that $D \neq D_0$, and it is false that $\lim_{n \rightarrow \infty} \hat{\mu}(D)^n = 0$. Thus, by Lemma 3.2.2, $\hat{\mu}(D)$ has some eigenvalue α such that $|\alpha| \geq 1$. Let η be an eigenvector of $\hat{\mu}(D)$ of unit length corresponding to the eigenvalue α : $\hat{\mu}(D)\eta = \alpha\eta$, $\|\eta\| = 1$. Let the dimension of D be k and let $\xi = (1, 0, 0, \dots, 0)$ have k coordinates. Then there is a k -rowed unitary matrix U such that $U\xi = \eta$. Define a representation \tilde{D} of G as follows: $\tilde{D}(x) = U^{-1}D(x)U$ for each $x \in G$. Then \tilde{D} is equivalent to D so D is irreducible, continuous and, since U is unitary, D is unitary. Moreover $\hat{\mu}(\tilde{D})\xi = U^{-1}\hat{\mu}(D)U\xi = U^{-1}\hat{\mu}(D)\eta = U^{-1}\alpha\eta = \alpha U^{-1}\eta = \alpha\xi$. Hence ξ is an eigenvector of $\hat{\mu}(\tilde{D})$ having eigenvalue α . Thus

$$\hat{\mu}(\tilde{D}) = \begin{pmatrix} \alpha & & & \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{pmatrix}$$

and hence

(²) The sufficiency statement in this theorem is similar to, but strictly stronger than, a result of Kawada and Itô [6, Theorem 8(2)]. They require the stronger hypothesis that $S(\mu)$ be contained in no coset of any proper closed (not necessarily normal) subgroup of G . Our example in 5.1 shows that part (1) of Theorem 8 in [6] is incorrect.

$$(1) \quad \alpha = \int_G \bar{d}_{11}(x) d\mu(x).$$

Since D is unitary, we have

$$(2) \quad |\bar{d}_{11}(x)| \leq 1$$

for each $x \in G$ and therefore

$$|\alpha| \leq \int_G |\bar{d}_{11}(x)| d\mu(x) \leq \mu(G) = 1.$$

Accordingly, by the choice of α , we have $|\alpha| = 1$.

Assume that $\alpha = 1$. Let

$$H = \{x: x \in G, \bar{d}_{11}(x) = 1\} = \left\{ x: x \in G, \bar{D}(x) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & * & & \\ \vdots & & & \\ 0 & & & \end{pmatrix} \right\}.$$

Then H is a closed subgroup of G . Since $\bar{D} \neq D_0$ and is irreducible, there is some $x \in G$ such that $\bar{d}_{11}(x) \neq 1$ and hence $H \neq G$. Then relations (1) and (2), the assumption that $\alpha = 1$, and Lemma 3.3.1 imply that $S(\mu) \subset H$. Hence $G = K \subset H$: a contradiction. Therefore $\alpha \neq 1$.

Thus $\alpha = e^{i\theta} \neq 1$, where θ is a real number. Again, by (1), (2) and Lemma 3.3.1, we have

$$\begin{aligned} S(\mu) \subset F &= \{x: x \in G, \bar{d}_{11}(x) = e^{i\theta}\} \\ &= \left\{ x: x \in G, D(x) = \begin{pmatrix} e^{i\theta} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & * & & \\ \vdots & & & \\ 0 & & & \end{pmatrix} \right\}. \end{aligned}$$

Let $x_0 \in F$. Simple computations show that $x_0 H = F = H x_0$ and therefore, by Lemma 3.3.3, H is a normal subgroup of G . Thus H is a proper closed normal subgroup of $G = K$ and $S(\mu) \subset F = x_0 H$. But this contradicts our hypothesis. We conclude that $\lim_{n \rightarrow \infty} \mu^n = \omega$.

Conversely suppose that $\lim_{n \rightarrow \infty} \mu^n$ exists. Assume however that there exists a proper closed normal subgroup $H \subset G$ and a point $x_0 \in G \setminus H'$ such that $S(\mu) \subset x_0 H$. Set $J = \{x_0^n: n = 0, \pm 1, \pm 2, \dots\}$. Then J is a closed commutative subgroup of G . Since H is a normal subgroup, it follows that $J \cdot H$ is a subgroup of G . Since J and H are both compact, $J \cdot H$ is compact. But $S(\mu) \subset x_0 H \subset J \cdot H$ which is a closed subgroup of G so, since $K = G$, we have $J \cdot H = G$.

Consider the mapping $x \rightarrow xH$ of J onto G/H . This is a homomorphism so, since J is commutative, G/H is a compact commutative group. Since there exist sufficiently many continuous characters of G/H to distinguish points of G/H , [13, p. 99], there is a continuous character ψ of G/H such that $\psi(H) = 1$ and $\psi(x_0H) = e^{i\alpha} \neq 1$. Define ψ' on G by $\psi'(x) = \psi(xH)$ for each $x \in G$. Then ψ' is a continuous character (one-dimensional unitary representation) of G such that $\psi'(x) = \psi(x_0H) = e^{i\alpha} \neq 1$ for each $x \in x_0H$. Thus

$$\hat{\mu}(\psi') = \int_G \psi'(x) d\mu(x) = \int_{S(\mu)} \psi'(x) d\mu(x) = e^{i\alpha}.$$

But $\lim_{n \rightarrow \infty} e^{in\alpha}$ does not exist. Hence $\lim_{n \rightarrow \infty} \hat{\mu}(\psi')^n$ does not exist, and it follows that $\lim_{n \rightarrow \infty} \mu^n$ does not exist. This contradiction completes the proof of the theorem.

Theorems characterizing those $\mu \in \mathcal{P}(G)$ such that $\lim_{n \rightarrow \infty} \mu^n$ exists have also appeared in [11] and [8].

Kloss, in [8], studies $\mathcal{P}(G)$ by using the general theory of compact semigroups. He uses a theorem of K. Numakura and S. Schwarz to observe that, since $\mathcal{P}(G)$ is a compact Hausdorff semigroup, if $\mu \in \mathcal{P}(G)$, then there exists exactly one measure $\lambda \in \{\mu^n: n = 1, 2, \dots\}^-$ such that $\lambda * \lambda = \lambda$. He states in Theorem 3, that if λ is this measure, then the sequence $\{\mu^n: n = 1, 2, \dots\}$ converges to λ if and only if $S(\mu)$ is contained in no coset of $S(\lambda)$ except for $S(\lambda)$ itself.

Urbanik, in [11], calls a sequence $\{\mu_n: n = 1, 2, \dots\} \subset \mathcal{P}(G)$ a normal sequence if for every positive integer k there exists a sequence of positive integers $n_1 < n_2 < n_3 < \dots$ such that

$$\mu_s = \mu_{n_j+s} \quad (s = 1, 2, \dots, k; j = 1, 2, \dots).$$

In particular, the sequence $\mu_1 = \mu_2 = \dots$ is a normal sequence. He proves (Theorem 1) that if $\{\mu_n: n = 1, 2, \dots\}$ is a normal sequence and $\lim_{n \rightarrow \infty} \mu_1 * \dots * \mu_n = \lambda$, then λ is Haar measure on the smallest closed subgroup of G containing $\cup \{S(\mu_n): n = 1, 2, \dots\}$. He also proves (Theorem 2) that if $\{\mu_n: n = 1, 2, \dots\}$ is a normal sequence, H is the smallest closed subgroup of G containing $\cup \{S(\mu_n): n = 1, 2, \dots\}$ and K is the smallest closed subgroup of G containing

$$\cup \{S(\mu_1) \cdot \dots \cdot S(\mu_n) \cdot S(\mu_n)^{-1} \cdot \dots \cdot S(\mu_1)^{-1}: n = 1, 2, \dots\},$$

then the sequence $\{\mu_1 * \dots * \mu_n: n = 1, 2, \dots\}$ converges if and only if $H = K$. This theorem implies that if $\mu \in \mathcal{P}(G)$, then $\lim_{n \rightarrow \infty} \mu^n$ exists if and only if the smallest closed subgroup of G containing $S(\mu)$ is equal to the smallest closed subgroup of G containing $\cup \{S(\mu)^n \cdot (S(\mu)^{-1})^n: n = 1, 2, \dots\}$. In proving these theorems Urbanik makes strong use of the transform $\mu \rightarrow \hat{\mu}$.

3.4. INFINITE PRODUCTS.

3.4.1. DEFINITION. A measure $\mu \in \mathcal{P}(G)$ is called degenerate if $\mu = \epsilon_x$ for some $x \in G$; otherwise μ is called nondegenerate.

3.4.2. DEFINITION. Let $\mu \in \mathcal{P}(G)$. Then μ is said to be an infinite product to the right (left) if there exists a sequence $\{\mu_n: n=1, 2, \dots\} \subset \mathcal{P}(G)$ such that each μ_n is nondegenerate and

$$\mu = \lim_{n \rightarrow \infty} \mu_1 * \mu_2 * \dots * \mu_n \quad \left(\mu = \lim_{n \rightarrow \infty} \mu_n * \mu_{n-1} * \dots * \mu_1 \right).$$

We shall now prove a number of theorems which give sufficient conditions for $\mu \in \mathcal{P}(G)$ to be an infinite product to the right (left).

3.4.3. THEOREM. Let $\mu_1, \dots, \mu_n \in \mathcal{P}(G)$. Suppose that there exist numbers $\alpha_1, \dots, \alpha_n$ ($0 < \alpha_j < 1$) such that $\mu_j(E) \geq \alpha_j \omega(E)$ ($j=1, 2, \dots, n$) for each $E \in \mathcal{B}$. Then there exist $\lambda_1, \dots, \lambda_n \in \mathcal{P}(G)$ and a number t ($0 < t < 1$) such that $\mu_j = \lambda_j * (t\epsilon_e + (1-t)\omega)$ ($j=1, 2, \dots, n$).

Proof. Let $\alpha = \min \{\alpha_1, \dots, \alpha_n\}$ and set $t = 1 - \alpha$. Set $\lambda_j = (\mu_j - (1-t)\omega) \cdot t^{-1}$, ($j=1, 2, \dots, n$). Then each λ_j is in $\mathcal{P}(G)$. Thus $\mu_j = t\lambda_j + (1-t)\omega = t\lambda_j * \epsilon_e + (1-t)\lambda_j * \omega = \lambda_j * (t\epsilon_e + (1-t)\omega)$, ($j=1, 2, \dots, n$).

3.4.4. THEOREM. Suppose that $0 < t < 1$, and that $\text{card } G > 1$. Then $t\epsilon_e + (1-t)\omega$ is an infinite product to the right (left).

Proof. First notice that if $0 < \alpha < 1$ and $0 < \beta < 1$, then

$$\begin{aligned} (\alpha\epsilon_e + (1-\alpha)\omega) * (\beta\epsilon_e + (1-\beta)\omega) &= \alpha\beta\epsilon_e + [\alpha(1-\beta) + (1-\alpha)\beta + (1-\alpha)(1-\beta)]\omega \\ &= \alpha\beta\epsilon_e + (1-\alpha\beta)\omega. \end{aligned}$$

Thus the set $\{\alpha\epsilon_e + (1-\alpha)\omega: 0 \leq \alpha \leq 1\}$ is a subsemigroup of $\mathcal{P}(G)$ which, under the mapping $\alpha \rightarrow \alpha\epsilon_e + (1-\alpha)\omega$, is isomorphic to the multiplicative semigroup of all numbers in the closed unit interval. Thus it follows that if

$$\mu_n = t^{2^{-n}} \cdot \epsilon_e + (1 - t^{2^{-n}}) \cdot \omega \quad (n = 1, 2, \dots),$$

then

$$\begin{aligned} \mu_1 * \mu_2 * \dots * \mu_n &= t^{(2^{-1}+2^{-2}+\dots+2^{-n})} \cdot \epsilon_e + (1 - t^{(2^{-1}+2^{-2}+\dots+2^{-n})}) \cdot \omega \\ &= t^{1-2^{-n}} \cdot \epsilon_e + (1 - t^{1-2^{-n}}) \cdot \omega \end{aligned}$$

and therefore $\lim_{n \rightarrow \infty} \mu_1 * \dots * \mu_n = t \cdot \epsilon_e + (1-t) \cdot \omega$.

3.4.5. THEOREM. Let $\mu \in \mathcal{P}(G)$ and $0 < \alpha < 1$. Suppose that $\mu(E) \geq \alpha\omega(E)$ for each $E \in \mathcal{B}$ and that $\text{card } G > 1$. Then μ is an infinite product to the right (left).

Proof. By Theorem 3.4.3, there exists t ($0 < t < 1$) and $\lambda \in \mathcal{P}(G)$ such that $\mu = \lambda * (t\epsilon_e + (1-t)\omega)$. Then applications of Theorem 3.4.4 and the continuity of convolution on $\mathcal{P}(G)$ complete the proof.

3.4.6. THEOREM. *Let H be a closed subgroup of G such that $\text{card } H > 1$. Suppose that $\mu \in \mathcal{P}(G)$, $S(\mu) = H$, and that there is a real number α , $0 < \alpha < 1$, such that $\mu(E) \geq \alpha\omega_H(E)$ for each $E \in \mathcal{B}$. Then μ is an infinite product to the right (left).*

Proof. Clearly H is a compact group. Define $\mu' \in \mathcal{P}(H)$ by $\mu'(E) = \mu(E)$ for each Borel set $E \subset H$. Then $\mu'(E) \geq \alpha\omega_H(E)$ for each Borel set $E \subset H$. Thus, by Theorem 3.4.5, there exists a sequence $\{\mu'_n : n = 1, 2, \dots\} \subset \mathcal{P}(H)$ such that $\mu' = \lim_{n \rightarrow \infty} \mu'_1 * \dots * \mu'_n$. Now extend each μ'_n to a probability measure $\mu_n \in \mathcal{P}(G)$ by defining $\mu_n(E) = \mu'_n(E \cap H)$ for each $E \in \mathcal{B}$. Then we have $\mu = \lim_{n \rightarrow \infty} \mu_1 * \dots * \mu_n$.

3.4.7. LEMMA. *Let A be a nonvoid closed subset of G and let $x \in G$. Suppose that $\mu \in \mathcal{P}(G)$ and that $S(\mu) = xA$. Set $\lambda = \epsilon_{x^{-1}} * \mu$. Then $S(\lambda) = A$, $\mu = \epsilon_x * \lambda$ and $\lambda(E) = \mu(xE)$ for each $E \in \mathcal{B}$.*

The proof is left to the reader.

3.4.8. THEOREM. *Let H be a closed subgroup of G such that $\text{card } H > 1$ and let F be a finite subset of G such that no two points of F are in the same left (right) coset of H . Let $\mu \in \mathcal{P}(G)$ and suppose that $S(\mu) = FH$ ($S(\mu) = HF$). Suppose also that there exists a number α such that $0 < \alpha < 1$ such that $\mu(E) \geq \alpha\omega_H(x^{-1}E)$ ($\mu(E) \geq \alpha\omega_H(Ex^{-1})$) for every $x \in F$ and $E \in \mathcal{B}$. Then μ is an infinite product to the right (left).*

Proof. Let $F = \{x_1, x_2, \dots, x_n\}$. For each j ($1 \leq j \leq n$) define μ'_j by $\mu'_j(E) = \mu((x_jH) \cap E)$ for all $E \in \mathcal{B}$. Clearly

$$\mu'_j(x_jH) = \mu(x_jH) \geq \alpha\omega_H(x_j^{-1}x_jH) = \alpha\omega_H(H) = \alpha > 0.$$

Let $\alpha_j = \mu'_j(x_jH)$ and note that $\alpha_j \geq \alpha > 0$ ($j = 1, 2, \dots, n$). For each j let $\mu_j = (1/\alpha_j) \cdot \mu'_j$. Then $\mu_j \in \mathcal{P}(G)$ ($j = 1, 2, \dots, n$). Also it is easily verified that $S(\mu_j) = x_jH$ for each j . Notice that

$$\sum_{j=1}^n \alpha_j \mu_j(E) = \sum_{j=1}^n \mu'_j(E) = \sum_{j=1}^n \mu(E \cap (x_jH)) = \mu(E \cap (FH)) = \mu(E)$$

for all $E \in \mathcal{B}$ since $x_jH \cap x_kH = \emptyset$ if $j \neq k$. Thus $\mu = \sum_{j=1}^n \alpha_j \mu_j$.

Applying Lemma 3.4.7, we have that for each j there exists a $\lambda_j \in \mathcal{P}(G)$ such that $S(\lambda_j) = H$ and $\mu_j = \epsilon_{x_j} * \lambda_j$. Then $\mu = \sum_{j=1}^n \alpha_j \mu_j = \sum_{j=1}^n \alpha_j \epsilon_{x_j} * \lambda_j$.

Now for each $E \in \mathcal{B}$ and for all j we have

$$\begin{aligned} \lambda_j(E) &= \epsilon_{x_j}^{-1} * \mu_j(E) = \mu_j(x_jE) = \mu'_j(x_jE) \cdot (1/\alpha_j) = \mu(x_jE \cap x_jH) \cdot (1/\alpha_j) \\ &= \mu(x_j(E \cap H)) \cdot (1/\alpha_j) \geq (\alpha/\alpha_j) \cdot \omega_H(E \cap H) \geq \alpha\omega_H(E). \end{aligned}$$

Hence, by Theorem 3.4.3 there exist $\nu_j \in P(G)$ ($j=1, 2, \dots, n$) and a number t ($0 < t < 1$) such that $S(\nu_j) = H$ and $\lambda_j = \nu_j * (t\epsilon_e + (1-t)\omega_H)$ for each j . Then

$$\mu = \sum_{j=1}^n \alpha_j \epsilon_{x_j} * \lambda_j = \left[\sum_{j=1}^n \alpha_j \epsilon_{x_j} * \nu_j \right] * (t\epsilon_e + (1-t)\omega_H).$$

Evidently $S(t\epsilon_e + (1-t)\omega_H) = H$, so by Theorem 3.4.4 $t\epsilon_e + (1-t)\omega_H$ is an infinite product to the right and hence μ is an infinite product to the right. This completes the proof.

4. Finite groups. In this section G will be an arbitrary finite group, the topology on G being the discrete topology. The letter n will be reserved to denote the order of G .

Since G is discrete, every subset of G is a Borel set. If $E \subset G$, it follows that

$$\mu(E) = \sum_{x \in E} \mu(\{x\}).$$

Moreover if $\{\mu_n: n=1, 2, \dots\}$ is a sequence in $\mathcal{O}(G)$ and if $\mu \in \mathcal{O}(G)$, it is clear that $\mu_n \rightarrow \mu$ if and only if $\mu_n(\{x\}) \rightarrow \mu(\{x\})$ for each $x \in G$.

4.1. INFINITE PRODUCTS IN $\mathcal{O}(G)$. In this section we identify all infinite products in $\mathcal{O}(G)$.

4.1.1. LEMMA. *Let $\mu \in \mathcal{O}(G)$ and suppose that μ is an infinite product to the right (left). Then there exists a sequence $\{\mu_j: j=1, 2, \dots\} \subset \mathcal{O}(G)$ such that $S(\mu) \subset S(\mu_1) = S(\mu_1 * \dots * \mu_k)$ ($k=1, 2, \dots$) and $\mu = \lim_{k \rightarrow \infty} \mu_1 * \dots * \mu_k$.*

Proof. Since μ is an infinite product to the right, there exists a sequence of nondegenerate measures $\{\mu_j: j=1, 2, \dots\} \subset \mathcal{O}(G)$ such that $\mu = \lim_{k \rightarrow \infty} \mu'_1 * \dots * \mu'_k$. Set $\lambda'_k = \mu'_1 * \dots * \mu'_k$ for each k . Since G has exactly 2^n subsets there exists a subsequence $\{\lambda'_{k_j}: j=1, 2, \dots\}$ of $\{\lambda'_k: k=1, 2, \dots\}$ such that $S(\lambda'_{k_1}) = S(\lambda'_{k_j})$ for each j . Now define $\mu_1 = \lambda'_{k_1}$, $\mu_2 = \mu'_{k_1+1} * \dots * \mu'_{k_2}$, \dots , $\mu_j = \mu'_{k_{j-1}+1} * \dots * \mu'_{k_j}$, \dots . Then $\mu_1 * \mu_2 * \dots * \mu_j = \lambda'_{k_j}$ so $\lim_{j \rightarrow \infty} \mu_1 * \dots * \mu_j = \lim_{j \rightarrow \infty} \lambda'_{k_j} = \lim_{k \rightarrow \infty} \lambda'_k = \mu$. Clearly each μ_j is nondegenerate and $S(\mu_1) = S(\lambda'_{k_1}) = S(\lambda'_{k_j}) = S(\mu_1 * \dots * \mu_j)$ for each j .

Let $x \in S(\mu)$. Then $\mu(\{x\}) > 0$, so that there exists an integer j_0 such that $|\mu_1 * \dots * \mu_j(\{x\}) - \mu(\{x\})| < 2^{-1}\mu(\{x\})$ if $j \geq j_0$. Hence $\mu_1 * \dots * \mu_{j_0}(\{x\}) > 0$ so $x \in S(\mu_1 * \dots * \mu_{j_0}) = S(\mu_1)$ and therefore $S(\mu) \subset S(\mu_1)$.

4.1.2. THEOREM. *Let $\mu \in \mathcal{O}(G)$ and suppose that $\mu = \lim_{k \rightarrow \infty} \mu_1 * \dots * \mu_k$ where $\{\mu_k: k=1, 2, \dots\} \subset \mathcal{O}(G)$. Then there exists a sequence $\{\nu_{k+1}: k=1, 2, \dots\} \subset \mathcal{O}(G)$ such that $\mu = \mu_1 * \dots * \mu_k * \nu_{k+1}$ for each k .*

This theorem is proved for the case that G is commutative in [3, p. 608], but the proof given there applies equally well to the present theorem.

4.1.3. THEOREM. *Let $\mu \in \mathcal{O}(G)$. Then μ is an infinite product to the right*

(left) if and only if there exist a subgroup H of G of order > 1 and a nonvoid set $A \subset G$ such that $S(\mu) = AH(S(\mu) = HA)$.

Proof. The sufficiency of this condition follows from Theorem 3.4.8, as the following argument shows. It is possible to find a subset B of A such that $AH = BH$ and no two points of B are in the same left coset of H . Such a set B can be formed as follows: for each left coset L of H such that $L \cap A \neq \emptyset$ let x_L be a point of $L \cap A$, then set $B = \{x_L : L \text{ is a left coset of } H, L \cap A \neq \emptyset\}$.

Also, if $\alpha = \min \{\mu(\{x\}) : x \in S(\mu) = AH\}$, then $\mu(E) \geq \alpha \geq \alpha \omega_H(x^{-1}E)$, for each $x \in A$ unless $\mu(E) = 0$, in which case $E \cap AH = 0$ and $A^{-1}E \cap H = 0$. Then $\omega_H(x^{-1}E) = 0$ for each $x \in A$.

We now prove the necessity of the condition. Suppose that μ is an infinite product to the right. Choose a sequence $\{\mu_k : k = 1, 2, \dots\} \subset \mathcal{P}(G)$ as in Lemma 4.1.1 and set $\lambda_k = \mu_1 * \dots * \mu_k$ ($k = 1, 2, \dots$). Then $\mu = \lim_{k \rightarrow \infty} \lambda_k$ and $S(\mu) \subset S(\mu_1) = S(\lambda_k)$ for each k . Let $A = S(\mu_1)$. Since μ_2 is nondegenerate, there exist $x, y \in S(\mu_2)$ such that $x \neq y$. Now $A \cdot S(\mu_2) = S(\mu_1)S(\mu_2) = S(\mu_1 * \mu_2) = S(\lambda_2) = S(\mu_1) = A$. Hence $Ax \subset A$ and $Ay \subset A$. But $\text{card } Ax = \text{card } A = \text{card } Ay \leq n$. Hence $Ax = A = Ay$ and $Axy^{-1} = A$. Let $h = xy^{-1} \neq e$ and let H be the cyclic subgroup of G generated by h . Since $Ah = A$ we have $Ah^k = Ah^{k-1} = \dots = Ah = A$ ($k = 1, 2, \dots$) and hence $AH = A$.

By Theorem 4.1.2, there exists $\nu \in \mathcal{P}(G)$ such that $\mu = \mu_1 * \nu$. Then $S(\mu) = S(\mu_1) \cdot S(\nu) = A \cdot S(\nu)$. Accordingly $A \cdot S(\nu) = S(\mu) \subset S(\mu_1) = A$. But

$$\text{card } A \cdot S(\nu) \geq \text{card } A$$

and hence $S(\mu) = A = AH$. This completes the proof.

4.1.4. DEFINITION. Let $\mu \in \mathcal{P}(G)$. Then μ is said to be infinitely factorable if for each positive integer m there exists a set $\{\mu_1, \dots, \mu_m\} \subset \mathcal{P}(G)$ such that each μ_j is nondegenerate and $\mu = \mu_1 * \dots * \mu_m$.

4.1.5. THEOREM. Let $\mu \in \mathcal{P}(G)$ and suppose that μ is infinitely factorable. Then there exist a subgroup H of order > 1 of G and two nonvoid subsets A and B of G such that $S(\mu) = AHB$.

Proof. There exists a set $\{\mu_1, \dots, \mu_n\} \subset \mathcal{P}(G)$ such that each μ_j is nondegenerate and $\mu = \mu_1 * \dots * \mu_n$. Then $2 \leq \text{card } S(\mu_1) \leq \text{card } S(\mu_1 * \mu_2) \leq \dots \leq \text{card } S(\mu_1 * \mu_2 * \dots * \mu_n) = \text{card } S(\mu) \leq n$. Thus there exists k such that $1 \leq k \leq n$ and $\text{card } S(\mu_1 * \dots * \mu_k) = \text{card } S(\mu_1 * \dots * \mu_{k+1})$. Set $A = S(\mu_1 * \dots * \mu_k)$ and $C = S(\mu_{k+1})$. Then $\text{card } A = \text{card } AC$. Since μ_{k+1} is nondegenerate, there exist $x, y \in C$ such that $x \neq y$. Then $Ax \subset AC$ and $Ay \subset AC$. But $\text{card } Ax = \text{card } A = \text{card } AC$ and $\text{card } Ay = \text{card } A = \text{card } AC$. Hence $Ax = AC = Ay$. Thus $Axy^{-1} = A$ and $xy^{-1} \neq e$. Set $h = xy^{-1}$ and let H be the cyclic subgroup generated by h . Then the order of H is > 1 and, as in the previous proof, $AH = A$. Now set $B = S(\mu_{k+1} * \dots * \mu_n)$. Then $S(\mu) = S(\mu_1 * \dots * \mu_k) \cdot S(\mu_{k+1} * \dots * \mu_n) = AB = AHB$. This completes the proof.

4.1.6. COROLLARY. Let $\mu \in \mathcal{P}(G)$. Suppose that μ is an infinite product to the right or to the left. Then μ is infinitely factorable.

Proof. This follows immediately from Theorem 4.1.2.

4.1.7. COMMENT. Theorems 4.1.3, 4.1.5 and 4.1.6 show that if G is commutative, then a measure in $\mathcal{P}(G)$ is infinitely factorable if and only if it is an infinite product. A theorem appears in [12] which claims that this is true even when G is not commutative. This theorem however is false as is shown in 5.1. It would be interesting to know whether or not the converse of Theorem 4.1.5 is true.

5. Counterexamples. In this section we give counterexamples to two published theorems. The first refers to Theorem 8(1) in [6] and the second to a theorem in [12].

5.1. COUNTEREXAMPLE. In [6] it is claimed that if G is any metrizable compact group, $\mu \in \mathcal{P}(G)$, μ is proper on G , and $S(\mu)$ is contained in a coset x_0H or Hx_0 ($x_0 \notin H$, $H \neq G$) of a closed subgroup H , then H is normal. Consider the following example.

Let $G = S_3$, the symmetric group on three letters. The elements of G will be written in cycles: $G = \{1, (12), (13), (23), (123), (132)\}$. Define μ on G by $\mu(\{(123)\}) = \mu(\{(13)\}) = 1/2$ and $\mu(\{x\}) = 0$ otherwise. Then $\mu \in \mathcal{P}(G)$. Now μ is proper on G since $S(\mu) = \{(123), (13)\}$ and the only subgroup of G containing $S(\mu)$ is G itself. Let $H = \{1, (12)\}$ and $x_0 = (123)$. Then $x_0H = S(\mu)$ so $S(\mu) \subset x_0H$ ($x_0 \notin H$ and $H \neq G$). But $Hx_0 = \{(123), (23)\} \neq x_0H$. Hence H is not a normal subgroup of G .

5.2. COUNTEREXAMPLE. The following is an example of an infinitely factorable measure which is neither an infinite product to the right nor to the left.

Let $G = A_4$, the alternating group on four letters. The elements of A_4 are written in cycles:

$$G = A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (124), (132), (134), (142), (143), (234), (243)\}.$$

Let $A = \{1, (123)\}$ and $H = \{1, (12)(34)\}$. Then

$$AHA = \{1, (12)(34), (123), (134), (243), (132), (124)\}$$

and hence AHA has exactly seven elements so, by Lagrange's theorem, can be neither a union of right cosets nor a union of left cosets of any subgroup of A_4 of order > 1 . Thus no probability measure on A_4 having support equal to AHA can possibly be an infinite product to the right or to the left.

Now let μ_1 and μ_2 be any two members of $\mathcal{P}(A_4)$ such that $S(\mu_1) = S(\mu_2) = A$ and let ω_H be, as usual, Haar measure on H . Then ω_H is idempotent. Set $\mu = \mu_1 * \omega_H * \mu_2$. Then $S(\mu) = AHA$ and μ is not an infinite product, but $\mu = \mu_1 * \omega_H * \mu_2 = \mu_1 * \omega_H^m * \mu_2$ for each positive integer m and hence μ is infinitely factorable.

BIBLIOGRAPHY

1. Paul Halmos, *Measure theory*, New York, D. Van Nostrand Co., Inc., 1950.
2. Edwin Hewitt, *Remarks on the inversion of Fourier-Stieltjes transforms*, Ann. of Math. ser. 2 vol. 57 (1953) pp. 458-474.
3. Edwin Hewitt and H. S. Zuckerman, *Arithmetic and limit theorems for a class of random variables*, Duke Math. J. vol. 22 (1955) pp. 595-615.
4. ———, *Finite dimensional convolution algebras*, Acta Math. vol. 93 (1955) pp. 67-119.
5. Tetujiro Kakehashi, *Stationary periodic distributions*, J. Osaka Inst. Sci. Tech. vol. 1 (1949) pp. 21-25.
6. Yukiyosi Kawada and Kiyosi Itô, *On the probability distributions on a compact group*, I, Proc. Phys.-Math. Soc. Japan ser. 3, vol. 22 (1940) pp. 977-998.
7. J. L. Kelley, *General topology*, New York, D. Van Nostrand Co., Inc., 1955.
8. B. M. Kloss, *Limiting distributions of sums of independent random variables, taking values from a bicomact group*, Dokl. Akad. Nauk SSSR (N.S.) vol. 109 (1956) pp. 453-455 (Russian).
9. L. H. Loomis, *An introduction to abstract harmonic analysis*, New York, D. Van Nostrand Co., Inc., 1953.
10. Karl Stromberg, *A note on the convolution of regular-measures*, to appear in Math. Scand.
11. K. Urbanik, *On the limiting probability distributions on a compact topological group*, Fund. Math. vol. 3 (1957) pp. 253-261.
12. N. N. Vorob'yov, *Addition of independent random variables on finite abelian groups*, Mat. Sb. vol. 34 (1954) pp. 89-126 (Russian).
13. Andre Weil, *L'integration dans les groupes topologiques et ses applications*, Actualités Sci. Ind., no. 869, 1940.
14. J. G. Wendel, *Haar measure and the semigroup of measures on a compact group*, Proc. Amer. Math. Soc. vol. 5 (1954) pp. 923-929.

UNIVERSITY OF WASHINGTON,
 SEATTLE, WASHINGTON
 YALE UNIVERSITY,
 NEW HAVEN, CONNECTICUT