DERIVATIONS OF OPERATOR GROUP ALGEBRAS.

By RICHARD V. KADISON and JOHN R. RINGROSE.*

1. **Introduction.** In [2, Theorem 9] Kaplansky proves that each derivation of a type I von Neumann algebra is inner. Establishing a conjecture of Kaplansky, Sakai shows [5] that each derivation of a C^*-algebra is bounded. Using these results Miles [3] notes that each derivation of a C^*-algebra is induced by an operator in the weak closure of some faithful representation of the algebra (a direct sum of irreducible representations from each equivalence class). Again using [2] and [5], it is shown in [1, Theorem 4] that each derivation of a concretely represented C^*-algebra is spatial (i. e., has the form $A \rightarrow BA - AB$ for some bounded operator B). It is also shown in [1, Theorem 7] that each derivation of a hyperfinite von Neumann algebra is inner; that under various assumptions on B the derivation is inner and that the question of whether all derivations of a semifinite von Neumann algebra are inner is equivalent to the question of whether all derivations of a finite von Neumann algebra are inner.

The main result of this paper is:

THEOREM 1.1. *Each derivation of the von Neumann algebra generated by the regular representation of a discrete group is inner.*

This result coupled with those of [1] makes it seem very likely that all derivations of von Neumann algebras are inner. It implies, in particular that certain non-hyperfinite factors [4, Lemma 6.3.1] have only inner derivations. We establish it in a sequence of seven lemmas in Section 2, deferring to the last section a Tauberian result which is at the heart of the proof. This Tauberian result, as we need it for the derivation theorem, states that a function on a space acted upon by a transitive permutation group which differs from each of its transforms under the group by a function from a fixed ball in l_2 is itself an l_2 function plus a constant. In the final section, we prove the more general form of this fact corresponding to the action of arbitrary permutation groups. Its application is to the action of a group on a right coset homogeneous space by right translation.

Received April 2, 1965.

* Research conducted with the support of ONR contract NR 043-325 and NSF GP 4059.

We review some facts about operator group algebras and establish some notation. Let G be a (discrete) group, L_a the unitary operator on $l_2(G)$ defined by $L_af(g) = f(a^{-1}g)$ and R_a the unitary operator defined by $R_af(g) = f(ga)$. The mappings $a \rightarrow L_a$ and $a \rightarrow R_a$ are unitary representations of G, the left and right regular representations of G, respectively. The weak closures of finite linear combinations of L_a's and R_a's are von Neumann algebras, the left and right von Neumann group algebras, $\mathcal{L}$ and $\mathcal{R}$, respectively. From [4, Lemma 5.3.4], $\mathcal{R} = \mathcal{L}'$ (the commutant of $\mathcal{L}$).

We shall show that each derivation of $\mathcal{L}$ (equivalently, from [1, Lemma 5], of $\mathcal{R}$) is inner. To this end, we consider the basis $\{x_a\colon a \text{ in } G\}$ for $l_2(G)$ defined by $x_g(h) = \delta_{h,g}$, and determine the properties which the matrix representation of an operator on $l_2(G)$ must have in order that it lie in $\mathcal{L}$, in $\mathcal{R}$, in $\mathcal{L} + \mathcal{R}$ or in $D(\mathcal{L})$ $(= D(\mathcal{R}))$, the set of bounded operators on $l_2(G)$ which induce derivations of $\mathcal{L}$. From [1, Theorem 4], we need establish only that $D(\mathcal{L}) = \mathcal{L} + \mathcal{R}$ in order to prove that all derivations of $\mathcal{L}$ (and $\mathcal{R}$) are inner. Assume that A lies in $D(\mathcal{L})$.

For T a bounded operator on $l_2(G)$, let $T(a,b) = (Tx_b, x_a)$ and note that $L_c{}^*TL_c(a,b) = T(ca,cb)$ while $R_c{}^*TR_c(a,b) = T(ac^{-1},bc^{-1})$. Thus T lies in $\mathcal{L}$ if and only if $T(ac,bc) = T(a,b)$ and T lies in $\mathcal{R}$ if and only if $T(ca,cb) = T(a,b)$, for each a, b, c in G (this under the assumption that $(T(a,b))$ is the matrix of a *bounded* operator T). It follows from these considerations that $\mathcal{L} \cap \mathcal{R}$ consists of scalar multiples of the identity operator I (we say that $\mathcal{L}$ and $\mathcal{R}$ are factors) if and only if for each a in G other than the identity e the set (a) of conjugates of a is infinite. Since $T - L_c{}^*TL_c = L_c{}^*(L_cT - TL_c)$, T lies in $D(\mathcal{L})$ if and only if $T - L_c{}^*TL_c$ lies in $\mathcal{L}$ for each c in G (equivalently, if and only if $T - R_c{}^*TR_c$ lies in $\mathcal{R}$ for each c in G). Thus T lies in $D(\mathcal{L})$ if and only if

$$T(a,b) - T(ca,cb) = T(ag,bg) - T(cag,cbg) \tag{1}$$

for each a, b, c and g in G. In words rather than formulas, T lies in $D(\mathcal{L})$, if and only if the difference of two left translates of a matrix coefficient of T is right invariant.

We are grateful to H. Sah for discussions of group theoretic constructs which led us to consider the Tauberian result (Theorem 3.8) in the setting of a permutation group acting on a set.

2. The main result. If we knew that $A = B + C$ with B in $\mathcal{L}$ and C in $\mathcal{R}$, then $A(g,ag) = B(g,ag) + C(g,ag) = B(e,a) + C(e,g^{-1}ag)$; so that as g ranges through distinct representatives of the cosets Z_ag in G/Z_a,

$C(e, g^{-1}ag)$ ranges through distinct matrix coefficients in the e row of $(C(a,b))$. In particular we should have that A_a is a function on G/Z_a, where Z_a is the centralizer of a and $A_a(Z_a g) = A(g, ag)$. Since $(C(a,b))$ is to be the matrix of a bounded operator, each of its rows is in $l_2(G)$, and we should have A_a tends to the limit $B(e,a)$ at ∞ on G/Z_a if (a) is infinite. If $(A(a,b))$ satisfies the condition:

(2) $\quad A(ca, cb) = A(a,b)$, for each c in G when (ba^{-1}) is finite

then $B(e, ghg^{-1}) = A(g, gh) - C(e,h) = A(e,h) - C(e,h) = B(e,h)$ for each g in G when (h) is finite, i.e., $g \to B(e,g)$ is constant on (h) and it turns out that we may choose 0 as this constant value. The sequence of lemmas which follows establishes that A_a is a function on G/Z_a which has a limit at ∞, that A can be replaced by an operator whose matrix satisfies (2) and that, after this replacement is made, $B(e,a)$ as described is the e row of a matrix corresponding to an operator B in $\mathcal{L}$ such that $A - B$ $(= C)$ lies in $\mathcal{R}$.

We adopt the usual terminology that the point added in forming the one point compactification of a locally compact space is the point ∞ and that the behavior of a function on the locally compact space at ∞ is the behavior of the function on the one-point compactification in the neighborhood of ∞. In particular we may speak of $\overline{\lim} f$ and $\underline{\lim} f$ at ∞, as well as $\lim f$ at ∞ (if this limit exists). We make use of Lemma 3.7, in the following lemma and Lemma 3.1 in the proof of Lemma 2.7, deferring until the final section the proofs of Lemmas 3.1 and 3.7.

LEMMA 2.1. *A_a is single-valued and has a limit at ∞ on G/Z_a.*

Proof. We wish to show that $A(bg, abg) = A(g, ag)$, when $ba = ab$. Since $A(bg, abg) = A(bg, bag)$, we have, from (1)

$$\begin{aligned}\alpha = A(g, ag) - A(bg, bag) &= A(e,a) - A(b, ba) = A(b, ab) - A(b^2, bab)\\ &= A(b, ba) - A(b^2, b^2 a) = \cdots = A(b^{n-1}, b^{n-1}a) - A(b^n, b^n a).\end{aligned}$$

Thus $n\alpha = A(e,a) - A(b^n, b^n a)$ and $n|\alpha| \leqq 2\|A\|$ for each n. Hence $\alpha = 0$.

Note that

$$\begin{aligned}\sum_{G/Z_a} |A_a(Z_a g) - A_a(Z_a gh)|^2 &= \sum_n |A(g_n, ag_n) - A(g_n h, ag_n h)|^2\\ &= \sum_n |A(e, g_n^{-1}ag_n) - A(h, g_n^{-1}ag_n h)|^2 \leqq 4\|A\|^2\end{aligned}$$

where $\{g_n\}$ is a complete set of representatives of the cosets in G/Z_a. This inequality results from the fact that $\{A(e, g_n^{-1}ag_n)\}$ and $\{A(h, g_n^{-1}ag_nh)\}$ are distinct elements of the e and h rows for the matrix for A and the known relation of the l_2-norm of such rows to the bound of the operator.

Since G acts as a transitive permutation group on G/Z_a by right multiplication, Lemma 3.7 applies and A_a has a limit at ∞.

LEMMA 2.2. *If $(A(a,b))$ satisfies (2) and $C(a,b) = A(a,b) - B(e,ba^{-1})$, where $B(e,h) = 0$ if (h) is finite and $B(e,h) = \lim_\infty A_h$ if (h) is infinite, then $C(ca,cb) = C(a,b)$, for each a, b and c in G.*

Proof. If (ba^{-1}) is finite,

$$C(ca,cb) = A(ca,cb) - B(e, cba^{-1}c^{-1})$$
$$= A(ca,cb) = A(a,b) = A(a,b) - B(e,ba^{-1}) = C(a,b),$$

from (2).

Suppose that (ba^{-1}) is infinite. We wish to show:

(3) $A(ca,cb) - A(a,b) = B(e, cba^{-1}c^{-1}) - B(e, ba^{-1})$, for each c in G.

If $\{g_n\}$ is a complete set of representatives for the cosets in $G/Z_{ba^{-1}}$, then $\{cg_nc^{-1}\}$, hence $\{cg_n\}$, are complete sets of representatives for the cosets in $G/Z_{cba^{-1}c^{-1}}$. Thus, with positive ϵ assigned, for suitable n,

$$\epsilon > |B(e,ba^{-1}) - A(g_n, ba^{-1}g_n)| + |A(cg_n, cba^{-1}g_n) - B(e, cba^{-1}c^{-1})|$$
$$\geqq |B(e,ba^{-1}) - B(e,cba^{-1}c^{-1}) - [A(g_ng_n^{-1}a, ba^{-1}g_ng_n^{-1}a)$$
$$- A(cg_ng_n^{-1}a, cba^{-1}g_ng_n^{-1}a)]|,$$

from which (3) follows.

LEMMA 2.3. *If $B_a(Z_ag) = B(e, g^{-1}ag)$ and $C_a(Z_ag) = C(e, g^{-1}ag)$, then with (a) infinite B_a and C_a vanish at ∞ on G/Z_a.*

Proof. From Lemma 2.2, we have $A(g,ag) = B(e,a) + C(e, g^{-1}ag)$. Since $A_a(Z_ag) = A(g,ag)$ and $B(e,a)$ is $\lim_\infty A_a$ on G/Z_a, C_a vanishes at ∞ on G/Z_a. But A'_a defined on G/Z_a by
$A'_a(Z_ag) = A(e, g^{-1}ag)$ $(= B(e, g^{-1}ag) + C(e, g^{-1}ag) = B_a(Z_ag) + C_a(Z_ag))$ vanishes at ∞, since the e row of $(A(a,b))$ lies in $l_2(G)$. Since C_a vanishes at ∞ on G/Z_a, B_a $(= A'_a - C_a)$ does.

LEMMA 2.4. *If $bhg^{-1}b^{-1} = ahg^{-1}a^{-1}$ then $A(bg,bh) = A(ag,ah)$.*

Proof. Since $(ag)^{-1}(ahg^{-1}a^{-1})ag = (bg)^{-1}(bhg^{-1}b^{-1})bg$ and $ahg^{-1}a^{-1} = bhg^{-1}b^{-1}$, we have $A(ag,ah) = A(ag, (ahg^{-1}a^{-1})ag) = A(bg, (bhg^{-1}b^{-1})bg)$
and only if that induced by A is. If ba^{-1} lies in S, then $A^{|S}(ca,cb) = A^{|S}(a,b)$;
$= A(bg,bh)$, from Lemma 2.1.

For each finite (h), we choose a set $a_1, \cdots, a_n$ of elements in G which give rise to all (distinct) permutations of (h) induced by inner automorphisms of G; and we denote by $A^{|h}$ the operator $\frac{1}{n}(L_{a_1}{}^*AL_{a_1} + \cdots + L_{a_n}{}^*AL_{a_n})$ (we write $A^{|h_1|h_2}$ for $(A^{|h_1})^{|h_2}$).

LEMMA 2.5. *If (h_j) is finite for $j = 1, \cdots, m$, then* $\|A^{|h_1\cdots|h_m}\| \leqq \|A\|$, *$A^{|h_1\cdots|h_m}$ induces the same derivation of $\mathcal{R}$ as A does and*

$$A^{|h_1\cdots|h_m}(ca, cb) = A^{|h_1\cdots|h_m}(a, b)$$

for each c in G when $ba^{-1} = h_j$ for some j.

Proof. Since each L_g is a unitary operator in $\mathcal{L}$, if T induces a derivation of $\mathcal{L}$, $L_g{}^*TL_g$ induces the same derivation of $\mathcal{R}$ as T does (cf. [1, Lemma 5]), and $\| L_g{}^*TL_g \| = \| T \|$.

The first and second assertions follow from this and the definition of $T^{|h}$.

With $T^{|h_j} = \frac{1}{n}(L_{a_1}{}^*TL_{a_1} + \cdots + L_{a_n}{}^*TL_{a_n})$, we have

$$T^{|h_j}(ca, cb) = \frac{1}{n}\sum_j T(a_jca, a_jcb) = \frac{1}{n}\sum_j T(a_ja, a_jb) = T^{|h_j}(a, b),$$

from Lemma 2.4, since $a_{j'}ba^{-1}a_{j'}{}^{-1} = a_jcba^{-1}c^{-1}a_j{}^{-1}$ for some permutation $j \to j'$ of $\{1, \cdots, n\}$, by choice of $a_1, \cdots, a_n$. Hence

$$L_g{}^*T^{|h_j}L_g(ca, cb) = T^{|h_j}(gca, gcb) = T^{|h_j}(a, b)$$

for each g in G; so that

$$T^{|h_j|h_{j+1}}(ca, cb) = T^{|h_j|h_{j+1}}(a, b) \text{ and } T^{|h_j\cdots|h_m}(ca, cb) = T^{|h_j\cdots|h_m}(a, b).$$

Replacing T by $A^{|h_1\cdots|h_{j-1}}$ completes the proof.

For each finite subset S of G_0, the subgroup of G consisting of elements h with (h) finite, we assign a linear order $h_1, h_2, \cdots, h_m$ to its members and denote $A^{|h_1\cdots|h_m}$ by $A^{|S}$.

LEMMA 2.6. *Relative to the family $\mathcal{S}$ of finite subsets of G_0 directed by inclusion, the net $\{A^{|S}\}$ has a (cofinal) subnet weak-operator convergent to an operator A_0 satisfying $A_0(ca, cb) = A_0(a, b)$ for each c in G and each a, b in G such that (ba^{-1}) is finite. A_0 induces a derivation of $\mathcal{L}$ which is inner if and only if that induced by A is.*

Proof. Since $\| A^{|S} \| \leqq \| A \|$, the ball of radius $\| A \|$ is weak-operator compact, and $A^{|S}$ induces the same derivation of $\mathcal{R}$ as A does, the net $\{A^{|S}\}$ has a subnet convergent to A_0, and A_0 induces the same derivation of $\mathcal{R}$ as A does. From [1, Lemma 5], A_0 induces a derivation of $\mathcal{L}$ which is inner if and only if that induced by A is. If ba^{-1} lies in S, then $A^{|S}(ca, cb) = A^{|S}(a, b)$; so that $A_0(ca, cb) = A_0(a, b)$, for each c in G, from Lemma 2.5 and the fact that A_0 is the limit of a (cofinal) subnet of $\{A^{|S}\}$.

We may assume, henceforth, that A satisfies (2) (replacing A by A_0).

LEMMA 2.7. *Taking $B(a,b)$ as $B(e, ba^{-1})$, $(B(a,b))$ is the matrix of a (bounded) operator B in $\mathcal{L}$.*

Proof. Let $\mathcal{F}$ be the family of finite subsets of $\bigcup_{(a)\text{ infinite}} G/Z_a$ directed by inclusion. From Lemma 3.1, we can choose an element a_S^{-1} in G, for each S in $\mathcal{F}$, which lies in none of the cosets in S. The net $\{A - L_{a_S}{}^* A L_{a_S}\}$ lies in the weak-operator compact ball of radius $2\,\|A\|$ in $\mathcal{L}$ and therefore has a (cofinal) subnet weak-operator convergent to some T in this ball.

We show that $T(a,b) = T(e, ba^{-1}) = B(a,b) = B(e, ba^{-1})$. Note that

$$\begin{aligned}(A - L_{a_S}{}^* A L_{a_S})(e,h) &\\ &= A(e,h) - A(a_S, a_S h) = B(e,h) - B(e, a_S h a_S^{-1})\\ &= B(e,h) - B_h(Z_h a_S^{-1}),\end{aligned}$$

by Lemma 2.2. Now B_h tends to 0 at ∞ on G/Z_h, for $(A(a,b))$ satisfies (2) so that $B_h(Z_h a^{-1}) = B(e, aha^{-1}) = 0$, with (h) finite; and with (h) infinite Lemma 2.3 applies. Thus $B(e,h) - B_h(Z_h a_S^{-1})$ tends to $B(e,h)$ over $\mathcal{F}$, for if S contains a suitable finite subset of G/Z_h, $|B_h(Z_h a_S^{-1})|$ is small since $Z_h a_S^{-1}$ is not in this subset by choice of a_S. Hence $T(e,h) = B(e,h)$ for each h; so that $(B(a,b))$ is the matrix for T.

Proof of Theorem 1.1. Since $C(a,b) = A(a,b) - B(a,b)$, $(C(a,b))$ is the matrix of a bounded operator C. Since $C(ca,cb) = C(a,b)$ (Lemma 2.2), C lies in $\mathcal{R}$. Since $A = B + C$ with B in $\mathcal{L}$ and C in $\mathcal{R}$, the derivation of $\mathcal{L}$ induced by A is inner.

3. A Tauberian result. We now prove the results, concerning groups and in particular permutation groups, which were assumed in the previous section. The first of these is the following.

LEMMA 3.1. *A group G cannot be expressed as the union of a finite number of right (left) cosets of subgroups with infinite index.*

Proof. Suppose the contrary, and that $H_1, \cdots, H_n$ is a minimal set of subgroups of G, each with infinite index in G, such that G can be expressed as the union of a finite number of (right) cosets of $H_1, \cdots, H_n$. Let $H_1 g_1, \cdots, H_1 g_k$ be the cosets of H_1 which appear in some such expression for G, and let $H_1 g$ be a coset distinct from each $H_1 g_j$ $(j = 1, \cdots, k)$. Then

$$H_1 g \subseteq G - H_1 g_1 \cup \cdots \cup H_1 g_k,$$

and since the right hand side is contained in a finite union of cosets of $H_2, \cdots, H_n$, the same is true of $H_1 g$ and therefore, also, of each $H_1 g_j$ $(j = 1, \cdots, k)$. It follows that G can be expressed as a finite union of cosets of $H_2, \cdots, H_n$, contrary to the minimal nature of the set $H_1, \cdots, H_n$. This contradiction proves the lemma.

COROLLARY 3.2. *Let Π be a group of permutations of a set X, and let S be a finite subset of X such that, for each x in S, the orbit $\{\pi(x) : \pi \in \Pi\}$ is infinite. Then there exists π in Π such that the sets S and $\pi(S)$ are mutually disjoint.*

Proof. Given x and y in X, let $H_{x,y} = \{\pi : \pi \in \Pi \text{ and } \pi(y) = x\}$. Then $H_{x,x}$ is a subgroup of Π, and $H_{x,y}$ is either empty or a right coset of $H_{x,x}$. If $x \in S$ then $H_{x,x}$ has infinite index in Π, since $H_{x,y}$ runs through an infinity of distinct cosets of $H_{x,x}$ as y runs through the (infinite) orbit of x. By Lemma 3.1 there exists π in Π such that $\pi \notin H_{x,y} (x, y \in S)$; and the sets S and $\pi(S)$ are then mutually disjoint.

Before proving the second result which was assumed in Section 2 (Lemma 3.7), we require the following definition and two auxiliary lemmas.

Definition 3.3. Let Π be a group of permutations of an infinite set X, and let Y and Z be mutually disjoint infinite subsets of X. We say that Y "penetrates" Z, and write "$Y \leftrightarrow Z$" if, given any positive integer n, there exists π in Π such that $\pi(Y) \cap Z$ contains at least n members. If Y does not penetrate Z, we write "$Y \not\leftrightarrow Z$."

Remark 3.4. Let Y and Z be mutually disjoint infinite subsets of X, and let R be a finite subset of X. Since, for each π in Π,

$$\operatorname{card}\{\pi(Y) \cap Z\} = \operatorname{card}\{Y \cap \pi^{-1}(Z)\},$$

$$\operatorname{card}\{\pi(Y) \cap Z\} \geqq \operatorname{card}\{\pi(Y - R) \cap (Z \cup R)\} - \operatorname{card}\{R\}$$

(where "card" denotes the cardinal of the set in question), it is apparent that $Y \leftrightarrow Z$ if and only if $Z \leftrightarrow Y$, and that $Y \leftrightarrow Z$ if $Y - R \leftrightarrow Z \cup R$. Furthermore, if $Y_1, \cdots, Y_p$, $Z_1, \cdots, Z_q$ are pairwise disjoint infinite subsets of X, then

$$Y_1 \cup Y_2 \cup \cdots \cup Y_p \leftrightarrow Z_1 \cup Z_2 \cup \cdots \cup Z_q$$

if and only if there exist j and k such that $Y_j \leftrightarrow Z_k$; for

$$\operatorname{card}\{\pi(\bigcup_j Y_j) \cap \bigcup_k Z_k)\} = \sum_{j,k} \operatorname{card}\{\pi(Y_j) \cap Z_k\},$$

and the right hand side of this equation is unbounded, as π runs through Π, if and only if at least one of the summands $\operatorname{card}\{\pi(Y_j) \cap Z_k\}$ is unbounded.

LEMMA 3.5. *Let Π be a transitive group of permutations of an infinite set X. Let $Y_1, \cdots, Y_n$ and $Z_1, \cdots, Z_n$ be infinite subsets of X such that*

(i) $Y_1 \subseteq Y_2 \subseteq \cdots \subseteq Y_n$, $Z_1 \subseteq Z_2 \subseteq \cdots \subseteq Z_n$,

(ii) $Y_m \not\leftrightarrow X - Y_{m+1}$ *and* $Z_m \not\leftrightarrow X - Z_{m+1}$ $(m = 1, \cdots, n-1)$,

(iii) Y_n *and* Z_n *are mutually disjoint.*

Then there exists π in Π such that $\pi(Y_n) \cap Z_n$ contains at least n elements.

Proof. We shall prove by induction on m that, for $m = 1, \cdots, n$, the following statement $[m]$ holds: $[m]$ there exist a sequence $(Q_1, Q_2, \cdots)$ of pairwise disjoint subsets of Y_m, each containing just m elements, and a sequence $(\rho_1, \rho_2, \cdots)$ of members of Π, such that $(\rho_1(Q_1), \rho_2(Q_2), \cdots)$ is a sequence of pairwise disjoint subsets of Z_m. It is clear that the statement $[n]$ implies the conclusion of the lemma.

Since Y_1 and Z_1 are infinite sets, the assertion $[1]$ follows at once from the transitivity of Π. Suppose that $[m]$ has been established for some m satisfying $1 \leqq m < n$, and that Q_j and ρ_j $(j = 1, 2, \cdots)$ have been chosen in accordance with $[m]$. We shall prove $[m+1]$ in the following form: $[m+1]$ there exist a sequence $(R_1, R_2, \cdots)$ of pairwise disjoint subsets of Y_{m+1}, each containing just $m+1$ elements, and a sequence $(\sigma_1, \sigma_2, \cdots)$ of members of Π, such that $(\sigma_1(R_1), \sigma_2(R_2), \cdots)$ is a sequence of pairwise disjoint subsets of Z_{m+1}.

Suppose that k is a positive integer, and that suitable σ_j and R_j have been chosen for j (if any) such that $1 \leqq j < k$. We shall prove the existence of suitable σ_k and R_k.

We begin by noting that there exists x in Y_m such that, for an infinity of values of r, $\rho_r^{-1}(x) \in Y_{m+1} - R$, where R is the finite set $R_1 \cup R_2 \cup \cdots \cup R_{k-1}$. For suppose that no such x exists. Then, given any finite subset Q of $Y_m - R$, we have $\rho_r^{-1}(Q) \subseteq (X - Y_{m+1}) \cup R$ for all sufficiently large r. It follows that $Y_m - R \leftrightarrow (X - Y_{m+1}) \cup R$, and hence that $Y_m \leftrightarrow X - Y_{m+1}$, contrary to hypothesis. This proves the existence of x in Y_m with the stated property. If we replace (ρ_r), and correspondingly (Q_r), by suitable subsequences, we may suppose that $\rho_r^{-1}(x) \in Y_{m+1} - R$ $(r = 1, 2, \cdots)$. Since $\rho_r(Q_r) \subseteq Z_m \subseteq X - Y_m$, while $\rho_r(\rho_r^{-1}(x)) = x \in Y_m$, it follows that $\rho_r^{-1}(x) \notin Q_r$. By recalling the definition of R, we now obtain

$$\rho_r^{-1}(x) \in Y_{m+1} - R_1 \cup R_2 \cup \cdots \cup R_{k-1}, \qquad \rho_r^{-1}(x) \notin Q_r. \tag{4}$$

Since Π acts transitively on X, there exists π in Π such that

$$\pi(x) \in Z_{m+1} - \sigma_1(R_1) \cup \sigma_2(R_2) \cup \cdots \cup \sigma_{k-1}(R_{k-1}). \tag{5}$$

We assert that only a finite number of the sets $(\pi\rho_1)(Q_1), (\pi\rho_2)(Q_2), \cdots$ meet $(X - Z_{m+1}) \cup R'$, where

$$R' = \sigma_1(R_1) \cup \sigma_2(R_2) \cup \cdots \cup \sigma_{k-1}(R_{k-1}).$$

For suppose this assertion is false. Then since $\rho_1(Q_1), \rho_2(Q_2), \cdots$ are pairwise disjoint subsets of Z_m, and an infinity of their images $(\pi\rho_1)(Q_1), (\pi\rho_2)(Q_2), \cdots$ under π meet $(X - Z_{m+1}) \cup R'$, it follows that π maps an infinite subset of Z_m into $(X - Z_{m+1}) \cup R'$. Since R' is finite, π maps an infinite subset of Z_m into $X - Z_{m+1}$, and so $Z_m \leftrightarrow X - Z_{m+1}$, contrary to hypothesis. This proves the assertion made in the first sentence of this paragraph. Furthermore, since $Q_1, Q_2, \cdots$ are pairwise disjoint, only a finite number of them meet the finite set $R_1 \cup R_2 \cup \cdots \cup R_{k-1}$. It follows that, by avoiding a finite set of values, we may choose r such that

$$Q_r \subseteq Y_m - R_1 \cup R_2 \cup \cdots \cup R_{k-1}, \tag{6}$$

$$(\pi\rho_r)(Q_r) \subseteq Z_{m+1} - \sigma_1(R_1) \cup \sigma_2(R_2) \cup \cdots \cup \sigma_{k-1}(R_{k-1}). \tag{7}$$

If we now define

$$R_k = Q_r \cup \{\rho_r^{-1}(x)\}, \sigma_k = \pi\rho_r$$

then it follows at once from (4), $\cdots$, (7) that R_k consists of just $m+1$ elements of Y_{m+1} and does not meet any of the sets $R_1, \cdots, R_{k-1}$, while $\sigma_k(R_k)$ is a subset of Z_{m+1} which does not meet any of the set $\sigma_1(R_1), \cdots, \sigma_{k-1}(R_{k-1})$.

This inductive construction for R_k and σ_k proves the statement $[m+1]$, and so completes the proof of Lemma 3.5.

LEMMA 3.6. *Let Π be a transitive group of permutations of an infinite set X. Then*

(i) *if $X = Y \cup Z$, where Y and Z are mutually disjoint infinite subsets of X, then $Y \leftrightarrow Z$;*

(ii) *if, for each $n = 2, 3, \cdots, X$ is expressed in the form $X = \bigcup_{j=1}^{2^n} X_j^{(n)}$,* *where the sets* $X_j^{(n)}$ $(j = 1, \cdots, 2^n)$ *are infinite and pairwise disjoint, and*

$$(8) \qquad X_j^{(n)} = X_{2j-1}^{(n+1)} \cup X_{2j}^{(n+1)} \qquad (j = 1, \cdots, 2^n;\, n = 2, 3, \cdots),$$

then there exist integers n, j, k *such that* $n \geqq 2$, $1 \leqq j < j + 2 \leqq k \leqq 2^n$, *and* $X_j^{(n)} \leftrightarrow X_k^{(n)}$.

Proof. (i) Suppose that $Y \leftarrow\!\!\!\!\!\not\;\rightarrow Z$. Given any positive integer n, define $Y_m = Y$, $Z_m = Z$ $(m = 1, \cdots, n)$. The hypotheses of Lemma 3.5 are satisfied, so there exists π in Π such that $\pi(Y) \cap Z$ contains at least n elements. Hence, despite our assumption to the contrary, $Y \leftrightarrow Z$.

(ii) Suppose that there are no integers n, j, k with the stated properties. Given any n $(\geqq 2)$, we define Y_m and Z_m $(m = 1, \cdots, 2^{n-2})$ by

$$(9) \qquad Y_m = \bigcup_{r=1}^{m} X_r^{(n)}, \qquad Z_m = \bigcup_{r=1}^{m} X_{2^n+1-r}^{(n)}.$$

Since

$$X - Y_{m+1} = \bigcup_{r=m+2}^{2^n} X_r^{(n)}, \qquad X - Z_{m+1} = \bigcup_{r=m+2}^{2^n} X_{2^n+1-r}^{(n)},$$

our assumption that $X_j^{(n)} \leftarrow\!\!\!\!\!\not\;\rightarrow X_k^{(n)}$ when $k \geqq j + 2$ implies that

$$Y_m \leftarrow\!\!\!\!\!\not\;\rightarrow X - Y_{m+1} \text{ and } Z_m \leftarrow\!\!\!\!\!\not\;\rightarrow X - Z_{m+1}$$

(cf. Remark 3.4). Hence the conditions of Lemma 3.5 are satisfied (with n replaced by 2^{n-2}), so there exists π in Π such that

$$\pi(Y_{2^{n-2}}) \cap Z_{2^{n-2}}$$

contains at least 2^{n-2} elements. Since, by virtue of (8) and (9),

$$Y_{2^{n-2}} = X_1^{(2)}, \qquad Z_{2^{n-2}} = X_4^{(2)},$$

we have shown that, given any integer n $(\geqq 2)$, there exists π in Π such that $\pi(X_1^{(2)}) \cap X_4^{(2)}$ contains at least 2^{n-2} members. Thus $X_1^{(2)} \leftrightarrow X_4^{(2)}$ and, despite our assumption to the contrary, the conclusions of part (ii) of the lemma are satisfied when $n = 2$, $j = 1$, $k = 4$. This contradiction implies the existence of some n, j, k with the desired properties.

The following result will be subsumed in Theorem 3.8, but is needed during its proof.

LEMMA 3.7. *Let* Π *be a group of permutations of a set* X, *let* M *be a positive real number, and let* u *be a complex valued function which is defined on* X *and satisfies*

$$(10) \qquad \sum_{x \in X} | u(x) - u(\pi(x)) |^2 \leqq M^2 \quad (\pi \in \Pi).$$

Let Z be an infinite orbit. Then $\lim_\infty u$ *exists on Z.*

Proof. Let $u' = u \mid Z$, $\Pi' = \{\pi \mid Z : \pi \in \Pi\}$. Then Π' is a transitive group of permutations of Z, and u' satisfies the same hypotheses relative to Z and Π' as does u relative to X and Π. We have to show that $\lim_\infty u'$ exists on Z. Hence it is sufficient to consider the case in which Π acts transitively on X. Furthermore, we may assume without loss of generality that u is a real valued function.

Suppose therefore that Π is a transitive group of permutations on an infinite set X, and that u is a real valued function which is defined on X and satisfies (10). Given x and y in X, there exists π in Π such that $y = \pi(x)$, and it follows from (10) that $| u(x) - u(y) | \leqq M$. Hence u is bounded on X, and therefore has finite lower and upper limits. We define

$$(11) \qquad a = \underline{\lim}_\infty u, \qquad b = \overline{\lim}_\infty u.$$

We shall assume the non-existence of $\lim_\infty u$, so that $a < b$; in due course we shall obtain a contradiction.

We begin by proving the existence of real numbers c and d satisfying $a < c < d < b$ and such that, if

$$(12) \qquad Q = \{x : x \in X, u(x) < c\}, \qquad R = \{x : x \in X, u(x) \geqq d\},$$

then $Q \leftrightarrow R$. We deal separately with two cases.

Case 1. *The closure of the set* $\{u(x) : x \in X\}$ *does not contain the whole of the compact interval* $[a, b]$. In this case we may choose c and d so that $a < c < d < b$ and $u(x) \notin [c, d]$ $(x \in X)$. The sets Q and R defined by (12) are infinite (by (11)) and mutually disjoint, and $Q \cup R = X$. By Lemma 3.6 (i), $Q \leftrightarrow R$.

Case 2. *The closure of* $\{u(x) : x \in X\}$ *contains* $[a, b]$. Given any integer n $(\geqq 2)$, let $d_n = 2^{-n}(b - a)$, and define $X_j^{(n)}$ $(j = 1, \cdots, 2^n)$ by

$$X_j^{(n)} = \{x : x \in X, a + (j-1) d_n \leqq u(x) < a + j d_n\} \quad (j = 2, \cdots, 2^n - 1),$$
$$X_1^{(n)} = \{x : x \in X, u(x) < a + d_n\} \quad \text{and} \quad X_{2^n}^{(n)} = \{x : x \in X, u(x) \geqq b - d_n\}.$$

The hypotheses of Lemma 3.6 (ii) are satisfied, so there exist integers n, j, k such that $n \geqq 2$, $1 \leqq j < j + 2 \leqq k \leqq 2^n$, and $X_j^{(n)} \leftrightarrow X_k^{(n)}$. If we now take $c = a + j d_n$, $d = a + (k-1) d_n$, and define Q and R by (12), then $X_j^{(n)} \subseteq Q$ and $X_k^{(n)} \subseteq R$, so $Q \leftrightarrow R$.

In both cases, we have proved the existence of real numbers c and d

with the stated properties. Suppose now that n is any positive integer. Since $Q \leftrightarrow R$, we may find π in Π and a set S consisting of n members of Q, such that $\pi(S) \subseteq R$. From (10) and (12) it follows that

$$M^2 \geqq \sum_{x \in S} | u(x) - u(\pi(x)) |^2 \geqq n(d-c)^2.$$

If n is sufficiently large, we have a contradiction, so the lemma is proved.

THEOREM 3. 8. *Let Π be a group of permutations of a set X, let M be a positive real number, and let u be a complex valued function which is defined on X and satisfies*

$$\sum_{x \in X} | u(x) - u(\pi(x)) |^2 \leqq M^2 \quad (\pi \in \Pi). \tag{13}$$

Then u can be expressed (uniquely) in the form $u_1 + u_2$, where u_1 and u_2 are complex valued functions defined on X, u_2 is constant on each orbit and is bounded if u is bounded, while

$$\sum_{x \in X} | u_1(x) |^2 \leqq \tfrac{1}{2} M^2, \tag{14}$$

and u_1 satisfies the following condition: if Y is the union of a finite family of finite orbits, and $\Pi' = \{\pi \mid Y : \pi \in \Pi\}$, then

$$\sum_{\pi' \in \Pi'} u_1(\pi'(y)) = 0 \quad (y \in Y). \tag{15}$$

Proof. Let $x \in X$. If the orbit $\Pi(x)$ of x is finite, we define $u_2(x)$ to be the mean value of u on $\Pi(x)$. If $\Pi(x)$ is infinite, we define $u_2(x)$ to be $\lim_\infty u$ on $\Pi(x)$; the existence of the limit follows from Lemma 3. 7. The function u_2 defined in this way is constant on each orbit, and is bounded if u is bounded. Let $u_1 = u - u_2$. Then u_1 has mean value zero on each finite orbit, and has limit zero on each infinite orbit. Furthermore, since $u_2(x) = u_2(\pi(x))$ whenever $x \in X$ and $\pi \in \Pi$, it follows that u_1 satisfies (13).

Let Y be the union of a finite family of finite orbits, and let $\Pi' = \{\pi \mid Y : \pi \in \Pi\}$. If $y \in Y$ and $\rho, \sigma \in \Pi'$, then $\rho(y) = \sigma(y)$ if and only if ρ and σ belong to the same left coset of the subgroup $\{\pi' : \pi' \in \Pi', \pi'(y) = y\}$ of Π'; so, if n is the order of this subgroup, and $z \in \Pi(y)$, then there are just n elements π' in Π' such that $\pi'(y) = z$. Since u_1 has mean value zero on $\Pi(y)$,

$$\sum_{\pi' \in \Pi'} u_1(\pi'(y)) = n \sum_{z \in \Pi(y)} u_1(z) = 0.$$

Apart from the (straightforward) question of the uniqueness of u_1 and u_2, it remains only to prove (14). For this, it is sufficient to show that, if

Q is any finite subset of X and ϵ is any positive real number, then there exist complex numbers $a(x)$ and $b(x)$ $(x \in Q)$ such that

$$|a(x)| < \epsilon, \qquad |b(x)| < \epsilon \quad (x \in Q) \tag{16}$$

and

$$\sum_{x \in Q} |u_1(x) - a(x)|^2 + \sum_{x \in Q} |u_1(x) - b(x)|^2 \leqq M^2. \tag{17}$$

Suppose that we are given such Q and ϵ. We define

$$R = \{x : x \in Q \text{ and } \Pi(x) \text{ is finite}\}, \; Y = \bigcup_{x \in R} \Pi(x), \tag{18}$$

$$S = \{x : x \in Q \text{ and } \Pi(x) \text{ is infinite}\}, \; Z = \bigcup_{x \in S} \Pi(x). \tag{19}$$

Then Y is the union of a finite family of finite orbits. Let $\Pi' = \{\pi \mid Y : \pi \in \Pi\}$, let k be the order of Π', and choose $\rho_1, \cdots, \rho_k$ in Π such that $\Pi' = \{\rho_j \mid Y : j = 1, \cdots, k\}$.

Since u_1 has limit zero on each infinite orbit, while Z is the union of a finite family of infinite orbits, it follows that u_1 has limit zero on Z. Hence the sets S_1 and S_2, defined by

$$\begin{aligned} S_1 &= S \cup \{x : x \in Z \text{ and } |u_1(x)| \geqq \epsilon\}, \\ S_2 &= S_1 \cup \rho_1(S_1) \cup \cdots \cup \rho_k(S_1), \end{aligned} \tag{20}$$

are finite subsets of Z. By Corollary 3.2, there exists π in Π such that the sets S_2 and $\pi(S_2)$ are mutually disjoint. In particular, for each j $(= 1, \cdots, k)$, the sets S_1 and $(\pi\rho_j)(S_1)$ are mutually disjoint. Since $(\pi \mid Y) \in \Pi'$, $\Pi' = (\pi \mid Y)\Pi' = \{\pi\rho_j \mid Y : j = 1, \cdots, k\}$. Let $\pi_j = \pi\rho_j$ $(j = 1, \cdots k)$, so that

$$\Pi' = \{\pi_j \mid Y : j = 1, \cdots, k\}. \tag{21}$$

Furthermore, for each j, the sets S_1 and $\pi_j(S_1)$ are mutually disjoint, whence so are $\pi_j^{-1}(S_1)$ and S_1.

If $x \in S$ then, by (19), (20) and the stated properties of π_j, it follows that $\pi_j(x)$ and $\pi_j^{-1}(x)$ lie in $Z - S_1$; thus, again by (20),

$$|u_1(\pi_j(x))| < \epsilon, \quad |u_1(\pi_j^{-1}(x))| < \epsilon \qquad (x \in S; j = 1, \cdots, k). \tag{22}$$

By (21) and (15),

$$\begin{aligned} \sum_{j=1}^{k} \sum_{y \in Y} u_1(y)\overline{u_1(\pi_j(y))} &= \sum_{y \in Y} u_1(y) \sum_{\pi' \in \Pi'} \overline{u_1(\pi'(y))} \\ &= 0, \end{aligned}$$

so there is at least one value of j such that

$$Rl\{\sum_{y \in Y} u_1(y)\overline{u_1(\pi_j(y))}\} \leqq 0.$$

With this value of j,

$$\begin{aligned}
&\sum_{y \in Y} | u_1(y) - u_1(\pi_j(y)) |^2 \\
&\quad = \sum_{y \in Y} \{| u_1(y) |^2 + | u_1(\pi_j(y)) |^2 - 2Rl[u_1(y)\overline{u_1(\pi_j(y))}]\} \\
&\quad \geqq \sum_{y \in Y} \{| u_1(y) |^2 + | u_1(\pi_j(y)) |^2\},
\end{aligned}$$

and since $\pi_j(Y) = Y$,

$$\sum_{y \in Y} | u_1(y) - u_1(\pi_j(y)) |^2 \geqq 2 \sum_{y \in Y} | u_1(y) |^2. \tag{23}$$

Since $S \subseteq S_1$, the sets S and $\pi_j^{-1}(S)$ are mutually disjoint, and it is clear from (18) and (19) that neither of them meets Y. From (23), since $R \subseteq Y$, and since u_1 satisfies (13),

$$\begin{aligned}
&2 \sum_{y \in R} | u_1(y) |^2 + \sum_{x \in S} | u_1(x) - u_1(\pi_j(x)) |^2 \\
&\qquad + \sum_{x \in S} | u_1(x) - u_1(\pi_j^{-1}(x)) |^2 \\
&\leqq \sum_{x \in Y \cup S \cup \pi_j^{-1}(S)} | u_1(x) - u_1(\pi_j(x)) |^2 \\
&\leqq M^2.
\end{aligned} \tag{24}$$

Since $Q = R \cup S$, we may define $a(x)$ and $b(x)$ $(x \in Q)$ by

$$a(x) = u_1(\pi_j(x)), \quad b(x) = u_1(\pi_j^{-1}(x)) \qquad (x \in S),$$

and $a(y) = b(y) = 0$ $(y \in R)$. It follows from (22) and (24) that (16) and (17) are satisfied. This completes the proof of (14).

It is apparent that u_1 is determined to within an additive constant on each orbit Z. That u_1 is uniquely determined (on each orbit, and hence throughout X) now follows, from the condition $\sum_{x \in Z} | u_1(x) |^2 < \infty$ if Z is infinite, and from the fact (deduced from (15)) that u_1 has mean value zero on Z if Z is finite. This completes the proof of Theorem 3.8.

Remark 3.9. If, in Theorem 3.8, the inequalities (13) and (14) are replaced by

$$\sum_{x \in X} | u(x) - u(\pi(x)) |^2 < \infty \qquad (\pi \in \Pi),$$

and

$$\sum_{x \in X} | u_1(x) |^2 < \infty$$

respectively, then the statement so obtained is false. Simple counter-examples occur, for instance, when X is an arbitrary infinite set and Π consists of those permutations of X each of which moves only a finite number of elements.

UNIVERSITY OF PENNSYLVANIA.

REFERENCES.

[1] R. Kadison, "Derivations of operator algsbras," *Annals of Mathematics*, vol. 83 (1966), pp. 280-293.

[2] I. Kaplansky, "Modules over operator algebras," *American Journal of Mathematics*, vol. 75 (1953), pp. 839-859.

[3] P. Miles, "Derivations on B^*-algebras," *Pacific Journal of Mathematics*, vol. 15 (1965), pp. 1359-1366.

[4] F. Murray and J. von Neumann, "On rings of operators, IV," *Annals of Mathematics*, vol. 44 (1943), pp. 716-808.

[5] S. Sakai, "On a conjecture of Kaplansky," *Tôhoku Mathematical Journal*, vol. 12 (1960), pp. 31-33.