ON AUTOMORPHISMS OF COMPACT GROUPS

PAUL R. HALMOS

1. Introduction and definitions. Let G be a compact abelian group and α a continuous automorphism of G. We write G multiplicatively and use, accordingly, the exponent notation for automorphisms. Thus the image under α of the element $x \in G$ will be denoted by x^α; similarly we shall write for (complex valued) functions $f(x)$, $f^\alpha(x) = f(x^\alpha)$.[1]

If m is Haar measure[2] in G (normalized so that $m(G)=1$) we consider the set function $m'(E)=m(E^\alpha)$. (E^α is the set of all x^α, $x \in E$.) Since m' is a measure on G possessing all defining properties of m it follows from the uniqueness of Haar measure[3] that $m'(E)=m(E)$ for every measurable set E. In other words α is a measure preserving transformation of G; the purpose of this note is to investigate a few simple properties of α from the point of view of measure theory.

We shall make use of the Pontrjagin duality theory,[4] and, in particular, we shall need the fact that the group of automorphisms of G is essentially the same as that of the character group G^*. More precisely: if to any $\phi = \phi(x) \in G^*$ we make correspond $\phi^\alpha = \phi^\alpha(x) = \phi(x^\alpha)$, then $\phi^\alpha \in G^*$, and the correspondence $\phi \rightarrow \phi^\alpha$ is an automorphism of G^*. The duality theory also enables us to reverse this argument: every automorphism of G^* is induced in this way by a continuous automorphism of G.

We recall some standard definitions from ergodic theory. A measure preserving transformation α (not necessarily an automorphism) is *ergodic* if the only (complex valued, measurable) solutions f of the equation $f^\alpha = f$ are constant almost everywhere. The transformation α is *mixing* if the only (complex valued, measurable) solutions f of the equation $f^\alpha = \lambda f$, for any constant λ, are constant almost everywhere.[5] (It is true, though irrelevant, that for $\lambda \neq 1$ even a constant fails to be a solution unless it is zero.) It is well known that the mapping

Presented to the Society, December 27, 1942; received by the editors November 23, 1942.

[1] This notation dovetails, as usual, with ordinary exponentiation in G; thus $x^{3\alpha^2} = (x^3)^{\alpha^2} = (x^{\alpha^2})^3$, and so on.

[2] For a general discussion of measure theory in topological groups see A. Weil, *L'intégration dans les groupes topologiques et ses applications*, Paris, 1938.

[3] Weil, op. cit., pp. 36–38.

[4] Weil, op. cit., chap. 6.

[5] See E. Hopf, *Ergodentheorie*, Berlin, 1937, chap. 3, for a discussion of the fact that these definitions are equivalent to the ones more commonly given.

$f \to f^{\alpha}$ induced by a measure preserving transformation α on the space of functions over G is a unitary transformation of the Hilbert space $L_2(G)$.[6] Two measure preserving transformations α and β are of the *same spectral type* if there is a unitary transformation ω of $L_2(G)$ (ω need not be induced by a transformation of G) for which $f^{\omega\alpha\omega^{-1}} = f^{\beta}$ for all $f \in L_2(G)$. Given any point $x \in G$ (or function f on G) the set of all x^{α^n} (or f^{α^n}), $n = 0, \pm 1, \pm 2, \cdots$ is the *orbit* of x (or f). If α is an automorphism the orbit of the identity consists of the identity only; if this is the only finite orbit we shall say, for the sake of brevity, that α has no finite orbits.

In terms of the definitions of the preceding paragraph we can state our results quite concisely. In Theorem 1 we obtain a simple characterization of ergodicity and mixing in terms of the orbits of α in G^*. Theorem 2 is a statement concerning abstract groups and, prima facie, has nothing to do with measure theory; together with Theorem 1 and the duality theory it yields, however, a complete description of the spectral type of ergodic automorphisms. In the concluding section we state some unsolved problems and emphasize the importance of group automorphisms as a source of many new and simple examples of transformations with properties that were once considered difficult to obtain.[7]

2. **Ergodic and mixing automorphisms.** We prove the following theorem:

Theorem 1. *A continuous automorphism α of a compact abelian group G is ergodic (or mixing) if and only if the induced automorphism on the character group G^* has no finite orbits.*

We call attention to the somewhat surprising fact that for continuous automorphisms ergodicity is equivalent to the apparently stronger mixing condition. We shall see later that much more than this is true: if α is ergodic then it automatically has the strongest of the whole known hierarchy of mixing properties.

The similarity of our definitions of ergodicity and mixing to each other enables us to prove both parts of the theorem simultaneously. Suppose that $f \in L_2(G)$ and λ, $|\lambda| = 1$, are such that $f^{\alpha} = \lambda f$.[8] We may expand f in a Fourier series in the characters $\phi \in G^*$, $f(x) = \sum_{\phi} a(\phi)\phi(x)$.[9] Concerning this series we must make two comments. First, even if G^*

[6] Hopf, op. cit., p. 9.

[7] Hopf, op. cit., p. 42.

[8] The fact that, considered as a transformation of L_2, α is a unitary operator implies that if there is any proper value λ at all then it must be of modulus one.

[9] Weil, op. cit., p. 76.

is uncountable, at most a countable number of ϕ's fail to be orthogonal to f, so that at most a countable number of a's are different from zero. Second, the series need converge only in the sense of L_2 (mean square convergence); the known fact that a sub-sequence of its partial sums converges almost everywhere is sufficient to justify the simple formal steps that follow. Replacing x by x^α we obtain

$$\begin{aligned}\sum_\phi \lambda a(\phi)\phi(x) &= \lambda f(x) = f^\alpha(x) = f(x^\alpha)\\ &= \sum_\phi a(\phi)\phi(x^\alpha) = \sum_\phi a(\phi)\phi^\alpha(x) = \sum_\phi a(\phi^{\alpha^{-1}})\phi(x).\end{aligned}$$

Hence (using the orthogonality of the characters) we may equate coefficients and obtain $\lambda a(\phi) = a(\phi^{\alpha^{-1}})$, or $|a(\phi)| = |a(\phi^{\alpha^{-1}})|$. Since ϕ is arbitrary it follows that all coefficients $a(\phi)$ corresponding to ϕ's in the same orbit are equal in modulus. Since $\sum_\phi |a(\phi)|^2 < \infty$ it follows that all a's corresponding to ϕ's in the same infinite orbit vanish. This settles the *only if* part of our theorem: a non-constant f can exist only if α (considered as an automorphism of G^*) has finite orbits.

The converse is easier. Let $\phi \in G^*$ ($\phi \neq 1$) have a finite orbit; suppose, for definiteness, that n is the least positive integer for which $\phi^{\alpha^n} = \phi$. It follows that for the function $f = \phi + \phi^\alpha + \cdots + \phi^{\alpha^{n-1}}$ we have $f^\alpha = f$. The orthogonality and, a fortiori, linear independence of the ϕ's show that f is not constant. Since this shows that the existence of a finite orbit implies non-ergodicity, the proof of Theorem 1 is complete.

THEOREM 2. *Let α be any automorphism of the discrete abelian group H; if α has no finite orbits then it has an infinite number of orbits.*[10]

Case I. We assume first that there is in H an element ϕ_0 of finite order. By raising ϕ_0 to a suitable power we may assume that the order of ϕ_0 is a prime p. Write $\phi_n = \phi_0^{\alpha^n}$, $n = 0, \pm 1, \pm 2, \cdots$; we shall prove that the ϕ_n are independent mod p. (It is clear that the order of each ϕ_n is p.) Suppose, on the contrary, that $\phi_{i_1}^{r_1} \cdots \phi_{i_k}^{r_k} = 1$; it is merely a notational change to write $i_1 = 1, \cdots, i_k = k$, and we may, of course, assume that r_1 and r_k are not congruent to zero mod p. We have then

$$(1) \qquad \phi_1 = (\phi_2^{-r_2} \cdots \phi_k^{-r_k})^{r_1^{-1}}, \qquad \phi_k = (\phi_1^{-r_1} \cdots \phi_{k-1}^{-r_{k-}})^{r_k^{-1}}.$$

(The exponents r_1^{-1}, r_k^{-1} make sense since we may interpret them in the modular field $GF(p)$.) Consider now the finite subgroup H_0 of H

[10] The author's thanks are due to R. Baer, R. H. Fox, and H. Samelson for many valuable discussions of this theorem and its proof.

generated by $\phi_1, \cdots, \phi_k$. It follows from the definition of the ϕ_n and the relations (1) that H_0 is invariant under both α and α^{-1} and contains consequently the entire orbit of ϕ_0. Since this contradicts the assumed nonexistence of finite orbits, the ϕ_n must indeed be independent. The desired conclusion follows at once: the elements $\psi_n = \phi_1 \cdots \phi_n$, $n = 1, 2, \cdots$, must all lie in different orbits.

Case II. If ϕ_0 is an element of infinite order we write $\phi_i = \phi_0^{\alpha i}$ as before and we ask for which (positive or negative) integers i it is true that ϕ_i is a positive rational power of ϕ_0^r (that is, a positive integral power of some root of ϕ_0). If $\phi_i = \phi_0^r$ then $(\phi_{-i})^r = (\phi_0^r)^{\alpha^{-i}} = (\phi_i)^{\alpha^{-i}} = \phi_0$, so that ϕ_{-i} is an rth root of ϕ_0. If also $\phi_j = \phi_0^s$ then $\phi_{i+j} = (\phi_j)^{\alpha^i} = \phi_0^{s\alpha^i}$ $= \phi_0^{\alpha^i s} = \phi_0^{rs}$. In other words the set of i's under consideration is an additive group of integers; let i_0 be a generator of this group, $\phi_{i_0} = \phi_0^{r_0}$. Then for any integer n

$$\phi_{i_0 n} = (\cdots((\phi_0)^{r_0})^{r_0} \cdots)^{r_0} = \phi_0^{r_0^n};$$

in other words the set of possible r's that may occur as exponents in a relation $\phi_i = \phi_0^r$ consists of all (positive, negative, or zero) integral powers of r_0. Hence the set of powers of ϕ_0 which are in the same orbit as ϕ_0 consists only of powers of r_0, and consequently there is a power of ϕ_0 which does not lie in this orbit. We may choose this power of ϕ_0 as a new starting element (of infinite order) and repeat the above argument ad infinitum. This completes the proof of Theorem 2.

We are now prepared to describe the spectral type of ergodic automorphisms. Let $\mathfrak{S}$ be a complete orthonormal set in an abstract, not necessarily separable, Hilbert space and denote by ψ any particular element of $\mathfrak{S}$. Arrange all remaining elements of $\mathfrak{S}$ as an infinite matrix in such a way that each row contains a countably infinite number of elements. Use as row index any set of suitable power and as column index the set of all (positive, negative, or zero) integers. A unique unitary operator σ is defined on Hilbert space by the requirement that it send ψ into itself and $\phi_{i,j}$ into $\phi_{i,j+1}$ for $j = 0, \pm 1, \pm 2, \cdots$, and all i. The spectral type of σ depends only on the number of rows; if we agree to use $\aleph$ for this cardinal number we may write $\sigma = \sigma(\aleph)$. We summarize our result in terms of these σ's.

THEOREM 3. *If α is a continuous ergodic automorphism of a compact abelian group G and $\aleph$ is the (necessarily infinite) cardinal number of G^* then α has the spectral type of the unitary operator $\sigma(\aleph)$.*

For the proof we need remember only that the characters of G form a complete orthonormal set of elements of $L_2(G)$. The principal character plays the role of ψ and the orbits of the other characters may be written as the rows of the matrix mentioned above. Theorem 2 shows that there must be an infinite number of rows, and the well known fact that for any infinite cardinal $\aleph \cdot \aleph_0 = \aleph$[11] shows that the number of rows is the same as the total number of elements in G^*.[12]

3. **Examples and questions.** Let H be any compact abelian group and let G be the direct product of H with itself a countable number of times. We write G as the set of all sequences $\{x_n | n=0, \pm 1, \pm 2, \cdots\}$, and we define a continuous ergodic automorphism α of G by the relations

$$\{x_n\}^\alpha = \{x_n'\}, \quad x_n' = x_{n+1}, \qquad n = 0, \pm 1, \pm 2, \cdots .$$

Transformations isomorphic to such α's (not only in the spectral but even in the stronger, measure theoretic, sense) were among the first known examples of ergodic transformations.

Examples apparently very simple from the algebraic point of view, but very difficult to handle geometrically, are furnished by the solenoids. Consider for instance the multiplicative group of all real numbers of the form e^r, where r is a dyadic rational number. The operation of squaring is an automorphism of this group (with no finite orbits), and hence an ergodic automorphism of its compact character group.

More in the classical spirit than either of the last two examples are the (continuous) automorphisms of the n-dimensional toral group. In order to retain our multiplicative notation we write the torus as n-tuples $(x_1, \cdots, x_n)$ of complex numbers of modulus one; thus the product of $(x_1, \cdots, x_n)$ by $(y_1, \cdots, y_n)$ is $(x_1y_1, \cdots, x_ny_n)$ and the identity element is $(1, \cdots, 1)$. It is well known that the automorphism group of the torus is the unimodular group, in the following sense. Given any $n \times n$ matrix $\alpha = (a_{ij})$ whose elements are integers and whose determinant is ± 1, we consider the mapping $(x_i) \rightarrow (\prod_j x_j^{a_{ij}})$: this mapping is the most general continuous automorphism of the torus. The condition of ergodicity—that is, the condition that, considered as an automorphism of the character group, α have no finite orbits—is equivalent in classical terms to the requirement that no root of unity should be a proper value of α. This remark enables us to write down any desired number of quite different looking analytic ergodic (and hence mixing) measure preserving transformations on the finite dimensional torus.

[11] See F. Hausdorff, *Mengenlehre*, Berlin, 1935, p. 71.

[12] The first explicit discussion of the spectral form of a measure preserving transformation of type $\sigma(\aleph_0)$ was carried out by J. L. Doob and R. A. Leibler, *On the spectral analysis of a certain transformation*, Amer. J. Math. vol. 65 (1943) pp. 263–272.

This last example and the particular structure of the automorphisms it describes suggests a new, purely measure theoretic, invariant of measure preserving transformations. The Hamilton-Cayley equation says, in our notation, that if p is the characteristic polynomial of α then for every x in the torus $x^{p(\alpha)}=1$. It follows that for every character f of the torus we have, similarly, $f^{p(\alpha)}=1$. The existence or nonexistence of f's thus *annihilated* by certain polynomials in α (with, of course, integer coefficients) and, if they exist, their algebraic and measure theoretic structure, furnishes the invariant to which we referred. To illustrate the possible application of these invariants we mention the following: if it could be proved that the characters are (except for trivial changes on a set of measure zero) the only measurable functions of constant modulus one which are *annihilated* by $p(\alpha)$, it would follow rather easily that two ergodic automorphisms of the torus are measure theoretically isomorphic if and only if they correspond to conjugate elements in the unimodular group. We could thus obtain the first examples of measure theoretically distinct transformations of the spectral type of $\sigma(\aleph_0)$,[13] and the usual proper value theory would then point the way to further, more delicate, invariants.

In conclusion we mention an unsolved problem of purely technical interest, but one whose solution may throw some light on the deeper problems raised above. The question is simply: do there exist measure preserving transformations (on spaces of finite measure) of the spectral type of $\sigma(\aleph)$, where $\aleph$ is a *finite* cardinal?

Syracuse University

[13] The first examples of measure theoretically different but spectrally isomorphic transformations are due to J. von Neumann. These examples (not yet published) are, however, not mixing transformations.