Taking account to the boundedness of $f(P)$ we obtain immediately Birkhoff's general

TIME AVERAGE THEOREM. For any bounded and measurable function $f(P)$ the limit

$$\lim_{T=\infty} \frac{1}{T} \int_0^T f(P_t)dt$$

exists on Ω apart from a set of points P of measure zero.

* INTERNATIONAL RESEARCH FELLOW.

[1] Cf. B. O. Koopman, These PROCEEDINGS, **17**, 315–318 (1931).

[2] Cf. J. v. Neumann, These PROCEEDINGS, **18**, 70–82(1932).

[3] Cf. G. D. Birkhoff, These PROCEEDINGS, **17**, 656–660(1931).

[4] Cf. H. Weyl, *Math. Annalen*, **77**, 313–352 (1916).

SETS OF DISTINCT GROUP OPERATORS INVOLVING ALL THE PRODUCTS BUT NOT ALL THE SQUARES

BY G. A. MILLER

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS

Communicated November 16, 1931

Suppose that $s_1, s_2, \ldots, s_k$ represent a set of distinct operators which obey the group laws when they are combined and include the product of every pair thereof, irrespective of the order of the factors, but not necessarily the square of any operator of the set. It is well known that a necessary and sufficient condition that such a set constitutes a group is that it contains also the square of each of its elements. In all cases the set generates a group G of order $g \geqq k$. In what follows it will be assumed that g is finite, and we shall determine all the possible groups of finite order which have the property that it is possible to find in each of them a set of distinct operators which generate the group and include the product of every pair of the set, irrespective of the order of the factors, but not the square of all of them. In other words, for each of these sets $k < g$.

When $k = 2$ the set is obviously composed of an arbitrary operator and the identity, and a necessary and sufficient condition is that G is cyclic and this operator is an arbitrary generator of this cyclic group. In this case $k = g$ when $g = 2$ and only then. When $k = 3$ the three operators s_1, s_2, s_3 must be commutative and if one of them is the identity, the other two are inverses of each other but are not otherwise restricted. Hence in this case G must again be cyclic, but its order is unrestricted except that it must exceed 2. A necessary and sufficient

condition the $g = k$ in this case is that G is the group of order 3. When none of the three operators s_1, s_2, s_3 is the identity, then each of them must be of order 2 and G is the non-cyclic group of order 4, or the trirectangular group. This is a special case of the following elementary theorem: *If a set of k distinct operators of order 2 has the property that it includes the product of every pair of them, then these operators generate the abelian group of order* $k + 1 = 2^m$ *and of type* (1,1,1,. . .), *and every such group involves such a set.* Since these cases are very elementary, it may be assumed in what follows that $k > 3$, and that the set s_1, s_2,. . . ,s_k involves operators whose order exceeds 2.

Suppose that this set involves an operator s and also $s^n \neq s^{-1}$. If $n = 2$ the set involves all the powers of s including the identity. If $n \neq 2$ but less than the order of s diminished by unity the set must involve also s^{n+1}, s^{n+2}, . . .,s^{-1}. Hence it involves also s^{n-1}, s^{n-2}, . . .,s^2. That is, when the set s_1, s_2, . . .,s_k involves an operator s and also a lower positive power of s than the inverse of s than this set involves also all the powers of s including the identity. In particular, when G is a cyclic group and $k > 3$, then $k = g$. It should be noted that whenever the set s_1, s_2, . . .,s_k involves an operator, s which is not a power of s_1, then it includes also $s_1^n s$ and $s s_1^n$, where n is arbitrary. If it involves s but not s^2, each of the operators of the set except possibly the identity must therefore have the property that it generates s^2. Hence there results the following theorem: *If a set of distinct operators has the property that it includes the product of every pair of them irrespective of the order of the two factors but does not involve the square of some one of them, then this square must be generated by each of its elements except possibly the identity.*

From this theorem it follows directly that if such a set does not involve the square of some one of its operators, it also cannot involve the square of any other one except possibly the identity, for if the square of such a second operator would then appear in the set, all the powers of this second operator would also appear therein. This is, however, impossible since such powers would involve the square of the first operator. It also results from the theorem noted at the close of the preceding paragraph, that if the square of an element of such a set does not appear therein, then this square must appear in the central of G and hence the square of every element of this set must appear in this central. In particular, when $g > k$ and G is non-abelian than its central quotient group is the abelian group of order 2^m and of type (1,1,1, . . .)

It is now easy to prove that when $g > k$ then G cannot be a non-cyclic abelian group unless it is the abelian group of order 2^m and of type (1,1,1, . . .). If G were any other non-cyclic abelian group, the set of operators s_1, s_2,. . ., s_k would involve at least one operator s such that s^2 is not generated by every other operator of the set and hence it would involve all the powers of s.

In particular, we could take for such an s one of the independent generators of G of largest order. If an operator of the set which can be used as a second independent generator of G after s has been chosen as a first independent generator does not have its square in the set, then this square can be generated by s. As this second operator can clearly be so selected that either its square is in the set or that this square is not generated by s, the following theorem has been proved: *If a set of distinct commutative operators contains the product of every pair of them and generates a non-cyclic group, then this set involves all the operators of this group unless each of these operators is of order* 2.

It remains to consider the case when G is non-abelian and $g > k$. It may first be noted that none of the operators of the set $s_1, s_2, \ldots, s_k$ except possibly the identity can be of odd order since it would then be generated by its square and hence also by every operator of this set besides possibly the identity. As it would also generate the square of each of these operators and be commutative with each of them, it results that an operator of order 2 would appear in this set. As this is impossible, it results that besides possibly the identity, each of the operators $s_1, s_2, \ldots, s_k$ is of even order. This order must be the same for all of them and cannot exceed 4. From this there results the following theorem: *If a set of distinct operators has the property that it involves the product of every pair of them irrespective of the order of the two factors, and generates a non-abelian group but does not involve all the operators of this group, then it must be composed of the identity and the six operators of order* 4 *of the quaternion group.*

Any set of k distinct group operators is said to constitute a group whenever it involves the product of every pair of these operators, irrespective of the order of these two factors, and the square of every one of them. From what precedes it results that with the exception of a relatively small number of very elementary groups the latter of these two conditions is implied by the former. This is always the case when some of the operators of the set are non-commutative except when they generate the quaternion group but do not include the operator of order 2 contained in this group. In this case $k = 7$ and $g = 8$. When all the operators of the set are of order 2, they must be commutative, since the product of two operators of order 2 cannot be of order 2 unless these two operators are commutative. This is the only case when $g > k$ and the set of operators $s_1, s_2, \ldots, s_k$ does not include the identity. In all the possible cases when $k < g$ the value of k must be either 2 or of the form $2^m - 1$. When $k = 2$ or 3 the number of distinct groups is infinite; when $m = 3$ there are two possible groups, but for every larger value of m there is one and only one such group.