FAMILIES OF GROUPS GENERATED BY TWO OPERATORS OF THE SAME ORDER*

BY

ABRAHAM SINKOV

I. Introduction

The present paper is an extension of a paper by W. E. Edington† entitled *On an infinite system of non-abelian groups of order* nm^{n-1}, in which it was shown that given any two numbers n and m, there exists a group of order nm^{n-1} generated by two operators of order n. Edington's proof requires the assumptions that all the operators of the form $S_1^\alpha S_2^\alpha$ are commutative and of the same order; it follows from the present treatment that the second is a consequence of the first and may be dispensed with. The results herein obtained exhibit a more general system of groups of order nm^{n-k}, where k is an arbitrary factor of n, and obtain some properties of these groups not considered by Edington.

II. A property of groups G generated by two operators of the same order

To begin with, the generating operations S_1 and S_2 are assumed to be of the same order n, so that $S_1^n = S_2^n = 1$. As yet no further restrictions are supposed. A third relation which defines the order of a particular combination of S_1 and S_2 will be introduced later on, in order to show how it actually arises.

Under these conditions, then, consider the totality of operators

$$S_1^\alpha S_2^{n-\alpha} \qquad (\alpha = 1, 2, \cdots, n-1).$$

This set of operators

$$A: \begin{cases} S_1 S_2^{n-1} \\ S_1^2 S_2^{n-2} \\ \cdots \\ \cdots \\ S_1^{n-1} S_2 \end{cases}$$

* Presented to the Society, March 25, 1932; received by the editors September 12, 1932. This paper was written under the guidance of Professor F. E. Johnston.

† Annals of Mathematics, vol. 25 (1923), p. 85.

generates a sub-group H of G. The transform of the generator $S_1^\alpha S_2^{n-\alpha}$ by S_1 can be written

$$(S_1^{\alpha-1}S_2^{n-\alpha+1})(S_1^{n-1}S_2)^{-1}$$

and is in H. When transformed by S_2 this same generator becomes

$$(S_1^{n-1}S_2)^{-1}(S_1^{\alpha-1}S_2^{n-\alpha+1}),$$

a result which is again in H. Consequently, H is invariant in G.

Evidently, the adjunction of either S_1 or S_2 to H generates G. It follows that the index of H under G cannot exceed n; it will equal n if and only if H involves no power of either S_1 or S_2. Such will be assumed to be the case. The order of G is then equal to n times the order of H.

It is now possible to replace the operators $S_1^\alpha S_2^{n-\alpha}$, which generate H, by an equivalent set in the sense that this new set generates the same group, and possesses the added advantage that all of the new generators are of the same order. In fact, they are the complete set of conjugates of $S_1S_2^{n-1}$ under S_2:

$$S_2^q(S_1S_2^{n-1})S_2^{-q} = (S_1^qS_2^{n-q})^{-1}(S_1^{q+1}S_2^{n-q-1}) \qquad (q = 0, 1, 2, \cdots, n-1).$$

This new set will be denoted by ξ:

$$\xi: \begin{cases} S_1S_2^{n-1} \\ (S_1S_2^{n-1})^{-1}(S_1^2S_2^{n-2}) \\ (S_1^2S_2^{n-2})^{-1}(S_1^3S_2^{n-3}) \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ (S_1^{n-1}S_2)^{-1}. \end{cases}$$

Observe that this set is obtainable from the preceding one by multiplying each operator of A in turn by the inverse of the one which precedes it, provided that the identity is supposed to precede A_1 and to follow A_{n-1}. Conversely A is obtainable from ξ because of the relation

$$\prod_{i=1}^{a}\xi_i = S_1^\alpha S_2^{n-\alpha}$$

where ξ_i denotes the ith term in the set ξ. In particular

$$\prod_{i=1}^{n}\xi_i = 1.$$

The preceding results may now be summarized as follows:

THEOREM I. *The group G generated by two operators of the same order n contains an invariant sub-group H generated by n operators of the same order. The index of H under G is at most n.*

It is not amiss to remark at this point that the common order m of these new generators of H is quite arbitrary and may be assumed to be any integer whatever.

III. DEFINING RELATIONS OF A 3-PARAMETER FAMILY

It will now be assumed that the sub-group H is abelian and that it is possible to select q of the operators ξ which shall form a set of independent generators in the restricted sense. Its order will then be m^q.*

Suppose for a moment that n is composite and contains the factor k. Then $n=kx$, and the set of operators ξ can be divided up in order into x sub-sets of k each. Suppose further that it is possible for the k operators of one of these sub-sets to be dependent upon the remaining generators, which form an independent set in the restricted sense. Then, under such circumstances the most general sub-group H which can be obtained, i.e., the one of greatest order, will be of order $m^{(x-1)k}$. By analogy with the condition previously obtained on the ξ_i, the equation of connection will be chosen in the form

$$\prod_{i=0}^{x-1}\xi_{ik+\alpha} = 1 \qquad (\alpha = 1, 2, \cdots, k;\ n = kx).$$

Expressed in words this means that the product of the operations which are in corresponding positions in each sub-set is the identity.

Since

$$\xi_{\alpha+1} = S_2^{\alpha}S_1S_2^{kx-\alpha-1},$$

$$\prod_{i=0}^{x-1}\xi_{ik+\alpha} = 1 = (S_2^{\alpha-1}S_1S_2^{kx-\alpha})(S_2^{k+\alpha-1}S_1S_2^{kx-k-\alpha}) \cdots (S_2^{(x-1)k+\alpha-1}S_1S_2^{k-\alpha})$$
$$= S_2^{\alpha-1}(S_1S_2^{k-1})^xS_2^{-\alpha+1},$$

whence

$$(S_1S_2^{k-1})^x = 1.$$

In the particular case $k=1$, this condition reduces to an identity.

Conversely, if $(S_1S_2^{k-1})^x=1$, it follows from a reversal of the preceding manipulation that

$$\prod_{i=0}^{x-1}\xi_{ik+\alpha} = 1 \qquad (\alpha = 1, 2, \cdots, k),$$

---

* Miller, Blichfeldt and Dickson, *Theory and Applications of Finite Groups*, p. 90.

and hence that k of the operators ξ are expressible in terms of the remaining ones.

It is now necessary to examine this condition a bit more closely. Suppose it holds for some particular factor k of n. Then it can be shown that it is also satisfied by every factor of n which is a divisor of k. For, suppose $k=rt$. Then of the rt continued products

$$\prod_{i=0}^{x-1}\xi_{irt+\alpha} = 1 \qquad (\alpha = 1, 2, \cdots, rt),$$

select the following r:

$$\prod_{i=0}^{x-1}\xi_{irt+\alpha} = 1,$$

$$\cdots\cdots\cdots$$

$$\prod_{i=0}^{x-1}\xi_{irt+\alpha+(r-1)t} = 1 \qquad (\alpha = 1, 2, \cdots, t).$$

Multiplying together all of the left hand members and rearranging the terms (which is permissible because of the commutativity of the ξ_i),

$$\prod_{i=0}^{rx-1}\xi_{it+\alpha} = 1 \qquad (\alpha = 1, 2, \cdots, t).$$

The condition therefore holds for t.

This leads to the conclusion that if for a given S_1 and S_2 two or more values k satisfy the relation $(S_1S_2^{k-1})^x=1$, and if it is possible to choose one among them such that all the others are divisors of it, then that one is the value to be used in determining the number of independent generators of H.

Moreover, the assumption that the correct k requires the remaining $(x-1)k$ operators to be independent prevents two numbers, where neither is a multiple of the other, from simultaneously satisfying the required condition. For, in that case, there arises the obvious contradiction that the order of H is given by two different powers of m.

If the relation holds for no $k>1$, then $k=1$ and $q=n-1$.

The number k having been determined in this way, it follows that the order of H is m^{n-k}. Since it has already been shown that the index of H under G in the most general case is n, then the corresponding order of G is nm^{n-k}.

There thus results the following theorem:

THEOREM II. *Two operators S_1 and S_2 of the same order n for which the set ξ is commutative generate a group G whose order is at most nm^{n-k} where m is the common order of the operators ξ and the number k is defined as the greatest factor of n satisfying the relation*

$$(S_1S_2^{k-1})^x = 1 \qquad (kx = n).$$

IV. Generating operations of G

The maximum group thus defined exists for every number nm^{n-k} and a pair of generating operations S_1 and S_2, of a fairly simple form, can be set up for the general case. Let

$$S_1 = (a_1a_2 \cdots a_n)(a_{n+1}a_{n+2} \cdots a_{2n}) \cdots (a_{(m-1)n+1}a_{(m-1)n+2} \cdots a_{mn}),$$
$$S_2 = (a_{p+1}a_{p+2} \cdots a_{p+n})(a_{n+p+1}a_{n+p+2} \cdots a_{2n+p}) \cdots (a_{(m-1)n+p+1} \cdots a_{mn}a_1a_2 \cdots a_p).$$

Then it can be shown that the operators $S_1^{\alpha}S_2^{n-\alpha}$ are all of order m and are commutative. Moreover, if k is the greatest common divisor of p and n, it is found that $n-k$ of the operators ξ form an independent set in the restricted sense. Hence there results the following theorem:

Theorem III. *The two substitutions given above generate a group G of order nm^{n-k} where k is the greatest common divisor of p and n.*

V. Properties of the groups G

The quotient group of H under G is cyclic and as a consequence every G is solvable.

In order to determine the central it is first necessary to determine the subgroup of it which is contained in H, i.e., the combinations of the ξ_i which are invariant in G.

To obtain this result requires a knowledge of how the ξ_i are transformed under S_1 and S_2. First, consider the transform of ξ_{i+1} by S_1. Since

$$\xi_{i+1} = S_2^iS_1S_2^{n-i-1},$$
$$S_1^{-1}\xi_{i+1}S_1 = (S_1^{n-1}S_2)(S_1^{i-1}S_2^{n-i+1})^{-1}(S_1^iS_2^{n-i})(S_1^{n-1}S_2)^{-1}.$$

In this last result, the two factors $(S_1^{n-1}S_2)^{-1}$ and $(S_1^{n-1}S_2)$ will be eliminated as a result of the commutativity of the $S_1^{\alpha}S_2^{n-\alpha}$. Hence

$$S_1^{-1}\xi_{i+1}S_1 = (S_1^{i-1}S_2^{n-i+1})^{-1}(S_1^iS_2^{n-i}) = \xi_i.$$

Similarly

$$S_2^{-1}\xi_{i+1}S_2 = \xi_i$$

and the ξ_i are thus seen to be transformed in the same way by S_1 and S_2. This property is also obtainable from the fact that S_1 and S_2 are contained in the same co-set of H. As a consequence of it, the operators of H which are invariant under S_1 are identical with those which are invariant in G.

It has already been seen that for a given k the operators ξ can be divided up into k different sets

$$\xi_{ik+\alpha} \qquad (\alpha = 1, 2, \cdots, k)$$

each containing x operators, and such that $x-1$ of the operators in each set are independent. Moreover, no operators in any one of these sets can be expressed in terms of any of the other sets. Hence, since ξ_i and ξ_{i-1} are in different sets if $k>1$, it follows that a combination of operators in any single set can be invariant in G, only if $k=1$.

Suppose then that such is the case and that

$$\xi_1^{a_1}\xi_2^{a_2}\cdots\xi_{n-1}^{a_{n-1}} \qquad (a_i < m)$$

is invariant in G. (ξ_n may be omitted from this combination since it is expressible in terms of the remaining $(n-1)$ ξ's.) This operator is equal to its transform under S_1 and consequently the following relation must hold:

$$\begin{aligned}\xi_1^{a_1}\xi_2^{a_2}\cdots\xi_{n-1}^{a_{n-1}} &= S_1^{-1}(\xi_1^{a_1}\xi_2^{a_2}\cdots\xi_{n-1}^{a_{n-1}})S_1\\ &= \xi_n^{a_1}\xi_1^{a_2}\cdots\xi_{n-2}^{a_{n-1}}.\end{aligned}$$

This leads to

$$\begin{aligned}\xi_{n-1}^{a_{n-1}} &= \xi_n^{a_1}\xi_1^{a_2-a_1}\xi_2^{a_3-a_2}\cdots\xi_{n-2}^{a_{n-1}-a_{n-2}}\\ &= (\xi_n^{a_1}\xi_1^{a_1}\cdots\xi_{n-2}^{a_1})(\xi_1^{a_2-2a_1}\xi_2^{a_3-a_2-a_1}\cdots\xi_{n-2}^{a_{n-1}-a_{n-2}-a_1}).\end{aligned}$$

As a consequence of the relation

$$\prod_{i=1}^{n}\xi_i = 1$$

the first quantity in parentheses is reducible at once to $(\xi_{n-1})^{-a_1}$. Hence

$$\xi_{n-1}^{a_1+a_{n-1}} = \xi_1^{a_2-2a_1}\xi_2^{a_3-a_2-a_1}\cdots\xi_{n-2}^{a_{n-1}-a_{n-2}-a_1}.$$

This equality involves only $n-1$ of the ξ's, all of which are independent of one another. Therefore both members must reduce to the identity, and as a result we have the following series of congruences:

$$\left.\begin{aligned}a_1 &\equiv -a_{n-1}\\ a_2 &\equiv 2a_1\\ a_3 &\equiv a_2 + a_1\\ &\cdots\cdots\\ a_{n-1} &\equiv a_{n-2} + a_1\end{aligned}\right\} \qquad (\text{mod } m).$$

These yield

$$a_p \equiv pa_1 \pmod{m}$$

and

$$(C) \qquad na_1 \equiv 0 \pmod{m}.$$

The invariant operator is now representable in the form

$$(\xi_1\xi_2^2 \cdots \xi_{n-1}^{n-1})^{a_1},$$

a_1 being a root of the congruence C. Every combination of the generators ξ_1 to ξ_{n-1} which is invariant in G must take this form. Conversely every such operator is invariant in G and the above representation is necessary and sufficient.

If we were to consider a combination involving all the ξ's but ξ_a, the reasoning would be identical with the above and it would be found that an invariant operator is necessarily of the form

$$(\xi_{a+1}\xi_{a+2}^2 \cdots \xi_n^{n-a}\xi_1^{n-a+1} \cdots \xi_{a-2}^{n-2}\xi_{a-1}^{n-1})^{a_1},$$

where again a_1 satisfies the congruence

$$na_1 \equiv 0 \pmod{m}.$$

The above operator may be written

$$(\xi_{a+1}\xi_{a+2} \cdots \xi_{a-1})^{a_1}(\xi_{a+2}\xi_{a+3}^2 \cdots \xi_n^{n-a-1}\xi_1^{n-a} \cdots \xi_{a-1}^{n-2})^{a_1},$$

and by virtue of the relation

$$\prod_{i=1}^{n}\xi_i = 1$$

becomes

$$(\xi_{a+2}\xi_{a+3}^2 \cdots \xi_n^{n-a-1}\xi_1^{n-a} \cdots \xi_{a-1}^{n-2})^{a_1}\xi_a^{-a_1}.$$

But

$$-a_1 \equiv (n-1)a_1 \pmod{m},$$

so that

$$\begin{aligned}
&(\xi_{a+1}\xi_{a+2}^2 \cdots \xi_n^{n-a}\xi_1^{n-a+1} \cdots \xi_{a-2}^{n-2}\xi_{a-1}^{n-1})^{a_1} \\
&= (\xi_{a+2}\xi_{a+3}^2 \cdots \xi_n^{n-a-1}\xi_1^{n-a} \cdots \xi_{a-1}^{n-2}\xi_a^{n-1})^{a_1} \\
&= (\xi_1\xi_2^2 \cdots \xi_{n-1}^{n-1})^{a_1}.
\end{aligned}$$

This shows that all the operators

$$(\xi_{a+1}\xi_{a+2}^{2}\cdots\xi_{n}^{n-a}\xi_{1}^{n-a+1}\cdots\xi_{a-1}^{n-1})^{a_1}\quad(a=0,1,\cdots,n-1)$$

are identical, and that one may with perfect generality consider

$$(\xi_1\xi_2^{2}\cdots\xi_{n-1}^{n-1})^{a_1}$$

as being the only permissible combination. As a result, the invariant operators of G contained in H form a cyclic sub-group whose order is determined as soon as the possible values of $a_1<m$ are known.

To find these values it is necessary to return to the congruence

$$na_1\equiv 0\pmod{m}.$$

If m is prime to n, $a_1=0$ is the only solution which is less than m. In such a case the identity is the only invariant operator. If m and n have the greatest common divisor d, the congruence reduces to

$$\frac{n}{d}a_1\equiv 0\quad\left(\operatorname{mod}\frac{m}{d}\right).$$

Here a_1 may take on all the values mq/d $(q=1,2,\cdots,d)$ and the sub-group is of order d. Both of these cases are combined in the general result that the number of invariant operators in H is d, where d is the greatest common divisor of m and n; they are all expressible in the form

$$(\xi_1\xi_2^{2}\cdots\xi_{n-1}^{n-1})^{mq/d}\quad(q=1,2,\cdots,d).$$

The generalization to any value of k follows along the same lines. Suppose some combination of ξ_1 to ξ_{n-k} to be invariant. For convenience, it is set down in the form

$$(\xi_1^{a_1}\xi_{k+1}^{a_2}\cdots\xi_{n-2k+1}^{a_{x-1}})(\xi_2^{b_1}\xi_{k+2}^{b_2}\cdots\xi_{n-2k+2}^{b_{x-1}})\cdots(\xi_k^{k_1}\xi_{2k}^{k_2}\cdots\xi_{n-k}^{k_{x-1}}),$$

where the operators of each set are kept together. If it is equal to its transform,

$$(\xi_1^{a_1}\xi_{k+1}^{a_2}\cdots\xi_{n-2k+1}^{a_{x-1}})(\xi_2^{b_1}\xi_{k+2}^{b_2}\cdots\xi_{n-2k+2}^{b_{x-1}})\cdots(\xi_k^{k_1}\xi_{2k}^{k_2}\cdots\xi_{n-k}^{k_{x-1}})$$
$$=(\xi_n^{a_1}\xi_k^{a_2}\cdots\xi_{n-2k}^{a_{x-1}})(\xi_1^{b_1}\xi_{k+1}^{b_2}\cdots\xi_{n-2k+1}^{b_{x-1}})\cdots(\xi_{k-1}^{k_1}\xi_{2k-1}^{k_2}\cdots\xi_{n-k-1}^{k_{x-1}}),$$

from which

$$\xi_{n-k}^{k_{x-1}}=(\xi_n^{a_1}\xi_k^{a_2-k_1}\cdots\xi_{n-2k}^{a_{x-1}-k_{x-2}})(\xi_1^{b_1-a_1}\xi_{k+1}^{b_2-a_2}\cdots\xi_{n-2k+1}^{b_{x-1}-a_{x-1}})$$
$$\cdots(\xi_{k-1}^{k_1-j_1}\xi_{2k-1}^{k_2-j_2}\cdots\xi_{n-k-1}^{k_{x-1}-j_{x-1}}).$$

Treating the first parenthesis as before and simplifying,

$$\xi_{n-k}^{a_1+k_{x-1}} = (\xi_k^{a_2-k_1-a_1}\xi_{2k}^{a_3-k_2-a_1}\cdots\xi_{n-2k}^{a_{x-1}-k_{x-2}-a_1})(\xi_1^{b_1-a_1}\xi_{k+1}^{b_2-a_2}$$
$$\cdots\xi_{n-2k+1}^{b_{x-1}-a_{x-1}})\cdots(\xi_{k-1}^{k_1-j_1}\xi_{2k-1}^{k_2-j_2}\cdots\xi_{n-k-1}^{k_{x-1}-j_{x-1}}).$$

The above relation involves only $n-k$ of the ξ's and $x-1$ of each set. Hence these $n-k$ are all independent and both members reduce to the identity. As a result a series of congruences is obtained:

$$\begin{aligned} a_1 &\equiv b_1 \equiv c_1 \equiv \cdots \equiv k_1, \\ a_2 &\equiv b_2 \equiv c_2 \equiv \cdots \equiv k_2, \\ &\cdots\cdots\cdots \\ a_{x-1} &\equiv b_{x-1} \equiv c_{x-1} \equiv \cdots \equiv k_{x-1}, \\ k_{x-1} &\equiv -a_1, \\ a_2 &\equiv k_1 + a_1, \\ a_3 &\equiv k_2 + a_1, \\ &\cdots\cdots \\ a_{x-1} &\equiv k_{x-2} + a_1 \qquad \pmod{m}. \end{aligned}$$

These lead to the relations

$$\begin{aligned} a_2 &\equiv 2a_1, \\ a_3 &\equiv 3a_1, \\ &\cdots\cdots \\ a_{x-1} &\equiv (x-1)a_1 \equiv -a \qquad \pmod{m}, \end{aligned}$$

so that finally

$$xa_1 \equiv 0 \qquad \pmod{m}.$$

From this point on, the reasoning is exactly like the preceding except that the quantity n is now replaced by $x=n/k$. Hence the sub-group of the central which is contained in H is cyclic and of order D where D is the greatest common divisor of m and n/k. The final form of the invariant operators is

$$[(\xi_1\xi_{k+1}^2\cdots\xi_{n-2k+1}^{x-1})(\xi_2\xi_{k+2}^2\cdots\xi_{n-2k+2}^{x-1})$$
$$\cdots(\xi_k\xi_{2k}^2\cdots\xi_{n-k}^{x-1})]^{mq/D} \qquad (q=1, 2, \cdots, D)$$

and these operators will henceforth be denoted by h_i.

The question now arises "Are there any invariant operators in G which are not contained in H?" It will first be shown that if such operators exist they must be of the form $S_1^v h_j$ where S_1^v is invariant in G. For, every operator outside of H is of the form

$$S_1^v \mathcal{H},$$

where $\mathcal{H}$ is an operator in H. If such an operator is invariant in G it is invariant under S_1, which transforms it into

$$S_1^v(S_1^{-1}\mathcal{H}S_1),$$

and hence

$$\mathcal{H} = S_1^{-1}\mathcal{H}S_1.$$

Consequently

$$\mathcal{H} = h_j.$$

If now the transform of $S_1^v h_j$ under S_2 is considered it follows that

$$S_2^{-1}S_1^vS_2 = S_1^v.$$

Hence the only additional invariant operators which need be sought are powers of S_1. If no power of S_1 is invariant under S_2, the central will be wholly contained in H and will be identical with the cyclic sub-group already found.

The next step then is to investigate when a relation such as

$$S_2^{-1}S_1^vS_2 = S_1^v$$

is satisfied. If it holds, so will

$$S_2^{n-v}S_1^vS_2^{-n+v} = S_1^v,$$

from which modified form it is possible to deduce a first necessary condition. For it implies

$$S_2^{n-v}S_1^v = (S_1^{n-v}S_2^v)^{-1} = S_1^vS_2^{n-v}.$$

In terms of the ξ's, this becomes

$$\prod_{i=1}^{n-v}\xi_i^{-1} = \prod_{i=1}^{v}\xi_i,$$

$$\prod_{i=n-v+1}^{n}\xi_i = \prod_{i=1}^{v}\xi_i,$$

and therefore

$$n - v = v,$$

whence

$$v = \frac{n}{2}\cdot$$

That is, the only power of S_1 which can be invariant in G is $S_1^{n/2}$.

If $S_1^{n/2}$ is invariant, then so is $S_1^{n/2}S_2^{n/2}$ also. For it is in H and is transformed into itself by S_2. But

$$S_1^{n/2}S_2^{n/2} = \prod_{i=1}^{n/2}\xi_i$$

and is invariant only when $x=2$; $m=D$. The latter of these relations requires m to be a divisor of n/k; the former requires that $k=n/2$.

These necessary conditions are also sufficient, and the resulting theorem is

THEOREM IV. *The central of G is cyclic and of order D where D is the greatest divisor of m and n/k except in the special case*

$$k = \frac{n}{2};\ m = 2;$$

in this latter case the order of the central is 2D.

The quotient group of H under G is cyclic and therefore abelian, hence H contains the commutator sub-group of G. To determine this sub-group, consider first the case $k=1$, and the following set of operators in H:

$$\xi_1\xi_2^{-1},\ \xi_1\xi_3^{-1},\ \cdots,\ \xi_1\xi_n^{-1}.$$

Each of these operators is a commutator; for

$$\xi_1\xi_a^{-1} = S_1S_2^{a-1}S_1^{-1}S_2^{-(a-1)}.$$

Again, the first $n-2$ of them are at once seen to be independent since they involve only $n-1$ of the ξ's. The group generated by them is therefore of order m^{n-2}. If the operator $\xi_1\xi_n^{-1}$ or any of its powers were in this group, they would be obtainable from the continued product of the first $n-2$ generators; for, it has already been seen that the relation between the ξ's involved all of them in a continued product. Now

$$(\xi_1\xi_2)^{-1}(\xi_1\xi_3^{-1})\cdots(\xi_1\xi_{n-1}^{-1}) = \xi_1^{n-2}(\xi_2^{-1}\xi_3^{-1}\cdots\xi_{n-1}^{-1}) = \xi_1^{n-1}\xi_n.$$

Suppose

$$(\xi_1\xi_n^{-1})^\alpha = (\xi_1^{n-1}\xi_n)^\beta.$$

Then

$$\xi_1^\alpha\xi_n^{-\alpha} = \xi_1^{n\beta-\beta}\xi_n^\beta,$$

from which

$$\alpha \equiv -\beta \pmod{m}$$

and

$$n\beta \equiv 0 \pmod{m}.$$

This last result is identical with the congruence obtained in the study of the central. The smallest value of β which satisfies it is m/d where d is the greatest common divisor of m and n. Hence $\xi_1\xi_n^{-1}$ is contained in the sub-group under consideration if and only if $d=m$. Omitting that case for the time being, it follows that the $n-1$ operators $\xi_1\xi_a^{-1}$ are independent and generate a group K of index d under H.

It will now be shown that this group K is the commutator sub-group, by demonstrating that every commutator is contained in it. However it is first necessary to obtain some preliminary results.

Suppose $f(\xi)$ represents any combination of the ξ_i, which by virtue of commutativity may be written in the form

$$\xi_1^{a_1}\xi_2^{a_2}\cdots\xi_n^{a_n}.$$

Denote by $f_{(-q)}(\xi)$ the combination

$$\xi_{1-q}^{a_1}\xi_{2-q}^{a_2}\cdots\xi_{n-q}^{a_n} \qquad (a-q\equiv n-a+q).$$

Then

$$f(\xi)\cdot[f_{(-q)}(\xi)]^{-1}$$

is in K. For this product contains n pairs of factors,

$$\xi_r^{a_r}\xi_{r-q}^{-a_r}$$

which may be written

$$(\xi_1\xi_r^{-1})^{-a_r}(\xi_1\xi_{r-q}^{-1})^{a_r}.$$

Consider now a general commutator of G. Every operator of G is expressible as some operator in H multiplied by a power of S_1 so that the most general commutator is

$$H_iS_1^\alpha\cdot H_jS_1^\beta(H_iS_1^\alpha)^{-1}(H_jS_1^\beta)^{-1} = H_iS_1^\alpha H_jS_1^{-\alpha}S_1^\beta H_i^{-1}S_1^{-\beta}H_j^{-1}.$$

It has already been seen that

$$S_1^{-1}\xi_iS_1 = \xi_{i-1},$$

from which

$$S_1^{-\alpha}\xi_i S_1^{\alpha} = \xi_{i-\alpha};$$

also

$$S_1\xi_i^{-1}S_1^{-1} = \xi_{i-1}^{-1},$$

$$S_1^{\alpha}\xi_i^{-1}S_1^{-\alpha} = \xi_{i-\alpha}^{-1}.$$

The above results show that the transform of any combination of ξ's by S_1^{α} reduces every original subscript by α. That is, it changes $f(\xi)$ into $f_{(-\alpha)}(\xi)$. The quantity

$$H_i(S_1^{\alpha}H_jS_1^{-\alpha})(S_1^{\beta}H_i^{-1}S_1^{-\beta})H_j^{-1}$$

is therefore equal to

$$H_iH_{j(-\alpha)}H_{i(-\beta)}^{-1}H_j^{-1} = H_iH_{i(-\beta)}^{-1}H_{j(-\alpha)}H_j^{-1}.$$

According to the preliminary lemma, this is contained in K and therefore K is the commutator sub-group.

Returning now to the case $d=m$, a group of index d under H would be generated by $n-2$ operators, thus explaining why $\xi_1\xi_n^{-1}$ is in this case contained in the group generated by the other $n-2$ of the operators $\xi_1\xi_a^{-1}$.

This remark now makes the result perfectly general for the case $k=1$. The commutator sub-group for every group of order nm^{n-1} is of index d under H. In particular, when $d=1$, i.e., when G contains no other invariant operator than the identity, the commutator sub-group coincides with H.

The generalization to any value of k offers no essential difficulty. The reasoning follows along the same lines and in the final result the only change is the replacement of d by D where D is the greatest common divisor of m and n/k.

THEOREM V. *The commutator sub-group of G is contained in H and is of index D where D is the greatest common divisor of m and n/k. It is generated by the $n-1$ operators*

$$\xi_1\xi_a^{-1} \qquad (a = 2, 3, \cdots, n).$$

VI. SPECIAL CASES

The following special cases seem worthy of mention.

In the simplest case, $m=1$ and G is cyclic. $S_1=S_2$ and the relation

$$(S_1S_2^{k-1})^x = 1$$

reduces to an identity.

The family of groups G includes the dihedral groups as the special case $n=2$.

In the special case $n=3$, $k=1$, G is the group of order $3m^2$, previously studied by Edington* in his thesis and also by Miller.*

In the special case $n=4$, $k=2$, G is of order $4m^2$ and is another of the families obtained by Edington in his thesis. He defined the group by means of the relations

$$S_1^4 = S_2^4 = (S_1S_2)^2 = 1.$$

The condition $(S_1 S_2)^2=1$ is exactly what $(S_1S_2^{k-1})^x=1$ reduces to on setting $x=2$. It is interesting to note in connection with this family of groups that it is not necessary to assume the operators $S_1^\alpha S_2^{n-\alpha}$ commutative. In this particular case that property follows as a consequence of the defining relations.

Finally, Edington's groups of order nm^{n-1} mentioned in the introduction are simply isomorphic with the groups obtained on setting $k=1$.

* W. E. Edington, these Transactions, vol. 25 (1923), p. 193. G. A. Miller, Proceedings of the National Academy of Sciences, vol. 13 (1927), p. 24.

George Washington University,
Washington, D. C.