GROUPS IN WHICH THE SQUARES OF THE ELEMENTS ARE A DIHEDRAL SUBGROUP*

BY

G. A. MILLER

1. **The dihedral subgroup is non-abelian.** If a group G has the property that the squares of its operators constitute a given group then the direct product of G and any abelian group of order 2^m and of type $(1, 1, 1, \cdots)$ has the same property. Such direct products will always be excluded in what follows. It has been noted that a necessary and sufficient condition that there is at least one group G which has the property that the squares of its operators constitute a given non-abelian dihedral group H is that the order h of H is not divisible by 8 and that every odd prime number which divides h is congruent to unity modulo 4.† To determine the number of these groups when h is given and satisfies these conditions we let n represent the number of the different prime numbers which divide h. Since the cyclic subgroup K of index 2 contained in H is the direct product of its Sylow subgroups and all the groups of isomorphisms of these Sylow subgroups are cyclic it results that when h is twice an odd number there is one and only one group of order $h \cdot 2^{n-2}$ which satisfies the condition that the squares of its operators constitute K.

The given group of order $h \cdot 2^{n-2}$ is the largest group which has the property that the squares of its operators constitute K when h is twice an odd number, as will be assumed until the contrary is explicitly stated. It is merely the direct product of $n-1$ dihedral groups, each of order twice the power of an odd prime. The commutator subgroup of every G is K and the corresponding quotient group is the abelian group of type $(2, 1, 1, \cdots)$. This results directly from the fact that if two operators of G have squares which are contained in K then the square of their product is also contained therein since this square could not be an operator of order 2 in H in view of the fact that this product could not transform this cyclic subgroup according to an operator of order 4.

It should be emphasized that an operator of G which transforms some of the operators of the cyclic subgroup of index 2 in H according to an operator of order 2 does not necessarily transform all the operators of this subgroup, besides the identity, according to such an operator, but that every operator

* Presented to the Society, September 7, 1934; received by the editors April 13, 1934.

† G. A. Miller, Proceedings of the National Academy of Sciences, vol. 20 (1934), p. 129.

of G which transforms an operator of this cyclic subgroup according to an operator of order 4 transforms each of these operators besides the identity, according to such an operator. Hence G involves a subgroup of index 2 composed of all of its operators which transform the operators of the given cyclic subgroup either into themselves or into their inverses. Each of the remaining operators of G is of order 4 and transforms the operators of odd order in H according to one of the 2^{n-1} ways in which these operators can be transformed when they are transformed according to an operator of order 4. Since such an operator and its inverse transform the operators of odd order differently it results that we have to consider only 2^{n-2} of these different possible transformations.

The largest possible order of G is $h \cdot 2^{n-1}$ and there is one and only one G of this order. It involves as a subgroup of index 2 the given group of order $h \cdot 2^{n-2}$ composed of all the operators whose squares are the operators of odd order in H. To determine all the possible G's it is desirable to note the different possible subgroups composed of the operators whose squares constitute the operators of odd order in H. If such a subgroup is of order $h \cdot 2^{n-2-\alpha}$ the number of the possible G's which involve it is 2^{α} since there are 2^{α} sets of operators of order 4 which can be added to it to obtain a G having the required properties and each of these sets transforms the operators of odd order in H in a different way. The number of the possible subgroups of order $h \cdot 2^{n-2-\alpha}$ has been determined recently* and hence there results the following theorem:

The number of the groups which involve a given dihedral group whose order is twice an odd number as the group of the squares of their operators, when the number of the different prime factors of the order of this dihedral group is n and each of these odd factors is congruent to unity modulo 4 is equal to the sum of the indexes of all the subgroups, including the identity and the entire group, of the abelian group of order 2^{n-2} and of type $(1, 1, 1, \cdots)$ under this group.

It was noted above that the operators of odd order in H constitute the commutator subgroup of G. This fact can also be established by noting that every such group can be represented as a transitive substitution group whose degree is equal to the order of K, since its Sylow subgroup whose order is a power of 2 does not involve any invariant subgroup of G besides the identity. This follows from the fact that direct products are excluded. Hence it results that each of the groups determined above is contained in the holomorph of K. The subgroup composed of all the substitutions which omit a fixed letter of this holomorph is therefore in the group of isomorphisms of K. Since

* G. A. Miller, Proceedings of the National Academy of Sciences, vol. 20 (1934), p. 203.

the group of isomorphisms of a cyclic group is abelian it results that the Sylow subgroups whose orders are a power of 2 in such a G are always abelian and hence all of these Sylow subgroups are of type $(2, 1, 1, \cdots)$.

The number of these Sylow subgroups is $h/2$ and no two of them have an operator of order 4 in common. A necessary and sufficient condition that no two of them have an operator of order 2 in common is that the order of such a G is $2h$. The number of the groups of this order is 2^{n-2} and all of them are conformal. Every other G contains more than one of these conformal groups. In fact, if the order of such a G is $2^k \cdot h$ it contains 2^{k-1} of these groups. The number of the possible G's increases very rapidly with the increase of n. In particular, when $n=5$ there are 51 such groups; viz., 8 of order $2h$, 28 of order $4h$, 14 of order $8h$, and one of order $16h$. This number depends only on the number of the distinct prime numbers which divide h and is independent of the values of these primes.

It remains to determine the possible groups when h is four times an odd number and each of the odd prime factors of h is again congruent to unity modulo 4. None of these groups is contained in the holomorph of K, since half of the operators of H are negative when it is thus represented. Each of the two dihedral subgroups of index 2 contained in H is invariant under G since all the operators of G which are either commutative with every operator of K or transform some of these operators into their inverses constitute a subgroup of index 2 under G. Each of the remaining operators of G is of order 4 and has for its square a non-invariant operator of order 2 in H. Since these operators cannot transform the two given dihedral subgroups of H into each other none of the operators of G can have this property and therefore each of these dihedral subgroups is invariant under G.

The commutator subgroup of G is again composed of the operators of odd order in K. Hence it results that all the operators of G whose squares appear in one of the two dihedral subgroups of index 2 in H constitute a subgroup of index 2 under G. That is, every such G contains as a subgroup of index 2 one of the groups enumerated above which has the property that the squares of its operators are a dihedral group whose order is twice an odd number. To extend one of the given groups so as to obtain the desired result we may represent it as a regular substitution group and make it simply isomorphic with itself represented on a different set of letters so as to obtain an intransitive substitution group. To this we may adjoin a substitution of order 4 which is commutative with every substitution of this intransitive group, interchanges its two systems of intransitivity and has for its square the invariant substitution of order 2 contained in H. Each such G contains two subgroups of index 2 such that the squares of their operators are the dihedral subgroups of index 2

in H, and one such subgroup such that the squares of its operators constitute the cyclic subgroup of index 2 in H. The cross-cut of these three subgroups is the subgroup of index 4 composed of the operators of odd order in H.

From the preceding paragraph it results that G involves an invariant cyclic subgroup of order h and is contained in the holomorph of this cyclic subgroup. Its operators whose squares are the non-invariant operators of order 2 in H transform the operators of this cyclic subgroup into powers which are congruent to unity modulo 4 as otherwise these squares of operators of order 4 would not give all the non-invariant operators of order 2 in H. It therefore results that every such G contains an operator of order 4 which is commutative with each of its operators and hence there results the following theorem:

Each group in which the squares of the operators constitute a dihedral group whose order is twice an odd number is a subgroup of index 2 under one and only one group in which the squares of the operators constitute a dihedral group whose order is four times an odd number and the number of distinct groups in both of these cases is the same.

2. **The dihedral subgroup is the four group.** The special case when the operators which are the squares of the operators of a given group G constitute the four group is much more difficult than the more general case when these squares constitute a non-abelian dihedral group. The only abelian group which comes under this special case is the group of order 16 and of type (2, 2), and the order of every other group which comes thereunder is obviously also of the form 2^m. The commutator subgroup of every such non-abelian group is either of order 2 or of order 4. We shall first consider the former case and hence the operators of order 2 contained in G together with its operators of order 4 whose squares are equal to the commutator of order 2 constitute a subgroup of index 2 under G. This subgroup belongs to one of the three known infinite categories of groups involving separately two and only two operators which are squares. Its central involves at least three invariant operators of order 2 and at most seven such operators since G is supposed to have the property that it is not a direct product.

When the central of this subgroup involves only three operators of order 2 there are two such groups of order 2^m when m is odd and exceeds 3. These are the direct products of the cyclic group of order 4 and of the groups which involve only two operators which are squares but do not contain an invariant operator of order 4. There are also two such groups of order 2^m when m is even and exceeds 4. One of these two groups is also the direct product of the

cyclic group of order 4 and a non-abelian group which involves only two operators which are squares but involves an invariant operator of order 4, while the other is obtained by extending such a non-abelian group by an operator which does not transform into itself its invariant operator of order 4. When the central of the given subgroup of index 2 involves seven operators of order 2 there are two additional such groups when m is even and there is one such additional group when m is odd. Hence there results the following theorem:

There are four groups of order 2^m, m *being even and larger than* 4, *which satisfy the condition that each of them has the four group for the group of its squares and involves a commutator subgroup of order* 2. *When* m *is odd and larger than* 5 *there are three such groups.*

It remains to consider the case when the commutator subgroup of G is the same as the group of the squares of its operators and we shall first consider the special case when G involves an abelian subgroup of index 2. This subgroup is of one of the following three types: $(1, 1, 1, \cdots)$, $(2, 1, 1, \cdots)$, $(2, 2, \cdots)$ and G involves only one abelian subgroup of this index. There is one and only one G which involves such a subgroup of the first of these three types. It is of order 32 and involves 12 operators of order 4. When this abelian subgroup is of the second type the order of G is either 32 or 64. In the former case there is one such G. This involves 20 operators of order 4. In the latter case there is also one and only one such G. This contains 40 operators of order 4. It remains to consider the case when the abelian subgroup of index 2 is of type $(2, 2, 1, 1, \cdots)$ and hence the order of G is 32, 64, or 128.

In the first case there are two groups in which all of the remaining operators are of the same order. These are the generalized dihedral and the generalized dicyclic groups. When only four of the operators of the given abelian subgroup of index 2 are transformed into their inverses under G there are also two groups of order 32. In one of these each of the remaining operators is of order 4 while only half of these operators are of this order in the other. There is one additional such group of order 32 in which no one of the operators of order 4 in the given abelian subgroup of order 16 is transformed into its inverse under G. This group involves 24 operators of order 4 of which eight have a common square. When G is of order 64 it involves invariant operators of order 4 and there are two isomorphisms to be considered. One of these gives rise to two distinct groups while the other gives rise to only one group. There is obviously only one group of order 128 which involves this abelian subgroup of index 2 and hence the following theorem has been established:

There is one and only one group which satisfies the conditions that it involves the abelian group of type (1, 1, 1, · · ·) *as a subgroup of index* 2 *and that the squares of its operators as well as its commutator subgroup constitute the four group. There are two such groups which involve the abelian group of type* (2, 1, 1, · · ·) *as such a subgroup, and there are nine such groups which involve the abelian group of type* (2, 2, 1, 1, · · ·) *as such a subgroup.*

The most difficult case remains, viz., the one when G contains no abelian subgroup of index 2 and when the commutator subgroup of G coincides with the group of its squares. All these possible groups may be divided into three categories composed of those whose centrals are of order 4, 8, or 16 respectively. These centrals are of types (1, 1), (2, 1) and (2, 2) respectively. For each of these categories it is possible to construct an infinite system of groups such that every operator which does not appear in the central has four conjugates under the group. To do this we may start with any abelian group whose order is four times the order of the central and whose squares appear in the four group contained therein. The group thus obtained is then extended twice successively by two operators which are relatively commutative and are commutative only with the operators of the given subgroup which appear in the central, and whose product has the same property. The order of the group thus obtained is sixteen times the order of its central, and each of its own invariant operators has four conjugates under it. This group can be extended successively by two operators which have their squares therein and are commutative with each other and with each operator of the given group. The resulting group can be extended as before. By continuing this process we obtain a group whose order is an arbitrary power of 16 times the order of the central and all of whose operators which do not appear in this central have four conjugates under the group.

The lowest order of a group G which belongs to the infinite system described in the preceding paragraph is 64. This is also the lowest order of G whenever it does not involve an abelian subgroup of index 2. If such a G is of order 64 and all of its operators except those which are squares have four conjugates under G, then every such operator appears in an abelian subgroup of order 16 and G contains exactly five such subgroups. These subgroups have the central of G in common but no two of them have any other operator in common. There is one such group which involves two abelian subgroups of order 16 and of type (1, 1, 1, 1). The other three abelian subgroups of order 16 contained therein are of type (2, 2). When there is one and only one such subgroup in G there is also a subgroup of type (2, 2). Hence there is only one

such G. It also contains exactly 27 operators of order 2. There is one and only one G in which there is no abelian subgroup of type (1, 1, 1, 1). It contains only eleven operators of order 2. This proves the following theorem:

There are three and only three groups of order 64 *which separately satisfy the following conditions: the group of their squares and their commutator subgroup is the four group and each of the operators which is not in this four group has four conjugates under the group.*

UNIVERSITY OF ILLINOIS,
URBANA, ILL.