LEMMA 3. *For every even* $p \geqq 2$,

$$A_p \leqq A_{p-1} + 1, \quad a_{p+1} \leqq a_p + 1; \tag{11}$$

$$a_{p-1} \leqq a_p + 3, \qquad A_p \leqq A_{p+1} + 3. \tag{12}$$

The proof of (11_1) is typical. By (9_2) and (9_3) with $p-1$ and p in place of p, $A_p \equiv A_{p-1}+1 \pmod 4$. Hence the contrary of (11_1) would imply $A_p = A_{p-1}+5+4v_1$, and consequently $b_p = b_{p-1}-7-6v_1$, where $v_1 \geqq 0$. Hence, by $4A_p \geqq (b_p)^2$,

$$4(A_{p-1} + 5 + 4v_1) \geqq (b_{p-1} - 7 - 6v_1)^2,$$

contradicting (10_1) with $p-1$ in place of p, since

$$4(1 + 4v_1) \leqq 2(1 + 6v_1)(6 - b_{p-1}) + (6v_1 + 1)^2.$$

THE CALIFORNIA INSTITUTE OF TECHNOLOGY

GROUPS GENERATED BY TWO OPERATORS WHOSE SQUARES ARE INVARIANT

BY G. A. MILLER

It is well known that two operators of order two generate the dihedral group whose order is twice the order of the product of these operators. The groups that can be generated by two operators which have a common square are also well known. The groups considered in the present article are obviously a generalization of these two categories of well known groups. We shall represent their two generators by s and t. From the fact that s^2 and t^2 are invariant operators of the group G generated by s and t it results directly that

$$s^{-1}sts = t^{-1}stt = ts = (st)^{-1}s^2t^2,$$

$$s^{-1}tss = t^{-1}tst = st = (ts)^{-1}s^2t^2.$$

From these equations it follows that the abelian group H generated by s^2, t^2, and st is invariant under G and that its index under G cannot exceed 2.

A necessary and sufficient condition that H be identical with G is that G be abelian and can be generated by the product of two of its operators and the squares of these operators. It is not

difficult to find a characteristic property of the abelian groups which can be thus generated. In a cyclic group we could use the identity for one of these operators and any generator of the cyclic group for the other. Hence we may restrict our attention to the groups of rank 2. If an abelian group of rank 2 and of order 2^m has the generators s and t, then s^2 and t^2 must appear in a subgroup of index 4. As this subgroup contains $(st)^2$ it results that an abelian group of order 2^m cannot be generated by the product of two of its operators and their squares unless it is cyclic. Since an operator of odd order can always be generated by its square, we may state the following theorem.

THEOREM 1. *A necessary and sufficient condition that an abelian group can be generated by the product of two of its operators and their squares is that its Sylow subgroup of order 2^m is cyclic and that the rank of each of its other Sylow subgroups does not exceed* 2.

In view of this theorem we shall confine our attention in what follows to the non-abelian groups which can be generated by s and t, and involve s^2 and t^2 as invariant operators. The abelian subgroup H is therefore of index 2 under G, and the rank of H cannot exceed 3. The problem of determining all the groups which can be generated by two operators whose squares are invariant is therefore included in that of adjoining to the abelian group H an operator which has its square in H and also transforms the operators of H according to an automorphism of order 2. When H is cyclic, then all the groups which can be thus constructed obviously satisfy the condition that they can separately be generated by two operators whose squares are invariant, but this is not necessarily true as regards the groups thus constructed when H is non-cyclic. We shall first determine the total number of such groups when H is cyclic.

It is well known that the group of isomorphisms of a cyclic group of order p^m, p being an odd prime number, is cyclic and hence it involves only one operator of order 2, while the group of isomorphisms of the cyclic group of order 2^m involves three operators of this order when $m>2$, one such operator when $m=2$, and none when $m=1$. If l represents the number of the distinct prime numbers which divide h, the order of H, the number of operators of order 2 in the group of isomorphisms of the cyclic group H is 2^l-1 when h is either odd or divisible by

4 but not by 8; when h is divisible by 8 this number is $2^{l+1}-1$, and when h is twice an odd number it is $2^{l-1}-1$. When h is odd only one group results from such an automorphism of order 2 while there are two and only two such groups whenever h is even.* Hence the following theorem.

THEOREM 2. *The number of non-abelian groups which can be generated by two operators whose squares are invariant and involve a given cyclic subgroup of order h is 2^l-1 when h is odd, $2^{l+1}-2$ when h is divisible by 4 but not by 8, 2^l-2 when h is twice an odd number, and $6\cdot 2^{l-1}-2$ when h is divisible by 8, l being the number of the distinct primes which divide h.*

When H is non-cyclic and of odd order it is known that in any automorphism of order 2 of H a set of independent generators of H can be so selected that every operator of the set corresponds either to itself or to its inverse.† Moreover, if we extend such an H of rank two or three by an operator of order 2 which transforms one and only one of its independent generators into its inverse and is commutative with the remaining generator when H is of rank 2, or with the other two generators when H is of rank 3, there results a non-abelian group which can be generated by two operators whose squares are invariant. To prove this fact let s_1 and s_2 be two conjugates of the given extending operator of order 2, and suppose that they were so selected that their product is the independent generator of H which is transformed into its inverse. For s we may then use the product of s_1 and another independent generator of H while for t we may take s_2 if H is of rank 2 or s_2 into the remaining independent generator of H when H is of rank 3. Hence the following result has been proved.

THEOREM 3. *Every abelian group of odd order whose rank does not exceed 3, when extended by an operator of order 2 which transforms into its inverse one and only one operator of a set of its independent generators, and is commutative with the remaining operator or operators of the set, gives rise to a group which can be generated by two of its operators whose squares are invariant.*

---

* G. A. Miller, Proceedings of the National Academy of Sciences, vol. 14 (1928), p. 819.

† G. A. Miller, Transactions of this Society, vol. 10 (1909), p. 472.

It should be noted that this theorem includes all the non-abelian groups which can be thus generated when the order of H is odd since such a group must contain an operator of order 2 and this operator could not transform into their inverses two of the independent generators of H. To determine the number of the distinct groups which can involve such a given H we may confine our attention to the case when this H is non-cyclic since this number is included in the theorem given above when H is cyclic. It will be convenient to consider first the case when H is of rank 2 and hence at least one of its Sylow subgroups is of this rank. If one of the Sylow subgroups of H contains two equal invariants, then one of its independent generators must appear in one of the independent generators of H while the other appears in the second independent generator of H. The selection of s and t is therefore not affected by such a Sylow subgroup of H. On the other hand, if a Sylow subgroup of H is either cyclic or has two unequal invariants the operators s and t can be selected in two different ways as regards such a subgroup. Hence we have the following result.

THEOREM 4. *The number of the non-abelian groups which can be generated by two of their operators whose squares are invariant and involve a given abelian subgroup of rank* 2, *index* 2, *and of odd order is* 2^l *where* l *represents the number of the Sylow subgroups of this abelian subgroup which are either cyclic or have two unequal invariants.*

When H is of rank 3 at least one of its Sylow subgroups must be of this rank and a set of independent generators of H can be so selected that the remaining operators of G transform one of the operators of the set into its inverse while they are commutative with each of the other two operators of the set, as was noted above. Since the resulting group is affected only by the selection of the independent generator of H which is transformed into its inverse under G, it results that when H involves a Sylow subgroup which has three equal invariants the selection of s and t is not affected thereby. On the other hand, if H involves a Sylow subgroup which has either three distinct invariants, or only two invariants and these are distinct, the selection of s and t can be made in three different ways in regard thereto. Moreover, this selection can always be made in two

different ways as regards a Sylow subgroup which is either cyclic or involves two and only two equal invariants. This establishes the following theorem.

THEOREM 5. *Any given abelian group of odd order and of rank* 3 *appears as a subgroup of index* 2 *in* 2^l+3^k *non-abelian groups which can be generated separately by two of their operators whose squares are invariant, where* l *represents the number of its Sylow subgroups which are either cyclic or have two and only two equal invariants while* k *represents the number of these subgroups which have either three distinct invariants or have only two invariants but these are distinct.*

It remains to consider the case when H is both non-cyclic and of even order. Before considering this case it may be desirable to direct attention to the construction of two operators of even order which are commutative, independent, and have the property that the order of their product is equal to the order of the product of their squares. To construct two such operators we first write two cycles on distinct sets of letters such that their orders are equal to one-half of the orders of these operators and multiply one of these cycles on the right and the other on the left by a substitution of order 2 which connects each letter of these cycles with a letter which does not appear in either of them. The square of these products will consist of two equal cycles, one of which is the original cycle. The product of these products will be of the same order as the product of their squares and will be independent of the latter product.

Let H be any abelian group which has at least one even invariant and suppose that the corresponding independent generator of H is associated with st, while the other two are associated with s^2 and t^2, respectively. We may then find two operators of order 2 whose product is the independent generator associated with st and multiply one of these into an operator which is commutative with it and independent thereof such that its square is s^2. This product may be used for s. In a similar way the operator which may be used for t is selected as regards the second of the two given operators of order 2. When H is of rank 2 it may be assumed that $t^2=1$. Hence we have the following fact.

THEOREM 6. *Every abelian group whose rank does not exceed* 3 *and whose order exceeds* 2 *is a subgroup of index* 2 *of a non-abelian group which can be generated by two operators whose squares are invariant under the group, and every group which can be thus generated involves such an abelian subgroup.*

From this theorem it results that the category of groups which are characterized by the fact that each of them can be generated by two of its own operators whose squares are invariant under the group is very large. All such groups are solvable and have a simple structure. For the sake of illustration it may be desirable to note here the smallest of these groups in which H has three invariants. Hence the order of G could not be less than 16 and if G is of this order H must be of type $(1,1,1)$. It is well known that the group of isomorphisms of this H is the simple group of order 168 and that all of its operators of order 2 are conjugate. Hence we have to take for s an operator of order 4 which transforms H according to the said operator of order 2. Since t is also of order 4 and its square is different from s^2 and the commutator of G is s^2t^2, the group G is completely determined. Hence there is one and only one non-abelian group of order 16 which can be generated by two of its operators whose squares are invariant and involves an abelian subgroup of rank 3. It may be noted that this is also the only group of order 16 which is decomposable into two non-invariant cyclic subgroups. In fact, there is one and only one group of order p^4 which is thus decomposable, p being any prime number.*

THE UNIVERSITY OF ILLINOIS

* G. A. Miller, Proceedings of the National Academy of Sciences, vol. 16 (1930), p. 527.