GROUPS CONTAINING ONLY THREE OPERATORS WHICH ARE SQUARES*

BY

G. A. MILLER

Every group besides the abelian group of order 2^a and of type $(1, 1, 1, \cdots)$ contains at least two operators which are squares of other operators in the group. If there are only two such operators they constitute an invariant subgroup and the corresponding quotient group contains only one operator which is a square. All the groups which satisfy this condition have recently been determined.† The present paper is devoted to a complete determination of the groups involving just three operators which are squares. As the identity is its own square such a group (G) contains only two operators besides the identity which have the property in question.

If the order (g) of G is divisible by an odd number, this number is 3 and G includes only one subgroup of this order, since every operator of odd order is the square of some power of itself. As such a group cannot contain an operator of order 4 and its order is 3.2^a, it must be the direct product of the abelian group of order 2^a and of type $(1, 1, 1, \cdots)$, and the cycle group of order 3; or one of its subgroups of order 3.2^{a-1} must be of this type. In the latter case, G is evidently the direct product of the symmetric group of order 6 and the abelian group of order 2^{a-1} and of type $(1, 1, 1, \cdots)$. In what follows, these trivial cases will not be considered. Hence g will always be of the form 2^a and G contains only operators of orders two and four in addition to the identity. Moreover, each of the two operators (t_1, t_2) which are squares but are not the identity is of order two and hence it is the square of some operators of order four. We shall first prove that t_1, t_2 are invariant under G.

§ 1. *Invariance of the operators which are squares.*

If t_1, t_2 were not commutative their product would be of order four. As $t_1 t_2$ is transformed into its inverse by both t_1 and t_2 the square of $t_1 t_2$ could not be either t_1 or t_2. Hence the assumption that t_1, t_2 are not commutative leads to a contradiction. From this it follows that the four group $1, t_1, t_2, t_1 t_2$ is

* Presented to the Society (San Francisco) September 30, 1905. Received for publication September 4, 1905.

† Mathematische Annalen, vol. 60 (1905), p. 597.

invariant under G and that $t_1 t_2$ is an invariant operator of G. If t_1 is not invariant under G it must be invariant under a subgroup H whose order is $g/2$. As every operator of G transforms the given four-group into itself it follows that t_1 transforms every operator of $G - H$ into itself multiplied by $t_1 t_2$.

Let s be any operator of $G - H$. From the preceding paragraph it results that $t_1 s t_1 s = t_1 t_2 s^2$. If $s^2 = 1$ the operator $t_1 s$ would have $t_1 t_2$ for its square, which is contrary to the hypothesis. If $s^2 = t_2$ the operator $t_1 s$ would have t_1 for its square. Hence t_1 would be commutative with $t_1 s$ and as it is commutative with t_1 it would also be commutative with s, which is contrary to the hypothesis. Finally, s^2 is not t_1 since s and t_1 are not commutative. As the assumption that there is some operator in $G - H$ leads to an absurdity it follows that each of the operators of the four-group $1, t_1, t_2, t_1 t_2$ is invariant under G. This result may be stated as follows: *If a group of order* 2^a *contains only three operators which are squares of its operators, each of these three operators is invariant under the group.*

Since the quotient group of G with respect to the subgroup $1, t_1, t_2, t_1 t_2$ is composed of operators of order two in addition to the identity it is clear that the commutator subgroup is included in this four group. Hence every commumutator of G is invariant. Moreover, G cannot be abelian since the product of two square operators of any abelian group is a square under the same group. The commutator subgroup of G must therefore be either of order two or of order four.

§ 2. *Groups in which the commutator subgroup is of order two.*

There are two cases to be considered. In the first case the commutator subgroup is generated by an operator of order four contained in G, while this subgroup is $1, t_1 t_2$ in the other case. We shall see that there is just one group of order 2^β, $\beta > 3$, under each of these cases. In the first case it may be assumed that the commutator subgroup is $1, t_1$. Let s represent any operator of G whose square is t_2. Since $t_1 t_2$ is not a square under G it follows that s is not commutative with any operator whose square is t_1. That is, *in all the groups under consideration two operators of order four which have different squares must be non-commutative.* Hence s is commutative with each operator of a subgroup H· whose order is $g/2$.

It is easy to see that H includes all the operators of order 2 which are contained in G, otherwise the product of s into such an operator would have $t_1 t_2$ for its square. Hence $G - H$ is composed of operators of order 4, and includes all the operators of this order whose square is t_1. The product of s into an operator of $G - H$ whose square is t_1 is an operator whose square is t_2 while the square of the product of s into an operator of $G - H$ whose square is t_2 is t_1. Hence just half the operator of $G - H$ have t_1 for their squares.

Let s' be any one of these operators. The operators of G which are commutative with s' include just half the operators of H. All of these operators are of order 2 since all the operators of order 4 in H have t_2 for their square. Since the product of s into any of these operators is of order 4 it follows that exactly half the operators of H are of order 4 and that each of the operators of order 2 in H is commutative with every operator of G, as it is commutative with s and with at least half the operators in $G - H$. From this it follows that H is abelian and of type $(2, 1, 1, 1, \cdots)$. As these conditions define G completely it has been proved that *there is one and only one G of order 2^β, $\beta > 3$, in which the commutator subgroup is generated by an operator of order four.*

We proceed to consider the case in which the commutator subgroup is $1, t_1 t_2$. Let s and H have the same meaning as before, and let s' represent any operator of G whose square is t_1. As observed above s' is in $G - H$. No operator of $G - H$ can have t_2 for its square since $t_1 t_2$ is not a square under G. Moreover, s into any operator of order 4 in $G - H$ is an operator of order 2, and s into any of these operators of order 2 is of order 4. That is, just half the operators of $G - H$ are of order 2 and the operators of order 4 in $G - H$ have t_1 for their common square.

As s' is not commutative with any operator of order 4 in H it must be commutative with each of the operators of order 2 in H. That is, each of the operators of order 2 in H is commutative with every operator of order 4 in $G - H$, and as such an operator is also commutative with s it follows that *each operator of order two in H is invariant under G.* Hence H is again the abelian group of order $2^{\beta-1}$ and of type $(2, 1, 1, \cdots)$. As the given conditions determine G completely there is only one such G whose order is 2^β, $\beta > 3$. This completes the proof of the statement at the beginning of this section that *there are exactly two groups of order 2^β in which the commutator subgroup is of order two and just three operators, including the identity, are squares under the group.* In one of these groups the operators of order two together with the identity constitute a subgroup of order $2^{\beta-2}$ while these operators constitute a subgroup of order $2^{\beta-1}$ in the other.

§ 3. *Groups in which the commutator subgroup is of order four.*

An operator of order two cannot be transformed into itself multiplied by $t_1 t_2$ by an operator of order two since $t_1 t_2$ is not a square under G. Hence G must involve operators of order four which are transformed into themselves multiplied by $t_1 t_2$ under G. Let s represent such an operator of order four and let H represent the group formed by all the operators of G which are either commutative with s or transform s into $t_1 t_2 s$. Let H' be the subgroup of H which is composed of all its operators which are commutative with s. We proceed to prove that H' is abelian.

All the operators of order 4 in H' must have the same square (t_1) since they are commutative with s. Hence just half the operators of H' are of order 4. The product of s into any operator of order 4 in $H - H'$ is of order 2 and the product of s into any operator of order 2 in $H - H'$ is of order 4. Hence just half of the operators of $H - H'$ are of order 4 and all of these operators have t_2 for their square.

Let t be any operator of order two contained in H. As the commutator subgroup of H' is either 1 or $1, t_1$ it follows that the operators of H' cannot transform t into more than two operators, viz., into t, $t_1 t$. Moreover, none of the operators of $H - H'$ can transform t into $t_1 t_2 t$ since none of these operators has t_1 for its square. As these operators could not transform t into $t_1 t$ it follows that t is invariant under G. That is, *each of the operators of order two in H' is invariant under H.* This proves also that H' is abelian and that the commutator subgroup of H is $1, t_1 t_2$. It also proves that every operator of order four in G which has $t_1 t_2$ for a commutator must also have t_1 and t_2 for commutators and that the order of H is $g/2$.

Every operator of $G - H$ transforms each operator of order 4 in H into itself multiplied by either t_1 or t_2. There are two cases to be considered. In the first $G - H$ contains operators which are commutative with every operator of order two in H. Such an operator could not be of order two since $t_1 t_2$ is not a square. Hence we may assume that $G - H$ contains an operator (t) of order four which is commutative with every operator of order two in H and transforms each of the other operators into itself multiplied by t_1. Since t into some operator of order two in H transforms each operator of order 4 in H into itself multiplied by t_2 and since the product of t into the given operator has the same square as t has it follows that there is only one such group, and that each of the operators in $G - H$ is of order four.

This group of order 2^β, $\beta > 4$, contains an abelian subgroup of order $2^{\beta-1}$ and of type $(2, 1, 1, \cdots)$. The remaining operators are of order 4 and exactly half of them have the same square as the operators of order 4 in this abelian subgroup. It contains $2^{\beta-3}$ invariant operators and its operators of order 4 which are contained in the given abelian subgroup have only two conjugates under G while the remaining operators of order 4 have four such conjugates. Its group of cogredient isomorphisms is of order 8 and involves no operator of order 4. Its non-invariant operators of order two have only two conjugates; in fact, the non-invariant operators of order two in all the groups under consideration have only two conjugates.

If $G - H$ does not involve any operator which is commutative with every operator of order two in H, each of these operators transforms the operators of order 4 in H into themselves multiplied by the two distinct operators t_1, t_2. Each operator of order two in H is therefore transformed into itself or into itself multiplied by $t_1 t_2$ by means of every operator in $G - H$. Some of the operators which are invariant under H are transformed into themselves multiplied by $t_1 t_2$ by means of the operators in $G - H$, otherwise there would be operators in $G - H$ which would be commutative with every operator of order two in H. Hence all the transformations of H which need to be considered are conjugate under its group of isomorphisms, that is, it is necessary to consider only one such transformation.

All the operators in $G - H$ are again of order 4, since an operator of order two cannot transform another operator of order two into itself multiplied by $t_1 t_2$ in any of the groups under consideration. Since two operators may be found in $G - H$ such that their squares are distinct but that they transform H in exactly the same manner it follows that this case leads to only one group of order 2^β, $\beta > 5$. The group of cogredient isomorphisms of this group is of order 16 and contains only operators of order two in addition to the identity. It is conformal with the preceding group but each of its operators of order 4 has four conjugates under G while this is not the case in the one considered above. Hence it does not include an abelian subgroup of order $2^{\beta-1}$. In this respect it differs from the three which precede. The number of its operators whose square is t_1 is equal to the number of those whose square is t_2.

The main results may be stated as follows: If a group contains three and only three operators which are squares under the group it is the direct product of an abelian group of order 2^α and of type $(1, 1, 1, \cdots)$ into the cyclic group of order 3, the symmetric group of order 6, or a group of order 2^β, $\beta > 3$. When $\beta = 4$, there are two such groups of order 2^β; when $\beta = 5$, there are three; and when $\beta > 5$ there are four. In the last case, two of the groups have a commutator subgroup of order two while the other two have a commutator subgroup of order 4. Whenever the order of these groups exceeds the minimum order for which a group having the required properties can be constructed, they are the direct products of groups having the minimum order and an abelian group of type $(1, 1, 1, \cdots)$. Hence all the groups in question can be constructed by forming the direct products of an abelian group of this type and two groups of order 16, one of order 32 and one of order 64. The operators of order two in such groups have at most two conjugates while the operators of order 4 may have either two or four conjugates under the entire group.

Each of these four possible groups of order 2^β has exactly $2^{\beta-2} - 1$ subgroups of order $2^{\beta-1}$, since the only operators which are common to every possible subgroup of this order are $1, t_1, t_2, t_1 t_2$. The two possible groups of order $3.\ 2^\alpha$ have exactly $2^\alpha - 1$ subgroups of order $3.2^{\alpha-1}$, since there are only three operators which are common to all such subgroups. These facts exhibit the close contact between the present paper and the following: *On the invariant subgroups of prime index*, Transactions of the American Mathematical Society, vol. 6 (1905), p. 326; *Generalization of the Hamiltonian groups*, Mathematische Annalen, vol. 60 (1905), p. 597.