ON THE MINIMUM NUMBER OF OPERATORS WHOSE ORDERS EXCEED TWO IN ANY FINITE GROUP.

BY PROFESSOR G. A. MILLER.

LET the order of any group G be represented by $g = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda}$; $p_1, p_2, \cdots, p_\lambda$ being distinct odd prime numbers. When $\alpha_0 = 0$ all the operators of G except identity are of orders which exceed two. Hence we shall assume in what follows that $\alpha_0 > 0$. In this case it is easy to see that there is at least one group of order g in which the number of operators whose orders exceed two is exactly

$$\frac{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda} - 1)g}{2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda}} \equiv N.$$

Such a group may be constructed by forming the direct product of a group of order $2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda}$ in which just half the operators are of order two * and the abelian group of order $2^{\alpha_0 - 1}$ and of type $(1, 1, 1, \cdots)$. The main objects of this paper are to prove that N is the minimum number of operators whose orders exceed two that can occur in a group of order g, and if a group of this order has exactly N operators whose orders exceed two it is the direct product of a group in which just half the operators are of order two and the abelian group of order $2^{\alpha_0 - 1}$ and of type $(1, 1, 1, \cdots)$.

When $g = 2^{\alpha_0}$, $N = 0$ and the theorem requires no proof. When $\alpha_0 = 1$, $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda} - 1$ and the theorem is evident from the well-known theorem that every group whose order is twice an odd number contains a subgroup of half its order which is composed of operators of odd order in addition to identity. Hence we shall assume in what follows that $\alpha_0 > 1$ and $N > 0$. Since G is supposed to contain a minimum number of operators whose orders exceed two, it may be assumed that over half of the operators of G are of order two. Hence G is generated by its operators of order two, and as it contains oper-

* If just half the operators of a group are of order 2, the order of the group is twice an odd number, and all its operators of odd order together with identity constitute an abelian subgroup whose order is half the order of the group.

ators whose orders exceed two, it must be non-abelian. It must, therefore, contain non-invariant operators of order two.

Let H_1 be the subgroup of G which is composed of all the operators of G which are commutative with one of its non-invariant operators t_1 of order two. The products obtained by multiplying t_1 into operators of order two in $G - H_1$ are of orders which exceed two, since all of these operators of order two are non-commutative with t_1. Hence $G - H_1$ contains at least as many operators whose orders exceed two as of order two. From this it follows that more than half the operators of H_1 are of order two. If H_1 contains operators whose orders exceed two it is non-abelian and vice versa.

When H_1 is non-abelian, it contains a non-invariant operator t_2 of order two. In this case its subgroup composed of its operators which are commutative with t_2 may be denoted by H_2. More than half the operators of H_2 are of order two; and, if it is non-abelian, we continue in the same way until we arrive at an abelian subgroup H_m. All the operators of H_m except identity are of order two. Since at least half of the operators of $H_x - H_{x+1}$ $(x = 1, 2, \cdots, m - 1)$ are of orders which exceed two, it follows that at least half the operators of $G - H_m$ are of orders which exceed two.

It is possible that different choices of non-invariant operators of order two might affect the order of H_m. We suppose that the operations were effected in such a manner that the order of H_m is as large as possible. Such an H_m can be obtained by a finite number of operations since g is finite. The index of H_m under G cannot be less than $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda}$, as the order of H_m is a power of 2. Since at least half of the operators in $H_x - H_{x+1}$ are of orders which exceed two, it is clear that the minimum number of operators whose orders exceed two in a group of order g is one-half the number of operators in $G - H_m$ when the index of H_m under G has its minimum value, viz., $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda}$. That is, *$N$ is the minimum number of operators whose orders exceed two in any group of order g.*

It remains only to determine all the possible groups of order g which contain exactly N operators whose orders exceed 2. In what follows it will be assumed that G satisfies this condition. If an operator of order two in $H_{m-1} - H_m$ were commutative with some operator whose order exceeds two in H_{m-1} their product would be in $H_{m-1} - H_m$ and would be transformed into its inverse by t_m. As t_m would transform into its

inverse the given operator whose order exceeds two as well as this product, it would have to be commutative with the operator of order two from $H_{m-1} - H_m$. Since this is impossible, it follows that all the operators of order two in $H_{m-1} - H_m$ are commutative with exactly 2^{α_0} operators in H_{m-1}* and that these operators constitute a subgroup which is conjugate with H_m under H_{m-1}.

Since all the subgroups of order 2^{α_0} are conjugate under H_{m-1} and one of them contains an operator which is non-invariant under H_{m-1}, all of these Sylow subgroups must have this property. If an operator occurs in two of them it must occur in all of them, since it is commutative with operators of H_{m-1} whose orders exceed two. All the non-invariant operators of order two in H_{m-1} must therefore transform every operator whose order exceeds two in H_{m-1} into its inverse. As one of the latter operators is transformed into its inverse by at least half the operators in $H_{m-1} - H_m$ and by the operators of H_m which are not commutative with every operator of H_{m-1}, it must be transformed into its inverse by just half the operators of H_{m-1}. Hence H_m contains just 2^{α_0-1} operators which are invariant under H_{m-1}.

There are as many operators in H_{m-1} that are commutative with one of its operators whose order exceeds two as there are of those which transform this operator into its inverse. As the latter includes half the operators of H_{m-1} the former set must be composed of the remaining half. Hence every operator whose order exceeds two in H_{m-1} is commutative with each of the other operators in H_{m-1} which have this property. From this it follows that all the operators of odd order in H_{m-1} together with identity constitute an abelian subgroup, and that any non-invariant operator of order two together with this abelian subgroup generate an invariant subgroup in which just half its operators are of order two. This subgroup is invariant since it includes all the conjugates of its operators of order two. Hence H_{m-1} *is the direct product of a subgroup in which just half the operators are of order two and the subgroup of order* 2^{α_0-1} *formed by the invariant operators of* H_{m-1}.

We shall now prove that the order of H_x is divisible by $p_1^{\alpha_1}$ whenever it is divisible by p_1. Suppose that $p_1^{\alpha_1}$ is the highest power of p_1 which divides the order of H_x and that the order

* Every operator of order two must be found in one of the Sylow subgroups of order 2^{α_0}, and all of these subgroups are similar to H_m.

of H_{x-1} is divisible by $p_1^{\alpha'+1}$. Hence H_{x-1} contains a subgroup of order $p_1^{\alpha'+1}$ which has $p_1^{\alpha'}$ operators in H_x and the remaining operators in $H_{x-1} - H_x$. All the operators of H_x are commutative with t_x and all the operators whose orders exceed two in $H_{x-1} - H_x$ are transformed into their inverse by t_x. As this is impossible* it follows that the order of H_x is divisible by $p_1^{\alpha_1}$ whenever it is divisible by p_1.

Our next object is to prove that H_{m-1} is identical with G. This will be proved by showing that the opposite hypothesis leads to an absurdity. Suppose that the order of H_{m-1} is $2^{\alpha_0} p_1^{\alpha_1} \cdots p_{\lambda'}^{\alpha_{\lambda'}}$, $\lambda' < \lambda$. Hence the order of H_{m-2} is divisible by primes which do not divide the order of H_{m-1}. The operator t_{m-1} of order two which is invariant under H_{m-1} but not under H_{m-2} is found in the subgroup K of H_{m-1} which is composed of its 2^{α_0-1} invariant operators. All the operators whose orders exceed two in $H_{m-2} - H_{m-1}$ are transformed into their inverses by t_{m-1}. As the number of conjugates of t_{m-1} under H_{m-2} is the index of H_{m-1} under H_{m-2} it follows that the operators in $H_{m-2} - H_{m-1}$ cannot be transformed into more different operators to obtain their inverses than the given index. Hence these operators cannot include more operators of odd order than this index, since two distinct operators of odd order must be multiplied by two distinct operators in order to obtain products which are the inverses of the first two operators.

It is now easy to prove that the Sylow subgroup of order $p_1^{\alpha_1}$ contained in H_{m-1} is transformed into itself by operators of odd order in $H_{m-2} - H_{m-1}$. This is true when this is the only subgroup of order p^{α_1} in H_{m-2}. It is also true when this Sylow subgroup has less conjugates under H_{m-2} than the index of H_{m-1} under H_{m-2}, since this index involves no primes which divide the order of H_{m-1}. The remaining cases are when this Sylow subgroup has as many conjugates under H_{m-2} as this index and some of these Sylow subgroups have common operators or no two of them have common operators. The former of these two cases is excluded by the last footnote, since the Sylow subgroup in H_{m-1} would have operators in common with some other Sylow subgroup. The latter of the two cases is excluded by the fact

* The truth of this statement follows from the elementary theorem: If an operator transforms all the operators of a group which are not included in an invariant subgroup of index $k > 2$ into their inverses it transforms every operator of the group into its inverse and the group is abelian. Hence all the Sylow subgroups of odd order contained in G are abelian.

that the number of operators of odd order in $H_{m-2} - H_{m-1}$ cannot exceed the index of H_{m-1} under H_{m-2}.

Having proved that the assumption that the order of H_{m-1} is less than the order of G requires that the Sylow subgroup of order $p_1^{\alpha_1}$ in H_{m-1} is transformed into itself by operators of odd order in $H_{m-2} - H_{m-1}$, it is now easy to see that this assumption leads to an absurdity. In fact, the theorem of the last footnote shows clearly that this subgroup of order $p_1^{\alpha_1}$ cannot be transformed into itself by any operator of odd order in $H_{m-2} - H_{m-1}$, since it would be invariant in a group which would have only $p_1^{\alpha_1}$ operators in common with H_{m-1} and the remaining operators of this group would be transformed into their inverses by t_{m-1}. Hence the theorem: *If a group of order g contains the smallest possible number of operators whose orders exceed two, the subgroup which is composed of all its operators which are commutative with one of the non-invariant operators of order two contains no operator whose order exceeds two.* Moreover, this subgroup is a Sylow subgroup, and just half of the remaining operators are of order two.

If we combine with this theorem the one stated above in regard to H_{m-1}, we have a complete determination of all the possible groups of order g in which the number of operators whose orders exceeds two is a minimum. To construct these groups it is only necessary to construct all the possible abelian groups of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda}$ and add to each of them an operator of order two which transforms each of its operators into its inverse. The groups thus obtained may be multiplied directly into the group of order 2^{α_0-1} which contains only operators of order two in addition to identity. Hence there are as many such groups as there are abelian groups of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda}$.

The preceding considerations show that the minimum number of operators whose orders exceed two in any group with the single exception of the abelian group of order 2^α and of type $(1, 1, 1, \cdots)$ is one fourth of the order of the group. If more than one fourth of the operators have orders which exceed two, at least one third of the operators have this property. When the order of the group is a power of 2, all the possible ratios between the number of the operators whose orders exceed two and the order of the group have been determined on the hypothesis that this ratio is less than one half. It is clear that N, in the present article, has for its limits one third and one half respectively, — the former being attained, while the latter is not attained.