GROUPS IN WHICH EVERY OPERATOR HAS AT MOST A PRIME NUMBER OF CONJUGATES*

BY
G. A. MILLER

Let G represent a non-abelian group such that each of its operators is either invariant or has p conjugates, p being a prime number which is the same for every operator of G, and let s_1 represent one of the operators of lowest order contained in G and non-invariant under G. The subgroup H_1 composed of all the operators of G which are commutative with s_1 is of index p under G, and includes s_1 as well as the central H_0 of G. It will be proved first that G involves only one Sylow subgroup of order p^m. If it could contain more than one subgroup of order p^m the powers of some operator of one of these would transform the cross-cut of two of them into itself and would also transform one of these two subgroups into itself and the other into exactly p distinct subgroups, since this operator may be so selected that its pth power is in this cross-cut but it itself is not contained therein.

To prove that this operator would have more than p conjugates under G it is only necessary to observe that it would appear in one and only one of a set of p subgroups of order p^m which would be conjugate under the powers of some operator contained in one of the given $p+1$ subgroups of this order. As these p subgroups would contain an operator which would transform the given operator into at least one additional conjugate, the following theorem has been established:

If a group contains more than one Sylow subgroup of order p^m then it contains a set of conjugate operators whose order is a power of p and whose number exceeds p, where p is any prime number.

By hypothesis G transforms the operators contained in each set of conjugates according to a transitive permutation group of degree p and it has just been proved that this transitive group cannot involve more than one subgroup of order p since such a subgroup is a Sylow subgroup therein. As G must be isomorphic with every such transitive group it follows directly that each of these transitive groups is cyclic. Hence G must be isomorphic with an abelian group of type $(1, 1, 1, \cdots)$ whose order is a power of p. That is, G is the direct product of a non-abelian group of order p^m and an abelian group whose order is prime to p. In what follows it may therefore be

* Presented to the Society, June 19, 1933; received by the editors March 13, 1933.

assumed for the sake of simplicity that the order of G is p^m. Since every subgroup of index p under a group of order p^m is invariant thereunder it follows that H_1 is an invariant subgroup of G.

An operator of G which is not found in H_1 transforms s_1 into s_0s_1 where s_0 is commutative with s_1 since H_1 is an invariant subgroup of G and all of its operators are commutative with s_1. Hence it results that s_0 is of order p. To prove that s_0 appears in the central of G it may be noted that it must be transformed into itself by each of the operators which do not appear in H_1 since every such operator must be commutative with a subgroup of index p under H_1 and s_0 must be in such a subgroup since it arises from a p automorphism. If t were a non-invariant operator of G which would not be transformed into itself multiplied by a power of s_0, then G would involve operators which would be commutative neither with s_1 nor with t. Such an operator would therefore be transformed into more than p conjugates under G. It has therefore been proved that *if every non-invariant operator of a group has a given prime number of conjugates under this group then the order of the commutator subgroup of this group is this prime number and its operators are invariant under the group.*

When H_1 is non-abelian it contains an invariant subgroup H_2 composed of all of its operators which are commutative with one, s_2, of its operators of lowest order. By continuing this process we finally arrive at an invariant abelian subgroup H_λ which involves $s_1, s_2, \cdots, s_\lambda$ as well as H_0. A set of independent generators of H_λ can be so selected that it includes $s_1, s_2, \cdots, s_\lambda$ since these were always chosen so as to be of the lowest possible order. As H_0 includes the pth power of every operator of G it includes the pth powers of $s_1, s_2, \cdots, s_\lambda$ and the central quotient group of G is abelian and of type $(1, 1, 1, \cdots)$. In particular, G/H_λ has these properties. It should be noted that H_0 is the direct product of the group generated by the pth powers of $s_1, s_2, \cdots, s_\lambda$ and some other group which may be the identity. The order of G/H_0 is $p^{2\lambda}$ while that of G/H_λ is p^λ.

To exhibit the fact that the preceding theorems relate to an extensive category of groups it may be noted that for every value of $m>2$ there are groups which belong to this category and that the number of these groups increases with m. In particular, the two non-abelian groups of order p^3 belong to this category and six of the non-abelian groups of order p^4 belong thereto. When $p=2$ it is known that there are nine non-abelian groups of this order and when $p>2$ their number is always ten. Hence more than one-half of the non-abelian groups of order p^4 come under the heading of the present article. For all of these groups $\lambda=1$ since H_0 cannot be the identity and the order of

G/H_0 is always $p^{2\lambda}$, as was noted above. Whenever $m>4$ then λ can obviously have more than one possible value.

When m is given and greater than 2 the possible values of λ depend upon the type of the abelian group which is selected for H_λ since λ may assume successively the values 1, 2, $\cdots$ up to the number of the invariants of this abelian group if at least one of these invariants exceeds p. When all of these invariants are equal to p the value of λ may be any positive integer which does not exceed the number of these invariants diminished by unity in view of the following theorem:

If a non-abelian group G in which all the non-invariant operators have exactly a prime number p conjugates contains a non-invariant operator s_1 of order p, and if the subgroup composed of all of its operators which are commutative with s_1 is either abelian or contains a non-invariant operator s_2 of order p, etc., then the operators s_1, s_2, $\cdots$, s_λ generate an abelian group of order p^λ which does not include the commutator subgroup of G.

To prove this theorem it is only necessary to note that this abelian subgroup contains no operator besides the identity which is invariant under G.

To construct all the groups of order p^m which satisfy the conditions imposed on G at the opening of this article we may first consider those in which $\lambda=1$, then those in which $\lambda=2$, etc., until we arrive at those in which λ has its largest possible value, viz., $(m-1)/2$ when m is odd and $(m-2)/2$ when m is even. For the central of such groups we may take successively every possible abelian group of order $p^{m-2\lambda}$, and two groups in which the centrals are distinct groups must themselves be distinct, so that we may avoid duplicates by classifying these groups of the same order according to their distinct centrals. When H_λ is cyclic, $\lambda=1$ since H_λ involves $s_1, s_2, \cdots, s_\lambda$ as independent generators. Moreover, G must then be the quaternion group since H_1 is of index p and G must then involve $p+1$ cyclic subgroups of this index. It is well known that the quaternion group is the only group of order p^m, $m>2$, which involves $p+1$ cyclic subgroups of index p.

When $\lambda=1$ general formulas for the totality of the non-abelian groups which come under the heading of the present article may be obtained as follows. Suppose first that all the invariants of H_0 are equal to a fixed number p^α. It is known that if any abelian group has a subgroup of prime index then it is always possible to find a set of reduced independent generators of this group which has the property that all the operators of this set except one appear in this subgroup.* Hence a set of reduced independent generators of

* G. A. Miller, Bulletin of the American Mathematical Society, vol. 23 (1916), p. 14. The term "reduced set of independent generators" was used with its present meaning with respect to abelian groups in these Transactions, vol. 16 (1915), p. 22.

each of the $p+1$ abelian subgroups of index p contained in G can be so selected that all except one of them appear in H_0. The additional independent generator of such a reduced set can therefore be so selected in the present case that its order is either p or $p^{\alpha+1}$. In what follows it will be assumed that such a selection of a set of the reduced independent generators of these subgroups has been made.

When H_0 is cyclic there are always two possible groups. In the special case when $p=2$ and $m=3$ these are the octic and the quaternion groups while in all the other cases the additional generators of two abelian subgroups of index p under G can be so selected that either both are of order p or one is of order p and the other is of order p^{m-1}. When H_0 has two equal invariants p^α there are four groups. In one of these the additional generators of two of the abelian subgroups of index p can be so chosen that both are of order p. In two others one of these generators is of order p while the other is of order $p^{\alpha+1}$ except when $p=2$ and $m=4$. In this special case there is only one such additional group while there are two groups in which all the additional generators are of order $p^{\alpha+1}$. In the other cases there is only one such group. When the number of the equal invariants of H_0 exceeds two there is one additional group in which all the additional independent generators are of order $p^{\alpha+1}$ since the commutator subgroup for such groups can then be chosen in two distinct ways. When $p=2$ and $m=4$ this commutator subgroup can be chosen in three different ways but there are then only two distinct groups under the other cases.

For the sake of simplifying the consideration of the general case when $\lambda=1$ we let k_1 represent the number of the different values of the invariants of H_0, k_2 the number of the sets composed separately of all the equal invariants whenever such a set involves at least two such invariants, k_3 the number of such sets such that each set involves at least three equal invariants. The number of the distinct groups of order p^m which contain this H_0 and in which the additional invariant of each of two abelian subgroups of index p is equal to p is then k_1, since H_0 contains k_1 sets of subgroups of order p such that each set is composed of all of its subgroups of this order which are conjugate under the holomorph of H_0.

If one of the $p+1$ abelian subgroups of index p under G has an invariant which is equal to p but is not included among the invariants of H_0, while another has a larger invariant having these properties, there are $k_1^2+k_2$ groups of order p^m since the commutator subgroup may be taken from any one of the k_1 sets of conjugate subgroups of order p under the holomorph of H_0 and the second independent generator which does not appear among the independent generators of H_0 may have its pth power in any one of the k_1

sets of conjugate operators such that each set is composed of all the operators which can be separately used as an independent generator of H_0. In the special case when at least one of the invariants of H_0 is 2, one of the groups of this case is included among the k_1 groups defined in the preceding paragraph. Hence there are then only $k_1^2+k_2-1$ additional groups.

Finally, when none of the additional invariants is equal to p the pth powers of the independent generators of the $p+1$ abelian subgroups of index p under G which are not also independent generators of H_0 are equal to distinct independent generators of H_0 except possibly when $p=2$ and these additional invariants are equal to 4. In the latter case these operators of order 4 may generate the quaternion group and then the commutator subgroup of G is the subgroup of order 2 contained in this quaternion group. In all other cases two equal additional independent generators can be selected in k_2 essentially different ways while two such unequal generators can be selected in $k_1(k_1-1)/2$ essentially different ways.

In the former case the number of the distinct groups when none of these invariants is equal to 2 is $k_1k_2+k_3$ since in k_3 cases the subgroups of order p in H_0 which are conjugate under its holomorph are not conjugate in the holomorph of G. In the latter case the number of these groups is $k_1^2(k_1-1)/2$ $+k_2(k_1-1)$. Hence the total number of the distinct G's when $\lambda=1$ and H_0 does not involve an invariant which is equal to 2 is

$$k_1 + k_1^2(k_1+1)/2 + 2k_1k_2 + k_3.$$

This formula gives also the correct number of groups when H_0 involves at least one invariant which is equal to 2. It was noted above that in this case the number of groups in which only one additional invariant of the $p+1$ abelian subgroups of index p under G is p is one less than in the other cases, but the number of the groups in which all the additional invariants are equal to p^2 is then one more than in the other cases in view of the existence of the quaternion group. When H_0 involves more than one invariant which is equal to 2 and the commutator of order 2 is the square of one of the additional independent generators of order 4, and has a different square, then the operators of order 2 in the group generated by these operators of order 2 are not conjugate under its holomorph while they are thus conjugate in the other cases. This however does not affect the number of the possible distinct groups in this case.

If a group of order p^m contains more than one abelian subgroup of index p then the cross-cut of two such subgroups is its central and its commutator subgroup is of order p. Hence such a group belongs to the category of groups defined by the heading of the present article and the value of λ in this case is unity. The formula given in the preceding paragraph therefore gives also the number of these distinct groups whenever we use successively for H_0 the different possible abelian groups of order p^{m-2}. Since every group of order p^4 contains at least one abelian subgroup of order p^3, it results that the only non-abelian groups of order p^4 which are not enumerated by the given formula are those which contain only one abelian subgroup of index p. There are three such groups when $p=2$, but whenever $p>2$ there are four such groups.

University of Illinois,
Urbana, Ill.