ON THE INVARIANT SUBGROUPS OF PRIME INDEX*

BY

G. A. MILLER

The totality formed by all the operators of any group (G) which are common to all the invariant subgroups of prime index (p) constitutes a characteristic subgroup, and the corresponding quotient group is the abelian group of order p^λ and of type $(1, 1, 1, \cdots)$.† The number of the invariant subgroups of index p is therefore $p^\lambda - 1/p - 1$. The given totality includes all the operators of G which are pth powers, and it is composed of such operators whenever G is abelian. In this case λ is clearly equal to the number of the invariants in the Sylow subgroup of order p^m contained in G. This fact follows also directly from the theory of reciprocal groups, since p^λ is the order of the subgroup generated by all the operators of order p contained in G. For instance, the abelian group G contains only one subgroup of index p whenever its Sylow subgroup of order p^m, $m > 0$, is cyclic, it contains $p + 1$ such subgroups whenever this Sylow subgroup involves two invariants, $p^2 + p + 1$ whenever there are three invariants, etc.

When G is non-abelian the determination of λ is much more difficult. Its value can clearly not exceed the value of λ for a Sylow subgroup of order p^m contained in G, but it may be less. Hence it is of fundamental importance to determine the values of λ for the groups of order p^m, and we shall assume that this is the order of G in what follows. Instead of determining the value of λ for given types of groups, it seems much more desirable to determine the possible types of groups when the value of λ is given. This problem soon becomes very difficult. When $\lambda = 1$, G is cyclic; and when $\lambda = m$, G is the abelian group of type $(1, 1, 1, \cdots)$. These extreme cases relate to fundamental groups whose elementary properties are well known. The case when $\lambda = m - 1$ includes the Hamiltonian groups. All the groups which belong to this case have recently been determined.‡ The main object of the present paper is the study of an interesting category of groups which belong to the case when

* Presented to the Society (San Francisco) February 25, 1905. Received for publication March 2, 1905.

† BAUER, Nouvelles Annales, vol. 19 (1900), p. 509.

‡ Mathematische Annalen, vol. 60 (1905).

$\lambda = m - 2$; viz., all those whose commutator subgroup is of order p. The two abelian groups which come under this case are of types $(3, 1, 1, \cdots)$ and $(2, 2, 1, 1, \cdots)$ respectively. In what follows it will be assumed that G is non-abelian.

The following theorem is of considerable interest in itself and is proved here because it will be convenient to employ a special case of it in the study of the groups under consideration.

THEOREM. *If the commutator subgroup of a group of order p^m is of order p, each of the operators which are common to every subgroup of index p is invariant under the entire group.*

As an invariant subgroup of order p is composed of invariant operators under a group of order p^m, it follows that all the commutators of the group in question are invariant. Hence each operator of the group contains at most p conjugates. If an operator (s) were not commutative with each of the operators which are common to every subgroup of index p, the subgroup of index p composed of all the operators which are commutative with s would not include all the given common operators. As this is impossible each of the common operators is invariant under the entire group.

Let K represent the largest subgroup of G which is common to all its subgroups of index p. Since G contains just $1 + p + p^2 + \cdots + p^{m-3}$ subgroups of this index, the order of K is p^2. We shall consider the groups in question in two sections, — the first will be devoted to those in which K is cyclic and the second to those in which K is non-cyclic. The commutator subgroup of order p will be denoted by C in both of these sections.

§ 1. *Determination of all the possible groups when K is cyclic.*

Let I represent the commutator quotient group of G, that is, I is the quotient group of order p^{m-1} corresponding to C. Since I is abelian and contains just $1 + p + p^2 + \cdots + p^{m-3}$ subgroups of index p it is of type $(2, 1, 1, \cdots)$. The subgroup of G which corresponds to all the operators of I whose orders do not exceed p will be denoted by H. This subgroup is characteristic since it is composed of all the operators of G whose orders are less than p^3. This result follows also directly from the fact that H is composed of all the operators of G whose pth powers are commutators of G.

Since H is a characteristic subgroup of G any two G's must be distinct whenever their H's are distinct. The converse is not necessarily true; that is, two G's involving the same H may be distinct groups as will be seen in what follows. Moreover, H is one of the system of groups mentioned above in which $\lambda = m_1 - 1$; p^{m_1} being the order of H. The value of m_1 is $m - 1$ as stated above. Hence H may be regarded as known and it remains only to find the other possible operators of G. When H is abelian it is simply isomorphic

with I and it is easy to prove that only one group (G_1) can involve such an H and satisfy the conditions that K is cyclic and that there are just $1+p+p^2+\cdots+p^{m-3}$ subgroups of index p, p^m being the order of the group.

The group of cogredient isomorphisms of G_1 is of order p^2 since C is of order p and H is abelian. The truth of this statement may be seen as follows. If t is any operator of $G_1 - H^*$ it has just p conjugates under G_1 and hence it is commutative with a subgroup of order p^{m-2} contained in H. Since these p^{m-2} operators are commutative with every operator of H as well as with t they are commutative with every operator of G_1, that is, the group of cogredient isomorphisms of G_1 is of order p^2. Since the p^{m-2} invariant operators include K they constitute an abelian group of type $(2, 1, 1, \cdots)$.

It is now very easy to prove that there could not be two distinct G's involving the same abelian H. For in two such G's the H's could be made simply isomorphic in such a way that the K of one G would correspond to the K of the other, and that the subgroups composed of the invariant operators of the two H's would correspond. After this had been done, two operators of order p^3, one from each G, could be so chosen that their pth powers would correspond and that they would transform corresponding operators into corresponding operators. That is, the G's would be simply isomorphic.†

When H is non-abelian the considerations become a little more difficult. The results are as follows: *There are always just two G's for a given H except when H involves only p^2 invariant operators; in this special case there is only one G which involves a given H.* The main theorems which will be employed to arrive at these results are: The order of the group of cogredient isomorphisms of G is an even power of p, and the order of the group of cogredient isomorphisms of H is either the same as that of G or it is the quotient obtained by dividing that of G by p^2. This theorem is a direct consequence of the fact that the commutator subgroup of G is of order p, and hence requires no proof here.‡ The other fundamental theorem is as follows: It is possible to make H simply isomorphic with itself in such a way that a subgroup of index p corresponds to any arbitrary subgroup of this index provided these two subgroups involve the same number of invariant operators and include invariant operators of order p^2. Moreover, the subgroups formed by the invariant operators can be made simply isomorphic in any arbitrary manner such that the commutator subgroup corresponds to itself.

The proof of this theorem is readily obtained by means of the following known properties of H. There is one and only one H whose group of cogredient isomorphisms is of order $p^{2\alpha}$, $\alpha < (m-2)/2$; when $2\alpha < m-3$ this H

* This symbol represents the operators of G_1 which are not also in H.

† Bulletin of the American Mathematical Society, vol. 3 (1897), p. 218.

‡ FITE, Transactions of the American Mathematical Society, vol. 3 (1902), p. 342.

is the direct product of a group which has just p^2 invariant operators and an abelian group of type $(1, 1, \cdots)$. If a subgroup of index p in H includes all the invariant operators under H, the order of its group of cogredient isomorphisms is obtained by dividing the order of the group of cogredient isomorphisms of H by p^2. When this condition is not satisfied the subgroup of index p has the same group of cogredient isomorphisms as H has.*

By employing these theorems it is easy to prove that there is only one G which involves H and has the same group of cogredient isomorphisms as H has. For if there were two such G's they could be obtained by adding successively to H the two operators t_1, t_2 of order p^3. As the pth powers of these operators would be invariant under H it would be possible to make H simply isomorphic with itself in such a manner that t_1^p would correspond to t_2^p. Hence the entire groups would be simply isomorphic; that is, there is only one such G.

When the group of cogredient isomorphisms of G is not the same as that of H, it is necessary that H include at least p^3 invariant operators. Whenever this condition is satisfied it is evident that a G can be constructed. If there were two G's involving the same H they could again be constructed by adding to H two operators of order p^3, which may be represented respectively by t_1, t_2. As these operators would be commutative with all the operators of a subgroup of index p contained in H, and as H could be made simply isomorphic with itself in such a manner that these subgroups would correspond to themselves, and, moreover, t_1^p would correspond to t_2^p, it follows as before that there is only one such G. The results of this section may be summarized as follows:

When H is given it is always possible to construct two G's, provided H contains more than p^2 invariant operators. When H involves only p^2 invariant operators, only one G is possible. One of these two systems is composed of all the groups of order p^m which involve invariant operators of order p^3 and contain just $1 + p + p^2 + \cdots + p^{m-3}$ subgroups of index p. *There are just* $\frac{1}{2}(m-1)$ *such groups when* m *is odd. When* m *is even their number is* $\frac{1}{2}(m-2)$. The other system includes the same number of groups when m is even, but it contains one less when m is odd. That is, *the number of the groups which belong to this system is* $\frac{1}{2}(m-3)$ or $\frac{1}{2}(m-2)$, *as* m *is odd or even.* This system is composed of all the possible groups of order p^m which contain just $1 + p + p^2 + \cdots + p^{m-3}$ subgroups of index p and are generated by operators of order p^3 without also including invariant operators of this order.

If a group belongs to the latter system and contains more than p^2 invariant operators it is the direct product of a G which contains just p^2 invariant operators and an abelian group of type $(1, 1, \cdots)$. Similarly, if a group belongs to the former system and contains more than p^3 invariant operators it is the direct product of a G containing just p^3 invariant operators and an abelian group of type $(1, 1, 1, \cdots)$.

*Mathematische Annalen, loc. cit.

§ 2. *Determination of all the possible groups when K is non-cyclic.*

The commutator quotient group I is again the abelian group of type $(2, 1, 1, \cdots)$ and of order p^{m-1}. The characteristic subgroup H corresponds to all the operators of I whose orders do not exceed p just as in the preceding section. All the operators of $G - H$ are of order p^2 while in the preceding section the corresponding operators were of order p^3. As all the operators of H may be of order p it may be the abelian group of type $(1, 1, 1, \cdots)$. If it is not this group it contains just $1 + p + p^2 + \cdots + p^{m-3}$ subgroups of index p and hence it belongs to the known systems of groups which were mentioned above. The pth power of its operators are commutators of G.

Since any two invariant operators of H which are of order p without being commutators can be made to correspond in some simple isomorphism of H with itself it follows that there is one and only one G which has the same group of cogredient isomorphisms as the non-abelian H contained in it. That is, every non-abelian H which includes at least $p^2 - 1$ invariant operators of order p is contained in one and only one G whenever G includes invariant operators not contained in H. As the H's are known and these groups are obtained by extending H by means of an operator of order p^2 whose pth power is in H and which is commutative with every operator of H, this system of groups is completely determined. It therefore remains only to consider those G's whose group of cogredient isomorphisms are larger than those of the H's which they contain.

Every group in question may be constructed by extending some H by means of an operator t which is commutative with each of the operators of a subgroup H' of index p contained in H. As t^p is contained in H' and is commutative with every operator of G without being a commutator of G it follows that H' includes at least $p^2 - 1$ invariant operators of order p. Since the order of the group of cogredient isomorphisms of G is larger than that of H the subgroup H' cannot include all the invariant operators of H. Hence such an H must involve at least p^3 invariant operators under H, and whenever an H has this property a G can evidently be constructed. Since two G's must be distinct whenever their H's are distinct and we found the conditions which H must satisfy in order that a G can be constructed, it remains only to determine how many G's involve the same H. That is, if H is given it is required to find all the possible operators of order p^2 which may be used to extend H in such a way as to give rise to distinct groups.

Let t_1, t_2 be two operators which may be used to extend a fixed H so as to give rise to two distinct G's. Since it is possible to make H simply isomorphic with itself in such a way that any invariant operator of order p which is not a commutator can be made to correspond to any other operator having these properties, it is clear that the two G's would be simply isomorphic if the H' of the

one could be made to correspond to the H' of the other in some simple isomorphism of H with itself. That is, our problem is reduced to finding the number of subgroups of H which could be used as H' but could not be made simply isomorphic in any simple isomorphism of H with itself. In other words, the construction of all the possible groups in question is reduced to the determination of properties of a known system of groups.

As there are just three non-abelian H's which have the same group of cogredient isomorphisms * our problem is reduced to the determination of all the G's which involve these three distinct H's. Two of these contain no invariant operators of order p^2 while the third contains invariant operators of this order. It is not difficult to see that there is only one G which involves a given H that does not include invariant operators of order p^2. For the H' of such a G cannot include invariant operators of order p^2 since it cannot involve all the invariant operators of H. Hence all the subgroups which could be used for H' can be made to correspond in some simple isomorphism of H with itself. That is, there is only one G which involves such an H. It now remains only to consider the case when H includes invariant operators of order p^2 and has a given group of cogredient isomorphisms.

When such an H has more than p^3 invariant operators it follows directly from the known properties of H that it includes three distinct subgroups of index p which can be used as H' since they have the same group of cogredient isomorphisms as H has. These three H's are simply isomorphic with the three possible H's which have the same group of cogredient isomorphisms. When the H under consideration has only p^3 invariant operators there are only two such G's. Hence we have finally that *there are five G's which have the same group of cogredient isomorphisms provided the order of this group is less than p^{m-3}. When this order is p^{m-3} there are only four such G's.*

As these results follow directly from the known properties of H and from a known theorem in regard to simply isomorphic groups,† it seems unnecessary to enter upon further details. The special case when H is abelian presents no difficulty as there is only one possible G when H is of type $(1, 1, 1, \cdots)$, and there are two G's when H is of type $(2, 1, 1, \cdots)$. The infinite systems of groups determined in this paper are of interest on account of their elementary properties and also in view of the fact that they are completely defined by the number of their subgroups of index p and the order of the commutator subgroup. The close contact between this paper and the one in which the properties of every possible H are determined should be noted. The latter will shortly appear in the Mathematische Annalen under the title: *An Extension of the Hamiltonian Groups.*

* Mathematische Annalen, loc. cit.

† Transactions of the American Mathematical Society, vol. 3 (1902), p. 342.