GROUPS OF ORDER p^m CONTAINING EXACTLY $p+1$ ABELIAN SUBGROUPS OF ORDER p^{m-1}.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, October 27, 1906.)

IF an abelian group of order p^m, p being any prime, contains exactly $p+1$ subgroups of order p^{m-1} it has just two invariants and vice versa. Since these groups are so well known, we shall confine ourselves, in what follows, to non-abelian groups of order p^m. It is known that in every non-abelian group of this order the number of abelian subgroups of order p^{m-1} is 0, 1, or $p+1$. The present paper confines itself to the last of these three possible cases. Since any non-cyclic group of order p^m is generated by two of its subgroups of order p^{m-1}, and two such subgroups have p^{m-2} common operators, it follows that *the necessary and sufficient condition that a non-abelian group of order p^m contain $p+1$ abelian subgroups of order p^{m-1} is that it contain p^{m-2} invariant operators.* These invariant operators form a characteristic subgroup and the corresponding quotient group is of type (1, 1).

While we shall consider only non-abelian groups in the present paper, yet the abelian subgroups of order p^{m-1} will enter largely into our discussions. It seems therefore desirable to state here a few fundamental theorems with respect to abelian groups in the form in which they will be used. *If all the invariants of an abelian group of order p^m are equal, all its operators of the same order are conjugate under its holomorph and vice versa.* Any abelian group is the direct product of abelian subgroups in which all the invariants are equal. The number of complete sets of conjugate subgroups of order p^{m-1} under the holomorph of any abelian group of order p^m is equal to the number of its different sets of equal invariants, since this number is equal to the number of the different sets of conjugate subgroups of order p under the holomorph.* *The independent generators of any subgroup of order p^{m-1} in an abelian group of order p^m may be so chosen that they are either contained in a possible set of independent generators of the entire group, or that*

* *Amer. Jour. of Math.*, vol. 22 (1900), p. 21.

all of them except one are contained in such a set while this one is the pth power of the other independent generator of this set.

The last theorem may be proved as follows: Since the number of distinct sets of conjugate subgroups of order p^{m-1} under the holomorph is equal to the number of the different sets of equal invariants of the group G it is only necessary to observe that the independent generators of one out of each such set of these conjugate subgroups can be chosen in the given manner. This may be done by constructing, in succession, the groups which result by using the pth power of one of the independent generators of G together with all its other independent generators, using the pth power of only one of the independent generators of the same order in G. The independent generators of the subgroups of lower order than p^{m-1} cannot always be chosen in this way nor is it always possible to select the independent generators of G in such a way that they become, when one of them is raised to the pth power, identical with the independent generators of a subgroup of order p^{m-1} which have been arbitrarily chosen. These statements will be illustrated in the following paragraph.

Let s_1, s_2 represent two independent commutative operators of orders p^α, p respectively and suppose $\alpha > 1$. It is impossible to choose the independent generator of the subgroup $\{s_1^p s_2\}$ of index p^2 under $\{s_1, s_2\}$ in such a manner that it either is contained in a possible set of independent generators of $\{s_1, s_2\}$ or that it is a power of such a generator. This illustrates the former of the two statements in question. If we take as the independent generators of a subgroup of index p under $\{s_1, s_2\}$, the two operators $s_1^p s_2$, s_2 the latter of these statements is illustrated, since it is impossible to select the independent generators of $\{s_1, s_2\}$ in such a manner as either to include $s_1^p s_2$, s_2 or to make $s_1^p s_2$ a power of such a generator. In fact neither of the operators $s_1^p s_2$, s_2 is a power of a larger operator contained in $\{s_1, s_2\}$.

Since a characteristic subgroup of an abelian group cannot involve any of its operators of highest order, it follows that the largest characteristic subgroup of any abelian group is composed of all its operators which are not of highest order. In particular, *the necessary and sufficient condition that an abelian group of order p^m contains a characteristic subgroup of order p^{m-1} is that it has only one invariant of highest order.*

§1. *General Properties.*

Let H represent one of the $p+1$ abelian subgroups of order p^{m-1} and let K represent the subgroup of order p^{m-2} which is composed of the invariant operators under the entire group G. The general method which will be used in what follows is to assume H as known and then to consider all the possible groups of order p^m which contain this H. The three most important steps are: 1) the choice of K; 2) the possible transformations of H by the operators of G which are not contained in H; 3) the total number of groups which transform H in a given manner. The details of construction are given in the article * entitled "A method of constructing all groups of order p^m."

From the theorem mentioned above it follows that K can be chosen in as many distinct ways as there are different sets of equal invariants in H. That is, the number of sets of subgroups of order p^{m-2} in H which are such that each set includes all those which are conjugate under the holomorph of H is equal to the number of sets of equal invariants in H. This number will be denoted by k. As the invariants of the k distinct subgroups which are successively represented by K may be obtained by raising one of those of H, in succession, to the pth power, while the others remain unchanged, no two of these k subgroups are simply isomorphic. In particular, when all the invariants of H are equal, K can be chosen in only one way; so that $k=1$ in this case.

We shall now consider the transformations of H by possible operators of G. In other words, we shall consider the number of different sets of operators of order p in I (the group of isomorphisms of H) which are such that each operator is commutative with all the operators of a particular K and that each set includes all the operators of I which are conjugate under the subgroup of I which transforms K into itself. As all these transformations of H may be obtained by making it isomorphic with one of its subgroups of order p and multiplying corresponding operators,† the problem is reduced to finding the number of sets of conjugate subgroups of order p in H. This number is either k or $k+1$, as the invariant of H which is p times the corresponding invariant of K is unique or is equal to

* *Amer. Jour. of Math.*, vol. 24 (1902), p. 395.
† BULLETIN, vol. 7 (1901), p. 350.

at least one other invariant of H. Under the holomorph of G the subgroups of order p in K may be contained in $k-1$ sets of conjugates, as will be seen later.

It remains to consider the third of the three steps mentioned above, viz., the construction of the total number of groups which transform H in a fixed manner. There is clearly one and only one such G which involves an operator t of order p that is not contained in H. As K can be selected in k different ways, the total number of G's which involve H and also operators of order p which are not contained in H is $k(k+1)-l$, where l is the sum of the numbers of the sets of equal invariants of H which contain only one invariant $+1$ or 0, according as there is at least one invariant which is equal to p or no such invariant.

Each of the $k(k+1)-l$ groups considered in the preceding paragraph contains at least p abelian subgroups which are similar to H whenever $p>2$. The invariants of the remaining abelian subgroup of order p^{m-1} are obtained by dividing one of those of H by p and adding to this quotient and the other invariants of H one which is equal to p. In the groups in which these invariants are equal to those of H the $p+1$ abelian subgroups of order p^{m-1} in G are similar. There are k such groups when H contains more than one invariant which is equal to p, $k-1$ when H contains only one such invariant, and there is no such group when the smallest invariant of H exceeds p. When $p=2$ it is still true that at least two of the abelian subgroups of order 2^{m-1} are similar but they are not necessarily similar to H.

According to the general theory of constructing the groups of order p^m, all of the other groups having the required property may be constructed by making H simply isomorphic with itself written in p distinct sets of letters and replacing t by itself written in the same systems, multiplied by a substitution which simply interchanges these systems and by an operator s from one of these systems. The number of different groups is equal to the number of distinct ways of choosing s. This choice can generally be made in $k+1$ ways, but in special cases there may be a smaller number of choices, as follows directly from the general theory. The main result which we desire to emphasize here is that since s is in K but is not a power of an operator of higher order contained in K, the remaining p abelian subgroups of order p^{m-1} are similar to each other except when just $p-1$ of them are similar to H, while

the other involves more operators whose order is p times that of s than H does. We are thus led to the main theorem of this section, which may be stated as follows: *If a non-abelian group of order p^m involves $p+1$ abelian subgroups of order p^{m-1}, at least p of these subgroups are similar to each other, and the entire group is conformal with an abelian group whenever $p > 2$.*

Since a non-abelian group of order p^3 necessarily contains exactly $p+1$ subgroups of order p^2, the above theorem includes the theorem that a non-abelian group of order p^3 contains at least p similar subgroups of order p^2. It may also be stated that the preceding paragraph proves that the conformal non-abelian groups of order p^m which contain $p+1$ abelian subgroups of order p^{m-1} are not necessarily identical, while it is well known that abelian groups are identical whenever they are conformal.

§ 2. *Groups in Which the $p+1$ Abelian Subgroups of Order p^{m-1} are Similar to Each Other.*

Although these groups are included in the preceding section, yet it seems desirable to treat them somewhat more completely in view of the fact that they are of special interest. When all the invariants of H are equal to each other they are all equal to $p > 2$, or to 4. In the former case there is one and only one group of order p^m, $m > 2$. As all its operators are of order p, it is conformal with the abelian group of order p^m and of type $(1, 1, 1, \cdots)$. When all the invariants of H are equal to 4 there is one and only one group of order 2^{2n+1}, $n > 0$. Since the commutator of order 2 in such a group is the square of a non-invariant operator of order 4, it is the direct product of the quaternion group and the abelian group of order $2^{n'}$ and of the type $(1, 1, 1, \cdots)$. These results are expressed in the following theorem: *If a non-abelian group of order p^m involves $p+1$ abelian subgroups of order p^{m-1} and if all the invariants of these subgroups are equal to the same number, then either the group is the direct product of the quaternion group and an abelian group of order $2^{n'}$ and of the type $(2, 2, 2, \cdots)$, or it is the direct product of the non-abelian group of order p^3 $(p > 2)$ which involves no operator of order p^2 and the abelian group of order $p^{n'}$ and of type $(1, 1, 1, \cdots)$*

If the conditions of the preceding paragraph are made somewhat more general by merely requiring that the invariants of each one of the $p+1$ abelian subgroups be equal to each other, there are only two additional groups which satisfy these condi-

tions, viz., the octic group and the non-abelian group of order p^3 which involves operators of order p^2. These properties might be employed to give new definitions of these groups. For instance, the former of these two groups, which is so fundamental in elementary mathematics, may be defined as follows: the octic group is the only non-abelian group of order 2^m which contains three abelian subgroups of order 2^{m-1} such that the invariants of each subgroup are equal to each other, but not all these invariants are equal to the same number.

We shall now consider the case where the $p+1$ abelian subgroups of order p^{m-1} are similar to each other and where each of them involves more than one set of equal invariants. From the preceding section it follows that the invariants of H must satisfy at least one of the following two conditions: The smallest is either p or 4, or the ratio of some two is p. When the former of these conditions is satisfied, but not the latter, the invariants of K may be obtained from those of H by dropping one of the smallest ones, if these are equal to p, or by replacing a 4 by a 2. In the former case the number of possible G's, when $p > 2$, is either k or $k-1$, according as H contains more than one or only one invariant which is equal to p. When $p = 2$ there are always $k-1$ such G's. Finally, when the smallest invariants of H are equal to 4 there is just one such group involving a given H. This exhausts the possible cases where no two invariants of H have p for their ratio.

When H involves invariants whose ratio is p and also operators of order p or 4, the groups which have just been determined will still exist. The remaining possible groups are independent of whether H involves operators of order p or 4. When $p > 2$ there are $k+\gamma$ groups for every two sets of equal invariants which are such that the ratio of the invariants of one set with respect to those of the other is p. The value of γ is -1, 0, or 1, according as each of these two sets includes only one invariant, one includes one while the other includes more than one, or each of them includes more than one.

When $p = 2$ the remarks of the preceding paragraph remain true except when H involves invariants which are equal to 2 and also invariants which are equal to 4. In this special case it is only necessary to consider the possible groups where K does not involve all the operators of order 2, or where it involves one less invariant which is equal to 4 than H does. In the former case there are $k-1$ distinct G's. In the latter case there are

$k+2$, $k+1$, or k such G's. The number is $k+2$ when there is more than one invariant of each of values 2 and 4 in H. When there is only one invariant of one of these values and more than one of the other, the number of G's is $k+1$. Finally, there are only k such G's when H contains only one invariant of each of the values 2 and 4.

It may be added that in the study of all the possible non-abelian groups of order p^m which contain an abelian subgroup of order p^{m-1} it is especially desirable to know all of those groups which contain more than one such subgroup, as the other possible groups are distinct whenever they transform the abelian subgroup in different ways. When there is more than one abelian subgroup of order p^{m-1} in G, two such subgroups may be transformed differently by the remaining operators.

THE UNIVERSITY OF ILLINOIS,
September, 1906.

NOTE ON SYSTEMS OF IN- AND CIRCUMSCRIBED POLYGONS.

BY MISS S. F. RICHARDSON.

(Read before the American Mathematical Society, October 27, 1906.)

IN a paper read before the London Mathematical Society on March 12, 1874 (*Proceedings of the London Mathematical Society*, volume 5) Wolstenholme assumes two similar and similarly situated polygons of n sides, $ABC\cdots KLM$ and $abc\cdots klm$, and considers the conditions for an infinity of polygons which shall be inscribed in one of the similar polygons and circumscribed about the other.

He assumes that if ab meet AM in U and if am meet AB in V, then

$$AU/AM = AV/AB = k.$$

His solution finds $n-1$ values for k, that is, that there are $n-1$ points on AM, say, which may be taken as its intersection with ab, this point fully determining the polygon $abc\cdots klm$.

In particular he finds as the two solutions for the case $n=3$ that ab must divide AC in the ratio $\frac{1}{3}$ or in the ratio 1. In the first case the triangle abc becomes a point, the common