PROPERTIES OF THE SUBGROUPS OF AN ABELIAN PRIME POWER GROUP WHICH ARE CONJUGATE UNDER ITS GROUP OF ISOMORPHISMS*

BY

G. A. MILLER

1. Introduction

Two operators or two subgroups of a group will be called I-conjugate whenever they are conjugate under the group of isomorphisms of this group. It is well known that all the cyclic subgroups of highest order contained in any abelian group are I-conjugate. A necessary and sufficient condition that all the cyclic subgroups of any other order contained in an abelian group G of order p^m, p being a prime number, are I-conjugate is that all the invariants of G are equal to each other. When this condition is satisfied we shall prove, in particular, that the number of the subgroups of order p^α, $\alpha \leqq m$, contained in G is equal to the number of its subgroups of index p^α.

It is known that the ϕ-subgroup of G is composed of the pth power of every operator of G. The concept of ϕ-subgroup in connection with abelian groups can readily be extended by considering the characteristic subgroup of G composed of the p^αth power of every operator of G. This subgroup may be called the ϕ_α-subgroup of G. It is composed of all the operators of G which are found in each one of its subgroups of index p^α, and all the operators of highest order in a ϕ_α-subgroup of G are I-conjugate. In particular, the ϕ_α-subgroup generated by operators of order p is the fundamental characteristic subgroup of G.† In fact, when $p > 2$ the ϕ_α-subgroup which is generated by operators of order p^r is contained in every characteristic subgroup of G which involves operators of order p^r.

The quotient group of G corresponding to a ϕ_α-subgroup may be called a ϕ_α-quotient group. This quotient group is simply isomorphic with the subgroup of G generated by all its operators whose orders divide p^α. Hence the following:

Theorem. *The number of the subgroups of index p^α contained in any abelian*

* Presented to the Society, December 31, 1919.

† G. A. Miller, American Journal of Mathematics, vol. 27 (1905), p. 16.

group of order p^m *is equal to the number of the subgroups of index* p^α *contained in its subgroup composed of all its operators whose orders divide* p^α.

As a special case of this theorem it may be noted that the number of subgroups of index p contained in any abelian group is equal to the number of its subgroups of order p, since it is known that the number of the subgroups of index p contained in the abelian group of order p^m and of type $(1, 1, 1, \cdots)$ is equal to the number of its subgroups of order p. When $p^\alpha \leqq$ the smallest invariant of G it results from this theorem and the theorem proved in the following section that the number of subgroups of order p^α contained in G is equal to the number of its subgroups of index p^α.

Among the theorems of section 3 we may here note the one which establishes the fact that if h is the order of the largest cyclic subgroup of any abelian group and if d is a divisor of h then the number of sets of I-conjugate operators of order d contained in this group is the same as the number of its sets of I-conjugate operators of order h/d. In the special case when $d = 1$ this theorem reduces to the one according to which the operators of highest order in any abelian group are I-conjugate.

If the ϕ_α-subgroup of G is of type $(\alpha_1', \alpha_2', \cdots, \alpha_\lambda')$ and if the ϕ_α-quotient group is of type $(\alpha_1'', \alpha_2'', \cdots, \alpha_\lambda'')$; where some of these α's may be 0 then these α's may be so arranged that

$$\alpha_1' + \alpha_1'' = \alpha_1, \qquad \alpha_2' + \alpha_2'' = \alpha_2, \qquad \cdots, \qquad \alpha_\lambda' + \alpha_\lambda'' = \alpha_\lambda$$

where $(\alpha_1, \alpha_2, \cdots, \alpha_\lambda)$ represents the type of G. Two such subgroups of G may be said to be of *complementary types*. It should be noted that in general the type of a subgroup of an abelian group of order p^m does not determine completely the type of its complementary subgroup.

2. Abelian groups of order p^m all of whose invariants are equal to each other

When all the invariants of G are equal to each other all the operators of the same order contained in G are I-conjugate, and hence it results that the number of the characteristic subgroups of G is one less than the number of the different orders of the operators of G. A necessary and sufficient condition that two subgroups of G are I-conjugate is that they are of the same type, and any subgroup and the corresponding quotient group are of complementary types since every operator of such a G is a power of some operator of highest order contained in G.

The theorem noted in the Introduction as regards the equality between the number of subgroups of a given order and the number of the subgroups of the same index is clearly a corollary of the theorem that the number of the subgroups of a given type is the same as the number of the subgroups of the complementary type. To simplify a proof of this theorem we shall first consider the special case when all the invariants of G are equal to p.

Since the number of the subgroups of order p is known to be equal to the number of the subgroups of index p, and the type of one of the former subgroups is complementary to the type of one of the latter, the theorem in question will be proved for this special type of groups provided it is proved that the number of the subgroups of order p^α is equal to the number of the subgroups of index p^α whenever the number of the subgroups of order $p^{\alpha-1}$ is equal to the number of the subgroups of index $p^{\alpha-1}$, $m > \alpha > 1$.

As G is supposed to be of type $(1, 1, 1, \cdots)$ the number of its subgroups of order p^α which contain the same subgroup of order $p^{\alpha-1}$ is equal to the number of subgroups of order p in the abelian group of order $p^{m-\alpha+1}$ and of type $(1, 1, 1, \cdots)$. On the other hand, the number of the subgroups of index p^α which are contained in the same subgroup of index $p^{\alpha-1}$ is equal to the number of subgroups of index p in the abelian group of order $p^{m-\alpha+1}$ and of type $(1, 1, 1, \cdots)$. As this group is known to have exactly as many subgroups of order p as of index p it results that if we count each subgroup of order p^α as many times as it contains subgroups of order $p^{\alpha-1}$ we obtain the same sum as if we count each subgroup of index p^α as many times as it appears in some subgroup of index $p^{\alpha-1}$ since it was assumed that the number of subgroups of order $p^{\alpha-1}$ contained in G is equal to the number of its subgroups of index $p^{\alpha-1}$.

By the method of counting noted in the preceding paragraph each subgroup of order p^α is counted $(p^\alpha - 1)/(p - 1)$ times, and each subgroup of index p^α is counted the same number of times. Hence it results that the number of the subgroups of order p^α contained in G is equal to the number of the subgroups of order $p^{\alpha-1}$ multiplied by

$$\frac{p^{m-\alpha+1} - 1}{p^\alpha - 1}.$$

The number of the subgroups of index p^α may be found by multiplying the number of the subgroups of index $p^{\alpha-1}$ by the same factor. This completes the proof by induction of the theorem that in an abelian group of order p^m and of type $(1, 1, 1, \cdots)$ the number of the subgroups of a given type is equal to the number of the subgroups of the complementary type.

Having proved the theorem in question when G is of type $(1, 1, 1, \cdots)$ we proceed to give a proof of it when all the invariants of G are equal to p^{α_1}, $\alpha_1 > 1$. In this case the subgroups of order p^α contained in G can be of different types, but it may be assumed that the number of the subgroups of order $p^{\alpha-1}$ and of any possible type is equal to the number of the subgroups of index $p^{\alpha-1}$ and of the complementary type.

To find the number of the subgroups of order p^a and of a given type we may count each of these subgroups as many times as it contains subgroups of index p such that the orders of their independent generators differ from the orders of the independent generators of one of the former subgroups H only as regards the fact that one of the largest independent generators of H is replaced by one whose order is equal to the order of this generator divided by p. It should be noted that not all the subgroups of index p under H are thus counted but only those which are of the particular type just stated.

The number of these subgroups contained in H is $(p^\lambda - 1)/(p - 1)$, where λ is the number of the largest invariants of H, since all of these subgroups of index p contain the characteristic subgroup of H generated by all its operators which are not of highest order. This is also the number of the subgroups which contain a given subgroup of index p^a whose type is complementary to that of H and are of a type which is complementary to the type of one of the given subgroups of order p^{a-1}. Hence it results that if we count each subgroup which is of the same type as H as many times as it contains a subgroup of order p^{a-1} and of the given type we obtain the total number of subgroups which are I-conjugate with H multiplied by a given number k, and if we count each subgroup which is of a type complementary to that of H as many times as it is found in a subgroup of index p^{a-1} which is of a type complementary to the given subgroups of order p^{a-1} we obtain k times the total number of the subgroups whose type is complementary to that of H.

The number of the subgroups of G which have the same type as H and which contain a particular subgroup of order p^{a-1} and of the given type is $(p^{\gamma-\lambda+1} - p^{\gamma-\lambda'})/(p - 1)$, λ' being the number of the independent generators of H whose order is equal to or greater than the order of the largest independent generator of H divided by p and γ being the number of the independent generators of G. This results from the facts that all such subgroups are found in the characteristic subgroup of G which is generated by all the operators of G whose orders do not exceed the order of the largest operator of H and that the quotient group of this subgroup with respect to one of the given subgroups of order p^{a-1} contains $\gamma - \lambda + 1$ independent generators. The subgroups of order p in this quotient group which correspond to groups having only $\lambda - 1$ invariant which are equal to the largest invariant of H generate a group of order $p^{\gamma-\lambda'}$.

In a similar way it can be proved that the number of the subgroups whose type is complementary to that of H and which are found in a given subgroup of index p^{a-1} which is complementary to one of the given subgroups of order p^{a-1} is also $(p^{\gamma-\lambda+1} - p^{\gamma-\lambda'})/(p - 1)$. This can also be proved by finding the number of ways in which the independent generators of the former subgroup can be selected from the operators of the latter and by dividing this number by the number of ways in which these independent generators can be selected from the operators of the former subgroup.

From what precedes it follows that if the number of the subgroups of order $p^{\alpha-1}$ and of the given type is equal to the number of the subgroups of complementary type then if we count each subgroup of G which is simply isomorphic with H as many times as it contains a subgroup of order $p^{\alpha-1}$ and of the given type we get the same sum as when we count each of the subgroups of G whose type is complementary to the type of H as many times as it appears in a subgroup of index $p^{\alpha-1}$ whose type is complementary to that of the given subgroups of order $p^{\alpha-1}$. As by this process each of these two types of subgroups is counted the same number of times we have established the following:

THEOREM. *If all the invariants of an abelian group G of order p^m are equal to each other then the number of the subgroups of a given type contained in G is equal to the number of the subgroups which are of the complementary type.*

As an important corollary of this theorem it may be noted that *the number of the distinct subgroups of order p^α contained in any abelian group of order p^m whose invariants are equal to each other is the same as the number of its distinct subgroups of index p^α.*

3. Number of sets of I-conjugate operators of G

Let $p^{\alpha_1}, p^{\alpha_2}, \cdots, p^{\alpha_\lambda}$ represent all the different invariants of G arranged in descending order of magnitude. There may be more than one invariant of G which is equal to any one of these numbers but no two of these numbers are supposed to be equal to each other. Let $I_{\alpha_1-\beta}$, $\alpha_1 > \beta \geqq 0$, represent the substitution group according to which the operators of order $p^{\alpha_1-\beta}$ contained in G are permuted under I. It is known that I_{α_1} is transitive and that I_1 contains exactly λ transitive constituents. It was noted in the Introduction that one of the transitive constituents of $I_{\alpha_1-\beta}$ corresponds to the ϕ_β-subgroup of G.

To simplify the proof of the theorem that there are just as many transitive constituents in $I_{\alpha_1-\beta}$ as in I_β we shall first prove the special case of this theorem which relates to I_1 and I_{α_1-1}. It was noted above that I_1 contains λ transitive constituents and that the operators of highest order in the ϕ_1-subgroup of G correspond to a single transitive constituent of I_1. If we adjoin to the ϕ_1-subgroup of G all the smallest independent generators of G there results a group in which the operators of highest order correspond to two of the transitive constituents of I_1. The group thus obtained can be extended by the operators in a set of independent generators of G which are next to the lowest order and the resulting group will contain three sets of I-conjugate operators of order p^{α_1-1} whenever $\lambda > 2$, etc. Finally, the operators of highest order in the group generated by all the operators which are not of highest order in a set of independent generators of G, together with the pth powers of the operators of highest order in this set correspond to λ transitive constituents of I_1. This completes a proof of the special theorem that I_1 and I_{a_1-1} have the same number λ of transitive constituents.

Before proving the general theorem under consideration it may be desirable to indicate how the total number of the sets of I-conjugate operators of a given order p^r can be determined. This is evidently equivalent to the determination of the number of the transitive constituents of I_r and also of the number of the characteristic subgroups of G which are generated by operators of order p^r. The smallest of these transitive constituents of I_r, when, $p > 2$, corresponds to all the operators of order p^r contained in G which are powers of operators of order p^{a_1}. To the characteristic subgroup K_1 generated by these operators we adjoin a characteristic subgroup of G which satisfies the following two conditions: Its operators of largest order have the same order as the operators of the smallest order in K_1, and its order is as small as possible so as to contain operators not found in K_1. We thus obtain a characteristic subgroup whose operators correspond to two transitive constituents of I_r.

If the operators of lowest order in this extended characteristic subgroup do not include all the operators of the same order contained in G this process is repeated. Each repetition increases by one the number of I-conjugate operators in the characteristic subgroup thus extended. After the operators of lowest order in such a group include all the operators of the same order appearing in G we adjoin to K_1 the smallest characteristic subgroup of G generated by operators of next to the lowest order found in K_1 and involving operators not found in K_1. The characteristic subgroup K_2 thus constructed is first treated just like K_1 was treated to obtain successive characteristic subgroups, each involving one more set of I-conjugate operators of highest order than the preceding one. We then build K_3 on K_2 just as K_2 was obtained by extending K_1, etc.

This general method may be illustrated by finding the number of the I-conjugate operators of order p^3 in the abelian group of order p^{21} and of type $(6, 5, 4, 3, 2, 1)$. The subgroup K_1 is of order p^6 and may be extended three times, in order, by operators of order p. We thus obtain 4 sets of I-conjugate operators of order p^3. The group K_2 is of order p^8 and can be extended twice by operators of order p. We thus obtain 3 additional sets of I-conjugate operators of order p^3. The group K_3 is of order p^{10} and can be extended once by operators of order p while K_4 is of order p^{12}. As these groups contain together 3 additional sets of I-conjugate operators of order p^3 it results that in the characteristic subgroups which involve separately only one invariant which is equal to p^3 there are 10 sets of I-conjugate operators of order p^3.

When the characteristic subgroups which are generated by operators of order p^3 and contain two invariants which are equal to p^3 are considered we evidently have a repetition of a part of the preceding problem, and the number of additional sets of I-conjugate operators of order p^3 is 6. When the characteristic subgroups which are generated by operators of order p^3 involve three invariants which are equal to p^3 there are 3 additional sets of such I-conjugate operators and there is one additional set when there are four invariants which are equal to p^3. Hence the total number of transitive constituents in I_3 for the given group is $10 + 6 + 3 + 1 = 20$. This is also equal to the number of the characteristic subgroups which are generated by operators of order p^3.

Having given and illustrated a method by which the number of the sets of I-conjugate operators of order p^r can be found we proceed to prove that the number of the sets of I-conjugate operators of order $p^{\alpha_1 - r}$ is exactly the same. For this purpose it may evidently be assumed that $\alpha_1 \geqq 2r$. The proof is practically the same as the one given above. In the present case we begin with the subgroup generated by the p^r powers of the operators in a set of independent generators of G_1 and note that the operators of order $p^{\alpha_1 - r}$ contained in this subgroup constitute a single set of I-conjugate operators of G since they are separately generated by operators of order p^{α_1}. To obtain a subgroup which contains just two sets of I-conjugate operators of order $p^{\alpha_1 - r}$ we adjoin to this subgroup the p^{r-1} powers of the smallest independent generators of G, provided their order is at least equal to p^r. If their order is less than p^r we adjoin the smallest characteristic subgroup of G which is generated by operators of order p but is not found in the subgroup already constructed. This subgroup can be extended so as to obtain a subgroup containing one more set of I-conjugate operators just as in the preceding case, and hence it is clear that the number of sets of I-conjugate operators of order $p^{\alpha_1 - r}$ is exactly the same as the number of such sets of operators of order p^r.

In an abelian group whose order is not the power of a prime number the number of the sets of I-conjugate operators of a given order which is represented by operators of the group is equal to the product of the numbers of such sets for the prime power constituents of this order. Hence the method illustrated above enables one to determine directly the number of the different sets of I-conjugate operators of every order represented by the operators of the group. In particular, it results that if the largest order h of an operator of any abelian group is divisible by d the number of the different sets of its I-conjugate operators of order d is equal to the number of its different sets of I-conjugate operators of order h/d, as was noted in the Introduction.

It may be added that the present article extends along various lines the results obtained in an article by the present writer, published in volume 27 (1905), of the American Journal of Mathematics, page 15, under the title "Determination of all the characteristic subgroups of an abelian group." Each set of I-conjugate operators of a group generates a characteristic subgroup and every characteristic subgroup is composed of one or more than one complete set of I-conjugate operators. Hence the problem of determining the number of the characteristic subgroups of an abelian group is equivalent to the determination of the number of the transitive constituents in the group of isomorphisms of this abelian group.