I-CONJUGATE OPERATORS OF AN ABELIAN GROUP*

BY

G. A. MILLER

I. INTRODUCTION

Two operators of any group G are said to be I-conjugate if they correspond in at least one of the possible automorphisms of G. Every characteristic subgroup of G includes all the I-conjugates of each of its operators, and if a subgroup includes all the I-conjugates of its operators it is characteristic. In the present article it will be assumed that G is abelian. As two operators of any abelian group are I-conjugate if their prime power constituents have this property, and vice versa, it will only be necessary to consider the case when the order of G is of the form p^m, p being a prime number. Hence this will be done in what follows unless the contrary is stated.

Two fundamental questions in regard to the I-conjugate operators of G are: how many sets of I-conjugate operators are there in any abelian group, and how many operators are found in each of these sets? Both of these questions are answered in what follows, and the method for determining these numbers which is developed here seems to be as direct as possible. It is evident that every two I-conjugate operators are of the same order, and that a necessary and sufficient condition that every two operators of G which are of the same order be also I-conjugate is that all the invariants of G be equal to each other.

Two definitions of independent generators of G are in common use. According to one of these definitions the operators $s_1, s_2, \cdots, s_\lambda$ are called a set of independent generators of G whenever they satisfy the two conditions that they generate G and that no $\lambda - 1$ of them generate G. The number λ is known to be an invariant of G. According to the second definition, these λ operators must satisfy the additional condition that the subgroup generated by an arbitrary subset of them have only identity in common with the subgroup generated by the rest of these operators. According to the first definition, all the operators of G which do not appear in any one of the possible sets of independent generators of G constitute a subgroup of G known as its ϕ-subgroup, while these operators constitute such a subgroup according to the second definition when and only when the ratio of the largest invariant to the smallest invariant of G does not exceed p.

* Presented to the Society, December 30, 1920.

To distinguish between sets of independent generators satisfying the first, or also the second, of these definitions, the latter are called *reduced sets of independent generators*. The former sets of independent generators are usually the most convenient when only questions relating to subgroups are considered, while the latter are more convenient in the study of conjugacy. In the present article it will be assumed that the sets of independent generators under consideration are reduced sets unless the contrary is stated. It will be seen that all the operators of G which do not appear in any such set generate a subgroup which includes all the independent generators of G except those of highest order and those whose order is equal to this highest order divided by p, if any of the latter exist.

When G has independent generators of different orders, its independent generators which are of the same order are evidently I-conjugate and can be selected from a set of I-conjugate operators of G which has no operator in common with the group generated by the remaining independent generators of the set. The latter independent generators can usually be selected in a large number of different ways and the subgroups which such operators generate may differ, but none of the subgroups can involve an operator of the set of I-conjugate operators from which the former independent generators must be chosen.

The number of the subgroups of G which are separately generated by all the independent generators of G which are of the same fixed order in its various possible sets of independent generators can easily be determined. In fact, it is the quotient obtained by dividing the number of ways in which the independent generators of such a subgroup can be selected from the operators of G by the number of ways in which these generators can be selected from the operators of one of these subgroups. If p^α is the order of such an independent generator the totality of the operators of order p^β, $0 \leqq \beta \leqq \alpha$, contained in all of these subgroups constitutes a single set of I-conjugate operators of G. Hence the distinct operators in all of these subgroups constitute the operators of α I-conjugate sets of G excluding identity. Two such subgroups corresponding to different values of α can have only identity in common, and G is the direct product of an arbitrary set of subgroups such that one and only one of the subgroups of this set corresponds to a particular possible value of α.

II. I-REDUCED OPERATORS OF A GROUP

It has been noted that when G contains a set of independent generators composed of λ_1 operators of order p^{α_1}, λ_2 operators of order p^{α_2}, $\cdots$, λ_γ operators of order p^{α_γ}, so that

$$\lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \cdots + \lambda_\gamma \alpha_\gamma = m,$$

then the number of its sets of I-conjugate operators which are separately

powers of possible independent generators is $\alpha_1 + \alpha_2 + \cdots + \alpha_\gamma$, exclusive of identity. Each of these sets contains one and only one operator which satisfies both of the following conditions: It is the lowest possible power of an operator in the set of independent generators $s_1, s_2, \cdots, s_\lambda$ which appears in the former set, and this operator has the smallest possible subscripts. Such an operator will be called an *I-reduced operator* and hence each of the given sets of I-conjugate operators contains one and only one I-reduced operator, and this is a power of an independent generator of G.

In general, an I-reduced operator is defined as the single operator of a set of I-conjugate operators of G which satisfies the following conditions: It involves powers of the smallest possible number of constituents which are separately powers of the operators $s_1, s_2, \cdots, s_\lambda$ for the set of I-conjugate operators in which it is found, each of these constituents is raised to the lowest possible power, and the subscripts of operators of the set $s_1, s_2, \cdots s_\lambda$ of which these constituents are powers are as small as possible. A necessary and sufficient condition that an I-reduced operator involve powers of more than one of the operators $s_1, s_2, \cdots, s_\lambda$ is that all these powers be of different orders, and that the larger of two generators involved be raised to a higher power of p than the smaller, and this power have a larger order than the power of the smaller. In particular, no two of these constituents are powers of independent generators whose orders have a ratio which is less than p^2.

As each of the possible sets of I-conjugate operators of G is completely determined by the I-reduced operator which appears in the set, it results that the determination of the number of different sets of I-conjugate operators is equivalent to the determination of the possible number of different I-reduced operators. It should be noted that the number of I-reduced operators depends only upon the orders and the number of the different orders of the independent generators of G. That is, if G has more than one independent generator of the same order, the number of I-reduced operators of G is the same as that of the group having only one of these generators and only one generator whose order is equal to the order of every other independent generator of G.

To determine the number of operators of G which are I-conjugate with a given I-reduced operator T of G, it is convenient to call t-generators all the independent generators of G whose orders are equal to the orders of those independent generators whose powers appear in this I-reduced operator. The remaining independent generators of G will be called s-generators. Let $p^{\beta_1}, p^{\beta_2}, \cdots, p^{\beta_\theta}$ be the indices, in descending order of magnitude, of the various powers of t-generators which appear as constituents of T, and construct a subgroup of G whose independent generators are powers of s-generators which are determined as follows:

All the s-generators of G whose orders exceed the order of the largest

t-generator are raised to powers such that the common order of these powers is equal to that of the p^{β_1} power of this t-generator, and all the s-generators whose orders are smaller than the smallest t-generator are raised to the p^{β_θ} power. Each of the other s-generators of G is raised to the highest power whose index does not exceed the index of the power to which the next larger t-generator is raised to obtain a constituent of T and whose order is not less than the order of the power of the next lower t-generator which appears in T. The powers of the s-generators thus determined constitute a set of independent generators of the subgroup in question.

To obtain all the operators of the set of I-conjugate operators of T, we multiply all the operators of the subgroup noted in the preceding paragraph by the product of the operators of highest orders in the θ subgroups which are separately generated by the p^{β_1}, p^{β_2}, $\cdots$, p^{β_θ} powers respectively of the t-generators of the same order contained in G. As the invariants of each of these θ subgroups are equal to each other, these powers for any particular subgroup are evidently I-conjugate, but the powers for one subgroup are not I-conjugate with the powers in question contained in another of these θ subgroups. In particular, the number of operators in each set of I-conjugate operators of G besides identity is divisible by $p-1$, as results also directly from the fact that an automorphism of an abelian group can be obtained by letting each operator correspond to any given power of itself whose index is prime to the order of the group.

If the order of an abelian group is not a power of a prime number, the number of its sets of I-conjugate operators is evidently the product of the numbers of the sets of I-conjugate operators of its Sylow subgroups. In particular, it may be desirable to emphasize the theorem: *The number of sets of I-conjugate operators in any abelian group is equal to the product of the numbers of the I-reduced operators in its Sylow subgroups for a set of independent generators in which the order of each generator is a power of a prime number.* In this theorem, identity is included among the I-reduced operators of a Sylow subgroup.

For the purpose of illustrating the preceding developments, we shall consider the special abelian group of order p^{10} and of type (6, 3, 1). In addition to identity, the number of I-reduced operators involving a single constituent is 10, the number of those involving two constituents is 11, and the number involving three constituents is 2. Hence this group involves 24 sets of I-conjugate operators including identity. The numbers of I-conjugate operators in these 24 sets are as follows: $1, p-1, p^2-p, p^3-p^2, p^5-p^4, p^7-p^6, p^{10}-p^9, p^2-p, p^4-p^3, p^7-p^6, p^3-p^2, (p^2-p)(p-1), (p^3-p^2)(p-1), (p^3-p^2)(p-1), (p^4-p^3)(p-1), (p^4-p^3)(p-1), (p^5-p^4)(p-1), (p^5-p^4)(p-1), (p^7-p^6)(p-1), (p^7-p^6)(p-1),$

$(p^8-p^7)(p-1)$, $(p^4-p^3)(p-1)$, $(p^4-p^3)(p-1)^2$, $(p^5-p^4)(p-1)^2$. These numbers illustrate the obvious theorem that a necessary and sufficient condition that an operator of an abelian group of order p^m, $p>2$, having no two invariants which are equal to each other, be either a possible independent generator or a power of such a generator is that the number of its I-conjugates be not divisible by $(p-1)^2$.

This theorem is evidently a special case of the theorem that a necessary and sufficient condition that the I-reduced operator of a set of I-conjugate operators involve powers of α operators of a set of independent generators of G is that the number of operators in this set be divisible by $(p-1)^\alpha$ for a general value of p. It should be noted that the number of I-conjugate sets of operators of a group of order p^m depends on the type of this group, but is independent of the value of the prime number p, and that the theorem stated at the close of the preceding paragraph is not affected by the number of independent generators of the same order when G has a general value. For special given values of p, the theorem stated at the opening of the present paragraph is clearly not always valid.

III. Criteria for I-conjugate operators and for certain I-conjugate subgroups

It was noted in the preceding section that there is one and only one I-reduced operator in every complete set of I-conjugate operators of the abelian group G of order p^m, and that the number of constituents in terms of a fixed set of independent generators of G appearing in such an I-reduced operator can be determined from the number of operators involved in the set of I-conjugates to which this I-reduced operator belongs. A necessary and sufficient condition that two operators of G be I-conjugate is that they be I-conjugate with the same I-reduced operators. We proceed to develop another criterion for determining when two operators are I-conjugate.

The cyclic group generated by an I-reduced operator gives rise to a quotient group which is known to be simply isomorphic with a subgroup of G. The s-generators of G and all the t-generators of G with respect to this I-reduced operator except those whose powers actually appear in it can also be used as independent generators of the quotient group in question. To each of the latter t-generators, except the smallest one, there corresponds a generator of this quotient group whose order exceeds the order of all these t-generators whose order is less than that of the t-generator in question.

The quotient groups which correspond to two I-conjugate cyclic subgroups are evidently of the same type. To prove that, conversely, every two cyclic subgroups which give rise to quotient groups of the same type are I-conjugate, it should be noted that when these cyclic groups are replaced by those generated

by the I-reduced operators in the sets of I-conjugate operators to which their generators belong, their largest constituent groups with respect to the set of independent generators of G in question must be generated by the same power of independent generators of the same order, since, otherwise, in one quotient group the number of independent generators, beginning with the largest, whose orders coincide with those of G would differ from the number of the corresponding independent generators of the other quotient group.

If the generators of the cyclic groups in question involve powers of more than one t-generator of G, the second t-generator involved must again be the same for both of these cyclic groups, since the independent generators of the quotient group which corresponds to the first t-generator are of a larger order than the second t-generator, as was noted above. Moreover, the same power of this second t-generator must appear in a generator of each of the two cyclic subgroups in question. As this process may be continued until all the t-generators whose powers appear in the constituents of the cyclic subgroups under consideration have been exhausted, there results the following:

THEOREM. *A necessary and sufficient condition that two operators of any abelian group be I-conjugate is that the cyclic groups generated by these operators give rise to quotient groups which are of the same type.*

It results directly from the preceding theorem that the number of different sets of I-conjugate operators can be determined by counting the number of different types of quotient groups to which cyclic subgroups of G give rise. For instance, the cyclic subgroups of the abelian group of order p^4 and of type (3, 1) clearly give rise to quotient groups of the following types, and of no other types: (3, 1), (3), (2, 1), (2), (1, 1), (1). Hence this group has exactly six sets of I-conjugate operators, including identity. The number of operators in these sets is 1, $p^2 - p$, $p - 1$, $p(p-1)^2$, $p^2 - p$, $p^4 - p^3$, respectively. All of these operators are either possible independent generators or powers of such generators except those of the fourth set.

As a first step in a proof of the theorem that if two subgroups of the same type give rise to cyclic quotient groups they must be I-conjugate, it will be convenient to consider a necessary and sufficient condition that a subgroup H of G give rise to a cyclic quotient group. If G/H is cyclic, and if as many as possible of the operators of a set of independent generators of G are selected from the operators of H, the remaining operators of this set can be chosen as follows:

As one of the operators any operator s_1 of lowest order contained in a co-set corresponding to any operator of highest order in G/H may be selected. A necessary and sufficient condition that s_1 be the only operator of the set of independent generators in question which does not appear in H is that one of the operators of smallest order in every co-set corresponding to an operator

of G/H be a power of s_1. When this condition is not satisfied, find one of the largest operators of G/H such that a power of s_1 is not one of the smallest operators in the corresponding co-set. Let s_2 be any one of the smallest operators in such a co-set. It is evident that s_2 may then be chosen as a second operator of the set of independent generators in question.

If the powers of s_2 are not operators of lowest order in the co-sets with respect to H in which they appear, we select an operator s_3 of lowest order in the co-set which corresponds to the largest operator of G/H to which such an operator corresponds but is not an operator of lowest order in the co-set. This process is continued until an operator s_α is found such that its powers are operators of lowest order in all the co-sets with respect to H in which they appear. The operators $s_1, s_2, \cdots, s_\alpha$ are then the operators of the set of independent generators in question which do not appear in H. It may be noted that the ratio of the order of any one of these operators and the order of the one which follows it in this sub-set cannot be less than p^2.

For the independent generators of H which are not also independent generators of G we may choose the operators

$$s_1^{p^{\rho_1}} s_2, s_2^{p^{\rho_2}} s_3, \cdots, s_{\alpha-1}^{p^{\rho_{\alpha-1}}} s_\alpha, s_\alpha^{\rho_\alpha},$$

where $s_x^{p^{\rho_x}}$ $(x = 1, 2, \cdots, \alpha - 1)$ is the inverse of the lowest power of s_x which appears in a co-set with respect to H in which it is not an operator of lowest order, and $s_\alpha^{\rho_\alpha}$ is the lowest power of s_α which is found in H. The order of $s_x^{\rho_x}$ must exceed the order of s_{x+1}, since the latter is an operator of lowest order in the co-set in which the former appears and is an independent generator which cannot be replaced by an operator of H. Hence it follows that *a necessary and sufficient condition that a subgroup G give rise to a cyclic quotient group is that the α independent generators $(s_1, s_2, \cdots, s_\alpha)$ of G which cannot be selected from H can be so chosen that*

$$s_\alpha^{p^{\rho_\alpha}} \quad \text{and} \quad s_x^{p^{\rho_x}} s_{x+1} \qquad (x = 1, 2, \cdots, \alpha - 1)$$

are independent generators of H, where $s_x^{p^{\rho_x}}$ is of a larger order than s_{x+1} and $\rho_x > 0$. It should be noted that each of these independent generators of H is of a larger order than any of the independent generators of G whose powers appear in the succeeding independent generators of H.

By means of the theorem of the preceding paragraph, it is easy to find a necessary and sufficient condition that two subgroups H_1, H_2 of G which give rise to cyclic quotient groups be I-conjugate. It is evident that a necessary condition is that H_1 and H_2 be of the same type. To prove that this is also a sufficient condition, when it is assumed that both of the quotient groups G/H_1 and G/H_2 are cyclic, let $s_1, s_2, \cdots, s_\rho$ and $t_1, t_2, \cdots, t_\rho$ be two sets of independent generators of G which have been so chosen that as many as possible

of these operators are selected from those of H_1 and H_2 respectively. It results that the first operators of each of these sets, arranged in the descending order of magnitude, whose orders exceed the order of the corresponding reduced independent generator of H_1 and H_2, respectively, arranged similarly, must have the same order. The largest independent generator of H_1 which is not also an independent generator of G has the same order as the largest independent generator of H_2 which is not also an independent generator of G, since the order of this independent generator must exceed the order of all the other independent generators of G which are not also independent generators of H_1 or H_2. Hence it results that these independent generators of H_1 and H_2 may be regarded as products of powers of independent generators of G which are of the same order and independent generators of next to the highest order which are found in G but not in the H's.

Just as the operators of H_1 and H_2 which correspond to the largest independent generator of G which is not also an independent generator of H_1 or H_2 can be chosen from the operators of G as $s_1^{p^{\rho_1}} s_2$ was chosen, so the operators which correspond to the next to the largest independent generator of G which is not also an independent generator of H_1 or H_2 can be chosen in the same way as $s_2^{p^{\rho_2}} s_3$ was chosen, whenever not all the independent generators of G save one can be selected from the operators of H_1. Since these arguments apply to these successive independent generators, it results that *every two subgroups of G which are both of the same type and give rise to cyclic quotient groups are I-conjugate.*

If H_1 and H_2 are two subgroups of the same type which give rise to two quotient groups of the same type, it does not necessarily follow that H_1 and H_2 are I-conjugate, as may be seen by considering the group G of order p^9 and of type (5, 3, 1). If s_1, s_2, s_3 represent the three generators of G of orders p^5, p^3, and p respectively, and if $s_1^p s_2$, s_2^p and s_1^p, $s_2^p s_3$ are the independent generators of H_1 and H_2 respectively, it results that the two quotient groups G/H_1 and G/H_2 are of type (2, 1), and the two groups H_1, H_2 are of type (4, 2). The latter groups cannot be I-conjugate, since the operators of the highest order in the latter are powers of operators of highest order in G, but this is not the case as regards the operators of highest order of the former subgroup.

It may be noted that the sum of the number of independent generators of a subgroup of G plus the number of the independent generators of the quotient group corresponding to this subgroup is equal to the number of independent generators of G whose common order is p increased by a number which may vary from the number of independent generators of G whose orders exceed p to twice this number, but can have no other value. Both of the limiting values can evidently be actually attained, and the fact that this sum can have no other values results from the theorem that a quotient group of an abelian

group is always simply isomorphic with a subgroup of this group, and that the independent generators of a subgroup which gives rise to a cyclic quotient group can be selected as noted above.

It was noted above that when two subgroups of the same type give rise to cyclic quotient groups they must be I-conjugate, and when two cyclic subgroups give rise to quotient groups of the same type they are also I-conjugate. The other extreme cases are when two subgroups of the same type give rise to quotient groups of type $(1, 1, 1, \cdots)$ and when two subgroups of type $(1, 1, 1, \cdots)$ give rise to quotient groups of the same type. In each of these two cases the two subgroups in question are again I-conjugate. In the special case when a subgroup gives rise to a quotient group of type $(1, 1, 1, \cdots)$ which involves as many invariants as G itself, the subgroup is characteristic, being the ϕ-subgroup of G. In this special case, the subgroup is completely determined by the type of the quotient group to which it gives rise.

Every subgroup of G which gives rise to a quotient group of type $(1, 1, 1, \cdots)$ must include the ϕ-subgroup of G. If the ϕ-quotient group is of order p^α and a subgroup H gives rise to a quotient group of order p^β and of type $(1, 1, 1, \cdots)$, it results that exactly $\alpha - \beta$ of the independent generators of G are found in H, while the pth power of each of the other independent generators of G is found in this subgroup. From this it results directly that if two subgroups of the same type give rise to quotient groups of type $(1, 1, 1, \cdots)$ these subgroups must be I-conjugate. The number of the characteristic subgroups which give rise to quotient groups of type $(1, 1, 1, \cdots)$ is evidently equal to the number of the different orders of reduced independent generators of G. As every operator of order p found in G is a power of a possible independent generator of G, it results that when two subgroups of type $(1, 1, 1, \cdots)$ give rise to quotient groups of the same type their independent generators can be so chosen that they are powers of independent generators of G which are of the same orders. Hence these subgroups are I-conjugate.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.