RECIPROCAL SUBGROUPS OF AN ABELIAN GROUP.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society September 8, 1920.)

§ 1. *Introduction.* Every two subgroups of the group G which have the property that the product of their orders is equal to the order of G have been called *reciprocal subgroups* of G.* A group may have subgroups which have no reciprocals. For instance, the tetrahedral group contains subgroups of order 2 but it does not contain any subgroup of order 6. If a group is abelian, each of its subgroups is known to have at least one reciprocal subgroup. A necessary and sufficient condition that every subgroup of G have one and only one reciprocal is that G be cyclic.

Two invariant subgroups of G will be called *corresponding reciprocal subgroups* of G if each of them is simply isomorphic with the quotient group of G with respect to the other. One of the objects of the present paper is to prove that every subgroup of an abelian group has a corresponding reciprocal subgroup. All the subgroups in a complete set of conjugate subgroups under the group of isomorphisms of G, that is, all the subgroups in a set of I-conjugate subgroups of G, must evidently have the same reciprocal subgroups. Hence the theory of corresponding reciprocal subgroups of an abelian group establishes a correspondence between pairs of sets of I-conjugate subgroups. In what follows it will be assumed that G is abelian.

As G is the direct product of its Sylow subgroups when the order of G is not a power of a prime number p and as the number of I-conjugates of a subgroup of such a G is the product of the numbers of the I-conjugates of the Sylow subgroups of this subgroup it will be assumed in what follows that the order of G is of the form p^m and that G has λ_1 invariants which are separately equal to p^{m_1}, λ_2 invariants which are separately equal to p^{m_2}, $\cdots$, λ_γ invariants which are separately equal to p^{m_γ}. Hence

$$\lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_\gamma m_\gamma = m.$$

It will be convenient to assume that $m_1 > m_2 > \cdots > m_\gamma$.

* This BULLETIN, vol. 9 (1903), p. 541.

Since every subgroup of index p^r contained in G contains the p^rth power of every operator of G, these powers constitute the cross-cut of all the subgroups of index p^r. The quotient group Q_r of G with respect to this cross-cut is simply isomorphic with the characteristic subgroup of G composed of all the operators of G whose orders divide p^r. This characteristic subgroup and the given cross-cut are characteristic corresponding subgroups of G. That is, the subgroup composed of the p^rth power of every operator of G and the subgroup composed of all the operators of G whose orders divide p^r are two characteristic corresponding subgroups of G.

Hence there is a (1, 1) correspondence between the subgroups of G which give rise to quotient groups involving no operators whose orders exceed p^r and the subgroups Q_r. In particular, there is a (1, 1) correspondence between the subgroups of G which give rise to quotient groups of type (1, 1, 1, $\cdots$) and the subgroups of the characteristic subgroup of G generated by all its operators whose orders divide p. Since the latter is known to contain as many subgroups of order p^r as it contains subgroups of index p^r we may state the following theorem.

THEOREM 1. *In every abelian group of order p^m the number of the subgroups of order p^r and of type* (1, 1, 1, $\cdots$) *is equal to the number of the subgroups of index p^r which separately give rise to a quotient group of type* (1, 1, 1, $\cdots$).

In this theorem r has an arbitrary value from 1 to the number of the independent generators of the abelian group in question.

The subgroups of index p^r which separately give rise to a quotient group of type (1, 1, 1, $\cdots$) may be of various types. Hence the theorem stated near the end of the preceding paragraph relates to an enumeration in which no distinction is made between subgroups of somewhat different types. It should be noted that the present method is based on relative properties of subgroups whose largest operators are of a given order and subgroups which give rise to quotient groups involving operators of this order but of no larger order.

If two reciprocal subgroups of G are such that their cross-cut is the identity then the sum of an arbitrary set of independent generators of one of these subgroups and an arbitrary set of independent generators of the other is a set of independent generators of G. Any two such reciprocal sub-

groups are corresponding reciprocal subgroups. A necessary and sufficient condition that two reciprocal subgroups of an abelian group generate this group is that their cross-cut is the identity.

§ 2. *Form of the Number of Subgroups of Certain Types.* It is well known that the number of the subgroups of a given order contained in G is always of the form $1 + kp$. As the subgroups of the same order may be of various types it is of interest to inquire whether there is any general theorem relating to the number of the subgroups of the same type. It is easy to prove that whenever G contains subgroups of the same order but of different types then the number of the subgroups of each of these types except one is divisible by p. That is, every abelian group of order p^m contains one and only one type of subgroups of order p^α, $\alpha < m$, such that the number of the subgroups of this type is of the form $1 + kp$.

To prove this theorem it is only necessary to observe that the number of the subgroups of a given type can be obtained by dividing the number of ways in which a set of independent generators of such a subgroup can be selected from the operators of G by the number of ways in which such a set can be selected from the operators of this subgroup. The numerator and the denominator of this quotient are commonly represented as the product of binomial factors. The first term of such a factor represents the order of the group generated by all the operators of the order in question contained in the group under consideration, while the second term represents the order of the subgroup of the former group composed of its operators which cannot be used as independent generators after the preceding independent generators, if any, have been chosen.

In order that the number of subgroups of a given type be of the form $1 + kp$ it must therefore be necessary that the second term of a factor of the given numerator is always the same as the corresponding second term in the denominator. This implies that the subgroup in question must have the property that if it contains operators of different orders it must involve all the operators of G of the same orders with the possible exception that the operators of highest order found in this subgroup need not include all the operators of the same order found in G. Whenever at least one of these second terms in

the numerator is larger than the corresponding second term in the denominator the number of subgroups is clearly divisible by p. Hence the following theorem has been established.

THEOREM 2. *Whenever an abelian group of order p^m contains subgroups of the same order but of different types then the number of the subgroups of one and of only one of these types is of the form $1 + kp$. The number of the subgroups of each of the other of these types is divisible by p.*

While G contains one and only one type of subgroups of each order which divides p^m such that the number of its subgroups of this type is of the form $1 + kp$ it may contain one or more than one type of subgroups of a given order such that the number of the subgroups of this type is a power of p. It is not difficult to determine a necessary and sufficient condition that the number of the subgroups of a given type be of the form p^α. In fact, one such condition is that each binomial factor of the numerator of the given quotient which represents the number of these subgroups is the product of a power of p by the corresponding factor in the denominator of this quotient. Hence we have the following theorem.

THEOREM 3. *A necessary and sufficient condition that the number of the subgroups of a given type contained in an abelian group G of order p^m be a power of p is that the number of its independent generators of each order increased by the number of its larger independent generators in this set be equal to the number of the independent generators of G whose orders are not less than this order.*

In the special case when there is only one subgroup of a given type the number of these subgroups may be said to be both a power of p and also of the form $1 + kp$. Hence in this special case the conditions involved in the two theorems stated above coincide. In order to illustrate the conditions under which the number of subgroups of a given type is a power of p we shall consider the special case when G is of type $(1, 2, 3, \cdots, m')$. To every combination of one or more of the numbers $1, 2, 3, \cdots, m'$ there corresponds one and only one such type, except the combination which involves all of these numbers. Hence this G contains $2^{m'} - 2$ different types of subgroups besides the identity such that the number of the subgroups of each of these types is a power of p. This is also the number of such types when G has equal invariants but when its distinct invariants are $p, p^2, p^3, \cdots, p^{m'}$.

In general, when the different invariants of G are p^{m_1}, p^{m_2}, $\cdots$, p^{m_λ}, it is not difficult to find the number of the different types of subgroups such that the number of the subgroups of each of these types is a power of p. In every one of the possible combinations of numbers $m_1, m_2, \cdots, m_\lambda$, each of these numbers may be replaced by every smaller integer which exceeds the one which follows it in this set. The sum of the sets thus obtained is the required number. In particular when G is of type $(m-1, 1)$ the number of such types of subgroups besides the identity is $2(m-2)$, and when all the invariants of G are equal to $p^{m'}$ this number is $m'-1$.

§ 3. *Quotient Groups and their Corresponding Subgroups.* It is well known that every possible quotient group of any abelian group is simply isomorphic with at least one subgroup of this abelian group, but two simply isomorphic subgroups of G do not always give rise to simply isomorphic quotient groups of G. Hence the question arises whether it is possible to associate with an arbitrary subgroup H_1 of G another subgroup H_2 of G such that G/H_1 is simply isomorphic with H_2 and G/H_2 is simply isomorphic with H_1, that is, whether for every subgroup of G there is at least one corresponding reciprocal subgroup.

For the sake of simplicity it will first be assumed that G/H_1 is cyclic, and it will be useful to note the following three possible cases: In the first case at least one operator in the co-set of G which corresponds to a generator of G/H_1 is of the same order as this generator. In the second case the ratios of the order of the smallest operators in a co-set and the order of the corresponding operator in G/H_1 are equal to the same number greater than unity for all the co-sets, excluding the co-set which corresponds to the identity in G/H_1. In the third case, the ratios of these orders are equal to $\rho > 1$ distinct numbers. The significance of conditions which are satisfied in these three cases can easily be determined and may be formulated as follows:

In the first case, any set of independent generators of H_1 together with an arbitrary operator of lowest order in a co-set corresponding to a generator of G/H_1 constitutes a set of independent generators of G. Conversely, whenever a set of independent generators of G can be so chosen that all of them except one generate H_1 then this case will present itself. In this case it is evident that H_1 and the cyclic subgroup gener-

ated by the remaining independent generator of G are corresponding reciprocal subgroups.

The second case implies that a set of independent generators of G can be so selected that all except one of them are independent generators of H_1 while the remaining independent generator of H_1 is a power of the remaining independent generator of G. This generator s is an arbitrary operator of lowest order in a co-set corresponding to a generator of G/H_1. Conversely, whenever a set of independent generators can be so selected that all except one of them are found in H_1 but do not generate H_1, then this second case will present itself. The cyclic subgroup of G which constitutes a corresponding reciprocal subgroup of H_1 is generated by the power of s which is simple isomorphic with G/H_1. It should be noted that the group generated by this power s' does not have only the identity in common with H_1; in fact it may be contained in H_1.

In the third case, the largest number of operators of any set of independent generators of G that can be selected from the operators of H_1 is ρ less than the total number of the independent generators of G, and the ratio of the orders of any two of these ρ generators cannot be less than p^2. On the other hand, whenever the ratio of the orders of any two of ρ generators of G is at least p^2 it is possible to find such a subgroup H_1. In fact, for the independent generators of H_1 we may take the independent generators of G exclusive of these ρ generators, plus the pth power of the largest of these ρ generators multiplied by the next in size, plus the pth power of this second multiplied by the next following in order of magnitude, $\cdots$, plus the pth power of the next to the last of these ρ operators multiplied by the last one. Hence we have the following theorem.

THEOREM 4. *If G is any abelian group of order p^m and ρ is the largest number of operators belonging to a set of independent generators of G and satisfying the condition that the ratio of the orders of any two of these ρ operators is not less than p^2, then G contains a subgroup H_1 which gives rise to a cyclic quotient group and satisfies the condition that at least ρ of the operators of every possible set of independent generators of G are not found in H_1.*

The main element of interest connected with this theorem is the fact that the lowest operators of G which correspond to the various operators of a cyclic quotient group G/H_1 together with the order of this quotient group determine completely

the set of I-conjugate subgroups to which H_1 belongs as well as the set of I-conjugate subgroups of G to which G/H_1 must correspond in order that H_1 and G/H_1 may be corresponding reciprocal subgroups. The ρ or $\rho - 1$ independent generators of H_1 which are not also independent generators of G can be obtained as follows.

First select the ρ independent generators of G $s_1, s_2, \cdots, s_\rho$ which are not contained in H_1 by noting that the first of these generators is any one of the operators of lowest order in the co-set of G which corresponds to a generator of G/H_1. The second is any operator of lowest order in the first lower co-set in which a power of s_1 is not an operator of lowest order. The third is any operator of lowest order in the next lower co-set in which a power of s_2 is not an operator of lowest order. . . . The last is any operator of lowest order in the highest co-set in which a power of $s_{\rho-1}$ is not an operator of lowest order. The independent generators of H_1 in question are then the product of s_2 into the inverse of the power of s_1 which occurs in the same co-set as s_2, the product of s_3 into the inverse of the power of s_2 which occurs in the same co-set as s_3, $\cdots$, the product of s_ρ by x the inverse of the power of $s_{\rho-1}$ which appears in the same co-set is s_ρ, the power of s_ρ which appears in H_1 whenever this power is not equal to the identity.

The cyclic subgroup of G which corresponds to G/H_1 may be obtained as follows: Let $s_1', s_2', \cdots, s_\rho'$ represent the powers of $s_1, s_2, \cdots, s_\rho$ respectively such that these powers are of the same orders as the operators of G/H_1 which correspond to $s_1, s_2, \cdots, s_\rho$ respectively. The product $s_1', s_2', \cdots, s_\rho'$ generates a cyclic subgroup H_1' which is simply isomorphic with G/H_1 and G/H_1' is also simply isomorphic with H_1.

When G/H_1 is non-cyclic it is the direct product of cyclic groups and the preceding arguments apply to these separate cyclic groups. At least one independent generator of G corresponds to each of these cyclic groups. Hence it results that in this case H_1 has again a corresponding reciprocal subgroup, and we have established the following theorem.

THEOREM 5. *Every subgroup of an abelian group has at least one corresponding reciprocal subgroup.*

THE UNIVERSITY OF ILLINOIS.