INVERSE CORRESPONDENCES IN AUTOMORPHISMS OF ABELIAN GROUPS*

BY G. A. MILLER

The totality of the operators which correspond to their inverses in an automorphism of an abelian group G obviously constitutes a subgroup of G. It is well known that G cannot contain any characteristic operator besides the identity unless this operator is of order 2, and that it cannot contain more than one characteristic operator of this order. Hence it results that whenever G contains any characteristic operator besides the identity this operator must appear in every subgroup which is composed of all the operators of G which correspond to their inverses in a given automorphism of G. We proceed to prove that a necessary and sufficient condition that an automorphism of G can be established such that all the operators of a given subgroup H correspond to their inverses, while no other operator of G satisfies this condition, is that H involves all the characteristic operators of G. In particular, when G involves no characteristic operator besides the identity, it is possible to establish an automorphism of G such that all the operators of an arbitrary subgroup correspond to their inverses, while no other operator of G has this property.

When G is of order p^m, p being a prime number, and of type $(1, 1, 1, \cdots)$ it is well known that all of its operators besides the identity can be transformed cyclically and that none of its subgroups of order p is transformed into itself under such a transformation whenever $m > 1$. Moreover, when all the operators of G are arranged in co-sets with respect to H, where each of the operators of H corresponds to its inverse, then either all the operators of a co-set correspond to their inverses in the same automorphism or none of these operators has this property. Hence the theorem under consideration is obviously true when G is of order p^m and of type $(1, 1, 1, \cdots)$. Moreover, it results from the fact that an abelian group contains only one

---

* Presented to the Society, December 30, 1929.

Sylow subgroup of a given order that we may confine our attention to the case when the order of G is p^m in the proof of this theorem. We therefore assume that this condition is satisfied and that H is any subgroup of G which involves all the characteristic operators of G. If all the operators of G which are not in H are included in co-sets of G with respect to H, it is clear that these co-sets can be so ordered that each of the first k_1 involves a power of one independent generator of G, and none of the remaining ones has this property, while each of those of the next k_2 involves either a power of a second independent generator or the product of such a power and a power of the first independent generator, and none of the remaining ones has this property, etc.

We may now suppose that an automorphism of G has been established in which all the operators of H correspond to their inverses. When $p > 2$ it is clear that this automorphism can be extended so that no power of the first independent generator corresponds to its inverse except its powers which are in H. Similarly, no power of the second independent generator except its powers contained in H needs to correspond to its inverse in such an automorphism. As this process may be continued until the operators of G have been exhausted, it results that no operator of G except those of H corresponds to its inverse in the resulting automorphism. When $p = 2$ and G involves only one independent generator of highest order, H must involve the operator of order 2 which is a power of this generator, and we may evidently proceed as before except that the following independent generators are replaced by their products into this one when this is used as the first independent generator in the given process and the operator of order 2 which is a power of such an independent generator is not in the earlier co-sets. When this operator is in an earlier co-set no modification is necessary. Hence, we have established the following theorem.

THEOREM 1. *A necessary and sufficient condition that the operators of a given subgroup of an abelian group may correspond to their inverses in an automorphism of this group in which no other operator corresponds to its inverse is that this subgroup involves all the characteristic operators of the group.*

When G is a cyclic group of order p^m, $m > 1$, and all the

operators of its subgroup of order p^α correspond to their inverses, while no other operator has this property, it is very easy to see that the order of this automorphism is $2p$ whenever $\alpha = m - 1$ and p is odd, and that there are $p - 1$ such automorphisms of G, since each of the remaining operators can correspond to its inverse multiplied by an operator of order p contained in G in such an automorphism. When $p = 2$ there is only one such automorphism and its order is 2. The latter corresponds to the case when every operator of G is transformed into its $2^{m-1} - 1$ power. In general, when p is odd the automorphisms in which exactly p^α operators correspond to their inverses, $\alpha > 0$, are of order $2p^{m-\alpha}$, since in the square of such an automorphism exactly p^α operators correspond to themselves. When $p = 2$ and $1 < \alpha < m - 1$ these automorphisms are of order $2^{m-\alpha}$, since in the square of such an automorphism exactly $2^{\alpha+1}$ of the operators correspond to themselves. Hence we have established the following theorem.

THEOREM 2. *If exactly p^α, $\alpha > 0$, of the operators of a cyclic group of order p^m correspond to their inverses in an automorphism of this group, then this automorphism is of order $2p^{m-\alpha}$ whenever p is an odd prime number and also when $p = 2$ and $m = \alpha$. When $p = 2$ and $1 < \alpha < m$ this automorphism is of order $2^{m-\alpha}$, while it may have any order from 1 to 2^{m-2} when $\alpha = 1$.*

By means of this theorem it is easy to determine the order, or the possible orders, of the automorphisms of any cyclic group G in which the operators of a given subgroup H correspond to their inverses. If the order of H is divisible by all the odd prime factors of the order of G, then the order of each of these automorphisms is equal to a power of 2 into the largest odd factor of the index of H under G. When the order of G is odd this power of 2 is 2, and when the order of H is divisible by 4 but not by the highest power of 2 which divides the order of G, then this power of 2 is equal to the highest power of 2 which divides the index of H under G. When the order of H is not divisible by some prime factor which divides the order of G, then the order of the corresponding automorphisms may be the product of the order of any operator in the group of isomorphisms of the Sylow subgroup of G whose order is a power of this prime factor and the order as determined above. A

necessary and sufficient condition that there is only one automorphism in which all the operators of a proper subgroup of G correspond to their inverses, while no other operator of G has this property, is that this subgroup is of index 2 and involves an operator of order 2.

In order to determine the number of the automorphisms whose orders were determined above it may first be noted that when the order of G is of the form p^m and the order of H is p^α, $\alpha > 0$, the number of the possible automorphisms is $p^{m-\alpha} - p^{m-\alpha-1}$, since a generator of G must correspond to its inverse multiplied by an operator of order $p^{m-\alpha}$ in such an automorphism and all such products will obviously give rise to such an automorphism. This results also from the following theorem.

THEOREM 3. *A necessary and sufficient condition that an automorphism of the cyclic group of order* p^m, *p being an odd prime number, is of order* $2p^\beta$ *is that* $p^{m-\beta}$ *of its operators correspond to their inverses under this automorphism.*

A proof of this theorem results almost directly from the fact that the square of such an automorphism is of order p^β and hence leaves invariant $p^{m-\beta}$ of the operators of G. The corresponding theorem when $p = 2$ is somewhat less elegant since we have to restrict it by saying that when the operators of order 4 in an automorphism of order 2^α of a cyclic group of order 2^m correspond to their inverses then exactly $2^{m-\alpha}$ of the operators of this cyclic group must correspond to their inverses in this automorphism whenever $\alpha > 1$. When $\alpha = 1$ this number is either 2^{m-1} or 2^m.

Since all the commutators which arise from an automorphism of order 2 of any group whatever correspond to their inverses under this automorphism, it results that in every automorphism of order 2 of an abelian group the number of the operators which correspond to their inverses is a divisor of the product of the order of the group K generated by the operators of order 2 which correspond to themselves under this automorphism and the order of the corresponding commutator subgroup. It is also a multiple of the order of K and the order of the quotient group of this commutator subgroup with respect to its cross-cut with the subgroup composed of the operators which correspond

to themselves under this automorphism. Moreover, it is possible to construct a group of order 2^m, where m is any given number, which admits an automorphism of order 2 in which the number of inverse correspondences is an arbitrary number which satisfies these two conditions and the order of K is any divisor of 2^m. In particular, *the number of inverse correspondences under an automorphism of order 2 of any abelian group of odd order is always equal to the order of the corresponding commutator subgroup.* In fact, in an automorphism of order 2 of any group whatsoever of odd order a necessary and sufficient condition that an operator corresponds to its inverse is that it is a commutator under this automorphism, but these commutators do not necessarily constitute a group when the given group of odd order is non-abelian.

THE UNIVERSITY OF ILLINOIS

THE FOURTH POSTULATES OF
RIESZ AND HAUSDORFF*

BY ORRIN FRINK JR.

A question which has remained unanswered for some time is whether every space which satisfies the four postulates of Riesz for points of accumulation and the additional postulate that every derived set is closed, is necessarily a Hausdorff space. A paper on this subject was recently presented to the American Mathematical Society.† I have succeeded in constructing an example, given below, which shows that the answer is in the negative.

A good discussion of the two postulate systems of Riesz and Hausdorff may be found in Fréchet's recent Borel monograph, *Les Espaces Abstraits.* Although Hausdorff's postulates are in terms of neighborhoods and those of Riesz concern the accumulation points directly, there is almost a complete parallelism between them, provided we add to Riesz's four, as Fréchet does, a fifth postulate that every derived set is closed. The only

---