AUTOMORPHISMS OF ORDER TWO*

BY

G. A. MILLER

§ 1. *Introduction.*

If an operator t transforms a group G into itself without being commutative with each operator of G, and if t^2 is commutative with each operator of G, then t is said to transform the operators of G according to an automorphism of order two. Moreover, every automorphism of G which is of order 2 may be obtained by transforming G by operators having the given properties of t.† Let s be any operator of G and assume that

$$t^{-1}st = s_1 s, \qquad t^{-1}s_1 t = s_2 s_1 .$$

Since t^2 is commutative with every operator of G it results that

$$t^{-1}s_1 st = s_2 s_1^2 s = s, \qquad \text{or} \qquad s_2 s_1 = s_1^{-1} = t^{-1}s_1 t .$$

That is, *in every automorphism of order* 2 *some operator besides the identity must correspond to its inverse.* It also results that *the necessary and sufficient condition that an automorphism shall be of order* 2 *is that every commutator arising from the automorphism corresponds to its inverse under the automorphism.*

It is well known that automorphisms play a fundamental rôle in many problems in group theory, but little has been done toward a general theory of automorphisms. Even the automorphisms of order 2 present many difficulties at the present stage of development of group theory. Such a fundamental question as whether every group admits automorphisms of order 2 has not yet been answered. When G is an abelian group whose order exceeds 2 it clearly admits at least one automorphism of order 2.

The main results of the present paper relate to the case when G is abelian. In § 4 a few results are obtained which relate also to non-abelian groups, and the final theorem is an extension of results coming under the heading of the present paper.

---

* Presented to the Society (Chicago), April 9, 1909.

† FROBENIUS, Berliner Sitzungsberichte, 1895, p. 185.

§ 2. *Abelian groups of odd order.*

When G is an abelian group of odd order the identity is the only commutator arising from t and invariant under t. All the commutators which arise from transforming G by t constitute a group H, and to each operator of the quotient group $G/H = H'$ there corresponds one and only one operator of G which is commutative with t. The independent generators of G may be selected from H and these invariant operators under t. Hence the theorem: *The independent generators of an abelian group of odd order may be so chosen that in any given automorphism of order* 2 *each of these generators corresponds either to itself or to its inverse.* In particular, if an operator of order 2 transforms into itself an abelian group of odd order, it is possible to select the independent generators of this group in such a manner that each of them is transformed either into itself or into its inverse.

If a set of independent generators of G is so selected that the order of each of them is a power of a prime, every other possible set of such independent generators may be placed in a (1, 1) correspondence with this set. Hence it is easy to find the number of sets of conjugate operators of order 2 in the group of isomorphisms (I) of G. This may be accomplished as follows: Represent all the independent generators, which have been selected in the given manner, by letters in such a way that the generators of the same order are represented by the same letter and the generators of different orders by different letters. Form all the possible combinations of these letters, taking one, two, three, etc., at a time. The number of these combinations is the number of distinct sets of conjugate operators of order 2 in I. In particular, when G is of order p^α and of type $(1, 1, 1, \cdots)$ the number of complete sets of conjugate operators of order 2 in I is α.

By means of the results obtained in the preceding paragraph it is easy to determine the number of possible groups of order $2(2n+1)$ involving a given abelian subgroup of order $2n+1$. In fact, the number of these groups is exactly one more than the number of complete sets of conjugate operators of order 2 in the I of the abelian group of order $2n+1$. In particular, there are exactly $\alpha + 1$ groups of order $2p^{\alpha m}$ involving the abelian group of order $p^{\alpha m}$ and of type $(m, m, m, \cdots)$. Since the group of isomorphisms of a Sylow subgroup of G involves just one invariant operator of order 2,* *the total number of invariant operators of order* 2 *in* I *is* $2^\lambda - 1$, λ *being equal to the number of distinct Sylow subgroups in* G.

For the purpose of determining the total number of operators of order 2 in I it is convenient to observe that the group of isomorphisms of any abelian group is the direct product of the groups of isomorphisms of its Sylow sub-

*Transactions of the American Mathematical Society, vol. 2 (1901), p. 260.

groups. If $m_1, m_2, m_3, \cdots$ represent the numbers of operators of order 2 in the groups of isomorphisms of the various Sylow subgroups of G, the number of operators of order 2 in I is $(m_1+1)(m_2+1)(m_3+1)\cdots-1$. Hence we may confine our attention to the determination of the number of operators of order 2 in the group of isomorphisms of an abelian group (P) of order p^m, p being an odd prime. When P is cyclic its group of isomorphisms involves only one operator of order 2, viz., the invariant operator of this order, corresponding to the isomorphism in which every operator of P corresponds to its inverse. In all other cases this group of isomorphisms involves non-invariant operators of order 2 and the number of distinct operators in a complete set of conjugates is evidently equal to the number of conjugates under I of the corresponding pair of subgroups H, H'.

In general, H, H' are any two independent subgroups of G whose product equals G. Hence the number of operators of order 2 in I is equal to the number of pairs of independent generating subgroups contained in G, when H, H' and H', H are regarded as distinct pairs, and H differs from the identity while H' may be the identity. This number is clearly equal to the sum of the quotients obtained by dividing successively the order of I by the products of the orders of the groups of isomorphisms of H, H' when H, H' represent successively all the possible types of pairs of independent subgroups (except that H is not the identity) contained in G. When H is the direct product of Sylow subgroups, the corresponding quotient is equal to unity and vice versa. Hence this is another way of seeing that the number of invariant operators of order 2 in I is equal to $2^\lambda - 1$, λ being the number of Sylow subgroups in G. Some of these results may be expressed in a convenient form as follows: *The number of operators of order* 2 *in the group of isomorphisms* (I) *of an abelian group* (G) *of odd order is equal to the sum of the quotients obtained by dividing successively the order of* I *by the products of the orders of the groups of isomorphisms of all the possible pairs of independent generating subgroups* H, H' *of* G *such that* H *is not of the same type in two pairs and that* H *is not the identity. Each of these separate quotients represents the number of operators of order* 2 *in a complete set of conjugates under* I.

To illustrate this theorem we shall employ it to determine the number of operators of order 2 in the well known group of isomorphisms of the abelian group of order $p^3 (p>2)$ and of type $(1,1,1)$. The order of I is evidently $p^3(p^3-1)(p^2-1)(p-1)$, and H, H' are of one of the following three types (1), $(1,1)$; $(1,1)$, (1); $(1,1,1)$, (0). The number of operators of order 2 in I is therefore equal to the sum of the following three quotients:

$$p^2(p^2+p+1),\ p^2(p^2+p+1),\ 1.$$

Hence this I involves two sets of $p^2(p^2+p+1)$ conjugate operators of order

2, and, in addition to this, it involves the operator of order 2 which transforms every operator of G into its inverse. It may be added that H, H' are necessarily products of Sylow groups whenever G is cyclic. This establishes contact between the given theorem and the well known result that the group of isomorphisms of a cyclic group is abelian. As the type of H' is completely determined by that of H, we may confine our attention to the latter in determining the number of sets of conjugate operators of order 2 under I.

§ 3. *Abelian groups of even order.*

When the order of G is the double of an odd number its group of isomorphisms is the same as if its order were this odd number. This is a special case of the theorem that the group of isomorphisms of G is the direct product of the groups of isomorphisms of its Sylow subgroup. Hence we may confine our attention to the case when the order of G is of the form 2^m. This case presents much greater difficulties than the one considered above. As every non-cyclic abelian group of order 2^m is the direct product of abelian groups whose invariants are equal to each other, we shall generally confine our attention to the determination of automorphisms of order 2 in such an abelian group. Throughout the rest of this section it will be assumed therefore that the order of G is 2^m and that all the invariants of G are equal unless the contrary is stated.

Representing the commutator subgroup of G by H, as was done in the preceding section, it is easy to prove that each of the independent generators of H must be of order 2, $2^{\alpha-1}$, or 2^α, when 2^α $(\alpha > 1)$ is the common order of the independent generators of G. In fact, since each operator of H is transformed into its inverse by t and since each operator of G is generated by an operator of order 2^α contained in G, an operator (s) of H, whose order exceeds 2, must be generated by an operator of order 2^α which generates only two operators that are commutative with t. This generator of s is transformed by t into itself multiplied by an operator of order $2^{\alpha-1}$, since $t^{-1}st = s^{-2}s$. As this operator of order $2^{\alpha-1}$ generates s^2, it results that *the square of every operator of H whose order exceeds 2 is generated by an operator of order $2^{\alpha-1}$ which is contained in H.* This proves that *the independent generators of H whose orders are divisible by $2^{\alpha-1}$ generate the squares of all the operators of H whose orders exceed* 2. Hence there are three cases to consider: 1) When all the operators of H except the identity are of order 2. 2) When H involves operators of order $2^{\alpha-1}$ but none of order 2^α. 3) When H involves operators of order 2^α. These three cases will be considered in the given order.

When H involves no operator of order 4, the order of H must divide 2^d, $d = m/\alpha$. The number of automorphisms of order 2, when the order of H is equal to 2^d, is equal to the order of the group of isomorphisms of H. In gen-

eral, when the order of H is 2^{d-l}, $l < d$, the number of these automorphisms is equal to the order of the group of isomorphisms of H multiplied by the product of the number of the subgroups of order 2^l in the group generated by all the operators of order 2 in G and the number of subgroups of order $2^{\alpha l}$ and of type $(\alpha, \alpha, \alpha, \cdots)$ contained in G. As the numbers of these subgroups are well known,* the problem of determining all the automorphisms of order 2 that arise in the given manner is completely solved. Hence the theorem: *If G is an abelian group of order $2^{d\alpha}$ and of type $(\alpha, \alpha, \alpha, \cdots)$, $\alpha > 1$, the number of automorphisms of order 2 which give rise only to commutators of order 2 is equal to the sum of the products obtained by multiplying the order of the group of isomorphisms of the abelian group of order 2^{d-l} and of type $(1, 1, 1, \cdots)$ by the product of the number of the subgroups of order 2^l and of type $(1, 1, 1, \cdots)$, and the number of subgroups of order $2^{\alpha l}$ and type $(\alpha, \alpha, \alpha, \cdots)$ contained in G, for every value of $l = 0, 1, \cdots, d-1$.*

When $\alpha = 1$, both G and H are of type $(1, 1, 1, \cdots)$ and hence each operator of H is commutative with t. From this it follows that the number of independent generators of H is equal to or less than half the number of these generators in G. It is also evident that the number of sets of conjugate operators of order 2 in I is equal to the number of possible orders of H; i. e., it is equal to the largest integer which does not exceed $d/2$. If the order of H is 2^λ the number of operators of H which are commutative with t is $2^{d-\lambda}$ and the number of operators of I which are conjugate with an operator corresponding to such an H is clearly equal to the product of the following three numbers: 1) The number of subgroups of order $2^{d-\lambda}$ in G. 2) The number of subgroups of order 2^λ in such a subgroup of order $2^{d-\lambda}$. 3) The order of the group of isomorphisms of H. The total number of operators of order 2 in the group of isomorphisms of the abelian group of order 2^d and of type $(1, 1, 1, \cdots)$ may therefore be found by addition of these products for every value of λ from 1 to the largest integer which does not exceed $d/2$.† For instance, the group of isomorphisms of the abelian group of order 2^4 and of type $(1, 1, 1, 1)$ contains two sets of conjugate operators of order 2 involving respectively 105 and 210 operators, as may easily be verified, since this group of isomorphisms is the alternating group of degree 8.

The simplest case in which H involves operators of order $2^{\alpha-1}$ is that in which every operator of G corresponds to its inverse. In this case it is evident that H is the direct product of d cyclic groups of order $2^{\alpha-1}$ and that the corresponding operator of order 2 in I is invariant. When $\alpha = 2$, this is included in the preceding two paragraphs. Hence we may assume $\alpha > 2$. Since the given automorphism corresponds to an invariant operator of order 2 in I, it

*Cf. Annals of Mathematics, ser. 2, vol. 6 (1904), p. 5.

†Bulletin of the American Mathematical Society, vol. 8 (1902), p. 391.

may be followed by each one of the group of automorphisms giving rise to commutators of order 2 only. If it is followed by any other automorphism G must involve invariant operators of order 4 under the automorphism, since each commutator arising from the automorphism corresponds to its inverse in the automorphism. Hence the theorem: *The number of the automorphisms of order* 2 *in which* H *involves all the operators of order* $2^{\alpha-1}$, $\alpha > 2$, *contained in* G *is one more than the number of automorphisms of* H *which are of order* 2 *and lead only to commutators of order* 2. As the latter number was considered above, the determination of these automorphisms is complete.

Suppose that H involves an operator (c_1) of order 2^α. We proceed to prove that G must contain an invariant operator of order 2^α in this case. In fact, if $t^{-1}s_1 t = c_1 s_1$ it is necessary that s_1 be of order 2^α and also independent of c_1. Hence the group generated by c_1 and s_1 is of order $2^{2\alpha}$. Since $t^{-1}c_1 t = c_1^{-1} = c_1^{-2}c_1$, and $t^{-1}s_1^2 t = c_1^2 s_1^2$, it results that $c_1 s_1^2$ is invariant under t, and it is evident that $c_1 s_1^2$ is of order 2^α. This proves the theorem: *When* H *involves an operator of order* 2^α *an operator of order* 2^α *in* G *must correspond to itself in the automorphism of order* 2 *which gives rise to* H. It is also evident that $c_1 s_1^2$ and c_1 generate groups which have two and only two common operators.

The group of order $2^{2\alpha}$ $\{c_1, s_1\}$ cannot involve more than one commutator of order 2 since these commutators are invariant under t. It results from this that if H involves two independent generators $\{c_1, c_2\}$ of order 2^α, the group generated by c_2 has only the identity in common with $\{c_1, s\}$, as the latter involves no commutators under t except such as are generated by c_1. Hence t must transform a fourth independent generator s_2 as follows: $t^{-1}s_2 t = c_2 s_2$, whenever H involves at least two independent generators of order 2^α. This method of argument may be repeated until all the independent generators of order 2^α in H have been exhausted. As these arguments apply to any abelian group of even order the result may be stated as follows: *If the commutator subgroup arising from an automorphism of order* 2 *of any abelian group of even order* (K) *involves* n *independent generators of highest order in* K, *then* K *involves at least* $2n$ *independent generators of this order.*

It was observed in § 2 that every abelian group of odd order has an automorphism of order 2 giving rise to a commutator subgroup which involves all the independent generators of the abelian group, while the preceding theorem shows that the commutator subgroup arising from an automorphism of order 2 of an abelian group of even order cannot involve more than one half of the largest independent generators of the group. If this commutator subgroup involves exactly half of the independent generators of highest order, it cannot involve more than half of those of the second highest order whenever this order is also even, etc. All the operators of H which are not powers of operators of higher order contained in H must arise from operators of highest order in G.

§ 4. *Commutators of order p^α.*

In the preceding section it was observed that an automorphism of order 2 of an abelian group of even order must always give rise to at least one invariant commutator of order 2. Moreover if all the commutators arising from a given automorphism are of order 2 and correspond to themselves in the automorphism, this automorphism must be of order 2. In the present section we inquire into the properties of a non-abelian group (K) which has no commutator whose order exceeds 2 but which is not restricted in any other way. It is not assumed in this section that all the commutators of K arise from automorphisms of order 2.

Since all the commutators of K are of order 2, every operator (s) of order 2 in K must be transformed under K either into itself or into cs, where c is of order 2. Moreover, from the fact that both s and cs are of order 2 it results that c, s, and cs are three commutative operators which, together with the identity, constitute the four-group. That is, every complete set of conjugate operators of order 2 in K is composed of mutually commutative operators. In other words, all the operators of order 2 in K are found in invariant subgroups each of which is of type $(1, 1, 1, \cdots)$. From this it follows directly that K involves only one Sylow subgroup of order 2^m, and that the quotient group with respect to this Sylow subgroup is abelian. This result will be generalized in the following paragraph.

If the orders of all the commutators of a non-abelian group K are of the form p_1^λ, p_1 being a prime number, it follows directly that every Sylow subgroup of K whose order is not a power of p_1 is abelian. Moreover every operator of K that transforms into itself a subgroup of order p_α^γ, $(\alpha \neq 1)$, is commutative with every operator of this subgroup. Hence it results from a theorem due to FROBENIUS that K contains a characteristic subgroup of index p_α^δ, where p_α^δ is the highest power of p_α that divides the order of K.* As the orders of the commutators of this characteristic subgroup must also be of the form p_1^λ, we may repeat the given argument when the order of this subgroup is not itself of the form p_1^λ. Hence the following theorem: *If the orders of all the commutators of a non-abelian group K are of the form p_1^λ, p_1 being any prime number, K involves only one Sylow subgroup of order p_1^m and the corresponding quotient group is abelian.*

From the preceding paragraph it follows directly that every group in which the orders of all the commutators are powers of the same prime number must be solvable. It is also easy to see that K contains an abelian subgroup which is the direct product of Sylow subgroups of every order except p_1^m. This follows directly from the fact that all the Sylow subgroups of order p_α^δ are

*FROBENIUS, Berliner Sitzungsberichte, 1901, p. 1324.

contained in a characteristic subgroup of order $p_1^m p_a^\delta$. That such a group as K may involve more than one Sylow subgroup of every order except p_1^m, results directly from the fact that the metacyclic group of degree p and of order $p(p-1)$ is included among those which satisfy the conditions imposed on K.

URBANA, ILLINOIS.