ON THE HOLOMORPH OF THE CYCLIC GROUP OF ORDER p^m*

BY

G. A. MILLER

1. *Introduction.* The present article is a continuation of one published in this journal, vol. 4 (1903), p. 151, under the more general title, "On the holomorph of a cyclic group." It was observed that the holomorph of the cyclic group of any order is the direct product of the holomorphs of its Sylow subgroups, and hence the investigation of the holomorph of the general cyclic group may be divided into the consideration of the holomorph of the cyclic group of order p^m and the study of the direct product of given groups. The present article is devoted to some of the important questions under the first topic, which have not been explicitly treated in the earlier paper. The holomorph of a cyclic group not only plays a fundamental rôle in many group theoretic discussions, but also presents questions equivalent to those arising in the theory of exponents to which numbers belong with respect to a given arbitrary modulus m. For instance, the numbers which have recently been called † the primitive roots of m are those which correspond to the operators of highest order in the group of isomorphisms of the cyclic group of order m and hence the determination of the number of such primitive roots is a special case of the determination of the number of operators of a given order in an abelian group. ‡

2. *Cyclic groups of order* 2^m, $m > 3$. We begin with the case when $p = 2$ and shall assume that the cyclic group (H) of order 2^m, $m > 3$, is represented as a regular substitution group. The holomorph (G) of H is composed of all the substitutions in these 2^m letters which transform H into itself. Let s_1 represent a substitution § of order 2^{m-2} which generates all those substitutions of the group of isomorphisms (I) of H which are commutative with the operators of order 4 in H. From the manner in which s_1 transforms the substitutions of H, it is evident that s_1 is composed of 2 cycles of each of the orders

$$2^{m-2},\ 2^{m-3},\ \cdots,\ 4,\ 2.$$

Hence $s_1^{2^\alpha}$, $\alpha < m - 2$, contains $2^{\alpha+1}$ cycles of each of the orders

* Presented to the Society (Southwestern Section) November 30, 1907. Received for publication November 21, 1907.

† EPSTEIN, Archiv der Mathematik und Physik, vol. 12 (1907), p. 135.

‡ Annals of Mathematics (series 2), vol. 2 (1901), p. 77; vol. 6 (1904), p. 1.

§ Bulletin of the American Mathematical Society, vol. 7 (1901), p. 350.

$2^{m-\alpha-2}, 2^{m-\alpha-3}, \cdots, 2$. The number of the substitutions of a given order in the group $\{H, s_1\}$, generated by H and s_1, is exactly equal to this order whenever the degree is less than 2^m. That is, $\{H, s_1\}$ contains two such substitutions of order 2, four of order 4, etc., and all those of the same order are conjugate under $\{H, s_1\}$. Hence the total number of the substitutions of $\{H, s_1\}$ whose degree is less than 2^m is

$$1 + 2 + 4 + \cdots + 2^{m-2}$$

and all its remaining substitutions are regular. The totality of the substitutions of $\{H, s_1\}$ whose orders divide $2^\alpha (\alpha = 1, 2, \cdots, m)$ constitutes a characteristic subgroup under G.

To obtain G we may extend $\{H, s_1\}$ by means of a substitution (s_2) which transforms into their inverse the operators of order 4 contained in H and involves all the letters found in s_1. Then $\{s_1, s_2\}$ is the group of isomorphisms of H and it is of degree $2^m - 2$. All its substitutions except those generated by s_1 are of this degree and each of them is conjugate with 2^{m-1} substitutions under G. The characteristic subgroup of G which is generated by its substitutions which are squares is of index 8 under G. Hence G contains exactly seven subgroups of half its own order. In other words, *the holomorph of the cyclic group of order* 2^m, $m > 3$, *contains exactly seven subgroups of half its own order.*

3. *The auxiliary groups* I *and* I_0. The holomorph contains only one invariant operator besides the identity and hence its group of cogredient isomorphisms (I_0) is of order 2^{2m-2}. We proceed to determine some of the properties of I_0 with a view to a complete determination of the group of isomorphisms (I) of G, the group of isomorphisms of H being well known. As I_0 has a $(1, 2)$ isomorphism with G it contains two invariant cyclic subgroups corresponding to H and its conjugate under I. The operator of I_0 which corresponds to s_1 in this isomorphism is of the same order as s_1. The subgroup of I_0 which corresponds to $\{H, s_1\}$ is therefore similiar to $\{H, s_1'\}$, where s_1' transforms the operators of H in exactly the same manner as s_1 does but the order of s_1' is twice that of s_1. Hence I_0 involves three operators of order 2 which are invariant under I. One of these is generated by s_1'. The construction of I_0 is therefore like that of the holomorph of the cyclic group of order 2^{m-1} with the single exception that the operator which corresponds to s_1 is of order 2^{m-2} instead of being of order 2^{m-3}. In other words, we may construct I_0 by constructing the holomorph of the cyclic group of order 2^{m-1} and then replacing the operator which corresponds to s_1 by the product of this operator and an operator of order 2^{m-2} which is independent of and hence commutative with every operator of this holomorph. Hence it results that *the group of cogredient isomorphisms of the holomorph of the cyclic group of order* 2^m *is a* $(2, 2^m)$ *isomorphism between the cyclic group of order*

2^{m-2} and the holomorph of the cyclic group of order 2^{m-1} with respect to its dihedral subgroup involving this cyclic subgroup.

It is known that the order of I is four times that of I_0 and hence it remains to find operators which transform the operators of G among themselves and are not in I_0. One such operator (s_3) of order 2 is commutative with s_2 and with all the operators of $\{H, s_1\}$ which are commutative with the operators of order 8 in H while it transforms s_1 into itself multiplied by the operator of order 2 in H. As the operators of G which are commutative with s_3 form a characteristic subgroup, s_3 is invariant under I and hence I contains at least 7 invariant operators of order 2 and *the total number of operators which transform both H and G into themselves constitute the direct product of I_0 and an operator of order* 2.

4. *The group I continued.* To complete the determination of I it is only necessary to find a substitution (s_4) which transforms G into itself and a generator of H into itself multiplied by s_1^{m-3}. It is clear that s_4 transforms the square of such a generator into itself multiplied by the operator of order 2 in H and that we may assume that $s_4^{-1} s_2 s_4 = s_2 s_1^{m-3}$. As an operator of I, s_4 transforms the operators of I_0 which are of highest order into themselves multiplied by the invariant operator under I which corresponds to s_1^{m-3} in I_0. It also transforms the operator which corresponds to s_2 in I_0 into itself multiplied by the same operator of I_0. Hence s_4 is of order 2 and has two conjugates under I. Moreover, I is the direct product of $\{I_0, s_4\}$ and the group of order 2 generated by s_3 since s_3 and s_4 are commutative. Hence *I contains* 8 *and only* 8 *invariant operators and these constitute the group of type* $(1, 1, 1)$.

It is easy to determine the orders of all the operators of I by means of the given properties of I_0 and of s_3 and s_4. Just one-fourth of the operators of I_0 are of order 2^{m-1} and these correspond to the operators of order 2^m in $\{H, s_1\}$. The 3 invariant operators of order 2 in I_0 correspond to operators of $\{H, s_1\}$ and the 2^m non-invariant operators of this order correspond to other operators of G. Hence the number of operators of order 2 in I_0 is $2^m + 3$. The number of the operators of order $2^\alpha (1 < \alpha < m-1)$ is given by the expression $2^{m+\alpha-2} + 3.2^{2(\alpha-1)}$. From the properties of s_4 mentioned above it follows that the number of operators of each order in $\{I_0, s_4\}$ is the same as the number of such operators in the direct product of I_0 and an operator of order 2. This follows from the facts that s_4 transforms 2^{m-1} operators of order 4 in I_0 into their inverses and is also non-commutative with the same number of operators of order 2 in I_0. Hence it results that the number of the operators of order $2^\alpha (1 < \alpha < m)$ contained in I is four times the number of the operators of the same order in I_0. From this it follows that the number of operators of order 2 in I is 3 increased by four times the number of these operators in I_0.

5. *Cyclic group of order 2^m, $m < 4$.* In the above considerations it was

assumed that $m \geqq 4$. When $m < 4$ the order of G cannot exceed 32 and hence G is well known and its I has been determined. Hence we do not need to consider the special cases when $m < 4$.

6. *Alternative method of discussion.* Some of the above results can readily be deduced from the fact that G contains two invariant dihedral groups of order 2^{m+1} which have 2^m common operators. Their non-invariant operators of order 2 may be divided into three distinct sets each of which contains 2^{m-1} operators. One of these sets is composed of such operators as are common to both of the invariant dihedral groups while each of the other sets occurs in only one of these groups. As G contains only two operators which are commutative with each operator of the first of these sets as well as with each operator of one of the other sets it follows that I_0 may be represented as an intransitive substitution group of degree 2^m which is obtained by establishing a $(2, 2)$ isomorphism between the holomorph of the cyclic group of order 2^{m-1} written in two distinct sets of letters. From this it follows directly that I_0 contains exactly four invariant operators.

With respect to the three sets of 2^{m-1} operators of order 2 mentioned in the preceding paragraph, I_0 may be represented as an intransitive group of degree 3.2^{m-1} involving as its transitive constituents the holomorph of the cyclic group of order 2^{m-1} written in three distinct sets of letters. Two of these holomorphs are simply isomorphic and the group formed by this simply isomorphism has a $(2, 2)$ isomorphism with the third transitive constituent. The group $\{I_0, s_4\}$ may therefore be represented as a $(4, 2)$ isomorphism between an imprimitive group of degree 2^m and the holomorph of the cyclic group of order 2^{m-1} while I is the direct product of this intransitive group and the group of order 2. This intransitive group is simply isomorphic with the group of cogredient isomorphisms of the double holomorph of H and hence *the group of isomorphisms of the holomorph of the cyclic group of order* 2^m *is the direct product of the group of order* 2 *and the group of cogredient isomorphisms of the double holomorph of the cyclic group of order* 2^m.

7. *Cyclic groups of order* $p^m, p > 2$. When $p > 2$ the group of isomorphisms of H is cyclic and G is a complete group. Hence the considerations for this more general value of p are very much simpler than those for the special value $p = 2$. In view of its greater simplicity, this case seems to require no further developments than those found in the paper mentioned at the beginning of this article, with the exception of a few results which are of especial interest in contrast with results for $p = 2$. When H is represented as a regular group, its group of isomorphisms, which is known to be cyclic and of order $p^{m-1}(p-1)$, contains a subgroup of order p^{m-1} composed of all its substitutions which are commutative with an operator of order p in H. A generator of this subgroup is composed of $p - 1$ cycles of each of the orders $p^{m-1}, p^{m-2}, \cdots, p$; and each of

the substitutions of this group of order $p^{m-1}(p-1)$ which is not in this subgroup is of degree $p^m - 1$. Hence the group of isomorphisms of H is of degree $p^m - 1$ when $p > 2$ and of degree $p^m - 2$ when $p = 2$.

Moreover, when $p = 2$ the group of isomorphisms of H as a subgroup of degree $2^m - 2$ corresponds to a subgroup of degree 2^m in some holomorphism of G; while it must always correspond to a subgroup of its own degree when $p > 2$. In every case there are exactly p^m subgroups with which a particular subgroup transforming H into all its holomorphisms may correspond in some holomorphism of G. From the fact that, when $p > 2$, the maximal subgroup which omits a given letter is of degree $p^m - 1$ and cannot correspond to a subgroup of a different degree in a holomorphism of G, it follows that the group of isomorphisms of G can be represented as a transitive group involving G and hence we have a very simple proof of the known fact that G is a complete group.*

*Messenger of Mathematics, vol. 37 (1907), p. 55.

THE UNIVERSITY OF ILLINOIS,
URBANA, ILL.