DETERMINATION OF ALL THE GROUPS OF ORDER 2^m WHICH CONTAIN AN ODD NUMBER OF CYCLIC SUBGROUPS OF COMPOSITE ORDER*

BY

G. A. MILLER

It has recently been proved that in every non-cyclic group of order p^m, p being an odd prime, the number of cyclic subgroups of order p^β, $\beta > 1$, is always a multiple of p, and that this number is of the form $1 + p + kp^2$ when $\beta = 1$.† From this it follows almost directly that the number of cyclic subgroups of order p^β in any group (G) is always of the form kp whenever the Sylow subgroups of order p^m in G are non-cyclic, and that the number of subgroups of order p in such a G is always of the form $1 + p + kp^2$.‡ When $p = 2$, both of these theorems have exceptions. The present paper is devoted to an exhaustive study of the exceptions of the former theorem. Since the cyclic groups are so elementary we shall confine our attention to the non-cyclic groups of order 2^m. Moreover, every group of even order contains an odd

* Presented to the Society (San Francisco) October 1, 1904. Received for publication September 26, 1904.

† Proceedings of the London Mathematical Society, ser. 2, vol. 2 (1904), p. 142.

‡ The former of these facts was noticed in the article just mentioned. The second does not follow so easily, but it may be proved as follows: Since the number of subgroups of order p in such a Sylow subgroup (S) of order p^m is $\equiv 1 + p \pmod{p^2}$, it is only necessary to observe that the number of those which are found in G but not in S is of the form kp^2. If S transforms one of these subgroups (P) into only p conjugates, the operators of P are commutative with every operator of a subgroup of order p^{m-1} contained in S. In particular, P and an invariant (under S) operator of order p in this subgroup of order p^{m-1} generate a group of order p^2 and of type $(1, 1)$ which has just p conjugates under S. It could not be transformed into itself by S since a Sylow subgroup cannot transform a group of order p^γ into itself unless this group is contained in the Sylow subgroup. The given p subgroups of order p^2 contain p^2 distinct subgroups of order p which are not found in S and whose generators are commutative with each operator of the given subgroup of order p^{m-1}. If there is any other operator (P) of order p in G which is not found in S and is commutative with each operator of the given subgroup of order p^{m-1}, we use the same invariant operator under S and construct other p conjugate subgroups under S which have p^2 additional subgroups of order p, etc. Proceeding in the same manner with each of the other subgroups of order p^{m-1} in S, the theorem clearly follows since we do not need to consider those subgroups of order p which have more than p conjugates under S. When the Sylow subgroups of order p^m ($p > 2$, $m > 1$) in G are cyclic, the preceding argument proves that the number of subgroups of order p is of the form $1 + kp^2$.

number of subgroups of order 2 since the operators of order 2 and the identity are the only ones which are self inverse.

§ 1. *Cyclic subgroups whose order exceeds four.*

We shall first prove that a group of order 2^m cannot contain just $2n+1$, $n>0$, cyclic subgroups of order 2^α, $\alpha>2$. Suppose that such a group (G) contains $2n+1$ cyclic subgroups of order 2^α. At least one of them (H_1) is invariant under G. Let H_2 represent any other and let H_2' be the subgroup of H_2 such that the group $\{H_1, H_2'\}$ generated by H_1, H_2' is of order $2^{\alpha+1}$. When H_2' coincides with H_2 then $\{H_1, H_2'\}$ contains just 2 cyclic subgroups of order 2^α.[*] If this condition is not satisfied H_2' must transform H_1 according to the square of an operator in its group of isomorphism. Hence $\{H_1, H_2'\}$ has still just 2 cyclic subgroups of order 2^α and at least $2^{\alpha-1}$ invariant operators.[†] These two cyclic subgroups, which we may call H_1, H_2, contain just $2^{\alpha-1}$ common operators. It will next be proved that G contains an even number of cyclic subgroups of order 2^α which involve these $2^{\alpha-1}$ common operators. The main result thus far is that any group which contains an odd number (greater than one) of cyclic subgroups of order 2^α must contain two such subgroups which have $2^{\alpha-1}$ common operators.

Suppose that G contains an odd number of cyclic subgroups of order 2^α which have $2^{\alpha-1}$ operators in common with H_1. One of them (H_3) must be transformed into itself by $\{H_1, H_2\}$. The group $\{H_1, H_2, H_3\}$ is clearly conformal to an abelian group with respect to its operators whose orders exceed 4. This follows almost directly from the fact that the order of the commutator subgroup of this group cannot exceed 2. Hence $\{H_1, H_2, H_3\}$ contains four cyclic subgroups of order 2^α. At least one of the remaining cyclic subgroups of order 2^α which have $2^{\alpha-1}$ operators in common with H_1 is transformed into itself by $\{H_1, H_2, H_3\}$. Calling this H_5 we have again that the group $\{H_1, H_2, H_3, H_5\}$ is conformal with an abelian group with respect to its operators whose order exceed four. This group contains 8 cyclic subgroups of order 2^α. As this process could be continued indefinitely if there were an odd number of cyclic subgroups of order 2^α having $2^{\alpha-1}$ operators in common with H_1, this hypothesis is disproved.

The theorem in question is now practically proved, for the cyclic subgroups of order 2^α which have $2^{\alpha-1}$ common operators must occur in even sets and a cyclic group of order 2^α which is found in one set cannot also occur in another set. Hence G *cannot contain just* $2n+1$, $n>0$, *cyclic subgroups of order* 2^α, $\alpha>2$. We shall now consider the case when G contains only one cyclic

[*] BURNSIDE, *Theory of Groups of Finite Order*, 1897, p. 77.

[†] Bulletin of the American Mathematical Society, vol. 7 (1901), p. 352.

subgroup of order 2^a. It will result that in this case G must be one of these three well known groups of order $2^a + 1$ having this property; viz., the dihedral rotation group, the one obtained from this dihedral rotation group by replacing its non-invariant operators of order 2 by operators of order 4, and the one which transforms the operators of the cyclic subgroup of order 2^{a_1} into their $2^{a_1} - 1$ powers, containing $2^{a_1} - 1$ operators of each of the orders 2 and 4 in addition to the given cyclic subgroup.

If G contains only one cyclic subgroup of order 2^a it cannot contain more than one cyclic subgroup of any higher order (2^{a_1}), since some two subgroups of this order would generate a group which is conformal with the abelian group of the type $(\alpha_1, 1)$.[*] Let 2^{a_1} be the order of the largest cyclic subgroup H_1 of G. The operators of G must transform the operators of H_1 according to a group of order 2^{m-a_1}. Every subgroup of order 4 in the group of isomorphisms of H_1 contains the operator of order 2 which transforms just half of the operators of H_1 into themselves.[†] Hence $m = \alpha_1 + 1$, otherwise G would contain more than one cyclic subgroup of order 2^{a_1} as it would have to transform the operators of H_1 according to the given operator of order 2. As the groups of order $2^{a_1} + 1$ which contain a cyclic subgroup of order 2^{a_1} are well known, the results stated at the end of the preceding paragraph are established. That is, *if a group of order* 2^m *contains an odd number of cyclic subgroups of order* 2^a, $\alpha > 2$, *this number must be unity, and the group must be one of three containing a cyclic subgroup of order* 2^{m-1}. As the properties of these three groups are very elementary and their forms are so dissimilar (one contains $2^{m-1} + 1$, the other $2^{m-2} + 1$, and the third only one operator of order 2) it is easy to distinguish them. When α is given, m may have any arbitrary value which exceeds α.

§ 2. *Cyclic subgroups of order four.*

The three groups mentioned in the last paragraph contain respectively one, $2^{m-3} + 1$, and $2^{m-2} + 1$ cyclic subgroups of order 4. We proceed to prove that these are the only non-cyclic groups of order 2^m which contain an odd number of cyclic subgroups of order 4. The method of proof is very similar to the one employed in the preceding section.

Let G be any group of order 2^m which contains an odd number of cyclic subgroups of order 4. At least one of them (K_1) is invariant under G. At least half the operators of G are commutative with a generator (s) of K_1. It will be proved that the subgroup (G_1) formed by these 2^{m-1} operators must be cyclic. If G_1 were not cyclic K_1 would be contained in an abelian subgroup of

[*] American Journal of Mathematics, vol. 23 (1901), p. 173.

[†] Bulletin of the American Mathematical Society, vol. 7 (1901), p. 351.

type $(2, 1)$.* This subgroup would contain two cyclic subgroups of order 4, (K_1, K_2) having a common square. It will now be proved that G would then contain an even number of cyclic subgroups of order 4 including s^2.

If this number were odd, $\{K_1, K_2\}$ would transform at least one of the remaining ones (K_3) into itself. The commutator subgroup of $\{K_1, K_2, K_3]$ is generated by s^2 and hence this group contains an even number of cyclic subgroups of order 4 and all of these subgroups contain s^2.† Hence there would be another invariant cyclic subgroup K_4 involving s^2. The number of cyclic subgroups of order 4 in $\{K_1, K_2, K_3, K_4\}$ is again even since the commutator subgroup is still generated by s^2, and all of these subgroups include s^2. This follows almost directly from the fact that the product of an operator of order 4 in $\{K_1, K_2, K_3, K_4\}$ into an operator of order 2 is of order 4 when the two factors are commutative and of order 2 when they are not commutative, while the converse is true when the second factor is of order 4.

As this process could be continued indefinitely if there were an odd number of cyclic subgroups of order 4 which contained s^2, it results that the number of these subgroups is even. If there were an odd numbers of cyclic subgroups of order 4 in G which did not contain s^2, one of these and s^2 would again generate the abelian group of type (2, 1) and the number of those involving the same subgroup of order 2 would again be even. As similar remarks would apply to all the possible other cyclic subgroups of order 4 we have proved that G_1 *is cyclic whenever* G *contains an odd number of cyclic subgroups of order* 4. This proves the statement in the first paragraph of this section, since the other non-cyclic group of order 2^m which contains a cyclic subgroup of order 2^{m-1} contains an even number of cyclic subgroups of order 4.

Combining the results of the two sections we have that every group of order 2^m, $m > 3$, which contains an odd number of cyclic subgroups of order 4 contains just one cyclic subgroup of order 2^α, where α can have all the values from 3 to $m - 1$; and every group which contains only one cyclic subgroup of order 2^α contains an odd number of cyclic subgroups of order 4. For each value of α and m there are three such groups, hence there is a doubly infinite system of groups of order 2^m which contain an odd number of cyclic subgroups of composite order. When $m = 3$ there are only two groups having this property, viz. the quaternion group and the group of movements of the square. If all the non-cyclic groups of order $p^m (m > 3, p$ an arbitrary prime) were determined there would be just three among them in which the number of cyclic subgroups of composite order would not always be a multiple of p. In these three special cases the number of cyclic subgroups of every composite order is not divisible by p.

* BURNSIDE, loc. cit., p. 75.

† Quarterly Journal of Mathematics, vol. 28 (1896), p. 269.

In the exceptional groups noted above the number of the subgroups of order 2 is $\equiv 1 \pmod{4}$. That this number is $\equiv 3 \pmod{4}$ in every other non-cyclic group of order 2^m is a direct consequence of the fact that the number of cyclic subgroups of order 4 in all of these groups is even. From this fact it results that the number of operators whose order exceeds 2 is divisible by 4, since every cyclic subgroup of order 2^σ contains $2^{\sigma-1}$ operators which are not found in any other subgroup whose order $\leqq 2^\sigma$. Hence the given system of groups is composed of all the groups of order p^m in which the number of cyclic subgroups of order p is not $\equiv 1 + p \pmod{p^2}$. That is, the groups of order p^m in which the number of cyclic subgroups of composite order is not divisible by p coincide with those in which the number of subgroups of order p is not of the form $1 + p + kp^2$.