ON THE POSSIBLE NUMBERS OF OPERATORS OF ORDER 2 IN A GROUP OF ORDER $2^m$.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, September 7, 1905.)

It is well known that every group of order $2^m$ which contains only one operator of order 2 is either cyclic or it is composed of the cyclic group of order $2^{m-1}$ and $2^{m-1}$ operators of order 4 transforming each operator of this cyclic group into its inverse.* There are exactly two such groups for every value of $m > 2$. When $m = 3$ the latter of these two is the quaternion group, and when $m < 3$ the cyclic group is the only one that contains only one operator of order 2.

The groups of order $2^m$ in which the number of all the operators of order 2 is $\equiv 1 \pmod{4}$ have been determined incidentally in a recent paper.† Such groups exist only when the number of operators of order 2 is of the form $2^k + 1$, and there are exactly two possible groups for every arbitrary value of $k$. One of these is the dihedral rotation group of order $2^{k+1}$, and the other is obtained by adding to the cyclic group of order $2^{k+1}$ an operator of order two which transforms each of its operators into its $(2^k - 1)$th power. Just half of the additional operators are of order two and the others are of order 4.

For instance, there are just two groups whose orders are of the form $2^m$ and which contain just five operators of order two;

---

* Burnside, Theory of groups, 1897, p. 75.
one of these is the well known octic group, or the group of movements of the square, while the other is of order 16 and includes the cyclic group of order 8 in addition to four operators of each of the orders 2 and 4 transforming each operator of this cyclic subgroup into its third power. The latter constitute two complete sets of conjugates, while the operators whose orders exceed two in the cyclic subgroup of order 8 are conjugate in pairs. In general, the operators whose orders exceed two in the cyclic subgroup of orders $2^k$ or $2^{k+1}$ respectively are conjugate in pairs while the remaining operators constitute two complete sets of conjugates.

It is well known that every group whose order is divisible by 2 contains an odd number of operators of order 2. Moreover, it is clearly possible to construct a group which contains any arbitrary odd number of operators of order 2. To construct a group which contains exactly $2n + 1$ operators of this order it is only necessary to extend the cyclic group of order $2n + 1$ by an operator of order 2 which transforms each operator of this cyclic group into its inverse. From the theorem mentioned in the second paragraph it follows that it is impossible to construct a group whose order is of the form $2^m$ and which contains an arbitrary odd number of operators of order 2.

In view of the popular saying that 13 is an unlucky number, it is of interest to note that there is no group whose order is of the form $2^m$ and which contains exactly 13 operators of order 2, but there are groups which contain exactly any other odd number, less than twenty-one, of such operators. The truth of this statement follows almost directly from the second paragraph. It will be included among the results of the developments which follow. In these developments it will be assumed that the orders of all the groups under consideration are powers of 2.

The dihedral rotation group of order $2^{k+1}$ contains exactly $2^k + 1$ operators of order 2, whenever $k > 0$. By forming the direct product of this dihedral rotation group and the abelian group of order $2^k$ and of type $(1, 1, 1, \cdots)$ there results a group in which the number of operators of order 2 is exactly $3^{k+1} + 2^{k+1} - 1$. As the values of $\beta$ and $k$ are arbitrary except that $k \neq 0$ it follows that it is possible to construct groups in which the number of operators of order 2 is exactly $2^x + 2^y - 1$, where $x$ and $y$ can have any arbitrary pair of integral values with the exception of 0, 1. When the groups are abelian $x = y$, but the converse is not necessarily true.
From the preceding paragraph it follows that it is possible to construct a group of order $2^n$ in which the number of operators of order 2 is the sum of two arbitrary powers of 2 diminished by one. We shall now prove that it is possible to construct a group in which the number of these operators is the sum of three arbitrary powers of two diminished by one, provided the smallest of these powers is divisible by 4. It is clear that we may restrict ourselves to the case when the three powers are distinct since the other cases reduce to those considered in the preceding paragraph.

To prove this theorem it is convenient to consider the group $(G_i)$ of order $2^{a+2}$ which is obtained by taking all the operators of the holomorph of the cyclic group of order $2^a$ which transform this cyclic group into its $1, 2^{a-1} - 1, 2^{a-1} + 1,$ and $2^a - 1$ powers respectively. These powers are distinct when $a > 2$. In this case there are $1, 2^{a-1}, 2$ and $2^a$ operators of order 2 which transform the cyclic group into the respective powers mentioned above. It is clearly possible to establish a $\langle 2^a, 2^\beta \rangle$ isomorphism between $G_i$ and the dihedral rotation group of order $2^{\beta+2}$ in such a manner as to obtain a group $(G)$ which contains $3 + 2^{\beta+1} + 2^{a+\beta}$ operators of order 2, whenever $\beta > 0$.

As $a$ and $\beta$ are arbitrary independent positive integers, with the restriction that $a > 2$, it follows that the number of operators of order 2 in $G$ is the sum of two powers of 2, whose indices differ by at least two units but are otherwise arbitrary, increased by 3. In $G_i$ the number of these operators is the sum of two powers of 2, whose indices differ by one but are otherwise arbitrary, increased by 3. Hence by forming the direct product of an abelian group of order $2^\gamma$ and of type $(1, 1, 1, \ldots)$ into either $G$ or $G_i$ we obtain a group in which the number of operators of order 2 is $2^x + 2^y + 2^z - 1$, where $x, y, z$ satisfy the condition $x > y > z > 1$ are but otherwise arbitrary. This proves the theorem in question.

It has recently been proved that the number of operators of order 2 in a group of order $2^n$, in which more than half the operators are of order 2, is always the sum of two powers of 2 diminished by one, and that it is possible to construct such a group in which the number of operators of order 2 is an arbitrary number of this form. Hence it follows from the preceding paragraph that groups in which less than half the operators are of order 2 may involve a number of operators of this order which could not be the exact number of these opera-
tors in any group in which more than half the operators are of order 2.

A \((2^a, 2^b)\) isomorphism between \(G\) and the direct product of the dihedral rotation group of order \(2^{b+1}\) into an operator of order 2 can be established in such a manner as to obtain a group in which the number of operators of order 2 is either \(3 + 2^a + 2^{b+1} + 2^{a+b}\), or \(3 + 2^{a+1} + 2^{b+1} + 2^{a+b} - 1\), \(\beta > 0\). In fact, it is possible to form other such isomorphisms, but these two seem especially useful in this connection. Moreover, by establishing a \((2^a, 2^b)\) isomorphism between \(G\) and a group of order \(2^{b+2}\) which is constructed in the same way as \(G\), we arrive at groups which contain any of the following three numbers of operators of order 2: \(3 + 2^a + 2^b + 2^{a+b}, 3 + 2^{a+1} + 2^{b+1} + 2^{a+b} - 2, 3 + 2^{a+1} + 2^a + 2^{a+b} - 1\).

From the above results it follows directly that there are groups of order \(2^n\) which contain any prescribed number of operators of order 2 which satisfies the conditions that it is \(\equiv 3 \mod. 4\) and less than 124. By other considerations this limit can readily be extended, but my methods seem too special to be given here. It would be interesting to find a number \(\equiv 3 \mod. 4\) which could not equal the number of operators of order 2 in any group of order \(2^n\), or to prove the non-existence of such a number.

ON THE ARITHMETIC NATURE OF THE COEFFICIENTS IN GROUPS OF FINITE MONOMIAL LINEAR SUBSTITUTIONS.

BY DR. W. A. MANNING.

(Read before the American Mathematical Society, September 7, 1905.)

Professor Maschke* has proved (with a certain restriction) that the coefficients of finite linear substitution groups can, by proper transformations, be made rational functions of roots of unity. Professor Burnside† has also recently written on this subject. In this note it is proved that linear groups all of