ISOMORPHISMS OF A GROUP WHOSE ORDER IS A POWER OF A PRIME*

BY

G. A. MILLER

§ 1. *Groups of isomorphisms involving operators of order p^{m-1}.*

Let G be any group of order p^m, p being a prime number, and let I represent its group of isomorphisms. A necessary and sufficient condition that I involves operators of order p is that $m > 1$, since G can always be made isomorphic with one of its invariant subgroups of order p which corresponds to the identity in this isomorphism when $m > 1$. Hence the order of I is divisible by p whenever $m > 1$ and only then. Although the order of I may be divisible by a much higher power of p than p^m, it is very easy to prove that the order of every operator of I is a divisor of $p^{m-1}k$, k being prime to p. That is, I cannot involve any operator whose order is divisible by p^m.

To prove this theorem we may assume that t is an operator of I which has been so selected that its order is the highest possible power of p. As t and G generate a group whose order is a power of p it is possible to select a series of invariant subgroups of G

$$H_0,\ H_1,\ H_2,\ \cdots,\ H_m = G,$$

whose orders are respectively $1,\ p,\ p^2,\ \cdots,\ p^m$ and such that each one except the last is contained in the one which follows it and that t transforms each operator of each of these subgroups except the first into itself multiplied by an operator in the one which precedes it in the given series. Hence we have the following equations, s_α being an operator of H_α,

$$t^{-1}s_\alpha t = s_{\alpha-1}s_\alpha, \qquad t^{-p}s_\alpha t^p = s_{\alpha-2}s_\alpha \qquad (\alpha \geqq 2),$$

since $s_{\alpha-1}^p = s_{\alpha-2}$ and $s_{\alpha-1}^{-1}s_{\alpha-2}s_{\alpha-1} = s'_{\alpha-2}$, $s'_{\alpha-2}$ being an operator of $H_{\alpha-2}$.

If we replace t^p by t_1 it results from similar considerations that

$$t_1^{-p}s_\alpha t_1^p = s_{\alpha-3}s_\alpha \qquad (\alpha \geqq 3).$$

In general,

$$t^{-p^\beta}s_\alpha t^{p^\beta} = s_{\alpha-\beta-1}s_\alpha \qquad (\alpha \geqq \beta + 1).$$

From the last equation it follows directly that the order of t is a divisor of p^{m-1},

* Presented to the Society April 28, 1911.

and hence the following theorem has been proved: *The group of isomorphisms of a group of order p^m does not involve any operator whose order is divisible by p^m.*

It is well known that the group of isomorphisms of the cyclic group of order p^m, $p > 2$, contains operators of order p^{m-1}. We proceed to prove that no other group of order p^m with the exception of the non-cyclic group of order p^2 can have operators of order p^{m-1} in its group of isomorphisms. To prove this statement it is only necessary to observe that every non-cyclic group of order p^m contains an invariant non-cyclic subgroup of order p^2. Hence it results that

$$t^{-p^{m-3}} s_\alpha t^{p^{m-3}} = s_{\alpha-m+2} s_\alpha \qquad (\alpha \geqq m-2).$$

If we let $\alpha = m$ and observe that the orders of all the operators of H_2 divide p, it results that the $t^{p^{m-2}}$ is commutative with every operator of G. That is, *the group of isomorphisms of a non-cyclic group of order p^m cannot contain any operator whose order is divisible by p^{m-1} when $p > 2$ and $m > 2$.*

When $p = 2$ it is known that the group of isomorphisms of the cyclic group of order p^m is the direct product of the cyclic group of order 2^{m-2} and the group of order 2. Hence there is no operator of order 2^{m-1} in the I of the cyclic group of order 2^m when $m > 2$. Moreover it results from the preceding paragraph that the I of any group of order 2^m, $m > 3$, cannot involve any operator of order 2^{m-1} whenever this group of order 2^m involves the non-cyclic group of order 4 invariantly. A group of order 2^m contains an invariant non-cyclic group of order 4 when the number of its cyclic groups of this order is even. Hence it results that if the I of a group of order 2^m, $m > 3$, contains an operator of order 2^{m-1} this group must be one of the three non-cyclic groups of order 2^m which involve an odd number of cyclic subgroups of order 4.*

Two of these non-cyclic groups are the dihedral and the dicyclic groups, and it is easy to prove that the I of each of these groups involves operators of order 2^{m-1}. In fact, the I of such a group of order 2^m must involve an operator which is commutative with each of its operators in the invariant cyclic group of order 2^{m-1} but transforms the remaining operators into themselves multiplied by an operator of order 2^{m-1}. The order of such an operator in I is evidently 2^{m-1}, and hence it results that the groups of isomorphisms of the dihedral group and of the dicyclic group of order 2^m involve operators of order 2^{m-1}. The remaining one of the three non-cyclic groups of order 2^m which involve an odd number of cyclic subgroups of order 4 involves exactly 2^{m-2} non-invariant operators of order 2 when $m > 3$, and its group of isomorphisms may be represented as an intransitive substitution group having two transitive constituents of degree 2^{m-2}. Hence this I cannot involve any operator of order 2^{m-1} so that we have arrived at the theorem: *A necessary and sufficient condition that a group of order 2^m,*

*These Transactions, vol. 6 (1905), p. 58.

$m > 3$, *have an operator of order* 2^{m-1} *in its group of isomorphisms is that the group be either dihedral or dicyclic.* When $m \leqq 3$ every group of order 2^m, with the exception of the cyclic group of order 8, has an operator of order 2^{m-1} in its group of isomorphisms, as one may readily verify.

§ 2. *Groups of isomorphisms involving operators of order* p^{m-2}, $p > 2$.

Having considered all the possible groups of order p^m which involve an operator of order p^{m-1} in their groups of isomorphisms we proceed to consider those whose groups of isomorphisms involve operators of order p^{m-2} but none of order p^{m-1}. We shall again represent the group under consideration by G and its group of isomorphisms by I. Suppose that G contains an invariant subgroup of order p^4 which does not involve any operator of order p^3 and that the series of invariant subgroups

$$H_0, H_1, H_2, \cdots, H_m = G$$

has the same properties as in the preceding section.

From the equation

$$t^{-p^\beta} s_a t^{p^\beta} = s_{a-\beta-1} s_a \qquad (\alpha \geqq \beta + 1),$$

where s_a is any operator of H_a, it results that

$$t^{-p^{m-5}} s_m t^{p^{m-5}} = s_4 s_m \qquad (m > 4).$$

Let $t_1 = t^{p^{m-5}}$. We proceed to prove that $t_1^{p^2} = t^{p^{m-3}} = 1$. In fact,

$$t_1^{-p} s_{ma} t_1^p = s_2 s_3^{kp} s_4^p s_m = s_3 s_m \qquad (p > 2).$$

Since s_3 is commutative with s_2 and as G involves an invariant non-cyclic subgroup of order p^2, it results that the order of s_3 cannot exceed p. This proves that $t^{p^{m-3}} = 1$ whenever $m > 4$ and $p > 2$, since t_1^p must then be commutative with s_2. We have now proved that G cannot have an operator of order p^{m-2}, $m > 4$, in its group of isomorphisms when G involves an invariant subgroup of order p^4 which does not involve any operator of order p^3. It is evident that this proves also that G could not involve such an operator if it contained an invariant subgroup of order p^3 involving only operators of order p besides the identity. In seeking all the groups whose groups of isomorphisms involve operators of order p^{m-2} but none of order p^{m-1}, we may therefore confine our attention to such groups as give rise to a cyclic quotient group with respect to the invariant non-cyclic group of order p^2 and in which operators of order p^2 correspond to the operators of order p in this quotient group. This clearly implies that the groups in question contain operators of order p^{m-1}.

From the preceding paragraph it follows that if the I of G involves operators of order p^{m-2} but none of order p^{m-1}, G must be one of the two non-cyclic groups of order p^m which involve operators of order p^{m-1}. As the cyclic group of order p^{m-1} involves operators of order p^{m-2} in its group of isomorphisms it is evident that the I's of both of the non-cyclic groups in question involve operators of order p^{m-2}. Hence the theorem : *A necessary and sufficient condition that the group of isomorphisms of a group of order p^m, $p > 2$ and $m > 4$, involves operators of order p^{m-2} is that this group of order p^m involves operators of order p^{m-1}.* When $m = 3$ it is evident that the groups of isomorphisms of all the possible non-cyclic groups involve operators of order p^{m-2} but none of order p^{m-1}. When $m = 4$ a group of order p^m which does not involve operators of order p^{m-1} may also have operators of order p^{m-2} in its group of isomorphisms, as may readily be verified.

Incidentally the developments of this section have led to an important general theorem which may be stated as follows: *A necessary and sufficient condition that a group of order p^m, $p > 2$ and $m > 4$, contain an invariant subgroup of order p^4 which does not involve any operator of order p^3 is that the group of order p^m does not involve any operator of order p^{m-1}.* In fact, we may easily derive the more general theorem that the number of the subgroups of order p^4 which do not contain any operator of order p^3 is always of the form $1 + kp$ when G does not involve any operator of order p^{m-1}. When G involves such an operator this number is evidently zero, so that we may say that every group of order p^m, $p > 2$ and $m > 4$, contains either no subgroup of order p^4 which involves only operators whose orders divide p^2, or the number of its subgroups which have this property is of the form $1 + kp$. When it involves no such subgroup it must be one of the three groups of order p^m which involve operators of order p^{m-1}.

To prove this theorem we may confine our attention to the invariant subgroups of order p^4 which do not involve any operators of order p^3. From the theorem stated at the beginning of the preceding paragraph it results that G contains at least one such invariant subgroup if it does not involve any operator of order p^{m-1}. In what follows we shall assume that this condition is satisfied and let

$$K_1,\ K_2,\ \cdots,\ K_\lambda$$

be the totality of the invariant subgroups of order p^4 in G which do not involve operators of order p^3. We proceed to prove that the group generated by these λ subgroups does not involve any operator of order p^3. This fact will evidently establish the theorem in question.

To prove this fact we let t be any operator of the group generated by K_1, K_2, $\cdots$, K_λ such that $t^{p^2} = 1$, while s_a represents an operator of K_a, $1 \leqq a \leqq \lambda$, and s_3, s_2 represent operators belonging to invariant subgroups of orders p^3 and p^2 respectively in K_a, these subgroups being invariant under both K_a and t. We may evidently assume that s_2 is of order p and that it is invariant under both of the operators t^p and s_3^p. Hence the following equations

$$(s_\alpha t)^p = s_\alpha t s_\alpha t s_\alpha t \cdots = s_\alpha t s_\alpha t^{-1} t^2 s_\alpha t^{-2} t^3 \cdots t^p$$

$$= s_\alpha s_3 s_\alpha s_2 s_3^2 s_\alpha \cdots s_2' s_3^{p-1} s_\alpha t^p = s_2'' s_3^p s_\alpha^p t^p,$$

where s_2, s_2', s_2'' are operators of the same invariant subgroup of order p^2 in K_α. As all of the operators s_2'', s_3^p, s_α^p, t^p are commutative with s_2'' and s_3^p, and the order of each is a divisor of p it results that the order of $s_\alpha t$ cannot exceed p^2. This proves that the group generated by $K_1, K_2, \cdots, K_\lambda$ involves no operator of order p^3 and hence we have established the theorem : *If a group of order p^m, $p > 2$ and $m > 4$, involves no operator of order p^{m-1} the number of its subgroups of order p^4 which do not involve any operator of order p^3 is of the form* $1 + kp$. In other words, it has been proved that if G is any non-cyclic group of order p^m, $p > 2$ and $m > 4$, which does not involve any operator of order p^{m-1}, the number of its cyclic subgroups of order p^4 is congruent mod p to the number of its non-cyclic subgroups of order p^4 which involve an operator of order p^3, each of these numbers being divisible by p.

§ 3. *Groups of isomorphisms involving operators of order* 2^{m-2}.

In the present section we shall assume that the order of G is 2^m and that its group of isomorphisms I involves operators of order 2^{m-2} but none of order 2^{m-1}. It has already been observed that the I of the cyclic group of order 2^m contains operators of order 2^{m-2} but none of order 2^{m-1}, so that G may be cyclic. In what follows we shall consider the possible cases when G is non-cyclic. We begin, as in the preceding section, by finding an upper limit for m when G involves an invariant subgroup of order p^4 which does not contain any operator of order p^3. The equation

$$t^{-pm-5} s_m t^{pm-5} = s_4 s_m \qquad (m > 4),$$

which was obtained in the preceding section is evidently true also when $p = 2$, and if we assume that $m > 5$ it follows that

$$t_1^{-p} s_m t_1^p = s_2 s_4^2 s_m = s_3 s_m,$$

t_1, s_2, s_3, s_4, s_m having the same meaning as in the preceding section. As the order of s_3 divides 2 and as t_1^p is commutative with s_3, it results that the order of t must divide 2^{m-3}. That is, *if a group of order 2^m contains an invariant subgroup of order 16 which does not include any operator of order 8, the group of isomorphisms of this group of order 2^m does not involve any operator of order 2^{m-2} when $m > 5$.*

We shall now consider some of the properties of the groups of order 2^m, $m > 5$, which do not include an invariant subgroup of order 16 involving no operator of order 8. It is evident that all the groups of order 2^m which involve operators of order 2^{m-1} are included among these groups. If G is any other group of order 2^m which belongs to this category it involves a non-cyclic invariant subgroup of order 4 and the corresponding quotient group contains no invariant non-cyclic group of order 4. Hence this quotient group contains operators of order 2^{m-3}. To the invariant operator of order 2 in this quotient group there must correspond operators of order 4 in G and hence G involves operators of order 2^{m-2}. That is, every group of order 2^m, $m > 5$, whose group of isomorphisms involves operators of order 2^{m-2} must itself involve operators of this order. In other words, *if a group of order 2^m does not contain any operator of order 2^{m-2} its group of isomorphisms cannot contain any operator of this order when $m > 5$.*

As all the groups of order 2^m which involve operators of order 2^{m-2}, as well as all those whose orders divide 32, are known the preceding theorem reduces our problem to the study of known groups. Two of the six groups of order 2^m, $m > 3$, which involve operators of order 2^{m-1} have operators of order 2^{m-1} in their groups of isomorphisms in accord with the results of section 1. It is easy to see that two others have operators of order 2^{m-2} in their groups of isomorphisms while the largest operators in the I's of the remaining two groups are of order 2^{m-3}. That the group of order 2^m which is generated by an operator of order $2^{m-'}$ and an operator of order 2 which transforms this into its $(2^{m-2}-1)$th power involves an operator of order 2^{m-2} in its I, results immediately from the fact that the I of this group contains an operator which is commutative with each operator of the cyclic subgroup of order 2^{m-1} and which transforms the remaining operators into themselves multiplied by an operator of order 2^{m-2}. In fact, there is such an operator in its group of cogredient isomorphisms. As the cyclic group of order 2^m has also operators of order 2^{m-2} in its I, we have found the two groups of order 2^m whose I's contain operators of order 2^{m-2} but none of order 2^{m-1}.

Each of the two remaining groups of order 2^m which involve operators of order 2^{m-1} contains two cyclic subgroups of order 2^{m-1}. The I's of these G's may evidently be represented as substitution groups on two sets of 2^{m-2} letters corresponding to the operators of order 2^{m-1} in the G's. When I is represented in this way it contains an intransitive subgroup of half its own order composed of all its substitutions which do not interchange the two cyclic subgroups of order 2^{m-1} in G. These transitive constituents clearly involve operators of order 2^{m-3} but none of order 2^{m-2} and there is a $(2, 2)$ isomorphism between them, since the cyclic subgroups of order 2^{m-1} in G have their operators whose orders divide 2^{m-2} in common. One of the remaining operators of I is of order 2 and is commutative with all the operators of G whose orders divide 2^{m-2}. It must therefore be commutative with all the operators of I which transform each operator of order 2 in G into itself. From this fact it follows directly that I does not contain any operator of order 2^{m-2}, and hence the theorem: *The six groups of order 2^m, $m > 3$, which involve operators of order 2^{m-1} may be divided into three sets of two each such that the groups of isomorphisms of the first set involve operators of order 2^{m-1}, those of the second set involve operators of order 2^{m-2} but none of order 2^{m-1}, while the largest order of the operators in the groups of isomorphisms of the two groups of the third set is 2^{m-3}. All these groups of isomorphisms involve only operators whose orders are powers of 2.*

It remains to consider the groups of order 2^m, $m > 5$, which do not involve operators of order 2^{m-1} but contain operators of order 2^{m-2} in their groups of isomorphisms. It has been observed that the quotient group with respect to an invariant non-cyclic group of order 4 in such a group G cannot include a non-cyclic invariant subgroup of order 4, and that the operators of G which correspond to the invariant operator of order 2 in this quotient group must be of order 4. As this quotient group cannot be cyclic and does not involve an invariant non-cyclic subgroup of order 4 it must be one of three groups, viz., the dihedral, the dicyclic, or the group which involves both a dihedral and a dicyclic subgroup of half its own order. In the last two cases G involves operators of order 8 which correspond to operators of order 4 in some non-invariant subgroup of order 4 of the quotient group.

From the preceding paragraph it results that the only groups which remain to be considered are those which have an invariant subgroup of order 2^{m-1} involving two cyclic subgroups of order 2^{m-2}. This invariant subgroup must be one of two groups and the rest of the operators of G transform each operator of this subgroup into its inverse multiplied by one of the operators of the invariant non-cyclic subgroup of order 4 contained in G. Since t transforms each operator of the cyclic subgroup of order 2^{m-3} in the quotient group of G, with respect to its non-cyclic subgroup of order 4, into itself multiplied by an operator of lower order, it results that t must transform the operators of G which correspond to this cyclic subgroup in this quotient group according to an operator whose order cannot exceed 2^{m-3}. Hence t cannot be of order 2^{m-2} unless it transforms the remaining operators of G according to an operator of this order. It must therefore give rise to a commutator of order 2^{m-2} whenever its order is 2^{m-2}.

It is now easy to prove that the subgroup of G which involves two cyclic subgroups of order 2^{m-2} must be abelian.* If it were non-abelian, t could not transform the operators corresponding to non-invariant subgroups of order 2 or 4 in the given quotient group into themselves multiplied by operators of order 2^{m-2}, since the latter are not commutative with all the operators of order 2 in

* This is a special case of the general theorem that a commutator arising from either cogredient or contragredient isomorphisms of a group must be commutative with all the operators of every characteristic complete set of conjugates which involves only two operators or subgroups.

the non-cyclic invariant subgroup of order 4 in G. We shall therefore assume in what follows that G contains an abelian subgroup K of order 2^{m-1} involving two cyclic subgroups of order 2^{m-2}, and we shall consider the various possible groups when the quotient group as regards the non-cyclic invariant subgroup of G is one of the three possible subgroups.

If this quotient group is dihedral and all the operators of G which are not also in K are of order 2, it is evident that the I of G involves operators of order 2^{m-2}, since t transforms each operator of K into its inverse. When t transforms all the operators of K into their inverses and is of order 4, its square may be equal to the square of an operator of order 4 in K, or it may be one of the other two operators of order 2 in K. In the latter case, the possible group when t^2 is one of these operators of order 2 is evidently conjugate with the one when t^2 is the other operator of order 2. Hence there are three groups of order 2^m which involve K and in which all the operators of K are transformed into their inverses by t. In each of these three groups the group of isomorphisms clearly involves operators of order 2^{m-2}.

When t transforms half the operators of K into their inverses and the rest into their inverses multiplied by an operator of order 2, it is clearly only necessary to consider two of the three operators of order 2 in K. Moreover the two cyclic subgroups of order 2^{m-2} in K are evidently conjugate under I, and hence we need to consider only one of them. That is, it is necessary to consider only the four cases when the operators of G which are transformed into their inverses by t constitute either the cyclic subgroup of order 2^{m-2} or the non-cyclic subgroup of this order, and the remaining operators of K are transformed into their inverses multipled by one of two operators of order 2. One of these cases does not give rise to any group since the t which transforms all the operators of a cyclic subgroup of order 2^{m-2} into their inverses cannot transform the remaining operators into their inverses multiplied by an operator of order 2 that is included among these operators. It is therefore only necessary to consider three cases.

There are just two groups when t transforms all the operators of a cyclic subgroup of order 2^{m-2} into their inverses and the remaining operators of G into their inverses multiplied by the square of an operator of order 4 in G. In one of these G's half the operators which are not also in K are of order 2, while the other half are of order 4; in the other G all of these operators are of order 8. The I's of these groups must involve operators of order 2^{m-2} since operators of this order are transformed into their inverses by the operators of G which are not also in K, and hence one of the latter operators may be made to correspond to itself multiplied by an operator of order 2^{m-2} in K.

When t transforms all the operators of the non-cyclic subgroup of order 2^{m-2} in K into their inverses there are four possible groups, but only one of these four has operators of order 2^{m-2} in its group of isomorphisms. It is very evident that the two of these groups in which half the operators which are not in K are of order 2 cannot have operators of order 2^{m-2} in their groups of isomorphisms since the product of any one of these operators of order 2 and an operator of order 2^{m-2} in K is of order 4. In the other two possible groups all the operators of G which are not also in K are of order 4 and these operators have two distinct squares. When one of these squares is the square of an operator of order 4 in K the corresponding I involves operators of order 2^{m-3} but none of order 2^{m-2}, since this square is a characteristic operator of G. On the other hand, the G in which the squares of these operators of order 4 are the other two operators of order 2 in K has operators of order 2^{m-2} in its I. This completes the consideration of the possible cases when all the operators of K are transformed under G into their inverses multiplied by operators of its non-cyclic invariant subgroup of order 4.

It remains to consider the case when the quotient group of G with respect to this non-cyclic subgroup of order 4 contains both the dihedral group and the dicyclic group of half its own order. In this case half the operators of G which are not also in K are of order 8 while the orders of the other half of these operators divide 4. It is known that there is one and only one such group,* and that it involves $2^{m-3}+3$ operators of order 2. Hence the transitive constituents of its group of isomorphisms, which correspond to the operators of order 2 in G, cannot involve any operator of order 2^{m-2}. The group of isomorphisms of G may evidently be represented as a substitution group in which a transitive constituent corresponds to operators of highest order in G while the other constituents correspond to operators of order 2. As neither of these constituents could involve substitutions of order 2^{m-2}, it has been proved that the I of the group under consideration cannot involve any operator of order 2^{m-2}. We have therefore established the following theorem: *There are exactly six groups of order 2^m, $m > 5$, which do not involve operators of order 2^{m-1} but contain operators of order 2^{m-2} in their groups of isomorphisms. Each of these six groups includes an abelian subgroup of order 2^{m-1} and of type $(m-2, 1)$.* Hence the total number of groups of order 2^m, $m > 5$, which have operators of order 2^{m-2} in their groups of isomorphisms is 10 and the number of those which have operators of order 2^{m-2} but none of order 2^{m-1} in their groups of isomorphisms is 8.

§ 4. *Sylow subgroups of the groups of isomorphisms.*

Since every group G of order p^m contains a series of invariant subgroups of orders $1, p, p^2, \cdots, p^m$ which are also invariant under a Sylow subgroup of order p^a in the group of isomorphisms of G, it follows from the preceding

*These Transactions, vol. 2 (1901), p. 271.

theorems that $\alpha \leqq m-1+m-2+\cdots+2+1$. Hence it results that if p^α is the order of a Sylow subgroup in the group of isomorphisms of G then $\alpha \leqq \frac{1}{2}m(m-1)$. When G is cyclic the value of α is $m-1$, hence α cannot have this maximal value for every group of order p^m when $m>2$. On the other hand, there is always at least one group of order p^m for which $\alpha=\frac{1}{2}m(m-1)$, viz., the abelian group of type $(1, 1, \cdots)$. In the present section we shall determine all the possible groups of order p^m whose groups of isomorphisms involve Sylow subgroups whose orders are $p^{\frac{1}{2}m(m-1)}$. In what follows we shall represent such a group by G and its group of isomorphisms by I. A series of invariant subgroups of G which are also invariant under a Sylow subgroup of I and have the orders $1, p, p^2, \cdots, p^m$ (each including those which precede it) will be represented by

$$H_0, H_1, H_2, \cdots, H_m = G.$$

The maximum value of α evidently implies that the isomorphism of each operator in one of the $p-1$ divisions of $H_\beta - H_{\beta-1}$ with respect to $H_{\beta-1}$, $\beta \leqq m$, is independent of those of $H_{\beta-1}$ and hence G cannot involve any operator whose order exceeds p^2. For the same reason the order of the commutator subgroup of G cannot be divisible by p^2, and all the operators of order p^2 in G must generate the same subgroup of order p. This common subgroup must be the commutator subgroup when G is both non-abelian and also involves operators of order p^2. All the operators of $H_\beta - H_{\beta-1}$ are of the same order and H_{m-1} must be abelian, otherwise an operator of one of the $p-1$ divisions of $H_m - H_{m-1}$ could not be made to correspond to every other operator of such a division when the identical operators of H_{m-1} would correspond.

When G is abelian there are only two groups of order p^m, $m>1$, which satisfy the conditions imposed in the preceding paragraph. One of these is of type $(1, 1, \cdots)$ and the other is of type $(2, 1, 1, \cdots)$. It is evident that the I of each of these two groups involves a Sylow subgroup of order $p^{\frac{1}{2}m(m-1)}$. Hence the theorem: *There are two and only two abelian groups of order* p^m, $m>1$, *whose groups of isomorphisms have orders which are divisible by* p^α, *where* $\alpha=\frac{1}{2}m(m-1)$. *One of these is of type* $(1, 1, 1, \cdots)$, *while the other is of type* $(2, 1, 1, \cdots)$.

It remains to determine the possible groups when G is non-abelian. When $p=2$ and all the operators of $H_m - H_{m-1}$ are of order 2, the abelian subgroup H_{m-1} must be of type $(2, 1, 1, 1, \cdots)$, and hence G is the direct product of a group of type $(1, 1, 1, \cdots)$ and the octic group. When all the operators of $H_m - H_{m-1}$ are of order 4, H_{m-1} must again be of type $(2, 1, 1, \cdots)$, since the product of two such operators of order 4 is of order 2 when they are commutative and of order 4 when they are non-commutative. Hence G is the Hamiltonian group of order 2^m in this case. That is, it is the direct product of the quaternion group and the group of type $(1, 1, \cdots)$. Hence we have proved the theorem: *If the order of the group of isomorphisms of a non-abelian group of order* 2^m *is divisible by* $2^{m(m-1)/2}$ *it is either the Hamiltonian group or it is the direct product of the octic group and a group of type* $(1, 1, 1, \cdots)$.

When G is non-abelian and $p > 2$ all the operators of $G_m - G_{m-1}$ may be of order p. As one of the subgroups of order p^{m-2} is composed of invariant operators it must be characteristic and hence may be used for H_{m-2}. Hence there is one and only one such group in which all the operators have orders which divide p. Since the product of two operators of order p in G is of order p it remains to consider the case when all the operators of $G_m - G_{m-1}$ are of order p^2. If t and s are two such operators $(ts)^p = t^p s^p$ and hence the orders of all the operators of G_{m-1} must again divide p. This abelian group is therefore again completely determined and hence we have only one such group. This proves the theorem: *Every non-abelian group of order* p^m, $p > 2$, *whose group of isomorphisms has an order which is divisible by* $p^{m(m-1)/2}$ *is the direct product of a non-abelian group of order* p^3 *and an abelian group of type* $(1, 1, 1, \cdots)$, *and every such direct product has a group of isomorphisms whose order is divisible by* $p^{m(m-1)/2}$.

If we combine this theorem with what precedes it results that there are just four groups of order p^m, $m > 2$, which have groups of isomorphisms whose orders are divisible by p^α, where $\alpha = m(m-1)/2$. Two of these groups are abelian and two are non-abelian. If p^β is the order of an operator in such a group of isomorphisms $\beta \leqq m/2$ when m is even and $\beta \leqq (m+1)/2$ when m is odd. When $p = 2$, no two of the four given groups are conformal but when $p > 2$, each of the two abelian groups is conformal with one of the two non-abelian groups.

Since the series of subgroups $H_0, H_1, H_2, \cdots, H_m$ remains fixed under all the isomorphisms of a Sylow subgroup of order p^α in I, it results directly that *a necessary and sufficient condition that the group of isomorphisms of a group of order* p^m *involves only one Sylow subgroup of order* p^α *is that this group of order* p^m *involves a characteristic subgroup of order* p^γ, *for every value of* γ *from* 1 *to* $m-1$. In particular, every group of order p^m, $m > 3$, which involves operators of order p^{m-1} has a group of isomorphisms involving only one Sylow subgroup of order p^α. When the I of G involves only one Sylow subgroup of order p^α all of its operators whose orders are prime to p must have orders whose prime factors divide $p-1$. Hence the theorem: *A necessary and sufficient condition that the order of the group of isomorphisms of a group of order* 2^m *is of the form* 2^α *is that this group of order* 2^m *has a characteristic subgroup of order* 2^γ, $\gamma = 1, 2, \cdots, m-1$.

When two operators of the group of isomorphisms of any group give rise to commutators which are invariant under these operators then these operators have evidently the same orders and the same relative properties as their respective commutators. In particular, if a group G contains a subgroup H composed of operators which arise as commutators under operators of the group of isomorphisms of G which are commutative with each operator of H, then this group of isomorphisms involves a subgroup which is simply isomorphic with H. A number of other general theorems relating to the groups of isomorphisms are given in the article entitled: "The groups of isomorphisms of the groups whose degree is less than eight," *Philosophical Magazine*, vol. 231 (1908), p. 223. The present article has close contact with the one just mentioned.

§ 5. *Isomorphisms in which a large number of operators correspond to their inverses.*

If more than three fourths of the operators of a group correspond to their inverses in some one of its possible automorphisms the group must be abelian,* and all the operators of any abelian group evidently correspond to their inverses in one of its automorphisms. The totality of the operators which correspond to their inverses in an automorphism of any abelian group constitutes a subgroup whenever this totality does not include all the operators of the group, but the totality of the operators which correspond to their inverses in an automorphism of a non-abelian group does not necessarily constitute a subgroup, as one may directly see by means of the known theorem: A necessary and sufficient condition that exactly three fourths of the operators of a group correspond to their inverses in one of the possible automorphisms of the group is that its group of cogredient isomorphism is the four-group.† Hence the octic group and the quaternion group are the two groups of smallest order which admit automorphisms in which exactly three fourths of the operators correspond to their inverses.

In the present section we shall consider the non-abelian groups of order p^m in which the largest possible number of operators correspond to their inverses in some one automorphism. In particular, we shall prove the theorem: *A necessary and sufficient condition that a group of order* p^m, $p > 2$, *be abelian is that more than* p^{m-1} *of its operators correspond to their inverses in one of its possible automorphisms.* That is, at most p^{m-1} of the operators of any non-abelian group G of order p^m correspond to their inverses in a possible automorphism of G whenever $p > 2$. In what follows it will be assumed that $p > 2$ and that G is non-abelian, unless the contrary is stated. If exactly p^{m-1} of the operators of G correspond to their inverses in an automorphism of G these p^{m-1} operators do not necessarily constitute a subgroup as may be seen by

*Annals of Mathematics, ser. 2, vol. 7 (1906), p. 55.

†MANNING, these Transactions, vol. 7 (1906), p. 233.

considering the automorphisms of the non-abelian group of order p^3 which involves no operator of order p^2.

Suppose that more than p^{m-1} of the operators of G should correspond to their inverses in some automorphism of G. Every invariant operator s would correspond to its inverse in this automorphism. If this were not the case we could consider the quotient group of G with respect to the invariant subgroup generated by s. As not more than $1/p$ of the operators of G which would correspond to an operator of this quotient group could correspond to their inverses, it results that no more than p^{m-1} of the operators of G would correspond to their inverses. This proves that whenever more than p^{m-1} of the operators of a group of order p^m correspond to their inverses in an automorphism of the group then every invariant operator under the group must correspond to its inverse. This theorem applies also to the excluded case where $p = 2$.

To simplify the proof of the theorem that no more than p^{m-1} of the operators of G correspond to their inverses in a possible automorphism, we may consider the quotient group of G with respect to an invariant subgroup of order p, and then the quotient group of this first quotient group with respect to one of its invariant subgroups of order p, etc. By this process we must arrive after a finite number of steps at an abelian quotient group. As more than $1/p$ of the operators of G are supposed to correspond to their inverses in the automorphism under consideration it results that all the operators of this abelian quotient group must correspond to their inverses, while the quotient group which immediately precedes this abelian quotient group has a commutator subgroup of order p. Hence G cannot have an automorphism in which more than p^{m-1} of its operators correspond to their inverses unless a group of order p^β whose commutator subgroup is of order p has an automorphism in which more than $p^{\beta-1}$ of its operators correspond to their inverses.

Suppose that K is such a group of order p^β. Some non-invariant operator s of K must correspond to its inverse in the automorphism under consideration. Let K_1 be the subgroup of order $p^{\beta-1}$ composed of all the operators of K which are commutative with s. As the commutators of K are invariant under K they must correspond to their inverses in the automorphism in question, and hence all the operators of the invariant subgroup generated by s and by these commutators must have the same property. Consider the quotient group of K with respect to this invariant subgroup and observe that not more than $1/p$ of a set of operators of K which correspond to an operator of this quotient group can correspond to their inverses whenever this operator in the quotient group corresponds to operators of K which are not also in K_1.

If K_1 were non-abelian we would repeat the argument of the preceding paragraph as regards one of its non-invariant operators. Hence it remains only to consider the case when K_1 is abelian. As more than $1/p$ of its operators correspond to their inverses in the automorphism under consideration it results that all of these operators must correspond to their inverses. We proceed to prove that none of the operators of K which are not also in K_1 could correspond to its inverse. The group of cogredient isomorphisms of K is assumed to be of order p^2 so that K_1 involves $p^{\beta-2}$ operators which are invariant under K, and K_1 is generated by s and these invariant operators. Let s_0, t represent respectively a commutator of order p and an operator of K which is not also in K_1, and assume that

$$t^{-1}st = s_0 s, \quad \text{or that} \quad tst^{-1} = s_0^{-1} s.$$

Since s_0, s_0^{-1} and s, s^{-1} are two pairs of corresponding operators in the automorphism under consideration, as it was assumed that all the operators of K_1 correspond to their inverses in this automorphism, it results that t cannot correspond to t^{-1}. We have thus arrived at an absurdity by assuming that more than p^{m-1} of the operators of a group of order p^m can correspond to their inverses in some automorphism of the group and hence we have arrived at the theorem announced in the second paragraph of the present section, which may also be stated as follows: *A non-abelian group of order p^m, $p > 2$, has no automorphism in which more than p^{m-1} of its operators correspond to their inverses.* When $p = 2$ there are non-abelian groups of order p^m, for every value of $m > 2$, in which $\frac{3}{2}p^{m-1}$ of the operators correspond to their inverses, as was noted above.

The p^{m-1} operators of a non-abelian group of order p^m which correspond to their inverses in a possible automorphism of the group do not necessarily constitute a subgroup. If they constitute a subgroup this must be abelian but it does not follow that the operators of every abelian subgroup of order p^{m-1} in a non-abelian group of order p^m can correspond to their inverses in a possible automorphism of the group. In fact, it is very easy to see that all the operators of any one of the p cyclic subgroups of order p^{m-1} in the group of order p^m, $p > 2$, which involves operators of order p^{m-1} may correspond to their inverses in automorphisms of this group but the operators of the non-cyclic group of order p^{m-1} cannot all correspond to their inverses in a possible automorphism of this group. That is, *the group of isomorphisms of the non-abelian group of order p^m, $p > 2$, which involves operators of order p^{m-1} contains exactly p^2 operators of order 2 which transform p^{m-1} of the operators of the group into their inverses.*

This special theorem may serve to illustrate the more general developments of the following paragraphs. In the first place, it should be observed that every automorphism of a non-abelian group in which exactly p^{m-1} of the operators correspond to their inverses is affected by an operator of order 2 in the group of isomorphisms of this non-abelian group. This is evident in case the operators which correspond to their inverses generate the entire group. If they do not generate the entire group they constitute an abelian subgroup and each of the remaining operators is transformed into itself multiplied by an operator of this subgroup. As the commutators must all correspond to their inverses, the theorem has been proved. It may be observed that this proof does not necessarily hold when the group of order p^m is abelian, since in this case the commutators need not correspond to their inverses.

Suppose that s_1, s_2 are two non-commutative operators of any group, which correspond to their inverses in some automorphism of the group. From the equations $s_0 = s_2^{-1}s_1^{-1}s_2s_1$, $s_0s_1s_2 = s_1s_2s_0$, we deduce the following:

$$s_2^{-1}s_1s_2 = s_1s_0^{-1}, \qquad s_0^{-1} = s_1s_2s_1^{-1}s_2^{-1}, \qquad s_1^{-1}s_0^{-1} = s_2s_1^{-1}s_2^{-1}.$$

Hence it results that s must correspond to itself in this automorphism. In other words, if the product of two operators, which correspond to their inverses in an automorphism of a group, is commutative with their commutator then this commutator must correspond to itself in this automorphism. Since no operator is transformed into its inverse under the group of cogredient isomorphisms of a group of order p^m, $p > 2$, it results that *if two non-commutative operators of a group of order* p^m, $p > 2$, *correspond to their inverses in an automorphism of the group their commutator cannot correspond to its inverse in this automorphism.*

This theorem is a special case of the theorem, if two operators and their commutator correspond to their inverses in an automorphism of a group this commutator is transformed into its inverse by the product of these two operators. The proof of this more general theorem results immediately from the following considerations. Since s_1, s_2, $s_1^{-1}s_2^{-1}s_1s_2$ correspond to their inverses in some automorphisms of the group involving s_1, s_2 we have that $s_1^{-1}s_2^{-1}s_1s_2$ must correspond to both of the operators $s_2^{-1}s_1^{-1}s_2s_1$ and $s_1s_2s_1^{-1}s_2^{-1}$ in the automorphism in question. That is,

$$(s_1s_2)^{-1}s_2s_1 = s_1s_2(s_2s_1)^{-1}, \qquad \text{or} \qquad (s_1s_2)^2 = (s_2s_1)^2.$$

From the last equations and the fact that each of two operators having a common square transforms into its inverse the product of one of these operators and the inverse of the other * the theorem in question results immediately.

Suppose that G is a non-abelian group of order p^m, $p > 2$, in which p^{m-1} operators correspond to their inverses in an automorphism and these p^{m-1} operators constitute a subgroup H. It has been observed that H is abelian. We proceed to prove that G involves operators of order p which are not contained in H. Let s be any operator of G that is not also in H and let s_1 be the corresponding operator in the given automorphism. From the fact that the commutators of G correspond to their inverses it results that $s_1 = s's$ where s' is an operator of H.

*Archiv der Mathematik und Physik (3), vol. 9 (1905), p. 6.

Since $s_a s$ must correspond to $s_a^{-1} s' s$, s_a being any operator of H, it results that some operators of G which are not also in H must correspond to themselves in the given automorphism. These operators must be of order p since their pth powers correspond to their inverses. Hence it results that *a necessary and sufficient condition that a non-abelian group of order p^m, $p > 2$, has an automorphism in which p^{m-1} operators forming a subgroup correspond to their inverses is that this non-abelian group involves an abelian subgroup of order p^{m-1} which does not include all the operators of order p in the group.*

When the p^{m-1} operators of G which correspond to their inverses do not constitute a subgroup we may consider the smallest non-abelian quotient group of G. As the smallest non-abelian quotient group of any group of order p^m has a commutator subgroup of order p and a group of cogredient isomorphisms of order p^2, it results that the smallest non-abelian quotient group of G is of order p^3 since its generators correspond to their inverses in the given automorphism. As the commutators of order p of this quotient group correspond to themselves, the subgroup of G which corresponds to this commutator subgroup must involve p^{m-3} operators which correspond to their inverses and form an abelian invariant subgroup of G.

This invariant subgroup of order p^{m-3} must be composed of invariant operators under G since the commutator of any one of its operators and any other operator of G which corresponds to its inverse in the given automorphism is the identity, as this commutator corresponds to its inverse in this automorphism. Hence it results that G involves an invariant abelian subgroup of order p^{m-2} which corresponds to the commutator subgroup of its smallest non-abelian quotient group, and that the group of cogredient isomorphisms of G is either of order p^2 or of order p^3. This proves the theorem: *If a group of order p^m, $p > 2$, admits an automorphism in which p^{m-1} operators, which do not constitute a subgroup, correspond to their inverses, the order of its group of cogredient isomorphisms is a divisor of p^3.*

University of Illinois.