ON THE GROUPS OF ORDER $p^m$

WHICH CONTAIN OPERATORS OF ORDER $p^{m-2}$*

BY

G. A. MILLER

Burnside has considered the groups of order $p^m$ (p being any prime) which contain an invariant cyclic subgroup of order $p^{m-2}$.† Those in which a cyclic subgroup of order $p^{m-2}$ is transformed into itself by an abelian group of order $p^{m-1}$ and of type $(m - 2, 1)$ have also been studied.‡ The main object of the present paper is to determine the remaining groups of order $p^m$ ($m > 4$ when $p$ is odd, and $m > 5$ when $p = 2$) which contain a cyclic subgroup of order $p^{m-2}$. As such a subgroup must be transformed into itself by $p^{m-1}$ operators of the group of order $p^m$,§ each of these groups which does not come under one of the cases already considered must include the non-abelian group $H$ of order $p^{m-1}$ which contains $p$ cyclic subgroups of order $p^{m-2}$. The group of isomorphisms ($I$) of $H$ is of order $p^{m-1}(p - 1)$ and contains invariant operators of order $p^{m-3}$ when $p$ is odd and of order $p^{m-4}$ when $p = 2$.||

Let $P_1$ and $P_2$ represent two independent operators of $H$ whose orders are $p^{m-2}$ and $p$, respectively and let $P_1^{p^{m-3}} = P_3$. Suppose also that $P_2$ has been so chosen that $P_2^{-1}P_1P_2 = P_3P_1$. The group of cogredient isomorphisms ($I_2$) of $H$ is of order $p^2$ and of type $(1, 1)$. When $p$ is odd $I$ includes an operator ($t_1$) of order $p$ such that

$$t_1^{-1}P_1t_1 = P_2P_1, \quad t_1^{-1}P_2t_1 = P_2.$$  

Since $t_1$ permutes the $p$ cyclic subgroups of order $p^{m-2}$ in $H$ cyclically, while some of the operators of $I_2$ are commutative with each operator of only one of these subgroups, the group generated by $I_2$ and $t_1$ is the non-abelian group of

---

* Presented to the Society (Chicago) January 3, 1902. Received for publication December 2, 1901.

† Burnside, Theory of groups of finite order, 1897, p. 75.
|| With respect to the non-cyclic group of order $p^2$, when $p$ is odd, or $p^3$, when $p$ is even, all the operators of a division have the same $p$th power or $p^2$th power respectively. Cf. Bulletin of the American Mathematical Society, vol. 7 (1901), p. 350; J. W. Young, Transactions of the American Mathematical Society, vol. 3 (1902), p. 189.
order $p^3$ which contains no operators of order $p^2$. As this group contains only $p$ of the $p^{m-3}$ invariant operators of $I$ it follows that $I$ contains the non-abelian subgroup of order $p^{m-1}$ which includes no operator of order $p^{m-2}$ but has an invariant operator of order $p^{m-3}$, whenever $p$ is odd. This subgroup of order $p^{m-1}$ is invariant under $I$ according to Sylow's theorem. It is not difficult to see that the same group is invariant under the group of isomorphisms of the abelian group of type $(m - 2, 1)$.

§1. Determination of the groups when $p$ is even.

When $p = 2$, $I$ is of order $2^{m-1}$ and its subgroup $(I_2)$ which is composed of the group of cogredient isomorphisms of $H$ is the four-group. It includes an operator $t_2$ of order 2 such that

$$t_2^{-1}P_1t_2 = P_1^{-1}, \quad t_2^{-1}P_2t_2 = P_3P_2.$$ 

This operator is commutative with each operator of $I_2$ since it is evidently commutative with the operator ($t'_2$) which transforms $P_1$ into itself and $P_2$ into $P_3P_2$. Hence $I$ contains the abelian group of type $(m - 4, 1, 1)$ and all the operators of this subgroup transform $P_1$ into a power of itself. An additional generator of $I$ is $t_1$ as defined above. It should however be observed that $t_1$ is commutative with only $p^{m-3}$ operators of $H$ when $p = 2$, while it is commutative with $p^{m-2}$ of these operators when $p$ is odd.

It was observed above that $I$ contains an invariant operator of order $p^{m-4}$ when $p = 2$. Let $t_3$ represent the operator of order 2 which is a power of this invariant operator. From the properties mentioned above it follows that

$$t_3^{-1}t'_2t_1 = t_3t'_2, \quad t_3^{-1}t_1t_2 = t_1.$$

Hence, when $p = 2$, $I$ contains a subgroup of type $(m - 4, 1)$ which is composed of its invariant operators. It is completely defined by the fact that it contains such a subgroup and two non-commutative operators $(t_1, t'_2)$ of order 2 with properties noted above.

We proceed to determine all the groups of order $2^m$ which contain $H$ and permute its cyclic subgroups of order $2^{m-2}$. Such a group must transform $H$ according to a subgroup of order 8 in $I$, which includes the group of cogredient isomorphisms of $H$. As all the operators of orders two and four contained in $I$ are included in its subgroup of order 32 there are just four such subgroups of order 8 and each of them is simply isomorphic with the octic group.† They are generated by $I_2$ and the following four operators of order two respectively:

$$t_1, \quad t_1t_2, \quad t_1t_2t_4, \quad t_1t_2t'_2t_4,$$

* These equations may be verified by observing that each member transforms $P_1$ and $P_4$ in the same way.

where $t_4$ is an operator of order 4 in the group generated by an operator of order 8 in $I$.

The group $(G_1)$ generated by $H$ and $t_1$ contains just $2^{m-1}$ invariant operators and is conformal with the abelian group of type $(m - 2, 1)$; i.e., it contains $2^{m-1}$ operators of order $2^a$ ($1 < a < m - 1$) and 7 of order 2. Its four cyclic subgroups of order $2^{m-2}$ involve, in pairs, the two cyclic subgroups of order $2^{m-3}$ contained in $H$. It follows directly from a known theorem that there is no other group which transforms $H$ in the way in which $G_1$ transforms it.*

The group $(G_2)$ generated by $H$ and $t_1t_2$ contains only 2 invariant operators. Its operators not contained in $H$ are composed of $2^{m-3}$ operators of order 2 and $3.2^{m-3}$ of order 4. Since $P_1^{-2}t_1t_2P_1^2 = P_3P_1^{-4}t_1t_2$ there can be no other group which transforms $H$ in the same manner as $t_1t_2$ does. Let $G_2'$ represent the group generated by $H$ and $t_1t_2t_4$. Its $2^{m-3}$ invariant operators are generated by $P_1^2$ and it is conformal with $G_1$. As it contains an abelian subgroup of type $(m - 2, 1)$ it is not necessary to consider this group here. There is another group $(G_3)$ which transforms $H$ in the same way as $G_2'$ does and contains four cyclic subgroups of order $2^{m-2}$. In $G_3$ all of these contain the same subgroup of order $2^{m-3}$ while this is not the case in $G_2'$. Moreover, $G_3$ contains no operator of order 2 besides those in $H$ and it has no abelian subgroup of type $(m - 2, 1)$.

It remains to examine the case when $H$ is transformed in the same way as $t_1t_2t_2t_4$ transforms it. The group $(G_4)$ generated by $H$ and $t_1t_2t_2t_4$ contains only two invariant operators. Besides $H$ it contains $2^{m-2}$ operators of each of the orders 2 and 8. In the other group $(G_5)$ which transforms $H$ in the same manner as $G_4$ does, there are $2^{m-2}$ operators of each of the orders 4 and 8 besides $H$. There cannot be more than two such groups, since $H$ has only two invariant operators under $G_4$. Hence there are just five groups of order $2^m$ which contain operators of order $2^{m-2}$ and in which no cyclic subgroup of this order is either invariant or transformed into itself by an abelian group of order $2^{m-1}$. It may be of interest to observe that the group of isomorphisms of $H$ when $p = 2$ is identical with that of the abelian group of type $(m - 2, 1)$.

§ 2. Determination of the groups when $p$ is odd.

When $p > 2$ the two sets of $p$ conjugate subgroups in $H$ are permuted by $I$ according to an intransitive substitution group of order $p^2(p - 1)$, which is obtained by establishing a $(p, p)$ isomorphism between two metacyclic groups of degree $p$, just as in the case of the abelian group of type $(m - 2, 1)$.$\dagger$

* Transactions of the American Mathematical Society, vol. 2 (1901), p. 265. The latter part of this theorem clearly assumes that $p$ is odd. It remains true, however, when $v_1$ is a power of $r_1$ and the order of $r_1$ is greater than 4. The general method explained in §2 of the article cited is employed in the present article.

† l. c., p. 261.
groups under consideration must transform the operators of $H$ according to a subgroup of $I$, which includes $I_2$, is of order $p^3$, and permutes the $p$ cyclic subgroups of highest order in $H$. It is evident that there are just $p$ such subgroups. They are non-abelian and $p - 1$ of them include operators of order $p^2$.

To prove that these $p - 1$ subgroups are conjugate under $I$ it seems desirable to employ some additional equations, which we proceed to develop. Let $t$ represent an invariant operator of order $p^{m-3}$ in $I$ and let $t^{-1} = t$. It may be assumed without loss of generality that $t^{-1}P_1t_4 = P_1^{1+p^{-4}}$ and $t^{-1}P_2t_4 = P_2$. There are $p(p - 1)$ conjugates of $t_1t_4$ under $I$. They are

$$t^{-1}_a t_1 t_4 t^{-1}_b \quad (a = 1, 2, \ldots, p - 1; \beta = 1, 2, \ldots, p)$$

It follows that

$$(A) \quad (t^{-1}_a t_1 t_4 t^{-1}_b)^{-1}P_1^{a}(t^{-1}_a t_1 t_4 t^{-1}_b) = P_2^{P_1^{a+np^{-4}+\beta p^{-3}}}.$$

On the other hand

$$(B) \quad (t_1 t_4)^{-n}P_1^{a}(t_1 t_4)^n = P_2^{P_1^{(1+p^{-4})n+np^{-3}a(a-1)/2}}$$

The right hand members of $(A)$ and $(B)$ are the same only if

$$n = 1 + \beta p, \quad a = 1.$$

Hence not more than $p$ of the $p(p - 1)$ conjugates of $t_1t_4$ are powers of $t_1t_4$, i.e., the operators $t_{a\beta}$ transform $\{t_1t_4\}$ into at least $p - 1$ conjugate groups. It remains to observe that only one of these groups can be in any one $I_3$ of the $p - 1$ subgroups of order $p^3$ under consideration.

The last fact follows readily from the isomorphism between $I$ and the given intransitive substitution group of order $p^3(p - 1)$. In this isomorphism $I_3$ corresponds to the subgroup of order $p^2$ and $\{t_1t_4\}$ corresponds to an invariant subgroup of order $p$. The $I_3$ which includes $t_1t_4$ can therefore involve only $p$ of the conjugates of $t_1t_4$ under $I$. In other words, the conjugates of $t_1t_4$ are found in $p - 1$ conjugates of $I_3$.

Since these $p - 1$ subgroups of order $p^3$ are conjugate under $I$ it is necessary to consider only two cases, viz.: the one in which $H$ is transformed according to one of these $p - 1$ subgroups and the other in which $H$ is transformed by the groups in question according to the subgroup of order $p^3$ in $I$, which includes no operator of order $p^2$. In the former case there are only $p^{m-4}$ invariant operators while each of the groups which belongs to the latter contains $p^{m-3}$ such operators. We proceed to prove that there is only one group $(G_1)$ which comes under the former case, while there are two $(G_2, G_2')$ which come under the
latter. It is not difficult to see that the last one of these groups contains a sub-
group of type \((m - 2, 1)\).

Let \(t_6\) be an operator of order \(p^2\) which transforms \(H\) in the same way as \(t_1 t_4\)
does and suppose that it has been so chosen that \(t_6^2 = P_2\). The group generated
by \(H\) and \(t_6\) contains no operator of order \(p\) besides those of \(H\). That this is
the only group in question which transforms \(H\) in the same way as \(G_1\) does may
be proved in exactly the same manner as the theorem to which reference is made
in the last footnote. It may be observed that \(G_1\) is conformal with the abelian
group of type \((m - 2, 2)\).

The group \((G'_2)\) generated by \(t_i\) and \(H\) is conformal with the abelian group
of type \((m - 2, 1, 1)\). In fact, it includes the abelian group of type
\((m - 3, 1, 1)\) since \(t_i\) is commutative both with \(P_1^2\) and with \(P_2\). The other
group \(G'_2\), which transforms \(H\) in the same manner as \(G_2\) does, may be ob-
tained by the method mentioned in the last footnote. Since it includes the
abelian group of type \((m - 2, 1)\) it will not be considered here. Hence, there
are two and only two groups of order \(p^m\) \((p > 2 \text{ and } m > 5)\) which include
operators of order \(p^{m-2}\) without containing either an invariant cyclic subgroup
of this order or an abelian subgroup of type \((m - 2, 1)\). These two groups
are conformal respectively with the abelian groups of type \((m - 2, 2)\) and of
type \((m - 2, 1, 1)\). When \(m = 5\) the group \(G_1\) evidently contains an invariant
cyclic subgroup of order \(p^{m-2}\); hence there is only one group of order \(p^5\) \((p > 2)\)
which contains operators of order \(p^3\) without containing either an invariant cyclic
subgroup of this order or the abelian group of type \((3, 1)\).