DETERMINATION OF ALL THE PRIME POWER GROUPS CONTAINING ONLY ONE INVARIANT SUBGROUP OF EVERY INDEX WHICH EXCEEDS THIS PRIME NUMBER*

BY

H. A. BENDER

The groups of order p^m, p being any prime number, which satisfy the following conditions have been determined: (1) $m < 7$†, (2) those which contain operators of order p^α ($\alpha > m-4$)‡, (3) those containing the abelian group of order p^{m-1} and of type (1, 1, 1, $\cdots$)§, (4) those containing exactly $p+1$ abelian subgroups of order p^{m-1}||, (5) those containing exactly p cyclic subgroups of order p^α¶. The present paper is devoted to a complete determination of the groups of order p^m which satisfy the condition that each group contains only one invariant subgroup of every index which exceeds p. There exists at least one such group for every value of m and p, viz., the cyclic group of order p^m. This is, however, the only abelian group which satisfies the above condition.

Let G be a non-cyclic group of order p^m, p being any prime number, which contains but one invariant subgroup of every index which exceeds this prime number. Since G is non-cyclic it involves more than one subgroup of index p. The cross cut of any two such subgroups is invariant under G and hence is the invariant subgroup of index p^2. Since G contains but one invariant subgroup of index p^2 this cross cut must include all the commutators of G as well as the pth powers of all its operators. From this it follows that the quotient group corresponding to this cross cut is non-cyclic, and hence any quotient group of G whose order exceeds p must be non-cyclic.

* Presented to the Society, April 18, 1924.

† $m = 3$, 4, O. Hölder, Mathematische Annalen, vol. 43 (1893), p. 371. $m = 5$, G. Bagnera, Annali di Matematica, ser. 3, vol. 1 (1898), p. 137, and vol. 2 (1899), p. 263. $m = 6$, M. Potron, *Thèses*, Gauthier-Villars, Paris, 1904.

‡ $\alpha = m-1$, $m-2$, W. Burnside, *Theory of Groups of Finite Order*, 1897, p. 75. $\alpha = m-2$, G. A. Miller, these Transactions, vol. 2 (1901), p. 259, and vol. 3 (1902), p. 383. $\alpha = m-3$ ($p > 2$), L. I. Neikirk, these Transactions, vol. 6 (1905), p. 316. $\alpha = m-3$ ($p = 2$), Miss McKelden, American Mathematical Monthly, vol. 13 (1906), p. 121.

§ G. A. Miller, Bulletin of the American Mathematical Society, vol. 8 (1901), p. 391.

|| G. A. Miller, Bulletin of the American Mathematical Society, vol. 13 (1906), p. 171.

¶ G. A. Miller, these Transactions, vol. 7 (1906), p. 228.

If G contains but one invariant subgroup of index p^2 this subgroup must be the commutator subgroup of G, otherwise it would include the commutator subgroup and the commutator quotient group would be non-cyclic abelian and of a larger order than p^2. Since this quotient group would then contain more than one invariant subgroup of index p^2, it follows that G would contain more than one invariant subgroup of index p^2, contrary to hypothesis. Moreover, if the commutator subgroup of a group of order p^m is of index p^2 the group contains only one invariant subgroup of this index, since the commutator subgroup is found in every such subgroup.

We shall represent the invariant subgroups of orders $1, p, p^2, p^3, \cdots, p^{m-2}$ by $G_0, G_1, G_2, G_3, \cdots, G_{m-2}$ respectively, and the operators of G_α not in $G_{\alpha-1}$ by the major co-set $G_{\alpha-1}s_\alpha$*. Since an operator in the major co-set $G_1 s_2$ has but p conjugates there are p^{m-1} operators commutative with G_2, and we shall represent the subgroup composed of these operators by G_{m-1}.

It has been shown that G_{m-2} is the commutator subgroup of G. The second commutator subgroup is a subgroup generated by all the commutators of the group which have for one element a commutator while the other element is an arbitrary element of the group†. It is evident that this second commutator subgroup is invariant under G and hence is one of the invariant subgroups. Suppose $G_{m-\alpha}$ to be one of the successive commutator subgroups and suppose the commutators of G, which have for one element an operator of $G_{m-\alpha}$ while the other element is an arbitrary element of G, to generate the invariant subgroup $G_{m-\alpha-\beta}$. The quotient group of G with respect to $G_{m-\alpha-\beta}$ will at least contain a central of order p^β. Hence if β is greater than one, G will contain more than one invariant subgroup of order $p^{m-\alpha-\beta+1}$. From this it follows that the αth commutator subgroup is the invariant subgroup $G_{m-\alpha-1}$ $(\alpha = 1, 2, 3, \cdots, m-2)$.

If the $(m-2)$th commutator subgroup is of order p, it implies that the first commutator subgroup is of index p^2, the second of index p^3, etc. If a group which has only one invariant subgroup of order p^α, which is also one of the successive commutator subgroups, had more than one invariant subgroup of order $p^{\alpha-1}$, then the next successive commutator subgroup would be contained in each of these invariant subgroups, and hence would be of a lower order than $p^{\alpha-1}$. Hence the following theorem:

A necessary and sufficient condition that a group G of order p^m, p being any prime number, contain only one invariant subgroup of every index greater than p is that its $(m-2)$th commutator subgroup be of order p.

As an interesting system composed of groups of order p^m such that

*American Journal of Mathematics, vol. 45 (1923), p. 231.

† W. B. Fite, these Transactions, vol. 7 (1906), p. 61.

each group contains only one invariant subgroup of each of the orders $p, p^2, p^3, \cdots, p^{m-2}$, we may note the Sylow subgroup of order p^{p+1} contained in the symmetric group of degree p^2. It is obvious that such a Sylow subgroup contains a subgroup of order p^p which is the direct product of p regular cyclic groups of order p. If the generators of these p regular groups are represented by $s_1, s_2, s_3, \cdots, s_p$, respectively, and if t represents the substitution of order p and of degree p^2 which satisfies the condition

$$t^{-1}s_1t = s_2, \quad t^{-1}s_2t = s_3, \quad \cdots, \quad t^{-1}s_pt = s_1,$$

it is evident that t and the said p generators give rise to the following $p-1$ commutators:

$$s_1^{-1}s_2, \quad s_2^{-1}s_3, \quad \cdots, \quad s_{p-1}^{-1}s_p.$$

These commutators generate a group of order p^{p-1} which is therefore the only invariant subgroup of index p^2 contained in the group. The second commutator subgroup is of order p^{p-2}, etc. It follows from the preceding theorem that the Sylow subgroup of the symmetric group of degree p^2 contains only one invariant subgroup of each of the orders $p, p^2, p^3, \cdots, p^p$.

The operators of G which transform the operators of $G_\alpha (\alpha < m)$ into themselves multiplied by operators in $G_{\alpha-\beta}$ constitute an invariant subgroup of G. For suppose t_1 to be such an operator, and let s be an operator of G_α and t any operator of G, and $t^{-1}st = s's$; then

$$(tt_1t^{-1})^{-1}s(tt_1t^{-1}) = tt_1^{-1}s'st_1t^{-1} = ts'_{\alpha-\beta}s's_{\alpha-\beta}st^{-1}.$$

It follows from this that all the conjugates under G of t_1 transform the operators of G_α into themselves multiplied by operators in $G_{\alpha-\beta}$ and hence they constitute an invariant subgroup of G.

Since G_{m-1} is commutative with G_2 it transforms the operators of the major co-set G_1s_2 into themselves multiplied by operators in the second major co-set which precedes. Let us suppose the major co-set $G_{\alpha-1}s_\alpha$ to be the first in which the operators are not transformed into themselves multiplied by operators in at least the second major co-set which precedes. It is assumed that G_{m-1} transforms the operators of $G_{\alpha-1}$ into themselves multiplied by operators in $G_{\alpha-3}$, and that some of the operators of G_{m-1} transform the operators in the major co-set $G_{\alpha-1}s_\alpha$ into themselves multiplied by operators in the major co-set $G_{\alpha-2}s_{\alpha-1}$.

All the operators of G which transform the operators of G_α into themselves multiplied by operators in $G_{\alpha-3}$ form an invariant subgroup of G, say H. Suppose G_{m-1} to contain an operator t_1 which transforms the operators of the major co-set $G_{\alpha-1}s_\alpha$ into themselves multiplied by

operators in the major co-set $G_{\alpha-3}s_{\alpha-2}$. Evidently the pth power of t_1 will transform the operators of G_α into themselves multiplied by operators in $G_{\alpha-3}$, and hence the pth power of t_1 is in H. The group generated by H and t_1 will contain all the operators of G which transform the operators of G_α into themselves multiplied by operators in $G_{\alpha-2}$. For suppose t_2 transforms s_α into itself multiplied by some operator in the major co-set $G_{\alpha-3}s_{\alpha-2}$; then there exists some power of t_1 which will transform s_α into itself multiplied by an operator in the co-set containing the inverse of the commutator of t_2 and s_α. The product of t_1 to this power and t_2 will transform s_α into itself multiplied by an operator in $G_{\alpha-3}$ and hence this product is in H. Thus $H \cdot t_1$ contains all the operators of G which transform the operators of G_α into themselves multiplied by operators in $G_{\alpha-2}$.

In the same manner it can be shown that all the operators which transform the operators of G_α into themselves multiplied by operators in $G_{\alpha-1}$ will generate an invariant subgroup whose order is p times the order of $H \cdot t_1$, and as we have seen this must be G itself. Hence we have shown that G_{m-1} can not contain an operator which will transform s_α into itself multiplied by an operator in the major co-set $G_{\alpha-2}\, s_{\alpha-1}$ and at the same time contain another operator which will transform s_α into itself multiplied by an operator of the major co-set $G_{\alpha-3}\, s_{\alpha-2}$.

It should be noted that the group generated by the commutators of G which have for their elements operators of any two invariant subgroups is invariant under the original group G. From this and what precedes it follows that *the operators of G_{m-1} transform the operators of G_α into themselves multiplied by operators in $G_{\alpha-2}$ ($\alpha = 2, 3, 4, \cdots, m-2$).* Furthermore, *each operator of the major co-set $G_{m-1}\, s_m$ transforms the operators of the major co-set $G_{\alpha-1}\, s_\alpha$ into themselves multiplied by operators in the major co-set $G_{\alpha-2}\, s_{\alpha-1}$ ($\alpha = 1, 2, 3, \cdots, m-1$).* Thus it follows that *whenever a non-cyclic group of order p^m, p being any prime number, contains only one invariant subgroup of every index greater than p, it must also contain a subgroup of index p which includes all of its operators whose orders exceed p^2, and the pth powers of every operator not in this subgroup must be in the invariant subgroup of order p.* It should be noted that every operator in the commutator subgroup is a commutator.

Let G_β be the largest invariant abelian subgroup of G. It is evident that the operators of the major co-set $G_\beta\, s_{\beta+1}$ must be commutative with the operators of some subgroup of G_β, say $G_\alpha (\alpha < \beta)$, but not commutative with the operators of the major co-set $G_\alpha\, s_{\alpha+1}$. The commutators formed by the operators of $G_{\alpha+1}$ and $G_{\beta+1}$ are in G_α and hence are invariant under $G_{\beta+1}$. Suppose

$$s_{\beta+1}^{-1} s_{\alpha+1} s_{\beta+1} = s_1 s_{\alpha+1},$$

where s_1 is some operator of G_α; then

$$s_{\beta+1}^{-p} s_{\alpha+1} s_{\beta+1}^{p} = s_1^{p} s_{\alpha+1}.$$

Since the pth power of $s_{\beta+1}$ is in G_β it must be commutative with $s_{\alpha+1}$ and hence s_1 must be an operator of order p. Furthermore each operator of the co-set containing $s_{\beta+1}$ transforms every operator of the co-set containing $s_{\alpha+1}$ in this manner. Hence the commutators formed by the operators of $G_{\alpha+1}$ and $G_{\beta+1}$ generate the invariant subgroup of order p.

Again let us consider the commutator

$$s_{\beta+1}^{-1} s_{\alpha+1}^{-1} s_{\beta+1} s_{\alpha+1} = s_1,$$

and suppose t to be an operator of the major co-set $G_{m-1} s_m$ such that $t^{-1} s_i t = s_{i-1} s_i$ $(i = 1, 2, 3, \ldots, m-1)$; then

$$t^{-1} s_1 t = t^{-1} s_{\beta+1}^{-1} s_{\alpha+1}^{-1} s_{\beta+1} s_{\alpha+1} t = s_{\beta+1}^{-1} s_\beta^{-1} s_{\alpha+1}^{-1} s_\alpha^{-1} s_\beta s_{\beta+1} s_\alpha s_{\alpha+1} = s_1.$$

Let us now consider the commutator

$$s_{\beta+1}^{-1} s_{\alpha+2}^{-1} s_{\beta+1} s_{\alpha+2} = s_2$$

where s_2 is some operator of $G_{\alpha+1}$. Transforming by t,

$$t^{-1} s_2 t = s_{\beta+1}^{-1} s_\beta^{-1} s_{\alpha+2}^{-1} s_{\alpha+1}^{-1} s_\beta s_{\beta+1} s_{\alpha+1} s_{\alpha+2} = s_{\beta+1}^{-1} s_{\alpha+1}^{-1} s_{\beta+1} s_2 s_{\alpha+1} = s_1 s_2.$$

Thus it follows that the operators of the major co-set $G_\beta s_{\beta+1}$ transform the operators of the major co-set $G_{\alpha+1} s_{\alpha+2}$ into themselves multiplied by operators in the major co-set $G_1 s_2$.

Since this property must hold for the quotient group, and if we form the successive quotient groups with respect to the invariant subgroup of order p, it follows that the operators of the major co-set $G_\beta s_{\beta+1}$ transform the operators of the major co-set $G_{\alpha+\rho} s_{\alpha+\rho+1}$ into themselves multiplied by operators in the major co-set $G_\rho s_{\rho+1}$ $(\rho = 0, 1, 2, \cdots, \beta - \alpha - 1)$. That is, the operators of the major co-set $G_\beta s_{\beta+1}$ transform each operator of G_β into itself multiplied by an operator in the αth major co-set which precedes the major co-set containing this operator.

The transformation of any operator s_ρ of G_β by the pth power of t is

$$t^{-p} s_\rho t^{p} = s_{\rho-p} s_{\rho-p+1}^{p} \cdots s_{\rho-r-1}^{p(p-1)\cdots(p-r)/(r+1)!} \cdots s_{\rho-1}^{p} s_\rho,$$

where the elements with zero or negative subscripts are unity. Since the pth power of t is commutative with every operator of G, and if we let s_ρ represent successively an operator in the major co-sets $G_1 s_2$, $G_2 s_3$, $\cdots$ $\cdots$, $G_{p-1} s_p$ $(\beta \geqq p)$ it follows that all the operators of G_{p-1}, except identity, are of order p. If s_ρ is an operator in the major co-set $G_p s_{p+1}$ $(\beta \geqq p+1)$ it follows that $s_1 s_p^p = 1$, and hence all the operators of the major co-set $G_{p-1} s_p$ are of order p^2 and have their pth powers in G_1. Since this property must hold for the successive quotient groups with respect to the invariant subgroup of order p, it follows that all the operators of $G_{2(p-1)}$ not in G_{p-1} are of order p^3, and so on, and the pth power of each operator is in the $(p-1)$th major co-set which precedes the major co-set containing this operator. Hence it follows that $\alpha \geqq \beta - (p-1)$.

Let us now assume that G does not contain an invariant abelian subgroup of index p^2.

Since all the operators of G commutative with the operators of $G_{\alpha+1}$ form an invariant subgroup of G, it follows that the operators of the major co-set $G_{\beta+1} s_{\beta+2}$ can not be commutative with $G_{\alpha+1}$. Let us suppose the operators of $G_{\beta+2}$ to be commutative with the operators of G_δ. As before the commutators formed by the operators of $G_{\delta+1}$ and $G_{\beta+2}$ generate the invariant subgroup of order p.

If $\delta = \alpha$, then some operator of the major co-set $G_{\beta+1} s_{\beta+2}$ would transform $s_{\alpha+1}$ into itself multiplied by s_1^{-1} and the product of this operator and $s_{\beta+1}$ would be commutative with $G_{\alpha+1}$. The pth power of this operator is in G_β and hence would with G_β generate an invariant subgroup of order $p^{\beta+1}$ which differs from $G_{\beta+1}$ contrary to hypothesis, and hence $\delta < \alpha$.

In general we may suppose G_δ to be the largest invariant abelian subgroup of G composed of operators which are commutative with every operator of $G_\sigma (\sigma > \beta)$; then the operators of the major co-set $G_{\sigma-1} s_\sigma$ transform the operators of the major co-set $G_\delta s_{\delta+1}$ into themselves multiplied by operators in G_1. Let us assume the central of $G_{\sigma+1}$ to be $G_{\delta-\gamma}$ $(\gamma > 0)$, and suppose

$$s_{\sigma+1}^{-1} s_{\delta-\gamma+2}^{-1} s_{\sigma+1} s_{\delta-\gamma+2} = s.$$

Transforming by t, and since s_σ is not commutative with $s_{\delta-\gamma+2}^{-1}$ for $\gamma = 1$ but is commutative for $\gamma > 1$, then for $\gamma > 1$

$$t^{-1} s t = s_1 s$$

and hence s is in the major co-set $G_1 s_2$.

It follows in either case from the successive quotient groups that the central of $G_{\sigma+1}$ is contained in the central of G_σ and the two are distinct,

and that all the operators in the major co-set $G_\sigma s_{\sigma+1}$ will transform every operator of G_σ into itself multiplied by an operator in the δth major co-set which precedes the major co-set containing this operator ($\sigma = \beta+1, \beta+2, \cdots, m-2$). Furthermore, the commutator subgroup of G_{m-1} must be composed of operators of order p, and it can at most be of order p^{p-2}.

Let us now suppose $\beta < p$, and suppose the operators of the major co-set $G_\sigma s_{\sigma+1}$ to be of order p^2 ($\sigma < p$, $\sigma < m-1$). It would then be possible to construct a group having an invariant abelian subgroup of order p^p, and having G_σ for an invariant subgroup of its quotient group with respect to the invariant subgroup of order $p^{p-\beta}$, and hence the pth powers of the operators of the major co-set $G_{p+\sigma-\beta} s_{p+\sigma-\beta+1}$ would be at most in the σth major co-set which precedes, and, as we have seen, this must be the $(p-1)$th major co-set which precedes. Hence the properties established above hold for any value of β.

The index of the largest invariant abelian subgroup of G can not exceed $p^{(p+1)/2}$, and the order of this subgroup can not be less than $p^{(m+1)/2}$ for m odd, or $p^{(m+2)/2}$ for m even.

If $m > p$, then G_{m-1} can be generated by $p-1$ independent generators which are such that the cyclic groups they generate have only the identity in common, and the ratio of the orders of any two of these independent generators is either 1 or p. If G is of a lower order, then all the independent generators are of order p.

Since

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

it follows that all the operators of the major co-set $G_{m-2} t$ have the same pth power, and hence $(t s_{\alpha-1})^p = t^p$ whenever $s_{\alpha-1}$ is preceded by $p-3$, or less, independent generators

$$(t s_{m-1})^p = t^p t^{-(p-1)} s_{m-1} t^{p-1} \cdots t^{-1} s_{m-1} t s_{m-1} = t^p s s_{m-p} s_{m-p+1}^p \cdots s_{m-1}^p.$$

Since this is a product of operators in G_{m-p}, and s_{m-p+1} is an independent generator, it follows that t can be so chosen that this product is either the identity or an operator of order p in G_1, except in the case where s_{m-p} is the only operator in this major co-set, i.e., for $m=3$ and $p=2$. Hence for a given m and p the order of every operator of G_{m-1} is determined. For $m > p$ there are three groups containing the same subgroup of order p^{m-1}, either all the operators of the major co-set $G_{m-1} s_m$ are of order p, or all are of order p^2, or one pth of them are of order p and the remaining operators are of order p^2. For $m \leq p$ there are only two

such groups, either all the operators of this major co-set are of order p, or all the operators are of order p^2.

We shall now consider all the possible subgroups of order p^{m-1} $(m > p+1)$. If G_{m-1} is abelian there is only one possible subgroup of order p^{m-1}. If G_{m-2} is abelian, then the central of G_{m-1} can be either G_{m-p}, G_{m-p+1}, $\cdots$, or G_{m-3}. Hence there are $p-2$ subgroups of order p^{m-1} containing an invariant abelian subgroup of order p^{m-2}, without containing an abelian subgroup of a larger order. If G_{m-3} is abelian, then the central of G_{m-2} can be either G_{m-p+1}, G_{m-p+2}, $\cdots$, or G_{m-4}, and the number of groups of order p^{m-1} is $1, 2, 3, \cdots, p-4$, respectively $(p > 3)$. This process may be continued, and hence it follows that the number of subgroups of order p^{m-1} containing an invariant abelian subgroup whose order is exactly p^{m-r} is the sum of $p-2(r-1)$ terms of the figurate numbers of the $(r-1)$th order. Hence the number of subgroups of order p^{m-1} is

$$1+(p-2)+\frac{(p-3)(p-4)}{2!}+\frac{(p-4)(p-5)(p-6)}{3!}+\cdots$$
$$\cdots+\frac{\left(p-\frac{p+1}{2}\right)\cdots 1}{\left(\frac{p-1}{2}\right)!}.$$

The sum of this series is the $(p+1)$th term of the Pisano recurrent sequence*. This follows immediately, for if to the first term of the series for p equals $p-2$ we add the second term of the series for p equals $p-1$, etc., there results the series for p equals p. *Hence the number of non-abelian groups of order p^m containing only one invariant subgroup of every index which exceeds this prime number is*

$$\frac{3}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^p-\left(\frac{1-\sqrt{5}}{2}\right)^p\right] \quad (m>p+1),$$

$$\frac{3}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{m-2}-\left(\frac{1-\sqrt{5}}{2}\right)^{m-2}\right] \quad (m=p+1),$$

$$\frac{2}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{m-2}-\left(\frac{1-\sqrt{5}}{2}\right)^{m-2}\right] \quad (m<p+1),$$

with the single exception $m=3$ and $p=2$.

* L. E. Dickson, *History of the Theory of Numbers*, vol. 1, chapter xvii.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.