position and the number of the maxima and minima of the curve, and shows that all types actually exist. For example: for all $\delta > 0$ sufficiently small, the curve

$$y = (x + \delta i)(x - \delta i)(x + 1 + \delta^3 i)(x + 1 - \delta^3 i) \cdot$$
$$(x + 1 + \delta^2 + \delta^5 i)(x + 1 + \delta^2 - \delta^5 i)(x + 1 + \delta^2 + \delta^4)$$

has six extremes which, read for decreasing values of x, are arranged so that the first minimum of y is higher than the second maximum, and the second minimum higher than the third maximum.

E. J. MOULTON,
Acting Secretary.

FORM OF THE NUMBER OF SUBGROUPS OF PRIME POWER GROUPS.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society September 3, 1919.)

§1. *Introduction.*

IT is known that the number of the subgroups of order p^α, p being any prime number, which are contained in any group G is always of the form $1 + kp$. When $k = 0$ for every possible pair of values for α and p the group G must be cyclic and vice versa. There are two infinite systems of groups of order p^m containing separately $p + 1$ subgroups of every order which is a proper divisor of the order of the group, viz., the abelian groups of type $(m - 1, 1)$ and the conformal non-abelian groups.

These two infinite systems are composed of all the groups of order p^m involving separately exactly $p + 1$ subgroups of every order which is a proper divisor of p^m. Moreover, if a group of order p^m, $p > 2$, contains exactly $p + 1$ subgroups of each of the two orders p and p^2 it must contain exactly $p + 1$ subgroups of every order which is a proper divisor of the order of the group, and if a group of order 2^m contains exactly three subgroups of each of the orders 2, 4 and 8 it must also contain exactly three subgroups of every other order which is a proper divisor of 2^m.

The proof of the former part of this theorem may be based upon the fact that when $m > 3$ such a group has to contain an invariant abelian subgroup of order p^3 and of type (2, 1). The order of each of the remaining operators must be divisible by p^3 and the number of the operators of order p^3 is equal to $p^4 - p^3$. Hence G contains exactly p cyclic subgroups of order p^3 and only one non-cyclic subgroup of this order. If $m > 4$, this subgroup of order p^4 must again be abelian, and by successive similar steps we note that G must contain operators of order p^{m-1}.

When $p = 2$ it is possible to extend the abelian group of order 8 and of type (2, 1) by 24 operators of order 4 so as to obtain a group of order 32. In this case the preceding reasoning fails. If it is assumed, however, that G contains exactly three subgroups of order 8 in addition to the three subgroups of each of the orders 2 and 4 it may be proved as in the preceding paragraph that G contains only $p = 2$ cyclic subgroups of order 16, etc. The theorem stated in the second paragraph has therefore been established. This theorem may be compared with the well known theorem, due to W. Burnside, which affirms that every group of order p^m, $p > 2$, which contains only one subgroup whose order is a proper divisor of p^m is cyclic.

Another simple condition which implies that a group G of order p^m is cyclic is that all the operators of G which transform into itself one of its subgroups constitute a cyclic subgroup of G. In other words, a necessary and sufficient condition that a prime power group is cyclic is that it contains at least one subgroup whose normaliser is cyclic. This theorem results directly from the fact that every non-invariant subgroup of a group of order p^m is transformed into itself by at least p of its conjugates including itself. In the following section it will be proved that a necessary and sufficient condition that an abelian group of order p^m is cyclic is that the number of its subgroups of order p^α, $0 < \alpha < m$, is of the form $1 + kp^2$ for at least one value of α.

§2. *Abelian Groups.*

Let H represent a subgroup of order p^α contained in an abelian group G of order p^m and suppose that H has been so selected that its invariants are as small as possible when the order of H is fixed. It may happen that H is composed of all the operators of G whose orders do not exceed the largest invariant of H. If this is the case, G contains only one subgroup of order p^α having the same invariants as H. If it is not the case, we proceed to prove that the number of subgroups of G which have the same invariants as H must be of the form $1 + p + kp^2$.

Let $p^{\alpha+\lambda}$ represent the order of the subgroup of G composed of all its operators whose orders divide the largest invariant of H. If H has β such largest invariants, the β independent generators of H whose orders are equal to these invariants can be selected from the operators of G in a number of ways represented by the following product:

$$(p^{\alpha+\lambda} - p^{\alpha-\beta})(p^{\alpha+\lambda} - p^{\alpha-\beta+1}) \cdots (p^{\alpha+\lambda} - p^{\alpha-1}).$$

Similarly, these β independent generators can be selected from the operators of H in

$$(p^\alpha - p^{\alpha-\beta})(p^\alpha - p^{\alpha-\beta+1}) \cdots (p^\alpha - p^{\alpha-1})$$

different ways, and the remaining independent generators can be selected in the same number of ways from the operators of G and those of H. When $\lambda > 0$, the quotient of the first of these two products divided by the second is evidently of the form $1 + p + kp^2$, and hence the following theorem has been established:

THEOREM. *The number of the subgroups of order p^α contained in an abelian group of order p^m and satisfying the condition that their invariants are as small as possible when α is given is either unity or of the form $1 + p$, mod p^2.*

As a special case of this theorem it may be noted that the number of subgroups of order p^α contained in an abelian group of order p^m, $m > \alpha > 0$, and of type $(1, 1, 1, \cdots)$ is always of the form $1 + p$, mod p^2. In this special case α and β are always equal to each other.

Suppose that G contains only one subgroup H of order p^α such that its invariants are as small as possible and consider the subgroups of order p^α which have the property that their largest invariant is p times a largest invariant of H and that a second invariant is equal to one of the largest remaining invariants of H divided by p while the rest of the invariants of such a subgroup H' are the same as those of H. We shall prove that the number of the subgroups of G satisfying the conditions imposed on H' is always of the form $p + kp^2$, so that in this case the number of subgroups of G which satisfy the conditions imposed on H and H' is $1 + p \bmod p^2$.

It will first be assumed that H contains $\beta > 2$ largest invariants and that the subgroup of G composed of all its operators whose orders divide this largest invariant multiplied by p is of order $p^{\alpha+\lambda}$. Hence $\lambda \leqq \beta \leqq \alpha$. The number of ways in which a set of $\beta - 1$ largest independent generators of H' can be selected from the operators of G is expressed by the following product:

$$(p^{\alpha+\lambda} - p^{\alpha})(p^{\alpha} - p^{\alpha-\beta+1}) \cdots (p^{\alpha} - p^{\alpha-2}).$$

The number of ways in which these generators can be selected from the operators of H' is represented by the following product:

$$(p^{\alpha} - p^{\alpha-1})(p^{\alpha-1} - p^{\alpha-\beta+1}) \cdots (p^{\alpha-1} - p^{\alpha-2}).$$

As the remaining independent generators of H' can be selected in the same number of ways from the operators of G and from those of H', the quotient of the given products is equal to the number of subgroups of G satisfying the conditions imposed on H'. This number is evidently of the form $p + kp^2$, and hence the theorem in question has been proved whenever $\beta > 2$.

When $\beta = 2$ the largest independent generator of H' can be selected from the operators of G and from those of H' in

$$p^{\alpha+\lambda} - p^{\alpha} \text{ and } p^{\alpha} - p^{\alpha-1}$$

ways respectively while the remaining independent generators of H' can be selected in the same number of ways from each of these two groups. Hence the number of subgroups satisfying the conditions imposed on H' is $p(p^{\lambda-1} + p^{\lambda-2} + \cdots + 1)$ in this case.

Finally, when $\beta = 1$ and H' contains $\gamma > 1$ next to the largest invariants, the γ largest independent generators of H' can be selected from the operators of G in

$$(p^{\alpha+1} - p^{\alpha})(p^{\delta} - p^{\delta-\gamma}) \cdots (p^{\delta} - p^{\delta-2})$$

different ways, p^{δ} being the order of the subgroup of G composed of all its operators whose orders divide the second largest invariant of H'. These independent generators can be selected from the operators of H' in

$$(p^{\alpha} - p^{\alpha-1})(p^{\delta-1} - p^{\delta-\gamma}) \cdots (p^{\delta-1} - p^{\delta-2})$$

different ways and hence the number of these subgroups is again of the form $p + kp^2$. This completes a proof of the following theorem, since the case $\gamma = 1$ is evidently included therein:

THEOREM. *If a subgroup H of an abelian group G of order p^m is of order p^{α} and composed of all the operators of G whose orders divide a given number, then the number of the subgroups of G whose largest invariant is p times the largest invariant of H and whose second invariant is obtained by dividing by p the largest of the remaining invariants of H, while its other invariants are the same as the rest of the invariants of H, is always of the form $p + kp^2$.*

The preceding theorems have been established with a view to proving that the number of proper subgroups of order p^{α} contained in a non-cyclic abelian group G of order p^m is always of the form $1 + p \bmod p^2$. To complete the proof of this theorem it is only necessary to establish the fact that the number of subgroups of order p^{α} having a different type from those considered above must always be of the form kp^2, k being a natural number. As a step in the proof of this theorem we note the following fundamental fact which entered the preceding considerations in a special form.

An independent generator of order p^{δ} of the subgroup H of order p^{α} can be selected, if these generators are selected in the descending order of magnitude and k of them have already been selected, from the operators of G in

$$p^r - p^{s+k}$$

different ways, where p^r and p^s represent the orders of the subgroups of G composed of all its operators whose orders divide p^{δ} and $p^{\delta-1}$ respectively. Similarly, this independent generator can be selected from the operators of H in

$$p^{r'} - p^{s'+k}$$

different ways, where $r' \leqq r$ and $s' \leqq s$. To prove the theorem in question it is therefore only necessary to prove that either some s is at least two units larger than the corresponding

s' or at least two s's are each one unit larger than the corresponding s''s.

From this fact it follows that the highest power of p which divides the number of the subgroups of order p^α and of type $(\alpha_1, \alpha_2, \cdots, \alpha_\lambda)$ may be found as follows: Determine the orders of the characteristic subgroups composed separately of all the operators whose orders divide p^{α_1-1}, p^{α_2-1}, $\cdots$, $p^{\alpha_\lambda-1}$ in G and in a particular subgroup H of type $(\alpha_1, \alpha_2, \cdots, \alpha_\lambda)$ respectively. The product of the orders of these subgroups of G divided by the product of the orders of the corresponding subgroups of H gives a quotient which is the power of p in question. For instance, if G is of type (6, 6, 5, 4, 2) and H is of type (6, 3, 2, 1) the number of subgroups of G which are of order p^{12} and of type (6, 3, 2, 1) is divisible by

$$p^{21+10+5-11-7-4}$$

but not by any higher power of p.

In particular, it may be noted that the number of subgroups of order p^α and of a given type is always divisible by p^2 whenever the number of the invariants of G exceeds the number of the invariants of such a subgroup H by 2 and at least one of the latter invariants exceeds p. If at least two of these invariants exceed p, the number of these subgroups is divisible by p^2 whenever G has at least one more invariant than H has. Hence when the number of the subgroups of the same type as H has is not divisible by p^2 the number of invariants of H is either the same as that of G or one less than that of G except when H is of type $(1, 1, 1, \cdots)$.

Morever, when H has one invariant less than G and the number of subgroups having the same type as H has is not divisible by p^2, it results from the preceding considerations that either no invariant of H exceeds p, or that only one of these invariants exceeds p. In the latter case this invariant is p^2 unless G has also only one invariant greater than p. Hence the following:

THEOREM: *Whenever the number of subgroups of the same type as H is not divisible by p^2 and the number of invariants of H is less than the number of invariants of G there is one and only one subgroup in G having the same order as H but smaller invariants than H has.*

It remains only to consider the case when the subgroups of order p^α which have the same invariants as H have as many invariants as G. Suppose that the invariants of G arranged in descending order of magnitude are $p^{\alpha_1}, p^{\alpha_2}, \cdots, p^{\alpha_\lambda}$ while those of H arranged similarly are $p^{\alpha_1'}, p^{\alpha_2'}, \cdots, p^{\alpha_\lambda'}$. It is well known that $\alpha_1 \geqq \alpha_1', \alpha_2 \geqq \alpha_2', \cdots, \alpha_\lambda \geqq \alpha_\lambda'$. The number of the subgroups of type $(\alpha_1', \alpha_2', \cdots, \alpha_\lambda')$ is evidently divisible by p^2 whenever α_1' is at least two units larger than each of two other α''s which are separately smaller than the corresponding α's, and also when α_1' and α_2' are separately two units larger than some one α' which is less than the corresponding α, or α_1' is at least three units larger than such an α' provided this α' is not α_2' and $\alpha_2 = \alpha_2' + 1$.

From the preceding paragraph it results that whenever the number of subgroups of type $(\alpha_1', \alpha_2', \cdots, \alpha_\lambda')$ is not divisible by p^2 and an α_β' is less than α_β then there is at most one other α' which is two units larger than α_β'. If there is such an α' it is α_1' and α_γ', $\beta > \gamma > 1$, is equal to $\alpha_\beta' + 1$. It was noted above that when these conditions are satisfied the number of subgroups of G which are of type $(\alpha_1', \alpha_2', \cdots, \alpha_\lambda')$ is of the form $p + kp^2$. This is also the case when $\alpha_\lambda' = \alpha_\lambda$, $\alpha_\lambda'{}_{-1} = \alpha_{\lambda-1}, \ldots, \alpha_3' = \alpha_3, \alpha_2' = \alpha_2 - 1$, and $\alpha_1 < \alpha - 2$.

On the other hand, when none of the α''s is at least two units larger than the smallest α_β' which is less than α_β the number of subgroups of type $(\alpha_1', \alpha_2', \cdots, \alpha_\lambda')$ was proved above to be of the form $1 + p + kp^2$ provided there is at least one α' which exceeds α_β'. If there is no such α' there is only one subgroup of the given type. These results establish, in particular, the following:

THEOREM. *In any non-cyclic abelian group of order p^m the number of the subgroups whose order is a given proper divisor of the order of the group is always of the form* $1 + p$ *mod* p^2.

UNIVERSITY OF ILLINOIS.