AN EXTENSION OF SYLOW'S THEOREM

By G. A. MILLER.

[Received April 7th, 1904.—Read April 14th, 1904.]

FROBENIUS extended Sylow's theorem by proving that every group (G) whose order (g) is divisible by p^a, p being any prime number, contains $1+kp$ sub-groups of order p^a.* The present note is devoted to the theorem that *the number of cyclic sub-groups of order* p^a ($a > 1$, $p > 2$) *in G is always of the form kp whenever the Sylow sub-groups* † *of order p^m in G are non-cyclic.* In particular, every non-cyclic group of order p^m contains just lp cyclic sub-groups of order p^a, and hence the number of its non-cyclic sub-groups of this order is of the form $1+kp$. We shall first prove this particular case; that is, we shall first assume that $g = p^m$.

When G is Abelian the number of its operators of order p^a is

$$p^{m_1+m_2+\dots+m_a} - p^{m_1+m_2+\dots+m_{a-1}}$$

where m_β ($\beta = 1, 2, \dots, a$) is the number of the invariants of G which $\geqslant p^\beta$.‡ The number of the cyclic sub-groups of order p^a is the quotient obtained by dividing the number of the operators of this order by $p^a - p^{a-1}$. As $m_1+m_2+\dots+m_{a-1} > a-1$,§ it follows that the given theorem is true for any Abelian group of order p^m. In the next three paragraphs it is assumed that G is a non-Abelian group of order p^m, $p > 2$.

Since the number of the non-invariant cyclic sub-groups of order p^a in G is a multiple of p, it remains only to show that the number of its invariant cyclic sub-groups of this order is also a multiple of p. Let P_a be such an invariant sub-group. It is contained in some invariant sub-group of each of the orders $p^{a+1}, p^{a+2}, \dots, p^m$. Hence we may assume that there is an invariant non-cyclic sub-group of order $p^{a+\gamma}$, $\gamma > 0$, which includes an operator of order $p^{a+\gamma-1}$ which generates P_a. As this

* Frobenius, *Berliner Sitzungsberichte*, 1895, p. 984.

† *Bulletin of the American Mathematical Society*, Vol. IX., 1903, p. 543.

‡ Cf. Netto, *Vorlesungen über Algebra*, Vol. II., 1900, p. 247.

§ It will always assumed that G is non-cyclic. When G is cyclic

$$m_1+m_2+\dots+m_{a-1} = a-1,$$

since $m_\beta = 1$.

non-cyclic group contains just p cyclic sub-groups of order p^{α},* being conformal with the Abelian group of type $(\alpha+\gamma-1, 1)$, G must contain at least p cyclic invariant sub-groups of order p^{α} whenever it contains one such sub-group. These p sub-groups generate a group (H_1) of $p^{\alpha+1}$.

If G contains another invariant cyclic sub-group P'_{α} of order p^{α}, it must contain another invariant sub-group (H_2) of order $p^{\alpha+1}$ which involves just p such invariant cyclic sub-groups. If none of these is contained in H_1, we have found just $2p$ cyclic invariant sub-groups of order p^{α}. If one of them is in H_1, the $2p-1$ distinct cyclic invariant sub-groups which are found in H_1 and H_2 have just $p^{\alpha-1}$ common operators. We proceed to show that the group generated by H_1 and H_2, $\{H_1, H_2\}$, is conformal with an Abelian group whenever H_1 and H_2 have a common cyclic group of order p^{α}.

The commutator sub-group of $\{H_1, H_2\}$ is clearly the sub-group of order p contained in P_{α}, since a generator of P'_{α} transforms each one of a set of generators of H_1 into itself multiplied by an operator of this sub-group of order p. Moreover, if an operator (s_1) transforms an operator s_2 into itself multiplied by an operator of order p, which is commutative with s_1 and s_2, then $(s_2 s_1)^p = s_2^p s_1^p$.† Hence $\{H_1, H_2\}$ is conformal with the Abelian group of type $(\alpha, 1, 1)$. This process can be continued until the cyclic invariant sub-groups of order p^{α} which have $p^{\alpha-1}$ operators in common with P_{α} are exhausted. All of these generate a group which is conformal with an Abelian group of type $(\alpha, 1, 1, \ldots)$. As all the invariant cyclic sub-groups of order p^{α} can be divided into one or more sets, it is proved that every non-cyclic group of order p^m contains lp cyclic sub-groups of order p^{α}, $p > 2$, $\alpha > 1$.‡

That the theorem is also true when g is not a power of a prime follows directly from the fact that every Sylow sub-group of order p^m transforms any sub-group of order p^{α} which is found in G, but not in the Sylow sub-group, into p^{γ} conjugates. Hence the number of sub-groups of any particular type which are found in G, but not in a given Sylow sub-group, is a multiple of p. It is clear that the given theorem could also have been stated as follows :—If G contains a non-cyclic sub-group of order p^{α}, the numbers of its *non-cyclic* sub-groups of this order is of the form $1+kp$.

---

* Burnside, *Theory of Groups of Finite Order*, 1897, p. 76.

† *Bulletin of the American Mathematical Society*, Vol. VII., 1901, p. 350.

‡ It is easy to prove that all the operators of order p^{α} in G which have at most p conjugates under G generate a characteristic sub-group which is conformal with an Abelian group. In particular, the number of sub-groups of order p is of the form $1+p+kp^2$. Bauer proved that the number of sub-groups of order p^{m-1} is of the form $1+p+p^2+\ldots+p^{\gamma}$. *Nouvelles Annales*, Vol. XIX., 1900, p. 508.