# A FUNDAMENTAL THEOREM WITH RESPECT TO TRANSITIVE SUBSTITUTION GROUPS. 

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, February 28, 1903.)
Let $G$ represent any transitive group of degree $n$ and of order $g=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \cdots p_{m}^{\alpha_{m}} ; p_{1}, p_{2}, \cdots, p_{m}$ being distinct primes. According to Sylow's theorem $G$ contains at least one subgroup of each of the orders $p_{1}^{\alpha_{1}}, p_{2}^{\alpha_{2}}, \cdots, p_{m}^{\alpha_{m}}$. It will be convenient to speak of these subgroups as the Sylow subgroups of $G$. Since $G$ is transitive, all the prime factors of $n$ are included among the factors of $g$. The theorem in question may now be stated as follows:

Theorem. If $p_{1}^{\beta}$ is the highest power of $p_{1}$ which divides $n$, each Sylow subgroup of order $p_{1}^{a_{1}}$ in $G$ has a transitive constituent of degree $p_{1}^{\beta}$ and all its other transitive constituents are of degree $p_{1}^{\beta+\gamma}, \gamma \equiv 0$.

Corollary I. If $n=2 p^{a}, p$ being any odd prime, each of the Sylow subgroups whose order is a power of $p$ has just two transitive constituents, each being of degree $p^{a}$.

Corollary II. If $n$ is a power of a prime, a Sylow subgroup of $G$ whose order is a power of the same prime must be transitive.

The proof of the theorem results from the following elementary considerations : Let $G_{1}$ represent the subgroup of $G$ which is composed of all its substitutions which omit a given letter. Every Sylow subgroup of $G_{1}$ is found in some Sylow subgroup of $G$. Whenever the orders of these subgroups are different the former is composed of all the substitutions of the latter which omit one letter.*

Since $p_{1}$ is any prime divisor of $g$ we may confine our attention to the Sylow subgroups of $G_{1}$ and $G$ whose orders are $p_{1}^{a_{1}-\beta}$ and $p_{1}^{a_{1}}$ respectively. At least one transitive constituent of the latter must be such that the order of its largest subgroups of lower degree than its own may be obtained by dividing its own order by $p_{1}^{\beta} ; i$. e., one of its transitive consti-

[^0]
[^0]:    * Cf. Burnside, Theory of groups of finite order, 1897, p. 94.

