ON AN EXTENSION OF SYLOW'S THEOREM.

BY DR. G. A. MILLER.

(Read before the American Mathematical Society at the Meeting of February 26, 1898.)

SINCE we shall employ Cauchy's theorem * in what follows it seems desirable to give a simple proof of it. It may be stated as follows: *A group G whose order g is divisible by a prime number p contains an operator of order p.*

We shall first suppose that G is Abelian. If it is generated by a single operator S of order np, we have $S^n \neq 1$ and $(S^n)^p = 1$. Hence S^n is the required operator. If G cannot be generated by a single operator we may represent a set of generating operators by $S_1, S_2, \cdots, S_r$. Since these generators are commutative the order of the group which any number of them generate cannot be divisible by any prime number that is not contained in the order of at least one of the generators. Hence the order of at least one of the given generators of G must be divisible by p, and some power of this generator must be the required operator of order p.

We may now suppose that G is a non-Abelian group of order np, and that our theorem is proved for all Abelian groups and for all non-Abelian groups whose orders are less than np. Let g_1 be the order of the largest subgroup of G that transforms a given operator into itself; $g \div g_1$ is the number of conjugates of this operator. Hence

$$g = \frac{g}{g_1} + \frac{g}{g_2} + \cdots + \frac{g}{g_k} \qquad (A)$$

k being the number of systems of conjugate operators and $g_1, g_2, \cdots, g_k$ being the orders of the largest subgroups that transform one operator of each system into itself. The operators for which $g_\alpha = g$ form an Abelian subgroup of G. If the order of this subgroup is not divisible by p some $g_\beta < g$ must be divisible by p, since the second member of (A) must be divisible by this number. The main features of this method of proof are due to Frobenius.

THEOREM I. *If a group G contains r $(r > 0)$ subgroups $G_1, G_2, \cdots, G_r$ of order $p_1^\alpha p_2^\beta p_3^\gamma \cdots$ ($p_1, p_2, p_3, \cdots$ being different*

* Cauchy: Exercises d'analyse, III (1844), p. 250. Cf. Jordan: Traité des substitutions (1870), p. 26.

prime numbers) and if G contains no subgroup whose order may be obtained by merely increasing the power of any of these prime numbers, then will each of these r subgroups transform all the others according to a substitution group S whose degree is exactly $r - 1$ *and which is isomorphic to the transforming group. Hence* $r = 1 + k_1 p_1 + k_2 p_2 + k_3 p_3 + \cdots$ ($k_1, k_2, \cdots$ *being positive factors of* $p_1^{\alpha} p_2^{\beta} p_3^{\gamma} \cdots$).

If the degree of each of the transitive constituents of every S is divisible by the same prime factor, say p_1, *the r given subgroups are conjugate, and the order of G is divisible by* p_1^{α} *but is not divisible by* $p_1^{\alpha+1}$.

If all the operators of one of the given r subgroups G_1 transformed another one of them into itself this second subgroup and an operator of G_1 that is not contained in the second would generate a group whose order could be obtained by merely increasing the power of one or more of the factors of the order of G_1. As this is contrary to the hypothesis each one of the given r subgroups must transform all of the others according to some isomorphic substitution group of degree $r - 1$. When G is a simple group this isomorphism must be simple. The degree of each of the transitive constituents of S must be a divisor of the order of this constituent and hence it must also be a divisor of the order of S. This proves the first part of the theorem.

When the degree of each of the transitive constituents of any one S is divisible by p_1, $r \equiv 1 \mod p_1$ according to the preceding paragraph. We proceed to prove that G transforms the given r subgroups according to a transitive substitution group S_1, whenever the transitive constituents of each of the r S's satisfy the given condition. If S_1 were intransitive, any one of the given r subgroups that did not correspond to an element of a given transitive constituent of S_1 would transform the elements of this constituent in sets containing multiples of p_1 and such transforming subgroups could be found for each of the transitive constituents of S_1. This is impossible since r is not divisible by p_1. Hence S_1 is transitive, *i. e.*, the given r subgroups are conjugate when the degree of each of the transitive constituents of every S is divisible by the same prime number.

We shall now consider the largest subgroup that transforms one of the given subgroups, say G_1, into itself. The order q of its quotient group with respect to G_1 cannot be divisible by a factor of the order of G_1, otherwise there would be a subgroup whose order could be obtained by merely increasing the order of one or more of the prime factors of the order of G_1. The order of the largest sub-

group that transforms G_1 into itself must therefore be $q p_1^{\alpha} p_2^{\beta} p_3^{\gamma} \cdots$ and g must be the product of this order and the number of conjugates of G_1; *i. e.*,

$$g = r q p_1^{\alpha} p_2^{\beta} p_3^{\gamma} \cdots$$

When the given condition is satisfied rq is prime to p_1, hence p_1^{α} is the highest power of p_1 that divides g.

COROLLARY I. *When the order of a group is divisible by p^{β} but not by $p^{\beta+1}$ the group contains $1 + kp$ subgroups of this order. All these subgroups are conjugate.*

In the preceding theorem we may let $p = p_1$, and $1 = p_2 = p_3 = \cdots$, for Cauchy's theorem assures the existence of a subgroup of order p^{α}, $\alpha > 0$, when $\beta > 0$. Since S is isomorphic to a group of order p^{α} the degree of each of its transitive constituents must be a power of p, *i. e.*, $r = 1 + kp$ and $\alpha = \beta$. This is known as Sylow's theorem. By restricting ourselves to this special case in the proof of the above theorem we obtain a simple method of proving the fundamental theorem of Sylow. The steps are as follows: (1) We observe from Cauchy's theorem that there is a subgroup of order p^{α}, $\alpha > 0$. (2) If p^{α} is the highest order of such a subgroup the number of the subgroups of this order is $\equiv 1 \bmod p$. (3) All these subgroups are conjugate. (4) p^{α} is the highest power of p that divides the order of the group, *i. e.*, $\alpha = \beta$.

It will be observed that the order of these steps is different from that adopted in the recent works on groups. It seems that this method of proof would be more desirable than the one generally given since it is not less simple and it gives due credit to Cauchy's important contribution to the theorem which bears the name of Sylow.

COROLLARY II. *If one of the given r subgroups transforms all the others according to a simply isomorphic substitution group each of them has this property.*

For if an operator of one of these subgroups transforms all the others into themselves it must be contained in each of them.

The value of r can clearly not exceed the quotient obtained by dividing the order of G by that of G_1. This elementary condition, combined with the given form of r, is sometimes sufficient to restrict the value of r to a small number of values, *e. g.*, if a group of order 105 contains a subgroup of order 21 the number (r) of these subgroups must satisfy the relations $r = 1 + 7k_1 + 3k_2$, $r < 6$. Hence $r = 1$ or 4.

As a simple illustration of the given theorem we may consider the subgroups of order $p_1 p_2$ that are contained in a substitution group of degree p_1, $p_1 > p_2$, that does not contain any subgroup of order $p_1 p_2^{\alpha}$, $\alpha > 1$. If any one of these subgroups, G_1, had a substitution of order p_1 in common with another, G_2, these two subgroups would generate a metacyclic group of order $p_1 p_2^2$. As this is contrary to the hypothesis the number of these subgroups must $\equiv 1 \bmod p_1$ and all of them must be conjugate.

THEOREM II. *If any group G of order g contains a subgroup of order $p^{\alpha}q^{\beta}$, p and q being any prime numbers, the number of its subgroups of this order is of the form $1 + kp + lq$, k and l being positive integers.*

We may assume that $\alpha, \beta > 0$ since it is known that $k = 0$ when $\alpha = 0$* and that k and $l = 0$ when α and $\beta = 0$. We may also assume that the order of G is $p^{\alpha_1}q^{\beta_1}$, for if g contained a prime factor besides p and q, G contained a subgroup of order $p^a q^b$ where a and b are both maxima. This subgroup would transform all the subgroups of order $p^{\alpha}q^{\beta}$ that are not included in it according to an isomorphic substitution group. Hence the number of the latter subgroups would be $a_1 p + bq$ (a_1 and b_1 being positive integers) and it would only be necessary to prove that the number of these subgroups in the group of order $p^a q^b$ is $1 + a_2 p + b_2 q$. In what follows we shall therefore assume $\alpha, \beta > 0$ and $g = p^{\alpha_1}q$.

As the theorem is evidently true when $\alpha_1 = \beta_1 = 1$ we may assume that it is true with respect to every group of order $p^{\alpha'}q^{\beta'}$ when $p^{\alpha_1}q^{\beta_1} \div p^{\alpha'}q^{\beta'}$ is an integer which exceeds unity. The subgroups of order $p^{\alpha}q^{\beta}$ may be represented $G_1, G_2, \cdots, G_r$ and we may assume that these r subgroups generate G. If some one of them transforms each one of the others into a different group the theorem is evidently true. In general, we multiply a sufficient number of them together so that the product transforms each one of the subgroups of the given order that is not contained in it. This product may be G itself. At least one of the given subgroups G_{α} is self-conjugate in this product.

We now consider the number of the given subgroups which have more than one operator in common with G_{α} in the given product. The number of all those in which the total number of common operators do not form a self-conjugate subgroup of G_{α} is evidently $ap + bq$, a and b being positive integers. If we exclude G_{α} itself we may readily show that the number of those in which the total number of common operators is a self-conjugate subgroup of

* Frobenius, *Berliner Sitzungsberichte* (1895), p. 988.

G_α is of the same form. Hence it remains only to consider the number of those which have no operator besides identity in common with G_α.

All these subgroups may be divided into two classes, viz: (1) those which are transformed into themselves by G_α, and (2) those which are transformed into different groups by the operators of G_α. The number of the former class may evidently be written in the form $ap + bq$, a and b being positive integers. If a group of the latter class occurs, all its operators must be commutative to every operator of G_α * and hence $r > p(q-1)$. In this case the given theorem is evidently true. It may be observed that the number of self-conjugate subgroups of G is not necessarily of the given form, *e. g.*, the direct product of two non-commutative groups of order 21 contains only two self-conjugate subgroups of this order.

CORNELL UNIVERSITY,
February, 1898.

NOTE ON THE TETRAHEDROID.

BY DR. J. I. HUTCHINSON.

(Read before the American Mathematical Society at the Meeting of February 26, 1898.)

IN a brief paper, "A special form of a quartic surface," *Annals of Mathematics*, vol. 11, p. 158, I have called attention to an interesting special form of the locus of the vertex of a cone passing through six points. I wish to point out in this note the connection between this special surface and the tetrahedroid.

Given six arbitrary points in space 1, 2, 3, 4, 5, 6. These determine a system of ∞^3 quadric surfaces each of which pass through the six points. Denote this configuration by Σ.

Choose any arbitrary point P and consider the polar planes of P with respect to the system of quadrics. There are determined in this way ∞^3 planes forming a configuration Σ_1.

To a quadric in Σ corresponds a plane in Σ_1. The vertices of the cones of Σ have for locus a surface K of the fourth order. The planes of Σ_1 corresponding to the cones of Σ envelope a Kummer surface. The point in each plane corresponding to the cone vertex is the point of tangency.

* Dyck, *Mathematische Annalen*, vol. 22, p. 97.