SIMPLIFICATIONS RELATING TO A PROOF OF SYLOW'S THEOREM

BY G. A. MILLER

Sylow's theorem is usually developed very early in a course relating to the theory of groups of finite order. Hence simplifications in its proof are the more desirable, especially when they enable us to avoid the use of a number theory formula and therefore to confine the proof more closely to group theoretic considerations. Since the simplifications which will be developed in what follows involve a property of double cosets which is not directly used in the proof to which they relate* we shall first exhibit some of the fundamental properties of double co-sets, assuming as known the fact that if H_1 and H_2 are any two subgroups of a group G then all the operators of G may be uniquely represented in the following form. $G = H_1 s_1 H_2 + \cdots + H_1 s_\lambda H_2$ if we assume that in each double co-set only the distinct operators are considered.

The number of distinct operators in each double co-set is evidently divisible by h_1 and by h_2, h_1 and h_2 being the orders of H_1 and H_2 respectively. A necessary and sufficient condition that each of the given double co-sets contains the same number of distinct operators is that each of the conjugates of H_1 under G has the same number of operators in common with H_2. This is equivalent to saying that each of these conjugates of H_2 has the same number of operators in common with H_1. When this number of common operators is k then the number of distinct operators in each of these co-sets is $h_1 h_2 / k$, and vice versa. In particular, each of these double co-sets must involve the same number of distinct operators whenever at least one of the two subgroups H_1, H_2 is invariant under G, and each of the double co-sets with respect

* Miller, Blichfeldt, and Dickson, *Finite Groups*, 1916, p. 27.

to H_1 and H_2 involves exactly $h_1 h_2$ distinct operators whenever h_1 and h_2 are relatively prime. When H_1 and H_2 belong to the same set of conjugates under G then the number of these double co-sets which involve exactly h_1 distinct operators is evidently equal to the index of H_1 under the largest subgroup of G which transforms H_1 into itself, and all the other double co-sets involve a multiple of h_1 distinct operators. All of these multiples must be sub-multiples of h_1^2. When H_1 and H_2 are identical it is obvious that they may be regarded as conjugate, and hence the theorem which has just been stated applies directly to the double co-sets with respect to a single sub-group.

Suppose now that $h_1 = p^\alpha$, where p is a prime number, and assume that the index of H_1 under the largest subgroup of G which transforms H_1 into itself is k, k being prime to p. If the operators of G are represented as double co-sets with respect to H_1, i. e., if H_2 is assumed to be identical with H_1, it results that the order g of G can be represented as follows: $g = kp^\alpha + lp^{\alpha+1}$. Hence p^α must be the highest power of p which divides g. If c represents the number of conjugates of H under G it results that $kp^\alpha = g/c$, and hence $(c-1)g = lp^{\alpha+1}$. That is, $c \equiv 1 \bmod p$. It has therefore been proved by means of double co-sets that if H_1 is of index prime to p under the largest subgroup of G which transforms H_1 into itself then H_1 is a Sylow subgroup of G and the number of its conjugates under G is congruent to 1 mod p.

From the preceding paragraph it results that a necessary and sufficient condition that a subgroup H of order p^α is a Sylow subgroup of G is that the index of H under the group K formed by all the operators of G which transform H into itself is prime to p, for if this index were not prime to p the quotient group K/H would have an order which is divisible by p. Since the order of this quotient group is less than g it may be assumed that this group contains a subgroup whose order is a power of p and hence G contains a subgroup of order $p^{\alpha+1}$. This

suggests that a proof of Sylow's theorem as regards the symmetric group S of degree p^m can be based upon a proof of the fact that S involves a subgroup P of order p^α which is of index prime to p under the group formed by all the substitutions of S which transform P into itself. This fact can easily be proved by mathematical induction.

When $m = 1$ the theorem is evident. If we assume that the theorem is true for the symmetric group of degree p^{m-1} it is not difficult to prove it true for S. In fact, S obviously contains a substitution s of order p and of degree p^m. The p^{m-1} cycles of this substitution are evidently transformed according to the symmetric group of degree p^{m-1} by the largest subgroup of S which transforms s into itself. The substitutions of S which transform the cycles of s according to a Sylow subgroup in the symmetric group of degree p^{m-1} generate a group of order p^α which contains no invariant substitution besides those generated by s. Hence all the substitutions of S which transform this group of order p^α into itself also transform s into itself, and therefore this group of order p^α is of index prime to p under the group formed by all the substitutions of S which transform it into itself. This group must therefore be a Sylow subgroup of S. From the fact that S contains a Sylow subgroup of order p^α it is very easy to deduce that every group whose order is divisible by p contains at least one Sylow subgroup whose order is a power of p.

The considerations which precede prove incidentally that the Sylow subgroups of order p^α contained in S are of index $(p-1)^m$ under S, since the index of these Sylow subgroups is obviously $p-1$ times the index of the corresponding Sylow subgroups under the symmetric group of degree p^{m-1}. Hence we not only know that this index is prime to p but we also know its exact value. The said considerations also prove that the number of the Sylow subgroups of order p^α contained in S which have in common a given invariant subgroup of order p is equal to the number of the Sylow subgroups of order a power of p in the sym-

metric group of degree p^{m-1}. Moreover, the number of the Sylow groups of order p^α contained in S is this number times the number of the possible subgroups of order p and of degree p^m contained in S.

From the method of proof here employed it also results directly that if the largest possible subgroup common to two Sylow subgroups of order p^α in any group G is of order p^β then the number of these Sylow subgroups is $\equiv 1 \bmod p^{\alpha-\beta}$. For instance, it is well known that no two subgroups of order 4 contained in the simple group of order 60 have any operator in common besides the identity. Hence the number of these subgroups must be $\equiv 1 \bmod 4$. As a matter of fact it is 5. It should be added that the simplifications suggested above do not apply to the well and favorably known proof of Sylow's theorem due to G. Frobenius. They apply to the older proof based on some properties of the symmetric group, especially to the form in which this proof is developed in the work to which reference was made in the first paragraph.

In closing we wish to refer to a variation in the proof of another fundamental theorem in the theory of groups of finite order since this variation may possibly simplify the proof for some readers. This variation relates to a proof that every subgroup of index 2 of any group G is invariant under G. To prove this theorem it may first be noted that if s represents any operator of such a subgroup H while t represents any operator of G which is not contained in H then st cannot be in H as otherwise the equation $xy = z$ would have more than one solution in G when two of its symbols are replaced by operators of G. For the same reason the product of two operators of G, neither of which is in H, must be in H. As $t^{-1}st$ is such a product, since neither st nor t^{-1} is in H, $t^{-1}st$ is such a product and must be in H. That is, H must be an invariant subgroup of G as a result of the fact that it is composed of half the operators of G.

THE UNIVERSITY OF ILLINOIS