

THEOREMS OF SYLOW THEORY

by

SAMUEL A. MUSIL

B. S., Kansas State University, 1964

---

A MASTER'S REPORT

submitted in partial fulfillment of the  
requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY  
Manhattan, Kansas

1965

Approved by:

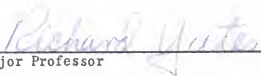
  
Major Professor

TABLE OF CONTENTS

INTRODUCTION .....	1
THEORY OF NORMAL SUBGROUPS .....	5
THEORY OF HOMOMORPHISMS.....	8
FACTOR GROUPS .....	9
CYCLIC GROUPS .....	15
NON-CYCLIC FINITE GROUPS .....	19
SYLOW THEOREMS .....	21
ACKNOWLEDGMENT .....	31
REFERENCES .....	32

## INTRODUCTION

Certain properties of finite groups are determined largely by the properties of certain positive integers. The order of a finite group as given in Definition E is always a positive integer, and so the Unique Factorization Theorem from the Theory of Numbers actually determines the existence of some of the subgroups of a finite group. This result follows from the Sylow Theorems of group theory.

L. Sylow discovered three remarkable theorems in 1872, which serve as the foundation of the study of subgroups of finite groups. The purpose of this report is to develop the preliminary theory and finally prove the three Sylow Theorems. To do this a basic knowledge of Cardinal number theory, the properties of integers, and elementary group theory will be assumed on the part of the reader. The initial part of the paper deals with groups of arbitrary order, and so certain definitions are given in terms of general cardinal numbers. Many of the more important properties used are listed in the introduction. Reference will be made to these throughout the paper.

The group product will be indicated throughout the paper by juxtaposition of the elements, i.e.  $ab$  represents the element obtained by operating on  $b$  with  $a$ . The identity element of any group throughout the paper will be denoted by the letter "e." The groups and subgroups will be denoted by capital letters  $G, H, \dots$ , while the elements will be denoted by lowercase letters  $a, b, c, \dots$ . The phrase "if and only if" will be abbreviated throughout the paper as "iffi."

The following is a list of definitions, theorems, and corollaries which will be used throughout the paper.

THEOREM A: If  $S$  is any collection of subgroups of a group  $G$ , the intersection of these subgroups is also a subgroup of  $G$ .

DEFINITION A: The subgroup  $[A, B]$  generated by  $A$  and  $B$  is the intersection of all subgroups containing  $A$  and  $B$ .

THEOREM B: The inverse of  $ab \in G$  is  $b^{-1} a^{-1}$ .

DEFINITION B: A 1-1 mapping  $G \rightarrow H$  of the elements of a group  $G$  onto those of a group  $H$  is called an isomorphism if whenever  $g_1 \rightarrow h_1$  and  $g_2 \rightarrow h_2$ , then  $g_1 g_2 \rightarrow h_1 h_2$ .

DEFINITION C: A mapping  $G \rightarrow H$  of the elements of a group  $G$  onto those of a group  $H$  is called a homomorphism if whenever  $g_1 \rightarrow h_1$  and  $g_2 \rightarrow h_2$ , then  $g_1 g_2 \rightarrow h_1 h_2$ .

THEOREM C: In the homomorphism  $G \rightarrow H$ , the identity element of  $G$  corresponds to the identity element of  $H$ .

DEFINITION D: Given a group  $G$  and a subgroup  $H$ , the set of elements  $hx$ ,  $h \in H$ ,  $x \in G$ ,  $x$  fixed, is called a left coset of  $H$ . We write  $Hx$  to designate this set. Similarly, the set of elements  $xh$ ,  $h \in H$ , is called a right coset  $xH$  of  $H$ .

THEOREM D: Two left (right) cosets of  $H$  in  $G$  are either disjoint or identical sets of elements.

THEOREM E: A left (right) coset of  $H$  contains the same cardinal number of elements as  $H$ .

COROLLARY E-1: There is a 1-1 correspondence between right and left cosets of  $H$ .

DEFINITION E: The order of a group  $G$ , denoted by  $o(G)$ , is the cardinal number of elements in  $G$ .

DEFINITION F: The cardinal number  $r$  of right or left cosets of a subgroup in a group  $G$  is called the index of  $H$  in  $G$  and is written  $[G:H]$ .

THEOREM F: (Theorem of Lagrange) The order of a group  $G$  is the product of the order of a subgroup  $H$  and the index of  $H$  in  $G$ . That is,  $o(G) = o(H) [G:H]$ .

COROLLARY F-1: The order of each subgroup of a finite group  $G$  is a divisor of the order of  $G$ .

DEFINITION G: If all powers of an element  $a$  are distinct elements of the group to which it belongs,  $a$  is said to be of infinite order. If  $n$  is the smallest positive integer such that  $a^n = e$ , we say that  $a$  is of finite order with order  $n$ .

In definitions H through L,  $S$  is an arbitrary subset of  $G$  and  $H$  is a subgroup of  $G$ .

DEFINITION H: The set  $S'$  of elements of the form  $x^{-1}sx$ ,  $s \in S$ ,  $x$  fixed, is called the transform of  $S$  by  $x$  and is written  $S' = x^{-1}Sx$ .

DEFINITION I: If  $S$  and  $S'$  are two subsets of  $G$  and some  $x \in H$  exists such that  $S' = x^{-1}Sx$ , we say that  $S$  and  $S'$  are conjugate under  $H$ .

DEFINITION J: The relation of being conjugate under  $H$  can be shown to be an equivalence relation, and we call the set of all  $S'$  conjugate to a given  $S$  a class of conjugates.

DEFINITION K: The set of  $x \in H$  such that  $x^{-1}Sx = S$  is a subgroup of  $H$  which we shall call the normalizer of  $S$  in  $H$ . We designate this as  $N_H(S)$ .

DEFINITION L: The set of  $x \in H$  such that  $x^{-1}sx = s$  for all  $s \in S$  may be shown to be a subgroup of  $H$  which we call the centralizer of  $S$  in  $H$  and designate  $C_H(S)$ . Note that if the subset  $S$  consists of a single element, the centralizer and normalizer are identical.  $C_G(G)$  is called the center of  $G$  and is often denoted by  $Z$ . If  $z \in Z$ , then  $z^{-1}xz = x$  for all  $x \in G$ .

THEOREM G: The number of conjugates of  $S$  under  $H$  is the index in  $H$  of the normalizer of  $S$  in  $H$ ,  $[H:N_H(S)]$ .

DEFINITION M: If  $S$  consists of a single element  $s$ , the conjugates of  $S$  under  $G$  form a class.

THEOREM H: The classes of elements in  $G$  are partitioning of the elements of  $G$ , and we write,

$$G = C_1 + C_2 + \dots + C_s$$

the  $C_i$  being disjoint classes and every element being in exactly one class.

THEOREM I: An Abelian group of order  $n$  contains an element of order  $p$  if  $p$  is a prime dividing  $n$ .

DEFINITION N: Given a group  $G$  and two subgroups  $H$  and  $K$  not necessarily distinct, the set of elements  $Hx \cap K$ , where  $x$  is some fixed element of  $G$ , is called a double coset.

THEOREM J: Two double cosets  $Hx \cap K$  and  $Hy \cap K$  are either disjoint or identical.

THEOREM K: The number of left cosets of  $H$  in  $Hx \cap K$  is  $[K:K \cap x^{-1}Hx]$ , and the number of right cosets of  $K$  in  $Hx \cap K$  is  $[x^{-1}Hx : K \cap x^{-1}Hx]$ .

## THEORY OF NORMAL SUBGROUPS

The nature of a group has been found to be most easily understood by analyzing the subgroups of that group. A unique type of subgroup of great interest is the normal subgroup.

DEFINITION 1: A subgroup  $H$  of a group  $G$  is normal in  $G$  if  $aH = Ha$  for each  $a \in G$ . That is, the set of all elements of the form  $ab$ ,  $b \in H$  is identical to the set of all elements of the form  $ba$ ,  $b \in H$ .

DEFINITION 2: Two elements  $a$  and  $b$  in  $G$  are conjugate in  $G$  if there exists  $g \in G$  such that  $b = g^{-1}ag$  (or  $a = g^{-1}bg$ ).

The following theorem is a convenient criterion for deciding whether a subsystem of a group is a subgroup.

THEOREM 1: A nonempty subset  $H$  of a group  $G$  is a subgroup iff  $ab^{-1} \in H$ , for arbitrary  $a, b \in H$ .

Proof: Suppose that  $H$  is a subgroup with  $a, b \in H$ . Then  $b^{-1} \in H$  since  $b$  must have an inverse in  $H$ . Then,  $a, b^{-1} \in H$  and the closure postulate implies that  $ab^{-1} \in H$ . To prove the converse, let us consider  $H$  to be a subset of  $G$ , such that  $ab^{-1} \in H$  for arbitrary  $a, b \in H$ . Then, if  $a \in H$ , we have  $aa^{-1} = e \in H$ , where  $e$  is the identity element of  $G$ . Now let  $b \in H$ . Then since  $e, b \in H$ , we have  $eb^{-1} = b^{-1} \in H$ . Thus, the inverse of each element in  $H$  lies in  $H$ . Hence, if  $a, b \in H$  we have  $a, b^{-1} \in H$  and by hypothesis,  $a(b^{-1})^{-1} = ab \in H$ . Thus, the closure axiom is satisfied. Since  $G$  is a group and the associative law holds for all elements of  $G$ , it holds for all elements of  $H$ . Thus, we have all four postulates of a group satisfied, and  $H$  is a subgroup of  $G$ .

Now we will state a theorem which leads to another characterization of a normal subgroup of a group.

THEOREM 2: If  $H$  is a subgroup of  $G$  and  $g \in G$  is a fixed element, then  $g^{-1}Hg$  is a subgroup of  $G$ .

PROOF: Let  $h_1, h_2 \in H$ . Then  $a = g^{-1}h_1g$  and  $b = g^{-1}h_2g$  are elements of  $g^{-1}Hg$ . Now

$$ab^{-1} = (g^{-1}h_1g)(g^{-1}h_2g)^{-1} = (g^{-1}h_1g)(g^{-1}h_2^{-1}g) = (g^{-1}h_1)(h_2^{-1}g) =$$

$g^{-1}(h_1h_2^{-1})g$ . Now  $h_3 = h_1h_2^{-1} \in H$  since  $H$  is a subgroup. Therefore,  $g^{-1}h_3g \in g^{-1}Hg$ . Hence,  $ab^{-1} = g^{-1}h_3g$  implies  $ab^{-1} \in g^{-1}Hg$  for all  $a, b \in g^{-1}Hg$ . By Theorem 1,  $g^{-1}Hg$  is a subgroup of  $G$ .

If we designate  $g^{-1}Hg$  as a conjugate subgroup of  $H$ , we see that if  $H$  is a normal subgroup, for all  $g \in G$ , we have  $g^{-1}(Hg) = g^{-1}(gH) = (g^{-1}g)H = eH = H$  and a normal subgroup has the property that it is equal to all of its conjugates in  $G$  or is self-conjugate. Thus we have proved:

COROLLARY 2-1:  $H$  is a normal subgroup iff  $g^{-1}Hg = H$  for all  $g \in G$ .

DEFINITION 3: If  $A$  and  $B$  are subsets of a group  $G$ ,  $AB$  is the set of all elements  $ab \in G$ , where  $a \in A$  and  $b \in B$ .

It is easy to verify that this multiplication of sets is associative; that is  $(AB)C = A(BC)$ , but not, in general commutative.

THEOREM 3: If  $A$  and  $B$  are normal subgroups of a group  $G$ , the subgroup  $[A, B]$ , generated by  $A$  and  $B$ , coincides with the product  $AB$ .

PROOF:  $[A, B]$  is a subgroup which contains  $A$  and  $B$ . Thus, if  $a \in A$  and  $b \in B$ , then  $a \in [A, B]$  and  $b \in [A, B]$  which implies  $ab \in [A, B]$  by the closure axiom. Hence,  $[A, B] \supseteq AB$ . Now we will show that  $[A, B] \subseteq AB$ . Let  $a_1b_1$  and  $a_2b_2$  be any two elements of  $AB$ , where  $a_1, a_2 \in A$  and  $b_1, b_2 \in B$ . Then,



$$(a_1 b_1)(a_2 b_2)^{-1} = (a_1 b_1)(b_2^{-1} a_2^{-1}) = (a_1 b_1)(b_2^{-1} a_2^{-1})(b_2 b_2^{-1}) =$$

$$(a_1 b_1)(b_2^{-1} a_2 b_2)^{-1} b_2^{-1}$$

since  $(b_2^{-1} a_2 b_2)^{-1} = b_2^{-1} a_2^{-1} b_2$ . Since A is a normal subgroup,

$$b_2^{-1} a_2^{-1} b_2 = a_3 \in A. \text{ Therefore, } (a_1 b_1)(a_2 b_2)^{-1} = (a_1 b_1)(a_3 b_2^{-1}) =$$

$$(a_1 a_3)(a_3^{-1} b_1 a_3) b_2^{-1} = (a_1 a_3)(b_3 b_2^{-1}) \in AB \text{ since } b_3 = a_3^{-1} b_1 a_3 \in B \text{ because}$$

B is a normal subgroup. Thus,  $a_1 a_3 \in A$  and  $b_3 b_2^{-1} \in B$ . Hence, by Theorem

1, AB is a subgroup of G. Therefore,  $[A, B] \subseteq AB$  since  $[AB]$  is the intersection of all subgroups that contain A and B. It follows that  $AB = [A, B]$  as asserted in the theorem.

At this time, we have explored some of the elementary properties of normal subgroups. However, certain groups that do have subgroups have no proper normal subgroups which leads us to the following definition.

**DEFINITION 4:** A group G that contains no proper normal subgroups is a simple group.

## THEORY OF HOMOMORPHISMS

We are assuming that the reader is familiar with the algebraic concept of a homomorphism. We are going to continue with several definitions and theorems that are intimately connected with the concept of a homomorphism between two groups.

DEFINITION 5: The kernel of a homomorphism of a group  $G$  onto a group  $H$  is the subset of  $G$  that is mapped onto the identity element of  $H$ .

THEOREM 4: The kernel  $T$  of a homomorphism of a group  $G$  is a normal subgroup of  $G$ .

PROOF: By Theorem C,  $e \rightarrow e$  and  $e \in T$ . If  $t \rightarrow e$ ,  $t^{-1} \rightarrow u$ , then,  $e = t t^{-1} \rightarrow eu$  by definition c. Now  $e \rightarrow e$ , so  $u = e$ . Therefore,  $t^{-1} \rightarrow e$  and  $t^{-1} \in T$ . Also, if  $t \rightarrow e$ ,  $t_2 \rightarrow e$ , then  $t_1 t_2 \rightarrow ee = e$  implies  $t_1 t_2 \in T$ . Thus, if  $t_1, t_2 \in T$ , then  $t_2^{-1} \in T$  and  $t_1 t_2^{-1} \in T$  and  $T$  is a subgroup by Theorem 1.

Moreover, if  $x \in G$ ,  $t \in T$ , then  $x \rightarrow y$ ,  $t \rightarrow e$ ,  $x^{-1} \rightarrow y^{-1}$  and  $x^{-1} t x \rightarrow y^{-1} e y = e$  implies  $x^{-1} t x \in T$ . Hence,  $T$  is a normal subgroup by Corollary 2-1.

THEOREM 5: In the homomorphism,  $G \rightarrow H$  with kernel  $T$ , two elements of  $G$  have the same image in  $H$  if they belong to the same coset of  $T$ .

PROOF: Suppose  $x \rightarrow u$ ,  $y \rightarrow u$ ,  $x, y \in G$ ,  $u \in H$ . Then  $xy^{-1} \rightarrow uu^{-1} = e$ , and  $xy^{-1} \in T$ . Thus,  $x \in Ty$  and  $x$  and  $y$  are in the same coset of  $T$  by definition D. Conversely, if  $x \in Ty$ , then  $x \in ty$ ,  $t \in T$  and if  $y \rightarrow u$ , we have  $x = ty \rightarrow eu = u$  and  $x$  and  $y$  have the same image in  $H$ .

## FACTOR GROUPS

Next we are going to define the factor group of  $G$  with respect to  $T$  where  $T$  is a normal subgroup of the group  $G$ .

Let  $T$  be a normal subgroup of  $G$  with  $[G:T] = r$ . We can write

$$G = T + Tx_2 + Tx_3 + \dots + Tx_r$$

to indicate that the cosets  $T, Tx_2, Tx_3, \dots, Tx_r$  are disjoint and exhaust  $G$ . Here the indicated addition is only a convenient notation and not to be regarded as an operation. We shall take the cosets  $Tx_i$  as the elements of a system  $H$ . We define a product in  $H$  by  $(Tx_i)(Tx_j) = Tx_k$  if  $x_i x_j \in Tx_k$  in  $G$ . It is conceivable that different elements of  $Tx_i$  and  $Tx_j$  would have a product that belonged to different cosets of  $H$ , and hence would not be well defined. The following theorem shows that this is not possible.

THEOREM 6: The product  $(Tx_i)(Tx_j) = Tx_k$  defined in the system  $H$  is unique, i.e.  $(Tx_i)(Tx_j) = Tx_i x_j$ .

PROOF: Let  $t_1 x_i$  and  $t_2 x_j$  be arbitrary elements of the cosets  $Tx_i$  and  $Tx_j$ , respectively. Here,

$$\begin{aligned}(t_1 x_i)(t_2 x_j) &= (t_1 x_i t_2 x_i^{-1})(x_i x_j) = t_1 (x_i t_2 x_i^{-1})(x_i x_j) \\ &= t_1 (t_2')(x_i x_j)\end{aligned}$$

and  $t_2' \in T$ , by Corollary 2-1 since  $T$  is a normal subgroup. Hence,

$$(t_1 x_i)(t_2 x_j) = (t_1 t_2')(x_i x_j) = t_3 x_i x_j$$

where  $t_3 \in T$  and  $x_i x_j \in Tx_k$  by hypothesis. If  $x_i x_j \in Tx_k$ , then  $t_3 x_i x_j \in Tx_k$ . Thus, all products of one element in  $Tx_i$  and another  $Tx_j$  yield elements of the same coset  $Tx_k$ . Hence, the product does not depend upon the choice of representatives and is well defined.

Now we want to show that the system  $H$  with its well defined binary product forms a group. This is the content of the following theorem.

THEOREM 7: The set of cosets of the normal subgroup  $T$  with the previously defined product forms a group of order  $r = [G:T]$ .

PROOF: Let  $G$  be the aforementioned group with the normal subgroup  $T$ . The product is associative since

$$(Tx_i Tx_j) Tx_k = (Tx_i x_j) Tx_k = Tx_i x_j x_k$$

by successive applications of Theorem 6. Similarly,

$$Tx_i (Tx_j Tx_k) = (Tx_i) (Tx_j x_k) = Tx_i x_j x_k.$$

Therefore,  $(Tx_i Tx_j) Tx_k = Tx_i (Tx_j Tx_k)$  which verifies associativity. Closure is obvious since the group  $G$  is closed.  $T$  is the identity element of  $H$  since  $T (Tx_i) = Tx_i$ .  $Tx_i = x_i T$ , since  $T$  is normal. Therefore,

$$(Tx_i) T = (x_i T) T = x_i T = Tx_i.$$

Thus,  $T$  is both a right and left hand identity. Next, we must show that every element has a right hand inverse. Let  $x_i \in G$ . Then there exist  $x_i^{-1} \in G$ . Hence,  $Tx_j Tx_i$  contains  $x_j x_i^{-1} x_i = e$  and so  $Tx_j Tx_i = T$ . This completes the verification that  $H$  is a group. By definition, the number of elements in  $H$  is  $[G:H] = r$  and  $r$  is the order of  $H$ .

Finally, we formulate the following definition.

DEFINITION 6: If  $G$  is a group and  $T$  is a normal subgroup, then the group  $H$  as defined above is called the factor group of  $G$  with respect to  $T$  written  $H = G/T$ .

In Theorem 3, we showed that the kernel of a homomorphism of a group  $G$  is a normal subgroup  $T$  of  $G$ . Conversely, it is true that every normal subgroup  $T$  is the kernel of a unique homomorphism.

THEOREM 8: Given a group  $G$  and a normal subgroup  $T$  with  $H = G/T$ , there exists a homomorphism  $G \rightarrow H$  whose kernel is  $T$ . This homomorphism is given by  $g \rightarrow Tx_i$  if  $g \in Tx_i$  in  $G$ .

PROOF: Consider the mapping  $g \rightarrow Tx_i$  of  $G$  onto  $H$  when  $g \in Tx_i$  in  $G$ . Let  $g_1 \in Tx_i$ ,  $g_2 \in Tx_j$ . Then,  $g_1 g_2 \in Tx_k$  where  $x_i x_j \in Tx_k$  by Theorem 6. Hence, due to the definition of our mapping,  $g_1 g_2 \rightarrow Tx_k = (Tx_i)(Tx_j)$  by the definition of product in  $H$ . Thus,  $g_1 \rightarrow Tx_i$  and  $g_2 \rightarrow Tx_j$  implies  $g_1 g_2 \rightarrow (Tx_i)(Tx_j)$  and products are preserved. So, we have a homomorphism. In the proof of Theorem 7, we showed that  $T$  is the identity element for  $H$ . Hence,  $g \rightarrow T$  iff  $g \in T$  in  $G$  and  $T$  is the kernel of the homomorphism.

The next theorems relate the homomorphic image of any group  $G$  to a certain factor group of  $G$ .

THEOREM 9: If  $K$  is the homomorphic image of a group  $G$ , then  $K$  is a group.

PROOF: The mode of procedure will be to show the group postulates are satisfied. If  $k_1, k_2 \in K$ , then there exist  $g_1, g_2 \in G$  such that  $g_1 \rightarrow k_1$ ,  $g_2 \rightarrow k_2$ . In general,  $g_1, g_2$  will not be unique. Now  $g_1 g_2 \in G$  and  $g_1 g_2 \rightarrow k_1 k_2$  implying that  $K$  is closed. If  $g_1 \rightarrow k_1$ ,  $g_2 \rightarrow k_2$ ,  $g_3 \rightarrow k_3$ , then  $(g_1 g_2) g_3 = g_1 (g_2 g_3)$  since  $G$  is a group. Also,  $(g_1 g_2) g_3 \rightarrow (k_1 k_2) k_3$  and  $g_1 (g_2 g_3) \rightarrow k_1 (k_2 k_3)$ . Hence, since a mapping assigns every element a unique image, we have  $(k_1 k_2) k_3 = k_1 (k_2 k_3)$  and the associative law holds. Now we must show that  $K$  has an identity. Let  $e$  be the identity of  $G$  and  $e \rightarrow e' \in K$ . Then if  $g \in G$ ,  $g \rightarrow k \in K$ . If  $e \rightarrow e'$ ,  $g \rightarrow k$ , then  $eg \rightarrow e'k$  and  $g \rightarrow e'k$  as well as  $g \rightarrow k$ . Thus,  $e'k = k$ , and  $e'$  is the left hand identity. Similarly, we can show that  $e'$  is the right hand identity of  $K$ . Finally, we must show that every element has a unique inverse. Let  $k \in K$ . Then there exists at least one element  $g \in G$  such that  $g \rightarrow k$ . Now let  $g^{-1} \rightarrow k'$

$$e = g g^{-1} \rightarrow k k',$$

$$e = g^{-1} g \rightarrow k'k$$

and  $e \rightarrow e'$  implies  $e' = k'k$  and  $k' = k^{-1}$ . Thus, every element has a unique inverse and  $K$  is a group.

THEOREM 10: If  $G \rightarrow K$  is a homomorphism of  $G$  onto  $K$  and  $T$  is the kernel, then  $K$  is isomorphic to  $H = G/T$ . If  $x \rightarrow x^*$  in the homomorphism  $G \rightarrow K$ , then  $x^* \mapsto Tx$  is an isomorphism between  $K$  and  $H$ .

PROOF: By Theorem 5, elements in the same coset of  $T$  have the same image in  $K$ . Thus,  $tx \rightarrow x^*$  and  $x^*$  corresponds to a unique  $Tx$ . This implies the correspondence  $x^* \mapsto tx$  is 1-1. Moreover, if  $x \rightarrow x^*$ ,  $y \rightarrow y^*$ , then  $xy \rightarrow x^*y^*$ . However,  $xy \in Txy$ ; hence,  $x^*y^* \mapsto Txy = (Tx)(Ty)$ . Thus, the correspondence  $x^* \mapsto Tx$  preserves products and is an isomorphism of  $K$  and  $H = G/T$ .

Next, we are going to prove a theorem relating the number of subgroups of the factor group  $H = G/T$  and the number of certain special subgroups of  $G$ .

THEOREM 11: Let  $T$  be a normal subgroup of  $G$ . There is a 1-1 correspondence between subgroups  $K^*$  of  $H = G/T$  and the subgroups  $K$  of  $G$  such that  $G \supseteq K \supseteq T$ , where  $K$  consists of all elements of  $G$  mapped onto elements of  $K^*$ .

PROOF: First, we note that for every subgroup  $K$  of  $G$ , there corresponds a subgroup  $K^*$  of  $H$ , the homomorphic image, by Theorem 9. Now, if  $K^*$  is a subgroup of  $H$ , the inverse image  $K$  of  $K^*$  will contain  $T$ , the inverse image of  $e^*$ . Also, if  $a, b \in K$ ,  $a \rightarrow a^*$ ,  $b \rightarrow b^*$ , then  $b^{-1} (b^*)^{-1} \in K^*$  and  $b^{-1} \in K$ . Therefore,  $ab^{-1} \rightarrow a^*(b^*)^{-1} \in K^*$  since  $K^*$  is closed. Hence,  $ab^{-1} \in K$  since  $K$  is the inverse of  $K^*$ . Thus, by Theorem 1,  $K$  is a subgroup of  $G$  and  $T \subseteq K$  implies that  $G \supseteq K \supseteq T$ .

Finally, the inverse image of a subgroup  $K^*$  of  $H$  is a unique subgroup  $K$  such that  $G \supseteq K \supseteq T$ , and the same  $K^*$  is the unique image of  $K$  in the homomorphism  $G \rightarrow H$ . Hence,  $K \mapsto K^*$  is a 1-1 correspondence between,  $G \supseteq K \supseteq T$  and  $H \supseteq K^* \supseteq \{e'\}$ .

Besides the fact that these two groups have certain subgroups in a 1-1 correspondence, we can also show that normal subgroups correspond to normal subgroups.

THEOREM 12: If  $K^*$  is a normal subgroup of the factor group  $H = G/T$  then  $K$  such that  $K \rightarrow K^*$  is a normal subgroup of  $G$  and conversely. Also,  $[G:K] = [H:K^*]$ .

PROOF: If  $K^*$  is normal in  $H$ , then  $x^{-1} Kx \rightarrow x^{*-1} K^* x^* = K^*$  by Corollary 2-1. Hence,  $x^{-1} Kx = K$  for any  $x$  since  $K$  is the inverse image of  $K^*$ . Since  $x^{-1} Kx = K$  for any  $x$ , we have  $y Ky^{-1} = K$  for  $x = y^{-1}$ . Hence,

$$y^{-1} (y Ky^{-1}) y = y^{-1} Ky$$

and  $e Ky = y^{-1} Ky$  for arbitrary  $y$ . Thus, we have  $x^{-1} Kx = K$ , and so  $K$  is normal in  $G$  by Corollary 2-1.

Now suppose that  $K$  is normal. Then, for all  $x \in G$ ,  $x^{-1} Kx = K$ . However,  $x^{-1} Kx \rightarrow x^{*-1} K^* x^*$  and  $K \rightarrow K^*$  implies that  $x^{*-1} K^* x^* = K^*$ . Thus,  $K^*$  is normal in  $H$ .

Finally, we must prove that the index of  $K$  in  $G$  is equal to the index of  $K^*$  in  $H$ . That is, there is a 1-1 correspondence between the cosets  $Kg$  of  $K$  and  $K^* g^*$  of  $H$ . Obviously,  $Kg \rightarrow K^* g^*$ . Also, the inverse image of a coset  $K^* g^*$  is seen to be a coset  $Kg$ , for if  $k^* g^* \in K^* g^*$ , then  $kg \rightarrow k^* g^*$  when  $k \in K$  and  $g \in G$ . Hence,  $[G:K] = [H:K^*]$ .

Next we prove a theorem relating the orders of an element and its image under a homomorphism.

THEOREM 13: If  $G \rightarrow K$  is a homomorphism of  $G$  onto  $K$  and  $x \in G$  such that  $x \rightarrow y$ , then the order of  $y$  in  $K$  divides the order of  $x$  in  $G$  for  $x$  of finite order.

PROOF: Let  $G_1$  be the subgroup of  $G$  generated by  $x$  and  $K_1$  be the subgroup of  $K$  generated by  $y$ . Since a homomorphism preserves the group operation, we have  $x^2 = x \cdot x \rightarrow y \cdot y = y^2$ . Assume that  $x^n \rightarrow y^n$  for  $n \leq k$ . Then,  $x^{k+1} = x \cdot x^k \rightarrow y \cdot y^k = y^{k+1}$  and by mathematical induction,  $x^n \rightarrow y^n$  for all positive integers. Assume that  $x$  is of order  $m$ . Then  $e = x^m \rightarrow y^m$  where  $y^m = e$  by Theorem c. Since  $y^m = e$ ,  $y$  must be of order  $m$  or some divisor of  $m$ , for if the order of  $y$  were equal to  $n < m$  and  $m = kn + r$ ,  $0 < r < n$ , then  $e = y^m = y^{kn+r} = (y^{kn}) (y^r) = e y^r = y^r$  which is a contradiction and completes the proof.



## CYCLIC GROUPS

According to the Corollary to the Theorem of Lagrange, Corollary F-1 of the introduction, the order of a subgroup of a finite group is a divisor of the order of the group. Thus, if  $g$  is the order of  $G$ , and  $h$  is the order of  $H$ , then  $g = hn$  where  $n = [G:H]$ . First, we shall prove some additional corollaries, then we shall show that the converse of the corollary does not hold.

COROLLARY F-2: If  $G$  is a finite group of order  $n$ , the order of every element of  $G$  is a factor of  $n$ .

PROOF: Let  $g \in G$  such that  $g$  is of order  $m$ . Then  $G$  contains the elements  $e, g, g^2, g^3, \dots, g^{m-1}$ . We shall show that the set

$$H = \{e = g^0, g, g^2, \dots, g^{m-1}\};$$

with the binary product defined on  $G$  extended to  $H$ , is a group. Let  $a, b \in H$ . Then  $a = g^{k_1}, b = g^{k_2}$  where  $k_1, k_2$  are nonnegative integers less than  $m$ . Note that,

$$(g^{m-k_2}) g^{k_2} = g^m = e$$

which implies  $b^{-1} = g^{m-k_2}$  unless  $k_2 = 0$  and then  $e^{-1} = e$ . Therefore,  $b^{-1} \in H$ . Moreover,  $ab^{-1} = g^{k_1} g^{m-k_2} = g^{m+k_1-k_2} = g^j$ . If  $j < m$ , then  $ab^{-1} \in H$  and  $H$  is a subgroup. If  $j > m$ , then  $j = mp + r$  where  $p > 0$  and  $0 \leq r < m$  with  $p, r$  both integers. Therefore,  $g^j = g^{mp+r} = (g^m)^p g^r = e^p g^r = e g^r = g^r, 0 \leq r < m$ . Finally, we conclude  $ab^{-1} = g^r \in H$  and  $H$  is a subgroup.

Thus,  $H$  is a subgroup of order  $m$ , and  $m$  must divide  $n$  by Corollary F-1. Since  $g$  was arbitrary, the theorem is proved.

Considerations in the proof of this theorem lead us to the following definitions.

DEFINITION 7: A cyclic group is of the form  $G = e + a + \dots + a^{n-1}$  with  $a^n = e$  where the additive notation indicates only that these elements are members of a group and hence have a binary product defined between them. We say that  $G$  is generated by the element  $a$  and write  $G = \{a\}$  to denote this fact.

Now we are ready to show that finite groups of certain orders must necessarily be cyclic.

COROLLARY F-3: A group of prime order has no proper subgroups and is necessarily cyclic.

PROOF: If the order of the group  $G$  is a prime number  $p$ , the order of a subgroup must be either 1 or  $p$ , that is the subgroup consists of either the single element  $e$  or contains all  $p$  elements of the group.

If  $a$  is an element other than  $e$ , its order, being greater than 1, is necessarily equal to  $p$ , since it must divide  $p$  by Corollary F-2. Hence, the  $p$  elements  $e, a, a^2, \dots, a^{p-1}$  are all distinct and belong to  $G$ . Thus, they must be all the  $p$  elements of  $G$  in some order and  $G = \{a\}$ .

As an immediate consequence of Corollary F-2, we have:

COROLLARY F-4: If  $G$  is a finite group of order  $n$ , then  $a^n = e$  for each  $a \in G$ .

Now we are ready to examine cyclic groups more closely. We can obtain complete information about all the possible subgroups of a cyclic group from the following theorem.

THEOREM 14: All subgroups of a cyclic group are cyclic. If  $G = \{a\}$  is a cyclic group of order  $n$ , then corresponding to every divisor  $d$  of  $n$  there exists one, and only one, subgroup of order  $d$ , which may be generated by  $a^m$  where  $n = md$ .

PROOF: The elements  $e, a^m, a^{2m}, \dots, a^{(d-1)m}$  are distinct (12-1) since an equality between any two of them would imply  $a^{k_1 m} = a^{k_2 m}$  where

$$0 \leq k_1 < k_2 \leq d-1.$$

Thus,  $k_2 = k_1 + j$  where  $0 < j \leq d-1$  and

$$a^{k_1 m} = a^{(k_1+j)m} = a^{k_1 m} a^{jm}$$

implies  $a^{jm} = e$ . However,  $a^{jm} = e$ ,

$$0 < jm \leq (d-1)m < dm = n$$

contradicts the assumption that  $a$  is of order  $n$ . Therefore, the elements

$$e, a^m, a^{2m}, \dots, a^{(d-1)m}$$

form a cyclic subgroup of order  $d$ . This shows that for every divisor  $d$  of  $n$  there exists at least one subgroup of order  $d$ .

Now we will show that the subgroup generated by  $a^m$  is the only subgroup of order  $d$  in  $G$ . Suppose,

$$H = e + a_1 + a_2 \dots + a_{d-1}$$

is a subgroup of order  $d$  of  $G$ . Since  $a_i$  is an element of  $\{a\}$ , it must be of the form  $a_i = a^{\lambda_i}$  where  $0 < \lambda_i < n$ . As  $H$  is of order  $d$ , the order of every element of  $H$  is a factor of  $d$ . Hence,

$$a_i^d = e \text{ for } i = 1, 2, \dots, d-1.$$

It follows that  $a_i^d = (a^{\lambda_i})^d = a^{d\lambda_i} = e$ . From this we see that  $d\lambda_i$  is a multiple of  $n$  since  $a$  is of order  $n$ . Let  $d\lambda_i = k_i n = k_i m d$  where  $k_i$  is a positive integer. Then  $\lambda_i = k_i m$  and  $a_i = a^{\lambda_i} = a^{k_i m} = (a^m)^{k_i}$  which shows

that each  $a_i$  is in fact a power of  $a^m$ . We have seen that not more than  $d$  of these powers are distinct, namely the  $d$  elements listed in (12-1). Hence, the  $d$  elements of  $H$  are the same as those listed in (12-1) and  $H = \{a^m\}$  which completes the proof.

## NON-CYCLIC FINITE GROUPS

From Theorem 14, we have gained complete understanding of the subgroups of a cyclic group. Also, we know that every finite group of prime order is cyclic and has no proper subgroups. Moreover, we can write down the order of every subgroup of a finite cyclic group of composite order. But what do we know about the nature of the subgroups of finite groups of composite order that are not cyclic? The Theorem of Lagrange and Corollary F-1 tell us that a finite group of order  $n$  cannot have a subgroup whose order is not a divisor of  $n$ . Now we will show that the converse of Corollary F-1 does not hold. Thus, we may not have a subgroup of order  $d$  even though  $d$  does divide  $n$ .

Consider the group of order 12 generated by elements  $a, b, c$  with defining relationships  $a^2 = b^2 = c^3 = e$ ,  $ab = ba$ ,  $ca = bc$ , and  $cb = abc$ . The subset  $H_1 = e + a$  is a subgroup of order 2.  $H_2 = e + c + c^2$  is a cyclic subgroup of order 3.  $H_3 = e + a + b + ab$  is an abelian subgroup of order 4. Now, we find that a subgroup of order 6 is going to have to include all three of the basis elements  $a, b$ , and  $c$ . If we try to omit  $c$ , we have  $H_3$ . If we try to form a subgroup omitting  $a$  or  $b$ , we reach the contradictions

$$(bc)(bc^2) = b(cb)c^2 = b(abc)c^2 = (ba)(b)c^3 = (ab)b = a$$

and

$$(ac^2)(ac) = ac(ca)c = ac(bc)c = a(cb)c^2 = a(abc)c^2 = b$$

respectively. However, if we include all three of the basis elements  $a, b$ , and  $c$  in our subgroup, we will have to generate the entire group of order 12. Hence, no subgroup of order 6 can exist for this particular group.

We may summarize our result in the following theorem.

THEOREM 15: A finite group of order  $n$  need not have a subgroup of order  $d$  if  $d$  is a divisor of  $n$ .

Thus, in general if  $m$  divides  $n$ , we cannot be sure that a group of order  $n$  contains a subgroup of order  $m$ . However, it is true that if  $m$  is a prime or prime power, then such subgroups always exist. The existence of and number of such subgroups are the subject of a division of group theory known as Sylow Theory. The remainder of this paper will be directly concerned with the exposition and proof of these remarkable results discovered by the Norwegian mathematician, L. Sylow in 1872. First, we will state some needed definitions.

DEFINITION 8: A group  $P$  is a  $p$ -group if every element of  $P$  except the identity has order a power of a prime  $p$ .

DEFINITION 9: A subgroup  $S$  of a group  $G$  is a Sylow subgroup of  $G$  if it is a  $p$ -group and is not contained in any larger  $p$ -group which is a subgroup of  $G$ .

## SYLOW THEOREMS

The following theorem will serve as a starting point for the more general Sylow theorems.

THEOREM 16: (Cauchy's Theorem) If the order of a group  $G$  is divisible by a prime  $p$ , then  $G$  contains an element of order  $p$ .

PROOF: Let  $n = mp$  be the order of  $G$ . Here, if  $m = 1$ ,  $G$  is the cyclic group of order  $p$  and the theorem is true. We proceed by induction on  $m$ . Assume that  $G$  contains an element of order  $p$  for  $o(G) = mp$  where  $m = 1, 2, \dots, k$ . Then we must show that  $G$  contains an element of order  $p$  for  $o(G) = (k+1)p$ . If  $G$  does not contain a proper subgroup, it is cyclic and of prime order. However,  $(k+1)p = n$  is not prime, so  $G$  must contain a proper subgroup  $H$ . If  $[G:H]$  is not divisible by  $p$ , then

$$(k+1)p = o(H) [G:H]$$

implies  $o(H)$  is divisible by  $p$ . Thus,  $o(H) = jp$  where  $j$  divides  $k+1$  and  $1 \leq j \leq k$  since  $H$  is a proper subset. Then, by the induction hypothesis,  $H$  contains an element of order  $p$ .

Now suppose that every proper subgroup of  $G$  has an index divisible by  $p$ . From Theorem H, we can write,

$$G = C_1 + C_2 + \dots + C_s$$

where the  $C_i$  are disjoint classes that exhaust  $G$ . Now taking the cardinal number of  $G$  and each set, we have

$$o(G) = o(C_1) + o(C_2) + \dots + o(C_s).$$

Therefore,

$$n = n_1 + n_2 + \dots + n_s,$$

where each  $n_i$  is the number of conjugates in a class of elements of  $G$ .

From Theorem G, the number of conjugates of  $\{s\}$  under  $G$  is the index in  $G$  of the normalizer of  $\{s\}$  in  $G$ . Therefore, if  $s \in C_i$ , then  $n_i = [G : N_G(\{s\})]$ . We note that  $N_G(\{s\})$  is the subgroup of all  $g \in G$  such that  $g^{-1}\{s\}g = \{s\}$ .

Thus, each  $n_i \neq 1$  is the index of a proper subgroup in  $G$ , and hence, by hypothesis, divisible by  $p$ . We let  $C_1 = \{e\}$  since the identity forms a class. This implies that  $n_1 = 1$ . Also,  $o(G) = (k+1)p$  and we have

$$(k+1)p = n = 1 + n_2 + n_3 + \dots + n_s$$

where  $n_i = m_i p$  if  $n_i \neq 1$ . Now  $p$  divides the right hand side of the above equation, hence, the number of  $n_i$ 's equal to one is a multiple of  $p$ . An element  $a_i$  is a class in  $G$  iff it belongs to the center  $Z$  of  $G$  since  $x^{-1} a_i x = a_i$  for each  $x \in G$  iff  $a_i^{-1} x a_i = x$  for each  $x \in G$ . This is easily verified by multiplying  $x^{-1} a_i x = a_i$  by  $a_i^{-1} x$ . Thus,  $o(Z)$  equals the number of  $n_i$  such that  $n_i = 1$ , and so  $o(Z)$  is divisible by  $p$ . Then for  $z \in Z$  and any of  $g \in G$ , we have  $z^{-1} g z = g$  implies  $gZ = Zg$ . Hence, the elements of  $Z$  certainly commute with each other and  $Z$  is an Abelian group. From Theorem I,  $Z$  contains an element of order  $p$ . Hence,  $G$  of order  $(k+1)p$  contains an element of order  $p$  and by induction the proof is complete.

**COROLLARY 16-1:** If the order of a group  $G$  is divisible by a prime  $p$ , then  $G$  contains an Abelian subgroup  $H$  of order  $p$ .

**PROOF:** From Theorem 15, we have  $a \in G$  such that  $a$  is of order  $p$ . Then  $H = \{a\}$  is a cyclic subgroup of order  $p$ . Since every cyclic subgroup is Abelian, the theorem is proved.



Next we shall show that if  $G$  is of order  $n = p^m s$ , then there will be subgroups of order  $p, p^2, p^3, \dots, p^m$ . First, we need the following lemma.

LEMMA 17-1: If  $H$  is a subgroup of  $G$  and  $G \subseteq N_G(H)$ , then  $H$  is a normal subgroup of  $G$ .

PROOF: Let  $g \in G$  be arbitrary. Then, by hypothesis,  $g \in N_G(H)$ . Therefore,  $g^{-1}Hg = H$  and  $Hg = gH$ . Hence, by definition,  $H$  is a normal subgroup of  $G$ .

THEOREM 17: (First Sylow Theorem) If  $G$  is of order  $n = p^m s$  where  $p$  does not divide  $s$  and  $p$  is prime, then  $G$  contains subgroups of orders  $p^i$ ,  $i = 1, 2, \dots, m$ , and each subgroup of order  $p^i$ ,  $i = 1, 2, \dots, m-1$ , is a normal subgroup of at least one subgroup of order  $p^{i+1}$ .

PROOF: The proof is by induction on  $i$ . First we must show that we have a subgroup of order  $p$ . Next we will show that if  $P$  is a subgroup of order  $p^i$ ,  $1 \leq i < m$ , then there exists a subgroup of order  $p^{i+1}$  containing  $P$  as a normal subgroup. Thus, if we let  $H_1$  be a subgroup of order  $p^1$ , we see that the existence of  $H_1$  implies  $H_2$  exists implies  $H_3$  exists and so on until  $H_{m-1}$  implies that  $H_m$  exists. Obviously, this will complete the proof of the theorem.

We see that  $H_1 = \{a\}$  is a cyclic subgroup of order  $p$  as discussed in Corollary 16-1. Now assume that  $P$  is a subgroup of order  $p^i$ ,  $1 \leq i < m$ . Write  $G$  in terms of double cosets of  $P$  as described by Definition N. Therefore,  $G = P + P x_2 P + \dots + P x_r P$  and let there be  $a_k$  right cosets of  $P$  in  $P x_k P$ . Then  $[G:P]$  equals the cardinal number of right cosets of  $P$  in  $G$  by Definition F and  $[G:P] = a_1 + a_2 + \dots + a_r$  where

$$a_k = [x_k^{-1} P x_k : x_k^{-1} P x_k \cap P]$$

from Theorem K. Moreover,  $a_1 = 1$  for the double coset  $P e P = P$  since the index of  $P$  in  $P$  is 1. From Theorem F, we have

$$o(x_k^{-1} P x_k) = o(x_k^{-1} P x_k \cap P) a_k.$$

Now  $P$  is a subgroup of order  $p^i$  and so by Theorem 2,  $x_k^{-1} P x_k$  is a subgroup of order  $p^i$ . Hence, we may write  $p^i = o(x_k^{-1} P x_k \cap P) a_k$ . From this equation, we can see that if  $a_k \neq 1$ , then  $a_k = p^j$ ,  $1 < j < i$ . Moreover,  $o(G) = o(P) [G:P]$  implies  $p^m s = p^i [G:P]$ , where  $i < m$ . Therefore,  $p^{m-i} s = [G:P]$ . Since  $p$  divides  $[G:P]$  and  $[G:P] = \sum_{k=1}^r a_k$  with each  $a_k = 1$  or a power of  $p$ , the number of  $a_k = 1$  must be an  $k=1$  integral multiple of  $p$ . Furthermore,  $a_1 = 1$  implies that the number of  $a_k$ 's equal to one must be a positive integral multiple of  $p$ . Let  $U$  be the number of  $a_k$ 's equal to one.

If  $a_k = 1$ , then  $o(x_k^{-1} P x_k) = o(x_k^{-1} P x_k \cap P)$  and  $x_k^{-1} P x_k = P$  since  $P$  and its transform are subgroups of the same order whose intersection has that order. Moreover,  $x_k$  and the coset  $P x_k = x_k P$  must belong to the normalizer  $K$  of  $P$ . Conversely, if  $x_k \in K$ , then  $x_k^{-1} P x_k = P$  and  $o(x_k^{-1} P x_k) = o(x_k^{-1} P x_k) a_k$  implies  $a_k = 1$ . Thus,  $U = [K:P]$  since for every coset  $x_k P$  of  $K$ , there corresponds one  $a_k = 1$  and vice versa. Therefore,  $p$  divides  $[K:P]$ .

Hence, the factor group  $K/P$  has order  $[K:P]$  divisible by  $p$  from Theorem 7. Thus,  $K/P$  contains a subgroup of  $J^*$  of order  $p$  from Corollary 16-1. By Theorem 11,  $J^* \cong J$  where  $P \subseteq J \subseteq K$ , and  $[J:P] = [J^*:\{e\}] = p$ . Therefore,  $o(J) = o(P) p$  and  $o(J) = p^i p = p^{i+1}$ . Thus,  $J$  is a subgroup of order  $p^{i+1}$  containing  $P$  as a subgroup. Furthermore,  $P$  is a normal subgroup of  $J$  from Lemma 16-1 since  $J \subseteq N_G(P) = K$ . This completes the proof.

Now we are ready to consider some of the consequences of the first Sylow Theorem.

Let us consider a group of order  $324 = 2^2 \cdot 3^4$ . From Theorem 17, we know that we have subgroups of orders

$$2, 2^2 = 4, 3, 3^2 = 9, 3^3 = 27, 3^4 = 81.$$

We may have several subgroups of a certain order, but we know that we must have at least one subgroup with each of the given order. If the group were generated by the elements  $a, b$  with defining relations,

$$ba = ab, a^4 = e, b^{81} = e,$$

then it would have exactly one subgroup with each of the above orders.

THEOREM 18: A group is of order  $p^m$ ,  $m$  a positive integer, iff it is a  $p$  group.

PROOF: From Corollary F-2, we find that if  $o(G) = p^m$ , then the order of every element of  $G$  divides  $p^m$ . Hence, every element except the identity has order  $p^i$ ,  $1 \leq i \leq m$ , and  $G$  is a  $p$  group.

Suppose that  $G$  is not of order  $p^m$ . Then  $o(G) = p \cdot q \cdot s$  where  $p$  and  $q$  are distinct primes. Then from Theorem 16,  $G$  contains at least one element of order  $p$  and one of order  $q$ . Thus, no prime can exist such that every element has order a power of that prime. Therefore,  $G$  is not a  $p$  group.

Recalling Definition 9, we prove the following corollary.

COROLLARY 18-1: Every finite group  $G$  of order  $n = p^m s$ , where  $p$  does not divide  $s$  and  $p$  is a prime, contains a Sylow subgroup of order  $p^m$ , and every  $p$  group which is a subgroup of  $G$  is contained in a Sylow subgroup of  $G$ .

PROOF: A Sylow subgroup is a  $p$  group which is not contained in any larger  $p$  group and from Theorem 17,  $G$  has a subgroup of order  $p^m$ . It is a Sylow group since  $p^{m+1}$  cannot divide  $n$  and so no larger  $p$  group can exist by Theorem 18.

The remainder of the Corollary follows directly from Theorem 18 since every  $p$  subgroup is of order  $p^i$ ,  $1 \leq i \leq m$ , and each of these groups is contained in a group of order  $p^m$  which is a Sylow subgroup of  $G$ . This result follows from Theorem 17.

The above theorem shows that every finite group  $G$  contains at least one Sylow subgroup that is a  $p$  group for every prime that divides  $o(G)$ . These subgroups for a fixed prime are the subject of the Second Sylow Theorem.

THEOREM 19: (Second Sylow Theorem) In a finite group  $G$ , the Sylow  $p$  subgroups are conjugate.

PROOF: By Sylow  $p$  subgroups, we mean the Sylow subgroups corresponding to the prime  $p$  that divides  $o(G)$ . Let  $P_1$  and  $P_2$  be two Sylow  $p$  subgroups. Then,

$$G = P_1 P_2 + P_1 x_2 P_2 + \dots + P_1 x_r P_2.$$

Let there be  $b_i$  right cosets of  $P_2$  in  $P_1 x_i P_2$ . From Theorem K,

$$b_i = [x_i^{-1} P_1 x : P_2 \cap x_i^{-1} P_1 x_i].$$

From Theorem F, we have,

$$o(x_i^{-1} P_1 x_i) = o(P_2 \cap x_i^{-1} P_1 x_i) b_i.$$

However,  $o(x_i^{-1} P_1 x_i) = o(P_1) = p^m$  from Theorem 2. Therefore,

$$p^m = o(P_2 \cap x_i^{-1} P_1 x_i) b_i.$$

From this equation we see that  $b_i$  is either 1 or a power of  $p$ . Now,

$$b_1 + b_2 + \dots + b_r = [G:P_2]$$

by Theorem K, and

$$[G:P_2] = o(G) / o(P_2) = p_m s / p^m = s$$

where  $p$  does not divide  $s$ . Hence, for some  $i$ ,  $b_i = 1$  and,

$$o(x_i^{-1} P_1 x_i) = o(P_2 \cap x_i^{-1} P_1 x_i).$$

Since  $P_2$  and  $x_i^{-1} P_1 x_i$  have exactly the same order and this order is the order of their intersection, they must be the same subgroup and

$$x_i^{-1} P_1 x_i = P_2$$

proving the Sylow  $p$  subgroups are conjugate.

The following theorem is the last Sylow Theorem. However, before proving the theorem we will state and prove a needed lemma.

**LEMMA 20-1:**  $S_i$  is the only Sylow  $p$  subgroup of  $G$  contained in the normalizer  $K_i = N_G(S_i)$ .

**PROOF:** Deny the Lemma. Then there exists a Sylow subgroup  $S_j$ , such that  $S_j \subseteq K_i$ . Let  $o(S_i) = p^r$  so that  $o(G) = p^r s$  where  $p$  does not divide  $s$ . Choose  $x \in S_j \setminus S_i$ . Since  $S_j$  is a  $p$  group, the order of  $x$  is  $p^k$  for some positive integer  $k$ . Also  $x \in S_j$  implies  $x \in K_i$ .

Now let  $\langle S_i, x \rangle$  be the group generated by  $x$  and all elements of  $S_i$ .  $\langle S_i, x \rangle$  is not a  $p$  group since it properly contains  $S_i$ , a Sylow  $p$  group. From Theorem 12,

$$o(\langle S_i, x \rangle / S_i) = [\langle S_i, x \rangle / S_i : \{e\}] = [\langle S_i, x \rangle : S_i]$$

and

$$o(\langle S_i, x \rangle) = o(S_i) [\langle S_i, x \rangle : S_i] = p^r o(\langle S_i, x \rangle / S_i).$$

Therefore,

$$o(\langle S_i, x \rangle / S_i) = s'$$

where  $p$  does not divide  $s'$  and  $s'$  divides  $s$ .

Next we show that  $\langle S_i, x \rangle / S_i$  is a cyclic group generated by  $xS_i$ .

Assume  $xS_i$  is of order  $m$ ; then  $\{xS_i\}$  contains

$$S_i = (xS_i)^m, xS_i, (xS_i)^2, \dots, (xS_i)^{m-1}.$$

Now all the cosets of  $\langle S_i, x \rangle$  other than  $S_i$  are of the form

$$xS_i, x^2 S_i, x^3 S_i, \dots, x^{p^k-1} S_i$$

since these  $p^k-1$  powers of  $x$  are the only elements of  $\langle S_i, x \rangle$  that do not belong to  $S_i$ . Now

$$(xS_i)^2 = (xS_i)(xS_i) = x(xS_i x^{-1})(xS_i) = x^2 S_i (x^{-1}x) S_i = x^2 S_i$$

where  $S_i = xS_i x^{-1}$  because  $x \in K_i$ . If we assume  $(xS_i)^n = x^n S_i$  for  $n \leq q$ , then

$$\begin{aligned} (xS_i)^{q+1} &= (xS_i)^q (xS_i) = (x^q S_i)(xS_i) = x^q (xS_i x^{-1})(xS_i) \\ &= x^{q+1} S_i (x^{-1}x S_i) = x^{q+1} S_i. \end{aligned}$$

Thus, by mathematical induction,  $(xS_i)^n = x^n S_i$  for all positive integers  $n$ . Thus,

$$(xS_i)^{p^k} = x^{p^k} S_i = e S_i = S_i$$

and  $m$  divides  $p^k$  by Corollary F-2. Therefore,  $\langle S_i, x \rangle / S_i$  is a cyclic group of order  $p^{k'}$  where  $1 \leq k' \leq k$ . However,

$$o(\langle S_i, x \rangle / S_i) = p^{k'} = s'$$

which is an obvious contradiction since we have previously shown that  $p$  does not divide  $s'$ .

**THEOREM 20:** (Third Sylow Theorem) The number of Sylow  $p$  subgroups of a finite group  $G$  is of the form  $1 + kp$  and is a divisor of the order of  $G$ .

PROOF: This is trivial if there is only one Sylow  $p$  subgroup since  $k = 0$ . Thus, we assume that we have more than one such subgroup. Let  $S_0$  be one Sylow  $p$  subgroup and

$$S_1, S_2, S_3, \dots, S_r$$

the remaining ones. All these subgroups have order  $p^m$  where  $p$  is a prime and  $o(G) = p^m s$  where  $p$  does not divide  $s$ . These fall into a number of disjoint conjugate sets with respect to transformation by elements of  $S_0$ . This follows from the Second Sylow Theorem and Definition J. Now  $H \subseteq N_G(H)$  for every subgroup  $H$  in  $G$  since  $h^{-1} H h = H$  for all  $h \in H$ . By Lemma 20-1,  $S_i$  is the only Sylow  $p$  subgroup in its normalizer  $K_i$ . Hence, the normalizer of  $S_i$  in  $S_0$ ,  $k \neq 0$ , is a proper subgroup of  $S_0$ . By Theorem G, the number of conjugates of  $S_i$  under  $S_0$  equals

$$n_i = [S_0 : N_{S_0}(S_i)].$$

From Theorem F,

$$o(S_0) = o(N_{S_0}(S_i)) \text{ and } p^m = o(N_{S_0}(S_i)) n_i.$$

Since  $N_{S_0}(S_i)$  is a proper subgroup of  $S_0$ ,  $n_i > 1$ . Hence,

$$[S_0 : N_{S_0}(S_i)] = n_i = p^{e_i}, \quad 1 \leq e_i \leq m,$$

for all  $i$  such that  $1 \leq i \leq r$ .

Now we shall show that exist a certain number of Sylow subgroups whose conjugates under  $S_0$  exhaust the total number of conjugates of  $S_0$  under  $G$  with no repetition. Let  $C_1$  be the set of all distinct conjugates of  $S'_1 = S_1$  under  $S_0$ . If  $C_1$  exhausts the set of conjugates of  $S_0$ , we are through. If not, choose a subgroup  $S_i$  such that  $S_i \notin C_1$ . Call this subgroup  $S'_2$ .

Note that none of the conjugates of  $S_2'$  under  $S_0$  can belong to  $C_1$ .

Assume the contrary. Then there exists  $x \in S_0$  such that  $x^{-1} S_2' x \in C_1$  and  $x^{-1} S_2' x = y^{-1} S_1 y$  for  $y \in S_0$ . Thus,

$$S_2' = x (y^{-1} S_1 y) x^{-1} = (yx^{-1})^{-1} S_1 (yx^{-1})$$

where  $yx^{-1} \in S_0$  and  $S_2' \in C_1$  which is a contradiction. Let  $C_2$  be the set of all distinct conjugates of  $S_2'$  under  $S_0$ . If  $C_1 \cup C_2$  exhausts the set of conjugates of  $S_0$ , the assertion is proved. If not, continue the process.

By the above argument, we can continue this process until the set of conjugates is exhausted which must be after a finite number of steps, say  $q$ .

Then,

$$C_1 \cup C_2 \cup \dots \cup C_q$$

is the set of all conjugates of  $S_0$  where the  $C_i$  are disjoint in pairs. Thus,  $r$  equals the sum of the number of elements in all of the  $C_i$  where  $C_i$  is the set of all conjugates of  $S_i'$  under  $S_0$ . As previously shown,

$$o(C_i) = [S_0 : N_{S_0}(S_i')] = n_i' = p^{e_i'}, 1 \leq e_i' \leq m,$$

and

$$r = p^{e_1'} + p^{e_2'} + \dots + p^{e_q'} = k p.$$

Thus, there are  $1 + r = 1 + kp$  Sylow  $p$  subgroups of  $G$ . The number of Sylow  $p$  subgroups is, by the Second Sylow Theorem and Theorem G, the index of the normalizer of  $S_0$  which is a subgroup of  $G$ . Thus,  $[G : N_G(S_0)] = 1 + kp$  is a divisor of the order of  $G$ .



## ACKNOWLEDGMENT

The author wishes to express his sincere appreciation to Dr. Richard L. Yates for his patient assistance in the preparation of this report.

## REFERENCES

- Birkhoff, G. and MacLane, S., A Survey of Modern Algebra, New York: The Macmillan Company, 1959.
- Carmichael, Robert D., Introduction to the Theory of Groups of Finite Order, New York: Dover Publications, 1956.
- Hall, Marshall, Jr., The Theory of Groups, New York: The Macmillan Company, 1959.
- Ledermann, Walter, Introduction to the Theory of Finite Groups, New York: Interscience Publishers, 1957.
- Moore, John T., Elements of Abstract Algebra, New York: The Macmillan Company, 1962.
- Scott, W. R., Group Theory, Englewood Cliffs: Prentice-Hall, Inc., 1964.
- Zassenhaus, Hans J., The Theory of Groups, New York: Chelsea Publishing Company, 1958.

THEOREMS OF SYLOW THEORY

by

SAMUEL A. MUSIL

B. S., Kansas State University, 1964

---

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY  
Manhattan, Kansas

1965

L. Sylow discovered three remarkable theorems in 1872, which serve as the foundation of the study of subgroups of finite groups. The purpose of this report is to develop the preliminary theory and finally prove the three Sylow Theorems.

In the first section we define normal subgroups and develop a simple test for determining whether or not a subset is a subgroup. Also, we develop some simple characteristics of normal subgroups.

The application of homomorphisms is developed in the second section and important theorems leading to the definition of a factor group and characterizations of their subgroups are proved. These theorems are essential in actually proving the Sylow theorems.

Certain properties of the elements and subgroups of finite groups are developed. Theorem 13 completely describes the structure of cyclic groups. Next we show that the order of a group may be divisible by  $d$  and yet no subgroup of order  $d$  need exist. This leads us to general questions about the existence of subgroups and hence, the Sylow Theorems.

In the last sections, the three Sylow Theorems, some necessary lemmas, and certain important corollaries are proved. Also, Sylow subgroups and  $p$ -groups are defined in the last section. With the Sylow theorems, we see that if  $p^m$  divides the order of  $G$ , then a subgroup of order  $p^m$  must exist.