SYLOW'S THEOREMS

A Thesis

Presented to

the Faculty of the Department of Mathematics

Kansas State Teacher's College

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

---

by

Douglas Scott Kelsey

July 1973

TABLE OF CONTENTS

ACKNOWLEDGMENT

I wish to express my gratitude to Dr. George Poole for his suggestions and many hours of assistance in writing this thesis.

George D. Poole

Approved for the Major Department

John E. Peterson

Approved for the Graduate Council

Chapter I

INTRODUCTION

After having read and studied a text in mathematics, many students find the approach similar to studying and reading a foreign language. Quite often there seems to be little application or utilization of the material which is to become an integral part of one's mathematical knowledge. Proofs are so concise, it is difficult to understand their actual meaning or implication.

The objective of this thesis is to survey a small area of mathematics, prove the necessary lemmas, theorems, and corollaries in detail, and present an application of these.

Group theory is the general area which is explored. Specifically, Sylow's theorems are presented, each proved in detail, and followed by an application of the theorems.

Ludwig Sylow (1832-1918) was a Scandanavian mathematician from Friedrichshald, Norway. Although his three theorems are very important in group theory, little has been written about his life, or even his contribution to the theory of groups. If one looks through history of mathematics texts, only once in a great while does the name Ludwig Sylow appear. In Smith's History of Mathematics, when speaking of great Scandanavian mathematicians, Sylow's

name is found only in the footnotes indicating that he wrote Discours in 1902. Also, he wrote a book with Marius Sophus Lie on the contributions of Niels Henrick Abel entitled Abel [3]. Of course, Abel is the man whom abelian groups are named after. As the material in this thesis is presented, one will have more insight as to Sylow's contribution to mathematics.

When writing in group theory, one must assume the reader has a basic knowledge of groups. Even so, Chapter II contains those definitions and theorems which are essential in reading this thesis. A proof of Cayley's theorem appears as a lemma, so that it may be used to prove an important theorem about simple groups.

Chapter III contains basic definitions about the structure of groups and proofs of Cauchy's theorems. This leads to proofs of Sylow's theorems, which is the essence of this thesis. An application of his theorems follow in Chapter IV.

Chapter II

BASIC DEFINITIONS AND CAYLEY'S THEOREM

The notation used in group theory varies widely from text to text. This chapter contains the notation used in this thesis, while stating the basic definitions which are fundamental in the study of Sylow's theorems. Also, there is an important theorem proved concerning simple groups, which is used in conjunction with Sylow's theorems in Chapter IV. The reader may refer to Ames [1] and Herstein [5] for general reference texts.

DEFINITION 2.1. A set G of elements is a group under the binary operation $(\cdot)$ if for all $a, b, c \in G$,

a) $a \cdot b \in G$ (Closure)

b) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associative)

c) There exist $e \in G$ such that $a \cdot e = e \cdot a = a$ (Identity)

d) There exist $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$ (Inverse)

The binary operation in all groups considered (including abelian groups) is denoted multiplicatively. Furthermore, G and G' usually denote groups while H, K, and P denote subgroups. An abelian group is a group which is commutative.

DEFINITION 2.2. If H is a subset of group G, and H satisfies the properties of a group under the same binary operation of G, then H is a subgroup of G.

DEFINITION 2.3. If S is a set with n elements, then the symmetric group of degree n, denoted by S_n, is the set of all bijective mappings on the set S under the binary operation of map composition. The order of S_n is $n!$ [5].

Coset is now defined. Once coset is defined, we define normal subgroup; and subsequently, define a simple group.

DEFINITION 2.4. Suppose H is a subgroup of G and $x \in G$. A right coset of H in G is the set Hx of all elements of the form hx, where $h \in H$. Similarly, a left coset is the set xH.

Any two right (left) cosets are either identical or disjoint. Also, the coset xH and Hx need not be equal. For abelian groups, xH must equal Hx. For non-abelian groups, the following example shows that xH need not equal Hx.

EXAMPLE 2.5. Consider the symmetric group S_3. By Definition 2.3 there are $3! = 6$ bijective mappings on set S. Let $S = \{x, y, z\}$ and f_1, f_2, f_3, f_4, f_5, and f_6 represent the bijective mappings as indicated below:

f_1: $x \to x$, $y \to y$, $z \to z$

f_2: $x \to x$, $y \to z$, $z \to y$

f_3: $x \to z$, $y \to y$, $z \to x$

f_4: $x \to y$, $y \to x$, $z \to z$

f_5: $x \to z$, $y \to x$, $z \to y$

f_6: $x \to y$, $y \to z$, $z \to x$

Now, under the binary operation of map composition, consider the following group table:

$\cdot$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

Consider the subgroup $H_1 = \{f_1, f_4\}$. To show $xH \neq Hx$ for some $x \in S_n$, let $x = f_2$.

$xH_1 = \{f_2f_1, f_2f_4\} = \{f_2, f_6\}$ and $H_1x = \{f_1f_2, f_4f_2\} = \{f_2, f_5\}$. Hence, for $x = f_2 \in S_n$, $xH_1 \neq H_1x$.

Consider another subgroup $H_2 = \{f_1, f_5, f_6\}$. $xH_2 = \{f_2f_1, f_2f_5, f_2f_6\} = \{f_2, f_4, f_3\}$ and $H_2x = \{f_1f_2, f_5f_2, f_6f_2\} = \{f_2, f_3, f_4\}$. Hence $xH_2 = H_2x$.

DEFINITION 2.6. A subgroup H of a group G is a <u>normal subgroup</u> if and only if $xH = Hx$ for all $x \in G$, or equivalently, $xHx^{-1} = H$ for all $x \in G$. Denote that H is normal in G by $H \triangleleft G$.

In Example 2.5, H_2 is a normal subgroup.

DEFINITION 2.7. A simple group is a group which has no proper normal subgroups.

It is easily determined that for a group G, G and $\{e\}$, where e is the identity element, are normal subgroups of G.

The set of right (left) cosets of H in G is represented by G/H. G/H forms a group in a natural way if $H \triangleleft G$. The binary operation on G/H is defined by $(xH) \cdot (yH) = xyH$. The group G/H is called the quotient group [1].

The index of G/H, or the number of distinct right (left) cosets of H in G, is denoted by $|G:H|$.

LaGrange's theorem is fundamental in Group Theory. In this thesis, the order of a group G is denoted by #G.

THEOREM 2.8. (LaGrange's Theorem). If H is a subgroup of a finite group G, then $|G:H| = \frac{\#G}{\#H}$ [1].

This Theorem implies that the order of a subgroup H of a finite group G must divide the order of G, and the quotient will yield the number of distinct right (left) cosets of H in G, or the index of H in G.

DEFINITION 2.9. A homomorphism is a mapping f from a group G into a group G' such that f preserves the group operation. That is, if $x, y \in G$, then $f(x)f(y) = f(xy)$.

DEFINITION 2.10. An isomorphism is a homomorphism which is bijective.

DEFINITION 2.11. The kernel of a homomorphism f from G to G' is the set of elements in G that are mapped to the identity element in G'. The kernel of f, denoted by $\ker(f)$, is a normal subgroup of G [1].

With the preceding terminology and background, the first important theorem of this thesis is now established. Two lemmas prepare the way.

Cayley observed that every finite group G could be realized as a subgroup of S_n where n is the number of elements in G. This actually states that every group is isomorphic to a group of mappings.

LEMMA 2.12. (Cayley's Theorem). Every group G is isomorphic to a subgroup of S_n, where n is the number of elements in G.

Proof: Suppose G is a group. For each $g \in G$ define a mapping θ_g: $G \to G$ by $\theta_g(x) = gx$ for every $x \in G$.

For $y \in G$, $y = ey = (gg^{-1})y = g(g^{-1}y) = \theta_g(g^{-1}y)$. Hence, θ_g is surjective.

Let $\theta_g(x) = \theta_g(y)$, then $gx = gy$ which implies $x = y$. Thus, θ_g is injective.

Hence, for each $g \in G$, θ_g is bijective and thus, $\theta_g \in S_n$.

Now, consider $g, h \in G$ where $gh \in G$ and θ_{gh}. $\theta_{gh}(x) = gh(x) = g(hx) = \theta_g(hx) = \theta_g(\theta_h(x)) = \theta_g\theta_h(x)$ or equivalently, $\theta_{gh} = \theta_g\theta_h$. Define a mapping ϕ: $G \to S_n$ by $\phi(g) = \theta_g$. ϕ is a homomorphism because $\theta_{gh} = \theta_g\theta_h$. That is, $\phi(g)\phi(h) = \theta_g\theta_h = \theta_{gh} = \phi(gh)$.

Let $m \in \ker(\phi)$. $\phi(m) = \theta_m$ and θ_m must be the identity map. Thus $\theta_m(e) = e$. But $\theta_m(e) = me = m$. Hence, $m = e$. Therefore, $\ker(\phi) = \{e\}$, and thus, ϕ is injective [1].

This implies that ϕ is an isomorphism of G onto some subgroup of S_n; thus, proving our theorem.

In Cayley's theorem, the size of S_n in comparison to the size of G is quite large. If the order of G equals n, then the order of S_n is $n!$. Thus, the problem now is to find a set S, which is smaller than G, to reduce the size of S_n. The following lemma defines the appropriate set S, and also yields valuable information about normal subgroups of G.

LEMMA 2.13. Suppose G is a group, H is a subgroup of G, and S is the set of all left cosets of H in G. Then there is a homomorphism α of G into S_n where n is the number of distinct left cosets, and the kernel of α is the largest normal subgroup of G which is contained in H.

Proof: Let G be a group, H a subgroup of G. Let S denote the set of all left cosets of H in G. Define a mapping τ for each $g \in G$, τ_g: $S \to S$ by $\tau_g(xH) = gxH$. Using the same argument as in Cayley's theorem, one can show $\tau_{gh} = \tau_g \tau_h$; and hence, $\tau_g \in S_n$ for every $g \in G$. Thus, if a mapping α : $G \to S_n$ is defined by $\alpha(x) = \tau_x$, α is a homomorphism.

Now let $K = \ker(\alpha)$. If $m \in K$, then $\alpha(m) = \tau_m$. Thus, τ_m is the identity map. Hence, $\tau_m(xH) = xH$ for every $x \in G$. But $\tau_m(xH) = mxH$ by the definition of τ_m. This shows that $xH = mxH$ for every $x \in G$. Therefore, $K = \{m \in G \mid xH = mxH \text{ for all } x \in G\}$. K is a normal subgroup of G because the kernel of a homomorphism is a normal subgroup of G [1].

To show that K is contained in H, suppose $b \in K$. Thus, $xH = bxH$ for all $x \in G$. In particular, $H = eH = beH = bH$, whence $b \in H$ and $K \subset H$.

To show that K is the largest normal subgroup of G in H suppose J is a normal subgroup of G which is contained in H. To verify $J \subset K$, let $j \in J$ and $g \in G$ and since $J \lhd G$, $g^{-1}jg \in J$. But $J \subset H$, so $g^{-1}jgH = H$ which implies $jgH = gH$. And hence, by the above characterization of K, $j \in K$. Thus, $J \subset K$.

This proves that K is the largest normal subgroup of G which is contained in H.

With the above two lemmas, the first theorem of great importance in this thesis is now established.

THEOREM 2.14. If G is a finite group, and $H \neq G$ is a subgroup of G such that $\#G$ does not divide $|G:H|\,!$ (or $\#G \nmid |G:H|\,!$), then H must contain a <u>nontrivial normal subgroup of</u> G. Hence G is not simple.

Proof: Suppose G is a group and H is a subgroup of G such that $G \neq H$. Consider the following three cases: $|G:H|\,! = \#G$, $|G:H|\,! < \#G$, and $|G:H|\,! > \#G$.

First, if $|G:H|! = \#G$, then $\#G$ divides $|G:H|!$, which contradicts the hypothesis.

Secondly, suppose that $|G:H|! < \#G$. Let S be the set of all left cosets of H in G as in Lemma 2.13. It is now shown that the mapping α (α as defined in Lemma 2.13) cannot be an isomorphism. If α were an isomorphism, then $\alpha(G)$ would contain $\#G$ elements. Since $S_n = |G:H|! < \#G$, $\alpha(G)$ cannot be a subgroup of S_n. (This is clear because $\alpha(G)$ would contain more elements than S_n).

Therefore, α is not injective and, hence, ker (α) must be larger than $\{e\}$. From Lemma 2.13, the kernel of α is the largest normal subgroup of G which is contained in H. Hence, H contains a nontrivial normal subgroup of G.

Finally, consider $|G:H|! > \#G$. If $\#G \nmid |G:H|!$, then by LaGrange's theorem, S_n does not contain a subgroup of $\#G$. This implies that S_n has no subgroups isomorphic to G. But $\alpha(G)$ is contained in S_n, and since $\alpha(G)$ cannot be isomorphic to G, α is not an isomorphism. Hence, as above, H contains a nontrivial normal subgroup of G.

Therefore, G cannot be simple, for in all cases, H contains a nontrivial normal subgroup of G.

Chapter III

SYLOW'S THEOREMS

The objective of this chapter is to prove Sylow's three theorems. Although they will be designated as three individual theorems in this thesis, many texts combine them into a single theorem. Regardless, whether they are written as one or three, the same conclusions are obtained.

Definitions concerning the structure of groups shall be necessary in establishing Sylow's theorems. Proofs of Cauchy's theorems follow these frequently used definitions. Cauchy's theorems are the basis for the proof of Sylow's first theorem.

DEFINITION 3.1. $Z(G)$, the <u>center</u> of a group G, is the set of all elements of G that commute with every other element of G.

LEMMA 3.2. $Z(G)$ is an abelian normal subgroup of G [1].

Every group G has a center, because $e \in Z(G)$ for all G. If G is an abelian group, $G = Z(G)$.

DEFINITION 3.3. The <u>normalizer</u> or <u>centralizer</u> of $a \in G$, is the set of all elements of G that commute with a. Thus, if $a \in G$, the normalizer of a is the set $N(a) = \{x \mid x \in G, xa = ax\}$.

LEMMA 3.4. $N(a)$ is a subgroup of G [5].

DEFINITION 3.5. Two elements x and y of a group G are <u>conjugate</u> if there exists $z \in G$ such that $zyz^{-1} = x$.

Conjugacy is an equivalence relation. This can be shown in the following manner.

Write $x \sim y$ to denote y is conjugate to x.

To show $\sim$ is reflexive, consider $z = e$. Then $exe^{-1} = x$; and thus, $x \sim x$.

For symmetry, if $x \sim y$ there exists $z \in G$ such that $zyz^{-1} = x$. But this implies $y = z^{-1}xz$. Thus, $y \sim x$, and hence, $\sim$ is symmetric.

Finally, if $x \sim y$ and $y \sim z$, for some $a, b \in G$, $aya^{-1} = x$ and $bzb^{-1} = y$. Hence, $a(bzb^{-1})a^{-1} = x = ab(z)b^{-1}a^{-1} = ab(z)(ab)^{-1}$ which implies $x \sim z$. Therefore, $\sim$ is transitive.

Since conjugacy is an equivalence relation, it partitions a group G into equivalence classes that are called <u>conjugate classes</u>. A conjugate class containing $x \in G$, consist of all elements of G that are conjugate to x.

LEMMA 3.6. For $x \in G$, x is the only member of its conjugate class if and only if $x \in Z(G)$ [1].

One may conclude from the contrapositive of the above lemma, that if $x \notin Z(G)$, then the conjugate class containing x contains more than a single element.

If one selects a representative x from a conjugate class, then $|G:N(x)|$ is the number of elements in that

conjugate class. Thus, if a representative is selected from each distinct conjugate class, then the total number of elements in all conjugate classes is $\sum_{x \in R} |G:N(x)|$, where R is the set of representatives. Hence, $\#G = \sum_{x \in R} |G:N(x)|$.

Now observe that if $x \in Z(G)$, then $N(x) = G$. Thus, the number of elements conjugate to x is $|G:G| = 1$.

An important equation is now derived from $\#G = \sum_{x \in R} |G:N(x)|$. Since $x \in Z(G)$ implies $|G:N(x)| = 1$, one may write $\#G = \#Z(G) + \sum_{x \notin Z(G)} |G:N(x)|$. This equation is called the <u>class equation</u>. For simplicity in following proofs, the class equation may be written as follows:

$$\#G = \#Z(G) + \sum_{x \notin Z(G)} \frac{\#G}{\#N(x)}$$

LEMMA 3.7. If G is finite and has no nontrivial subgroups H, then G is cyclic and of prime order.

Proof: Suppose $g \in G$, $g \neq e$, and $\langle g \rangle = \{g, g^2, g^3, \ldots, g^n = e\}$ where n is the smallest power such that $g^n = e$. $\langle g \rangle$ is cyclic and a subgroup of G. But by the hypothesis, G has no nontrivial subgroups; thus, $\langle g \rangle = G$, and hence G must be cyclic. If n is prime, then $\#G$ is prime. If n is not prime, then $g^n = g^{mp} = (g^m)^p = e$. Thus, $\#\langle g^m \rangle = p$. But by the hypothesis, $\langle g^m \rangle = G$. Hence, $\#\langle g^m \rangle = \#G = p$.

In 1844 A.L. Cauchy proved that if p divides the order of a finite group G, then G contains an element of order p. Although E. Galois first stated the theorem, Cauchy was responsible for the first proof.

p will denote a prime number hereafter.

LEMMA 3.8. (Cauchy's Theorem for Abelian Groups). Suppose G is a finite abelian group and p divides #G($p \mid \#G$). Then there is an element $a \in G$ ($a \neq e$) of order p.

Proof: Proceed by using induction on the order of G. For #G = 1, the theorem is vacuously true.

Assume the theorem is true for all abelian groups H such that #H is less than #G. Consider two cases: G does not contain a nontrivial subgroup and G contains a nontrivial subgroup.

First, suppose G does not contain a nontrivial subgroup. Then by Lemma 3.7 G is of prime order and must be cyclic. If this prime order is p, then G contains p-1 elements of order p.

Second, suppose H is a nontrivial subgroup of G. Consider two cases: $p \mid \#H$ and $p \nmid \#H$. If $p \mid \#H$, by the inductive hypothesis, there exists $x \in H$ ($x \neq e$) such that $x^p = e$. Thus there exists $b \in G$ of order p, since H is a subgroup of G. Now assume that $p \nmid \#H$. All subgroups of abelian groups are normal, thus $H \triangleleft G$ and G/H is a quotient group. Since $p \nmid \#H$, $p \mid \frac{\#G}{\#H} = |G:H| < \#G$. G/H is necessarily abelian since G is abelian, and by the inductive hypothesis, there exists $Hx \in G/H$ ($Hx \neq H$) such that $(Hx)^p = Hx^p = H$. Thus, $x^p \in H$; and hence, $(x^p)^{\#H} = e = (x^{\#H})^p$. Therefore, $x^{\#H}$ is the desired element of order p, providing $x^{\#H} \neq e$.

If $x^{\#H} = e$, then $(Hx)^{\#H} = Hx^{\#H} = H$. And since $Hx^p = H$, $Hx^{\#H} = Hx^p$. Thus, $\#H = p$, or is a multiple of p. Either way, $p \mid \#H$ which contradicts the assumption of case two. Thus, $x^{\#H} \neq e$, and $x^{\#H}$ is the desired element of order p.

LEMMA 3.9. (Cauchy's Theorem). Every finite group whose order is divisible by a given prime p, must contain an element of order p.

Proof: Proceed by induction on the order of G. For $\#G = 1$, the theorem is trivially true. Assume the theorem is true for all groups H such that $\#H$ is less than $\#G$.

Consider two cases: p divides $\#H$ (H a proper subgroup of G), and p does not divide $\#H$ (H a proper subgroup of G).

First, suppose H is a subgroup of G, $H \neq G$. Let p be a prime such that $p \mid \#H$. By the inductive hypothesis, H contains an element of order p; thus, G also contains an element of order p.

Secondly, consider the case where p does not divide the order of any proper subgroup of G. For $x \in G$, $x \notin Z(G)$ implies $N(x) \neq G$. Hence, $p \nmid \#N(x)$ which implies $p \mid \frac{\#G}{\#N(x)}$. It follows that $p \mid \sum_{x \notin Z(G)} \frac{\#G}{\#N(x)}$. Thus, considering the class equation, since $\#G = \#Z(G) + \sum_{x \notin Z(G)} \frac{\#G}{\#N(x)}$,

$\#G - \sum_{x \notin Z(G)} \frac{\#G}{\#N(x)} = \#Z(G)$. Hence, $p \mid \#G - \sum_{x \notin Z(G)} \frac{\#G}{\#N(x)}$

implies $p \mid \#Z(G)$. $p \mid \#Z(G)$ implies $Z(G)$ is a subgroup of G that is divisible by p. Since p does not divide any proper subgroup of G, $Z(G) = G$. Therefore, G is abelian. If G is abelian, Lemma 3.8 may be applied; and thus, G contains an element of order p.

Approximately thirty years after Cauchy's proofs, Ludwig Sylow gave lectures on groups in Christiania, Norway. He was actually extending the theorems of Cauchy. It was here that he introduced his three theorems.

THEOREM 3.10. (Sylow's First Theorem). If p is a prime number and p^{α} divides $\#G$, then G has a subgroup of order p^{α}.

Proof: Suppose G is a group of order n. Now consider $n = p^{\alpha}r$, where r is not divisible by p. That is, α is the highest power of p that divides $\#G$. G contains a subgroup of order p for each $0 < \beta \leq \alpha$. To establish this, induction on the order of G is used.

If G has no proper subgroups, then G is either trivial or of prime order. If $G = \{e\}$, there is nothing to prove. If G is of prime order, the theorem is satisfied.

Assume that every group of order less than $\#G$ has the required subgroups as stated in the theorem. Now consider two cases: p is prime to the index of some proper subgroup of G or p divides the index of every proper subgroup of G.

Case I: Suppose H is a proper subgroup of G and $p \nmid |G:H|$. That is, $\#H = p^{\alpha}s$ where $p \nmid s$. Thus, α is the highest power of p that divides $\#H$. By the inductive hypothesis, H has subgroups of order p^{β} for each $0 < \beta \leq \alpha$, since $\#H$ is less than $\#G$. Hence, if a subgroup of order p^{β} is a subgroup of H, it is also a subgroup of G. Therefore, the theorem is true in case I.

Case II: Suppose p divides the index of every proper subgroup of G. For $g \in G$, $N(g)$ is either a proper subgroup of G or $N(g) = G$. If $N(g)$ is a proper subgroup of G, the number of elements conjugate to g is $|G:N(g)|$. But $|G:N(g)| = pt$ since p divides every proper subgroup of G. If $N(x) = G$, then $x \in Z(G)$.

Now, using the class equation, $\#G = \#Z(G) + \sum_{g \notin Z(G)} |G:N(g)|$, make the following substitutions. Let $m = \#Z(G)$, and since $|G:N(g)| = pt$, let $\sum |G:N(g)| = pt'$. Thus, by substitution, $p^{\alpha}r = m + pt'$. Therefore, p must divide m.

Hence, $Z(G)$ is an abelian group whose order is divisible by p. Thus, by Cauchy's theorem, $Z(G)$ has an element of order p. Let x be the element of order p. The cyclic group $\langle x \rangle$ generated by x is a subgroup of G of order p. It is also a normal subgroup of G, since $x \in Z(G)$.

Let $\langle x \rangle = N$. Consider the group G/N. The order of G/N is $p^{\alpha-1}r$; hence, we may apply the inductive hypothesis. That is, G/N has subgroups of order $p^{\beta-1}$ for each $0 < \beta \leq \alpha$. This produces the necessary subgroups

for each β such that $0 < \beta \leq \alpha - 1$. Let the subgroups of G/N be of the form A/N for some abelian subgroup A of G that contains N. If the order of A/N is $p^{\beta-1}$ then $\#A$ is β. Thus, since there is a subgroup of order $p^{\alpha-1}$, there is a subgroup of order p^{α}.

Hence, the theorem is true in case II.

Another series of definitions and lemmas are required to prove Sylow's second and third theorems.

DEFINITION 3.11. A <u>p-group</u> is a group in which the order of every element is some power of p.

LEMMA 3.12. A finite group G is a p-group if and only if its order is a power of p.

Proof: If G is a p-group, then for a prime $q \neq p$, q cannot divide the order of G. (That is, if $q \mid \#G$, then G must contain an element of order q by Cauchy's theorem. But since G is a p-group, the order of all of its elements must be some power of p.) Thus, the order of G is a power of p.

Conversely, if the order of G is a power of p, then G must be a p-group, because the order of all elements of G must divide the order of G. Hence, the order of the elements of G must be a power of p.

DEFINITION 3.13. A <u>p-subgroup</u> of a group G is a subgroup which is a p-group.

DEFINITION 3.14. A p-subgroup of G is a Sylow p-subgroup if its order is the highest power of p that divides $\#G$.

For example, if $\#G = 72 = 2^3 \cdot 3^2$, then G has p-subgroups of order 2, 2^2, 2^3, 3 and 3^2. But only the 2-subgroups of order 2^3 and 3-subgroups of order 3^2 are Sylow p-subgroups.

DEFINITION 3.15. Two subgroups H and K of G are conjugate subgroups if $K = g^{-1}Hg$ for some $g \in G$. It can also be said that K is conjugate to H in G.

If H and K are subgroups of G, then the set K_H of subgroups conjugate to H in K, are those subgroups X such that $X = kHk^{-1}$ for some $k \in K$. $K_H = \{X \mid X$ is conjugate to H in $K\} = \{X \mid X = kHk^{-1}, k \in K\}$.

A self-conjugate subgroup H in G is a subgroup where $xHx^{-1} = H$ for some $x \in G$. Hence, all normal subgroups are self-conjugate.

DEFINITION 3.16. The normalizer $N(H)$ of a subgroup H of G are those elements of G that commute setwise with H. That is, $N(H) = \{x \in G \mid xH = Hx\}$. (xh does not necessarily equal hx.)

The normalizer of a subgroup H contains H; therefore, it always contains the identity element. Also, $N(H)$ is a subgroup of G [1].

LEMMA 3.17. If H and K are subgroups of a group G, then the number of distinct subgroups conjugate to H in K is $|K: K \cap N(H)|$.

Proof: Consider $K \cap N(H)$. K and $N(H)$ are subgroups; thus, $K \cap N(H)$ is a subgroup of K. Let ϕ be the mapping that takes each conjugate subgroup of H in K into the set of cosets of $K \cap N(H)$ in K. That is, for each $k \in K$, $\phi(kHk^{-1}) = k(K \cap N(H))$.

Suppose $\phi(k_1Hk_1^{-1}) = \phi(k_2Hk_2^{-1})$. Thus $k_1(K \cap N(H)) = k_2(K \cap N(H))$ which implies that $k_1^{-1}k_2 \in N(H)$. But $k_1^{-1}k_2 \in N(H)$ implies $k_1Hk_1^{-1} = k_2Hk_2^{-1}$. Therefore, ϕ is injective. Also, the mapping is obviously surjective; hence, ϕ is bijective. Since ϕ is bijective, the number of distinct subgroups conjugate to H in K is $|K: K \cap N(H)|$.

LEMMA 3.18. If H is a p-subgroup of G and P is a Sylow p-subgroup of G, then $H \cap N(P) = H \cap P$.

Proof: Since P is contained in its normalizer $N(P)$, $H \cap P \subseteq H \cap N(P)$.

Let $H^* = H \cap N(P)$. H^* is a p-subgroup of p-group H and also a p-subgroup of $N(P)$. P is a normal subgroup of its normalizer $N(P)$. Thus, by the second isomorphism theorem [1], $H^*/H^* \cap P$ is isomorphic to H^*P/P.

Therefore, since the order of $H^*/H^* \cap P$ is a power of p, H^*P/P is a power of p. Hence H^*P is a p-subgroup. This implies $P \subset H^*P$, but since P is the maximal p-subgroup of G, $P = H^*P$.

$H^*P = P$ implies $H^* \subset P$, and since $H^* \subset H$, it follows that $H^* \subset H \cap P$. But $H \cap P \subset H^*$. Therefore, $H^* = H \cap P$; and hence, $H \cap P = H \cap N(P)$.

COROLLARY 3.19. If H is a p-subgroup of G and P is a Sylow p-subgroup of G, then the number of distinct subgroups conjugate to P in H, is $|H: H \cap P|$.

Proof: This follows directly from Lemma 3.17 and Lemma 3.18.

LEMMA 3.20. If P is a Sylow p-subgroup of G, then every p-subgroup of G is contained in some subgroup conjugate to P in G.

Proof: Suppose H is a fixed p-subgroup of a group G whose order is divisible by the prime p, and P is a Sylow p-subgroup of G. $G_P = \{X \mid X$ is conjugate to P in $G\} = \{X \mid X = gPg^{-1}$ for some $g \in G\}$.

Define an equivalence relation on G_P as follows: $X_1 \sim X_2$ if $X_1 = hX_2h^{-1}$ for some $h \in H$. For $e = h$, $X_1 = eX_1e^{-1}$, thus, $X_1 \sim X_1$. If $X_1 \sim X_2$, then $X_1 = hX_2h^{-1}$ for some $h \in H$, but this implies $h^{-1}X_1h = X$. Hence, $X_2 \sim X_1$. If $X_1 \sim X_2$ and $X_2 \sim X_3$, then for some $h_1, h_2 \in H$, $X_1 = h_1X_2h_1^{-1}$ and $X_2 = h_2X_3h_2^{-1}$. Thus $X_1 = h_1(h_2X_3h_2^{-1})h_1^{-1} = h_1h_2X_3h_2^{-1}h_1^{-1}$. Hence, $X_1 \sim X_3$. Therefore, $\sim$ is an equivalence relation.

Now, $\sim$ partitions G_P into "H-conjugate classes". For any particular $X \in G_P$, the number of subgroups conjugate to X in H is $|H: H \cap N(X)| = |H: H \cap X|$. Also, the number of subgroups conjugate to P in G is $|G: G \cap N(P)| = |G: N(P)|$.

But, the number of subgroups conjugate to P in G may also be represented by $\sum |H:H \cap X|$ where the summation is taken over the distinct "H-conjugate" (equivalence) classes. Hence, $|G:N(P)| = \sum |H:H \cap X|$. Each entry in the summation must be a power of p or one. (That is, since H is a p-subgroup, $|H:H \cap X|$ is a power of p unless $H = X$ then $|H:H \cap X| = |H:H| = 1$.) Since P is a Sylow p-subgroup and p does not divide $|G:N(P)|$, at least one of the entries in the summation must be one. Hence, $H \cap X = H$ for some $X \in G_p$.

Therefore, $H \subseteq X = gPg^{-1}$ for some $g \in G$.

THEOREM 3.21. (Sylow's Second Theorem). Any two Sylow p-subgroups are conjugate.

Proof: If P is a Sylow p-subgroup of G and H is a p-subgroup of G, then by Lemma 3.20, H is contained in some subgroup conjugate to P in G. That is, $H \subseteq X$ where $X \in G_p = \{ X \mid X = gPg^{-1}$ for some $g \in G \}$. Now let H be an arbitrary Sylow p-subgroup. Hence, $\#H = \#X$ since H and X are both Sylow p-subgroups. Thus, $H = X = gPg^{-1}$ for some $g \in G$. Therefore, if H is a Sylow p-subgroup, it is conjugate to P.

THEOREM 3.22. (Sylow's Third Theorem). The number, n_p, of distinct Sylow p-subgroups of a finite group G is $n_p = 1 + kp$ where $k \geq 0$ and n_p divides $\#G$.

Proof: Suppose P is a Sylow p-subgroup of G. The number n_p of subgroups conjugate to P in G is

$|G:N(P)|$. If H is a p-subgroup of G, then as in Lemma 3.20, $n_p = |G:N(P)| = \sum_X |H:H \cap X|$. Set H = P. Thus, $n_p = |G:N(P)| = \sum |P:P \cap X|$.

Since $G_p = \{X \mid X = gPg^{-1}$ for some $g \in G\}$, if $g \notin N(P)$, then $X \neq P$. Therefore $|P:P \cap X|$ is a power of p.

If $g \in N(P)$, then X = P. Thus, $|P:P \cap X|$ becomes $|P:P \cap P| = |P:P| = 1$. But $g \in N(P)$ only when g = e; hence, one will occur only once in the summation.

Therefore, $n_p = |G:N(P)| = \sum |P:P \cap X| = 1 + kp$, where $k \geq 0$. Furthermore, 1 + kp divides #G by LaGrange's theorem. (That is, $n_p = |G:N(P)| = \frac{\#G}{\#N(P)}$ which implies $(1 + kp) \cdot (\#N(P)) = \#G$.)

This concludes the proof of Sylow's theorems. About twenty years after Sylow proved his theorems, they were extended further by George Frobenius at the University of Berlin. He showed not only the distinct number of Sylow p-subgroups is of the form 1 + kp, $k \geq 0$, but that the distinct number of p-subgroups is of the form 1 + kp, $k \geq 0$. Thus, even if $p^m \mid \#G$ and $p^{m+1} \mid \#G$, the number of distinct p-subgroups of order p^m is of the form 1 + kp, $k \geq 0$.

Chapter IV

AN APPLICATION OF SYLOW'S THEOREMS

One application of Sylow's theoremsis to show that all simple groups G of order less than 60 have prime order.

Before beginning on this problem a restatement of the four theorems which are of primary importance to this thesis is given.

Theorem 2.11. If G is a finite group and H is a subgroup of G such that $G \neq H$ and G does not divide $|G:H|!$, then H contains a nontrivial subgroup of G. Hence G cannot be simple.

Theorem 3.10. (Sylow I). If p is a prime and p^m divides $\#G$, then G contains a subgroup H of order p^m.

Theorem 3.21. (Sylow II). Any two Sylow p-subgroups of G are conjugate.

Theorem 3.22. (Sylow III). The number n_p of distinct Sylow p-subgroups of a finite group G is $n_p = 1 + kp$, $k \geq 0$; and furthermore, n_p divides $\#G$.

Also, a simple group is a group containing no proper normal subgroups.

Now, consider all groups of prime order less than 60.

Let $\#G = p$. By LaGrange's theorem, the order of a subgroup of G must divide the order of G. Since $\#G = p$, the only possibilities are 1 and p. But these are trivial

subgroups; hence, there are no proper normal subgroups. Therefore, G is simple.

Thus, when the order of G is 59, 53, 47, 43, 41, 37, 31, 29, 23, 19, 17, 13, 11, 7, 5, 3 and 2, G is simple.

Now consider groups of order less than 60 such that the order is a composite number, with the exception of 56, 40 and 30.

Suppose $\#G = 58 = 29 \cdot 2$. G has a subgroup H where $\#H = 29$ by Sylow I. By LaGrange's theorem, if $\#H = 29$, $|G:H| = 2$. Now apply the test of Theorem 2.11. (Does $\#G \mid |G:H|!$?) 29 does not divide $2! = 2$. Therefore, H contains a nontrivial normal subgroup of G; and hence, G is not simple.

In the following table, one can see that the above argument holds for all the composites less than 60 except for 56, 40, and 30. (See pages 26 and 27).

It remains to consider groups of composite order 56, 40, and 30.

To show why the above argument does not hold in these cases consider the following.

If $\#G = 56 = 2^3 \cdot 7$, then the possibilities for the #H, such that #H is a power of p, are 2, 2^2, 2^3, and 7. If $\#H = 2^3$, then $|G:H| = 7$. But 56 divides $7! = 5040$. If $\#H = 2^2$, then $|G:H| = 14$. But 56 divides 14!. If $\#H = 2$, then $|G:H| = 28$. But 56 divides 28!. If $\#H = 7$, then $|G:H| = 8$. But 56 divides 8!. Hence, for all possibilities, nowhere

TABLE 4.1.

Let the order of G equal	G contains a subgroup H of order	The order of $\|G:H\|$ equals	The order of G does not divide $\|G:H\|!$
$58 = 29 \cdot 2$	29	2	$58 \nmid 2! = 2$
$57 = 19 \cdot 3$	19	3	$57 \nmid 3! = 6$
$55 = 11 \cdot 5$	11	5	$55 \nmid 5! = 120$
$54 = 3^3 \cdot 2$	27	2	$54 \nmid 2! = 2$
$52 = 2^2 \cdot 13$	13	4	$52 \nmid 4! = 24$
$51 = 17 \cdot 3$	17	3	$51 \nmid 3! = 6$
$50 = 5^2 \cdot 2$	25	2	$50 \nmid 2! = 2$
$49 = 7^2$	7	7	$49 \nmid 7! = 5040$
$48 = 2^4 \cdot 3$	16	3	$48 \nmid 3! = 6$
$46 = 23 \cdot 2$	23	2	$46 \nmid 2! = 2$
$45 = 3^2 \cdot 5$	9	5	$45 \nmid 5! = 120$
$44 = 11 \cdot 2^2$	11	4	$44 \nmid 4! = 24$
$42 = 2 \cdot 3 \cdot 7$	7	6	$42 \nmid 6! = 720$
$39 = 13 \cdot 3$	13	3	$39 \nmid 3! = 6$
$38 = 19 \cdot 2$	19	2	$38 \nmid 2! = 2$
$36 = 2^2 \cdot 3^2$	9	4	$36 \nmid 4! = 24$
$35 = 7 \cdot 5$	7	5	$35 \nmid 5! = 120$
$34 = 2 \cdot 17$	17	2	$34 \nmid 2! = 2$
$33 = 11 \cdot 3$	11	3	$33 \nmid 3! = 6$
$32 = 2^5$	16	2	$32 \nmid 2! = 2$
$28 = 2^2 \cdot 7$	7	4	$28 \nmid 4! = 24$
$27 = 3^3$	9	3	$27 \nmid 3! = 6$
$26 = 13 \cdot 2$	13	2	$26 \nmid 2! = 2$

TABLE 4.1. (Continued)

Let the order of G equal	G contains a subgroup H of order	The order of $\lvert G:H \rvert$ equals	The order of G does not divide $\lvert G:H \rvert !$
$25 = 5^2$	5	5	$25 \nmid 5! = 120$
$24 = 2^3 \cdot 3$	8	3	$24 \nmid 3! = 6$
$22 = 11 \cdot 2$	11	2	$22 \nmid 2! = 2$
$21 = 3 \cdot 7$	7	3	$21 \nmid 3! = 6$
$20 = 2^2 \cdot 5$	5	4	$20 \nmid 4! = 24$
$18 = 3^2 \cdot 2$	9	2	$18 \nmid 2! = 2$
$16 = 2^4$	8	2	$16 \nmid 2! = 2$
$15 = 5 \cdot 3$	5	3	$15 \nmid 3! = 6$
$14 = 7 \cdot 2$	7	2	$14 \nmid 2! = 2$
$12 = 2^2 \cdot 3$	4	3	$12 \nmid 3! = 6$
$10 = 5 \cdot 2$	5	2	$10 \nmid 2! = 2$
$9 = 3^2$	3	3	$9 \nmid 3! = 6$
$8 = 2^3$	4	2	$8 \nmid 2! = 2$
$6 = 2 \cdot 3$	3	2	$6 \nmid 2! = 2$
$4 = 2^2$	2	2	$4 \nmid 2! = 2$

does #G not divide $|G:H|$!. Thus, theorem 2.11 does not verify that G is not simple. Similar results are obtained when considering groups of order 40 and 30. Therefore, another argument must be used to verify that groups of order 56, 40 and 30 are not simple.

It is necessary to interject one more theorem at this time.

THEOREM 4.2. Let G be a group and P a Sylow p-subgroup of G. If P is the only Sylow p-subgroup of G, then P is normal in G.

Proof: for each $g \in G$, let $X_g = \{gpg^{-1} \mid p \in P\}$. For $p_1, p_2 \in P$, if $gp_1g^{-1} = gp_2g^{-1}$, $p_1 = p_2$. Thus, $\#X_g = \#P$. Hence, X_g is a Sylow p-subgroup of G. But P is the only Sylow p-subgroup of G. Thus, $P = X_g$. By the construction of X_g, X_g is normal. Therefore, P is a normal subgroup of G.

Let $\#G = 56 = 2^3 \cdot 7$. By theorem 3.21 (Sylow III), there exist Sylow 2-subgroups of order 8 and Sylow 7-subgroups of order 7.

The number of Sylow 2-subgroups, n_2, is $1 + 2k$, $k \geq 0$, where $1 + 2k \mid 56$. Thus, $n_2 = 1$ or 7, when $k = 0$ and 3, respectively.

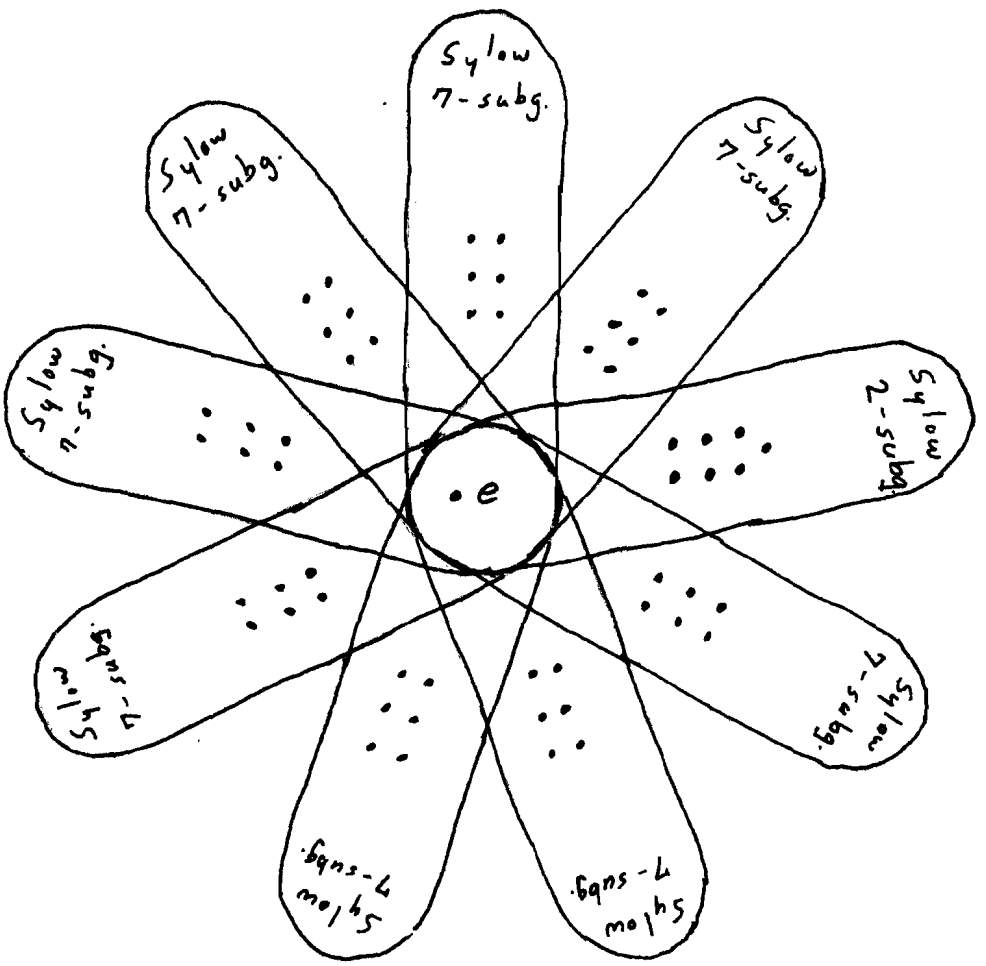
The number of Sylow 7-subgroups, n_7, is $1 + 7k$, $k \geq 0$, where $1 + 7k \mid 56$. Thus, $n_7 = 1$ or 8, when $k = 0$ and 1, respectively.

There must be at least one Sylow 7-subgroup, so consider $n_7 = 1$, and then, $n_7 = 8$.

If $n_7 = 1$, by theorem 4.2, that subgroup would be normal.

If $n_7 = 8$, then there exist only one Sylow 2-subgroup as can be seen in the following diagram. Hence, by theorem 4.2, this Sylow 2-subgroup is normal.

DIAGRAM 4.3.



One can see that the eight Sylow 7-subgroups account for 48 elements and if the identity element is counted, the total is 49. Now, since the order of G is 56, that leaves only 7 elements unaccounted for. There must be either 1 or 7 Sylow 2 subgroups of order 8; therefore, since only 7 elements are available, there can be only one Sylow 2-subgroup of order 8. That subgroup would contain the 7 elements plus the identity element. Hence, by Theorem 4.2, it is a normal subgroup.

All possibilities for the number of distinct Sylow 7-subgroups, n_7, has been considered. $n_7 = 1$ or 8. In either case, there exist a nontrivial normal subgroup. Therefore, if $\#G = 56$, G is not simple.

Let $\#G = 40 = 2^3 \cdot 5$. By Sylow III, there exist Sylow 2-subgroups of order 8 and Sylow 5-subgroups of order 5. $n_2 = 1 + 2k$, $k \geq 0$, where $1 + 2k \mid 40$. Thus, $n_2 = 1$ or 5 when $k = 0$ and 2, respectively. $n_5 = 1 + 5k$, $k \geq 0$, where $1 + 5k \mid 40$. Thus, $n_5 = 1$ when $k = 0$.

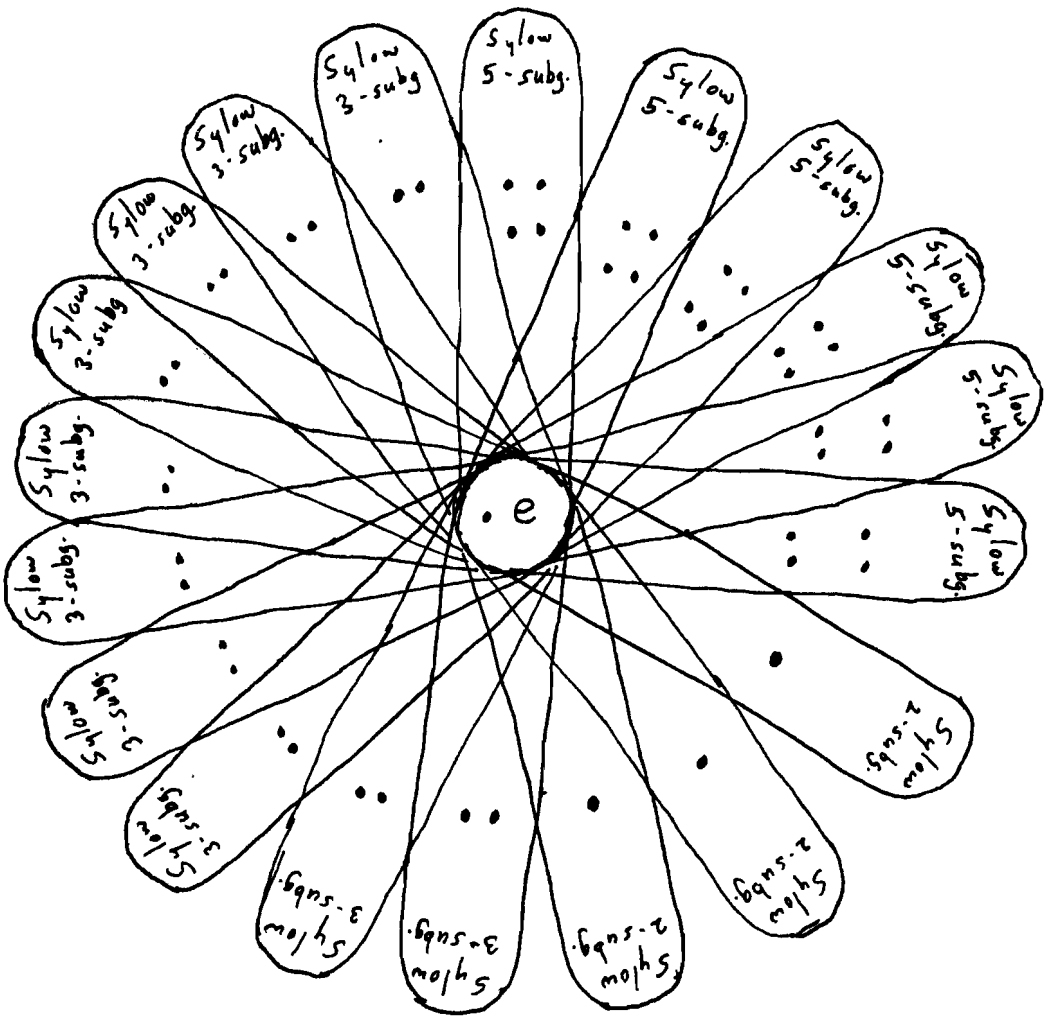
There is only one Sylow 5-subgroup regardless of n_2. Hence, by Theorem 4.2, the Sylow 5-subgroup is normal. Therefore, if $\#G = 40$, G is not simple.

Finally, to conclude the problem, let $\#G = 30 = 2 \cdot 3 \cdot 5$. Applying Sylow III, $n_2 = 1, 3, 5$, or 15 when k is 0, 1, 2 and 7, respectively. $n_3 = 1$ or 10 when k is 0 and 3, respectively. $n_5 = 1$ or 6 when k is 0 and 1, respectively.

Assume G is simple ($n_p > 1$). If $n_p > 1$, then n_2 would be at least 3, n_3 would be 10, and n_5 would be 6. This is the minimal case.

The following diagram shows that this minimal case yields 48 elements.

DIAGRAM 4.4



G cannot contain 48 elements since $\#G = 30$. Thus, if $\#G = 30$, G is not simple.

If $\#G = 1$, then $\#H = 1$. This is a trivial subgroup; thus, G is simple.

This concludes the problem of showing that all simple groups of order less than 60 have prime order.

Consideration is now given to a group of order 60.

A symmetric group has been previously defined (Definition 2.3). The order of $S_n = n!$.

DEFINITION 4.5. The <u>alternating group</u> A_n is the subgroup of S_n which consists of all even permutations on n elements. The order of A_n is $\frac{1}{2}n!$.

THEOREM 4.6. The alternating group A_n is a simple group except when n equals 4 [2].

Hence, the order of $A_5 = \frac{1}{2}(5!) = 60$, and by Theorem 4.3, A_5 is simple.

It has been shown that a group of order 60 may be simple. Therefore, 60 is the first order in which a group may be simple. (In fact, A_5 is simple).

Chapter V

CONCLUSION

The purpose of this thesis has been to present Sylow's theorems in such a way that a student with a basic knowledge of group theory might understand them.

As the reader now realizes, there is more preparation involved in preparing to prove the theorems, than there is in the actual proofs. This preparation is what many texts often omit when proving a theorem, and also what is eluded to in the introduction; that is, proofs are often too concise to understand them.

After having read the first three chapters, the ultimate test to see if this thesis has accomplished its goal, is whether or not one understands the application in Chapter IV. If so, the thesis has succeeded in presenting Sylow's theorems in an understandable manner.

BIBLIOGRAPHY

1. Dennis B. Ames, An Introduction to Abstract Algebra, International Textbook Co., Scranton, Pennsylvania, 1969.

2. William Burnside, Theory of Groups of Finite Order, Dover Publications, Inc., 1955.

3. Florian Cajori, A History of Mathematics, McMillian and Co., New York, 1961.

4. Robert D. Carmichael, Introduction to the Theory of Groups of Finite Order, Ginn and Co., 1937.

5. I.N. Herstein, Topics in Algebra, Blaisdell Publishing Co., Waltham, Massachusetts, 1964.

6. Ian D. McDonald, The Theory of Groups, Oxford University Press, London, 1968.

7. Joseph J. Rotman, Theory of Groups: An Introduction, Allyn and Bacon, Inc., Boston, 1965.