

A HISTORY OF FINITE SIMPLE GROUPS

by

Faun C.C. Doherty

B.A., Oberlin College, OH, 1993

A thesis submitted to the
University of Colorado at Denver
in partial fulfillment
of the requirements for the degree of
Master of Science
Applied Mathematics
1997

This thesis for the Master of Science
degree by
Faun C.C. Doherty
has been approved
by

J. Richard Lundgren

William E. Cherowitzo

Stanley E. Payne

Date _____

Doherty, Faun C.C. (M.S., Applied Mathematics)

A History of Finite Simple Groups

Thesis directed by Associate Professor J. Richard Lundgren

ABSTRACT

A group is a set together with an associative binary operation such that there exists an identity element for the set, and an inverse for each element in the set. All finite groups can be broken down into a series of finite "simple groups" which have been called the building blocks of finite groups. The history of finite simple groups originates in the 1830's with Evariste Galois and the solution of fifth degree polynomial equations. In the twentieth century, the recognition of the importance of finite simple groups inspired a huge effort to find all finite simple groups. This classification project was completed in 1981. We shall begin by taking a historical look at the earliest methods of analyzing the structure of finite groups according to their order. Finite simple groups can be divided into two types, those belonging to infinite families and the 26 sporadic simple groups. We shall look at the discovery and representation of many of these. Finally, we shall discuss the monumental 10,000 to 15,000 page proof of the classification of all finite simple groups.

This abstract accurately represents the content of the candidate's thesis. I recommend its publication.

Signed _____
J. Richard Lundgren

ACKNOWLEDGEMENTS

I would like to thank Professor Lundgren for his support in writing this thesis. Also, thanks to my parents for their example and Michael for his patience.

CONTENTS

<u>Chapter</u>		
1	Introduction	1
2	The Range Problem	3
	2.1 Introduction to the Problem	3
	2.1.1 Sylow's Theorems	4
	2.1.2 Other Theorems, Corollaries, Etc. That Will Prove Useful:	5
	2.2 Some History	7
	2.2.1 Hölder	7
	2.2.2 Cole, Burnside	12
	2.2.3 The Completion of the Range Problem Through Order One Million	16
	2.3 Some Examples	19
3	The Simple Groups	30
	3.1 Infinite Families of Simple Groups	30
	3.1.1 The Alternating Groups	30
	3.1.2 Simple Groups of Lie Type	35
	3.1.2.1 The Classical Linear Groups	36
	3.1.2.2 Other Lie Groups	39
	3.2 The Sporadic Simple Groups	40

3.2.1	The Mathieu Groups	42
3.2.2	Centralizer of Involution Problems	43
3.2.3	Rank 3 Permutation Groups	48
3.2.4	The Remaining Sporadic Simple Groups	49
4	The Classification Theorem	51
4.1	History	51
4.2	The Theorem	56
	<u>References</u>	63

1. Introduction

Some have referred to the study of simple groups as the ‘El Dorado’ of finite group theory. It has been a very active field of study through the twentieth century and has its roots in the nineteenth, as does group theory itself. A group is defined as a set together with an associative binary operation defined such that there exist an identity element for the set, and inverses for each element of the set. The set is closed under the operation. A *normal* subgroup H of a group G is a subgroup such that $aH = Ha$ for all $a \in G$. Another definition of normal is that $a^{-1}Ha = H$ for $a \in G$. A *simple group* is a group which has no normal subgroups except itself and the identity (which are always normal). Those groups with prime order have no subgroups except for the identity and the group itself, thus they are considered trivially simple. For the rest of this paper, the term simple group will refer to finite nontrivial simple groups. Simple groups are special kinds of groups that are the building blocks of all other groups, thus the importance in their study. This idea was recognized as early as 1832 by Evariste Galois, and later a search for the simple groups took place. In the twentieth century this search culminated in a monumental theorem which classifies all simple groups. One of the earliest methods of locating simple groups is called the range problem. This is a systematic examination of the internal structure of groups according to the order of the group. Chapter one of this paper will outline the history of this

problem and the methods used through the analysis of groups up to order one million. The second chapter will describe the simple groups by their types: infinite families of simple groups and the sporadic simple groups. How some of these groups can be represented as well as the methods of their discovery will be discussed. Finally, a general outline of the classification theorem will be given in the last chapter.

2. The Range Problem

2.1 Introduction to the Problem

Among the methods of determining all finite simple groups, the approach of examining individual groups of certain orders can seem at times slow and methodical. Yet this task, begun in 1892 by Otto Hölder, has proven fruitful in the advancement of group theory, if not always in the discovery of new simple groups. It has shed a great deal of light upon the structure of groups with given orders which allows one to understand the nature of simple groups, at least in so far as determining what they are not. This particular problem lasted through to 1975 when Marshall Hall, Jr. completed the individual examination of groups with particular orders through the order of 1,000,000. About eleven individuals from 1892 to 1975 participated in the solution of this problem, each aided by the work and discoveries of those who came before.

The range problem itself is not difficult to understand, in light of the search for simple groups. It is simply this: given a particular natural number, say n , what can we say about the structure of any group having n elements? And in particular, can we determine if the group has any normal subgroups besides itself and the identity, i.e., can we show that the group is not simple? If the group is simple, is it unique? Through the history of this problem, there were two main methods used to explore the structure of groups with a given order. One was to use the Sylow theorems and the other was to employ

character theory. It will be the task of this paper to concentrate only on the Sylow theorem methods, thus a word about these theorems is in order.

2.1.1 Sylow's Theorems

Ludvig Sylow, a Norwegian mathematician came up with the Sylow theorems in 1872 by way of the study of permutation group theory. These results lost no importance with the development of abstract group theory, in fact, their importance grew. The Sylow theorems as we state and prove them today are based on the fundamental concept known as Lagrange's theorem, and it is here that we shall start.

Theorem 2.1 [Lagrange's theorem] *Suppose $H \subseteq G$ is a subgroup. Then $|G| = |H| |G : H|$.*

Note that $|G : H|$ is the index of H in G , or the number of distinct right cosets of H in G . A right coset is the set $Hg = \{hg \mid h \in H\}$ where $H \subseteq G$. We can show easily that the group G is the disjoint union of the distinct right cosets. The cardinality of each coset is equal to the number of elements in the subgroup H , and with these two facts, we may deduce that the order of G is the order of H times the number of distinct right cosets that partition G .

Theorem 2.2 [Sylow's Theorem 1] *If $p^k \mid |G|$, then G has at least one subgroup of order p^k for any prime p .*

Thus if any power of a prime divides the order of our group, then the group has a subgroup of order that power of the prime.

Theorem 2.3 [Sylow's Theorem 2] *If $H \subseteq G$, and $|H| = p^k$ then H is*

contained in some “Sylow p -subgroup”.

A “Sylow p -subgroup” is a subgroup of G such that its order is equal to the full power of p in the order of G . For example, if we have a group of order $2^4 \cdot 5 \cdot 11^2$, a Sylow 2-subgroup would have order 2^4 . The set of all Sylow p -subgroups of G is denoted $Syl_p(G)$. We know from the first Sylow theorem that $Syl_p(G)$ is not empty. We can also find a Corollary ((2.8) below) which states that if only one Sylow p -subgroup exists, then it is normal in G . This fact will allow us to eliminate easily many integers as possible orders of simple groups.

Theorem 2.4 [Sylow’s Theorem 3] *The number of Sylow p -subgroups of G , i.e., $|Syl_p(G)|$ (written n_p) has the following properties:*

$$n_p \equiv 1 \pmod{p}$$
$$\text{and } n_p \equiv 1 \pmod{p^e}$$

if $p^e \leq |S : S \cap T|$ for all S and $T \in Syl_p(G)$ with $S \neq T$.

The examination of the structure of groups with a given order is feasible because of a number of other results besides the Sylow theorems, although many of these results are based on the Sylow theorems. A number of these results shall be listed below and referred to throughout this chapter.

2.1.2 Other Theorems, Corollaries, Etc. That Will Prove Useful:

Theorem 2.5 *A nontrivial finite p -group has a nontrivial center.*

A p -group (where p is prime) is defined as a group in which every element has order a power of p . The center of a group ($Z(G)$) is a normal subgroup of G composed of all elements which commute with all other elements of G .

Theorem 2.6 *If $|G| = p^a$, where p is prime and $a > 1$, then G is not simple.*

Proof: Let $|G| = p^a$, and suppose that G is simple. Since G itself is a p -group, by (2.5) we know that $1 < Z(G) \triangleleft G$, and since G is simple, $Z(G)$ must be G . But then G is abelian, and its simplicity implies that $|G| = p$. This is a contradiction, since $|G| = p^a$, so G is not simple.

Theorem 2.7 [The N/C Theorem] *If $H \subseteq G$, then the factor group of the normalizer of H in G by the centralizer of H in G is isomorphic to a subgroup of the group of all automorphisms of H . In mathematical notation, $N_G(H)/C_G(H) \cong M$ where $M \subseteq \text{Aut}(H)$.*

Corollary 2.8 *A unique Sylow p -subgroup is normal.*

Lemma 2.9 *Let $|G| = p^a m$, where $a > 0$, $m > 1$ and p does not divide m . If G is simple, then $n_p(G)$ satisfies all of the following:*

1. n_p divides m
2. $n_p \equiv 1 \pmod{p}$
3. $|G|$ divides $(n_p!)$

Corollary 2.10 *Let P be a Sylow p -subgroup of G . Then $n_p = |G : N_G(P)|$, and n_p divides $|G : P|$.*

Theorem 2.11 *Let $H \subseteq G$ with $|G : H| = n$. Then there exists $N \triangleleft G$ such that $N \subseteq H$ and $|G : N|$ divides $n!$. In particular, if $n > 1$ and $|G|$ does not divide $n!$, G is not simple.*

Corollary 2.12 *Let $H \subseteq G$, and $|G : H| = p$ where p is the smallest prime divisor of $|G|$. Then $H \triangleleft G$.*

Theorem 2.13 *Let B and C be cyclic of order $n < \infty$. Then $B \cong C$ and*

there are exactly $\varphi(n)$ different isomorphisms that map B to C .

Theorem 2.14 *Every two Sylow p -subgroups of G are conjugate.*

2.2 Some History

2.2.1 Hölder

The range problem was initiated by Otto Hölder (1859-1937) in 1892. Before 1892, Hölder published two papers that considerably contributed to the emphasis on this problem. The first was published in 1889 in the *Mathematische Annalen* [15]. It was a paper primarily dealing with the solution of equations. However, what was evolving into group theory, thanks to Evariste Galois, who we will discuss in chapter 2, seems to have proved useful to his work. The concepts of normal subgroups and a composition series are discussed. A composition series is a series of normal subgroups

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

where no normal subgroups exist between each G_i (i.e., each subgroup is maximal normal in the next.) The factor groups G_i/G_{i-1} are all simple groups. What is so important about this series is expressed in the Jordan-Hölder theorem which states that these simple groups (called composition factors) are uniquely determined up to isomorphism. Thus, it is apparent that the composition series acts as a type of “fingerprint” for a group. Hölder was among the first to recognize that the composition factors are building blocks of groups, and deserve special study. It was the second paper, published in 1892, in which Hölder states

“It would be of the greatest interest if a survey of all simple groups with

a finite number of operations [elements] could be known [15].”

One other advancement of this time deserves recognition. Group theory was evolving into a subject in its own right, and the idea of treating groups in the abstract, an idea attributed to Cayley, was finally being accepted. In his start upon the range problem, Hölder was the first to study groups in the abstract. More often in the past, groups were considered with respect to their mode of representation, for example, a linear transformation group. The range problem initiated the type of exploration that only required knowledge of the order of the group.

Hölder studied groups having orders from 1 to 200. He did not discover any new simple groups, since the unique simple group of order 60 was known to be simple (it is A_5 and will be discussed below), as was the group of order 168 ($PSL_2(7)$, found by Jordan in 1870). His methods were important, however, since they were used by all others working later on the range problem. His ideas provided important general theorems which can be, and were used within any range, and will be discussed below.

The most useful tools that Hölder employed were the Sylow theorems. Hölder was comfortable with permutation groups, and also used this theory. Many of the lemmas that he used in more general theorems came from permutation group theory combined with the results of Sylow’s theorems. One of his general theorems has to do with groups that have orders equal to a product of three or fewer primes, not necessarily distinct. Hölder proved that groups with orders pq , p^2q , or pqr are not simple. Sylow had already taken care of those groups with orders p^a (2.6). These theorems can be proven in a more effective

manner using only the Sylow theorems, which Burnside did in later years. The following proofs are similar to the methods used by Burnside, rather than the permutation theory used by Hölder.

Hölder's Proofs Using the Sylow Theorems

Theorem 2.15 *If $|G| = pq$, where p and q are primes, then G is not simple.*

Proof: Let $|G| = pq$, where p and q are primes, and assume G is simple. Without loss of generality, we may assume that $p > q$. Then the only choice for n_p is $n_p = q$, since n_p must divide q by (2.9), but cannot equal 1 by (2.8) and our assumption. This implies that $q \equiv 1 \pmod{p}$, which is a contradiction since $p > q$. Thus, our assumption is false, and G is not simple. ■

Theorem 2.16 *If $|G| = p^2q$, where p and q are primes, then G is not simple.*

Proof: Let $|G| = p^2q$, where p and q are primes, and assume G is simple. The choices for n_q are: $n_q = p$ or p^2 . Suppose that $n_q = p$. Then $p \equiv 1 \pmod{q}$, so $p > q$. But the only choice for n_p is q which implies $q \equiv 1 \pmod{p}$, thus, $q > p$. So $n_q \neq p$, which means that $n_q = p^2$. Let us now count elements in the group. Since $n_q = p^2$, we have p^2 subgroups each with order q . Notice that they have prime order, which means that they are cyclic, and have no two elements in common except for the identity. This means that there are $p^2(q - 1)$ elements with order q . Let Θ denote the number of the rest of the elements. Then

$$|G| = \Theta + p^2(q - 1), \text{ or } \Theta = p^2q - p^2(q - 1) = p^2.$$

Thus, there are enough elements not of order q to only fit into one Sylow p -subgroup, which means there is a unique Sylow p -subgroup, which must be normal in G . But this is a contradiction to our assumption that G is simple, which leaves us only with the alternative that one of the Sylow subgroups is

unique, thus normal (2.8). Thus, our assumption was wrong, and G is not simple. ■

Theorem 2.17 *If $|G| = pqr$, where p , q and r are primes, then G is not simple.*

Proof: Assume $|G| = pqr$, where p , q and r are primes, and assume G is simple. Without loss of generality, we may assume that $p > q > r$. The possibilities for the size of $Syl_p(G)$ are as follows:

$$n_p = q, r, \text{ or } qr$$

$$n_q = p, r, \text{ or } pr$$

$$n_r = p, q, \text{ or } pq.$$

Notice that we may eliminate q and r as possibilities for n_p since $p > q > r$ (using Sylow's 3rd (2.4)). Also, we may eliminate r as possibility for n_q for the same reasons. We may eliminate q as possibility for n_r since we know that $|G|$ cannot divide $q!$ since there is no p factor in $q!$. We conclude that there are four cases only:

$$\begin{array}{cccc}
 n_p = qr & n_p = qr & n_p = qr & n_p = qr \\
 1. \quad n_q = p & 2. \quad n_q = p & 3. \quad n_q = pr & 4. \quad n_q = pr \\
 n_r = p & n_r = pq & n_r = p & n_r = pq.
 \end{array}$$

If we examine each of these cases by counting elements, we find that none are feasible.

The First Case: we can conclude that the number of elements with order p is $qr(p - 1)$, the number of elements with order q is $p(q - 1)$, and the number of elements with order r is $p(r - 1)$. Note that this is possible since each Sylow subgroup has prime order, so no two Sylow subgroups of the

same order have elements in common except for the identity. If we add the number of elements that we have so far, it is $qr(p-1) + p(q-1) + p(r-1) = pqr - qr + pq - p + pr - p$ or, $pqr - qr + pq + pr - 2p$ Note that $-qr + pq$ is positive since $p > r$, and $pr - 2p$ is positive if $r > 2$ (zero otherwise). Thus, we have $pqr +$ some positive number as the number of elements in G , which is a contradiction. Thus, the number of Sylow subgroups is not the first case.

The Second Case: Using the same arguments as above, the second case provides us with the following number of elements: $qr(p-1) + p(q-1) + pq(r-1)$ but this is equal to $pqr - qr + pq - p + pqr - pq = pqr + pqr - qr - p$ or, $pqr + qr(p-1) - p$ and we see that $qr(p-1) - p$ must be positive. Thus, again we have over pqr number of elements, which is a contradiction.

The Third Case: Using the same arguments as above, the third case provides us the following number of elements: $qr(p-1) + pr(q-1) + p(r-1)$ which is equal to $pqr - qr + pqr - pr + pr - p = pqr + pqr - qr - p$ and this is identical with the second case, and thus a contradiction.

The Fourth Case: The same counting technique provides us with the following number of elements: $qr(p-1) + pr(q-1) + pq(r-1)$ which equals $pqr - qr + pqr - pr + pqr - pq = pqr + pqr - qr + pqr - p(q+r)$ and note that $pqr - qr$ is positive, as is $pqr - p(q+r)$ if $q+r < qr$, which is true if q and r are ≥ 3 and 2 respectively, which they are. Thus we have another contradiction, which implies that our original hypothesis was incorrect, and G is not a simple group. ■

The power of these theorems, along with a few others, eliminated all but seven orders out of the first 200 cases. The seven remaining groups had

orders 60 (known to be simple), 90, 112, 120, 144, 168 (known to be simple), and 180. Hölder was able to show that all but 60 and 168 were orders of non-simple groups using various techniques of permutation group theory, yet it has been said that his ability to use permutation groups was somewhat lacking. It did take him nearly twenty pages of calculation to demonstrate that groups of order 144 and 180 were not simple.

2.2.2 Cole, Burnside

It was an American mathematician who followed the path laid by Hölder. Frank Nelson Cole (1861-1927) continued the range problem in 1892-93 examining groups with orders ranging from 201 to 660. The methods used by Hölder were also used by Cole. The Sylow theorems provided the most powerful tool of investigation, and Cole also looked at groups in the abstract sense, “only recurring when convenient to their representation in terms of substitutions of n letters [permutation groups] [15].” Hölder’s theorems of three or fewer primes proved useful to eliminate all but 84 groups between 201 and 500. Sylow’s theorem that $n_p \equiv 1 \pmod p$ eliminated another 56. Eventually, Cole determined that A_6 , $PSL_2(11)$, and $PSL_2(2^3)$, groups of orders 360, 660 and 504 respectively, were the only simple groups with order between 201 and 660. The simple group of order 504 was never recognized as simple before Cole’s work, even though it had been discussed by mathematicians such as Mathieu and Kirkman. It was classified later as $PSL_2(2^3)$ following the advancements made by Dickson and Moore. It was a special discovery in more

ways than one, since it launched the work of Eliakim Hastings Moore (1862-1932) who discovered that the infinite family of groups, $PSL_2(p^n)$ was simple except when $p^n = 2$ or 3 . This in turn led to the proof by Dickson that the infinite family of groups $PSL_m(p^n)$ are simple, which is a generalization of Jordan's original 1870 result. This family shall be discussed further in the subsequent chapter. Notice that there were no new methods evident in Cole's work, the Sylow theorems served him well.

William Burnside (1852-1927), who has been called the first real group theorist in history because of his dedication to abstraction, was the next mathematician to work on the range problem. Once again, his techniques did not stray far from the Sylow theorems and permutation group theory. He did develop some arithmetic tests, the most important of which states that a simple group of even order must be divisible by either 12, 16, or 56. The understanding of permutation groups had advanced since Hölder's and Cole's work, which was a help in Burnside's pursuits. Ironically though, Burnside was very active in rewriting theorems previously based on permutation theory using only the abstract ideas such as conjugacy classes and normalizers. Burnside claimed that even in reference to the proofs of the Sylow theorems, "from the point of view of the right method they leave something to be desired [15]." He subsequently rewrote them. Notice that the proofs given above of Hölder's three or fewer primes theorem are essentially Burnside's rewrites. Not only did Burnside simplify the proofs for these, but he also extended the theorem to include combinations of four or fewer primes. A couple of his proofs are given below.

Burnside Theorems of Four or Fewer Primes

Theorem 2.18 *If $|G| = p^3q$, where p and q are primes, then G is not simple.*

Proof: Assume $|G| = p^3q$, where p and q are primes, and assume G is simple.

The choices for n_q are: $n_q = p$, p^2 , or p^3 , and $n_p = q$, which implies that $q > p$. Suppose that $n_q = p$. Then $p \equiv 1 \pmod{q}$, which contradicts $q > p$. Suppose that $n_q = p^3$. Count elements: there are p^3 subgroups, each with order q , which have trivial intersections. Thus there are $p^3(q - 1)$ elements with order q . Let Θ denote the number of the rest of the elements. Then $|G| = \Theta + p^3(q - 1)$, or $\Theta = p^3q - p^3(q - 1) = p^3$.

Thus, there are enough elements not of order q to only fit into one Sylow p -subgroup, which means there is a unique Sylow p -subgroup, which must be normal in G . But this is a contradiction to our assumption that G is simple, which leaves us with the last possibility.

Suppose that $n_q = p^2$. Then $p^2 \equiv 1 \pmod{q} \Rightarrow q \mid (p^2 - 1) \Rightarrow q \mid (p+1)(p-1)$. Since q is prime, this implies that $q \mid (p+1)$ or $q \mid (p-1)$. Since $q > p$, $q \mid (p+1)$ only. But this implies that $p < q \leq p+1$, so $q = p+1$ and p and q are consecutive primes. But the only consecutive primes are 2 and 3, so if G is indeed simple, $p = 2$ and $q = 3$ is the only possibility. Thus, if we show that a group of order $2^3 \cdot 3$ is not simple, we have a contradiction.

Suppose $|G| = 2^3 \cdot 3$. Then $n_2 = 1$ or 3. But note that $|G|$ does not divide $3!$. Thus $n_2 = 1$, which implies that G is not simple. So the only possibilities left are that one of the original Sylow subgroups is unique, thus normal, contradicting our hypothesis that G is simple. ■

Theorem 2.19 *If $|G| = p^2q^2$, where p and q are primes, then G is not*

simple.

Proof: Assume $|G| = p^2q^2$, where p and q are primes, and assume G is simple.

Without loss of generality, we may assume that $q > p$. The choices for n_q are: $n_q = p$ and p^2 . If $n_q = p$, then $p \equiv 1 \pmod{q}$, which contradicts the fact that $q > p$.

So suppose that $n_q = p^2$. Then the argument from the above proof holds, i.e., $p^2 \equiv 1 \pmod{q} \Rightarrow q \mid (p^2 - 1) \Rightarrow q \mid (p + 1)(p - 1)$. Since q is prime, this implies that $q \mid (p + 1)$ or $q \mid (p - 1)$. Since $q > p$, $q \mid (p + 1)$ only. But this implies that $p < q \leq p + 1$, so $q = p + 1$ and we can show that a group of order $2^2 \cdot 3^2$ is not simple:

Let $|G| = 2^2 \cdot 3^2$. Then $n_3 = 1, 2$, or 4 . But $2 \not\equiv 1 \pmod{3}$, and $|G|$ does not divide $4!$, thus the Sylow 3-subgroup is unique, thus normal in G . So the only possibilities left are that one of the original Sylow subgroups is unique, thus normal, contradicting our hypothesis that G is simple. ■

In 1895, Burnside completed the range problem up to order 1092. Shortly after this time, beginning in 1896, a new technique emerged developed by Burnside and Georg Frobenius (1849-1917) called character theory. This theory, which is based on the study of certain functions (“characters”) from a group into the complex numbers, has made a great impact on the study of simple groups through this century. It was character theory that provided Burnside with a proof of a monumental theorem that follows and outshines the four or fewer primes result. In 1904, Burnside proved that any group with order $p^a q^b$ where p and q are prime is not simple, unless it is of prime order [6]. Obviously, this theorem plays a significant role in the simplification of the

work required on the range problem after 1904. The extension of this result to orders made up of a combination of three primes, $p^a q^b r^c$, has been a difficult problem which has lasted until the present, and the method of investigation has most often been character theory. Unfortunately, it is beyond the scope of this paper to mention character theory in more depth.

2.2.3 The Completion of the Range Problem Through Order One Million

The turn of the century saw two mathematicians, George Abram Miller (1863-1951) and his student G. H. Ling work on the range problem for orders between 1092 and 2001 in 1900. The original techniques of investigation had not changed much, however there were a couple of new results which came from the older methods. One was that any group of order $p^a q$, $p^a q^2$, and $p^a q^b$ (for $a = 1, \dots, 5; p < q$) was not simple. Notice that these results were the previews of what was to come in Burnside's 1904 theorem. The problem of odd versus even orders was well under investigation at this time, as we shall examine in the next chapter. The result at this time which was put to good use was the fact that there were no simple groups with odd orders less than 2835. There was increased work on the theory of permutation groups, and on transitive groups in particular which helped with the investigation of individual orders. A permutation group on a set is called transitive if for each pair of elements of the set, there exists an element in G which sends one to the other. With these techniques, Miller and Ling showed that there was no simple group between 1093 and 2000. There seemed to be quite a gap after the work of Miller

in interest in the range problem. It was not until 1912 that anyone approached the orders following 2000. This may have been due to the difficulty that the larger orders presented, and the lack of new results which would act quickly and sweepingly, although one must remember the Burnside theorem which did exactly that. It was not until 1954 that new methods actually arose to handle groups of particular orders.

While work on the infinite families of simple groups was taking place, there was a bit of a lull in the advances on the range problem during the early twentieth century. In fact, work on the range problem was sporadic through the twentieth century. L. P. Siceloff was the next mathematician to tackle the orders 2001 through 3640 in 1912. He found simple groups with orders 2448, 2520 and 3420. He was not able to prove the uniqueness of the simple group with order 2520, and it was not until 1922 that Miller successfully showed that the group was A_7 , and unique. Cole came back to the game in 1924 with the orders 3641 through 6232. He found four simple groups having orders 3420, 4080, 5616, and 6048. He found difficulty with the uniqueness of two orders, 5616 and 6048. Both of these are unique simple groups, as shown by Richard Brauer in 1942 using character theory. It took eighteen years to find the methods to complete this task! The next time that someone chipped away at the range problem was in 1963. Michaels took the task of showing that the unique simple groups between 6233 and 20,000 were of orders 7800, 7920, 9828, 12,180, and 14,880.

In 1972, Marshall Hall, Jr (1910-1990) extended the range problem to order one million [12]. He drew together all of the methods used from the

late nineteenth century onwards, a great deal of the later methods relying on advanced techniques of character theory. His assortment of methods also included some computer work. Hall's methods were unsuccessful with only 21 orders. It was in 1975 that two students, Beisiegel and Stingl, extended work on the classification of simple groups according to the size of their Sylow 2-subgroups undertaken by Paul Fong. The remaining 21 orders were taken care of, and the range problem to one million was complete.

It was not necessarily the people working on the range problem that discovered new simple groups. In fact, not many new simple groups were found at all during the course of the range problem. In 1900, Dickson listed a total of 53 known simple groups, many members of infinite families of simple groups (see below). By 1972, only three new groups were added to this list. M. Suzuki discovered the simple group with order 29,120 in 1960 as he discovered the infinite family, $Sz(2^n)$. Z. Janko uncovered the simple group of order 175,560 in 1966, however this group was not a member of an infinite family (that is, it is a sporadic simple group). In 1967, Hall and Janko discovered a simple group (J_2) with order 604,800 which was also sporadic. None of these three groups was discovered because of work done on the range problem. Apart from these three, by 1900 those simple groups with orders less than one million were generally known to be simple before they were encountered in the course of the range problem. They consist of classical linear groups, alternating groups, and the Mathieu groups.

2.3 Some Examples

As examples of what the earlier work on the range problem was like, I have examined groups of various orders to demonstrate that they are not simple below.

Easy violation of Sylow's third theorem (2.4), and use of Corollary (2.8):

Example 1 If $|G| = 54,587 = 13^2 \cdot 17 \cdot 19$, then G is not simple:

We only need to look at the possible number of Sylow 13-subgroups to show that there is only one, thus it must be normal by (2.8). Note that by Lemma (2.9) the number of Sylow p -subgroups must divide the remaining numbers left in the order of the group. Thus we have $n_{13} = 1, 17, 19$, or $17 \cdot 19 (= 323)$. Only $1 \equiv 1 \pmod{13}$, thus $n_{13} = 1$.

Example 2 If $|G| = 35,321 = 11 \cdot 13^2 \cdot 19$, then G is not simple:

This works in the same manner as above; we shall look for the number of Sylow 11-subgroups to show that there can only be one:

$$n_{11} = 1, 13, 13^2, 19, 13 \cdot 19, \text{ or } 13^2 \cdot 19.$$

If we check each, none except 1 is $\equiv 1 \pmod{11}$. If we had looked first at n_{13} , we would have found that n_{13} could be $11 \cdot 19$ which is $\equiv 1 \pmod{11}$.

Example 3 If $|G| = 7480 = 2^3 \cdot 5 \cdot 11 \cdot 17$, then G is not simple:

This is an even order that works in the same manner. Notice the large number of possibilities for n_{17} :

$$n_{17} = 1, 2, 4, 8, 5, 11, 10, 22, 20, 44, 40, 88, 110, 220, \text{ or } 440.$$

However, none of these are $\equiv 1 \pmod{17}$, thus the Sylow 17-subgroup is solitary and normal.

Easy violation of Lemma (2.9)

Example 4 If $|G| = 7260 = 2^2 \cdot 3 \cdot 5 \cdot 11^2$, then G is not simple:

The possibilities for n_{11} are 1, 2, 4, 3, 5, 6, 12, 10, 20, 30, and 60.

If we ignore 1 for the moment, we can exclude all possibilities except 12 by (2.4) So if we assume G is simple, then $n_{11} = 12$. But notice that $|G|$ does not divide $12!$ since there is no second factor of 11 in $12!$. Thus, by (2.9), we have a contradiction and G is not simple.

Example 5 If $|G| = 6468 = 2^2 \cdot 3 \cdot 7^2 \cdot 11$, then G is not simple:

The possibilities for n_{11} , excluding the smallest factors since they cannot be $\equiv 1 \pmod{11}$, are: 1, 12, 14, 28, 21, 49, 147, 98, 196, 294, and 588. All except 1 and 12 violate (2.4). Thus, if we assume G is simple, then $n_{11} = 12$. Once again, $|G|$ does not divide $12!$ since there is no second factor of 7 in $12!$. Thus, by (2.9), we have a contradiction and G is not simple.

Notice that for (2.9) to work, n_p must be fairly small. Here are a couple of examples where n_p is too large to use (2.9), and a different technique is needed: counting elements.

Example 6 If $|G| = 616 = 2^3 \cdot 7 \cdot 11$, then G is not simple:

Assume that G is simple. The possibilities for n_{11} are the following: $n_{11} = 2, 4, 8, 7, 14, 28, 56$. Notice that only $56 \equiv 1 \pmod{11}$, so we may

rule out the other possibilities. Can we also rule out 56 using (2.9)? No, 56 is large enough that $|G| \mid 56!$. Let us check n_7 for an easier approach. $n_7 = 2, 4, 8, 11, 22, 44, 88$. The only possibility that does not violate (2.4) is 22, and similarly, $|G| \mid 22!$ since 22 is large enough. Thus, we have $n_{11} = 56$ and $n_7 = 22$. A new strategy is needed for this problem. We know $|Syl_{11}(G)|$ and $|Syl_7(G)|$ and we know that each Sylow 11- and Sylow 7-subgroups have 11 and 7 elements in them respectively. Any group of prime order is also cyclic and we know that two different cyclic groups of the same order that have more than one element in common must be equal. Thus, each of the elements of $Syl_{11}(G)$ and $Syl_7(G)$ must intersect only trivially. We could count the elements in each. We have 56 groups with $11 - 1$ distinct elements in each. The number of elements in $Syl_{11}(G)$ is then $56(11 - 1)$, and similarly, the number of distinct elements in $Syl_7(G)$ is $22(7 - 1)$. We have accounted for $56(11 - 1) + 22(7 - 1) = 560 + 132 = 692$ elements so far. There are only 616 elements in the group, so we have a contradiction. Thus, our assumption was incorrect, and G is not simple.

Example 7 If $|G| = 520 = 2^3 \cdot 5 \cdot 13$, then G is not simple:

This is similar to the above order. Assume that G is simple. Note the possibilities: $n_{13} = 2, 4, 8, 5, 10, 20, 40$ and $n_5 = 2, 4, 8, 13, 26, 104, 52$. Using (2.4), we find that $n_{13} = 40$ and $n_5 = 26$, and both numbers are too large to use (2.9). Noticing that the subgroups in $Syl_{13}(G)$ and $Syl_5(G)$ are of prime order, thus cyclic, we may count elements. We have $40(13 - 1) + 26(5 - 1) = 480 + 140 = 584 > 520$. Thus, we have a

contradiction, and G is not simple.

The following two are more difficult cases using (2.9) and (2.4).

Example 8 If $|G| = 800 = 2^5 \cdot 5^2$, then G is not simple.

Assume that G is simple. Notice that $n_5 = 2, 4, 8, 16, 32$ and only $16 \equiv 1 \pmod{5}$. Also, $|G| \mid 16!$. So $n_5 = 16$. Notice also that 16 is not $\equiv 1 \pmod{5^2}$ so we may use (2.4), the later half, which states that there exists S and $T \in Syl_5(G)$ such that $S \neq T$ and $5^2 > |S : S \cap T|$ by contrapositive. This implies that $|S : S \cap T| = 5$. (This is because $S \cap T$ is a subgroup of S , and $|S| = 5^2$ thus if $S \cap T \neq \{1\}$ which is necessary if $5^2 > |S : S \cap T|$, then $|S \cap T|$ must be 5 or 5^2 . It cannot be 5^2 because that would imply that $S \cap T = S = T$) By Lagrange's theorem, (2.1), we have that $|S| = 5^2 = |S : S \cap T| |S \cap T| = 5 \cdot 5$. Thus, $|S \cap T| = 5$ and we may use Corollary (2.12) which states that since 5 is the smallest prime divisor of $|S|$, $S \cap T \triangleleft S$ and by the same argument, $S \cap T \triangleleft T$. Consider the normalizer of $S \cap T$ in G , $N_G(S \cap T)$. By the previous discovery, we have that $S \subseteq N_G(S \cap T)$ and also $T \subseteq N_G(S \cap T)$. Thus S and T must be subgroups in the Syl_5 subgroup of $N_G(S \cap T)$. Since $N_G(S \cap T) \subseteq G$, by Lagrange's theorem again,

$$|N_G(S \cap T)| = |S| |N_G(S \cap T) : S| = 5^2 \cdot |N_G(S \cap T) : S|.$$

Thus, $|N_G(S \cap T) : S|$ has to be $= 2, 2^2, 2^3, 2^4$, or 2^5 . If we look at the number of Sylow 5-subgroups in $N_G(S \cap T)$, we see that it must also be $2, 2^2, 2^3, 2^4$, or 2^5 , depending on $|N_G(S \cap T) : S|$. One further condition, that $n_5(N_G(S \cap T)) \equiv 1 \pmod{5}$, leaves us with $n_5(N_G(S \cap T)) = 2^4$. This

implies that 2^4 divides $|N_G(S \cap T)|$. Thus, $|N_G(S \cap T)| = 5^2 \cdot 2^4$ or $5^2 \cdot 2^5$. If $|N_G(S \cap T)| = 5^2 \cdot 2^5$, then $N_G(S \cap T) = G$, and $S \cap T \triangleleft G$ which is a contradiction to our assumption that G is simple. Thus, $|N_G(S \cap T)| = 5^2 \cdot 2^4$. But this implies by Lagrange that $|G : N_G(S \cap T)| = 2$. Note that $|G|$ does not divide $2!$, (or alternately, any subgroup with index 2 is normal). Thus, we have by theorem (2.11) that G is not simple, a contradiction to our assumption, but the last alternative. Thus, our assumption was incorrect, and G is not simple.

Example 9 If $|G| = 864 = 2^5 \cdot 3^3$, then G is not simple.

Assume that G is simple. The possibilities for n_3 are the following:

$$n_3 = 2, 4, 8, 16, \text{ or } 32.$$

(2.4) eliminates all but 4 and 16. Using (2.9) and noting that $|G|$ cannot divide $4!$, we are left with $n_3 = 16$. But 16 is not $\equiv 1 \pmod{3^2}$, so we can conclude by (2.4) that there exists S and $T \in \text{Syl}_3(G)$ such that $S \neq T$ and $3^2 > |S : S \cap T|$. Using the same process as above, we can conclude that $|S : S \cap T| = 3$ and by Lagrange, $|S \cap T| = 3^2$. By (12), since 3 is the smallest prime divisor of $|S|$, $S \cap T \triangleleft S$ and similarly, $S \cap T \triangleleft T$. Thus, $S \subseteq N_G(S \cap T)$ and $T \subseteq N_G(S \cap T)$. We have by Lagrange that $|N_G(S \cap T)| = |S| |N_G(S \cap T) : S| = 3^3 \cdot |N_G(S \cap T) : S|$. And since $N_G(S \cap T) \subseteq G$, $|N_G(S \cap T) : S| = 2, 2^2, 2^3, 2^4$, or 2^5 . We know that $n_3(N_G(S \cap T))$ must divide $|N_G(S \cap T) : S|$ and also that $n_3(N_G(S \cap T)) \equiv 1 \pmod{3}$, thus $n_3(N_G(S \cap T)) = 2^2$ or 2^4 . If $n_3(N_G(S \cap T)) = 2^4$, then $|N_G(S \cap T) : S| = 2^4$ or 2^5 , and $|N_G(S \cap T)| = 3^3 \cdot 2^4$ or $3^3 \cdot 2^5$. $|N_G(S \cap T)|$ cannot be

$3^3 \cdot 2^5$, since that would make $G = N_G(S \cap T)$ and thus not simple. Suppose $|N_G(S \cap T)| = 3^3 \cdot 2^4$. Then $|G : N_G(S \cap T)| = 2$ and since $|G|$ does not divide $2!$, G is not simple by (2.11). This is a contradiction to our assumption, thus $|N_G(S \cap T)| \neq 3^3 \cdot 2^4$. If $n_3(N_G(S \cap T)) = 2^2$, then $|N_G(S \cap T)| = 3^3 \cdot 2^2, 3^3 \cdot 2^3, 3^3 \cdot 2^4$, or $3^3 \cdot 2^5$. We know that $|N_G(S \cap T)| \neq 3^3 \cdot 2^4$, or $3^3 \cdot 2^5$. Thus, suppose $|N_G(S \cap T)| = 3^3 \cdot 2^3$. Then $|G : N_G(S \cap T)| = 2^2$, and $|G|$ does not divide $4!$, showing that G cannot be simple (2.11). Suppose that $|N_G(S \cap T)| = 3^3 \cdot 2^2$. Then $|G : N_G(S \cap T)| = 2^3$, and still the index is too small, and $|G| \nmid 8!$. Thus since this is our last alternative, we conclude that our assumption was incorrect, and G is not simple.

The following example uses a well known theorem, The “N/C Theorem” (2.7).

Example 10 If $|G| = 792 = 2^3 \cdot 3^2 \cdot 11$, then G is not simple.

Assume that G is simple. The possibilities for n_{11} are the following: $n_{11} = 2, 4, 8, 3, 9, 6, 12, 24, 18, 36$, or 72 . Only $12 \equiv 1 \pmod{11}$, thus $n_{11} = 12$. Look at one subgroup in $Syl_{11}(G)$, say $S \in Syl_{11}(G)$. Let N be the normalizer in G of S , $N = N_G(S)$. Then since $n_{11} = 12 = |G : N|$ (2.10), we know that $|N| = 2 \cdot 3 \cdot 11$ by Lagrange. Let C be the centralizer of S in G , $C = C_G(S)$. We know by the N/C theorem that the factor group N/C is isomorphic to a subgroup of $Aut(S)$. The set of automorphisms of S has order $\varphi(11) = 10$, since S is cyclic (2.13). This implies that $|N : C|$ divides 10. By Lagrange again, since $|N| = 2 \cdot 3 \cdot 11 = |C| |N : C|$, the only choice

for $|N : C|$ is 2, thus $|C| = 3 \cdot 11$. We see that the centralizer in G of S has Sylow 3-subgroups. Let $P \in \text{Syl}_3(C)$. Then $|P| = 3$. Consider $N_G(P)$ and note that $N_G(P)$ cannot equal G since we are assuming G is simple, and $P \triangleleft N_G(P)$. Clearly $P \subseteq C = C_G(S)$. Since P commutes with all elements of S , then $S \subseteq C_G(P)$. But $C_G(P) \subseteq N_G(P)$, so $S \subseteq N_G(P)$ which means that $|N_G(P)|$ is divisible by 11. By (2.3), there exists a $Q \in \text{Syl}_3(G)$ such that $P \subseteq Q$. But $|Q| = 3^2$, so $|Q : P| = 3$. By (2.10) then, $P \triangleleft Q$. Thus, $Q \subseteq N_G(P)$, which implies that $|N_G(P)|$ is also divisible by 3^2 . So the least order of $N_G(P)$ is $11 \cdot 3^2$, which means that $|G : N_G(P)| \leq 2^3$. But 2^3 itself is too small, since $|G|$ cannot divide $2^3!$. This implies that G is not a simple group (2.11), which is a contradiction, thus our assumption was incorrect and G is not a simple group.

Notice that the strategy in the previous problem was to find a subgroup of G which has order large enough to make the index of it in G too small to be divisible by the order of G , thus utilizing the theorem (2.11). The way to find a subgroup of G large enough to achieve this is to examine centralizers and normalizers of subgroups within G . The following example also uses normalizers in conjunction with (2.10), digging a few layers deep into the structure of the group.

Example 11 If $|G| = 3465 = 3^2 \cdot 5 \cdot 7 \cdot 11$, then G is not simple.

Assume that G is simple. The following lists the possibilities for all

$Syl_p(G)$ subgroups:

$$n_{11} = 3, 9, 5, 7, 15, 21, \mathbf{45}, 63, 105, 315$$

$$n_5 = 3, 9, 7, 11, \mathbf{21}, 33, 77, 63, 99, \mathbf{231}, 693$$

$$n_7 = 3, 9, 5, 11, \mathbf{15}, 45, 33, \mathbf{99}, 55, 165, 495$$

$$n_3 = 5, 7, 11, 35, \mathbf{55}, 77, \mathbf{385}$$

The numbers in bold are those that do not violate either (2.4) or (2.9).

These numbers indicate that the only possibilities for $|N_G(s_p)|$, where $s_p \in Syl_p$, by (2.10) are the following:

$$|N_G(s_{11})| = 7 \cdot 11$$

$$|N_G(s_5)| = 3 \cdot 5 \cdot 11, \text{ or } 3 \cdot 5$$

$$|N_G(s_7)| = 3 \cdot 7 \cdot 11, \text{ or } 5 \cdot 7$$

$$|N_G(s_3)| = 3^2 \cdot 7, \text{ or } 3^2$$

Working systematically, we shall try to eliminate each of these as possibilities. Suppose that $|N_G(s_5)| = 3 \cdot 5 \cdot 11$. Look at $|Syl_{11}|$ in $N_G(s_5)$, denoted $n_{11}(N_G(s_5)) : n_{11}(N_G(s_5)) = 1, 3, 5, \text{ or } 15$. Note that the only choice that does not violate (2.4) is $n_{11}(N_G(s_5)) = 1$. Thus, by (2.10), $1 = |N_G(s_5) : N_{N_G(s_5)}(s_{11}(N_G(s_5)))|$ and thus $|N_G(s_5)| = 3 \cdot 5 \cdot 11 = |N_{N_G(s_5)}(s_{11}(N_G(s_5)))|$ by Lagrange. But $N_{N_G(s_5)}(s_{11}(N_G(s_5)))$ is the normalizer in $N_G(s_5)$ of a Sylow 11-subgroup, and note that $N_G(s_{11})$ is the group of all elements in G that normalize a Sylow 11-subgroup. Thus, $N_{N_G(s_5)}(s_{11}(N_G(s_5))) \subseteq N_G(s_{11})$, which implies that $3 \cdot 5$ divides $|N_G(s_{11})|$. But we know that $|N_G(s_{11})| = 7 \cdot 11$ from above, thus we have a contradiction. We now know that $|N_G(s_5)| = 3 \cdot 5$, and $n_5 = 231$. Suppose that $|N_G(s_7)| = 3 \cdot 7 \cdot 11$. Note that $n_{11}(N_G(s_7)) = 1, 3, 7, \text{ or } 21$. By (2.4),

$n_{11}(N_G(s_7)) = 1$ is the only possibility. Then by (2.10) and Lagrange,
 $|N_{N_G(s_7)}(s_{11}(N_G(s_7)))| = 3 \cdot 7 \cdot 11$. But this implies that $3 \mid |N_G(s_{11})| = 7 \cdot 11$,
which is a contradiction. Thus, $|N_G(s_7)| = 5 \cdot 7$ and $n_7 = 99$. Now look
at the possibilities for $n_5(N_G(s_7))$: 1 or 7. By (4), $n_5(N_G(s_7)) = 7$, and
by the same argument as above, this implies that $7 \mid |N_G(s_5)|$. We have
from above that $|N_G(s_5)| = 3 \cdot 5$, thus we have a contradiction. The only
possibility is that one of the Sylow subgroups is unique, thus normal.
Therefore, G is not simple.

The strategy of this last example is to use theorems about the size
of $Syl_p(G)$ more than once to draw a contradiction. The following example
starts in this manner, then requires a method previously seen, and comes to a
conclusion with the same method used at first.

Example 12 If $|G| = 760 = 2^3 \cdot 5 \cdot 19$, then G is not simple.

Assume that G is simple. The following list the possibilities for the sizes
of all $Syl_p(G)$:

$$n_2 = 5, \mathbf{19}, \mathbf{95}$$

$$n_5 = 2, 4, 8, 38, \mathbf{76}, 152, 19$$

$$n_{19} = 2, 4, 8, 5, 10, \mathbf{20}, 40$$

The numbers in bold indicate those that do not violate (2.4) or (2.9). The
following are the possible orders of the normalizers of the Sylow subgroups

by (2.10):

$$|N_G(s_2)| = 2^3 \cdot 5, \text{ or } 2^3$$

$$|N_G(s_5)| = 2 \cdot 5$$

$$|N_G(s_{19})| = 2 \cdot 19$$

We would like to determine $|N_G(s_2)|$, so suppose $|N_G(s_2)| = 2^3 \cdot 5$. Then $n_5(N_G(s_2)) = 1, 2, 4, \text{ or } 8$. We conclude by (2.4) that $n_5(N_G(s_2)) = 1$. Thus, using the same process as above, by (2.10) and Lagrange, we can conclude that $|N_{N_G(s_2)}(s_5(N_G(s_2)))| = 2^3 \cdot 5$. Since $N_{N_G(s_2)}(s_5(N_G(s_2))) \subseteq N_G(s_5)$, then 2^3 divides $|N_G(s_5)| = 2 \cdot 5$, a contradiction. Thus, $|N_G(s_2)| = 2^3$, and $n_2 = 95$. Note that $95 \not\equiv 1 \pmod{2^2}$, so by (2.4), there exist S and $T \in \text{Syl}_2(G)$ such that $S \neq T$ and $2^2 > |S : S \cap T|$. This implies that $|S : S \cap T| = 2$. By (2.10) we have that $S \cap T \triangleleft S$, and by similar argument, $S \cap T \triangleleft T$. Thus, $S \subseteq N_G(S \cap T)$ and $T \subseteq N_G(S \cap T)$, so $2^3 \mid |N_G(S \cap T)|$. In fact, our possibilities for $|N_G(S \cap T)|$ are: $2^3 \cdot 19, 2^3 \cdot 5, \text{ or } 2^3 \cdot 5 \cdot 19$. We may rule out $|N_G(S \cap T)| = 2^3 \cdot 5 \cdot 19$ since that would imply that $N_G(S \cap T) = G$, and thus $S \cap T \triangleleft G$, which is a contradiction. Suppose that $|N_G(S \cap T)| = 2^3 \cdot 19$. Then $|G : N_G(S \cap T)| = 5$, but $|G| \nmid 5!$, which implies a contradiction by (2.9). Thus, $|N_G(S \cap T)| = 2^3 \cdot 5$. Look at the size of $\text{Syl}_5(N_G(S \cap T))$: $n_5 = 1, 2, 4, \text{ or } 8$. By (2.4), $n_5 = 1$. By (2.10) and Lagrange, we have that $|N_{N_G(S \cap T)}(s_5(N_G(S \cap T)))| = 2^3 \cdot 5$. But this implies that $2^3 \mid |N_G(s_5)|$ since $N_{N_G(S \cap T)}(s_5(N_G(S \cap T))) \subseteq N_G(s_5)$, and this is a contradiction since $|N_G(s_5)| = 2 \cdot 5$. Thus, our original assumption must be incorrect, and G is not simple.

The orders used for these examples are obviously fairly small. As one can guess, the larger the order, the more cumbersome are the choices for such numbers as $n_p(G)$. Take the simple group, J_1 for example. This group (described further below) has order $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$. In order to determine n_{19} , one must consider 56 possibilities. Out of this 56, there are four numbers which cannot be eliminated using (2.4) or (2.9). Since 19 is the largest prime divisor of $|G|$, n_{19} should be the most accessible of all sizes of the $Syl_p(G)$ to find. Imagine what the others must be like! The shear magnitude of the problems increase as the orders become very large. Not all groups of large order are difficult to handle, however. Take for example $|G| = 1,000,000$. It is a simple matter of using (2.9) on the possibilities for n_5 that proves G is not simple. Nonetheless, when the larger orders are difficult, they can be very difficult. They are generally more cumbersome when their orders are comprised of quite a few primes close in size. It is no wonder that Marshall Hall, Jr. employed computer assistance in the course of his completion of the range problem up to order one million.

3. The Simple Groups

3.1 Infinite Families of Simple Groups

3.1.1 The Alternating Groups

“I have often in my life ventured to advance propositions of which I was uncertain; ... it is too much to my interest not to deceive myself that I have been suspect of announcing theorems of which I had not the complete determination ... subsequently there will be, I hope, some people who will find it to their profit to decipher all this mess.” (Galois [15])

The history of group theory itself begins with the discovery of the first compositely ordered simple group, A_5 . The process that led to the discovery of this simple group actually led to the idea of the study of group theory. It began with Evariste Galois (1811-1832) who led a very short but mathematically productive life, although it took time and scrutiny for anyone to understand his ideas. The above quotation was on the final page written by Galois before he died “for so trivial a thing” [16] in a duel when he was twenty one years of age. Many of the terms that he used were not rigorously defined, and his results were not often proven, being hurriedly jotted on a piece of paper. Yet Galois did have the first concept of groups as we define them today, and used them somewhat abstractly in his studies of solvable polynomials. Galois was working on the popular algebra problem of the eighteenth and into the nineteenth centuries, the factorability of polynomials over a field F .

Galois' approach to this problem is rooted in the workings of permutations. The possible roots of a polynomial of degree n can be permuted in $n!$ different ways. For example, look at the fourth order polynomial in the complex field: $f(x) = (x^2 + 1)(x^2 - 3)$. The four roots of the polynomial are $x = i, -i, \sqrt{3}$, and $-\sqrt{3}$. Suppose we let

$$\begin{aligned}\alpha &= i \\ \beta &= -i \\ \gamma &= \sqrt{3} \\ \delta &= -\sqrt{3}.\end{aligned}$$

Then we have permutations of these four letters such as $R_1 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \gamma & \delta \end{pmatrix}$ which switches α and β and leaves the other two fixed. There are $4! = 24$ similar permutations. A subgroup of the group of 24 permutations can be formed in the following way. Look at any polynomial equations involving α, β, γ , or δ . Some equations express a true statement if the numerical values of α, β, γ , or δ are substituted, and some do not. For example, the equation $\gamma^2 - 3 = 0$ is true for $\gamma = \sqrt{3}$, as is $\alpha + \beta = 0$ for the given values of α and β . An equation such as $2\beta - \delta = 2$ is obviously not true. The group of permutations which preserve the truth of the true equations form a subgroup of the permutation group. Notice that any true equation remains true if α and β are interchanged, and similarly if γ and δ are interchanged. Galois called this subgroup of permutations the group of the equation, G . In our example, this group consists

of

$$R_1 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \gamma & \delta \end{pmatrix}, R_2 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \delta & \gamma \end{pmatrix}, R_3 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \end{pmatrix}, I = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \gamma & \delta \end{pmatrix}.$$

The first concept of a normal subgroup was born by examining the group G . Choose a polynomial expression, Ψ , which is rational in the roots of our original equation but has the following property: its numerical value, t , stays fixed for some elements of G , but changes for others. Then those elements of G which fix t form a subgroup, H , of G . Galois showed that if t is a root of the (irreducible over F) binomial equation $x^p - c = 0$ where p is prime, then the subgroup H is in fact normal in G . This process continues to reveal a method of solving equations by radicals, and also the inspiration for studying simple groups. Form a new field $F(t)$ which is the smallest field containing both F and t . The subgroup H is then the group of the equation over the new field, $F(t)$. Repeat the above process on H to find a normal subgroup of H , and a new field, $F(t, t_1)$ where t_1 is the numerical value of the chosen expression. The process can be repeated until we are left with the identity permutation as the subgroup. In this case, the original equation is said to be solvable by radicals over the created field, $F(t, t_1, \dots, t_n)$. Furthermore, we have a series of normal subgroups much like

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_{n-1} \triangleleft H_n = G$$

where the index of one in the other, H_i/H_{i-1} was shown to be the prime number p in the appropriate equation $x^p - c = 0$. This looks remarkably like the composition series discussed earlier, and since each index is prime we see that each composition factor, $|H_i/H_{i-1}|$ must be trivially simple. Galois discovered

that an equation was solvable if each index in the composition series was prime, and not solvable if some index was not prime. This is precisely what happens to quintic equations. Some composition factor in the composition series is compositely simple, not having prime order, and the end result of the identity permutation is never obtained.

The simple group that was discovered by Galois by way of the insolubility of the quintic was the simple group of order 60. By 1832, Galois recognized this group as simple stating “The smallest group of permutations which an indecomposable group can have, when this number is not prime is $5 \cdot 4 \cdot 3$ [15].” Galois stated this without proof and it wasn’t until 1870 that Jordan would verify this result. In fact, Jordan gave better definition to the notion of a composition series which was only one great feat of his 1870 work, *Traité des substitutions et des équations algébriques* [15], which further inspired the study of simple groups. By this time, mathematicians were still concerned with the solution of algebraic equations, and this was the foremost purpose of the *Traité*. The use of permutation groups was still being explored and expanded, and groups were generally represented as such. Thus, Jordan discovered that the simple group of order 60 which was tied to the quintic equation was actually the alternating group on five letters, A_5 . An alternating group is the subgroup of the permutation group made up of all even permutations. (A permutation is even if it can be written as a product of an even number of 2-cycles, or transpositions.) Jordan went further than proving the simplicity of A_5 . He presented a (flawed) proof for the simplicity of all alternating groups, A_n , for $n \geq 5$. This was the first infinite family of simple groups

to be discovered. As an example of the permutation group theory used, the following is a proof for the simplicity of A_5 :

Theorem 3.1 A_5 is simple.

Proof: The cycle structures of the elements in A_5 are the following: $1^5, 1 \cdot 2^2, 1^2 \cdot 3$, and 5 . This notation indicates that there are permutations which fix five letters (the identity), fix one letter and has two 2-cycles, fix 2 letters and has one 3-cycle, and which has one 5-cycle. The orders of the elements in A_5 which are made up of these cycle structures can be obtained by finding the least common multiple of the sizes of cycles for each type. That is, the order of the elements that are made up of two 2-cycles and fix one point is 2 (LCM of 2 and 1), etc. as shown below:

cycle structure	order of elements	number of elements
1^5	1	1
$1 \cdot 2^2$	2	15
$1^2 \cdot 3$	3	20
5	5	24.

The last column above shows the number of elements of each order. These numbers are easily obtained by looking at the order of A_5 . For example, the number of elements of order 3 is $\frac{2^2 \cdot 3 \cdot 5}{3}$, the number of elements of order 5 is $\frac{2^2 \cdot 3 \cdot 5}{5}$, etc. To show that A_5 is simple, we shall proceed by contradiction. Suppose that A_5 contains a normal subgroup, S , which is not the identity or A_5 itself. The possible orders of S must divide $2^2 \cdot 3 \cdot 5$. Suppose that $3 \mid |S|$. Then S contains a Sylow 3-subgroup of A_5 and since S is normal and every two Sylow p -subgroups are conjugate (2.14), S must contain all Sylow

3-subgroups. Thus, S contains all elements of order 3. There are 20 elements of order 3, so $|S| > 20$ (accounting for the identity). Also, $3 \mid |S|$ and $|S| \mid |A_5|$, so $|S| = 30$.

Now suppose that $5 \mid |S|$. By the same argument as above, S contains all Sylow 5-subgroups, and thus all 24 elements of order 5. So $|S| > 24$, thus $|S| = 30$. Since 30 is divisible by both 3 and 5, S must contain all elements of both orders, 20 + 24, but this is impossible if $|S| = 30$.

So suppose $|S| = 4$. Then S would be a normal Sylow 4-subgroup, and thus would be the unique Sylow 4-subgroup. But there are 15 elements of order 2, so this is also impossible.

Finally, suppose $|S| = 2$. Then $|Aut(S)| = 1$ since $\varphi(2) = 1$. (2.13) Using the N/C theorem (7), $N_{A_5}(S)/C_{A_5}(S) = 1$ thus, $N_{A_5}(S) = C_{A_5}(S)$. Since S is normal in A_5 , $N_{A_5}(S) = A_5$ which implies that $C_{A_5}(S) = A_5$. This is not true, since a counterexample can be found easily as a 3-cycle which does not commute with a product of two 2-cycles. So none of the possibilities work, and our assumption must be incorrect. Therefore, A_5 is simple. ■

3.1.2 Simple Groups of Lie Type

The remainder of the infinite families of simple groups can be classified as Lie groups. These include the classical groups, the groups of type G_2 , the Chevalley groups (of types E_4, E_6, E_7 , and E_8), the twisted groups (of types E_6 and D_4), the Suzuki groups, and the Ree groups (of types G_2 and F_4). These groups arise as automorphism groups of corresponding simple Lie algebras. In general, since the theory of Lie algebras is too extensive for this

paper, a Lie algebra is a vector space over a field with a product $[X, Y]$ that is linear in both variables which also meets the following criteria:

- 1) $[X, X] = 0$ for all X in the vector space.
- 2) $[[X, Y], Z] + [[Y, X], X] + [[Z, X], Y] = 0$ (the Jacobi identity)

3.1.2.1 The Classical Linear Groups

It was Jordan again in his *Traité* who found the next four infinite families of simple groups, although he was not completely aware of the simplicity of each. Jordan obtained orders, generators and the factors of composition of some of these groups and was not explicit about the infinite families involved. We have seen how the simplicity of the infinite family $PSL(m, p^n)$ was finally proven by Dickson in 1897. In fact, Dickson worked on extending Jordan's results on all of the linear groups from 1897 to 1899. Dickson and Dieudonné are also credited with further investigating all of the linear groups in the years 1948 to 1958. The groups are now known as the projective special linear, the symplectic, the orthogonal, and the unitary groups. All four are collectively called the classical linear groups. They are each groups of matrices. The construction of the first two are given below, and the construction of the orthogonal and unitary are similar in that they are each groups of invertible matrices factored out by the group's center.

Projective special linear: The general linear group, $GL_n(q)$ is the group of all nonsingular linear operators of a vector space V where V has dimension n over the field of order q . Thus, $GL_n(q)$ is a group of n by n matrices. The order of $GL_n(q)$ can be given by the following:

$$|GL_n(q)| = (q - 1)q^{n(n-1)/2}(q^2 - 1)\dots(q^n - 1).$$

The subgroup of matrices with determinant 1 is normal and called the special linear group, $SL_n(q)$. The order of $SL_n(q)$ is given by $q^{\frac{n(n-1)}{2}}(q^2 - 1)\dots(q^n - 1)$. The center, Z , of $GL_n(q)$ consists of transformations of the form $Tx = \lambda x$ for λ not 0. The center of $SL_n(q)$ can be denoted $Z \cap SL_n(q)$ and the factor group is the projective special linear group, $PSL_n(q)$. Its order is given by the following $|PSL_n(q)| = \frac{1}{(n, q-1)} q^{n(n-1)/2} (q^2 - 1)\dots(q^n - 1)$. Let the field be the Galois field $GF(q)$ where q is a power of a prime. This group is simple for $n \geq 2$ except for $PSL_2(2)$ and $PSL_2(3)$.

Let us look at a specific example of a projective special linear group. The simple group $PSL_3(2)$ is isomorphic to $PSL_2(7)$, both with order 168. We would construct $PSL_3(2)$ by looking first at $GL_3(2)$ which consists of all nonsingular 3 by 3 matrices over the Galois field, $GF(2)$. For example, the matrix $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ is an element in $GL_3(2)$. The order of $GL_3(2)$ is $(2 - 1)2^3(2^3 - 1)(2^2 - 1) = 168$. Note that this is the same as the order of $PSL_3(2)$ and indeed, they are isomorphic. The reason for this is that all matrices in $GL_3(2)$ have determinant equal to 1 mod 2, thus all elements in $GL_3(2)$ are also in $SL_3(2)$. The center of $SL_3(2)$ consists of the identity only, thus $SL_3(2)/Z \cap SL_3(2) = SL_3(2) = PSL_3(2)$.

The construction of $PSL_2(7)$ isomorphic to $PSL_3(2)$ begins with $GL_2(7)$, the group of nonsingular 2 by 2 matrices over $GF(7)$. $GL_2(7)$ has order $6 \cdot 7 \cdot (7^2 - 1) = 2016$. An element in this group looks something like

$\begin{bmatrix} 6 & 2 \\ 1 & 3 \end{bmatrix}$ or $\begin{bmatrix} 4 & 1 \\ 0 & 5 \end{bmatrix}$ where the matrix entries are modulo 7. If we restrict ourselves to all matrices in $GL_2(7)$ with determinant 1 mod 7, for example $\begin{bmatrix} 3 & 3 \\ 1 & 6 \end{bmatrix}$, we have $SL_2(7)$ with order 336. The center of $GL_2(7)$ consists of

matrices like $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, ..., $\begin{bmatrix} 6 & 0 \\ 0 & 6 \end{bmatrix}$. The center of $SL_2(7)$ are those

matrices in the center with determinant 1 mod 7, which are only 2, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

and $\begin{bmatrix} 6 & 0 \\ 0 & 6 \end{bmatrix}$. The simple group $PSL_2(7)$ is the factor group of $SL_2(7)$ and these two elements. Comparing the order with the formula given above, we

see that $|PSL_2(7)| = \frac{1}{2} \cdot 7 \cdot (7^2 - 1) = 168$.

Projective Symplectic: Suppose that the vector space V from above has a skew-symmetric, bilinear non-singular scalar product so that $(x, y) = -(y, x)$, and $(x, x) = 0$. The symplectic group, $Sp_n(q)$ where $n = 2m$, consists of those linear transformations which preserve the above symplectic form. In particular, if A , B , C , and D are $m \times m$ matrices, then the transformation represented by the matrix $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ is symplectic exactly when the following hold: $A^t C - C^t A = 0$, $A^t D - C^t B = I$, and $B^t D - D^t B = 0$ [5]. The projective symplectic group, $PSp_n(q)$, is the factor group $Sp_n(q)/Z(Sp_n(q))$ where $Z(Sp_n(q))$, the center of $Sp_n(q)$ is made up of scalar matrices. $PSp_n(q)$ is simple except for $PSp_2(2)$, $PSp_2(3)$, and $PSp_4(2)$. The order of $PSp_n(q)$ is given by the following formula: $(q^{m^2}(q^{2m} - 1)(q^{2m-2} - 1) \dots (q^2 - 1))/(q - 1, 2)$.

An example of a projective symplectic group is $PSp_2(9)$ which contains 360 elements and is isomorphic to A_6 . $Sp_2(9)$ is a subgroup of $GL_2(9)$, the set of 2×2 matrices over the Galois field of 9 elements. First, we construct $GF(9)$ by looking at the irreducible polynomial $x^2 + 1$ over Z_3 . We find that $GF(9) \cong \{ax + b + \langle x^2 + 1 \rangle\}$ and the elements are

$$\{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}.$$

Following the equations above, and simplifying our example by only looking at elements for which $B = C = 0$, we can write a couple of elements of $Sp_2(9)$:

$$\begin{bmatrix} x + 1 & 0 \\ 0 & x + 2 \end{bmatrix}, \text{ and } \begin{bmatrix} 2x & 0 \\ 0 & x \end{bmatrix}. \text{ The two elements in } Z(Sp_2(9)) \text{ are } \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and since $PSp_2(9)$ is the factor group of $Sp_2(9)$ and these two

elements, we know that $\begin{bmatrix} x + 1 & 0 \\ 0 & x + 2 \end{bmatrix}$ and $\begin{bmatrix} 2x & 0 \\ 0 & x \end{bmatrix}$ are also in $PSp_2(9)$.

One can easily verify that $(x + 1)(x + 2) = 1$, and $(2x)(x) = 1$ in $GF(9)$.

3.1.2.2 Other Lie Groups

A brief mention of the history of other groups of Lie type is in order. During the period 1901 to 1905 a new family of simple groups of Lie type was discovered by Dickson. Until 1955, classical linear and this new family were the only simple groups of Lie type known. Claude Chevalley produced a much needed new way of approaching these simple groups and in the process, he discovered several more infinite families of simple groups of Lie type. These are referred to as the Chevalley groups. Chevalley's progress on the groups of

Lie type successfully increased the interest in the field, and it wasn't long before new infinite families of simple groups of Lie type were found. In particular, in 1960 Suzuki discovered his infinite family while working on what is now called a classification problem (see Chapter 4). He was trying to find all simple groups in which the centralizer of an involution (that is all elements that commute with a particular element of order two) is a group of order 2^n . In the process of trying to eliminate all possibilities except for $PSL(2, 2^n)$ and $PSL(3, 2^n)$, $n \geq 2$, Suzuki found another family with the given property. These are $Sz(2^n)$. In 1961, Rhimak Ree was analyzing the Suzuki groups using a particular method (Steinberg's) which had produced infinite families of Lie type before, and came up with two additional families. Thus, the Chevalley, Steinberg, Suzuki, and Ree groups are the simple groups of Lie type along with the classical linear groups.

3.2 The Sporadic Simple Groups

The remaining known simple groups do not fit into any large model of similar attributes as do the infinite families. They were discovered often one by one. Some do fit together by method of discovery or by construction. We will examine these properties briefly below. First, the following table lists the 26 sporadic simple groups, their order (if not too large), their discoverer (according to some references), and the date of their discovery.

Name	Order	Discovered by	Date
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	Mathieu	1895
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	Mathieu	1899
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Mathieu	1900
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu	1900
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu	1900
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	Janko	1966
$J_2(HaJ)$	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	Hall, Janko	1967
$J_3(HJM)$	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	Janko, Higman, McKay*	1969
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	Higman, Sims	1968
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McLaughlin	1969
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Suzuki	1969
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	Held, Higman, McKay	1969
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway, Leech*	1969
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway*	1969
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway*	1969
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23$	Fischer	1969
Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer	1969
Fi'_{24}	*	Fischer	1969
Ly	*	Lyons, Sims	1971
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	Rudvalis, Conway, Wales	1972
$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	O'Nan, Sims	1973
M	*	Fischer	1974
B	*	Fischer	1974
F_3	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Thompson, Smith*	1974
F_5	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	Fischer, Smith, Harada*	1974
J_4	*	Janko*	1975

Table 3.2: The Sporadic Simple Groups

* The names of discoverers followed by a star are those which have some discrepancy depending on sources. Those orders denoted by a star are

too large to fit this table. For example, the order of the group M , the largest of the sporadic simple groups is

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

3.2.1 The Mathieu Groups

The Mathieu groups, M_{11} , M_{12} , M_{22} , M_{23} , and M_{24} are the earliest sporadic simple groups to be discovered. They were described by Emile Mathieu (1835 - 1900) in 1861 and 1873. Mathieu was influenced by Cauchy's work on permutations. Mathieu was investigating multiply transitive functions, and thus permutation groups and multiply transitive permutation groups. A permutation group on a set A is said to be n -transitive if for any ordered pair of n -tuples of elements of A , there exists some element of the permutation group that maps one tuple to the other. That is, $x_i g = y_i$ for $1 \leq i \leq n$ where x_i and $y_i \in A$ and $g \in$ permutation group of A . A transitive function is one which is left invariant under the permutations of a transitive group, which was discovered by Mathieu. In the course of his work, Mathieu attempted to 'extend' transitivity by constructing an n -transitive permutation group out of a $(n-1)$ -transitive permutation group. He was able to find an algorithm for the construction of these groups, when their construction was possible. The highest transitivity found in a simple group is 5-transitive, and Mathieu discovered the 5-transitive permutation groups on 12 symbols and on 24 symbols which are M_{12} and M_{24} . The other Mathieu groups arose as subgroups of these and a subgroup of M_{23} . For example, M_{11} is the subgroup of M_{12} formed as the

stabilizer of a point in M_{12} . Each of the Mathieu groups are multiply transitive. The simplicity and uniqueness of the Mathieu groups was not expressed until the 1930's in a paper by Witt who was describing what is called the Steiner system. The Mathieu groups are now normally described in terms of this system.

3.2.2 Centralizer of Involution Problems

The next sporadic simple groups were not discovered until around one hundred years after Mathieu's find. The first of these is Janko's first, J_1 , and the method by which it was discovered became an important part of the theory of simple groups and an important method to discover other simple groups. The central feature of the method is the centralizer of an involution, or the centralizer of an element of order two. We have seen how centralizer of involution questions led to Suzuki's infinite families of simple groups of Lie type. The centralizer of an involution as an entity is important due to a number of results. Two of these are a theorem due to Brauer and Fowler and the Feit-Thompson Theorem (or Odd Order theorem), which are both looked at below.

Because an involution is an element of order two, the order of a group containing an involution must be divisible by two. If it were guaranteed that a simple group contained an involution, this may increase the potential of classifying simple groups according to something related to involutions. This result was indeed obtained, in the Feit-Thompson Theorem. It was not a swift theorem to come up with however, and the odd versus even order of simple

groups was a long standing question. In fact, conjectures on this question date back to 1895 and Burnside. Burnside had a good hunch that simple groups must necessarily have even order, and from 1895 to 1901, he attempted to show this. He was successful at proving that all simple groups with orders under 40,000 had even orders, yet he could not generalize his result. He believed that the necessary technique to prove his conjecture was character theory. The problem came alive again in 1957 with the work of Suzuki who was indeed using character theory. Suzuki was able to prove that any simple group in which the centralizer of any element (other than the identity) was abelian has even order. This result was extended in 1960 by Feit, Hall, and Thompson who proved that a simple group must have even order if the centralizer of any non-identity element is nilpotent, i.e., all of its Sylow subgroups are normal. Three years later, the same two, Feit and Thompson, took 255 pages of the *Pacific Journal of Mathematics* [6] to prove that all groups of odd order are solvable. This means that the composition series of a group of odd order contains composition factors of prime order, which indicates that the group is not simple. Thus, any simple group must have even order, and therefore, must contain involutions.

A result pertaining directly to the centralizers of involutions was actually found earlier than the Feit-Thompson Theorem. In 1954, Brauer and Fowler proved that there are at most a finite number of simple groups in which the centralizer of an involution has a given structure:

Theorem 3.2 *If G is a finite simple group of even order, and t is an involution in G , then $|G| \leq (|C_G(t)|^2)!$.*

$C_G(t)$ denotes the centralizer in G of t . Since there can only be a finite number of groups with orders less than a particular number, then there are only a finite number of groups with the centralizer of an involution isomorphic to a given centralizer. This provided the idea of at least some classification of finite simple groups by the structure of the centralizer of involutions. The importance of this result was furthered by the Feit-Thompson Theorem since then the result pertained to all simple groups, not just simple groups of even order. This theorem has been improved upon in the more recent years in many variations using the idea of a central involution which is an involution in the center of a Sylow 2-subgroup. In general, it has been established that if a centralizer of a central involution in a questionable simple group is isomorphic to the centralizer of a central involution in a known simple group, then the two simple groups are isomorphic. These are powerful results which may allow for the characterization of a simple group by its centralizer of a central involution. An example of this type of theorem is the following due to Brauer:

Theorem 3.3 *Let G be a simple group which contains an involution whose centralizer is isomorphic to $GL_2(q)$ factored by a subgroup of odd order in the center of $GL_2(q)$, and where q is an odd prime power congruent to $-1 \pmod{4}$. Then either*

1. $G \cong PSL_3(q)$, or
2. $G \cong M_{11}$ and $q = 3$.

There are many other such theorems, and the theory involved in the study of centralizers of involutions is extensive. This paper will only be able to concern itself with a brief description of the discovery of some of the sporadic simple

groups due to centralizer of involution theory.

Let us return to the next sporadic simple group to be discovered, J_1 . The story of Janko's first group begins with the centralizer of the involutions in one family of Ree groups of Lie type, denoted $R(3^n)$. It was found that the centralizer of an involution of $R(3^n)$ is isomorphic to the group $Z_2 \times PSL_2(3^n)$, the external direct product. It was also noted that the Sylow 2-subgroups are elementary abelian of order 8. Thus, an interesting task became to determine all simple groups with Sylow 2-subgroups with the above properties which have centralizers of involutions isomorphic to $Z_2 \times PSL_2(p^n)$, p an odd prime. For $p^n = 5$, the new simple group J_1 was discovered. Janko proved the following theorem:

Theorem 3.4 If G is a simple group with abelian Sylow 2-subgroups of order 8 and the centralizer of an involution of G is isomorphic to $Z_2 \times PSL_2(5)$, then G is a uniquely determined simple group of order 175,560. Moreover, G is isomorphic to the subgroup of $GL_7(11)$ generated by the following two elements of order 7 and 5:

$$S_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad S_2 = \begin{bmatrix} -3 & 2 & -1 & -1 & -3 & -1 & -3 \\ -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ -1 & -1 & -3 & -1 & -3 & -3 & 2 \\ -1 & -3 & -1 & -3 & -3 & 2 & -1 \\ -3 & -1 & -3 & -3 & 2 & -1 & -1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \end{bmatrix}.$$

Janko was the lucky receptor of further inspiration which led to two

other sporadic simple groups, J_2 and J_3 . After the discovery of J_1 , Janko looked further for possible centralizers of involutions inspired by those in the Mathieu groups. He tried a centralizer of an involution which was isomorphic to the extension of a group of order 32 by A_5 . He actually found two new groups with the same centralizer of an involution, J_2 and J_3 . Hall and Wales proved the existence of J_2 , and Higman and McKay proved the existence of J_3 .

The question of the existence of two simple groups with isomorphic centralizers of involutions led to the discovery of the next sporadic simple group in the story. (We now cease chronological order). D. Held knew that the groups M_{24} and $PSL_5(2)$ have involutions with isomorphic centralizers. While investigating this phenomena, Held discovered yet another simple group with the same centralizer of an involution, He . This is the only case of three simple groups with isomorphic centralizers of involutions.

The next sporadic simple group to be obtained by examining centralizers of involutions is Ly . John McLaughlin's group, Mc , to be discussed below, has a centralizer of an involution which is isomorphic to the group \hat{A}_8 which denotes the perfect extension of A_8 by Z_2 . The idea then arose to study centralizers of involutions which are isomorphic to \hat{A}_n for $n \geq 5$. On such an investigation, Richard Lyons, who was a student of Thompson's, made the following discovery:

Theorem 3.5 *If G is a simple group in which the centralizer of an involution is isomorphic to \hat{A}_n , $n = 10$ or 11 , then $n = 11$, and*

$$|G| = 2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67.$$

In fact, the result was shown that simple groups could only arise from centralizers of involutions isomorphic to \hat{A}_8 and \hat{A}_{11} . Incidentally, It was Janko who had worked on this problem. He showed that when $n = 9$ and 10 , there were no simple groups with the said centralizer of an involution. He gave up before working on $n = 11$. He did however discover the last sporadic simple group falling under the category of centralizer of involution problems, and that was J_4 .

3.2.3 Rank 3 Permutation Groups

The group J_2 has a structure which became important to the construction of four more sporadic simple groups. J_2 is said to be a primitive rank 3 permutation group. A group G has permutation rank r if G is transitive on a set Ω and the subgroup of G that fixes a point of Ω has exactly r orbits on Ω . Recall that a group is transitive if for a set Ω , and any two elements α and $\beta \in \Omega$, there exists an element $g \in G$ such that $\alpha \cdot g = \beta$. Also, the subgroup of G that fixes a point of Ω are those elements in G for which $\alpha \cdot g = \alpha$. The orbits on Ω are sets of the form $\{\alpha \cdot g \mid g \in G\} \subseteq \Omega$. The orbits of Ω partition Ω . The group J_2 fits this description if one considers the maximal subgroup of index 100, $H \subseteq J_2$. The permutation representation of J_2 on the right cosets of H is a transitive action which produces a primitive permutation representation of J_2 of degree 100 (i.e., J_2 is a transitive permutation group of degree 100), which takes the role of the set Ω above. On this set, H fixes one point and its action produces two other orbits, rendering J_2 a rank 3 permutation

group. In fact, the existence of J_2 was proven using the theory of rank 3 permutation groups. The maximal subgroup H happened to be isomorphic to the simple projective special unitary group, $U_3(3)$. Donald Higman and C. Sims noted the similarity in permutation properties between the groups $U_3(3)$ and M_{22} , and in record time were able to construct a new simple primitive rank 3 permutation group using M_{22} as the maximal subgroup and ‘extending’ it to obtain the group HS . A similar technique was used by McLaughlin who started with the group $U_4(3)$ to extend it to a rank 3 permutation group that is simple, called McL . Suzuki obtained his sporadic simple group Su in the same manner starting with $G_2(4)$ (a Chevalley Lie type simple group). Finally, the fourth rank 3 permutation group was constructed by Rudvalis using the Ree group, ${}^2F_4(2)$. It is Ru .

3.2.4 The Remaining Sporadic Simple Groups

This shall serve to briefly describe the discovery of the remaining sporadic simple groups. The Conway groups, Co_1 , Co_2 , and Co_3 came out of the study of an automorphism group of a lattice called the Leech lattice which is determined by a set of vectors in 24-dimensional Euclidean space with integral coordinates. The three simple groups happen to have been subgroups of this automorphism group. The Fischer groups, Fi_{22} , Fi_{23} , and Fi'_{24} were discovered by Fischer while studying classes of 3-transpositions. These are conjugacy classes generated by involutions such that the product of two involutions in the class has order 2 or 3. Fischer generated groups by these classes, and put further conditions on the groups proving that the new group

is either a symmetric group, a certain classical group, or one of the three Fischer groups. Fischer then turned to groups generated by $\{3,4\}$ -transpositions (two involutions in a class have a product of order 2, 3, or 4). Two groups, B and M , or Baby Monster and Monster were discovered. The Monster is the largest sporadic simple group, and a representation for it was obtained *by hand* by Robert Griess. It was in terms of square matrices that were 196,883 by 196,883 in size. The groups B , F_3 , and F_5 are actually subgroups of the Monster. F_3 was found by Thompson, and F_5 is attributed to Harada, Norton, and Smith. The O’Nan group came out of the study of groups with particular Sylow 2-subgroup structure.

The methods used to discover new sporadic simple groups were often haphazard, as Daniel Gorenstein says, “some of the groups seemed literally plucked from thin air [9].” Sometimes the techniques used were character theory-based. In fact, Feit, Thompson, and Brauer were quite well known for their work in and development of character theory. There are really three phases in determining a new simple group, and only one of those phases I have taken consideration of here. There is the discovery, which is what I have described, there is the existence and there is the uniqueness. Often several different individuals contribute to the determination of the existence and the uniqueness of a new simple group. The discoverer is generally who the group is named after. The simple groups found later than J_1 had the timely advantage of computers to aid in their discovery, existence, and uniqueness questions.

4. The Classification Theorem

4.1 History

The study of centralizers of involutions proved not only very useful in locating certain sporadic groups, but also marks what some would consider the start of the classification project. As noted above, in 1954 Brauer made his great discovery that there are only a finite number of groups with their centralizers of an involution having a particular structure. This seemed to spur the idea of the characterization of simple groups according to their centralizer of an involution. It was in fact Brauer who suggested such a thing, and was successful with his use of character theory in certain cases. Others contributed to this line of study, and some good results were obtained, often with the discovery of sporadic simple groups. Brauer's ideas served to provide a new avenue down which some could dream of an overall classification of all finite simple groups. There were also certain advances in theory that inspired many to take part in the study of simple groups. The work of Brauer and Suzuki in character theory provided one. The new discoveries about Lie groups in the 1950's is another. But in the 50's, there was still much to be accomplished before a classification idea could become a reality.

The 1960's provided the study of simple groups with some of those high powered results it needed. The most influential is the famous 1963 Feit-Thompson theorem, or the odd order theorem, which states that all groups of

odd order are solvable. It was not only the result that was terribly influential, but also the structure of this 255 page proof. Thompson was also responsible for another very important result which took 410 pages and six years (1968-1974) to complete. This is the classification of minimal simple groups, or those simple groups which have only solvable groups as subgroups. Following Brauer's program, Suzuki was able to characterize all simple groups in which the centralizer of an involution has a normal Sylow 2-subgroup in 1965. Sylow 2-subgroups were becoming as telling as centralizers of involutions, and many results stemmed from their study. In particular, Gorenstein and Walter characterized simple groups with dihedral Sylow 2-subgroups also in 1965. In 1969, Walters classified simple groups with abelian Sylow 2-subgroups. These are general characterizations. An example of a specific characterization is Glauberman's Z^* -theorem of 1966 which showed that every involution is conjugate to another involution in its centralizer. These are only a few of the important steps taken in the 1960's, and many other results were to follow.

By the 1970's, there were many roads to classification, although no systematic idea of its achievement. There were also many sporadic groups discovered in the 1960's, and some wondered if there was an endless supply of them. Thus, in 1972 at the University of Chicago, when Gorenstein presented his idea of a 16-step plan to classify all simple groups, not many were optimistic. Gorenstein projected that to complete his program would take about thirty years. The task seemed daunting, yet a few tackled portions of the plan. The project was propelled rather suddenly by a newcomer, Michael Aschbacher, who "came on now like a whirlwind, moving directly to a leadership

position and sweeping aside all obstacles, as he proved one astonishing result after another [9].” The results being made at this time were obviously highly complex, and therefore cannot be handled in this paper. It should be noted that the original plan of 30 years was decreased to an actual 10 years, and Gorenstein attributes this to Aschbacher. The completion of the classification theorem took place in January of 1981.

Some Methods

The methods used in pursuing the idea of the complete classification of finite simple groups naturally changed as progress was made. As can be noted from previous chapters, character theory was used frequently for many results. It turns out that character theory is limited in handling ‘large’ simple groups. Smaller groups, such as lower ordered groups, or groups with Sylow 2-subgroups that are restricted structurally (such as abelian) are good candidates for the use of character theory in examining them closely. However, as the questions about the group’s internal structure became more broad, new techniques were needed. These techniques are called *local group-theoretic analysis*, or local analysis. It was the Feit-Thompson theorem that initiated the practice of local analysis. The predecessors of the Feit-Thompson theorem, Suzuki’s abelian centralizer result and the Feit, Thompson and Hall result on nilpotent centralizers (see p.45) used character theory to develop the lattice of proper subgroups of the group in question. This required analysis of every subgroup. This process could not be used in the Feit-Thompson theorem, since there was no information on the structure of centralizers to rely on. A new set of techniques was developed by Thompson, and their main emphasis

was to look at centralizers and normalizers of prime power order subgroups and analyze their relationships. A new term was coined for the normalizer of a nonidentity prime power subgroup, and that was local or p-local subgroup (p being the prime power). Thus, the techniques of local analysis are the methods of examining local subgroups.

The local analytic methods were explored further by Thompson in his classification of minimal simple groups, and his N -group theorem of 1968. An N -group is a simple group whose local subgroups are each solvable. Thompson explored all possible simple groups fitting this description, and was able to classify the N -groups:

Theorem 4.1 *If G is a simple N -group, then G is isomorphic to one of the following groups:*

- $PSL_2(q)$, where $q > 3$,
- $Sz(q)$, where $q = 2^{2n+1}$, $n \geq 1$,
- $PSL_3(3)$, $U_3(3)$, ${}^2F_4(2)'$, A_7 , or M_{11} .

$U_3(3)$ is a unitary group, and ${}^2F_4(2)'$ is a Ree group of Lie type. Thompson's strategy was to show that an arbitrary N -group has internal structure that looks like one of the groups listed. Then resemblance was shown to be actual isomorphism. This process is mirrored in the classification theorem, as will be seen below. One concept that was invaluable to Thompson's N -group theorem and later to local analysis in general was the idea of 'embedded subgroups'. An example of a type of embedded subgroup is a 'strongly embedded subgroup' M of G . This means that $|M|$ is even and the following hold:

1. $C_G(t) \subseteq M$ for every involution t of M
2. $N_G(S) \subseteq M$ for each Sylow 2-subgroup S of M .

Strongly embedded subgroups themselves were actually classified by Bender in 1971 as either $PSL_2(q)$, $U_3(q)$, or $Sz(q)$ for q even.

While local analysis was developed, and results of a different nature were obtained because of the change of emphasis, there were also further changes in direction by creative individuals. A couple of these different approaches are mentioned now. The method of both the Feit-Thompson theorem and many classification theorems that followed was generally to look at minimal counterexamples and either derive a contradiction to the theorem statement, or show isomorphism of the group in question to a known simple group. The procedure to achieve this was to examine relatively small subgroups to develop the local subgroup structure. Helmut Bender changed this approach in his attempt to simplify the proof of the Feit-Thompson theorem. He studied the intersections of maximal subgroups which contained the centralizer of some involution. This approach is called the *Bender method*, and was used to dramatically reduce the complexity of such theorems as Walter's result about abelian Sylow 2-subgroups, and Gorenstein's and Walter's result about dihedral Sylow 2-subgroups. Originally, Bender was looking for a revision of the classification as a whole, beginning with the Feit-Thompson theorem, but his method became a useful tool in itself.

Another innovation that was second only to local analysis techniques

was Fischer's *internal geometric analysis*. We have seen the work of Fischer with respect to the discovery of sporadic simple groups. His ideas of 3-transpositions went much further than only the discovery of his sporadic groups however. Recall that a class of 3-transpositions is a conjugacy class of involutions where the product of any two has order 1, 2, or 3. Also, the group G in question is generated by this conjugacy class. Fischer's geometric approach was to consider a graph whose vertices are the elements of the conjugacy class, and any two elements which commute with each other are connected by an edge. The group G acts as a group of automorphisms of the graph since under conjugation, G permutes the vertices of the graph but preserves the incidence relation on the graph. Thus, Fischer saw that the structure of the group G is related to the geometry of the graph. His work inspired others such as Aschbacher, and the definitions of *connected* and *nonconnected* came from the nature of the graphs. We will see that these play a very important role in the classification theorem.

4.2 The Theorem

The entire classification theorem is a monumental enterprise of between 10,000 and 15,000 pages, taken from around 100 contributors, and written over a period of more than 30 years. There are articles stretching out among perhaps 500 journals that comprise the theorem. The main contributors are an international group mainly from the U.S., Germany, England, Canada, Australia, and Japan. Results were collected starting around the late 1940's and complete classification was obtained in the early 1980's. We

have seen that a systematic approach to the classification was proposed as late as 1972. The theorem itself states that all finite simple groups have been found. That is, any finite simple group is isomorphic to one of those already discovered:

Theorem 4.2 *Main Classification Theorem: Every (nontrivial) finite simple group is isomorphic to one of the following:*

1. *A group of Lie type*
2. *An alternating group*
3. *One of the above mentioned 26 sporadic groups (see p.42).*

The general structure of the theorem is that of induction. A minimal simple counterexample G is chosen such that G is assumed not isomorphic to any known simple group, and any simple group with order less than G is a known simple group. Also, suppose that the group G has a set of properties, X . Given this information, one can prove that G is actually a known simple group, deriving a contradiction. The inductive nature of the proof is important for looking at internal properties of subgroups of G . For example, there is a result which states that:

Theorem 4.3 *Given a minimal simple counterexample G with a set of properties X , if $H \subset G$ and $K \triangleleft H$, then H/K is a simple group with properties X .*

An alternate form of the classification theorem which makes the inductive nature obvious is the following:

Theorem 4.4 *Main Classification Theorem, alternate form: If G is a finite simple group each of whose proper subgroups is a known simple group, then G*

is a known simple group.

Suppose that we have a minimal counterexample G with X properties that we assume is not a known simple group. This assumption forces us to consider the internal properties of G to be as complicated as *any* finite group. We cannot assume that G looks like a known simple group from the start, for that is what we are trying to prove. The next step is to force our counterexample to look like a known simple group. Obviously, this is not an easily accomplished task and many of the high powered local analysis techniques must be used carefully in the examination of the internal structure of the group. There are many possibilities for a group G with X properties, and each must be considered. This accounts for much of the complexity and length of the theorem, since there are around 100 different paths to follow to show that G looks like a known simple group. The paths themselves are determined by the properties of G , so each case is different. The classification theorem is complete in that it exhausts all of the possible structures of G and leads all possible simple groups to the structure of a known simple group. In order for us to know that our simple group looks like a known simple group, we must have a very detailed description of the known simple groups. This part of the theorem is called the recognition theorems. Once it is determined that G ‘looks like’ a known simple group, then the steps toward isomorphism must be taken. That is, internal resemblance must be shown to be actual isomorphism.

It is to be noted that the structure of the classification theorem is very similar to that of the Feit-Thompson theorem. In fact, one can break

down the process of both into three steps: [10]

1.) Use the given properties of G to determine the structure and embedding of maximal subgroups containing or intersecting centralizers of involutions by local analysis.

2.) Eliminate as many of these possible configurations by using character theory on smaller groups, local analysis on larger groups, and arithmetic methods.

3.) Use recognition theorems (generators and relations) to prove that the only possible configuration left is isomorphic to a known simple group.

Beginning with the last step first, each of the known simple groups must be recognizable by some defining feature. These recognition theorems usually are in terms of generators and relations, especially for the groups of Lie type. The alternating groups can also be characterized by generators and relations, as the following theorem shows:

Theorem 4.5 *If the group G is generated by the elements x_1, x_2, \dots, x_{n-2} subject only to the relations $x_1^3 = 1$, $x_i^2 = 1$ for $2 \leq i \leq n-2$, $(x_i x_{i+1})^3 = 1$ for $1 \leq i \leq n-3$, and $(x_i x_j)^2 = 1$ for $1 \leq i \leq n-4$ and $i+1 < j$, then $G \cong A_n$.*

The recognition theorems for the sporadic groups usually depend on how the sporadic group was constructed. For example, those sporadic groups which were constructed by their centralizer of an involution can be characterized by this centralizer. (Theorems 3.4 and 3.5 are examples of recognition theorems). Those sporadic groups which are rank 3 are characterized by their one point stabilizers. (See p.49) Thus, much of the discussion in Chapter two serves to describe some of the recognition theorems. If the counterexample

group G^* is shown to have such characteristics as are given in the recognition theorem of group G , then the purpose of the recognition theorems is to state that G^* is necessarily isomorphic to G .

The first two steps of the classification theorem are then to prove that G^* has some defining features that are in one recognition theorem. We have seen that centralizers of involutions and Sylow 2-subgroups play an important role in the internal structure of any simple group. Many sophisticated features of a group have been discovered in relation to these two. One of the reasons for this is that Sylow 2-subgroup structure depends on the properties of centralizers of involutions (since Sylow 2-subgroups contain all of a group's involutions, and there is always an involution in the center of a Sylow 2-subgroup), and centralizers of involutions can often lead to recognition theorems. There are complicated techniques to achieve this leap however, including what are called 'fusion arguments'. The purpose of this line of theory is to give precise descriptions of the way in which involutions in a Sylow 2-subgroup are conjugate in the group. Some of the famous results are Glauberman's Z^* theorem, Thompson's fusion lemma, and Alperin's fusion theorem. Embedding is another property of subgroups which developed into important theory. What are called 'signalizer functor methods' grew out of the study of embedded subgroups. The accumulation of all of the possible internal structures of a simple group can be summarized in the four part division of the main classification theorem proof:

- The classification of nonconnected simple groups,
- The classification of connected simple groups of component type,
- The classification of 'small' simple groups of characteristic 2 type

- The classification of ‘large’ simple groups of characteristic 2 type [10].

The definitions of each of these are quite involved. We have seen how connected and nonconnected groups might arise. Let us now define characteristic 2 type.

Definition X is characteristic 2 type if $F^*(H)$ is a 2-group for every 2-local subgroup H of X .

Now $F^*(H)$ is called the *generalized fitting subgroup* of X and

$$F^*(H) = L(X)F(X).$$

$F(X)$ is the *fitting subgroup* of X , which means it is the unique largest nilpotent subgroup of X .

$L(X)$ is the *layer* of X , which means that $L(X)$ is the product of all *subnormal quasisimple* subgroups of X , with $L(X) = 1$ if no subnormal subgroups exist.

A subnormal subgroup of X is a subgroup Y such that $Y = Y_1 \triangleleft Y_2 \triangleleft \dots \triangleleft Y_n = X$ for appropriate subgroups Y_i of X .

A quasisimple subgroup of X is a subgroup K such that $K = [K, K]$ and $K/Z(K)$ is simple.

$$[K, K] = \langle [k, k] \mid k \in K \rangle \text{ where } [k, k] = k^{-1}k^{-1}kk.$$

This gives a glimpse of the complexity involved in pinning down the internal structure of a simple group. The four part division above can actually be reduced to two parts, that concerning noncharacteristic 2 type, and that concerning characteristic 2 type groups.

We have taken a rather nontechnical look at the ‘enormous theorem’ as Gorenstein refers to it. Hopefully this will serve as at least an introduction

to the main objective and some methods of the proof. A revision of the proof has been suggested, and begun. It was spearheaded by Daniel Gorenstein who unfortunately died in 1992. With such a large proof to begin with, it is generally held that completely new techniques would have to be obtained before any remarkable reduction in length could be realized. When the theorem was nearing completion, a headline in the *New York Times* read, “A School of Theorists Works Itself Out of a Job”, 1980. Yet all of those involved in the proof had positive ideas of the future of group theory. Gorenstein cited applications to such fields as mathematical logic and number theory due to the classification theorem [11]. The relationship between finite group theory and finite geometries was mentioned by Aschbacher as possibly benefitting from the classification theorem [1]. Also even within the field of group theory, many felt there was much to do. As Gorenstein comments, “the obituary for finite group theory has been totally premature [9].” The theorem itself is a testament to the perseverance and cooperative nature of human kind. It has been said in reference to the length and complexity of the theorem that either they have been a bit dim in finding the most effective techniques to prove the classification theorem, or they have been *very* clever indeed.

REFERENCES

- [1] M. ASCHBACHER, **The Finite Simple Groups and Their Classification**, Yale University Press, 1980.
- [2] —, **Finite Group Theory**, Cambridge University Press, 1986.
- [3] R. W. CARTER, **Simple Groups of Lie Type**, John Wiley and Sons, 1989.
- [4] M. J. COLLINS, **Finite Simple Groups II**, Academic Press Inc., 1980.
- [5] J. CONWAY, R. CURTIS, S. NORTON, R. PARKER, AND R. WILSON, **Atlas of Finite Groups**, Clarendon Press Oxford, 1985.
- [6] J. GALLIAN, **The Search for Finite Simple Groups**, *Mathematics Magazine*, 49 (1976), pp. 163–179.
- [7] —, **Contemporary Abstract Algebra**, DC Heath and Co., 1994.
- [8] D. GORENSTEIN, **Finite Simple Groups and Their Classification**, *Israel Journal of Mathematics*, 19 (1974), pp. 5–66.
- [9] —, **Finite Simple Groups, An Introduction to their Classification**, Plenum Press, NY, 1982.
- [10] —, **Classification of Finite Simple Groups Vol I**, Plenum Press, NY, 1983.
- [11] —, **The Enormous Theorem**, *Scientific American*, 253 (1985), pp. 104–115.
- [12] M. HALL JR., **A Search for Simple Groups of Order Less than One Million**, in *Computational Problems in Abstract Algebra*, J. Leech, ed., Pergamon Press, NY, 1969, pp. 137–168.
- [13] I. M. ISAACS, **Algebra A Graduate Course**, Brooks/Cole Publishing Co, 1994.

- [14] M. B. POWELL AND G. HIGMAN, **Finite Simple Groups**, Academic Press Inc., 1971.
- [15] R. SILVESTRI, **Simple Groups of Finite Order in the Nineteenth Century**, *Archive for the History of Exact Sciences*, 20 (1979), pp. 313–356.
- [16] I. STEWART, **Galois Theory**, Chapman and Hall, 1989.
- [17] H. WEYL, **The Classical Groups**, Princeton University Press, 1946.