AN ABSTRACT

OF THE THESIS WRITTEN BY

Elisabeth Bletscher Henkle for the degree

Master of Arts in mathematics presented on

December 11, 1986 .

Title: Finite Simple Groups

Abstract approved: Marion P Emerson

A specific type of mathematical construct, called a finite simple group, is the subject of this paper. The information presented attempts to be comprehensive in the fact that it covers a broad range of topics connected to finite simple groups. A historical overview is given along with a survey of both past and present research. The direction and purpose of this research is explained in addition to mentioning those papers of key significance.

Simplicity, the special property possessed by all finite simple groups, is given a concrete foundation through definitions and frequent comparisons with the prime numbers. Each of the four types of finite simple groups are discussed within the limitations of the length of the paper and the technical knowledge of the author.

Since all finite simple groups are now known, they can be used to construct any finite group imaginable. This fundamental nature of finite simple groups is justified in this thesis with major theorems and examples. Miscellaneous facts, uniquely associated with finite simple groups, serves as a conclusion.

FINITE SIMPLE GROUPS

A Thesis
Submitted To
The Division of Mathematical and Physical Sciences
Emporia State University

In Partial Fulfillment
of the Requirements for the Degree
Master of Arts

By
Beth Bletscher Henkle
December 1986

James Lowell

Approved by the Graduate Council

Marion P. Emerson

Approved by the Major Department

ACKNOWLEDGMENTS

The completion of this thesis would not have been possible without the contributions of three individuals.

I want to thank Dr. Marion P. Emerson for suggesting the topic of this thesis and for his assistance throughout the writing of this paper.

I also want to thank my mother, Carlene Bletscher, for her endless hours of proofreading my somewhat peculiar punctuation.

Finally, I am indebted to my husband, Jeff Henkle, for his encouragement and patience. He listened to many discussions concerning simple groups without understanding a word I said to him.

TABLE OF CONTENTS

LIST OF TABLES

Chapter I

INTRODUCTION

It is natural for the human mind to impose a hierarchial structure on real world phenomena. Organizing chaotic perceptions is generally the purpose of such ordering schemes. For instance, processes are designed so that from a beginning point there occurs a step-by-step progression to completion. Likewise, most objects are built up in layers from an underlying framework, as in the construction of a house or an automobile. With a world view such as this, there are numerous areas of concern. The focus, however, is often the beginning point and its basic components. Whether it is biologists studying the genetic code of life or physicists in pursuit of subatomic particles, no one is immune from the desire to both know and understand fundamental structures. Contrary to Gestalt philosophy, the whole is frequently perceived as the sum of its parts. This implies both knowing the parts and how they interact.

Mathematicians are especially prone to this perspective due to the logical and axiomatic nature of their subject. Finite groups are mathematical constructs not immune from this point of view. A lengthy search has been conducted for the building blocks of finite groups with the outcome being what are called finite simple groups. Four types of finite simple groups have been uncovered. These categories are cyclic groups of prime order, alternating groups, groups of

Lie type (pronounced Lee), and sporadic groups.

Another separate but related part-whole relationship arises from the role played by prime numbers in the set of positive integers. Almost everyone knows what it means for a positive integer to be prime since all of us, at one time or another, sat in elementary school studying factor trees. It is an intuitive concept that feels right. Finite simple groups can be viewed like prime numbers with a resemblance in both definition and purpose.

The area of finite simple groups has generated an enormous amount of research over the past thirty years. During this time, experts have been concerned with both the discovery of new finite simple groups and with what has grown to be called the Classification Theorem. In February 1981 the uniqueness of the last finite simple group, a member of the sporadic category, was confirmed by a mathematician named Simon Norton. Consequently, a milestone had been reached, since the entire substructure of finite groups, at that point, could be considered known and describable.

It is the intention of this thesis to explore three major areas. First, the author will review both past and present finite simple group research. Secondly, the various types of finite simple groups will be explained. Finally, the importance of finite simple groups to the general field of finite group theory will be demonstrated. Miscellaneous subjects, of special interest to finite simple groups, will

conclude the paper.

Although there exist infinite simple groups, only finite simple groups and finite groups will be considered in this thesis. Therefore, the phrases "group" and "simple group" should be understood to mean the finite case.

Dates of events are troublesome in the field of mathematics. Theoretically, discovery occurs the instant a mathematician proves an unproven theorem or finds an unknown entity. Often, however, this date is not recorded. Anywhere from one to three years can pass before the new result is published in a mathematical journal. This date of publication is recorded and available to any interested person. So frequently a publication date is substituted for a questionable discovery date, and this convention will be followed in this thesis when necessary.

Notation, Definitions, and Theorems

Notation in this paper is standard for the topics involved. In several instances, it is defined as it is initially used, but knowledge of general group theoretical concepts is assumed to be known. The following list of notational explanations, definitions, and theorems should be familiar. They are presented here, however, for review and reference.

Notation

The ring of integers modulo n is denoted Z_n.

Notation

Let N be a normal subgroup of G. The factor group formed by all cosets of N in G is indicated by G/N.

Definition
The order of G, denoted $|G|$, is the number of elements in G.

Definition
Two groups G and H are isomorphic, denoted $G \sim H$, if there is an isomorphism $f: G \rightarrow H$.

Definition
The center of a group G is the set of c in G such that $cx = xc$ for all x in G.

Definition
If a, b are elements of G, the commutator of a and b is the element $a^{-1}b^{-1}ab$. The commutator subgroup of G is the subgroup of G generated by all the commutators in G.

Definition
Let $H_1, H_2, \ldots, H_n$ be nonempty subsets of a group G. Then $H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_1 \in H_1, h_2 \in H_2, \ldots, h_n \in H_n\}$.

Definition
A subgroup N of a group G is a normal subgroup of G if and only if $g^{-1}Ng = N$ for all g in G.

Definition
Let N be normal in G. The map $f: G \rightarrow G/N$ is called the natural map.

Theorem (Lagrange's Theorem)
If S is a subgroup of a finite group G, then $[G:S] = |G|/|S|$ where $[G:S]$ is the number of right cosets of S in G.

Theorem (Correspondence Theorem)
Let K be a normal subgroup of G and let $f: G \rightarrow G/K$ be the natural map; f defines a one-to-one correspondence between the set of those subgroups of G containing K and the set of all subgroups of G/K. If the subgroup of G/K corresponding to the subgroup S of G is denoted S^*, then
(i) $S^* = S/K = f(s)$;
(ii) S is normal in G if and only if S^* is normal in G/K.

Theorem (External Direct Product)
If $G_1, G_2, \ldots, G_n$ are groups, the set of elements $(x_1, x_2, \ldots, x_n)$ with x_i in G_i for $i = 1, \ldots, n$ form a group G under the operation $(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n)$, where y_i is also in G_i and x_iy_i denotes the product in G_i. The group G is called the external direct product of the G_i and this is expressed as $G = G_1 \times G_2 \times \cdots \times G_n$.

Theorem (Internal Direct Product)

Let G_i be normal subgroups of G, $1 \leq i \leq n$, which satisfy the following conditions:

(a) $G = G_1 G_2 \cdots G_n$.

(b) $G_i \cap (G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n) = \{e\}$, $1 \leq i \leq n$.

Then it follows that

(i) Each x in G has a unique representation of the form $x = x_1 x_2 \cdots x_n$ with x_i in G_i, $1 \leq i \leq n$.

(ii) The mapping $f(x) = (x_1, x_2, \ldots, x_n)$ of G into $G_1 \times G_2 \times \cdots \times G_n$ is an isomorphism.

Under these criteria, G is called the internal direct product of its normal subgroups G_i, $1 \leq i \leq n$. It is customary to abandon the above isomorphism and write this fact as $G = G_1 \times G_2 \times \cdots \times G_n$. When direct product is used in this paper, the point of view is internal.

Chapter II

A HISTORICAL PERSPECTIVE

Early Beginnings

The abstract concept of a group was introduced into mathematics during the nineteenth century. Although no individual is solely responsible for its development, Evariste Galois is credited with beginning the field of group theory since he was the first to apply groups towards the study of algebraic problems. His work led to a proof of the insolvability of fifth degree polynomials and to the name "group." So the concept of a simple group is not new to mathematics. In fact, infinitely many simple groups, primarily the alternating groups of degree greater than or equal to five and the cyclic groups of prime order, have been known to exist for over one hundred years. Likewise, most of the simple groups of Lie type were known well before Chevalley's systematic and unifying treatment of them in a journal article published in 1955. Around 1860 a mathematician named Emile Mathieu discovered the first five simple groups belonging to a new and unusual category now called sporadic. But until the 1940s, when Richard Brauer entered the field, this academic area was incomplete and suffered from neglect.

Two factors share responsibility for this inattention. First, there were inadequate techniques available to study subgroup structures from which new simple groups might be constructed. Secondly, the enumeration of all simple groups

was viewed as an impossible task. Mathematicians would have to search through an infinite number of groups in order to classify the ones that were simple. Pioneers such as Brauer solved the first problem by developing novel methods of analyzing the relationships between a group and its special types of subgroups. These techniques form the basis of what is presently called "local group-theoretic analysis" [11, p. 11]. The second problem was simplified by the monumental paper entitled "Solvability of Groups of Odd Order" written by John Thompson and Walter Feit in 1963. By proving William Burnside's conjecture that all finite groups of odd order are solvable, these mathematicians narrowed the search for simple groups to those groups having an even number of elements. The proof of their theorem "required a full 255-page issue of the Pacific Journal of Mathematics" forshadowing the length of future investigation [11, p. 1].

Soon thereafter, research into simple groups increased dramatically. The amount of time and labor invested in their discovery is staggering. "This unprecedented group effort, which has been described as a mathematical equivalent of the Manhattan project, has been carried out primarily by finite-group theorists in the U.S., Britain and West Germany" [13, p. 84]. Mathematicians Michio Suzuki and Rimhak Ree completed the list of groups of Lie type when they stumbled across several unrecognized exceptions. Sporadic simple groups, a category which had been dormant for one hundred years since Mathieu's work, were revived

when a new group was discovered by Zvonimir Janko in 1966. During the next ten years, twenty additional sporadic groups were uncovered, the last one being the Fischer-Griess group F_1 whose uniqueness was established in 1981. Not surprisingly, the focal point of this inquiry was the sporadic simple groups. Unlike the other categories of simple groups, sporadic groups were difficult to discover due to their ambiguous structures.

Experts did not expect their search to end so quickly. Mathematicians constantly debated whether a complete list or catalogue of all simple groups was feasible. Although intuition implied this should be the case, the sporadic category kept producing groups that created havoc and doubt. This is exemplified in a speech given by Richard Brauer at a meeting of the American Mathematical Society in 1976. There he stated, "The crux of the matter then is the question: 'Are there finitely many or infinitely many sporadic groups?'" [3, p. 22]. His death in 1977 was unfortunate. This pioneer did not live to see the full classification of all finite simple groups of which only twenty-six are sporadic.

Classification Theorem

Finite simple group research can be divided into two separate but interdependent areas. Discovery of new simple groups constitutes the first. It is a several-step process beginning when a mathematical expert obtains evidence indicating a new simple group might exist. Next, in order to

substantiate its existence, the simple group must be constructed. For some groups this stage was accomplished by hand, while others required the assistance of a computer. The last stage of discovery involves proving the existence of the simple group to be unique. Occasionally these steps occurred concurrently due to the brillant insight of one mathematician. On the other hand, discovery was often attributable to a team effort prevailing after several years of research. For example, evidence pointing to the existence of the Fischer-Griess sporadic simple group F_1 was simultaneously realized by Robert Griess and Bernd Fischer in 1974. Griess constructed the group by hand in 1980. Uniqueness of F_1 was established in two stages by John Thompson in 1979 and Simon Norton in 1981. Thus, discovery of the elusive simple group F_1 required approximately seven years. Searching for simple groups was not always this successful. More often than not, a step of the discovery process would lead to a contradiction rendering a suspected group nonexistant.

Classification is the second category. Generally speaking, classifying a collection of objects refers to finding a single global explanation for their existence. This was achieved on a local and specific level throughout the busy research years when mathematicians determined every simple group satisfying various properties. For instance, all simple groups having order of the form $p^aq^br^c$ with p, q, r primes and $p < q < r$ are known [11, p. 12]. This

description classifies a special subset of simple groups. In a similar but more global manner, the Classification Theorem classifies all simple groups by asserting that every one of them has been realized and can be described. At the outset of the simple group odyssey, this goal was not specifically delineated. Instead, repeated applications of the previously mentioned discovery process gradually spawned this theorem. It is not a theorem in the the usual mathematical sense, since its proof is scattered across approximately 500 journal articles [12, p. 31]. When combined, these papers form a verification of the Classification Theorem that is around 15,000 pages long [12, p. 55].

Informally, the Classification Theorem asserts that every finite group is on a completely specified list. Stated more rigorously:

CLASSIFICATION THEOREM. Every finite simple group is isomorphic to one of the following:

1. A cyclic group of prime order;
2. An alternating group;
3. A member of one of sixteen infinite families of groups of Lie type;
4. One of twenty-six sporadic groups. [12, p. 3]

Presently, the direction of study has shifted from finding and constructing new simple groups to refining the Classification Theorem. Since it is a first in mathematical history, the classification proof has received mixed reviews

from the mathematics community. It is inaccessible to most mathematicians due to its length and complicated intertwining of journal articles. Many feel the extreme size is enough to discredit the proof since ". . . the possibility of an apparently 'local' error having 'global' implications is ever present" [12, p. 53]. Consequently, they support an untried approach to the classification problem. Others, such as Daniel Gorenstein, Richard Lyons, and Ronald Soloman, view the overall direction of the proof as valid. Currently, these three men are working together giving the proof "major surgery," to use Gorenstein's own words [12, p. 55]. They have devised an outline for a condensed proof which, when completed, should be roughly 3,000 pages long. For a detailed treatment of this outline see [12, pp. 53-93]. Only the passage of time and further research can determine whether this reduction in length and in-depth reanalysis will increase the appeal and acceptance of the Classification Theorem's proof.

Chapter III

THE NATURE OF FINITE SIMPLE GROUPS

Before the general relationship between finite groups and finite simple groups can be presented, it is important to look specifically at what it means for a group to be simple. Understanding the parts is a prerequisite to comprehending any part-whole relationship.

General Description

Definition

A group G is **simple** if and only if it contains no proper normal subgroups and $G \neq \{e\}$.

The similarity between this definition and that of a prime number should be noted. A positive integer $p \neq 1$ is called prime if its only positive divisors are the trivial divisors 1 and p. Likewise, a group G is simple if its only normal subgroups are the identity subgroup and the whole group G. Corresponding to the fact that 1 is not prime is the fact that the identity subgroup $\{e\}$ is not simple. Thus, a simple definition for a simple group has been established, but this is where the simplicity ends. As a whole, these groups are not simple in the uncomplicated or elementary sense. Their structures are exceedingly complex and their elements intricately interrelated. It is now time to describe the four categories of finite simple groups.

Cyclic Groups Of Prime Order

Before giving a definition, the following notation is needed. If $g \in G$, let $[g]$ denote the set of all powers of g.

Definition
A group G is **cyclic** if $G = [g]$ for some $g \in G$.

Thus, a cyclic group of prime order is a cyclic group G such that $|G| = p$ where p is a prime number. A group of this type will be expressed as C_p.

Theorem
Every group of prime order is simple.

Proof. Let G be a group such that $|G| = p$ with p a prime number. Then G is cyclic. Let H be a subgroup of G. By Lagrange's Theorem, $|H|$ divides $|G|$ so that $|H|$ divides p. Then $|H| = 1$ or $|H| = p$ implying $H = \{e\}$ or $H = G$. Therefore, G has no proper normal subgroups and must be simple.

Cyclic groups of this type are the only "simple" simple groups. Their internal structures are orderly and predictable. Also, this class of simple groups is unique among the others for the following properties they satisfy. Cyclic groups of prime order are the only simple groups with odd order. Consequently, they are the only simple groups which are solvable. Below is a theorem which explains the last of their special attributes.

Theorem
The only simple abelian groups are the cyclic groups of prime order.

Proof. Let G be an abelian simple group with $|G| > 1$. Then there exists $g \in G$ with $g \neq e$. Let $H = [g]$. Now $G = H$ since any subgroup of an abelian group is normal. Hence, G is a cyclic group. Assume the order of G is composite. That is, $|G| = n$ where $n = mp$ for some prime p. Then

$e = g^n = g^{mp} = (g^m)p$. Let $K = [g^m]$. It follows that $|K| = p < n$. Thus, K is a proper normal subgroup of G. This contradicts G being simple. Therefore, G is a cyclic group of prime order.

Clearly, alternating groups, groups of Lie type, and sporadic groups do not satisfy the commutative property.

Alternating Groups

Alternating subgroups of symmetric groups are the second most familiar category of simple groups after the well known cyclic groups of prime order. They are defined as follows.

Definition

For every positive integer n, the group S_n of all the permutations on $X_n = \{1, 2, \ldots, n\}$ is called the symmetric group on X_n. The **alternating group**, denoted by A_n, is the set of all even permutations in S_n.

Theorem

If $n \geq 5$, then A_n is a simple group.

For a proof of this theorem using conjugates and centralizers see [17, pp. 44-46].

A few comments concerning this theorem are in order. The groups $A_1 = \{(1)\}$ and $A_2 = \{(1)\}$, both the trivial identity group, are not simple. But simplicity is found in $A_3 = \{(1), (123), (132)\}$ since it is isomorphic to C_3. The group A_4 is not simple. It has $N = \{(1), (12)(34), (13)(24), (14)(23)\}$ as a proper normal subgroup. So the above theorem is not entirely accurate. Justification for stating it in this form, however, can be given. When $n \geq 5$, the A_n have similar nonabelian structures causing them to

form a family of simple groups. If $1 \leq n \leq 4$, the A_n are inconsequential, for their random natures force either multiple representation or nonsimplicity.

Since $|S_n| = n!$ implies $|A_n| = n!/2$, these alternating groups are inordinately large. This is attributable to the rapidly increasing values of factorials. But the group A_5, possessing 60 elements, is the smallest nonabelian simple group.

Symmetric groups and their corresponding alternating subgroups are important to the concept of solvability and its connection to simplicity. This will be covered more fully in chapter five.

Groups of Lie Type

Groups of Lie type, unlike other simple groups, possess appealing algebraic structures. The sixteen infinite families of groups under the Lie label originate from what are called Lie groups. Sophus Lie, a Norwegian mathematician, developed Lie groups in an effort ". . . to explain why certain elementary differential equations could be solved, whereas others could not be" [20, p. 205]. Each Lie group is infinite and can be represented by matrices whose entries are taken from the field of complex numbers. Due to this fact, several Lie groups are equivalent to the classical matrix groups. These are the linear groups A_n, the symplectic groups C_n, and the orthogonal groups B_n and D_n. They comprise four infinite families of Lie groups. Five exceptional Lie groups G_2, F_4, E_6, E_7, and E_8, which

possess no classical analogues, complete the list. It is customary for simple group theorists to use the same notation for the alternating groups and the linear Lie groups. Generally, the context will determine which type of group is being discussed.

Lie groups are not simple but have finite versions, called groups of Lie type, which are simple. Groups of Lie type exist as derivatives of their corresponding parent Lie groups by using matrices over finite fields. So there is a key difference between Lie groups and groups of Lie type apparent amid the confusing terminology. The former are infinite groups over the complex field, while the latter are finite simple groups over finite fields.

A method will be given below for constructing the simple groups of Lie type corresponding to the linear family A_n. Throughout this discussion, GF(q) will represent a finite field with q elements. A basic theorem about finite fields forces q to have the form p^m where p is a prime number and m is a positive integer.

Definition

The **general linear group** GL(n,q) is the multiplicative group of all nonsingular n x n matrices over GF(q).

Recall that a matrix having an inverse is said to be nonsingular. Furthermore, it can be shown that $|GL(n,q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$.

Definition

The **special linear group** SL(n,q) is the multiplicative group of n x n matrices over GF(q) having determinant 1.

Unless $n = 2$ and $q \leq 3$, SL(n,q) is the commutator

subgroup of GL(n,q). Let Z_0 denote the center of SL(n,q). Then Z_0 consists of the group of scalar matrices, that is, each scalar $k \in GF(q)$ with $k^n = 1$ is multiplied by the identity matrix to form elements in Z_0. Also, $|Z_0| = d$ where d is the greatest common divisor of n and q - 1. It will be expressed throughout the rest of this paper as gcd(n,q-1).

Definition

The **projective linear group** PSL(n,q) is the group $SL(n,q)/Z_0$.

It can be demonstrated that if d = gcd(n,q-1),

then $$|PSL(n,q)| = \frac{(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})}{d(q-1)}.$$

Simplifying gives $$|PSL(n,q)| = 1/d\ q^{n(n-1)/2} \prod_{i=2}^{n}(q^i - 1).$$

Except when n = 2 and $q \leq 3$, PSL(n,q) is simple for all $n \geq 2$. It is also the finite analogue of the Lie group family A_m for m = n - 1.

What follows is an elementary example of the group PSL(2,3). Although it is not simple, it provides insight into the structure of these groups.

To begin, it is necessary to define the finite field from which all subsequent matrices will be composed.

GF(3)

$Z_3 = \{0, 1, 2\}$

There are $3^4 = 81$ 2 x 2 matrices constructable in Z_3, but only $|GL(2,3)| = (3^2 - 1)(3^2 - 3) = 48$ of them possess

an inverse or, equivalently, have a nonzero determinant. Moreover, the reader should remember that addition and multiplication are performed using modular arithmetic.

GL(2,3)

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\ \begin{bmatrix}0&1\\1&0\end{bmatrix},\ \begin{bmatrix}2&0\\0&2\end{bmatrix},\ \begin{bmatrix}0&2\\2&0\end{bmatrix},\ \begin{bmatrix}1&1\\1&0\end{bmatrix},\ \begin{bmatrix}1&1\\0&1\end{bmatrix},\ \begin{bmatrix}0&1\\1&1\end{bmatrix},\ \begin{bmatrix}1&0\\1&1\end{bmatrix},$$

$$\begin{bmatrix}1&1\\1&2\end{bmatrix},\ \begin{bmatrix}1&1\\2&1\end{bmatrix},\ \begin{bmatrix}2&1\\1&1\end{bmatrix},\ \begin{bmatrix}1&2\\1&1\end{bmatrix},\ \begin{bmatrix}2&2\\2&0\end{bmatrix},\ \begin{bmatrix}2&2\\0&2\end{bmatrix},\ \begin{bmatrix}0&2\\2&2\end{bmatrix},\ \begin{bmatrix}2&0\\2&2\end{bmatrix},$$

$$\begin{bmatrix}2&2\\2&1\end{bmatrix},\ \begin{bmatrix}2&2\\1&2\end{bmatrix},\ \begin{bmatrix}1&2\\2&2\end{bmatrix},\ \begin{bmatrix}2&1\\2&2\end{bmatrix},\ \begin{bmatrix}0&1\\1&2\end{bmatrix},\ \begin{bmatrix}0&1\\2&1\end{bmatrix},\ \begin{bmatrix}0&1\\2&0\end{bmatrix},\ \begin{bmatrix}0&1\\2&2\end{bmatrix},$$

$$\begin{bmatrix}1&0\\1&2\end{bmatrix},\ \begin{bmatrix}1&0\\2&1\end{bmatrix},\ \begin{bmatrix}1&0\\0&2\end{bmatrix},\ \begin{bmatrix}1&0\\2&2\end{bmatrix},\ \begin{bmatrix}1&2\\0&1\end{bmatrix},\ \begin{bmatrix}1&2\\1&0\end{bmatrix},\ \begin{bmatrix}1&2\\0&2\end{bmatrix},\ \begin{bmatrix}1&2\\2&0\end{bmatrix},$$

$$\begin{bmatrix}2&1\\0&1\end{bmatrix},\ \begin{bmatrix}2&1\\1&0\end{bmatrix},\ \begin{bmatrix}2&1\\0&2\end{bmatrix},\ \begin{bmatrix}2&1\\2&0\end{bmatrix},\ \begin{bmatrix}0&2\\1&2\end{bmatrix},\ \begin{bmatrix}0&2\\2&1\end{bmatrix},\ \begin{bmatrix}0&2\\1&0\end{bmatrix},\ \begin{bmatrix}0&2\\1&1\end{bmatrix},$$

$$\begin{bmatrix}2&0\\1&2\end{bmatrix},\ \begin{bmatrix}2&0\\2&1\end{bmatrix},\ \begin{bmatrix}2&0\\0&1\end{bmatrix},\ \begin{bmatrix}2&0\\1&1\end{bmatrix},\ \begin{bmatrix}1&1\\0&2\end{bmatrix},\ \begin{bmatrix}1&1\\2&0\end{bmatrix},\ \begin{bmatrix}2&2\\0&1\end{bmatrix},\ \begin{bmatrix}2&2\\1&0\end{bmatrix}$$

Now collect those matrices in GL(2,3) that have determinant 1 and form the group below.

SL(2,3)

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\ \begin{bmatrix}2&0\\0&2\end{bmatrix},\ \begin{bmatrix}1&1\\0&1\end{bmatrix},\ \begin{bmatrix}1&0\\1&1\end{bmatrix},\ \begin{bmatrix}2&2\\0&2\end{bmatrix},\ \begin{bmatrix}2&0\\2&2\end{bmatrix},\ \begin{bmatrix}2&2\\2&1\end{bmatrix},\ \begin{bmatrix}1&2\\2&2\end{bmatrix},$$

$$\begin{bmatrix}1&1\\1&2\end{bmatrix},\ \begin{bmatrix}2&1\\1&1\end{bmatrix},\ \begin{bmatrix}1&0\\2&1\end{bmatrix},\ \begin{bmatrix}0&1\\2&1\end{bmatrix},\ \begin{bmatrix}0&1\\2&0\end{bmatrix},\ \begin{bmatrix}0&1\\2&2\end{bmatrix},\ \begin{bmatrix}2&0\\1&2\end{bmatrix},\ \begin{bmatrix}0&2\\1&2\end{bmatrix},$$

$$\begin{bmatrix}0&2\\1&0\end{bmatrix},\ \begin{bmatrix}0&2\\1&1\end{bmatrix},\ \begin{bmatrix}1&2\\1&0\end{bmatrix},\ \begin{bmatrix}1&2\\0&1\end{bmatrix},\ \begin{bmatrix}2&1\\2&0\end{bmatrix},\ \begin{bmatrix}2&1\\0&2\end{bmatrix},\ \begin{bmatrix}1&1\\2&0\end{bmatrix},\ \begin{bmatrix}2&2\\1&0\end{bmatrix},$$

The center of SL(2,3) is needed next and will contain two elements since $|Z_0| = \gcd(2,2) = 2$.

Z_0

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\ \begin{bmatrix}2&0\\0&2\end{bmatrix}$$

The simple group that is being built as a factor group, PSL(2,3), will now be represented. It can be shown to have twelve elements, each one of which is a coset.

PSL(2,3)

$$\begin{bmatrix}1&0\\0&1\end{bmatrix}Z_0 = \begin{bmatrix}2&0\\0&2\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}2&0\\0&2\end{bmatrix}\right\} \quad (\text{order} = 1)$$

$$\begin{bmatrix}2&2\\2&1\end{bmatrix}Z_0 = \begin{bmatrix}1&1\\1&2\end{bmatrix}Z_0 = \left\{\begin{bmatrix}2&2\\2&1\end{bmatrix}, \begin{bmatrix}1&1\\1&2\end{bmatrix}\right\} \quad (\text{order} = 2)$$

$$\begin{bmatrix}1&2\\2&2\end{bmatrix}Z_0 = \begin{bmatrix}2&1\\1&1\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&2\\2&2\end{bmatrix}, \begin{bmatrix}2&1\\1&1\end{bmatrix}\right\} \quad (\text{order} = 2)$$

$$\begin{bmatrix}0&1\\2&0\end{bmatrix}Z_0 = \begin{bmatrix}0&2\\1&0\end{bmatrix}Z_0 = \left\{\begin{bmatrix}0&1\\2&0\end{bmatrix}, \begin{bmatrix}0&2\\1&0\end{bmatrix}\right\} \quad (\text{order} = 2)$$

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}Z_0 = \begin{bmatrix}2&2\\0&2\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&1\\0&1\end{bmatrix}, \begin{bmatrix}2&2\\0&2\end{bmatrix}\right\} \quad (\text{order} = 3)$$

$$\begin{bmatrix}1&0\\1&1\end{bmatrix}Z_0 = \begin{bmatrix}2&0\\2&2\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&0\\1&1\end{bmatrix}, \begin{bmatrix}2&0\\2&2\end{bmatrix}\right\} \quad (\text{order} = 3)$$

$$\begin{bmatrix}1&0\\2&1\end{bmatrix}Z_0 = \begin{bmatrix}2&0\\1&2\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&0\\2&1\end{bmatrix}, \begin{bmatrix}2&0\\1&2\end{bmatrix}\right\} \quad (\text{order} = 3)$$

$$\begin{bmatrix}0&1\\2&1\end{bmatrix}Z_0 = \begin{bmatrix}0&2\\1&2\end{bmatrix}Z_0 = \left\{\begin{bmatrix}0&1\\2&1\end{bmatrix}, \begin{bmatrix}0&2\\1&2\end{bmatrix}\right\} \quad (\text{order} = 3)$$

$$\begin{bmatrix}0&1\\2&2\end{bmatrix}Z_0 = \begin{bmatrix}0&2\\1&1\end{bmatrix}Z_0 = \left\{\begin{bmatrix}0&1\\2&2\end{bmatrix}, \begin{bmatrix}0&2\\1&1\end{bmatrix}\right\} \quad (\text{order} = 3)$$

$$\begin{bmatrix}1&2\\1&0\end{bmatrix}Z_0 = \begin{bmatrix}2&1\\2&0\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&2\\1&0\end{bmatrix}, \begin{bmatrix}2&1\\2&0\end{bmatrix}\right\} \quad (\text{order} = 3)$$

$$\begin{bmatrix}1&2\\0&1\end{bmatrix}Z_0 = \begin{bmatrix}2&1\\0&2\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&2\\0&1\end{bmatrix}, \begin{bmatrix}2&1\\0&2\end{bmatrix}\right\} \quad (\text{order} = 3)$$

$$\begin{bmatrix}1&1\\2&0\end{bmatrix}Z_0 = \begin{bmatrix}2&2\\1&0\end{bmatrix}Z_0 = \left\{\begin{bmatrix}1&1\\2&0\end{bmatrix}, \begin{bmatrix}2&2\\1&0\end{bmatrix}\right\} \quad (\text{order} = 3)$$

Using the formula $(aZ_0)(bZ_0) = (ab)Z_0$ for the product of cosets, it is possible to find the order of each element in PSL(2,3). These orders are specified next to the elements listed above. Now there exist five nonisomorphic

groups of order twelve which are $C_{12} = C_3 \times C_4$, $C_6 \times C_2$, the dihedral group D_6, the quaternion group Q_6, and the alternating group A_4. Since A_4 is the only one of the five that contains eight elements of order three, PSL(2,3) must be isomorphic to A_4.

For all of the classical Lie groups, the procedure exposed here of finding the commutator subgroup G^* then obtaining the center C of G^* yields a family of simple groups G^*/C most of the time [16, p. 696]. This gives, however, only five families of simple groups of Lie type which include the linear groups $A_n(q)$; the symplectic groups $C_n(q)$; the orthogonal groups $B_n(q)$, $D_n(q)$, and ${}^2D_n(q)$; and the unitary groups ${}^2A_n(q)$.

The remaining simple groups of Lie type are also derived from the Lie groups but necessitate an application of modified techniques. This was done by Claude Chevalley, and his procedures produced most of the previously described classical groups along with several original families correlating to the exceptional Lie groups. These newer simple groups of Lie type are denoted by $G_2(q)$, $F_4(q)$, $E_6(q)$, $E_7(q)$, and $E_8(q)$. Accuracy demands, however, that Leonard Dickson be given credit for his independent construction of $G_2(q)$ and $E_6(q)$ before Chevalley. Variations on Chevalley's work by Robert Steinberg produced the simple families ${}^3D_4(q)$ and ${}^2E_6(q)$. In 1960 Michio Suzuki constructed a family of simple groups outside the realm of general Lie theory and at first believed it was sporadic. Later Rimhak Ree

demonstrated that when n is odd and $q = 2^n$, 3^n, and 2^n, respectively, the three simple families $B_2(2^n)$, $G_2(3^n)$, and $F_4(2^n)$ acquire extra characteristics not explainable by Lie theory. He used this knowledge to construct the last three families of simple groups of Lie type: ${}^2B_2(2^n)$, ${}^2G_2(3^n)$, and ${}^2F_4(2^n)$ of which ${}^2B_2(2^n)$ was the group disclosed by Suzuki. Important information concerning the simple groups of Lie type is summarized in Table I - page 22. It is borrowed from [16, p. 708].

Table I. Simple Groups of Lie Type*

Lie Notation	Name or Discoverer	Order	d
$A_{n-1}(q)$	PSL(n,q) ($n\geq 2$)	$1/d\ q^{n(n-1)/2} \prod_{i=2}^{n}(q^i-1)$	$\gcd(n,q-1)$
${}^2A_{n-1}(q)$	PSU(n,q) ($n\geq 3$)	$1/d\ q^{n(n-1)/2} \prod_{i=2}^{n}(q^i-(-1)^i)$	$\gcd(n,q+1)$
$C_n(q)$	PSp(2n,q) ($n\geq 2$)	$1/d\ q^{n^2} \prod_{i=1}^{n}(q^{2i}-1)$	$\gcd(2,q-1)$
$B_n(q)$	PSO(2n+1,q) ($n\geq 3$)	$1/d\ q^{n^2} \prod_{i=1}^{n}(q^{2i}-1)$	$\gcd(2,q-1)$
$D_n(q)$	PSO(2n,q,+) ($n\geq 4$)	$1/d\ q^{n(n-1)}(q^n-1) \prod_{i=1}^{n-1}(q^{2i}-1)$	$\gcd(4,q^n-1)$
${}^2D_n(q)$	PSO(2n,q,-) ($n\geq 4$)	$1/d\ q^{n(n-1)}(q^n+1) \prod_{i=1}^{n-1}(q^{2i}-1)$	$\gcd(4,q^n+1)$
${}^3D_4(q)$	Steinberg	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	
$G_2(q)$	Dickson	$q^6(q^6-1)(q^2-1)$	
$F_4(q)$	Chevalley	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	
$E_6(q)$	Dickson	$1/d\ q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$	$\gcd(3,q-1)$
${}^2E_6(q)$	Steinberg	$1/d\ q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$	$\gcd(3,q+1)$
$E_7(q)$	Chevalley	$\prod 1/d\ q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$**	$\gcd(2,q-1)$
$E_8(q)$	Chevalley	$\prod q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$**	
${}^2B_2(q)$	Suzuki ($q=2^{2n+1}$)	$q^2(q^2+1)(q-1)$	
${}^2G_2(q)$	Ree ($q=3^{2n+1}$)	$q^3(q^3+1)(q-1)$	
${}^2F_4(q)$	Ree ($q=2^{2n+1}$)	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	

* Here q is an arbitrary power of an arbitrary prime unless otherwise specified.
** The symbol $\prod$, without indices, means to find the product of all quantities after it.

All groups above are nonabelian simple groups except:
(a) PSL(2,2), PSL(2,3), PSU(3,2), and ${}^2B_2(2)$ are solvable.
(b) PSp(4,2), $G_2(2)$, and ${}^2F_4(2)$ all have a simple commutator subgroup of index two.
(c) ${}^2G_2(3)$ has a simple commutator subgroup of index three.

It is worthwhile to pause and observe an interesting fact apparent in the above table. Although $C_n(q)$ and $B_n(q)$ are distinct families, their order formulas are identical. In other words, for $n \geq 3$ and $q \neq 2^a$, the corresponding groups in $C_n(q)$ and $B_n(q)$ possess the same order but are not isomorphic. This situation proves an important theorem about simple groups: that there exist infinitely many nonisomorphic simple groups having the same number of elements.

Since there are only twenty-six sporadic groups and one infinite family each of the cyclic and alternating groups, the sixteen infinite families of groups of Lie type dominate the simple groups. Consequently, the most common simple group is a group of Lie type.

Sporadic Groups

There is nothing of a general nature to be stated about sporadic groups. They are sometimes characterized as ". . . the simple groups which are neither of prime order, nor alternating groups, nor of Lie type" [3, p. 24]. William Burnside was the first individual to refer to them as sporadic (see [4, p. 504]). The twenty-six groups in this category have dissimilar structures causing the collection to resemble a miscellaneous account. Hence, no single definition can be furnished to explain their existence. Some collections of two or three sporadic groups originate out of a single context. For example, the three Conway sporadic groups .1, .2, and .3 were discovered from

the 24-dimensional Leech lattice. Yet this occasional bonding is not enough to overcome the fact that each one is a distinct type of simple group.

Sophisticated characterizations of the sporadic groups, although beyond the scope of this paper, consist of describing each one of them individually (see [11, pp. 78-134]). Uncomplex examples are furnished by the Mathieu groups M_{11} and M_{12} which are represented next as permutation groups.

Let A, B, and C be the following permutations:
A = (1 2 3 4 5 6 7 8 9 10 11)
B = (5 6 4 10)(11 8 3 7)
C = (1 12)(2 11)(3 6)(4 8)(5 9)(7 10).

Then $M_{11} = \langle A,B \rangle$ and $M_{12} = \langle A,B,C \rangle$. [11, p. 79]

Here $\langle A,B \rangle$ is the subgroup of S_{11} generated by the permutations A and B, and $\langle A,B,C \rangle$ is the subgroup of S_{12} generated by the permutations A, B, and C. It should be mentioned that other descriptions of the Mathieu groups exist, and this multirepresentation is typical of most sporadic groups. In the following table, each sporadic group is listed along with its order, original founder, and approximate year of discovery. In those instances where the efforts of several mathematicians were required for discovery, the group was named after the individual who found the initial evidence for the group. The years provided in the table are not publication dates, but are actual discovery dates again based on the initial evidence concept. They are borrowed from a journal article written by Arunas Rudvalis [16, p. 709], the discoverer of the

sporadic group Ru, who can be considered a reliable source for this information.

Table II. Sporadic Simple Groups

Name	Order	Discoverer	Date
M_{11}	7,920	Emile Mathieu	1861
M_{12}	95,040	Emile Mathieu	1861
M_{22}	443,520	Emile Mathieu	1873
M_{23}	10,200,960	Emile Mathieu	1873
M_{24}	244,823,040	Emile Mathieu	1873
J_1	175,560	Zvonimir Janko	1965
J_2	604,800	Zvonimir Janko	1967
J_3	50,232,960	Zvonimir Janko	1968
J_4	$\sim 8.7 \times 10^{19}$	Zvonimir Janko	1975
HS	44,352,000	Donald Higman, Charles Sims	1967
Mc	898,128,000	John McLaughlin	1968
Suz	$\sim 4.5 \times 10^{11}$	Michio Suzuki	1968
Ru	$\sim 1.5 \times 10^{11}$	Arunas Rudvalis	1972
He	$\sim 4 \times 10^{9}$	Dieter Held	1968
Ly	$\sim 5 \times 10^{16}$	Richard Lyons	1970
ON	$\sim 4.6 \times 10^{11}$	Michael O'Nan	1973
.1	$\sim 4 \times 10^{18}$	John Conway	1968
.2	$\sim 4 \times 10^{13}$	John Conway	1968
.3	$\sim 5 \times 10^{11}$	John Conway	1968
M(22)	$\sim 6.5 \times 10^{13}$	Bernd Fischer	1969
M(23)	$\sim 4 \times 10^{18}$	Bernd Fischer	1969
M(24)′ *	$\sim 1.3 \times 10^{24}$	Bernd Fischer	1969
F_1	$\sim 8 \times 10^{53}$	Bernd Fischer, Robert Griess	1974
F_2	$\sim 4 \times 10^{33}$	Bernd Fischer	1973
F_3	$\sim 9 \times 10^{16}$	John Thompson	1974
F_5	$\sim 2.7 \times 10^{14}$	Koichiro Harada	1974

*M(24)′ is the commutator subgroup of index 2 in M(24).

An examination of the table reveals that overall, the orders of sporadic groups are large. The smallest one is M_{11} which has 7,920 elements. Occupying the opposite end of the size continuum is the group F_1 whose order is approximately 10^{54}. Due to its massive size, it was originally named the "monster." The next largest group F_2, having order of roughly 10^{33}, was also initially called a

jesting name, that of "baby monster."

This size issue contributed to the problematic discovery of sporadic groups. The techniques available to study simple groups, before the famous Feit-Thompson paper, were only effective for small groups. Hence, before new sporadic groups could be discovered, new methods had to be developed. In addition, since each sporadic group is unlike any of the others, discovery of one did not imply discovery of all. Every group was an individual project. A comparison with the other types of simple groups highlights this problem. The cyclic groups, alternating groups, and groups of Lie type form eighteen families of simple groups. Even though there exist infinitely many groups in each family, there are also small ones to examine from which properties and patterns for the whole set can be inferred. At this time, the sporadic groups do not exhibit any kind of family structure. Instead, they are a random set of unrelated groups collected together under the label sporadic.

It is interesting to examine the literature published in the early 1970s. Doubt as to whether there was a finite or infinite number of sporadic groups is prevalent. Mathematicians were concerned that a new, unpredictable, and irregular family of simple groups was unfolding which could defy description. Such a situation would have halted the whole classification project. Again Richard Brauer aptly described this climate when he stated ". . . it is quite possible that we have an infinite sequence $\{G_n\}$ with the

orders $|G_n|$ strictly increasing and that infinitely often, entirely new types of groups occur in our sequence (or, as some people say, new 'monsters' appear)" [3, p. 22-23]. This suspicion, of course, turned out to be false since only twenty-six sporadic groups have been proven to exist.

Necessity of computer assistance further emphasizes the complications involved in sporadic group disclosure. The groups J_3, J_4, He, Ly, ON, F_2, F_3, F_5, and Ru required computer calculations to establish their existence. A mathematician named Charles Sims was a key figure in evolving computer algorithms capable of constructing groups, and shares responsibility for the existence of Ly, ON, and F_2. Currently, however, only the three groups Ly, ON, and J_4 depend on the computer for their livelihood. During the past several years, hand constructions have been derived for the others. This is due in part to the noncomputer construction of the "monster" by Robert Griess as "a group of rotations of a symmetric object in a space of 196,883 dimensions" [7]. Since a number of the twenty-six sporadic groups are known to be embedded one way or another in F_1, their constructions follow easily from Griess' work. It is remarkable that a group so large could be built by hand when much smaller groups required computer aid. This accomplishment stimulated Griess to rename F_1 the "friendly giant."

Connections between certain sporadic groups and groups of Lie type have been uncovered. Others, specifically the

Mathieu groups M_{23} and M_{24}, are related to codes used in reconstructing messages distorted by noise. A majority of the twenty-six sporadic groups are embedded in the group F_1, Conway's group .1, or both. These observations imply that sporadic groups may not be as random as they appear. An undetected family structure might exist causing these mysterious tricksters to one day yield a unifying common denominator.

Chapter IV

THE IMPORTANCE OF FINITE SIMPLE GROUPS

This chapter will demonstrate the significance of simple groups in addition to showing the fundamental position they occupy in the whole spectrum of group theory. The recent flurry of research activity has not been theoretical playtime. Simple groups are important. They are the fundamental particles of groups, and this fact will be substantiated below. Finite groups will be divided into two categories for examination: those that are abelian and those that lack the commutative property. This division is necessary since each case entails unique and notable features.

Finite Abelian Groups

Knowing that a group is abelian simplifies the investigation of properties in question. Even though it lacks generalization potential, it is often best to start with the specific. Before giving the major theorems, two introductory definitions are needed.

Definition

Let p be a prime number. A group G is a **p-group** in case every element in G has order a power of p.

Definition

A **primary cyclic group** is a cyclic group of order p^n with p a prime number and $n \geq 1$.

Primary cyclic groups are merely cyclic p-groups singled out for special emphasis. Undoubtedly, they are crucial to this section. The connection between simple

groups and finite abelian groups will be presented in an important theorem known as the Fundamental Theorem of Finite Abelian Groups. Understanding its meaning and proof, however, requires some preparatory work.

Theorem

If G is an abelian group of order $p_1^{k1}p_2^{k2}\cdots p_r^{kr}$ where, for $i = 1,\ldots,r$, each k_i is a positive integer and each p_i is a prime number, then G is the direct product of p-groups.

Proof. The internal direct product theorem forms the basis for this proof. For $1 \leq i \leq r$, define $G_{pi} = \{x \in G : \text{order of } x \text{ is a power of } p_i\}$. Each p-group G_{pi} is a normal subgroup of G since it is a nonempty and closed subset of the abelian group G.

I. Show $G = G_{p1}G_{p2}\cdots G_{pr}$.

Let $g \in G$ with $g \neq e$ and let the order of g be n. Since n divides $|G|$, $n = p_1^{j1}p_2^{j2}\cdots p_r^{jr}$ where $0 \leq j_i \leq k_i$ for $1 \leq i \leq r$. Let $n_i = n/p_i^{j_i}$ for $1 \leq i \leq r$. Then $\gcd(n_1,n_2,\ldots,n_r) = 1$. So there exist integers m_i such that $n_1m_1 + n_2m_2 + \cdots + n_rm_r = 1$. This gives,

$$g = g^1 = g^{(n_1m_1 + n_2m_2 + \cdots + n_rm_r)} = g^{n_1m_1}g^{n_2m_2}\cdots g^{n_rm_r}.$$

Examination of the general term $g^{n_im_i}$ reveals that

$$\left(g^{n_im_i}\right)^{p_i^{j_i}} = \left(g^{n_ip_i^{j_i}m_i}\right) = g^{nm_i} = (g^n)^{m_i} = e^{m_i} = e.$$

Hence, $g^{n_im_i}$ has order a power of the prime p_i which means $g^{n_im_i} \in G_{pi}$ for $1 \leq i \leq r$. Therefore, $G = G_{p1}G_{p2}\cdots G_{pr}$.

II. Show $G_{pi} \cap (G_{p1}G_{p2}\cdots G_{p(i-1)}G_{p(i+1)}\cdots G_{pr}) = \{e\}$.

Let $x \in G_{pi} \cap (G_{p1}G_{p2}\cdots G_{p(i-1)}G_{p(i+1)}\cdots G_{pr})$. Then $x \in G_{pi}$ and $x \in G_{p1}G_{p2}\cdots G_{p(i-1)}G_{p(i+1)}\cdots G_{pr}$. It follows

that $x^{pi^a} = e$ for some a. At the same time, for $1 \leq j \leq r$ and $j \neq i$, $x = \Pi x_j$ with $x_j \in G_{pj}$ and $x_j^{pj^{tj}} = e$ for positive integers tj. Let $s = \Pi pj^{tj}$ for $1 \leq j \leq r$ and $j \neq i$. Then $x^s = (\Pi x_j)^s = e$. Since $\gcd(pi^a, s) = 1$, there exist integers c and d such that $pi^a c + sd = 1$. Thus,

$$x = x^1 = x^{(pi^a c + sd)} = \left(x^{pi^a}\right)^c (x^s)^d = e^c e^d = e.$$

Therefore, $G_{pi} \cap (G_{p1} G_{p2} \cdots G_{p(i-1)} G_{p(i+1)} \cdots G_{pr}) = \{e\}$. Since the hypothesis of the internal direct product have been satisfied, it can be concluded that $G = G_{p1} \times G_{p2} \times \cdots \times G_{pr}$.

It is seen that any finite abelian group G can be factored into the direct product of p-groups unless G itself is already a p-group. The prime numbers around which these p-groups are constructed are those that divide the order of G. Since e may be the only element in G having order a power of the prime p, that is, $|e| = p^0 = 1$, a p-group can be the identity group. The term factored is intended throughout this chapter to have the group theory meaning of direct product not the customary connotation of factoring a number. An example will clarify the technicalities of the p-group theorem.

Let $C_{12} = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}$.

order	1	12	6	4	3	12	2	12	3	4	6	12

Since $12 = 2^2 3$, only two p-groups can be formed. They are $G_2 = \{e, a^3, a^6, a^9\}$ and $G_3 = \{e, a^4, a^8\}$. According to the theorem, $C_{12} = G_2 \times G_3$.

This illustration emphasizes the fact that not all elements in a group G need necessarily belong to a p-group. It is as if the elements in G pass through p-group filters with some being selected for emphasis and others being discarded. The special elements, bonded together by the common prime they share, are assembled into p-groups. Those that are rejected have composite order and can be generated by elements in the various p-groups. At this point it may be unclear as to why the emphasis has been placed on p-groups when the goal is to arrive at a factorization of G into primary cyclic groups. Going directly to the primary cyclic groups is more difficult than arriving at them through p-groups. Conceptually, the elements of G are filtered in two stages: first into p-groups and then the p-groups divided into primary cyclic groups. Preparation for the major theorem of this section is now complete.

Fundamental Theorem of Finite Abelian Groups
Every finite abelian group is a direct product of primary cyclic subgroups.

Proof. Due to the previous theorem, it is sufficient to consider p-groups only. Let M be a p-group and let $a \in M$ such that the order of a, denoted p^m, is maximal. The group $A = [a]$ is cyclic with $|A| = p^m$. Also, let $b \in M$ with b not in A and define $B = [b]$. Since $b \notin A$, $B \cap A = \{e\}$. The group B is normal in M so M/B is a group with the coset aB as an element.

I. Show the order of aB is equal to the order of a.

Let z = order of aB. Since the order of a is p^m, $(aB)^{p^m} = (a^{p^m})(B^{p^m}) = (a^{p^m})B = eB = B$. Thus z divides p^m. Also, since $a \in aB$ and $(aB)^z = B$, then $a^z \in B$. But a to any power belongs to A. Hence, $a^z \in A \cap B = \{e\}$ which implies that $a^z = e$. But p^m is the smallest positive integer for which this relationship holds for a. Thus p^m divides z. Therefore, $z = p^m$, which means the order of aB is equal to the order of a. From this it can be concluded that aB is of maximal order in M/B and [aB] generates a cyclic group.

II. Show M is the direct product of primary cyclic subgroups.

The proof will be completed by induction on n, where $|M| = p^n$. If n = 1, M is cyclic of prime order. Assume the hypothesis is true if $|M| = p^k$ with $k < n$. When $|M| = p^n$, the order of $M/B < p^n$. So the induction hypothesis applies to M/B giving M/B = [aB] x T where T is a subgroup of M/B. Since B is normal in M, the natural map from M to M/B can be formed. By the correspondence theorem, there exists a subgroup Q of M such that $Q \longrightarrow Q/B = T$. Also due to previous work, A is mapped to [aB]. Therefore, M = A x Q where Q is the direct product of primary cyclic groups by the induction hypothesis.

Although this theorem yields an astonishing result, that any finite abelian group can be represented as the direct product of primary cyclic groups, it does not address the issue of uniqueness. Are there several ways to factor

an abelian group or just one? It is implied by the theorem that if G is a primary cyclic group of order p^n with $n \geq 1$, such as C_8, it cannot be factored. All other finite abelian groups can be factored in only one way as the following theorem indicates.

Theorem

If a finite abelian group G is the direct product of primary cyclic groups in two ways, $G = A_1 \times A_2 \times \cdots \times A_r = B_1 \times B_2 \times \cdots \times B_s$, then the number of factors is the same in both cases, $r = s$, and the orders of $A_1, \ldots, A_r$ are the same as those of $B_1, \ldots, B_s$ in some arrangement.

At this time it is worthwhile to reintroduce the correspondence between simple groups and prime numbers with a fact from number theory. It has a striking resemblance to the topics currently under investigation.

Fundamental Theorem of Arithmetic I

Every positive integer $n > 1$ can be written as $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where, for $i = 1, 2, \ldots, r$, each a_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$. If n has two representations, $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$, then $r = s$, and the $p_i^{a_i}$ are the same as the $q_j^{b_j}$ except, possibly, for their order of appearance.

Now the technicalities of procedure will be addressed. A common method used to find the unique factorization of a group G is based on the following concept. If an abelian group G is not a primary cyclic group and N is a normal subgroup of G, then $G = N \times G/N$. This is derived from the fact that G contains a subgroup isomorphic to G/N. Factoring the group C_6 will demonstrate this technique.

Let $C_6 = \{e, a, a^2, a^3, a^4, a^5\}$.

Let $N = \{e, a^3\} \sim C_2$.

Then $G/N = \begin{matrix} N = \{e, a^3\} \\ aN = \{a, a^4\} \\ a^2N = \{a^2, a^5\} \end{matrix} \sim C_3$.

So that $C_6 = C_2 \times C_3$.

The group C_{30} serves as a second example. It has a normal subgroup C_2, and performing the above process obtains $C_{30} = C_2 \times C_{15}$. Repeating the procedure on C_{15} yields $C_{30} = C_2 \times C_3 \times C_5$ as the final factorization of C_{30} into primary cyclic groups. Depending on which normal subgroup of C_{30} was initially selected, the first factoring stage could produce $C_{30} = C_2 \times C_{15} = C_5 \times C_6 = C_3 \times C_{10}$ as three ways to write C_{30} as a direct product. They are not, however, factorizations which satisfy the primary cyclic group standard. This criterion is what connects the Fundamental Theorem of Finite Abelian Groups to the topic of this paper: finite simple groups. If all finite commutative groups could be written as the direct product of simple groups, then the analogy between prime numbers and simple groups would be complete. This is not the case, however, and the factorization $C_{40} = C_5 \times C_8$ serves as a counterexample. Primary cyclic groups of order p^n are the problem. When $n = 1$ they are simple, but if $n > 1$, they are not. Therefore, only some finite abelian groups factor into the direct product of simple groups. A stronger assertion is impossible, and this leaves the sought after analogy between prime numbers and simple groups in a state of

imperfection. Finite nonabelian groups will be enlisted to resolve these difficulties.

Finite Nonabelian Groups

As alluded to earlier, the goal is to establish a theory for finite groups analogous to the Fundamental Theorem of Arithmetic which utilizes simple groups as basic building blocks. Exploring finite abelian groups produced results towards this end, but limitations prevented an absolute correspondence. It is desired to replace this slight similarity with something more concrete. Properties possessed by finite nonabelian groups, when the commutative property is not under assumption, will accomplish this objective.

If factoring a finite group into simple groups is not always guaranteed, then it is best to abandon this concept and examine the problem from a different perspective. Granted, the Fundamental Theorem of Arithmetic states that any positive integer greater than one can be factored into a product of prime powers uniquely. The emphasis of this theory, however, is on factoring. It can be restated in an equivalent form which shifts the focus from factoring to collections of prime numbers.

Fundamental Theorem of Arithmetic II

For every positive integer $n > 1$ there is a sequence $n = n_0 \geq n_1 \geq \cdots \geq n_{r-1} \geq n_r = 1$ such that each n_i/n_{i+1} is a prime, and the collection of primes which so occur and their multiplicities are uniquely determined by n up to reordering [16, p. 693].

In a sense, the approach is backwards. Instead of

beginning with a positive integer and factoring it into prime numbers, a set of prime numbers is selected and multiplied to form a positive integer. Thus, through collections of prime numbers, it is possible to obtain or survey all positive integers. If positive integers were difficult to identify, then this tool would be indispensable. Since they can be easily listed, the theorem appears trivial. For more complex mathematical entities like finite groups, however, it is realistic to know only a small part of the whole collection. In this situation, a theorem such as that given above, which allowed a mathematician to acquire all finite groups from some type of primitive elements, would be extremely useful. One does exist and is called the Jordan-Holder theorem. It has, not surprisingly, simple groups as its basic building blocks. The following derivation is meant to formally establish this assertion.

To begin, a special type of subgroup needs to be defined. Let N be a normal subgroup of a group G. The subgroup N is called a maximal normal subgroup of G if K is any other normal subgroup of G containing N, then K = N or K = G. A composition series is another necessary concept.

Definition

A **composition series** of G is a chain of subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ with G_{i+1} a maximal normal subgroup of G_i.

The resemblance between a composition series and the sequence of integers defined in the second Fundamental Theorem of Arithmetic should be apparent. It can be shown

that every finite group possesses a composition series which is necessary if the assertion under demonstration is to have any value. Consider the group C_{30} for an illustration of a composition series. Since normality is automatic, the construction is simplified. Using this particular group offers a comparison with the abelian example of C_{30}.

Composition Series of C_{30}

$$C_{30} \supset C_{15} \supset C_5 \supset \{e\}$$

An attempted correspondence with the second Fundamental Theorem of Arithmetic suggests an approach to a composition series through its factor groups G_i/G_{i+1}. They are constructed next for the composition series of C_{30}.

$$G_0/G_1 = C_{30}/C_{15} \sim C_2$$

$$G_1/G_2 = C_{15}/C_5 \sim C_3$$

$$G_2/G_3 = C_5/\{e\} \sim C_5$$

As suspected, these factor groups are simple. A theorem can be stated to formalize this observation.

Theorem

Let G be a finite group and $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ be any composition series of G. Then the factor groups G_i/G_{i+1} are simple for $i = 1, \ldots, r-1$.

Proof. Assume that for some i, $1 \leq i \leq r-1$, G_i/G_{i+1} is not simple. Then there exists a proper normal subgroup H_i^* of G_i/G_{i+1}. Since G_{i+1} is a normal subgroup of G_i, it is possible to define $f: G_i \longrightarrow G_i/G_{i+1}$ as the natural map. From the correspondence theorem, there exists a subgroup H_i of G_i with H_i normal in G_i and $G_i \supset H_i \supset G_{i+1}$. The group H_i contradicts G_{i+1} being a maximal normal subgroup of G_i. Therefore, G_i/G_{i+1} is simple.

The G_i/G_{i+1} are called the composition factors of G. Results from this discussion are summarized in a theory which is the analogue for finite groups of the Fundamental Theorem of Arithmetic.

Jordan-Holder Theorem

Every finite group G has a composition series $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ such that each factor group G_i/G_{i+1} is a simple group, and the collection of associated simple groups is unique up to reordering.

A composition series of C_{30}, different from the one given previously, is $C_{30} \supset C_6 \supset C_3 \supset \{e\}$. But the factor groups $C_{30}/C_6 \sim C_5$, $C_6/C_3 \sim C_2$, and $C_3/\{e\} \sim C_3$ are identical to those found before. Thus, the same collection of simple composition factors are obtained regardless of how the composition series for a finite group is constructed.

Sets of prime numbers are combined by the operation of multiplication to produce positive integers. Therefore, to finalize the analogy between simple groups and prime numbers, an operation must be demonstrated that will combine a collection of simple groups into a finite group. It seems intuitively correct to use direct product as the desired group operation. This is, however, a solution which is too simplistic. The circumstances surrounding the group operation are more complicated and ambiguous than the clear-cut process of multiplying prime numbers. To fully comprehend it, the idea of extensions must be introduced.

Definition

If K and Q are groups, an **extension of K by Q** is a group G such that:

(i) G contains K as a normal subgroup;

(ii) $G/K \sim Q$.

Given two groups K and Q, a search is conducted for a group G such that K is normal in G and G/K is isomorphic to Q. This is known as Holder's Extension Problem.

Extensions form a complex area that deviates too far from the purpose of this chapter for a detailed explanation. A general exposure, however, is sufficient. The direct product of K and Q is always one way to form an extension of K by Q. Finding the semidirect product of two groups is a more useful extension. Recall an automorphism is an isomorphism from a group to itself. A special mapping f, called an inner automorphism, is defined for a fixed g in a group G as $f(x) = g^{-1}xg$ for all x in G. It is now possible to explain the semidirect product in which automorphisms play a vital role.

Theorem

Given two groups Q and K and for every element q in Q an automorphism of K, $f(k) = k^q$ for all k in K, such that $(k^{q1})^{q2} = k^{q1q2}$ with q1 and q2 in Q. Then the symbols $(q, k), q \in Q$ and $k \in K$ form a group under the product rule $(q1, k1)(q2, k2) = (q1q2, k1^{q2}k2)$, called the **semidirect product of K by Q.**

Elements in a semidirect product group are the same as those in an external direct product group, ordered pairs, but their operations are different. Automorphisms are used in finding the semidirect product of two elements. It is seen that for each q in Q, an automorphism of the group K is constructed. In the given product rule, $k1^{q2}$ means the image of k1 under the automorphism of K associated with the element q2 in Q. Any automorphism possessed by the group K can be selected. For a variety of reasons related to

extensions, however, inner automorphisms of K induced by elements in Q are used.

The semidirect product of C_3 by C_2 will be found. Elements in these groups will be represented as permutations to enhance the discussion.

Let $K = C_3 = \{(1), (123), (132)\}$ and $Q = C_2 = \{(1), (12)\}$.

There will be two inner automorphisms of K since there are two elements in Q.

k	$f_{(1)}(k)$
(1)	$\xrightarrow{} (1)^{-1}(1)(1) = (1)$
(123)	$\xrightarrow{} (1)^{-1}(123)(1) = (123)$
(132)	$\xrightarrow{} (1)^{-1}(132)(1) = (132)$

k	$f_{(12)}(k)$
(1)	$\xrightarrow{} (12)^{-1}(1)(12) = (1)$
(123)	$\xrightarrow{} (12)^{-1}(123)(12) = (132)$
(132)	$\xrightarrow{} (12)^{-1}(132)(12) = (123)$

Six ordered pairs (q, k) with $q \in C_2$ and $k \in C_3$ form this semidirect product group. It is either C_6 or S_3 depending on whether the operation is commutative. The following two products will settle this question.

$$\big((12), (123)\big)\big((12), (132)\big) = \big((12)(12), (123)^{(12)(132)}\big)$$

since $f_{(12)}((123)) = (132)$, then

$$\big((12), (123)\big)\big((12), (132)\big) = \big((1), (132)(132)\big)$$

$$= \big((1), (123)\big)$$

Also,

$$\big((12),\ (132)\big)\big((12),\ (123)\big) = \big((12)(12),\ (132)^{(12)}(123)\big)$$

since $f_{(12)}((132)) = (123)$, then

$$\big((12),\ (132)\big)\big((12),\ (123)\big) = \big((1),\ (123)(123)\big)$$

$$= \big((1),\ (132)\big)$$

Seeing that $\big((12),\ (123)\big)\big((12),\ (132)\big)$ does not equal $\big((12),\ (132)\big)\big((12),\ (123)\big)$, the group under consideration is not abelian. Hence, S_3 is the semidirect product of C_3 by C_2, and this is often written as $C_3 \times_f C_2 = S_3$. When compared with the fact that C_6 is the direct product of C_3 and C_2, it can be concluded that both C_6 and S_3 are extensions of C_3 by C_2. Unlike multiplication of prime numbers, an extension G of K by Q is not uniquely determined by the groups K and Q.

Extensions have been thoroughly covered in the literature, and a more detailed discussion is found in [17, pp. 127-147]. All extensions G of K by Q can be constructed even though it is frequently a tedious undertaking. For what follows, it is satisfactory to know that extensions are a way to obtain possibly more than one bigger group from smaller groups with direct products and semidirect products being specific examples. Clearly, this summary describes a group operation. Although its properties differ somewhat from those of multiplication, it may be safely concluded that the group operation has been found and is embodied in extensions.

It is now time to discover how extensions relate to

simple groups and the Jordan-Holder theorem. This will tie together several different topics that may appear at this point to be unrelated. Beginning with a set of simple groups $Q_1, Q_2, \ldots, Q_r$, it is desired to find the group or groups they determine. The Jordan-Holder theorem guarantees that any obtainable G has a composition series $G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\}$ with simple composition factors isomorphic to the Q_i. Thus, with a slight abuse of terminology, $G_0/G_1 = Q_1$, $G_1/G_2 = Q_2, \ldots, G_{r-1}/G_r = Q_r$. Recovering G from the set of simple groups begins with finding G_{r-1} from Q_r. It is an easy process, since $G_r = \{e\}$ forces $G_{r-1} = G_{r-1}/\{e\} = G_{r-1}/G_r = Q_r$. The second step consists of using the group G_{r-1} from the first stage and Q_{r-1} to determine the group G_{r-2}. Due to the relationships $G_{r-2}/G_{r-1} = Q_{r-1}$ and $G_{r-1} = Q_r$, it is possible to recapture G_{r-2} through the application of extensions. All extensions G_{r-2} of Q_r by Q_{r-1} are computed, causing one or more groups to be produced for G_{r-2}. Next, in order to get the various groups represented by G_{r-3}, extensions are calculated from $G_{r-3}/G_{r-2} = Q_{r-2}$ for every group G_{r-2} found in the second phase. Reapplications of this procedure occur, each time climbing up the composition series, until all $G = G_0$ are obtained. Consequently, it is possible to acquire at least one group G from any given collection of simple groups. In a sense, the groups G_i/G_{i+1} are factors of G.

An example will serve to clarify this process. Let $Q_1 = C_2$ and $Q_2 = C_3$. At least one finite group G is

determined by these simple groups and will now be recaptured. Since there are only two composition factors, G has $G = G_0 \supset G_1 \supset \{e\}$ as a composition series. From the relationships $G_0/G_1 = C_2$ and $G_1/\{e\} = C_3$, it is automatically known that $G_1 = C_3$. Thus, $G = G_0$ will originate from $G_0/C_3 = C_2$ by finding all extensions of C_3 by C_2. Results from previous examples will be used to reduce the work involved. The direct product of C_3 and C_2, which has been shown to be C_6, constitutes the first extension group. Next, the semidirect product of C_3 by C_2 is found. Due to an earlier outcome, this produces S_3 as the second extension group. No other extensions are possible since there are only two groups of order six. Therefore, the finite groups C_6 and S_3 are obtained from the simple groups C_2 and C_3.

There is a drastic difference in complexity between a positive integer and a finite group. Yet there is a method for acquiring finite groups from simple groups similar to the way the Fundamental Theorem of Arithmetic produces positive integers from prime numbers. This situation, which appears trivial for positive integers, is remarkable for finite groups. It is largely due to the fact that all finite simple groups are known, or more formally, the Classification Theorem. If some simple groups were not known, then a number of finite groups, those that had the missing simple groups in their composition series, would not be constructable. The probability of being able to describe

these finite groups would be minimal. Only a complete list of simple groups can be used to make a complete catalogue of finite groups. Thus, finite simple groups are truly the basic building blocks of finite groups. The motivation for the time and effort invested in their discovery should now be evident.

Chapter V

SOLVABLE GROUPS AND OTHER TOPICS

This chapter will explore subjects of special interest to simple groups and then conclude the paper with a summary.

Solvability as it Relates to Simplicity

There is a distinctive type of group, called solvable, which is inversely associated with finite simple groups. Recall the previously mentioned Feit-Thompson theorem which asserts that all finite groups of odd order are solvable. This result is equivalent to stating that all finite simple groups, except those which are cyclic, have even order. Clearly, the concepts of simplicity and solvability are related in a somewhat mutually exclusive manner. Explaining this connection is the purpose of this section. Further applications for the Jordan-Holder theorem and composition series are also offered. Before a comparison can occur, it is necessary to define what it means for a group to be solvable.

Definition

A finite group is **solvable** if and only if it has a composition series with cyclic factor groups of prime order.

This definition indicates the property of solvability is determined solely by a group's composition factors. They must all be simple cyclic groups. When combined with the method for constructing finite groups outlined in the preceding section, it is possible to specifically obtain or access a subset of all finite groups, finite solvable

groups. If $Q_1, Q_2, \ldots, Q_r$ are chosen to be cyclic groups of prime order, then the application of extensions and the Jordan-Holder theorem produces one or more finite solvable groups for $G = G_0$.

The chief relationship between simple groups and solvable groups is addressed by the next theorem.

Theorem

Let G be a finite simple group whose order is not prime. Then G is not solvable.

Proof. Let G be a simple group whose order is not prime. Then $G \supset \{e\}$ is the only composition series for G, and $G/\{e\}$ is the only composition factor. It follows that $|G/\{e\}| = |G|$ which is not a prime number. Therefore, G is not solvable.

According to the theorem, a group whose order is not prime cannot be both simple and solvable. This concept, once Feit and Thompson established Burnside's conjecture as fact, offered a more precise characterization of simple groups. If a noncyclic group is simple and has an odd number of elements, then due to Feit and Thompson's result, it must also be solvable. The above theorem is contradicted by this reasoning. Consequently, in order to avoid possessing the property of solvability, a noncyclic simple group must contain an even number of elements. As noted before, this knowledge assisted immensely in the search for simple groups.

Clearly, alternating groups, groups of Lie type, and sporadic groups are not solvable. But cyclic groups of

prime order are solvable. This is due to the fact that solvability is a characteristic of all cyclic groups and explains why cyclic simple groups have been excluded from the above assertions. Since they are the only groups being both simple and solvable, cyclic groups of prime order are stubborn exceptions to the rule. Hence, a way to indicate a group is not simple, in almost all instances, is to call it solvable.

There are two examples which further characterize the relationship between the two topics under comparison. First, consider the symmetric group S_4. A composition series for this group is

$$S_4 \supset A_4 \supset \text{Klein 4-group} \supset C_2 \supset \{(1)\},$$

where

$$\text{the Klein 4-group} = \{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

and

$$C_2 = \{(1),\ (12)(34)\}.$$

The factor groups C_2, C_3, C_2, and C_2 are all cyclic of prime order. Thus, S_4 is a solvable group. Secondly, note the symmetric group S_5. One composition series of S_5 is $S_5 \supset A_5 \supset \{(1)\}$. The composition factors are C_2 and A_5 of which A_5 is not cyclic. Hence, S_5 is not solvable. Notice how the simplicity of the alternating groups effects the solvability of the symmetric groups. Since A_4 is not simple, it has a proper normal subgroup which follows it in the composition series of S_4. Due to the simplicity of A_5, however, it is impossible to find a proper normal subgroup of A_5 to insert between A_5 and $\{(1)\}$ in the composition series of S_5. Consequently, S_5 has A_5 as a noncyclic

composition factor. These results can be generalized as follows.

Theorem

If $n \geq 5$, then S_n is not solvable.

Proof. Since A_n is a normal subgroup of S_n, one composition series for S_n is $S_n \supset A_n \supset \{e\}$. The factor groups $C_2 \sim S_n/A_n$ and $A_n \sim A_n/\{e\}$ are unique by the Jordan-Holder theorem. If $n \geq 5$, then A_n is not cyclic. Therefore, S_n is not solvable.

Although this result appears to be no more significant than any other, it is partly responsible for the birth of group theory. Galois used the presence or absence of solvability, specifically in symmetric groups, to determine whether the roots of a polynomial equation could be expressed in terms of its coefficients using only addition, subtraction, multiplication, division, and extraction of roots. Curiously enough, simple groups are found embedded in another important segment of group theory.

Simple Facts

Now that all simple groups are known, the time has arrived for mathematicians to explore the ramifications. There are long-standing conjectures about both simple groups and related areas that are either instantly proven by the classification or should be verifiable. For the next several years, the effects of the Classification Theorem will be explored in such diverse fields as "finite group

theory, number theory, finite geometry, and infinite groups" [11, p. 57].

What follows are several interesting theorems and a conjecture all pertaining to simple groups. Since three of the four types of simple groups possess quite complex structures, these shared relationships are surprising. They are stated without comment or proof.

Theorem
If G is a simple group of even order (not 2), then 12, 16, or 56 divides the order of G.

Theorem
The outer automorphism group of every simple group is solvable.

Theorem
Let $f: G \longrightarrow H$ be a nontrivial homomorphism; that is, f does not send every element into one. If G is simple, then f is one-to-one.

Theorem
Let Pr(G) denote the probability that two elements selected at random (with replacement) from a group G are commutative. If G is a nonabelian simple group, then $Pr(G) \leq 1/12$, with equality for the alternating group on five letters. [14, p. 1033]

Conjecture
Every simple group can be generated by two elements.

Also, isomorphisms exist among the different categories of simple groups, with one being between the groups A_5 and PSL(2,4).

Simple group study is definitely not over. Future applications of simple groups and the probable new knowledge surrounding them, in all likelihood, will be an exciting area of research.

Conclusion

Finite simple groups have been explored in detail by this paper. Historical and mathematical information has been presented from both specific and general points of view. Beginning with an elementary definition, the topic of this paper escalated in complexity. Hence, quite a simple versus complex paradox surrounds finite simple groups. Perhaps the best recapitulation is a song borrowed from the November 1973 issue of the American Mathematical Monthly. It was "found scrawled on a library table in Eckhart Library at the U. of Chicago; author unknown, or in hiding" [19, p. 1028]. The loops referred to in the song are cyclic groups of prime order.

(Sung to the tune of "Sweet Betsy from Pike")

What are the orders of all simple groups?
I speak of the honest ones, not of the loops.
It seems that old Burnside their orders has guessed
Except for the cyclic ones, even the rest.

Groups made up with permutes will produce some more:
For An is simple, if n exceeds 4.
Then, there was Sir Matthew who came into view
Exhibiting groups of an order quite new.

Still others have come on to study this thing.
Of Artin and Chevalley now we shall sing.
With matrices finite they made quite a list
The question is: Could there be others they've missed?

Suzuki and Ree then maintained it's the case
That these methods had not reached the end of the chase.
They wrote down some matrices, just four by four,
That made up a simple group. Why not make more?

And then came the opus of Thompson and Feit
Which shed on the problem remarkable light.
A group, when the order won't factor by two
Is cyclic or solvable. That's what is true.

Suzuki and Ree had caused eyebrows to raise,
But the theoreticians they just couldn't faze.
Their groups were not new: if you added a twist,
You could get them from old ones with a flick
  of the wrist.

Still, some hardy souls felt a thorn in their side.
For the five groups of Mathieu all reason defied;
Not An, not twisted, and not Chevalley,
They called them sporadic and filed them away.

Are Mathieu groups creatures of heaven or hell?
Zvonimir Janko determined to tell.
He found out that nobody wanted to know:
The masters had missed 1 7 5 5 6 0.

The floodgates were opened! New groups were the rage!
(And twelve or more sprouted, to greet the new age.)
By Janko and Conway and Fischer and Held
McLaughlin, Suzuki, and Higman, and Sims.

No doubt you noted the last lines don't rhyme.
Well, that is, quite simply, a sign of the time.
There's chaos, not order, among simple groups;
And maybe we'd better go back to the loops. [19, p. 1028]

BIBLIOGRAPHY

[1] G. L. Alexanderson and A. P. Hillman, A First Undergraduate Course in Abstract Algebra, 3rd ed., Wadsworth Publishing Co., Belmont, CA, 1983.

[2] C. B. Boyer, A History of Mathematics, John Wiley and Sons, NY, 1968.

[3] R. D. Brauer,"Blocks of Characters and Structure of Finite Groups," Bull. Amer. Math. Soc. 1 (1979), 21-38.

[4] W. Burnside, Theory of Groups of Finite Order, 2nd ed., Cambridge Univ. Press, NY, 1911; reprint ed., Dover, NY, 1955.

[5] D. M. Burton, Elementary Number Theory, Allyn and Bacon, Boston, MA, 1980.

[6] W. Feit and J. Thompson, "Solvability of Groups of Odd Order," Pacific J. Math. 13 (1963), 775-1029.

[7] J. Friendly, "A School of Theorists Works Itself Out of a Job," New York Times (June 22, 1980), sec. 4, p. E11.

[8] M. Gardner, "Mathematical Games," Scientific American 242 (June 1980), 16-22.

[9] D. Gorenstein, Finite Groups, Harper and Row, NY, 1968.

[10] --------, "The Classification of Finite Simple Groups," Bull. Amer. Math. Soc. 1 (1979), 43-199.

[11] --------, Finite Simple Groups, Plenum Press, NY, 1982.

[12] --------, "Classifying the Finite Simple Groups," Bull. Amer. Math. Soc. 14 (1986), 1-98.

[13] "Group Therapy," Scientific American 242 (May 1980), 82-84.

[14] W. H. Gustafson, "What is the Probability that Two Group Elements Commute?", Amer. Math. Monthly 80 (1973), 1031-1034.

[15] M. Hall, Jr., The Theory of Groups, Macmillan, NY, 1959.

[16] J. F. Hurley and A. Rudvalis, "Finite Simple Groups," Amer. Math. Monthly 84 (1977), 693-714.

[17] J. J. Rotman, The Theory of Groups: An Introduction, Allyn and Bacon, Boston, MA, 1965.

[18] W. R. Scott, Group Theory, Prentice-Hall, Englewood Cliffs, NJ, 1964.

[19] "Simple Groups," Amer. Math. Monthly 80 (1973), 1028.

[20] L. A. Steen, "A Monstrous Piece of Research," Science News 118 (Sept. 27, 1980), 204-206.

[21] --------, "Mathematics," Encyclopaedia Britannica Book Of The Year, 1981.