EXAMPLES OF FINITE GROUPS

5/5

A Thesis

Presented to

the Faculty of the Department of Mathematics

Kansas State Teachers College

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

by

H. Dean Johnson

August 1967

Approved for the Major Department

Approved for the Graduate Council

To Lester E. Laird for his many helpful suggestions, the writer wishes to express his appreciation.

I also wish to thank my wife for her patience and understanding during the development of this paper.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 THE PROBLEM

The student of mathematics begins to find early in his study that certain basic concepts seem to occur again and again in every area of investigation. One of these concepts of great universality in mathematics is the group.

Historically, groups arose and were used as a tool in the study of the theory of equations. Groups were first used by Augustin Louis Cauchy (1789-1857) and by Evariste Galois (1811-1832) as a mapping of the roots of an equation onto themselves [4;24]. The results of their work greatly enriched the study of polynomials and fields and furnished incentive for further development of group theory.

The axiomatic formulation of an abstract group was first given in 1870 by Leopold Kronecker (1823-1891) [4;24]. Since that time the group concept has undergone a considerable degree of sophistication.

As the study of mathematical concepts becomes more abstract, problems of communication arise for the student and the teacher of mathematics. One of the areas of difficulty in the theory of groups is the small number of examples in many textbooks. Both the teacher and the student find it helpful when examples are provided which illustrate the content of a definition.

The realization that a part of the development of the student of mathematics is the ability to provide examples for abstract definitions, has been the motivation for study in this particular area.

The purpose of this thesis is to present definitions for and to provide examples of many of the more common types of groups. In addition to the examples provided, theorems are given so that the reader may provide examples for himself.

In this thesis it is assumed that the reader has had a course in abstract algebra. To present examples on this level, all definitions and theorems are limited to finite groups except in a few cases where a particular definition or theorem may apply to both finite and infinite groups. Chapters II and III contain many definitions and terms which are already well known to the student of abstract algebra. They are listed in these chapters to serve as a review and for ease of reference.

1.2 ORGANIZATION OF THE THESIS

Chapter II contains the basic definitions of terms used in the thesis, as well as a few common examples.

The simpler groups are defined with examples in Chapter III. Many of the groups given as examples in Chapter III serve again as examples in later chapters. Chapter IV contains a presentation of groups defined in terms of elements of a group and powers. Groups with normal subgroups are presented in Chapter V.

The method of organization in this thesis follows a pattern of definition, example or examples, theorems and more examples.

CHAPTER II

DEFINITION OF TERMS

2.1 DEFINITION OF A GROUP

Definition. A nonempty set G with binary operation "$*$" is a <u>group</u> if and only if it satisfies the following properties:

(i) (closure) for $a,b \in G$ there is a unique $c \in G$ such that $a*b = c$,

(ii) (associativity) for $a,b,c \in G$, $a*(b*c) = (a*b)*c$,

(iii) (identity) there is an $e \in G$ such that if $a \in G$ then $a*e = a$,

(iv) (inverses) for $a \in G$ there is an $a^{-1} \in G$ such that $a*a^{-1} = e$.

Since the abstract system called a group is defined in terms of a set and an operation on that set, it is often denoted as an ordered pair, $(G,*)$, the first element of the pair being the set G, the second being the operation "$*$". However, $(G,*)$ will be denoted by G except in cases where misunderstanding may occur.

The set G of a group may be either finite or infinite. The term order of a group refers to the number of elements in G.

Definition. If G has n elements, where n is a positive integer, $(G,*)$ is said to have <u>order</u> n. If there exists no such positive integer, $(G,*)$ is said to have infinite order.

The operation "$*$" is customarily called addition or multiplication although the operation as used in a particular group may not be the same as the addition and multiplication of arithmetic.

A number of easy theorems follow from the defining properties i-iv.

2.1.1 The identity of a group is unique [6;169].

2.1.2 The inverse of every element of a group is unique [6;169].

2.1.3 If $a,b,c\in G$ such that $ab=ac$, then $b=c$ [6;169].

2.1.4 If $a,b,c\in G$ such that $ba=ca$, then $b=c$ [6;169].

2.1.5 For $a\in G$, $e*a=a$ [9;7].

2.1.6 For $a\in G$, $a^{-1}*a=e$ [9;6].

2.1.7 If $a,b\in G$ then there exists $x\in G$ such that $a*x=b$ [9;7].

2.1.8 If $a,b\in G$ then there exists $x\in G$ such that $x*a=b$ [9;7].

2.1.9 If $a*b=e$, then $b=a^{-1}$ [9;7].

2.1.10 $(a^{-1})^{-1}=a$ [9;7].

2.2 POWERS OF ELEMENTS OF A GROUP

In the discussion of groups it is necessary to consider an element of a group raised to a power. Since the exponent of a group element is an integer, the exponent is quite often not an element of the group itself. It is therefore helpful to define exponents in the following manner:

$a^o = e$,

$a^n = (a^{n-1}) * a$, and

$a^{-n} = (a^{-1})^n$, so that

$a^o = e$

$a^1 = a^o * a$

$a^2 = a^1 * a$

$a^3 = a^2 * a$

.

.

.

$a^n = (a^{n-1}) * a$.

By induction:

$a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

The elements of a set G in (G,*) have order, defined in terms of exponents.

Definition. For $a \in G$, a has order n if n is the smallest positive integer such that $a^n = e$ where e is the identity of G. If no such integer n exists, a has infinite order.

2.3 EXAMPLES OF GROUPS

The set of integers with "*" as the usual operation of addition forms a group of infinite order denoted (I,+). The identity element is 0 and the inverse of a is -a.

The set of rational numbers form a group under the operation of addition. The inverse of $\frac{p}{q}$ is $-\frac{p}{q}$ and the identity element is 1.

The set of positive rational numbers with "$*$" as the usual arithmetic operation of multiplication forms a group of infinite order denoted $(+Ra,\cdot)$. Each rational $\frac{p}{q}$ has an inverse $\frac{q}{p}$ and the identity element is 1.

The rational numbers of $[0,1)$ form a group where addition is defined as $a+b=c$ where $c<1$, $a+b=c-1$ where $c\geq 1$. The identity element of the group is 0 and the inverse of a is $1-a$.

The set $\{0,1,2,\ldots,n-1\}$ with addition modulo n is a finite group of order n with identity element 0. This group is referred to as the additive group $^{I}/(n)$.

The set $\{1,2,3,\ldots,n-1\}$ with multiplication modulo n where n is a prime, is a finite group of order $n-1$. The identity element is 1. This group is referred to as the multiplicative group $^{I}/(n)$.

The following example of a multiplicative group $^{I}/(n)$ is given so as to help in the illustration of some later definitions.

The set $\{1,2,\ldots,6\}$ with multiplication modulo 7 forms a group of order 6. The operation table below shows the identity element to be 1. Note that each of the elements in the group has an inverse. ($2^{-1}=4$, $3^{-1}=5$, $4^{-1}=2$, $5^{-1}=3$, $6^{-1}=6$, $1^{-1}=1$)

TABLE I

THE MULTIPLICATIVE GROUP $^{I}/(7)$

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

2.4 SUBGROUPS

Definition. If a subset H of G has elements which satisfy the properties of a group under the operation of G, then H is said to be a <u>subgroup</u> of G.

The theorem of La Grange is stated here because it will be of value later in the thesis in finding subgroups of groups. "If G and a subgroup H have order m and n respectively then n divides m" [7;19].

Subgroups often have what might be termed "inheritance properties", that is, if G is a certain type of group, every subgroup H often is of that type.

2.5 EXAMPLES OF SUBGROUPS

For G, the multiplicative group $^{I}/(7)$, G has subsets $H = \{1,2,4\}$ and $J = \{1,6\}$ whose elements satisfy the properties of groups. Notice H and J have order 3 and 2 respectively, both of which divide the order of G.

2.6 DEFINITION OF COSET

Definition. If H is a subgroup of G, then a <u>right</u> <u>coset</u> of H in G is a subset S of G such that there exists $x \in G$ for which $S = Hx$. A <u>left</u> <u>coset</u> of H in G is a subset S' of G such that there exists $x \in G$ for which $S' = xH$.

2.7 EXAMPLES OF COSETS

For G, the multiplicative group $^I/(7)$, $H = \{1,2,4\}$ and $J = \{1,6\}$ are subsets of G. To illustrate the definition of coset, the right cosets of H in G are determined below.

$H1 = \{1,2,4\}1 = \{1*1,\ 2*1,\ 4*1\} = \{1,2,4\}$.

$H2 = \{1,2,4\}2 = \{1*2,\ 2*2,\ 4*2\} = \{2,4,1\}$.

$H3 = \{1,2,4\}3 = \{1*3,\ 2*3,\ 4*3\} = \{3,6,5\}$.

$H4 = \{1,2,4\}4 = \{1*4,\ 2*4,\ 4*4\} = \{1,2,4\}$.

$H5 = \{1,2,4\}5 = \{1*5,\ 2*5,\ 4*5\} = \{5,3,6\}$.

$H6 = \{1,2,4\}6 = \{1*6,\ 2*6,\ 4*6\} = \{6,5,3\}$.

The right cosets of H in G are $\{1,2,4\}$ which is H itself and $\{3,5,6\}$. In this particular example the left cosets of H in G are the same as the right cosets as shown below.

$1H = 1\{1,2,4\} = \{1*1,\ 1*2,\ 1*4\} = \{1,2,4\}$.

$2H = 2\{1,2,4\} = \{2*1,\ 2*2,\ 2*4\} = \{2,4,1\}$.

$3H = 3\{1,2,4\} = \{3*1,\ 3*2,\ 3*4\} = \{3,6,5\}$.

$4H = 4\{1,2,4\} = \{4*1,\ 4*2,\ 4*4\} = \{4,1,2\}$.

$5H = 5\{1,2,4\} = \{5*1,\ 5*2,\ 5*4\} = \{5,3,6\}.$

$6H = 6\{1,2,4\} = \{6*1,\ 6*2,\ 6*4\} = \{6,5,3\}.$

The left cosets of J in G are determined below. It can easily be seen that the right cosets of J in G are equal to the left cosets.

$1J = 1\{1,6\} = \{1,6\}.$

$2J = 2\{1,6\} = \{2,5\}.$

$3J = 3\{1,6\} = \{3,4\}.$

$4J = 4\{1,6\} = \{4,3\}.$

$5J = 5\{1,6\} = \{5,2\}.$

$6J = 6\{1,6\} = \{6,1\}.$

The left cosets of J in G are $\{1,6\}$, $\{2,5\}$, and $\{3,4\}$.

2.8 OPERATIONS ON COSETS

For a subgroup H of G, if A, the set of right cosets of H in G, is equal to B, the set of left cosets of H in G, an operation can be defined on A such that A forms a group under that operation. Let A $A_1, A_2, A_3, \ldots, A_k$. The product of any two cosets of A, $A_i \cdot A_j$, with m and n elements respectively is

$$A_i \cdot A_j = \{a_{1_i} * a_{1_j},\ a_{2_i} * a_{1_j}, \ldots, a_{m_i} * a_{1_j},\ a_{2_i} * a_{2_j}, \ldots,\ a_{m_i} * a_{2_j},\ a_{1_i} * a_{3_j},\ a_{2_i} * a_{3_j}, \ldots,\ a_{1_i} * a_{n_j},\ a_{2_i} * a_{n_j}, \ldots,\ a_{m_i} * a_{n_j}\}.$$

The operation just defined on cosets will be referred to as multiplication of cosets.

2.9 DEFINITION OF FACTOR GROUP

From section 2.7, A, the set of right cosets of H in G, is equal to the set of left cosets of H in G.

Definition. The set of cosets A of H in G under the operation "multiplication of cosets" is a group called the <u>factor group</u> of H in G, denoted G/H.

Using the set of cosets A = $\left[\{1,2,4\},\ \{3,5,6\}\right]$ and the operation "multiplication of cosets" defined in 2.7, the following example of a factor group is given.

$$\{1,2,4\} \cdot \{3,5,6\} = \{1*3,\ 2*3,\ 4*3,\ 1*5,\ 2*5,\ 4*5,\ 1*6,\ 2*6,\ 4*6\} = \{3,6,5,5,3,6,6,5,3\} = \{3,5,6\}$$

$$\{1,2,4\} \cdot \{1,2,4\} = \{1*1,\ 2*1,\ 4*1,\ 1*2,\ 2*2,\ 4*2,\ 1*4,\ 2*4,\ 4*4\} = \{1,2,4,2,4,1,4,1,2\} = \{1,2,4\}$$

$$\{3,5,6\} \cdot \{1,2,4\} = \{3*1,\ 5*1,\ 6*1,\ 3*2,\ 5*2,\ 6*2,\ 3*4,\ 5*4,\ 6*4\} = \{3,5,6,6,3,5,5,6,3\} = \{3,5,6\}$$

$$\{3,5,6\} \cdot \{3,5,6\} = \{3*3,\ 5*3,\ 6*3,\ 3*5,\ 5*5,\ 6*5,\ 3*6,\ 5*6,\ 6*6\} = \{2,1,4,1,4,2,4,2,1\} = \{2,1,4\}$$

TABLE II

A FACTOR GROUP OF ORDER 2

•	{1,2,4}	{3,5,6}
{1,2,4}	{1,2,4}	{3,5,6}
{3,5,6}	{3,5,6}	{1,2,4}

2.10 ISOMORPHISMS

Two groups of the same order may be found upon examination to have exactly the same properties so that the only way in which they differ is in the choice of symbols used to represent the elements of each group. Accordingly, such groups are said to be isomorphic.

Definition. A 1-1 mapping of a group G onto a group G^1 is called an *isomorphism* if the operation is preserved under this mapping; that is, if for arbitrary elements a,b of G: $a*b$ maps into a^1*b^1. If there exists an isomorphism of G onto G^1, G is *isomorphic* to G^1.

CHAPTER III

COMMON GROUPS OF ABSTRACT ALGEBRA

3.1 PERMUTATION AND SYMMETRIC GROUPS

Definition. Let S be a set of elements. A permutation P on the set S is a 1-1 mapping of S onto itself.

The number of possible permutations of a set S onto itself is, of course, dependent upon the number of elements in S. It can be shown that if a set has n elements, there are n! permutations on that set.

Let S be a set of n elements. $S_n = \{P_1, P_2, \ldots, P_{n!}\}$ is the set of permutations on a set S of n elements.

The set S_n of all permutations on a set of n elements forms a group under the operation of composition.

Definition. The group of all permutations of a set of n elements is called the symmetric group on n symbols and is denoted "S_n".

Definition. Any group whose elements are permutations is called a permutation group.

In the following examples, permutations P_n on a set S are denoted by listing the elements of S on two rows. Immediately below an element of the top row is listed its image under the particular mapping P_i.

For the first example let $S = \{a,b,c\}$. The set $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ is the set of permutations on the set S of 3 elements. The permutations $P_1,\ldots,P_6$ are identified by their row representations.

$P_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}.$

$P_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}.$

$P_3 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}.$

$P_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}.$

$P_5 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}.$

$P_6 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}.$

Since $P_1,\ldots,P_6$ are all 1-1 functions, the composition of those functions will also be 1-1. Using the operation composition of functions, the following table is constructed.

TABLE III

THE SYMMETRIC GROUP S_3

*	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_1	P_5	P_6	P_3	P_4
P_3	P_3	P_4	P_1	P_2	P_6	P_5
P_4	P_4	P_3	P_6	P_5	P_1	P_2
P_5	P_5	P_6	P_2	P_1	P_4	P_3
P_6	P_6	P_5	P_4	P_3	P_2	P_1

Other examples of symmetric groups are S_4, the set of permutations on 4 elements of order 24; S_5, the set of permutations on 5 elements of order 120.

An important theorem of group theory is Cayleys Theorem which states, "Any group is isomorphic to a group of permutations" [9;47].

Any element of a set of permutations can be expressed in terms of what is termed cycle notation. A cycle is a set of ordered n-tuples $(a_1,a_2,a_3,\ldots,a_n)$ of elements of a group. The n-tuple $(a_1,a_2,a_3,\ldots,a_n)$ represents the permutations which maps each a_i onto a_{i+1} and a_n onto a_1. $P_4=\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$ of S_3 is represented by the cycle (a b c). $P_5=\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$ of S_3 is represented by the cycle (a c b).

If a particular permutation maps an element into itself that element is omitted from the cycle representing that permutation. In $P_2=\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$ of S_3, a is mapped into itself and is omitted from the cycle. P_2 would be represented by the cycle (b c). P_3 and P_6 of S_3 are represented by (a c) and (a b). P_1 of S_3 maps every element into itself so that all elements are omitted from the cycle. The permutation which maps every element of a group onto itself is denoted "I".

In permutation groups larger than S_3, some permutations require two or more cycles for their representation. The permutation $\begin{pmatrix} a & b & c & d \\ b & c & d & e \end{pmatrix}$ of S_4 would be represented by the two cycles (a b) (c d).

3.2 ALTERNATING GROUPS

An alternating group is a subgroup of a symmetric group. In order to see exactly what type of subgroup, it is necessary to introduce the idea of a transposition and an even permutation.

Definition. If the elements of a set S are written as an ordered n-tuple $(x_1,x_2,x_3,\ldots,x_n)$, a transposition on S is a permutation which exchanges the position of any 2 elements.

Definition. A permutation is called an even permutation if it can be expressed as the product of an even number of transpositions.

It is possible to write a definition for odd permutations but it is not given here because it will not be needed.

It can be shown that the set of all even permutations of the symmetric group S_n is a subgroup of S_n of order $n!/2$.

Definition. The subgroup of all even permutations of a symmetric group of n elements is called the alternating group on n symbols and is denoted "A_3".

For the example of alternating groups the elements of S_3 are listed, showing that 3 of them are transpositions and 3 are the product of an even number of transpositions. The 3 elements which are products of an even number of transpositions are the elements of A_3, the alternating group on 3 elements.

There are 3 elements of S_3 which are transpositions. $P_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$ exchanges the position of b and c. $P_3 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$ exchanges the position of a and c. $P_6 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$ exchanges the position of a and b.

From Table III it is obvious that P_1, P_4 and P_5 can be expressed as the product of an even number of transpositions and are the even permutations of S_3.

The operation table of A_3 is listed below.

TABLE IV

THE ALTERNATING GROUP A_3

*	P_1	P_4	P_5
P_1	P_1	P_4	P_5
P_4	P_4	P_5	P_1
P_5	P_5	P_1	P_4

The other examples of alternating groups are A_2, A_4, $A_5, \ldots, A_n$ of order $1, 12, 60, \ldots, n!/_2$.

3.3 CYCLIC GROUPS

Each element of a cyclic group can be expressed as a power of a single element of the group.

Definition. If a group G contains an element a such that every element of G is of the form a^n for some integer n, then G is a <u>cyclic group</u> and is said to be generated by a or a is a generator of G.

The set of integers under the operation addition is an infinite cyclic group. 1 is the generator of this group since $1+1 = 2$, $1+1+1 = 3, \ldots$ and is of infinite order.

The multiplicative group of integers $I/(5)$ is cyclic. Either 2 or 3 will generate the group.

$(2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1;\ 3^1 = 1,\ 3^2 = 4,\ 3^3 = 2,$
$3^4 = 1)$.

THEOREMS ON CYCLIC GROUPS

3.3.1 Every subgroup H of a cyclic group G is itself a cyclic group [6;185].

3.3.2 For every prime p, the multiplicative group of integers I/(p) is cyclic [6;186].

3.3.3 There is a cyclic group of order n for each natural number n [9;34].

3.3.4 Every cyclic group of infinite order is isomorphic to the additive group of integers [6;184].

3.3.5 Any two cyclic groups of the same order are isomorphic [6;184].

3.3.6 If G is a cyclic group of order n, G has exactly one cyclic subgroup of order m for each positive divisor m of n, and no other subgroup [9;35].

The nth roots of unity under the operation of multiplication as defined for complex numbers form a group. Each group is of order n, has 1 as the identity and has a generator of order n (a primitive root).

3.4 DIHEDRAL GROUPS

The dihedral groups are characterized as the set of rotations and reflections about the axes of symmetry of an n sided polygon. However, the definition of dihedral groups used here is an abstract one given in terms of generators and their relationships.

Definition. The <u>dihedral group</u> D_n is a group of order 2n generated by 2 elements s and t which satisfy the relations $s^n = e$, $t^2 = e$, and $tst = s^{-1}$.

To illustrate how 2 elements can generate a group, let n = 3. The elements of the dihedral group D_3 will be the powers of s, $(s, s^2, e = s^3)$; the powers of t, $(t, e = t^2)$; and their products, (ts, ts^2, st, s^2t). Listing e only once gives $e, s, s^2, t, ts, st, ts^2, s^2t$ the set of 8 elements whereas the definition of dihedral groups says there should be only 6 distinct elements. The relationship $tst = s^{-1}$ shows that $st = ts^2$ and $ts = s^2t$ thereby eliminating ts^2 and s^2t from the set. This leaves 6 elements in the set so that D_3 has order 6. The operation on this set is similar to the regular multiplication of arithmetic except that the commutative property does not apply. The relation $tst = s^{-1}$ must be used in working out the group table to change some of the products to a form contained in the original set. As an example, the product of s^2 and t is s^2t, but by the relation $tst = s^{-1}$, $s^2t = ts$. Therefore the product of s^2 and t is listed as ts in the table to better illustrate closure.

Dihedral groups exist for any natural number n. The smallest, of course, would be D_1 of order 1. The example used here is D_3. To show how dihedral groups can be characterized as a group of rotations and reflections of a regular n-sided polygon, the equilateral triangle PQR of Figure 1 with axes of symmetry a, b, and c is used. Let elements E, B and C represent clockwise rotations about the centroid of 0, 120, and 240 degrees. The elements F, G and H represent reflections of the triangle about the axes a, b, and c respectively. The operation "*" in this group is interpreted as "followed by". The symbols B*C indicate a rotation of 120 degrees followed by a rotation of 240 degrees. These rotations leave the triangle in its original position and are the equivalent of a rotation of 0 degrees, so that B*C = E.

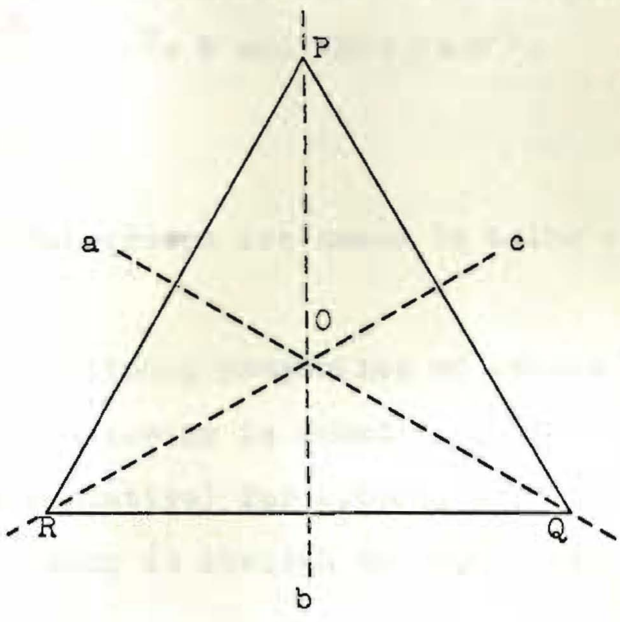

FIGURE 1

THE AXES OF SYMMETRY OF
AN EQUILATERAL TRIANGLE

With the set and operation defined, the following table describes the group D_3.

TABLE V

THE DIHEDRAL GROUP D_3

*	E	B	C	H	G	F
E	E	B	C	H	G	F
B	B	C	E	G	F	H
C	C	E	B	F	H	G
H	H	F	G	E	C	B
G	G	H	F	B	E	C
F	F	G	H	C	B	E

It can be seen that B and F are the generators of this group. $B^3 = E$, $F^2 = E$ and $FBF = C = B^{-1}$.

3.5 ABELIAN GROUPS

The Abelian groups are named in honor of N.H. Abel (1802-1829).

To the 4 defining properties of groups listed in section 2.1 the following is added:

(v) (commutative) for $a, b, \in G$, $a*b = b*a$.

Definition. A group is Abelian or commutative if and only if it satisfies (v).

An Abelian group is easily recognized when its operation table is given as the entries of the table are symmetric with respect to the main diagonal.

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

FIGURE 2

THE SYMMETRY OF THE TABLE
FOR AN ABELIAN GROUP

The integers form an Abelian group under addition since addition is commutative in the integers.

The rational numbers form an Abelian group under addition since addition is commutative in the rationals.

The multiplicative group of integers I/(n) is Abelian.

Other examples of Abelian groups are given throughout the remaining chapters.

CHAPTER IV

p-GROUPS AND RELATED GROUPS

4.1 p-GROUPS

Definition. A group G is a p-group if and only if every element of G except the identity has order a power of a prime p.

The operation table below gives a group of order 9 which is Abelian. Each element except e has order 3.

TABLE VI

AN ABELIAN p-GROUP OF ORDER 9

*	e	a	b	c	d	o	f	g	h
e	e	a	b	c	d	o	f	g	h
a	a	b	e	o	g	f	c	h	d
b	b	e	a	f	h	c	o	d	g
c	c	o	f	d	e	g	h	a	b
d	d	g	h	e	c	a	b	o	f
o	o	f	c	g	a	h	d	b	e
f	f	c	o	h	b	d	g	e	a
g	g	h	d	a	o	b	e	f	c
h	h	d	g	b	f	e	a	c	o

THEOREMS ON p-GROUPS

4.1.1 A subgroup or factor group of a p-group is a p-group [9;131].

4.1.2 A finite group G is a p-group if and only if the order of G is a power of some prime number [9;132].

4.1.3 Any group of order p^2 is Abelian [7;87].

The characterization of p-groups given in theorem 4.1.2 makes the problem of finding examples of p-groups a very simple one. Any group of order 2,3,4,5,7,8,9,11,13,16, 17,...is a p-group.

To find a cyclic p-group of order p, a prime, let $a^p = e$. The elements of the group are e (the identity), a, $a^2, \ldots, a^{p-1}$. The operation is regular multiplication. In this group $a^p = e$, $(a^2)^p = e, \ldots,$ $(a^{p-1})^p =$ r which satisfies the definition of a p-group.

For groups of order p^2, p a prime, $a^{p^2} = e$ gives p-groups which are also cyclic. $a^p = e$, $b^p = e$, $ba = ab$ defines groups which are p-groups. The example given in section 4.1 is defined by $a^3 = e$, $c^3 = e$, $ca = ac$. ($b = a^2$, $d = c^2$, $e = ac$, $f = a^2c$, $g = ac^2$, $h = a^2c^2$).

The dihedral group D_4 is a non-Abelian p-group of order 8.

Other examples of p-groups can be found by consulting a table of defining relations for p-groups [5;51,187].

4.2 THE QUATERNION GROUP

The quaternion group satisfies the definition of p-groups and can be defined in terms of generators.

Definition. The group G of order 8 generated by a,b where

$a^4 = e$, $a^2 = b^2$, $b^{-1}ab = a^{-1}$ is the quaternion group.

The operation table below is given in terms of ± 1, $\pm i$, $\pm j$, $\pm k$ with the multiplication rules: i^2, j^2, $k^2 = -1$; $ij = k$; $jk = i$; $ki = j$; $ji = -k$; $kj = -i$; $ik = -j$; and the usual rules for multiplying -1. The 8 elements of this group are the basis units of the quaternion; that is, every quaternion can be written as a linear combination of these elements.

TABLE VII

THE QUATERNION GROUP

*	1	i	j	k	-1	-i	-j	-k
1	1	i	j	k	-i	-i	-j	-k
i	i	-1	k	-j	-i	1	-k	j
j	j	-k	-1	i	-j	k	1	-i
k	k	j	-i	-1	-k	-j	i	1
-1	-1	-i	-j	-k	1	i	j	k
-i	-i	1	-k	j	i	-1	k	-j
-j	-j	k	1	-i	j	-k	-1	i
-k	-k	-j	i	1	k	j	-i	-1

4.3 SYLOW p-SUBGROUPS

The Sylow p-subgroups are named for Ludwig Sylow (1832-1918), an important contributor to group theory.

Definition. A subgroup S of a group G is a Sylow p-subgroup of G if and only if it is a p-group and is not contained in any larger p-group which is a subgroup of G.

Any proper subgroup of a p-group G is not a Sylow p-subgroup since it is contained in the larger p-group G which is a subset of itself. For this reason the examples chosen will be proper subgroups of non p-groups.

The group S_3 has subgroups $\{P_1, P_6\}$, $\{P_1, P_3\}$, $\{P_1, P_2\}$ and $\{P_1, P_4, P_5\}$. Since the order of the subgroups is 2 and 3, they are p-groups by theorem 4.1.2. None of them are contained in a larger p-group, therefore they are Sylow p-subgroups of S_3. The three groups $\{P_1, P_6\}$, $\{P_1, P_3\}$ and $\{P_1, P_2\}$ are sometimes called Sylow 2-subgroups. $\{P_1, P_4, P_5\}$ would be a Sylow 3-subgroup.

The group S_4 has subgroups of order 1,2,3,4,6,8,12 and 24. By theorem 4.1.2 the subgroups of order 6, 12 and 24 are not p-groups and therefore are not Sylow p-subgroups. All subgroups of order 1,2,3,4 and 8 are p-groups. However, in S_4 all subgroups of order 1 and 2 are contained in larger p-groups (those of order 4) and are therefore not Sylow p-subgroups. All subgroups of order 4 are contained in the subgroups of order 8 so that the Sylow p-subgroups of S_4 are the 4 subgroups of order 3 and the 3 subgroups of order 8.

THEOREMS FOR SYLOW p-SUBGROUPS

4.3.1 If G is a group of order $p^r m$, where p is a prime and p and m relatively prime, a subgroup H is a Sylow p-subgroup if it has order p^r [9;132].

4.3.2 (Sylow's theorem) If G is a group of order $p^r m$, where p is a prime and p and m are relatively prime, the number n of Sylow p-subgroups is such that $n \equiv 1 \pmod p$ [9;133].

Note how theorems 4.3.1 and 4.3.2 verify the results of S_4 above.

4.4 DICYCLIC GROUPS

Definition. A group G is dicyclic if and only if it is of order 4n and is generated by 2 elements a and b such that $a^{2n} = e$, $a^n = b^2$, $aba = b$.

The dicyclic group of lowest order is the group of order 4, found by letting $n = 1$. The elements are e, a, b, and ab.

For $n = 2$, the expression $a^{2n} = e$, $a^n = b^2$, $aba = b$ becomes $a^4 = e$, $a^2 = b^2$, $aba = b$. In the following it is shown that $aba = b$ is equivalent to $b^{-1}ab = a^{-1}$.

$aba = b.$

$ab = ba^3.$

$b^{-1}ab = a^3.$

$b^{-1}ab = a^{-1}.$

By the definition of the quaternion group in section 4.2 it is obvious that the dicyclic group obtained for $n = 2$ is isomorphic to the quaternion group.

The dicyclic group of order 12 ($n = 3$) along with the dihedral group D_6 are the only 2 non-Abelian groups of order 12.

4.5 METACYCLIC GROUPS

Definition. A group G is metacyclic if and only if it is generated by two elements a and b such that $x^m = y^n = e$ $y^{-1}xy = x^r$ where $(m,r-1) = 1$ and $r^n \equiv 1 \pmod{n}$.

Finding the examples for metacyclic groups amounts to finding the numbers m, n and r which meet the conditions of the definition.

For $m = 5$, $n = 2$ and $r = 9$ the set of elements for the group are $e, x, x^2, x^3, x^4, y, xy, yx, x^2y$ and yx^2 which is the dihedral group D_5.

By letting $m = 3$, $n = 2$ and $r = 5$ the group D_3 is obtained which is of order 6 and is isomorphic to S_3.

For $m = 3$, $n = 2$ and $r = 1$ a group of order 6 is obtained which is Abelian. This group is isomorphic to the cyclic group of order 6.

CHAPTER V

GROUPS WITH NORMAL SERIES

5.1 NORMAL SUBGROUPS

The idea of a coset as defined in Chapter II is used here to define normal subgroup.

Definition. A subgroup H of G is a <u>normal subgroup</u> if and only if every left coset of H in G is also a right coset. The symbol H G denotes H is a normal subgroup of G.

Since every subgroup of an Abelian group is normal, the more interesting examples are non-Abelian groups with normal subgroups. The quaternion group of section 4.2 is such an example. The subset $\{1, -1, i, -i\}$ is normal in the group since the left cosets $\{i, -1, -i, 1\}$ and $\{j, k, -j, -k\}$ are also the right cosets. The subset $\{1, -1\}$ is also normal in this group with cosets $\{1, -1\}$, $\{i, -i\}$, $\{j, -j\}$ and $\{k, -k\}$.

The dihedral group D_3 of section 3.4 with subgroup $\{E, B, C\}$ is normal in D_3 with cosets $\{E, B, C\}$ and $\{H, F, G\}$.

The group $G = \{I, (12)(34), (13)(24), (14)(23)\}$ given in cycle notation is a normal subgroup of S_4, and is isomorphic to the non-cyclic group of order 4 called the 4-group.

THEOREMS ON NORMAL SUBGROUPS

5.1.1 Any subgroup of an Abelian group is normal [4;61].

5.1.2 If $n \neq 4$, A_n is the only proper normal subgroup of S_n [7;46].

5.1.3 If the order of the group divided by the order of the subgroup gives a quotient of 2, the subgroup is normal [5;26]. (This is the case in both examples given above.)

Other examples of normal subgroups will be given throughout the remainder of this chapter in the sections on nilpotent, supersolvable and solvable groups.

5.2 HAMILTONIAN GROUPS

Definition. A group is <u>Hamiltonian</u> if and only if every subgroup is normal.

Every subgroup of the quaternion group is normal and therefore Hamiltonian.

5.3 SIMPLE GROUPS

For the groups which have no normal subgroups, the following definition assigns a name.

Definition. A group G is a <u>simple group</u> if and only if it contains no proper normal subgroups.

The notable examples of simple groups are the alternating groups A_n where $n \neq 4$ as is pointed out in theorem 5.3.2 which follows.

The cyclic group of order 5 given in the table below is a simple group.

TABLE VIII

A SIMPLE GROUP OF ORDER 5

*	e	r	s	t	u
e	e	r	s	t	u
r	r	u	e	s	t
s	s	e	t	u	r
t	t	s	u	r	e
u	u	t	r	e	s

THEOREMS ON SIMPLE GROUPS

5.3.1 The finite cyclic groups of prime order are simple groups [5;26].

5.3.2 If $n \neq 4$, A_n is a simple group [7;45].

5.4 NORMAL SERIES

Definition. A <u>normal series</u> of a group G is a finite sequence $A_0,\ldots,A_r$ of proper subgroups such that $e = A_0 \lhd A_1 \lhd \ldots \lhd A_r = G$.

For the examples of groups with normal series, S_4, S_3 and D_4 are used. These same groups are to appear later as examples of types of groups which are defined in terms of conditions on finite normal series.

The subgroups which form a normal series in S_4 are given in cycle notation.

$A_4 = \{I\}$

$A_3 = \{I, (12)(34)\}$

$A_2 = \{I, (12)(34), (13)(24), (14)(23)\}$

$A_1 = \{I, (123), (124), (132), (134), (142), (143),$
$(234), (243), (12)(34), (13)(24), (14)(23)\}$

$A_o = S_4 = \{I, (12), (13), (14), (23), (24), (34), (123),$
$(124), (132), (134), (142), (143), (234),$
$(243), (12)(34), (13)(24, (14)(23),$
$(1234), (1243), (1324), (1342, (1423),$
$(1432)\}.$

The cosets of

A_4 in A_3 are $\{I\}$ and $\{(12)(34)\}$;

A_3 in A_2 are $\{I, (12)(34)\}$ and $\{(13)(23), (14)(23)\}$;

A_2 in A_1 are $\{I, (12)(34), (13)(24), (14)(23)\}$,
$\{(134), (243), (142), (123)\}$ and
$\{(234), (132), (143), (124)\}$.

A_1 in A_o are A_1 and $\{(12), (13), (14), (23), (24),$
$(34), (1234), (1243), (1324),$
$(1342), (1423), (1432)\}$.

The subgroups which form a normal series in S_3 from Table III of section 3.1. are:

$A_2 = \{P_1\}$,

$A_1 = \{P_1, P_4, P_5\}$, and

$A_o = S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$.

The cosets of

A_2 in A_1 are $\{P_1\}$, $\{P_4\}$ and $\{P_5\}$;

A_1 in A_o are $\{P_1, P_4, P_5\}$ and $\{P_2, P_3, P_6\}$.

The subgroups which form a normal series in D_4 of section 4.3. are:

$A_3 = \{e\}$,

$A_2 = \{e, s^2\}$,

$A_1 = \{e, s, s^2, s^3\}$,

$A_o = D_4 = \{e, s, s^2, s^3, t, ts, st, s^2t\}$.

The cosets of

A_3 in A_2 are $\{e\}$ and $\{s^2\}$,

A_2 in A_1 are $\{e, s^2\}$ and $\{s, s^3\}$,

A_1 in A_o are $\{e, s, s^2, s^3\}$ and $\{t, ts, st, s^2t\}$.

5.5 THE CENTER OF A GROUP

Definition. The <u>center of a group</u> G is the set of all x G that commute with every element of G.

In Abelian groups all elements commute and the set itself is the center. In some groups the only element which commutes with every other element is the identity in which case the center is said to be trivial.

The group D_4 with elements $\{e, s, s^2, s^3, t, ts, st, s^2t\}$ has a non-trivial center $\{e, s^2\}$.

From the quaternion group of section 4.2., $\{1, -1\}$ is the non-trivial center.

A helpful theorem on p-groups states, "The center of a finite p-group is greater than the identity alone" [5;47].

5.6 NILPOTENT GROUPS

The nilpotent groups are the first of three types of groups defined in terms of finite normal series.

Definition. A group G is <u>nilpotent</u> if and only if it possesses a finite normal series $G\ A_o \supseteq A_1, \supseteq A_2 \supseteq \ldots \supseteq A_r = e$, in which A_{i-1}/A_i is in the center of G/A_i for $i = 1, \ldots, r$.

The example for nilpotent groups is the group D_4. The finite normal series $A_o, \ldots, A_3$ has already been shown in section 5.4. All that remains to be shown is that each factor group A_{i-1}/A_i is in the center of the factor group G/A_i.

A_o/A_1 is in the center of G/A_1.

A_1/A_2 is in the center of G/A_2.

A_2/A_3 is in the center of G/A_3.

THEOREMS ON NILPOTENT GROUPS

5.6.1 Every subgroup of a nilpotent group G is nilpotent [7;122].

5.6.2 A finite nilpotent group is supersolvable [9;155].

5.6.3 Every finite p-group is nilpotent [7;123].

5.7 SUPERSOLVABLE GROUPS

The supersolvable groups are also defined in terms of a finite normal series.

Definition. A group G is <u>supersolvable</u> if and only if it possesses a finite normal series $G = A_o \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_r = e$, in which each factor group A_{i-1}/A_i is cyclic.

The group S_3 is an example of a supersolvable group which is not nilpotent. The factor group A_0/A_1 has elements $\{P_1\}$, $\{P_4\}$ and $\{P_5\}$ with generator $\{P_4\}$. The factor group A_1/A_2 is cyclic, has elements $\{P_1, P_4, P_5\}$ and $\{P_2, P_3, P_6\}$ with $\{P_2, P_3, P_6\}$ as generator.

THEOREMS ON SUPERSOLVABLE GROUPS

5.7.1 Subgroups and factor groups of supersolvable groups are supersolvable [9;155].

5.7.2 A finite nilpotent group is supersolvable [9;155].

5.7.3 If the order of G is $2p^n$, p a prime, G is supersolvable [9;158].

5.7.4 A supersolvable group is solvable [9;155].

5.8 SOLVABLE GROUPS

The solvable groups get their name from Galois theory. A polynomial is solvable by radicals if and only if its Galois group has a finite normal series in which every factor group of succeeding normal subgroups is Abelian.

Definition. A group G is <u>solvable</u> if and only if it possesses a finite normal series $G = A_0 \supseteq A_1 \supseteq A_2 \ldots \supseteq A_s = e$ in which every $A_{i-1}/A_i, i = 1, \ldots, s$ is Abelian.

The example of a solvable group is S_4. In section 5.4 the subgroups which make up the finite normal series are shown. To show each factor group is Abelian, the operation table for each factor group can be constructed.

THEOREMS ON SOLVABLE GROUPS

5.8.1 Any subgroup of a solvable group is solvable [7;112].

5.8.2 If $N \geq 5$, S_n is not solvable [7;114].

5.8.3 Every finite p-group is solvable [7;114].

5.8.4 Every group of odd order is solvable [8;222].

5.8.5 If $n \leq 4$, then S_n is solvable [7;114].

5.8.6 The dihedral groups are solvable [7;115].

The theorems above suggest numerous other examples of solvable groups.

5.9 THE HIERARCHY OF FINITE GROUPS

Through the use of a few theorems it is possible to show a hierarchy of classes of finite groups.

5.9.1 Every cyclic group of order n is isomorphic to the additive group $I/_{(n)}$ [6;184]. (This implies every finite cyclic group is Abelian.)

5.9.2 If G is Abelian then G is nilpotent [7;121].

5.9.3 Every finite nilpotent group is supersolvable [9;155].

5.9.4 A supersolvable group is solvable [9;155].

The theorems establish the following result:

$$\text{Cyclic groups} \subset \text{Abelian groups} \subset \text{Nilpotent groups} \subset \text{Supersolvable groups} \subset \text{Solvable groups}$$

Some examples show that each subset is proper as shown in the table below.

TABLE IX

EXAMPLES AND COUNTEREXAMPLES
OF FIVE FINITE GROUPS

CLASS	EXAMPLES					
	S_2	4-group	D_4	S_3	S_4	S_5
Solvable	Yes	Yes	Yes	Yes	Yes	No
Supersolvable	Yes	Yes	Yes	Yes	No	No
Nilpotent	Yes	Yes	Yes	No	No	No
Abelian	Yes	Yes	No	No	No	No
Cyclic	Yes	No	No	No	No	No

CHAPTER VI

CONCLUSION

6.1 SUMMARY

Several examples for each of 18 different types of groups have been listed. In addition there are theorems given relating to certain of these types of groups which enable the reader to find many other examples not listed.

In Chapter II, groups, subgroups, cosets and operations on cosets were defined for later use in the thesis.

The groups commonly encountered in a course of abstract algebra were introduced in Chapter III for a review and to supply examples for other types of groups introduced in later chapters.

Chapter IV supplies examples of groups which are defined in terms of the power of the elements of the group.

The normal subgroup was defined in Chapter V. The groups of that chapter were then defined and presented in terms of normal subgroups and normal series.

6.2 SUGGESTION FOR FURTHER STUDY

The idea of this thesis could be profitably extended to other topics of abstract algebra. Examples of vector spaces, rings or fields would be helpful to students and teachers alike. In such a topic the effectiveness could be increased by the inclusion of counter examples as well as examples.

In the study and preparation of this thesis several topics have aroused the curiosity of the writer.

1) How is an algorithm for solving a polynomial equation related to the solvability of a group associated with the polynomial equation?

2) Can group theory be studied strictly from the standpoint of generators and relations?

3) What is being accomplished in the area of semi-groups, quasi-groups and loops?

Answers to these questions could lead to very interesting studies in the field of group theory.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Adler, Irving. The New Mathematics. New York: John Wiley and Sons, Inc., 1966. 187 pp.

2. Beckman, David and Ralph Crouch. Algebraic Systems. Glenview, Ill.: Scott, Foresman and Company, 1966. 304 pp.

3. Coxeter, Harold S.M. and W.O.J. Moser. Generators and Relations for Discrete Groups. New York: Springer-Verlag, Inc., 1965. 161 pp.

4. Dean, Richard A. Elements of Abstract Algebra. New York: John Wiley and Sons, Inc., 1966. 324 pp.

5. Hall, Marshall, Jr. The Theory of Groups. New York: The Macmillan Company, 1959. 431 pp.

6. McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, Inc., 1960. 304 pp.

7. Rotman, Joseph J. The Theory of Groups: An Introduction. Boston: Allyn and Bacon, Inc., 1965. 305 pp.

8. Schenkman, Eugene. Group Theory. Princeton, New Jersey: D. Van Nostrand and Company, Inc., 1965. 289 pp.

9. Scott, William Raymond. Group Theory. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1964. 479 pp.