AN INVESTIGATION OF CAYLEY'S THEOREM
FOR FINITE GROUPS

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
Hugh Harlan Imboden
July 1967
Thesis
1989
I

Approved by Graduate Council

[Signature]

Approved by Major Department

[Signature]

255077
I wish to thank Mr. Lester Laird for suggesting the problem to me and for his assistance during the writing of the paper. I also wish to thank my wife, Rochelle, for many hours spent typing the final copy.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. PRELIMINARY IDEAS</td>
<td>3</td>
</tr>
<tr>
<td>III. THE PROBLEM FOR CYCLIC GROUPS</td>
<td>7</td>
</tr>
<tr>
<td>IV. ABELIAN GROUPS WITH TWO GENERATORS</td>
<td>16</td>
</tr>
<tr>
<td>V. CERTAIN NON-ABELIAN GROUPS</td>
<td>22</td>
</tr>
<tr>
<td>VI. CONCLUSIONS AND CONJECTURES</td>
<td>26</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>29</td>
</tr>
</tbody>
</table>
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Operation Table for the Group ( (G, o) )</td>
<td>5</td>
</tr>
<tr>
<td>II. Summary of Selected Results of Theorem 4.3</td>
<td>20</td>
</tr>
<tr>
<td>III. Selected Results of 5.1, ( n ) Even</td>
<td>24</td>
</tr>
<tr>
<td>IV. Selected Results of 5.1, ( n ) Odd</td>
<td>24</td>
</tr>
</tbody>
</table>
CHAPTER I
INTRODUCTION

In 1854, Cayley stated the following theorem.

"Every group is isomorphic to a permutation group of its elements." Scott and others show that Cayley's theorem can be stated in a slightly different way. "Let G be a group, and, for each x an element of G, let Rx be the function from G into G such that yRx = yx for all x in G. If T is defined by xT = Rx for x in G, then T is an isomorphism of G into Sym(G)." In other words, every group, G, can be shown to be isomorphic to a subgroup of the symmetric group on the elements of G. Since the statement of this theorem, there has been considerable speculation about the possibility of a given group, G, being isomorphic to a subgroup of a smaller symmetric group than the symmetric group of its elements.

The central problem of this investigation was this. Given a group, G, find the minimum positive integer, n, so that G is isomorphic to a subgroup of the symmetric group on n elements.

---

In reporting the results of this investigation, groups will be defined in terms of generators and relations. All permutations will be expressed in cycle notation. The report is restricted to finite groups.

In carrying out the investigation, the method of attack varied with the type of group under consideration. Usually, however, several concrete examples were used to suggest a general principal which was then tested and proved.

The content of succeeding chapters is as follows. Chapter II is a brief overview of some basic ideas from group theory and also establishes notation and symbolism employed in the remainder of the paper. Chapter III contains the results of the investigation pertinent to cyclic groups. Chapter IV gives a method for finding the smallest symmetric group containing a subgroup that is isomorphic to a given Abelian group with two generators. Chapter V contains the results of the investigation for certain non-Abelian groups. Chapter VI gives a summary of the more important findings and some conjectures on extending ideas developed in Chapters III, IV, and V. The Bibliography following Chapter VI lists some of the more useful publications in the area of groups.
CHAPTER II

PRELIMINARY IDEAS

An extensive knowledge of group theory, while desirable, is not essential to this report. The definition and some basic properties of groups, together with some concepts from abstract algebra, are sufficient background for the ideas presented.

A group is defined to be an ordered pair \((G, 0)\), such that \(G\) is a set, and \(0\) is an associative binary operation on \(G\), and there exists an element, \(e\), of \(G\) so that:

i) if \(a\) is in \(G\), then \(a 0 e = a\), and

ii) if \(a\) is in \(G\), then there exists \(a^{-1}\) in \(G\) such that \(a 0 a^{-1} = e\).  

The order of a group, \((G, 0)\), is the number of elements in \(G\).

A subset \(H\) of \(G\) may itself be a group with respect to the operation defined for \(G\). If so, \(H\) is a subgroup of \(G\). The theorem of Lagrange, which states that if \(G\) is a finite group and if \(H\) is a subgroup of \(G\), then the order of \(H\) divides the order of \(G\), is of considerable use in working with subgroups. For example, according to this theorem, a

\(^1\)Scott, op. cit., pp. 6-8.
group of order 20 could have subgroups of order 1, 2, 4, 5, or 10. A group of order 10, on the other hand, could not have subgroups of order 3, 4, 6, 7, 8, or 9.

A permutation of a set \( M \) is defined to be a 1-1 function from \( M \) onto \( M \).\(^2\) A permutation group, then, is a set of permutations that fulfills the minimum conditions for a group. Of the various methods of denoting permutations, the cycle notation is perhaps the simplest. The symbol \((123)(45)\) is understood to mean that permutation on the set \{1, 2, 3, 4, 5\} that maps 1 to 2, 2 to 3, 3 to 1, 4 to 5, and 5 to 4. If \( P \) and \( Q \) are permutations on some set \( G \), then if \( a \) is an element of \( G \), \( a(PQ) = (aP)Q \). (This binary operation is associative.) For example, \((123)(45) \circ (12)(345)\) is the permutation \((324)\).\(^3\)

Two groups \( G \) and \( H \) are isomorphic if and only if there exists a 1-1 mapping, \( T \), from \( G \) onto \( H \) such that if \( x \) and \( y \) are members of \( G \), then \((x \circ y)T = xT \circ yT \). That is, \( T \) is a 1-1 function that preserves operation.

There are several ways to display the elements of a group and their relationships. One method employs the operation table introduced by Cayley. For example, consider the set \( G = \{e, a, b, c, d\} \), and the operation, \( \circ \), defined

\(^2\)Ibid., pp. 8-12.

\(^3\)For a more detailed account see Neal H. McCoy, Introduction to Modern Algebra, Boston, 1960, pp. 175-176.
by Table 1, page 5. It can be easily verified that the ordered pair \((G, 0)\) satisfies the definition and is a group. The group \((G, 0)\) will be referred to as group \(G\). The group \(G\) has order five, written \(o(G) = 5\).

Another method of representing a group is to establish an isomorphism with a group whose properties are well known. For example, the integers modulus 5 under ordinary addition form a group which is isomorphic to the group in Table I.

**TABLE I**

**OPERATION TABLE FOR THE GROUP \((G, o)\)**

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
</tr>
</tbody>
</table>

A third method, and the one to be used in succeeding chapters, is to represent the group in terms of its generators and relations.

Certain elements of a finite group are called generators of the group if every element of the group can be expressed as a finite product of their powers.\(^4\) That is, if \(A\) and \(B\) generate the group \(L\), then \(x\) is an element of \(L\) implies \(x\) can be written as some finite product of their

powers, such as $x = A^2 B A B^3$. When the set of generators is restricted to a single element, the group is *cyclic*. The group of Table I can be shown to be a cyclic group of order five. Consider the group with the single generator $T$ which obeys the relation $T^5 = E$, where $E$ is the identity element of the group. This group is a cyclic group with elements $\{T, T^2, T^3, T^4, E\}$, and by means of the correspondence $a$ to $T$, $b$ to $T^2$, $c$ to $T^3$, $d$ to $T^4$, and $e$ to $E$, is isomorphic to the group of Table I.
CHAPTER III

THE PROBLEM FOR CYCLIC GROUPS

In terms of abstract definition, the simplest groups are the cyclic groups of various orders. A cyclic group is a group with the single generator $T$, such that $T^n = E$, where $n$ is a natural number. This group is denoted $C_n$ and has order $n$. Thus, the group $C_4$, defined by $T^4 = E$, is the cyclic group $\{E, T, T^2, T^3\}$ of order four. The elements of this group can also be represented by the set of permutations $\{E, (1234), (13)(24), (1432)\}$, where $T = (1234)$.

By the nature of the definition of the product of permutations, if $T^n = E$ defines a group, then a permutation that will replace $T$ could, in every case, be $(123\ldots n)$, since the only powers of this permutation that are equal to the identity are multiples of $n$.

It is relatively easy to establish the isomorphism between $C_3$ and a permutation group. By the preceding discussion, one representation of $T$ is $T = (123)$. Then $T^2 = (132)$ and $T^3 = E$ where $E$ is the identity element. Then the isomorphism can be established since it can be verified that operation is preserved under this mapping. The group $C_3$ is isomorphic to a subgroup of $S_3$ (the set of all permutations on three elements), since the isomorphism is between elements of $C_3$ and $S_3$. 
In the same manner, it can be shown that $C_4$ is isomorphic to a subgroup of $S_4$, and that $C_5$ is isomorphic to a subgroup of $S_5$. In fact, every cyclic group $C_n$ is isomorphic to a subgroup of $S_n$.

3.1 THEOREM: There exists $S$, a subgroup of $S_n$, such that $C_n$ is isomorphic to $S$.

Proof: There is an element $x$ of $S_n$ such that $x = (123...n)$ of length $n$. $(123...n)$ generates a cyclic group of order $n$ since $(123...n)^k = E$ iff $k = sn$ where $s$ is some integer. Two cyclic groups of the same order are isomorphic.\(^1\) Then $S$, generated by $(123...n)$, is isomorphic to $C_n$ and is also a subgroup of $S_n$.

The group $C_6$, according to Theorem 3.1, is isomorphic to a subgroup of $S_6$. It is also possible to express the elements of $C_6$ in such a way that an isomorphism can be shown to exist between $C_6$ and a subgroup of $S_5$. If $T = (123)(45)$, then $T^2 = (132)$, $T^3 = (45)$, $T^4 = (132)(45)$, and $T^6 = E$. Then $C_6$ is isomorphic to the cyclic subgroup of $S_5$ that is generated by $(123)(45)$.

The central concept of this chapter can be stated in the following way. If $C_n$ is a cyclic group of order $n$, where $n = a_1 x a_2 x ... x a_t$, where each $a_i$ is a power of a prime

\(^1\)Scott, Op. Cit., p. 34.
and \((a_i, a_j) = 1\) if \(i \neq j\), then \(G_n\) is isomorphic to a subgroup of \(S_{a_1+a_2+\ldots+a_t}\); also, this is the smallest symmetric group that will permit imbedding of \(G_n\).

3.2 LEMA: If \(a\) and \(b\) are natural numbers, each greater than or equal to two, then \(a + b \leq a \times b\).

Proof: Without loss of generality, let \(a \leq b\). Then \(b = a + k\) where \(k\) is some non-negative integer. Then \(a \geq 2\) implies \(a^2 \geq 2a\). Also, \(a > 1\) implies \(ak \geq k\). But then \(a^2 + ak \geq 2a + k\), which implies that \(a(a + k) \geq a + (a + k)\).

Since \(b = a + k\), then \(a + b \leq a \times b\).

3.3 LEMA: Given any finite set of \(a_i\), where each \(a_i\) is a natural number greater than one, then

\[
\sum_{i=1}^{n} a_i \leq \prod_{i=1}^{n} a_i,
\]

where \(n\) is the number of \(a_i\).

Proof: By induction on \(n\). First, \(a_1 \leq a_i\) for all \(a_i\) in the set of natural numbers. Then suppose \(a_1+a_2+\ldots+a_k \leq a_1 \times a_2 \times \ldots \times a_k\). To show that \(a_1+a_2+\ldots+a_k+a_{k+1} \leq a_1 \times a_2 \times \ldots \times a_{k+1}\), add \(a_{k+1}\) to each side of the inequality involving \(k\) terms.

Then \(\sum_{i=1}^{k+1} a_i \leq \prod_{i=1}^{k} a_i + a_{k+1}\). By 3.2, \(\prod_{i=1}^{k} a_i + a_{k+1} \leq \prod_{i=1}^{k+1} a_i\).

By the transitivity of inequality, \(\sum_{i=1}^{n} a_i \leq \prod_{i=1}^{n} a_i\). Therefore, \(\sum_{i=1}^{n} a_i \leq \prod_{i=1}^{n} a_i\) for \(n\) any natural number.

3.4 LEMA: If \(n = \prod_{i=1}^{t} a_i\), where \(a_i\) is a natural number and \((a_j, a_k) = 1\) if \(j \neq k\), and \(r = \sum_{i=1}^{t} a_i\), then if \(a_i\) is
a power of a prime, \( p_i^{\alpha_i} \), then \( r \) is minimum.

Proof: If \( a_i = p_i^{\alpha_i} \), then \( r_1 = \sum_{i=1}^{s} a_i^{\alpha_i} \). Suppose

\( a_i \neq p_i^{\alpha_i} \). Then since \( n \) has a unique prime factorization

into primes and the \( a_i \)'s must be pairwise relatively prime,

then at least one \( a_i = \prod_{k=1}^{s} p_i^{\alpha_i} \), \( s-k > 1 \). But then \( r_2 = \sum a_i \).

By \( 3.3 \), \( \sum a_i^{\alpha_i} \leq \prod p_i^{\alpha_i} \) which implies that \( r_1 \leq r_2 \) for all

\( r_2 \). Then \( r \) is minimum if \( a_i = p_i^{\alpha_i} \).

If \( P \) is a permutation so that the group defined by

\( T^n = E \) is isomorphic to the group generated by \( P \), then \( P \) is

a permutation such that if \( P^s = E \), then \( s \) is a multiple of

\( n \). If \( P \) is a single cycle of length \( n \), then \( P \) is an element

of \( S_n \) and \( C_n \) is isomorphic to a subgroup of \( S_n \). If \( n =

p_1 p_2 p_3 \), where each \( p_i \) is a power of a different prime, then

a three cycle permutation (one cycle of length \( p_1 \), one of

length \( p_2 \), and one of length \( p_3 \)), where the cycles are dis-

joint gives a permutation that generates the cyclic group of

order \( n \). Since this is true, \( C_n \) is isomorphic to a subgroup

of \( S_{p_1 p_2 p_3} \) since the generating permutation is an element

of \( S_{p_1 p_2 p_3} \).

3.5 THEOREM: If \( C_n \) is a cyclic group of order \( n \) and

if \( n = p_1 p_2 \ldots p_t \) where each \( p_i \) is a power of a different

prime, then \( C_n \) is isomorphic to a subgroup of \( S_{\sum p_i} \).
Proof: $C_n$ is generated by an element $T$ such that $T^n = E$. For every case, $C_n$ is isomorphic to a subgroup of $S_n$. Since $n$ can be factored so that each factor is some power of a different prime, then $n = \prod_{i=1}^{t} p_i$, where each $p_i$ is a power of a different prime. Then it is possible to form $t$ disjoint cycles so that one cycle has length $p_1$, one has length $p_2$, and so on to the final cycle of length $p_t$. This permutation (formed by multiplying the cycles) gives a representation of $T$ so that the only powers of the permutation that are equal to the identity element will be multiples of $n$. Using this permutation, an isomorphism can be established between $C_n$ and a subgroup of $S_{\sum_{i=1}^{t} p_i}$.

3.6 THEOREM: The symmetric group established by 3.5 is the smallest such group so that the symmetric group will permit imbedding of $C_n$.

Proof: By 3.3, if $n$ is a power of a single prime, then the shortest permutation that will generate a group of order $n$ is a one cycle permutation of length $n$. Then the minimum symmetric group that allows imbedding of $C_n$ is $S_n$. If $n$ is a number of the form $\prod_{i=1}^{t} p_i$ where each $p_i$ is a power of a different prime, then by 3.4, $\sum_{i=1}^{t} p_i$ is the minimum sum of the form required in 3.5. Then the shortest possible permutation that will generate a cyclic group isomorphic to $C_n$ is an element of $S_{\sum_{i=1}^{t} p_i}$. The symmetric group $S_{\sum_{i=1}^{t} p_i}$ is, therefore, the smallest symmetric group that permits imbed-
If $S_n$, a specific symmetric group, is given, it is possible to find cyclic subgroups of $S_n$. The following theorems give a method for finding the largest cyclic subgroup of $S_n$ under a special condition.

3.7 THEOREM: Given $r$, a natural number, the maximum $m$ so that $m = a_1 a_2$ where $r = a_1 + a_2$ and $(a_1, a_2) = 1$ is given by:

i) $\frac{r^2 - 1}{4}$ if $r$ is odd,

ii) $\frac{r^2 - 1}{4}$ if $r$ is even and $4 | r$, and

iii) $\frac{r^2 - 4}{4}$ if $r$ is even and $4 \not| r$.

Proof: i) Consider pairs of integers $a$ and $b$ such that $a + b = r$. Then $a = r - m$, $b = m$, and $a \times b = (r - m)m$. If $f(m) = (r - m)m = rm - m^2$, then, upon differentiation, $f'(m) = r - 2m$. If $r - 2m = 0$, then $m = \frac{r}{2}$, and this is a maximum since $f''(m) = -2$. However, since $r/2$ is not an integer ($r$ is odd), consider pairs of integers near $(r/2, r/2)$. The numbers $\frac{r-1}{2}$ and $\frac{r+1}{2}$ are integers with the required characteristics, since $\frac{r^2-1}{4} > \frac{r^2-9}{4} > \frac{r^2-25}{4} > \ldots$.

To show that $\frac{r+1}{2}$ and $\frac{r-1}{2}$ are relatively prime, suppose that they are not. Then $(\frac{r+1}{2}, \frac{r-1}{2}) = d \neq 1$ implies that $\frac{r+1}{2} = dp$ and $\frac{r-1}{2} = dq$ where $p$ and $q$ are integers. Then $r = 2dp - 1$ and $r = 2dq + 1$ implies that $2dp - 1 = 2dq + 1$. Then
2d(p-q) = 2 and d(p-q) = 1 and then d|1 which implies that d = 1. This contradicts the assumption that d ≠ 1; therefore, \((\frac{r+1}{2}, \frac{r-1}{2}) = 1\).

i) Given 4|r, then the maximum product occurs at (r/2, r/2). While these numbers are integers, they are not relatively prime. As before, examine pairs of numbers near (r/2, r/2). Consider \(\frac{r}{2} + 1, \frac{r}{2} - 1, \ldots\). Certainly, \(\frac{r^2}{4} - 1 > \frac{r^2}{4} - 4 > \ldots\). Then checking to see that \(r + 1\) and \(\frac{r}{2} - 1\) are relatively prime, since 4|r then \(r = 4p\), where \(p\) is some integer. To show that \((2p-1, 2p+1) = 1\), suppose instead that \((2p-1, 2p+1) = d ≠ 1\). Then there exist integers \(s\) and \(t\) so that \(2p-1 = ds\) and \(2p+1 = dt\). Then ds+2 = dt implies that \(d(s-t) = 2\) which in turn implies that \(d|2\). Then either \(d = 1\) or \(d = 2\). Since 2p-1 is odd, \(d ≠ 2\). Then \(d = 1\), but this is a contradiction of the assumption that \(d ≠ 1\). By contradiction, \(\frac{r}{2} - 1\) and \(\frac{r}{2} + 1\) are relatively prime.

ii) Given 4|r and 4|r, the maximum product occurs at (r/2, r/2). While these are integral, they are not relatively prime. Consider \(\frac{r}{2} + 1\) and \(\frac{r}{2} - 1\), since \(r\) is even but not divisible by four, \(\frac{r}{2} + 1\) and \(\frac{r}{2} - 1\) are both even and so they are not relatively prime. Now, since \(r^2/4 > r^2/4 - 1 > r^2/4 - 4 > \ldots\), then consider \(r^2/4 - 4\), given by \(r/2 + 2\) and \(r/2 - 2\). These numbers are relatively prime. To show this, suppose that \((r/2 + 2, r/2 - 2) = d ≠ 1\). Then there exist-
t and s, integers, such that \( r/2 + 2 = dt \), and \( r/2 - 2 = ds \).

This implies that \( ds + 4 = dt \) or that \( d(s-t) = 4 \) and so \( d \mid 4 \). Then either \( d = 1 \), \( d = 2 \), or \( d = 4 \). However, \( r/2 + 2 \) is odd so \( d \) must be odd and then \( d = 1 \), which contradicts the assumption that \( d \neq 1 \), and so \( (r/2 + 2, r/2 - 2) = 1 \).

3.6 THEOREM: Given \( S_n \), a) if \( n \) is odd, \( S_n \) contains \( \frac{n^2 - 1}{4} \), b) if \( n \) is even and \( 4 \mid n \), then \( S_n \) contains \( \frac{n^2 - 1}{4} \), and c) if \( n \) is even and \( 4 \nmid n \), \( S_n \) contains \( \frac{n^2 - 1}{4} \).

Proof: a) Let \( n \) be odd and let \( e \) be an element of \( S_n \). Then each \( e \) is a permutation of length less than or equal to \( n \) and consisting of disjoint cycles. Then some \( e_p \) consists of two disjoint cycles (cycle I and cycle II) such that the order of I is \( \frac{n+1}{2} \), the order of II is \( \frac{n-1}{2} \). Then the order of their product is \( \frac{n^2 - 1}{4} \) and \( S_n \) contains \( \frac{n^2 - 1}{4} \). Further, this is the largest cyclic group in \( S_n \) generated by a two cycle permutation. To show this, the following argument could be employed. Given \( B \), a permutation from \( S_n \), such that \( B \) has two cycles (for example, in \( S_4 \), \( B \) might be \( (13)(24) \)) and the two cycles together contain all \( n \) elements, then \( B \) is a generator of a cyclic group. If the lengths of the two cycles are relatively prime integers, then by 3.7, the largest cyclic group generated by a two cycle permutation from \( S_n \) will be generated by the permu-
tation with cycles of length \( \frac{n-1}{2} \) and \( \frac{n+1}{2} \).

b) Let \( n \) be even and \( 4 \mid n \), and let \( e \) be an element of \( S_n \). Then each \( e \) is a permutation consisting of disjoint cycles and \( e \) is of length \( n \) or less. Then some \( e_r \) is a product of two disjoint cycles (cycle I and cycle II) such that the order of I is \( \frac{n}{2} - 1 \) and the order of II is \( \frac{n}{2} + 1 \) and the order of the cyclic group generated by \( e_r \) is \( \frac{n^2}{4} - 1 \). Then \( S_n \) contains \( C_2 \) if \( 4 \mid n \). The same type of argument as in a) will show that \( C_2 \) is the largest cyclic subgroup generated by a two cycle permutation from \( S_n \).

c) Let \( n \) be even but not divisible by four, and let \( e \) be an element of \( S_n \). Then some \( e_q \) is a permutation consisting of two disjoint cycles (I and II) such that the order of I is \( \frac{n}{2} - 2 \) and the order of II is \( \frac{n}{2} + 2 \). The degree of \( e_q \) is \( \frac{n^2}{4} - 4 \). Once again, by 3.7, this is seen to give the largest cyclic subgroup generated by a two cycle permutation of \( S_n \).

In terms of the central problem of this investigation, Theorems 3.5 and 3.6 are the important concepts in this section. They give a general rule for finding the minimum symmetric group that will permit imbedding of a given cyclic group.
CHAPTER IV

ABELIAN GROUPS WITH TWO GENERATORS

Abelian groups are those groups with the property that the elements of the group are commutative with respect to the operation. This chapter will deal with Abelian groups generated by two elements $R$ and $T$ such that $R^m = T^n = E$ where $RT = TR$.

If $G$ and $H$ are groups, then the direct product of $G$ and $H$ is:

$$G \times H = \{(R, T) | R \text{ is in } G \text{ and } T \text{ is in } H\}.$$ 

As an example, the group $C_3 \times C_2$, where $C_3$ is generated by $R$ such that $R^3 = I$ and $C_2$ is generated by $T$ such that $T^2 = I$, has elements $\{(I, I), (R, I), (R^2, I), (R, T), (R^2, T), (I, T)\}$. The order of a group formed by the direct product of groups of orders $m$ and $n$ is $mn$.

Two theorems will be used without proof in this chapter. Their proofs can be found in the sources cited.

4.1 THEOREM: Every Abelian group is the direct product of cyclic groups whose orders are powers of primes.\(^1\)

4.2 THEOREM: The direct product of cyclic groups of orders $p$ and $q$ is an Abelian group of order $pq$ which is

cyclic if $p$ and $q$ are relatively prime. 

4.3 Theorem: If $A$ is an Abelian group generated by $R$ and $T$ such that $R^m = T^n = I$, $RT = TR$, then $A$ is isomorphic to the group $C_m \times C_n$ where $C_m$ is generated by $R$ such that $R^m = I$ and $C_n$ is generated by $T$ such that $T^n = I$.

Proof: The group $A$ has elements \{I, RT, R^2T, ..., R^{m-1}T, RT, R^2T, ..., R, R^2, ..., R^{m-1}, T, T^2, ..., T^{n-1}\}. The elements of $C_m \times C_n$ are \{(I, I), (R, T), (R^2, T), ..., (R^{m-1}, T), (R, T^2), (R, T^3), ..., (R, T^{n-1}), (R^2, T^2), (R^2, T^3), ..., (R^2, I), (R, I), (R^2, I), ..., (R^{m-1}, I), (I, T), (I, T^2), ..., (I, T^{n-1})\}. If $(A, B)$ and $(C, D)$ are in $C_m \times C_n$, then $(A, B)(C, D) = (AC, BD)$. If $F$ is a function from $A$ to $C_m \times C_n$ such that $(R^pT^q)F = (R^p, T^q)$, then $F$ is 1-1 and onto. Also, since $R^pT^qR^xT^y = R^{p+x}T^{q+y}$, then $(R^pT^q)(R^xT^y)F = (R^{p+x}, T^{q+y}) = (R^p, T^q)o(R^x, T^y) = (R^pT^q)o(R^xT^y)F$. Since $F$ preserves operation, $F$ is an isomorphism from $A$ onto $C_m \times C_n$.

The shortest permutation that will generate a cyclic group of a given order is a product of disjoint cycles. By 4.3, each element of $C_m \times C_n$ can be expressed as the product of the permutations that generate $C_m$ and $C_n$. Then each element of $C_m \times C_n$ can be expressed as the product of pairwise disjoint cycles. For example, if $A$ is the group

---

generated by $R$ and $T$ such that $R^4 = T^2 = I$, $RT = TR$, then $A$ is isomorphic to $C_4 \times C_2$. Theorem 3.5 gives the shortest permutation that will generate $C_4$, $(abcd)$, and the shortest permutation that will generate $C_2$, $(ef)$. The group elements can be expressed as $\{I, (abcd), (ac)(bd), (adcb), (ef), (abcd)(ef), (ac)(bd)(ef), (adcb)(ef)\}$. Then every element of $A$ can be represented as an element of $S_6$ and $A$ is isomorphic to a subgroup of $S_6$.

The group $A$ generated by $R$ and $T$ such that $R^{12} = T^{15} = I$ where $RT = TR$ is isomorphic to the group $C_{12} \times C_{15}$. By 4.2, $C_{12}$ is isomorphic to $C_4 \times C_3$ and $C_{15}$ is isomorphic to $C_5 \times C_3$. Then the group can be expressed as $C_4 \times C_3 \times C_5 \times C_3$ and, using 3.7, the shortest generating elements for $C_4$, $C_5$, and $C_3$ can be found. Since the permutations used to generate each of the four cyclic groups must be pairwise disjoint, then, by 4.3, every element of $A$ can be expressed as a permutation of length fifteen or less, and there is at least one element of length fifteen. Then $S_{15}$ is the smallest symmetric group containing a subgroup isomorphic to the given group.

4.4 Theorem: If $A$ is an Abelian group generated by $R$ and $T$ such that $R^m = T^n = I$, $RT = TR$, then $A$ is isomorphic to a subgroup of $S \sum_{i=1}^{s} a_i + \sum_{i=1}^{k} b_i$ where $m = \prod_{i=1}^{s} a_i$ and $n = \prod_{i=1}^{k} b_i$ where each $a_i$ is a power of a different prime and each $b_i$ is a power of
a different prime.

Proof: By 4.3, $A$ is isomorphic to $C_m \times C_n$. By 4.1 and 4.2, since $m = \prod_{i=1}^{t} a_i$ and $n = \prod_{i=1}^{t} b_i$, then $A$ is isomorphic to the direct product $C_{a_1} \times C_{a_2} \times \cdots \times C_{a_t} \times C_{b_1} \times \cdots \times C_{b_t}$. By 3.5, the shortest permutation that will generate a cyclic group of order $a_i$, where $a_i$ is a power of a prime, is a single cycle of length $a_i$. Then since all generating permutations of the cyclic groups are disjoint, each element of $A$ will be a permutation on $\sum_{i=1}^{t} a_i + \sum_{i=1}^{t} b_i$ elements. $A$ is then isomorphic to a subgroup of $S_\sum_{i=1}^{t} a_i + \sum_{i=1}^{t} b_i$.

Table II shows selected results of this theorem. The groups whose definitions are followed by a $\Delta$ are cyclic groups. (See Ch. III).

4.5 THEOREM: Theorem 4.4 gives the minimum symmetric group containing a subgroup isomorphic to a given Abelian group with two generators.

Proof: By contradiction. Suppose $A$ is isomorphic to a subgroup of $S_q$, where $q < \sum_{i=1}^{t} a_i + \sum_{i=1}^{t} b_i$. Then $A$ has no element of length $\sum_{i=1}^{t} a_i + \sum_{i=1}^{t} b_i$. But, since all $C_{a_i}$ and $C_{b_i}$ are generated by permutations that are disjoint, then at least one element of $A$ has length $\sum_{i=1}^{t} a_i + \sum_{i=1}^{t} b_i$. Therefore, $S_{\sum_{i=1}^{t} a_i + \sum_{i=1}^{t} b_i}$ is the smallest symmetric group containing a subgroup isomorphic to $A$.

As an example of 4.5, in the group $A$ generated by $R$
# TABLE II

SUMMARY OF SELECTED RESULTS OF THEOREM 4.3

<table>
<thead>
<tr>
<th>Abstract Definition</th>
<th>Factorization</th>
<th>Sum of Powers of Primes</th>
<th>Order of Smallest Symmetric Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A^2 = B^2 = I, AB = BA$</td>
<td>$m = 2$  $n = 2$</td>
<td>$2+2 = 4$</td>
<td>$4$  $S_4$</td>
</tr>
<tr>
<td>$A^6 = B^3 = I, AB = BA$</td>
<td>$m = 3x2$  $n = 3$</td>
<td>$3+2+3 = 8$</td>
<td>$18$  $S_8$</td>
</tr>
<tr>
<td>$A^{12} = B^{15} = I, AB = BA$</td>
<td>$m = 4x3$  $n = 5x3$</td>
<td>$4+3+5+3 = 15$</td>
<td>$180$  $S_{15}$</td>
</tr>
<tr>
<td>$A^{10} = B^{15} = I, AB = BA$</td>
<td>$m = 5x2$  $n = 5x3$</td>
<td>$5+2+5+3 = 15$</td>
<td>$150$  $S_{15}$</td>
</tr>
<tr>
<td>$A^3 = B^2 = I, AB = BA$</td>
<td>$m = 3$  $n = 2$</td>
<td>$3+2 = 5$</td>
<td>$6$  $S_5$</td>
</tr>
<tr>
<td>$A^{20} = B^{21} = I, AB = BA$</td>
<td>$m = 5x4$  $n = 7x3$</td>
<td>$5+4+7+3 = 19$</td>
<td>$420$  $S_{19}$</td>
</tr>
<tr>
<td>$A^{48} = B^{66} = I, AB = BA$</td>
<td>$m = 3x2^4$  $n = 11x3x2$</td>
<td>$3+16+11+3 = 31$</td>
<td>$3168$  $S_{35}$</td>
</tr>
</tbody>
</table>
and $T$ such that $R^{20} = T^{36} = I$, $RT = TR$, represented by $C_{20} \times C_{36} = C_4 \times C_5 \times C_9 \times C_4$, the generating permutations for each of the four cyclic groups must be disjoint so that $A$ is Abelian. By inspection of the elements of $A$, one element is formed by the product of the four generating permutations. This element must have length $4 + 5 + 9 + 4 = 22$, and so $S_{22}$ is the smallest symmetric group that has a subgroup isomorphic to $A$. 
CHAPTER V

CERTAIN NON-ABELIAN GROUPS

The groups generated by two elements $R$ and $T$ such that $R^n = T^2 = (RT)^2 = I$ where $n > 2$ are non-Abelian groups of order $2n$. These groups, denoted by $R_n$, are called dihedral groups if $n$ is even, and metacyclic if $n$ is odd.

The group generated by $R$ and $T$ such that $R^4 = T^2 = (RT)^2 = I$ is the group with elements \{ $R, R^2, R^3, T, RT, R^2 T, R^3 T, I$ \}. Thus, $R_4$ is a group of order eight and is, by Cayley’s theorem, isomorphic to a subgroup of $S_6$. However, if $R = (1234)$ and $T = (14)(23)$, then $RT = (13)(24)$, and since $R^4 = (1234)^4 = I$, $T^2 = [(14)(23)]^2 = I$, and $(RT)^2 = [(13)(24)]^2 = I$, the group has elements \{ $(1234)$, $(13)(24)$, $(1432)$, $(14)(23)$, $(13)$, $(12)(34)$, $(24)$, $I$ \} corresponding (in the same order) to the elements of the group above. Then $R_4$ is isomorphic to the group generated by $(1234)$ and $(14)(23)$, and $R_4$ is isomorphic to a subgroup of $S_4$.

If $G$ is a group of order eight and $G$ is isomorphic to group $H$, then $o(H) = 8$. The smallest integer $n$ so that $8 | n!$ is four, so by Lagrange’s theorem, four is the smallest integer $n$ such that $R_4$ is isomorphic to a subgroup of $S_n$.

The group generated by $R$ and $T$ where $R^6 = T^2 = (RT)^2 = I$, denoted by $R_6$, is a group of order twelve and is isomorphic
to a subgroup of $S_{12}$. However, if $R=(123456)$ and $T=(16)(25)(34)$, then $RT=(15)(24)$. Since $(123456)^6=I$, $[(16)(25)(34)]^2=I$, and $[(15)(24)]^2=I$, then $R_6$ is isomorphic to a subgroup of $S_6$. $S_6$ is not the smallest symmetric group with a subgroup isomorphic to $R_6$. If $R=(123)(45)$ and $T=(13)$, then $R^2=(132)$, $R^3=(45)$, ..., $R^6=I$, ..., $T^2=I$, ..., $RT=(12)(45)$, $(RT)^2=I$. Thus the group $R_6$ is isomorphic to a subgroup of $S_6$.

5.1 THEOREM: If $R_n$ is a group with generators $R$ and $T$ such that $R^n=T^2=(RT)^2=I$, then $R_n$ is isomorphic to a subgroup of $S_n$.

Proof: Case 1. If $n$ is even, let $R=(a_1a_2...a_n)$ and $T=(a_1a_n)(a_2a_{n-1})...(a_{n/2}a_{n/2+1})$. Then $RT=(a_1a_{n-1})(a_2a_{n-2})...(a_{n/2-1}a_{n/2+1})$. Every element of $R_n$ is isomorphic to a subgroup of $S_n$. (Table III gives some specific results of 5.1 for $n$ even.)

Case 2. If $n$ is odd, let $R=(a_1a_2...a_n)$ and $T=(a_1a_{n-1})(a_2a_{n-2})...(a_{n-1}a_{n-1})$. Then $RT=(a_1a_{n-2})(a_2a_{n-3})...(a_{n-3}a_{n+1})(a_{n-1}a_n)$. Every element of $R_n$ can then be represented as an element of $S_n$, and $R_n$ is isomorphic to a subgroup of $S_n$. (Table IV gives some results of 5.1 for $n$ odd.)

5.2 THEOREM: If $R_n$ is the group generated by $R$ and $T$ such that $R^n=T^2=(RT)^2=I$, then if $n$ is prime, $S_n$ is the smallest symmetric group containing a subgroup isomorphic to $R_n$. 
### TABLE III

**SELECTED RESULTS OF 5.1, n EVEN**

<table>
<thead>
<tr>
<th>Order</th>
<th>Abstract Definition</th>
<th>Cyclic Decomposition</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>$R^4 = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(1234)$ $T=(14)(23)$ $RT=(13)$</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>$R^6 = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(123456)$ $T=(16)(25)(34)$ $RT=(15)(24)$</td>
<td>6</td>
</tr>
<tr>
<td>16</td>
<td>$R^8 = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(12345678)$ $T=(18)(27)(36)$ $RT=(17)(26)(35)$</td>
<td>8</td>
</tr>
<tr>
<td>20</td>
<td>$R^{20} = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(a_1a_2\ldots a_{10})$ $T=(a_1a_{10})\ldots (a_5a_6)$ $RT=(a_1a_9)\ldots (a_4a_6)$</td>
<td>10</td>
</tr>
</tbody>
</table>

### TABLE IV

**SELECTED RESULTS OF 5.1, n ODD**

<table>
<thead>
<tr>
<th>Order</th>
<th>Abstract definition</th>
<th>Cyclic Decomposition</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$R^3 = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(123)$ $T=(12)$ $RT=(23)$</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>$R^5 = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(12345)$ $T=(14)(23)$ $RT=(13)(45)$</td>
<td>5</td>
</tr>
<tr>
<td>14</td>
<td>$R^7 = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(1234567)$ $T=(16)(25)(34)$ $RT=(15)(24)(67)$</td>
<td>7</td>
</tr>
<tr>
<td>30</td>
<td>$R^{15} = T^2 = (RT)^2 = \mathbb{E}$</td>
<td>$R=(a_1a_2\ldots a_{15})$ $T=(a_1a_{14})\ldots (a_7a_8)$ $RT=(a_1a_{13})\ldots (a_{14}a_{15})$</td>
<td>15</td>
</tr>
</tbody>
</table>
Proof: If \( n \) is prime, then by 5.1, \( S_n \) contains a subgroup that is isomorphic to \( R_n \). Suppose there exists some integer \( m \) such that \( m < n \) where \( R_n \) is isomorphic to a subgroup of \( S_m \). Since \( \sigma(R_n) = 2n \), then by Lagrange's theorem, \( 2n | m! \), and so \( n | \frac{m^!}{2} \). Suppose \( n | \frac{m^!}{2} \), then \( n \) is a product of integers less than or equal to \( m \). Since \( n \) is prime, then \( n \) is not a product of integers. Further, \( n \) is not a single integer less than or equal to \( m \) since \( m < n \). Therefore, the statement that \( n | \frac{m^!}{2} \) is false and \( n \) is the smallest integer so that \( S_n \) contains a subgroup isomorphic to \( R_n \).
CHAPTER VI

CONCLUSIONS AND CONJECTURES

This paper contains the results of an investigation of Cayley's theorem. The investigation was restricted to selected finite groups. The most important conclusions are the following.

If \( C_n \) is a cyclic group of order \( n \), then the smallest \( m \) such that \( S_m \) contains a subgroup isomorphic to \( C_n \) is obtained by adding the factors of the prime factorization of \( n \). Thus, \( C_{60} \) is isomorphic to a subgroup of \( S_{12} \) since \( 60 = 2^2 \times 3 \times 5 \) and \( 4 + 3 + 5 = 12 \).

If \( A \) is an Abelian group generated by two elements \( R \) and \( T \) such that \( R^n = T^m = I \), \( RT = TR \), then the smallest \( q \) so that \( S_q \) contains a subgroup isomorphic to \( A \) is the sum of the factors in the prime factorization of \( n \) and \( m \).

If \( R_n \) is a group generated by \( R \) and \( T \) such that \( R^n = T^2 = (RT)^2 = I \), then \( R_n \) is isomorphic to a subgroup of \( S_n \). If \( n \) is prime, then \( S_n \) is the smallest symmetric group containing a subgroup isomorphic to \( R_n \).

Some conjectures that could furnish material for further study are:

1. If \( A \) is an Abelian group generated by \( A_1, A_2, \ldots, A_r \) where \( A_1^n = A_2^n = \ldots = A_r^n = I \), \( A_i A_j = A_j A_i \), then the sum of the prime factorization of \( m, n, \ldots, z \) gives the minimum
q so that $S_q$ is the smallest symmetric group containing a
subgroup isomorphic to $A$.

2. If $R_n$ is a group generated by $R$ and $T$ such that
$R^n = T^2 = (RT)^2 = I$ and $n$ is not prime, then the smallest $m$
so that $S_m$ contains a subgroup isomorphic to $R_n$ is the sum
of the factors in the prime factorization of $n$. 
BIBLIOGRAPHY
BIBLIOGRAPHY


