RINGS ASSOCIATED WITH FINITE ABELIAN GROUPS

A Thesis

Presented to

the Department of Mathematics

The Kansas State Teachers College of Emporia

In Partial Fulfillment of

the Requirements for the Degree

Master of Arts

by

L. Jay Butler

May 1971

Marion P. Emerson

Approved for the Mathematics Department

Approved for the Graduate Council

ACKNOWLEDGEMENTS

I would like to thank my wife, Donna, for her work at the typewriter, her lonely hours, and her courage throughout the preparation of this paper. I would like to thank Dr. Marion Emerson for his insight and for his confidence in me.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

The purpose of this paper is to examine the relationship between finite Abelian groups and rings associated with those groups. This paper will consider only finite groups, and since rings by definition are commutative with respect to the additive binary operation the group must be Abelian. A group is a set of elements together with a binary operation that exhibits certain properties: closure, associativity, identity, and inverses. Every ring must exhibit all of those properties. Groups and rings are thus closely related. They are so closely related that a ring is often defined in part in terms of a commutative group. With respect to the additive binary operation the elements of a ring are isomorphic to some commutative group. It is in this manner that rings may be associated with Abelian groups.

Looking at this association from the reverse point of view presents the problem. Given any finite Abelian group, are there rings associated with it? Is there one ring associated with the given group? If there is at least one, how many are there? How can we find them, and are we able to find all of them?

The problem may be stated in this form. List all of the distinct finite rings whose elements, with respect to the additive binary operation, are isomorphic to a given finite Abelian group. A ring is distinct if it is not isomorphic to some previously listed ring.

The thesis will be organized in this fashion. The remainder of this chapter will identify part of the notation and define terms. The second chapter will state and prove the three basic theorems of the thesis. The theorems will be those concerning the zero ring, the ring of endomorphisms, and the specific ring isomorphism theorem. Chapter three will examine more closely finite Abelian groups. Chapter three also will define new notation to facilitate working with endomorphisms on commutative groups. Chapter four will show the method for listing the rings and determining which are isomorphic. The fifth chapter will give a few more complicated examples, and the sixth chapter is a conclusion and summary.

As a general rule the set of elements of the given group will be represented by an upper case letter G. Rings as sets will be represented by upper case letters R with various subscripts for additional identification. Elements of rings on groups will be represented by lower case letters. Endomorphisms will be represented by upper case letters other than G or R. The algebraic notation $\langle G, ^{+} \rangle$, and $\langle R, ^{+\cdot} \rangle$ will be adopted for use throughout this report. $\langle R, ^{+\cdot} \rangle$ is an algebraic structure with a set of elements R and two binary operations on those elements denoted by + and $\cdot$. Other notation may be generated in the course of this report and will be specifically identified.

DEFINITION: A homomorphism is a mapping A: $G \rightarrow H$ from a group G to a group H that preserves the operation of G. That is, if * and $\cdot$ are the operations of G and H respectively, then A preserves the operation of G if, for all a and b in G it is true that $(a * b) A =$ $(aA) \cdot b(A)$. An isomorphism is a 1-1 homomorphism of G onto H. [1, p.33]

DEFINITION: A group $\langle G,+\rangle$ is a non-empty set $G = \{a,b,c,\ldots\}$ together with a binary operation (which will be referred to as the additive binary operation) such that:

1. $+$ is closed, i.e., for all a and b in G, $a + b$ is in G.

2. $+$ is associative, i.e., for any a, b, c in G, $a + (b + c) = (a + b) + c$.

3. There is an identity element 0 in G such that for all a in G, $a + 0 = 0 + a = a$.

4. For each a in G, there exists an inverse element $-a$ in G such that $a + (-a) = (-a) + a = 0$.

5. For all a, b in G, $a + b = b + a$. [1, p.17]

DEFINITION: A group $\langle G,+\rangle$ is cyclic if there is an element a in G such that for any b in G there is some integer n such that $b = na$ (where na means the n-fold addition of a). Such an element is called a generator of the cyclic group. [1,p.26]

DEFINITION: A ring $\langle R,+\cdot\rangle$ is a non-empty set R, together with two binary operations, called addition and multiplication and written $+$ and $\cdot$ respectively, such that for any a, b, c in R:

1. $a + b$ is in R and $a \cdot b$ is in R.

2. $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

3. There is an element 0 in R such that $a + 0 = 0 + a = a$.

4. There is $(-a)$ in R such that $a + (-a) = (-a) + a = 0$.

5. $a + b = b + a$.

6. $(b + c)a = ba + ca$ and $a(b + c) = ab + ac$. [1, p.77]

DEFINITION: An endomorphism is a homomorphism of G into G. [1, p.33]

DEFINITION: An isomorphism of G onto G is called an automorphism. [1, p.33]

DEFINITION: Let R and S be rings. A mapping $A : R \to S$ of R is called a ring homomorphism if, for any x and y in R,

$$(x + y)A = xA + yA \qquad (x \cdot y)A = (xA) \cdot (yA).$$

If for any s in S, $xA = s$ for some x in R, then A is said to be a homomorphism of R onto S. If also, $sA = yA$ implies $S = y$, then A is an isomorphism of R onto S. [1, p.89]

The commutative property in the definition of a group was included intentionally. When this paper now identifies a group, it will be commutative by definition. Since it has already been stated that only finite groups are in consideration, any group mentioned will be finite and Abelian.

In this thesis the rings associated with groups will be restricted to only those rings that have one element that is not a zero divisor. The need for this restriction will become clear in chapter two. Every ring is now assumed to have one element that is not a zero divisor.

Chapter 2

THE RING OF ENDOMORPHISMS

Given an Abelian group $\langle G,^{+}\rangle$ the most obvious question is, does there exist at least one ring associated with it? The term associated is now used to mean the isomorphism between the group and the ring with respect to addition. The proof that there is one ring associated with every Abelian group is given here.

THEOREM 2.1. For any Abelian group $\langle G,^{+}\rangle$, there exists a ring $\langle G,^{+}\,\cdot\rangle$ with the second binary operation $\cdot$ defined for any x and y in G as $x \cdot y = 0$ where 0 is the additive identity in $\langle G,^{+}\rangle$. This ring is called the zero ring.

Proof: Given any Abelian group $\langle G,^{+}\rangle$. Define a binary operation $\cdot$, as $x \cdot y = 0$ for all x and y in G. Since $\langle G,^{+}\rangle$ is a group it is not necessary to demonstrate those properties for addition.

1. For any x and y in G, $x \cdot y = 0$ and 0 is in G. Therefore $\cdot$ is closed in G.

2. For any x, y, and z in G $x \cdot (y \cdot z) = x \cdot 0 = 0 = 0 \cdot z = (x \cdot y) \cdot z$ and $\cdot$ is associative.

3. For any x, y, and z in G $(y + z) \cdot x = 0 = 0 + 0 = y \cdot x + z \cdot x$; also $x \cdot (y + z) = 0 = 0 + 0 = x \cdot y + x \cdot z$ and $\cdot$ distributes over +.

$\langle G,^{+}\rangle$ is a ring, thus for any Abelian group there always exists at least one ring, the zero ring. It should be noted that every zero ring is similar, differing only in the number of elements and the additive nature of the group. In this respect it is a trivial exercise.

Having shown that there is one ring associated with every group, it now remains to list all others. If the given group is cyclic of order n, then it is isomorphic to the integers modulo n. In this case the integers modulo n have a multiplicative binary operation already defined on them, and they form a ring. This method of arbitrarily searching for multiplicative operations is not in order since it would not be known whether all the rings had been listed.

Turning to another method, it will be shown that, given a group $\langle G,^{+}\rangle$, the set R of endomorphisms on that group form a ring. Accomplishing that, it must be demonstrated that this ring of endomorphisms generates all the rings in that group.

THEOREM 2.2. The set R of endomorphisms on a finite Abelian group $\langle G,^{+}\rangle$ with operations,

$x(A \oplus B) = xA + xB$ and
$x(A \odot B) = (xA)B$ for all x in G, where A and B are elements of R, forms a ring with unity, $\langle R, \oplus \odot\rangle$.

Proof: To prove this it is necessary to show the five group properties: closure, associativity, identity, commutativity and inverse hold for $\oplus$. Closure is the most important since the other properties hinge on closure for $\oplus$ and the corresponding properties of $\langle G,^{+}\rangle$. In addition closure, associativity and identity for $\odot$, and that $\odot$ distributes over $\oplus$, must be proved.

To show closure for $\oplus$, it must be proven that for all elements of $\langle G,^{+}\rangle$, the image of the sum of any two elements of $\langle G,^{+}\rangle$ is equal to the sum of the images.

By definition, for x, y in G and A, B in R, $(x + y)(A \oplus B) = (x + y)A + (x + y)B$, and by the properties of an endomorphism $(x + y)A + (x + y)B = xA + yA + xB + yB$. Since xA, yA, xB and yB are all elements of $\langle G, ^+\rangle$, they are commutative and $xA + yA + xB + yB = xA + xB + yA + yB$. By definition $xA + xB + yA + yB = x(A \oplus B) + y(A \oplus B)$. The image of the sum is equal to the sum of the images. $A \oplus B$ is an endomorphism and $\oplus$ is closed.

For A, B, and C in R, $x((A \oplus B) \oplus C) = x(A \oplus B) + xC$ and $x(A \oplus B) + xC = (xA + xB) + xC$. The elements xA, xB, and xC belong to $\langle G, ^+\rangle$ thus $(xA + xB) + xC = xA + (xB + xC)$ and $xA + (xB + xC) = xA + x(B \oplus C) = x(A \oplus (B \oplus C))$ and $\oplus$ is associative.

Consider a mapping E such that for all x in G, $xE = 0$ where 0 is the identity in G. Then $(x + y)E = 0 = 0 + 0 = xE + yE$ and E is an endomorphism. For $A \in R$, $x(E \oplus A) = xE + xA = 0 + xA$ and since 0 and xA are elements of $\langle G, ^+\rangle$, $0 + xA = xA$. E is the identity for $\oplus$.

For $A \in R$, let $x(-A) = (-xA)$ for all x in G. Then $(x + y)(-A) = (-(x + y)A) = ((-x-y)A) = (-xA) + (-yA)$ by the properties of an endomorphism. $(-xA) + (-yA) = x(-A) + y(-A)$ by definition, and $-A$ is an endomorphism. Then $x(A \oplus (-A)) = xA + x(-A)$ and $xA + x(-A) = xA + (-xA) = xA + (-x)A = (x + (-x))A = 0A = E$ and $(-A)$ is an inverse for A.

For all x in G, $x(A \oplus B) = xA + xB$. xA and xB are elements of $\langle G, ^+\rangle$ and are commutative, thus $xA + xB = xB + xA$ and $xB + xA = x(B \oplus A)$. $x(A \oplus B) = x(B \oplus A)$ and $\oplus$ is commutative.

Consider the operation $\odot$. $(x + y)(A \odot B) = ((x + y)A)B$ by definition and $((x + y)A)B = (xA + yA)B$ by the properties of an endomorphism. $(xA + yA)B = (xA)B + (yA)B$ by the properties of an endomorphism, and $(xA)B + (yA)B = x(A \odot B) + y(A \odot B)$ by definition. The image of the sum is equal to the sum of the images, $A \odot B$ is an endomorphism, and $\odot$ is closed.

For all x in G, $x((A \odot B) \odot C) = (x(A \odot B))C = ((xA)B)C$ by definition. Also $x(A \odot (B \odot C)) = (xA)(B \odot C) = ((xA)B)C$ by definition, thus $x((A \odot B) \odot C) = x(A \odot (B \odot C))$ and $\odot$ is associative.

Consider a mapping I: $G \to G$, such that for all $x \in G$, $xI = x$. Then $(x + y)I = x + y = xI + yI$ and I is an endomorphism. For $A \in R$, $x(A \odot I) = (xA)I$ and $(xA)I = xA$ since $xA \in G$. Also $x(I \odot A) = (xI)A = xA$. Therefore I is the unity element for R.

Finally for all x in G, $x(A \odot (B \oplus C)) = (xA)(B \oplus C)$ by the definition of $\odot$ and closure for $\oplus$. By definition $xA(B \oplus C) = (xA)B + (xA)C$ and $(xA)B + (xA)C = x(A \odot B) + x(A \odot C)$, and $x(A \odot B) + x(A \odot C) = x\left[(A \odot B) \oplus (A \odot C)\right]$. Also $x((A \oplus B) \odot C) = (x(A \oplus B))C$ by definition, and $(x(A \oplus B))C = (xA + xB)C = (xA)C + (xB)C$. Thus by definition $(xA)C + (xB)C = x(A \odot C) + x(B \odot C) = x\left[(A \odot C) \oplus (B \odot C)\right]$ and $\odot$ distributes over $\oplus$.

$\langle R, \oplus \odot \rangle$ is a ring with unity.

That the ring of endomorphisms is related to each of the rings associated with a given Abelian group must be proved. The next theorem shows that every ring is isomorphic to a ring of endomorphisms on its own elements. The importance of this is that if a ring is isomorphic to a set of endomorphisms of its own elements then it is a subring of the ring of endomorphisms generated by the additive group of its own elements.

THEOREM 2.3. Every finite ring $\langle R, + \cdot \rangle$ is isomorphic to a ring of endomorphism on $\langle R, + \rangle$.

Proof: Since the additive group $\langle R, + \rangle$ is part of the ring $\langle R, + \cdot \rangle$, it is possible to define mappings from R to R and use cautiously the properties of $\langle R, + \rangle$ and $\langle R, + \cdot \rangle$. Having defined the mappings from R to R, it will be shown that these mappings are endomorphisms.

For each a in $\langle R, + \cdot \rangle$ define a mapping A_a: $R \to R$ by $xA_a = x \cdot a$ for all x in $\langle R, + \rangle$. For x and y in $\langle R, + \rangle$, $(x + y)A_a = (x + y) \cdot a$, but since x and y are in $\langle R, + \rangle$ they are also in $\langle R, + \cdot \rangle$. By the distributive property of $\langle R, + \cdot \rangle$, $(x + y) \cdot a = x \cdot a + y \cdot a$, $x \cdot a + y \cdot a = xA_a + yA_a$, thus $(x + y)A_a = xA_a + yA_a$, and the image of the sum of any two elements of $\langle R, + \rangle$ is equal to the sum of the images. A_a is an endomorphism.

Let R^1 be the set of all endomorphisms of the above form. Then with operations $\oplus$ and $\odot$ as defined in Theorem 2.2., if R^1 is closed with respect to $\oplus$ and $\odot$, then R^1 is a ring $\langle R^1, \oplus \odot \rangle$.

For all x in $\langle R, + \rangle$ and a, b in R, $x(A_a \oplus A_b) = xA_a + xA_b = x \cdot a + x \cdot b$ by definition. But for all x in $\langle R, + \rangle$, x is also in $\langle R, + \cdot \rangle$ and $\langle R, + \cdot \rangle$ has the distributive property. $x \cdot a + x \cdot b = x \cdot (a + b) = xA_c$ where $a + b = c \in \langle R, + \cdot \rangle$. $\oplus$ is closed in R^1.

For all x in $\langle R, + \rangle$ and a, b in $\langle R, + \cdot \rangle$, $x(A_a \odot A_b) = (xA_a)A_b = (x \cdot a)A_b = (x \cdot a) \cdot b$. But for all x in $\langle R, + \rangle$, x is also in $\langle R, + \cdot \rangle$ and $(x \cdot a) \cdot b = x \cdot (a \cdot b) = xA_d$ where $a \cdot b = d \in \langle R, + \cdot \rangle$. $\odot$ is closed in R^1.

Thus $\langle R^1, \oplus \odot \rangle$ is a ring. It remains to be proven that $\langle R, + \cdot \rangle$ is isomorphic to $\langle R^1, \oplus \odot \rangle$.

Define a mapping θ: $R \to R^1$ by $a\theta = A_a$ for each a in $\langle R, + \cdot \rangle$. θ is clearly one to one. Since a + b is closed in $\langle R, + \cdot \rangle$, let a + b = c as above. Then $(a + b)\theta = c\theta = A_c$, but from above $A_a \oplus A_b = A_c$ and $A_a = a\theta$ and $A_b = b\theta$. Thus $(a + b)\theta = a\theta + b\theta$. In the same manner $(a \cdot b) = d \in \langle R, + \cdot \rangle$ from above, and $(a \cdot b)\theta = d\theta = A_d$. Also from above, $A_d = A_a \odot A_b$, but $A_a = a\theta$ and $A_b = b\theta$. Thus $(a \cdot b)\theta = a\theta \cdot b\theta$. The operations are preserved, and θ is an isomorphism that maps R to R^1.

Every ring then can be generated by the group associated with it by taking the set of all endomorphisms and listing each subring where the subgroup with respect to addition is isomorphic to the given group.

The reason for the requirement in chapter one that every ring have at least one element that does not divide zero should now be clear. In the proof of Theorem 2.3 the mapping θ is clearly 1 to 1 because of this requirement. Suppose $xA_a = xA_b$, then $xA_a - xA_b = 0$ and $x \cdot a - x \cdot b = 0$. Thus $x \cdot (a - b) = 0$ for all x in $\langle R, + \cdot \rangle$. If there exists one x in $\langle R, + \cdot \rangle$ that is not a zero divisor, then $a - b = 0$; and $a = b$. If each element of $\langle R, + \cdot \rangle$ were a zero divisor, then there would be no justification for setting $a - b$ equal to zero; and the proof would not be valid.

If each element of $\langle R, + \cdot \rangle$ is a zero divisor, is $\langle R, + \cdot \rangle$ isomorphic to the zero ring? Consider the set $R = \{0, 2, 4, 6\}$ with the operations of ordinary addition and multiplication mod 8. The set R does then form a ring, $\langle R, + \cdot \rangle$.

+	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

	0	2	4	6
0	0	0	0	0
2	0	4	0	4
4	0	0	0	0
6	0	4	0	4

As shown in the tables each element of $\langle R, + \cdot \rangle$ is a zero divisor, and $\langle R, + \cdot \rangle$ is not isomorphic to the zero ring.

Theorem 2.3 would break down in this instance when generating the endomorphisms in accordance to Theorem 2.3. Using the method in Theorem 2.3 there would only be two endomorphisms: the zero endomorphism, and the endomorphism that maps the generator, 2, of $\langle R, + \cdot \rangle$ to 4. A set of two elements cannot be isomorphic to a set of four elements.

Given below are three examples demonstrating the theory just established.

The rings of order one are a trivial but consistent example. The group of order one can be represented by the following table.

+	0
0	0

There is only one endomorphism on the group of order one, the one that maps 0 to 0. Call it A. By definition $0(A + A) = 0A + 0A = 0 + 0 = 0$ and $0(A \quad A) = (0A) = (0)A = 0$. Therefore the only ring of order one is the zero ring,

⊕	A
A	A

⊙	A
A	A

.

0 is mapped to A isomorphically and the ring appears

+	0
0	0

·	0
0	0

.

There exists only one group of order two [3, p.38], and that group is represented by the integers modulo 2.

Addition for I/2 is given by the table

+	0	1
0	0	1
1	1	0

.

There exists two endomorphisms on I/2. One is called the zero map. As would be expected, it maps each element of I/2 to 0. The other is called the identity map, and it maps each element of I/2 to itself. The mappings, for convenience, can be represented in the following manner

$$\begin{array}{c} A \\ 0 \longrightarrow 0 \\ 1 \longrightarrow 0 \end{array} \qquad \begin{array}{c} B \\ 0 \longrightarrow 0 \\ 1 \longrightarrow 1 \end{array} .$$

The ring of endomorphisms has the operations

⊕	A	B
A	A	B
B	B	A

⊙	A	B
A	A	A
B	A	B

.

0 maps to A, and 1 maps to B and the ring is

+	0	1
0	0	1
1	1	0

	0	1
0	0	0
1	0	1

.

There are only two rings of order two, the above ring and the zero ring.

There are two groups of order four; one is cyclic, and the other is not. The cyclic group affords a final simple example. The cyclic group of order four is isomorphic to I/4, and the addition table is

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.

There are four endomorphisms on I/4

A	B	C	D
$0 \to 0$	$0 \to 0$	$0 \to 0$	$0 \to 0$
$1 \to 0$	$1 \to 1$	$1 \to 2$	$1 \to 3$
$2 \to 0$	$2 \to 2$	$2 \to 0$	$2 \to 2$
$3 \to 0$	$3 \to 3$	$3 \to 2$	$3 \to 1$

The ring of endomorphisms is

$\oplus$	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

$\odot$	A	B	C	D
A	A	A	A	A
B	A	B	C	D
C	A	C	A	C
D	A	D	C	B

Thus there are only two rings on the cyclic group of order four, the zero ring and the ring below which is isomorphic to the ring of endomorphisms.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

The other group of order four is neither simple nor cyclic. It will be given as an example after a discussion of the problems of notation and isomorphic subrings.

Chapter 3

FUNDAMENTAL THEORY OF ABELIAN GROUPS

The background of theory is now established for the solution of the problem. The more practical aspects of the elements of that theory should be studied more thoroughly. The definitions for the binary operations, although theoretically sound, leave much to be desired with regard to application. The notation for the endomorphisms is extremely bulky when applied. There are other practical problems regarding the order of the ring of endomorphisms and the actual application of the binary operations.

In chapter two we denoted the endomorphisms on I/4 in the following manner.

A	B	C	D
$0 \to 0$	$0 \to 0$	$0 \to 0$	$0 \to 0$
$1 \to 0$	$1 \to 1$	$1 \to 2$	$1 \to 3$
$2 \to 0$	$2 \to 2$	$2 \to 0$	$2 \to 2$
$3 \to 0$	$3 \to 3$	$3 \to 2$	$3 \to 1$

Using the definition of $\oplus$, to add elements C and D it was necessary to follow this procedure.

$$
\begin{aligned}
x(C \oplus D) &= xC + xD \text{ for all } x \text{ in } \langle G,^{+}\rangle. \\
0C + 0D &= 0 + 0 = 0 \\
1C + 1D &= 2 + 3 = 1 \\
2C + 2D &= 0 + 2 = 2 \\
3C + 3D &= 2 + 1 = 3
\end{aligned}
$$

Thus C $\oplus$ D is equal to the element which maps 0 to 0, 1 to 1, 2 to 2, and 3 to 3; that element of course is the identity element B.

Using the definition for $\odot$, to multiply B times D, this procedure was necessary.

$x(B \odot D) = (xC)D$ for all x in $\langle G,^{+}\rangle$.
$(0B)D = 0D = 0$
$(1B)D = 1D = 3$
$(2B)D = 2D = 2$
$(3B)D = 3D = 1$

Thus $B \odot D$ equals D.

This procedure, which is sufficiently bulky for simple examples such as I/4, becomes completely unmanageable for groups that are of greater order or are not cyclic. In the examples up to this point, the number of endomorphisms generated by the group have been equal to the order of the group. This will be untrue of examples that are not cyclic. Knowing the order or being able to compute the order of the ring of endomorphisms is important. If the order of the ring of endomorphisms is known, then the generation of all distinct endomorphisms on the group may be completed with confidence.

Since all of the groups used to generate these rings of endomorphisms are Abelian, the fundamental Theorem of Abelian groups will apply. This theorem states that every finite Abelian group is the direct sum of a finite number of cyclic groups of prime power order. [2, p.39] This theorem and the fact that every finite cyclic group of order n is isomorphic to I/n will provide the basis for the solution of these two problems.

The proof to the solution of these problems consists of three parts which are of independent interest and will be given as lemmas.

The first two lemmas are fundamental properties of commutative groups and will not be proved here.

Lemma 3.1. A finite cyclic group of order n is isomorphic to the additive group of residue classes of the rational integers mod n. [2, pp.22-23]

Lemma 3.2. A finite group is the direct sum of a finite number of cyclic groups of prime power order. [2, p.39]

Lemma 3.3. Every homomorphism from a cyclic group A to a cyclic group B, where A and B are of prime power order, can be represented by a single non-negative integer.

Proof: Let A be of order m and B be of order n. By Lemma 1 any cyclic group of order n is isomorphic to I/n; the homomorphism will be represented by the integer to which 1 is mapped.

Let g be a homomorphism from A to B where 1 is mapped to b in B. Assume h is another homomorphism from A to B where 1 is mapped to b in B. Then g is the map g: $1 \to b$, $2 \to b^2$, $3 \to b^3$, . . . , $n \to b^n$; and h is the map h: $1 \to b$, $2 \to b^2$, $3 \to b^3$, . . . , $n \to b^n$. Then $g = h$. Thus the number to which 1 is mapped determines the homomorphism and can be used to represent the homomorphism.

If m and n in the proof of the above Lemma 3.3. are relatively prime, there exists only one homomorphism. That homomorphism is the one in which each element of A is mapped to the zero element in B. If m and n are not relatively prime, then they must be powers of the same prime by the uniqueness of prime factorization. This fact will be used in applying the next theorem.

Theorem 3.1. Every endomorphism on a finite Abelian group G can be represented by an n-tuple of non-negative integers.

Proof: The proof of this theorem hinges upon two facts. The first is that every endomorphism is dependent upon the elements to which the basis elements of G are mapped. The second is that each element of G must be mapped to an element whose order is equal to or is a divisor of the order of that element of G.

Lemma 3.3. proves that each cyclic group of prime power order can be represented by a one-tuple consisting of one non-negative integer.

If G is not a cyclic group of prime power order, then Lemma 3.2. asserts that $G = H_1 + H_2 + \cdot \cdot \cdot + H_n$ where each of the H_i for $i = 1, 2, \ldots, n$ is a non-trivial cyclic group of prime power order. Thus each H_i is a cyclic group of order m_i, and by Lemma 3.1. it is isomorphic to I/m_i. Each element of H_i is the isomorphic image of a non-negative integer.

Every element g of G can be represented by an n-tuple, $g = (h_1, h_2, \ldots, h_n)$ where $h_i \epsilon H_i$. Since H_i is isomorphic to some I/m_i, the integer 1 will generate each of the H_i for all i since the H_i are non-trivial. The set $A = \{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ is a basis for G, that is, A generates G. [3, p.141] Let $a_1 = (1, 0, \ldots, 0)$ be the generator of H_1, $a_2 = (0, 1, 0, \ldots, 0)$ be the generator of H_2, and in general a_i will generate H_i and will indicate a 1 in the ith position of the n-tuple.

The properties of an endomorphism guarantee that every endomorphism is determined by the element of G to which each element of the set A, the basis for G, is mapped. By showing to which element of G each a_i is mapped, the endomorphisms can be represented by n^2-tuples of n sets of n integers. Each set of n integers will represent an element to which an element of the set A is mapped. In particular the ith set of n integers will be the element to which a_i is mapped.

The question of the order of the element to which a_i is mapped must be disposed of first. Each element a_i of A must be mapped to an element of G whose order is equal to or is a divisor of the order of a_i. If this were not the case, the result would be that the zero element of G would be mapped to an element other than zero. That is not acceptable in an endomorphism. If a_i, of order m_i, is mapped to an element $g_o = (g_1, g_2, \ldots, g_n)$, then g_o must be of order m_i or a divisor of m_i. For g_o to be of order m_i, the order of each of the g_i in the n-tuple $(g_1, g_2, \ldots, g_n)$ must be equal to or a divisor of m_i. This is true since $m_i a_i = 0$ must imply that $m_i g_o = 0$, and for $m_i g_o$ to equal 0 the order of each of the g_i must be equal to or a divisor of m_i.

A method for assuring the proper order of each of the g_i must be provided. Consider the n^2 sets of homomorphisms: $H_1 \rightarrow H_1$, $H_1 \rightarrow H_2$, $\ldots$, $H_1 \rightarrow H_n$, $H_2 \rightarrow H_1$, $H_2 \rightarrow H_2$, $\ldots$, $H_2 \rightarrow H_n$, $\ldots$, $H_n \rightarrow H_1$, $H_n \rightarrow H_2$, $\ldots$, $H_n \rightarrow H_n$. Each homomorphism $H_i \rightarrow H_j$ can be represented by a single non-negative integer by Lemma 3.3. The n^2-tuples of non-negative integers representing the homomorphisms from H_i to H_j will represent the endomorphisms from G to G. These n^2-tuples will be called S_α representations. Partition the n^2-tuples into n sets of n integers having the same arrangement as that of the n^2 sets of homomorphisms above. The order of the first n integers of the S_α n-tuple is equal to or a divisor of the order of H_1, and consequently of a_1, since they represent homomorphisms from H_1 to each of the H_i. Moreover the order of the ith set of n integers is equal to or is a divisor of the order of H_i, and consequently of a_i, since they represent homomorphisms from H_i to each of the H_j.

By the manner in which the n^2 sets of homomorphisms were arranged, each ith set of n integers of S_α is a representation of an element of G. Each a_i in A is then mapped to the element represented by the ith set of n integers in S_α. Since the proper order is assured, each of the S_α is an endomorphism.

Let X be any endomorphism on G, then each a_i is mapped to an element $g_o = (g_1, g_2, \ldots, g_n)$ of G where the order of each g_i is equal to or is a divisor of the order of a_i. But each such g_i is in one of the S_α representations. Thus each of the endomorphisms from G to G can be represented by an S_α.

When all of the qualifications concerning the order of each element in the S_α representation and its relation to the n^2 sets of homomorphisms are removed, Theorem 3.1. states that any endomorphism on a group G can be represented as an n^2-tuple of elements of G to which the basis is mapped. This simplifies the notation by reducing the number of elements involved in representing the map and the use of integers from I/n provides a more consistent notation for all groups.

Although the S_α notation is more consistent for all examples, if it does not facilitate a handier method for using the binary operations, it is of little value.

Consider the S_α representation of the endomorphism $(a_1, \ldots, a_n; a_{n+1}, \ldots, a_{2n}; \ldots a_{(n^2-1)+1}, \ldots, a_{n^2})$. The first n integers represent the element to which $(1, 0, \ldots, 0)$ is mapped. The ith n integers represent the element to which the generator, that has a 1 in the ith position, is mapped. The operation $\oplus$ has been defined as $x(A \oplus B) = xA + xB$ for all x in G. If the elements to which the basis elements are mapped are known, then the endomorphic image of each element is known. The S_α representation provides exactly that information. Thus if xA is an endomorphism on $\langle G,+\rangle$, then it has an S_α representation, and the same is true for xB. By the manner in which they are arranged the elementwise addition of the S_α representations in their relative modular settings is equivalent to $xA + xB$. Since $xA + xB = x(A \oplus B)$, $\oplus$ can be redefined as the elementwise addition of the S_α

representations of the endomorphisms.

If the operation $\odot$ can be redefined, a completely consistent method of dealing with the endomorphisms and the binary operations would be available. This would facilitate the application of any theory presented in this report.

As before the ith n elements of the S_α representation is the element of $\langle G,^+\rangle$ to which the generator, that has a 1 in the ith position, is mapped. The first n elements is the element of $\langle G,^+\rangle$ to which $(1, 0, \ldots, 0)$ is mapped, but the first n elements of an S representation is equivalent to an element of $\langle G,^+\rangle$. Thus the first n elements of an S_α representation can be broken down into the elementwise multiple addition of the generators of $\langle G,^+\rangle$. The first n elements of an S_α representation can be broken down in this manner, $n_1(1, 0, \ldots, 0) + n_2(0, 1, 0, \ldots, 0) + \cdots + n_n(0, \ldots, 0, 1)$, where each of the n_i represent multiple additions. But in a composite mapping elements of the form $(1, 0, \ldots, 0)$ must be mapped to the first n elements of the S representation, elements of the form $(0, 1, 0, \ldots, 0)$ must be mapped to the second n elements and so on in the general form already described. In a modular system repeated additions of the same element are equivalent to multiplicationin the modular setting. Thus composite mappings of S representations can be redefined in the following fashion: for S and T elements of the ring of endomorphisms and $S = (s_1, \ldots, s_n; s_{n+1}, \ldots, s_{2n}; \ldots; s_{(n^2-1)+1}, \ldots, s_{n^2})$, $T = (t_1, \ldots, t_n; t_{n+1}, \ldots, t_{2n}; \ldots; t_{(n^2-1)+1}, \ldots, t_{n^2})$. $S \odot T = (\sum_{i=1}^{n} s_i t_{(i-1)n+1}, \sum_{i=1}^{n} s_i t_{(i-1)n+2}, \ldots, \sum_{i=1}^{n} s_i t_{(i-1)n+n}, \sum_{i=1}^{n} s_{n+1} t_{(i-1)n+1},$

$\sum_{i=1}^{n} s_{n+i}t_{(i-1)n+2}, \ldots \sum_{i=1}^{n} s_{n+i}t_{(i-1)n+n}, \ldots$
$\sum_{i=1}^{n} s_{(i-1)n+1}t_{(i-1)n+n})$. Although complicated to represent, the operation is handled quite easily in practice. For an example, the n-tuples (2, 0, 0, 3) and (1, 0, 0, 1) are endomorphisms on the group $G = I/3 \times I/4$. A convenient method for applying the new definition for $\odot$ is

$$\begin{array}{cccc}
2 & 0 & 0 & 3 \\
1 & 0 & 0 & 1 \\
\hline
2\cdot 1 & 2\cdot 0 & 0\cdot 1 & 0\cdot 0 \\
0\cdot 0 & 0\cdot 1 & 3\cdot 0 & 3\cdot 1 \\
\hline
2 & 0 & 0 & 3
\end{array} .$$

The number of endomorphisms on a group $\langle G, +\rangle$ is now easy to compute. In the S_4 representation the first element represents the homomorphisms from H_1 to H_1, and there are only a finite number x of them. The kth element, $1 \leq k \leq n^2$, represents the homomorphisms from some H_i to some H_j and there are only a finite number X_k of them. The numbers of the endomorphisms then is simply the product of the X_k.

As stated before if the order of H_i and H_j are relatively prime, there exists only one homomorphism from H_i to H_j, the one that maps each element of H_i to the zero element of H_j. In addition if H_i and H_j are not relatively prime, they are powers of the same prime. Then if they are powers of the same prime the number of homomorphisms from H_i to H_j is a power of the same prime. Thus the order of $\langle G, +\rangle$ is a factor of the order of the ring of endomorphism by prime factorization.

As an example of the representation of endomorphisms and binary operations, the ring of endomorphisms on I/6 will be given. Six is not a power of a prime, and therefore I/6 is the direct sum of cyclic groups of prime power order. $I/6 = I/2 + I/3$. Since $I/6 = H_1 + H_2$, n is 2;

and n^2 is 4. Using S_α one-tuples to represent the homomorphisms, the n^2 sets of homomorphisms are as follows:

$H_1 \to H_1$	$H_1 \to H_2$	$H_2 \to H_1$	$H_2 \to H_2$
(0), (1)	(0)	(0)	(0), (1), (2).

There are six endomorphisms on I/6, and the S_α representations are as follows: (0, 0, 0, 0), (1, 0, 0, 0), (0, 0, 0, 1), (1, 0, 0, 1), (0, 0, 0, 2), (1, 0, 0, 2).

The table for the additive binary operation would appear as

⊕	0000	1001	0002	1000	0001	1002
0000	0000	1001	0002	1000	0001	1002
1001	1001	0002	1000	0001	1002	0000
0002	0002	1000	0001	1002	0000	1001
1000	1000	0001	1002	0000	1001	0002
0001	0001	1002	0000	1001	0002	1000
1002	1002	0000	1001	0002	1000	0001

The multiplication table would appear as

⊙	0000	1001	0002	1000	0001	1002
0000	0000	0000	0000	0000	0000	0000
1001	0000	1001	0002	1000	0001	1002
0002	0000	0002	0001	0000	0002	0001
1000	0000	1000	0000	1000	0000	1000
0001	0000	0001	0002	0000	0001	0002
1002	0000	1002	0001	1000	0002	1001

The isomorphism between the ring $\langle R, \oplus \odot \rangle$ and the ring I/6 is: $0 \to (0, 0, 0, 0)$, $1 \to (1, 0, 0, 1)$, $2 \to (0, 0, 0, 2)$, $3 \to (1, 0, 0, 0)$, $4 \to (0, 0, 0, 1)$, $5 \to (1, 0, 0, 2)$. Chapter four will deal with those groups that are not cyclic.

Chapter 4

IDENTIFICATION

The remaining problems are the identification of the subgroups of $\langle R, \oplus \odot \rangle$ that are isomorphic to the given group $\langle G, + \rangle$, and the classification of the isomorphic subrings. The problem of finding all of the subgroups of a ring of endomorphisms isomorphic to the given group is a difficult one. There is a solution that can be generalized. It is more convenient to begin with an example. Let $G = C_2 x C_2 x C_4$ where C_2 is the cyclic group of order two and C_4 is the cyclic group of order four. The elements (1, 0, 0), (0, 1, 0), and (0, 0, 1) generate G. (1, 0, 0) and (0, 1, 0) are of order two and (0, 0, 1) is of order four. For the subgroup of endomorphisms to be isomorphic to G, (1, 0, 0) and (0, 1, 0) must be mapped to different elements of order two, and (0, 0, 1) must be mapped to an element of order four. In looking at the S_α representations of the endomorphisms to which the generators of g must be mapped, the individual elements of the n-tuples must be of order, or a divisor of order, 2, and there must be at least one element of order 2 present.

Returning to the method in which the S_α representations were originated, the homomorphisms of order 2 may be counted.

C_2xC_2	C_2xC_2	C_2xC_4	C_2xC_2	C_2xC_2	C_2xC_4	C_4xC_2	C_4xC_2	C_4xC_4
2	2	2	2	2	2	2	2	x

The C_4xC_4 may be discounted, since the element (0, 0, 1) must be mapped to an element of order four, and all such mappings are equivalent. There are $2^8 - 1$ ways an element of order 2 may be chosen as an image of (1, 0, 0), and there are $(2^8 - 1) - 1$ elements to which (0, 1, 0) may be mapped. It is most convenient to map (0, 0, 1) to (0, 0, 0, 0, 0, 0, 0, 0, 1) of the S_α representation. There are $(2^8 - 1)((2^8 - 1) - 1)$ subgroups of $C_2xC_2xC_4$, but they are not all distinct. For example let (1, 0, 0) be mapped to (1, 0, 0, 0, 0, 0, 0, 0, 0) and (0, 1, 0) be mapped to (0, 1, 0, 0, 0, 0, 0, 0, 0) then (1, 1, 0) is mapped to (1, 1, 0, 0, 0, 0, 0, 0, 0). If (1, 0, 0) were mapped to (1, 1, 0, 0, 0, 0, 0, 0, 0) and (0, 1, 0) were mapped to (1, 0, 0, 0, 0, 0, 0, 0, 0), then (1, 1, 0) would be mapped to (0, 1, 0, 0, 0, 0, 0, 0, 0) and the group would be isomorphic to the one obtained first. Any one of the three endomorphisms could be chosen to be mapped to (1, 0, 0) and then either of the remaining two could be chosen to be mapped to (0, 1, 0). Thus for each subgroup there are six subgroups isomorphic to it. The number of distinct subgroups isomorphic to G would be $(2^8 - 1)((2^8-1)-1)/6$.

The group $G = C_2xC_2$ will be used as an example in chapter five. The homomorphisms of order two can be generated like this:

C_2xC_2 C_2xC_2 C_2xC_2 C_2xC_2

2 2 2 2

There are fifteen endomorphisms that (1,0) could be mapped to and fourteen to which (0,1) could be mapped. But again they are arranged in isomorphic groups of six. The number of distinct subgroups is 210/6 or 35.

In general it is easier to arrange $G = H_1 + H_2 + \cdot \cdot \cdot + H_n$ such that the order of the H_i H_{i+1}. The set of n^2 maps of $H_1 \rightarrow H_1$, $H_1 \rightarrow H_2$, . . . , $H_n \rightarrow H_n$ will identify all of the elements to which the generator of each H_i is to be mapped. The product of the number of mappings for each H_i is adjusted to account for the isomorphic maps as in the examples above will give the number of subgroups that are isomorphic to $\langle G,^{+}\rangle$.

Examples of non-cyclic groups using the S_{α} notation seemed to point up very little difference between automorphisms of a group onto itself and endomorphism of a group into itself. The following theorem gives a method for determining whether an element of $\langle R,^{\oplus\odot}\rangle$ is an endomorphism or an automorphism. Each element of the given group $\langle G,^{+}\rangle$ will generate a cyclic subgroup of $\langle G,^{+}\rangle$.

THEOREM 4.1. An endomorphism A on $\langle R,^{\oplus\odot}\rangle$ is an automorphism if and only if both of the following conditions are true:

(1) The order of the ith set of n integers in the S_{α} representation of A is equal to the order of H_i where $\langle R,^{+}\rangle = H_1 + H_2 + \cdot\cdot\cdot + H_i + \cdot\cdot\cdot + H_n$.

(2) The ith set of n integers in the S_{α} representation is not an element of a subgroup of $\langle R,^{+}\rangle$ generated by all other ith sets of n integers, $1\leq i$.

Proof: Let A be an automorphism on $\langle R,^{\oplus}\rangle$. A is a 1 to 1 mapping from $\langle R,^{+}\rangle$ onto $\langle R,^{+}\rangle$. Suppose 1 is not true. Let H_i be of order n, and let the ith set of n integers of A be of order $k<n$. The generator H_i generates n elements of $\langle R,^{+}\rangle$ and thus generates n elements of the mapping from $\langle R,^{+}\rangle$ to $\langle R,^{+}\rangle$. 0 is mapped to 0 and the element of the endomorphism that is the ith set of n integers added k times since $k<n$ is also mapped to 0 thus A is not an automorphism and that is contradictory to the given condition.

Suppose (2) is not true. Let the ith set of n integers be an element of the subgroup of $\langle R,^{+}\rangle$ generated by all other ith sets of n integers. Since it is a group, each element of this subgroup must have an inverse. Since the ith set of n integers is an element of the subgroup generated by all other ith sets of n integers, an element of this subgroup must be its inverse. Adding the ith set of n integers and its inverse must equal 0. Then A is not an automorphism which is again a contradiction. Thus both (1) and (2) must hold.

Let A be an endomorphism and let (1) and (2) be true. Then each ith set of n integers of the S_α representation of A generates n_i elements of A where n_i is the order of the H_i. Suppose A is as n to 1 endomorphism. Consider the kernel of the endomorphism. Some multiple of the ith set of n integers and an element of the subgroup generated by all other ith sets of n integers must be mapped to zero which indicates that those sets of n integers are from the same subgroup of $\langle R,+\rangle$. That contradicts (2) and A must be an automorphism.

As an example of Theorem 4.1 consider the endomorphisms A = (1,0,0,1,1,0,0,1,0) and B = (1,0,0,0,1,0,0,0,1) on the group G = $I/2 \times I/2 \times I/2$. Written out for all x in G the endomorphisms are

A	B
$(0,0,0)\longrightarrow(0,0,0)$	$(0,0,0)\longrightarrow(0,0,0)$
$(1,0,0)\longrightarrow(1,0,0)$	$(1,0,0)\longrightarrow(1,0,0)$
$(0,1,0)\longrightarrow(1,1,0)$	$(0,1,0)\longrightarrow(0,1,0)$
$(0,0,1)\longrightarrow(0,1,0)$	$(0,0,1)\longrightarrow(0,0,1)$
$(1,1,0)\longrightarrow(0,1,0)$	$(1,1,0)\longrightarrow(1,1,0)$
$(1,0,1)\longrightarrow(1,1,0)$	$(1,0,1)\longrightarrow(1,0,1)$
$(0,1,1)\longrightarrow(1,0,0)$	$(0,1,1)\longrightarrow(0,1,1)$
$(1,1,1)\longrightarrow(0,0,0)$	$(1,1,1)\longrightarrow(1,1,1)$

In the S_α representation of the endomorphism A, the second set of three integers is an element of the subgroup generated by the first and third sets of three integers. When the endomorphism A is written out for all x in G, A is clearly seen to be a two to one endomorphism. Both conditions (1) and (2) hold for the endomorphism B, and it is, as shown above, an automorphism.

All that remains is to find the isomorphic subrings. The multiplicative operation on the ring of endomorphisms is the common operation of composite mapping. The set of automorphisms of a group with an operation defined as composite mapping is a group. [3, p.109] The identity of the group of automorphisms is the identity mapping, which is also the unity mapping of the ring of endomorphisms. The fact that each element of a group commutes with its inverse precipitates the following theorem which provides a sufficient condition for two subrings to be isomorphic.

THEOREM 4.2. Given a subring $\langle S, \oplus \odot \rangle$ of the ring of endomorphisms $\langle R, \oplus \odot \rangle$, the set $T = \{X: X \in \langle R, \oplus \odot \rangle$ and $X = A \odot Y \odot A^{-1}$ for all Y in $\langle S, \oplus \odot \rangle$, where A is a fixed automorphism in $\langle R, \oplus \odot \rangle\}$ is a subring $\langle T, \oplus \odot \rangle$ of $\langle R, \oplus \odot \rangle$ and is isomorphic to $\langle S, \oplus \odot \rangle$.

Proof: It is important to the proof of this theorem to note that the composite mapping of an automorphism on a group $\langle G, + \rangle$ and any endomorphism on $\langle G, + \rangle$ is distinct. Thus each $A \odot Y \odot A^{-1}$ gives a distinct element of T for each element Y of $\langle S, \oplus \odot \rangle$.

The remainder of the proof is to demonstrate that the set T with the operations $\oplus$ and $\odot$ is isomorphic to $\langle S, \oplus \odot \rangle$.

Define a mapping θ: $S \rightarrow T$ by $\theta Y = A \odot Y \odot A^{-1}$ for all Y in $\langle S, \oplus \odot \rangle$ where A is a fixed automorphism in $\langle R, \oplus \odot \rangle$. $A \odot Y_1 \odot A^{-1} = X_1$ where X_1 is a distinct element of T, and Y_1 is a distinct element of $\langle S, \oplus \odot \rangle$.

Then $\theta(Y_1 \oplus Y_2) = A \odot (Y_1 \oplus Y_2) \odot A^{-1} = ((A \odot Y_1) \oplus (A \odot Y_2)) \odot A^{-1}$ by the distributive property of $\langle R, \oplus \odot \rangle$. Also by the distributive property $((A \odot Y_1) \oplus (A \odot Y_2)) \odot A^{-1} = (A \odot Y_1 \odot A^{-1}) \oplus (A \odot Y_2 \odot A^{-1}) = X_1 \oplus X_2$.

Also $\theta(Y_1 \odot Y_2) = A \odot (Y_1 \odot Y_2) \odot A^{-1} = A \odot (Y_1 \odot I \odot Y_2) \odot A^{-1} = A \odot (Y_1 \odot A^{-1} \odot A \odot Y_2) \odot A^{-1} = (A \odot Y_1 \odot A^{-1}) \odot (A \odot Y_2 \odot A^{-1})$ by the associative property and the properties of the unity element I. Thus $(A \odot Y_1 \odot A^{-1}) \odot (A \odot Y_2 \odot A^{-1}) = X_1 \odot X_2$.

θ is a ring isomorphism and $\langle T, \oplus \odot \rangle \cong \langle S, \oplus \odot \rangle$.

Every set of elements T that is related to a subring $\langle S, \oplus \odot \rangle$ by a fixed automorphism and its inverse is a subring of the ring of endomorphisms and is isomorphic to $\langle S, \oplus \odot \rangle$.

Chapter 5

EXAMPLES

In concurrence with the notation and theory presented in the first four chapters, this chapter will give as examples all groups and rings associated with them through order eight except the groups $G = C_2 x C_3$, $G = C_2 x C_2 x C_2$, and C_7. Some of these groups have been used in previous chapters but will be shown in the S_α notation.

The group of order one has one element and one endomorphism. The ring of endomorphisms is

$\oplus$	(0)
(0)	(0)

$\odot$	(0)
(0)	(0)

.

There is only one group of order two, and it is isomorphic to the integers modulo two. The ring of endomorphisms is

$\oplus$	(0)	(1)
(0)	(0)	(1)
(1)	(1)	(0)

$\odot$	(0)	(1)
(0)	(0)	(0)
(1)	(0)	(1)

.

The zero rings will not be shown in each case since they are all similar in structure.

There is only one group of order three, and it is isomorphic to I/3. There are three endomorphisms, but there are only two rings, the ring of endomorphisms and the zero ring. The ring of endomorphisms is

$\oplus$	(0)	(1)	(2)
(0)	(0)	(1)	(2)
(1)	(1)	(2)	(0)
(2)	(2)	(0)	(1)

$\odot$	(0)	(1)	(2)
(0)	(0)	(0)	(0)
(1)	(0)	(1)	(2)
(2)	(0)	(2)	(1)

.

All of the cyclic groups are isomorphic to I/n where n is the order of the cyclic group. That being true it would be inconsistent with the properties of the integers for the ring of endomorphisms to generate a ring that is not isomorphic to I/n with multiplication defined as usual. In addition I/3 is a field, and the ring of endomorphisms as expected has preserved that property.

There are two groups of order four, and both are commutative. The first is isomorphic to I/4. There are four endomorphisms on I/4, and the resulting ring is

$\oplus$	(0)	(1)	(2)	(3)
(0)	(0)	(1)	(2)	(3)
(1)	(1)	(2)	(3)	(0)
(2)	(2)	(3)	(0)	(1)
(3)	(3)	(0)	(1)	(2)

$\odot$	(0)	(1)	(2)	(3)
(0)	(0)	(0)	(0)	(0)
(1)	(0)	(1)	(2)	(3)
(2)	(0)	(2)	(0)	(2)
(3)	(0)	(3)	(2)	(1)

.

The S_α representations of cyclic groups of prime power order, as simple as they are, are consistent with Theorem 4.2. Since in the ring of endomorphisms on I/4 the elements (2) and (0) are not of order equal to the order of the group they are endomorphisms and not automorphisms.

The other group of order four is $G = C_2xC_2$ and is called the "four-group" or "quadratic group" or more commonly the "Klein group." [3, p.49] The n^2 sets of homomorphisms as S_α one-tuples are

$H_1 \to H_1$	$H_1 \to H_2$	$H_2 \to H_1$	$H_2 \to H_2$
(0)(1)	(0)(1)	(0)(1)	(0)(1)

.

There are sixteen endomorphisms on G. They will be listed below and then given an alphabetic representation to preserve space. The S_α representations are:

0-(0, 0, 0, 0)	c-(0, 0, 1, 1)	g-(0, 1, 0, 0)	k-(1, 1, 0, 0)
I-(1, 0, 0, 1)	d-(1, 0, 0, 0)	h-(0, 1, 1, 0)	l-(1, 1, 1, 0)
a-(0, 0, 1, 0)	e-(1, 0, 1, 0)	i-(0, 1, 0, 1)	m-(1, 1, 0, 1)
b-(0, 0, 0, 1)	f-(1, 0, 1, 1)	j-(0, 1, 1, 1)	n-(1, 1, 1, 1) .

The tables for the ring of endomorphisms are

⊕	0	I	a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	0	I	a	b	c	d	e	f	g	h	i	j	k	l	m	n
I	I	0	f	d	e	b	c	a	m	n	k	l	i	j	g	h
a	a	f	0	c	b	e	d	I	h	g	j	i	l	k	n	m
b	b	d	c	0	a	I	f	e	i	j	g	h	m	n	k	l
c	c	e	b	a	0	f	I	d	j	i	h	g	n	m	l	k
d	d	b	e	I	f	0	a	c	k	l	m	n	g	h	i	j
e	e	c	d	f	I	a	0	b	l	k	n	m	h	g	j	i
f	f	a	I	e	d	c	b	0	n	m	l	k	j	i	h	g
g	g	m	h	i	j	k	l	n	0	a	b	c	d	e	I	f
h	h	n	g	j	i	l	k	m	a	0	c	b	e	d	f	I
i	i	k	j	g	h	m	n	l	b	c	0	a	I	f	d	e
j	j	l	i	h	g	n	m	k	c	b	a	0	f	I	e	d
k	k	i	l	m	n	g	h	j	d	e	I	f	0	a	b	c
l	l	j	k	n	m	h	g	i	e	d	f	I	a	0	c	b
m	m	g	n	k	l	i	j	h	I	f	d	e	b	c	0	a
n	n	h	m	l	k	j	i	g	f	I	e	d	c	b	a	0

⊙	0	I	a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I	0	I	a	b	c	d	e	f	g	h	i	j	k	l	m	n
a	0	a	0	0	0	a	a	a	b	b	b	b	c	c	c	c
b	0	b	a	b	c	0	a	c	0	a	b	c	0	a	b	c
c	0	c	a	b	c	a	0	b	b	c	0	a	c	b	a	0
d	0	d	0	0	0	d	d	d	g	g	g	g	k	k	k	k
e	0	e	0	0	0	e	e	e	i	i	i	i	n	n	n	n
f	0	f	a	b	c	e	d	I	i	j	g	h	n	m	l	k
g	0	g	d	g	k	0	d	k	0	d	g	k	0	d	g	k
h	0	h	d	g	k	a	e	l	b	I	i	m	c	f	j	n
i	0	i	e	i	n	0	e	n	0	e	i	n	0	e	i	n
j	0	j	e	i	n	a	d	m	b	f	g	l	c	I	h	k
k	0	k	d	g	k	d	0	g	g	k	0	d	k	g	d	0
l	0	l	d	g	k	e	a	h	i	l	b	I	n	j	f	c
m	0	m	e	i	n	d	a	j	g	l	b	f	k	h	I	c
n	0	n	e	i	n	e	0	i	i	n	0	e	n	i	e	0

Using the method given in chapter four there are thirty-five subgroups of the ring of endomorphisms that are isomorphic to $\langle G,+\rangle$. Of these thirty-five only thirteen are closed with respect to the operation $\odot$. Using the automorphisms to check for isomorphic sub-rings, those that are isomorphic are:

$(0, 0, 0, 0), (1, 0, 0, 1), (0, 0, 1, 0), (1, 0, 1, 1) \cong$

$(0, 0, 0, 0), (1, 0, 0, 1), (0, 1, 0, 0), (1, 1, 0, 1) \cong$

$(0, 0, 0, 0), (1, 0, 0, 1), (0, 1, 1, 0), (1, 1, 1, 1)$;

$(0, 0, 0, 0), (1, 0, 0, 1), (0, 0, 0, 1), (1, 0, 0, 0) \cong$

$(0, 0, 0, 0), (1, 0, 0, 1), (0, 0, 1, 1), (1, 0, 1, 0) \cong$

$(0, 0, 0, 0), (1, 0, 0, 1), (0, 1, 0, 1), (1, 1, 0, 0)$;

$(0, 0, 0, 0), (0, 0, 1, 0), (1, 0, 0, 0), (1, 0, 1, 0) \cong$

$(0, 0, 0, 0), (0, 0, 0, 1), (0, 1, 0, 0), (0, 1, 0, 1) \cong$

$(0, 0, 0, 0), (0, 0, 1, 1), (1, 1, 0, 0), (1, 1, 1, 1)$;

$(0, 0, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1), (0, 0, 1, 1) \cong$

$(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1) \cong$

$(0, 0, 0, 0), (1, 0, 0, 0), (0, 1, 0, 0), (1, 1, 0, 0)$;

$(0, 0, 0, 0), (1, 0, 0, 1), (0, 1, 1, 1), (1, 1, 1, 0)$.

The last ring listed is not isomorphic to any other ring listed, and it is a field.

There is only one group of order five, and it is isomorphic to I/5. [3, p.51] There are five endomorphisms on I/5. The ring of endomorphisms is

⊕	(0)	(1)	(2)	(3)	(4)
(0)	(0)	(1)	(2)	(3)	(4)
(1)	(1)	(2)	(3)	(4)	(0)
(2)	(2)	(3)	(4)	(0)	(1)
(3)	(3)	(4)	(0)	(1)	(2)
(4)	(4)	(0)	(1)	(2)	(3)

⊙	(0)	(1)	(2)	(3)	(4)
(0)	(0)	(0)	(0)	(0)	(0)
(1)	(0)	(1)	(2)	(3)	(4)
(2)	(0)	(2)	(4)	(1)	(3)
(3)	(0)	(3)	(1)	(4)	(2)
(4)	(0)	(4)	(3)	(2)	(1)

.

There are two groups of order six. Only one is commutative, and that group was used as an example in chapter three with the S_α notation. The two groups are $G = C_2 x C_3$ and the permutation group of three elements.

There is only one group of order seven. It is isomorphic to I/7, and it is very similar to I/5. For that reason the ring of endomorphisms on I/7 will be omitted here.

There are five groups of order eight, and three of them are commutative. [3, p.51] The commutative groups are $G = C_8$, $G = C_2 x C_4$, and $G = C_2 x C_2 x C_2$. C_8 is isomorphic to I/8, and the ring of endomorphisms is

⊕	(0)	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(0)	(0)	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1)	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(0)
(2)	(2)	(3)	(4)	(5)	(6)	(7)	(0)	(1)
(3)	(3)	(4)	(5)	(6)	(7)	(0)	(1)	(2)
(4)	(4)	(5)	(6)	(7)	(0)	(1)	(2)	(3)
(5)	(5)	(6)	(7)	(0)	(1)	(2)	(3)	(4)
(6)	(6)	(7)	(0)	(1)	(2)	(3)	(4)	(5)
(7)	(7)	(0)	(1)	(2)	(3)	(4)	(5)	(6)

⊙	(0)	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(0)	(0)	(0)	(0)	(0)	(0)	(0)	(0)	(0)
(1)	(0)	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(2)	(0)	(2)	(4)	(6)	(0)	(2)	(4)	(6)
(3)	(0)	(3)	(6)	(1)	(4)	(7)	(2)	(5)
(4)	(0)	(4)	(0)	(4)	(0)	(4)	(0)	(4)
(5)	(0)	(5)	(2)	(7)	(4)	(1)	(6)	(3)
(6)	(0)	(6)	(4)	(2)	(0)	(6)	(4)	(2)
(7)	(0)	(7)	(6)	(5)	(4)	(3)	(2)	(1)

The group $G = C_2 x C_4$ is the last example. There are thirty-two endomorphisms on G, and they will be listed below. Since there are only seven subgroups of the ring of endomorphisms that are isomorphic to G, it will be more convenient to look only at the subgroups and not the entire ring of endomorphisms. Of the seven subgroups only three are closed under the operation ⊙ . These three will be listed below. The thirty-two endomorphisms are as follows:

0-(0, 0, 0, 0)	8-(0, 2, 0, 3)	16-(1, 2, 0, 0)	24-(1, 0, 1, 0)
1-(1, 0, 0, 0)	9-(0, 0, 1, 0)	17-(1, 2, 0, 1)	25-(1, 0, 1, 1)
2-(1, 0, 0, 1)	10-(0, 0, 1, 1)	18-(1, 2, 0, 2)	26-(1, 0, 1, 2)
3-(1, 0, 0, 2)	11-(0, 0, 1, 2)	19-(1, 2, 0, 3)	27-(1, 0, 1, 3)
4-(1, 0, 0, 3)	12-(0, 0, 1, 3)	20-(0, 2, 1, 0)	28-(1, 2, 1, 0)
5-(0, 2, 0, 0)	13-(0, 0, 0, 1)	21-(0, 2, 1, 1)	29-(1, 2, 1, 1)
6-(0, 2, 0, 1)	14-(0, 0, 0, 2)	22-(0, 2, 1, 2)	30-(1, 2, 1, 2)
7-(0, 2, 0, 2)	15-(0, 0, 0, 3)	23-(0, 2, 1, 3)	31-(1, 2, 1, 3)

The additive group is given once as elements of $\langle G, + \rangle$.

+	(0,0)	(1,0)	(0,1)	(0,2)	(0,3)	(1,1)	(1,2)	(1,3)
(0,0)	(0,0)	(1,0)	(0,1)	(0,2)	(0,3)	(1,1)	(1,2)	(1,3)
(1,0)	(1,0)	(0,0)	(1,1)	(1,2)	(1,3)	(0,1)	(0,2)	(0,3)
(0,1)	(0,1)	(1,1)	(0,2)	(0,3)	(0,0)	(1,2)	(1,3)	(1,0)
(0,2)	(0,2)	(1,2)	(0,3)	(0,0)	(0,1)	(1,3)	(1,0)	(1,1)
(0,3)	(0,3)	(1,3)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(1,1)	(1,1)	(0,1)	(1,2)	(1,3)	(1,0)	(0,2)	(0,3)	(0,0)
(1,2)	(1,2)	(0,2)	(1,3)	(1,0)	(1,1)	(0,3)	(0,0)	(1,1)
(1,3)	(1,3)	(0,3)	(1,0)	(1,1)	(1,2)	(0,0)	(1,1)	(0,2)

The isomorphisms between the three subgroups and the group $\langle G, + \rangle$ will be given instead of displaying three similar tables for the operation $\oplus$.

$0 \to (0,0)$	$0 \to (0,0)$	$0 \to (0,0)$
$1 \to (1,0)$	$5 \to (1,0)$	$9 \to (1,0)$
$13 \to (0,1)$	$13 \to (0,1)$	$13 \to (0,1)$
$14 \to (0,2)$	$14 \to (0,2)$	$14 \to (0,2)$
$15 \to (0,3)$	$15 \to (0,3)$	$15 \to (0,3)$
$2 \to (1,1)$	$16 \to (1,1)$	$10 \to (1,1)$
$3 \to (1,2)$	$7 \to (1,2)$	$11 \to (1,2)$
$4 \to (1,3)$	$8 \to (1,3)$	$12 \to (1,3)$

The tables for the operation $\odot$ for the three subrings are

$\odot$	0	1	13	14	15	2	3	4
0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	1	1	1
13	0	0	13	14	15	13	14	15
14	0	0	14	0	14	14	0	14
15	0	0	15	14	13	15	14	13
2	0	1	13	14	15	2	3	4
3	0	1	14	0	14	3	1	3
4	0	1	15	4	14	4	3	2

⊙	0	5	13	14	15	6	7	8
0	0	0	0	0	0	0	0	0
5	0	0	5	0	5	5	0	5
13	0	0	13	14	15	13	14	15
14	0	0	14	0	14	14	0	14
15	0	0	15	14	13	15	14	13
6	0	0	6	14	8	6	14	8
7	0	0	7	0	7	7	0	7
8	0	0	8	14	6	8	14	6

⊙	0	9	13	14	15	10	11	12
0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
13	0	9	13	14	15	10	11	12
14	0	0	14	0	14	14	0	14
15	0	9	15	14	13	12	11	10
10	0	9	13	14	15	10	11	12
11	0	0	14	0	14	14	0	14
12	0	9	15	14	13	12	11	10

All three of these subrings are distinct.

The last group of order eight is the group $G = C_2 x C_2 x C_2$. This example will be omitted due to its bulk. There are five hundred twelve endomorphisms on $C_2 x C_2 x C_2$, and there are 1241 distinct subgroups of the ring of endomorphisms as well. There would be nearly one and one half million individual arithmetic steps to find out how many of the 1241 subgroups were closed with respect to the multiplicative operation. This completes the work to be done with examples.

Chapter 6

SUMMARY

Given any finite Abelian group there is always a ring, the zero ring, associated with it. If there are more rings associated with the group, they are subrings of a ring of endomorphisms and can be isolated provided they are not the direct product or sum of the zero ring and some other ring.

Notation has been introduced to facilitate the representation of the endomorphisms on the group. A method for identifying automorphisms among the endomorphisms has been provided. One method of identifying the subrings that are isomorphic has also been developed.

There are some avenues of further study that are immediately apparent. The ring of endomorphisms on the group $G = C_2 x C_2$ had some characteristics that the ring of endomorphisms on $G = C_2 x C_4$ did not have. All of the right ideals of the ring of endomorphisms on $G = C_2 x C_2$ were isomorphic subrings associated with G. The left ideals had the same property. There was also a field of four elements associated with G. It could be fruitful to see if the rings of endomorphisms on a group $G = C_3 x C_3$ or a group $G = C_2 x C_2 x C_2$ or any group $G = C_p x C_p x \cdot \cdot \cdot C_p$, where p is a prime, had the same properties.

It would be an interesting problem to write a program to let a computer do all the arithmetic on large groups. Since it can all be reduced to working with positive integers, it should be suitable to computer application.

In chapter four a sufficient condition was given for two subrings of the ring of endomorphisms to be isomorphic. One further problem would be to show that given two isomorphic subrings, there exists an automorphism in $\langle R, \oplus \odot \rangle$ that relates the two subrings as in Theorem 4.2.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Barnes, Wilfred E. Introduction to Abstract Algebra. Boston: D. C. Heath and Company, 1963.

2. Fuchs, L. Abelian Groups. New York: Pergamon Press, 1960.

3. Lederman, Walter. Introduction to the Theory of Finite Groups. London: Oliver and Boyd, 1961.

4. McCoy, Neal H. The Theory of Rings. New York: The Macmillan Company, 1964.

Appendix

In chapter one it was required that every ring have at least one element that did not divide zero. The reason for that requirement and a simple example of the problem if that requirement were not made was set forth in chapter two.

The example in chapter two brings out two interesting points. Given a ring where each element is a zero divisor; it is not necessarily isomorphic to the zero ring, and it is not necessarily the direct product of the zero ring and some other ring. It can be proved however that if a ring is of prime order and each element is a zero divisor, then that ring is isomorphic to the zero ring.

Theorem 7.1. If a ring, $\langle R,^{+\cdot}\rangle$, is of prime order and if every element of $\langle R,^{+\cdot}\rangle$ is a zero divisor, then $\langle R,^{+\cdot}\rangle$ is a zero ring.

Proof: To prove this it must be shown that $x \cdot y = 0$ for any x and y in R. Since $\langle R,^{+\cdot}\rangle$ is of prime order, each element of R generates $\langle R,^{+}\rangle$. Let x be any element of R. Since every element of R is a zero divisor, there must exist a nonzero element a in R such that $x \cdot a = 0$. Therefore $x \cdot na = n(x \cdot a) = 0$ for each integer n; and since a is a generator of $\langle R,^{+}\rangle$, $x \cdot y = 0$ for each element y in $\langle R,^{+\cdot}\rangle$. Since x was chosen arbitrarily, this completes the proof.

The following corollary is a direct result of Theorem 2.3.

Corollary 7.2. Every ring $\langle R,^{+\cdot}\rangle$, with unity, is isomorphic to a ring of endomorphisms on $\langle R,^{+}\rangle$.

It can be shown that any ring $\langle R,^{+\cdot}\rangle$ is isomorphic to a subring $\langle R^{*},^{+\cdot}\rangle$ of a ring $\langle B,^{+\cdot}\rangle$ that has unity. This is done by extending

$\langle R, +\cdot\rangle$ to $\langle B, +\cdot\rangle$ where $\langle B, +\cdot\rangle$ has an identity. The ring $\langle R^*, +\cdot\rangle$ is a subring of $\langle B, +\cdot\rangle$ isomorphic to $\langle R, +\cdot\rangle$. If it could be shown that any ring could be imbedded in a finite ring with unity, then the material in chapters three and four could be used to associate all rings with finite groups.