1965

Analogous Concepts of Normal Subgroups and Ideals

Ellen Joyce Stone
College of William & Mary - Arts & Sciences

ANALOGOUS CONCEPTS OF NORMAL SUBGROUPS AND IDEALS

A Thesis

Presented to

The Faculty of the Department of Mathematics

The College of William and Mary in Virginia

In Partial Fulfillment

Of the Requirements for the Degree of

Master of Arts

By

Ellen Joyce Stone

May 1965

APPROVAL SHEET

This thesis is submitted in partial fulfillment of
the requirements for the degree of
Master of Arts

Ellen Joyce Stone

Author

Approved, May 1965:

Thomas L. Reynolds

Thomas L. Reynolds, Ph.D. (Chairman)

Luther T. Conner Jr.

Luther T. Conner, Jr., M.A.

William C. Turner

William C. Turner, M.A.

ACKNOWLEDGMENT

The author wishes to express her appreciation to Professor Thomas L. Reynolds, under whose guidance this investigation was conducted, for the great care with which he has read the manuscript and the many helpful suggestions he has made.

TABLE OF CONTENTS

ABSTRACT

The purpose of this thesis is to study the parallel roles of normal subgroups in group theory and those of ideals in ring theory.

Chapter I interrelates various definitions of normal subgroups as well as illustrates the manner in which normal subgroups decompose their respective groups. Certain types of normal subgroups, such as the center, commutator, and anticenter, are investigated in detail.

Chapter II describes several important ideals of a ring, such as principal ideals, maximal and minimal ideals, prime ideals, and the radical. Special emphasis is given to the development of properties of the radical of a ring which are analogous to those of the anticenter of a group.

In the last chapter, the results of the preceding chapters are utilized to compare analytically normal subgroups and ideals. Analogous concepts are given with respect to set theory, homomorphisms, isomorphisms, direct products, and direct sums.

ANALOGOUS CONCEPTS OF NORMAL SUBGROUPS AND IDEALS

INTRODUCTION

It has been mentioned in many books, including those written by Kurosh [4], Birkhoff and MacLane [1], and Van der Waerden [7], that ideals in a ring are analogous to normal subgroups in a group. We wish to investigate normal subgroups and ideals with the purpose of giving a systematic comparison of the two concepts.

In order to give a comparison of normal subgroups and ideals, we must first investigate the manner in which normal subgroups decompose a group. It is assumed that the reader is familiar with certain group terminology and definitions such as the definition of a subgroup, cosets of a group, factor groups, and the order of a finite group. One may find these notions readily in most textbooks on group theory or abstract algebra. In particular, the reader is referred to Birkhoff and MacLane [1]. Several definitions and characterizations of normality are given in the first chapter. These characterizations are applied to several important normal subgroups such as the center and the commutator subgroup. A normal subgroup introduced by Levine [5] is considered in detail. We shall summarize Mr. Levine's results as well as utilize previous concepts of normality to develop some further results.

Chapter II is devoted to the study of ideals and the effect they have on ring decomposition. Again, the reader's familiarity with subrings, residue classes, factor rings, and the elementary theory of congruences is assumed. These concepts may be found in any book on ring theory such as that by McCoy [6]. In characterizing ideals, we describe principal ideals, maximal and minimal ideals, and prime ideals as well as give several theorems connecting these ideals. Special attention is given to the radical of an ideal, whose properties are analogous to those of an anti-center of a group.

The last chapter serves to show the parallelism between normal subgroups and ideals by means of set theory, homomorphisms, isomorphisms, direct products, and direct sums. With the tools we have developed in the preliminary chapters, we may define concepts and prove theorems concerned with the intersection, union, product, and sum of arbitrary sets of normal subgroups and ideals. Although the Fundamental Homomorphism Theorem for Groups may be found in the texts of Birkhoff and MacLane [1], Van der Waerden [7], and Zassenhaus [8], there are two other important homomorphism theorems which are not so readily available in the literature. We shall prove the three homomorphism theorems for groups and give analogous theorems for rings. Lastly, certain relations involving direct products of normal subgroups will be compared to direct sums of ideals.

CHAPTER I

A CHARACTERIZATION OF NORMALITY

In order to compare normal subgroups of a group and ideals of a ring, it is necessary to investigate the manner in which these subsets decompose their respective group or ring. We begin this analysis with the characterization of normal subgroups.

Definition: If G is a group and H is a subgroup of G, then H is said to be normal in G if and only if aha^{-1} is in H for all a in G and all h in H.

Theorem 1.1: For any subgroup H of G and any element a of G, the set $aHa^{-1} \equiv \{aha^{-1} \mid h \text{ is in } H\}$ is a subgroup S of G such that $S \cong H$.

Proof: Let aha^{-1} and aka^{-1} be elements of aHa^{-1}.

$$(aha^{-1})(aka^{-1}) = aha^{-1} \cdot aka^{-1} = a(hk^{-1})a^{-1},$$

which is in aHa^{-1}, since hk^{-1} is in the subgroup H. Hence S is a subgroup of G. Furthermore, the mapping $h \to aha^{-1}$ can be readily shown to be well-defined, one-to-one, onto, and product-preserving [7, page 26]. It follows that $S \cong H$.

Definition: For H a subgroup of G and a in G, aHa^{-1} is called a conjugate subgroup of H, the isomorphic mapping of H, $h \to aha^{-1}$, is called <u>conjugation by a</u>, and the elements h and aha^{-1} are said to be <u>conjugate elements</u>.

If we take H = G, the mapping $g \to aga^{-1}$ for all g in G and some a in G defines an inner automorphism of G. Thus, we may define normality as follows:

<u>Definition</u>: The subgroup H of G is <u>normal</u> in G if and only if H is invariant under all the inner automorphisms of G.

<u>Theorem 1.2</u>: The set of inner automorphisms of G form a normal subgroup of the group of all automorphisms of G.

<u>Proof</u>: Let the set of inner automorphisms of G be denoted by

$$A_g \equiv \{f_a \mid a \in G \text{ and for all } g \text{ in } G,\ f_a(g) = aga^{-1}\}.$$

For any a and b in G and the corresponding f_a and f_b in A_g, it follows that

$$f_{ab^{-1}}(g) = f_a(b^{-1}gb) = a(b^{-1}gb)a^{-1} = (ab^{-1})g(ab^{-1})^{-1},$$

which is in A_g. Hence A_g is a subgroup. Now consider the automorphism Φ of G. Let f_a be in A_g and g be in G.

$$[\Phi f_a \Phi^{-1}](g) = [\Phi f_a](\Phi^{-1}(g)) = \Phi\ [a\Phi^{-1}(g)a^{-1}] =$$

$$\Phi(a)\cdot g\cdot\Phi(a^{-1}) = \Phi(a)\cdot g\cdot\Phi^{-1}(a),$$

which is in A_g. Thus we see that A_g is normal in the group of all automorphisms of G.

As another definition of normality, we consider the

the decomposition of G with respect to right and left cosets of H.

Definition: The subgroup H of G is normal in G if and only if $aH = Ha$ for all a in G.

With the aid of these definitions, we may state the following:

Theorem 1.3: The subgroup H of G is normal in G if and only if H is equal to all its conjugates.

Proof: The proof is immediate from the above definitions.

For a normal subgroup H, the group G/H, called the factor group of G with respect to H, denotes the set of all cosets of H under the operation $aH \cdot bH = (ab)H$ for all a and b in G.

Let us now consider a homomorphism $f: G \to G'$ where G and G' are groups.

Definition: The kernel of f, denoted by K_f, is the set of all elements a in G such that $f(a) = e'$ where e' is the identity element of G'.

The following Theorem 1.4 is often called the Fundamental Homomorphism Theorem for Groups. Various proofs of this theorem may be found in the works of Van der Waerden [7, page 38], Zassenhaus [8, page 29], and Birkhoff and MacLane [1, page 153]. It will essentially be the latter proof that we shall use.

Lemma 1: K_f is a normal subgroup.

Proof: Let a and b be elements of K_f. It follows that

$$f(ab^{-1}) = f(a) \cdot f(b^{-1}) = e' \cdot (e')^{-1} = e'.$$

Hence K_f is a subgroup. Now let $x \in K_f$ and $g \in G$.

$f(gxg^{-1}) = f(g)\cdot f(x)\cdot f(g^{-1}) = f(g)\cdot e'\cdot f^{-1}(g) = e'$,

and therefore gxg^{-1} is in K_f. This implies gK_fg^{-1} is in K_f, or K_f is normal.

Lemma 2: $f(a) = f(b)$ if and only if $aK_f = bK_f$ for a and b in G.

Proof: Let $f(a) = f(b)$ and let x be in K_f.

$f(axb^{-1}) = f(a)\cdot f(x)\cdot f(b^{-1}) = f(a)\cdot e'\cdot f^{-1}(b) = f(b)\cdot f^{-1}(b) = e'$.

Thus axb^{-1} is in K_f, which implies that $aK_fb^{-1} \subset K_f$. It then follows that $aK_f \subset K_fb$. Since K_f is a normal subgroup, $bK_f = K_fb$, and $aK_f \subset K_fb = bK_f$. By symmetry, it can be readily shown that $bK_f \subset aK_f$, and, thus, the cosets aK_f and bK_f are equal.

Now, suppose $aK_f = bK_f$. Since f is a homomorphic function from G onto G', $f(e) = e'$, where e is the identity element of G [8, page 36]. Therefore, e is in K_f and $ae = a$ is in the coset aK_f. Since $aK_f = bK_f$, it follows that a is in bK_f. This implies there exists an element x in K_f such that $a = bx$. We, therefore, have that

$$f(a) = f(bx) = f(b)\cdot f(x) = f(b)\cdot e' = f(b).$$

Hence $f(a) = f(b)$, and the lemma is proved.

We are now able to establish the following:

Theorem 1.4: If f is a homomorphism from a group G onto a group G', then $G/K_f \cong G'$.

Proof: Let the mapping be given by Φ: $aK_f \rightarrow f(a)$ where a is in G.

That Φ is well-defined is evident, since $aK_f = bK_f$ implies by Lemma 2 that $f(a) = f(b)$ or $\Phi(aK_f) = \Phi(bK_f)$. Also, by Lemma 2, it follows that if $\Phi(aK_f) = \Phi(bK_f)$, or equivalently, if $f(a) = f(b)$, then $aK_f = bK_f$. Hence the mapping is one-to-one. Now suppose a' is in G'. Since f is a homomorphic function, there is an element a in G such that $f(a) = a'$. Thus, there is a coset aK_f in G/K_f such that $f(a) = a' = \Phi(aK_f)$. This shows that Φ is onto. It suffices to show that the mapping Φ is product-preserving. Let aK_f and $bK_f \in G/K_f$.

$$\Phi(aK_f \cdot bK_f) = \Phi[(ab)K_f] = f(ab) = f(a) \cdot f(b) = \Phi(aK_f) \cdot \Phi(bK_f),$$

and, thus, the mapping is the isomorphism : $G/K_f \cong G'$.

We now turn our attention to specific normal subgroups and the homomorphisms determined by them.

Definition: The set C of elements $c \in G$ such that $ca = ac$ for all $a \in G$ is called the center of G.

We observe that the center of a group is the group itself if and only if the group is Abelian. Furthermore, C is a normal subgroup of G, and the center of G/C consists of the identity coset, i.e., the coset C, only.

Theorem 1.5: An inner automorphism f_a of G is the identity automorphism if and only if a belongs to the center of G.

Proof: Suppose f_a is the identity automorphism. Let g be in G. Then,

$$f_a(g) = aga^{-1} = g \text{ implies } ag = ga.$$

It follows that a is in C.

Now suppose $a \in C$. For every g in G, $ag = ga$. It follows that $aga^{-1} = g$, and, thus, f_a is the identity automorphism.

Theorem 1.6: $G/C \cong A_g$.

Proof: Since G is a subgroup of itself, it follows by Theorem 1.1 that the set aGa^{-1}, where a is an arbitrary element of G is isomorphic to G. This set is precisely the set, A_g, of inner automorphisms of G, and, therefore $G \cong A_g$. By the previous theorem, the kernel of the isomorphism is the center C of G. Applying the Fundamental Theorem, we have $G/C \cong A_g$.

In particular, we state the following corollary:

Corollary: If the center of G consists only of the identity element e, then the center of the group of automorphisms of G consists only of the identity automorphism.

Definition: For any group G, elements of the form $aba^{-1}b^{-1}$, where a and b are in G, are called commutator elements. Furthermore, the commutator subset Z of G is the set of all finite products of commutator elements of G.

Theorem 1.7: Z is a normal subgroup of G.

Proof: Since the inverse of a commutator element is again a commutator element, it follows that Z is a subgroup of G. It suffices to show that Z is normal in G. Let $g \in G$ and $z \in Z$. Since z is a finite product of commutator elements, we may denote z by

$$z = x_1 \cdot x_2 \cdot x_3 \cdots x_n, \text{ where } x_1 = a_1 b_1 a_1^{-1} b_1^{-1},$$

$$x_2 = a_2 b_2 a_2^{-1} b_2^{-1}, \ \ldots, \ \ x_n = a_n b_n a_n^{-1} b_n^{-1}.$$

It follows that gzg^{-1} can be written as

$$gzg^{-1} = g\cdot(a_1 b_1 a_1^{-1} b_1^{-1})\cdot(a_2 b_2 a_2^{-1} b_2^{-1})\cdots(a_n b_n a_n^{-1} b_n^{-1})\cdot g^{-1} =$$

$$ga_1(g^{-1}g)b_1(g^{-1}g)a_1^{-1}(g^{-1}g)b_1^{-1}(g^{-1}g)a_2\cdots a_n^{-1}(g^{-1}g)b_n^{-1}g^{-1}.$$

We now replace ga_1g^{-1} by a_1', gb_1g^{-1} by $b_1', \ldots,$ gb_ng^{-1} by b_n'.

Hence,

$$gzg^{-1} = a_1'\cdot b_1'\cdot(a_1')^{-1}\cdot(b_1')^{-1}\cdot a_2'\cdot b_2'\cdots(a_n')\cdot(b_n')\cdot(a_n')^{-1}(b_n')^{-1}.$$

It follows that gzg^{-1} is in Z, or $gZg^{-1} \subset Z$. Hence Z is a normal subgroup of G.

<u>Theorem 1.8</u>: G/Z is Abelain.

<u>Proof</u>: Let aZ and bZ $\in$ G/Z. We have,

$$aZ.bZ = abZ = (baa^{-1}b^{-1}ab)Z = baZ = bZ\cdot aZ,$$

since $a^{-1}b^{-1}ab \in Z$. It follows that G/Z is Abelian.

<u>Theorem 1.9</u>: A group G is Abelian if and only if all commutator elements equal the group identity.

<u>Proof</u>: The proof is immediate since if G is Abelian, for any elements x and y in G, xy = yx implies $xyx^{-1}y^{-1} = e$. Conversely, if for any x and y in G, $xyx^{-1}y^{-1} = e$, then xy = yx and G is Abelian.

Theorem 1.10: If N is a normal subgroup of G, G/N is Abelian if and only if $Z \subset N$.

Proof: Suppose G/N is Abelian. Consider the homomorphic mapping, f, of G onto G/N with kernel N. Let x and $y \in G$ such that $f(x) = u$ and $f(y) = v$. It follows that

$$f(xyx^{-1}y^{-1}) = f(x) \cdot f(y) \cdot f^{-1}(x) \cdot f^{-1}(y).$$

By the preceding theorem, since $f(x) \cdot f(y) \cdot f^{-1}(x) \cdot f^{-1}(y)$ is a commutator element of the Abelian group G/N, it is true that $f(xyx^{-1}y^{-1}) = e'$. Hence $xyx^{-1}y^{-1}$ is in the kernel of f, which is N. This implies $Z \subset N$.

Now, suppose $Z \subset N$. Let u and v be elements of G/N. There exists elements x and y in G such that $f(x) = u$ and $f(y) = v$. Since $xyx^{-1}y^{-1} \in Z$ implies $xyx^{-1}y^{-1} \in N$,

$$f(xyx^{-1}y^{-1}) = f(x) \cdot f(y) \cdot f^{-1}(x) \cdot f^{-1}(y) = e',$$

and $f(x) \cdot f(y) = f(y) \cdot f(x)$. Hence G/N is Abelian.

As an illustration of the content of the last theorem as well as the concepts of normality, factor groups, and inner automorphisms, let us consider the following example [2, page 482]:

Example: Let G be a group, Φ a homomorphism of G onto G such that Φ commutes with every inner automorphism of G. Define K as the set of all elements x of G, where $\Phi(\Phi(x)) = \Phi(x)$. Show K is a normal subgroup of G and G/K is Abelian.

Proof: It is clear that for all y and z in G,

$[\Phi f_y](z) = [f_y \Phi](z)$ implies

$$[\Phi f_y](z) = \Phi(yzy^{-1}) = [f_y \Phi](z) = y\Phi(z)y^{-1},$$

i.e., $\Phi(yzy^{-1}) = y\Phi(z)y^{-1}$. The following assertions are made and justified.

<u>Assertion 1</u>: K is a subgroup of G.

<u>Proof</u>: Let a and b ϵ K.

$$\Phi(\Phi(ab^{-1})) = \Phi(\Phi(a)\Phi(b^{-1})) = \Phi(\Phi(a))\cdot\Phi(\Phi^{-1}(b)) =$$

$$\Phi(a)\cdot\Phi(\Phi^{-1}(b)) = \Phi(a)\cdot[\Phi(\Phi(b))]^{-1} = \Phi(a)\cdot\Phi^{-1}(b) =$$

$$\Phi(a)\cdot\Phi(b^{-1}) = \Phi(ab^{-1}).$$

Hence $ab^{-1} \in$ K, and K is a subgroup of G.

<u>Assertion 2</u>: K is normal in G.

<u>Proof</u>: Let $k \in$ K and $y \in$ G.

$$\Phi(\Phi(yky^{-1})) = \Phi(y\Phi(k)y^{-1}) = y\Phi(\Phi(k))y^{-1} =$$
$$y\Phi(k)y^{-1} = \Phi(yky^{-1})$$

implies yky^{-1} is in K, and K is normal in G.

<u>Assertion 3</u>: G/K is Abelian.

<u>Proof</u>: Let y and z be in G. It is sufficient to show that $yzy^{-1}z^{-1} \in$ K, which implies by Theorem 1.10 that G/K is Abelian.

$$\Phi(\Phi(yzy^{-1}z^{-1})) = \Phi(\Phi(yzy^{-1})\cdot\Phi(z^{-1})) = \Phi(y\cdot\Phi(z)\cdot y^{-1}\cdot\Phi^{-1}(z)) =$$

$$\Phi(y)\cdot\Phi[\Phi(z)y^{-1}\Phi^{-1}(z)] = \Phi(y)\Phi(z)\Phi^{-1}(y)\Phi^{-1}(z) = \Phi(yzy^{-1}z^{-1}),$$

which implies $yzy^{-1}z^{-1} \in$ K.

Having seen earlier the correspondence between normality and invariance under inner automorphism, we now turn our attention to subgroups invariant under all automorphisms of the group.

Definition: A subgroup H of a group G is called a characteristic subgroup of G if H is invariant under all automorphisms of G.

It is clear that a characteristic subgroup is normal in G. Furthermore, G and $\{e\}$ are examples of characteristic subgroups.

Theorem 1.11: The center C is a characteristic subgroup.

Proof: Let c be in C. For all g in G, gc = cg. Let Φ be an automorphism of G.

$$\Phi(g)\cdot\Phi(c) = \Phi(gc) = \Phi(cg) = \Phi(c)\cdot\Phi(g).$$

Since $\Phi(g)$ varies over G as g varies, $\Phi(c)$ is in C, and, thus, C is a characteristic subgroup.

We state the following corollary, which may be proved in a similar manner as Theorem 1.11.

Corollary: G/C is a characteristic subgroup.

Theorem 1.12: Z is a characteristic subgroup.

Proof: The proof is immediate, since for z in Z, and Φ an automorphism of G,

$$\Phi(z) = \Phi(a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_n b_n a_n^{-1} b_n^{-1}) = \Phi(a_1)\Phi(b_1)\Phi^{-1}(a_1)\Phi^{-1}(b_1)$$

$$\cdots\Phi(a_n)\Phi(b_n)\Phi^{-1}(a_n)\Phi^{-1}(b_n),$$ which is in Z.

We are now ready to investigate a normal subgroup introduced by Norman Levine [5, page 61].

Definition: The set of all elements a in G such that for any b in G, ab = ba implies there is an element c in G such that $a = c^i$ and $b = c^j$, where i and j are integers, is called the rim of G. The rim of G is denoted by R(G).

It can be readily shown [5, page 61] that the identity, e, of G is in the rim of G and, also, that the inverse of any element a in R(G) is itself in R(G). However, in general, the rim of G is not a subgroup of G. For example, in the group of symmetries of a square [1, page 114], we find that R(G) consists of the elements I, R, and R". Since R"$\cdot$R" = R' which is not in R(G), it follows that the rim in this case is not a subgroup.

Theorem 1.13: If a is in R(G), then for all b in G, $bab^{-1} \in R(G)$.

Proof: Let $(bab^{-1})x = x(bab^{-1})$ for some x in G. Multiplying on the left by b^{-1}, and on the right by b yields $a(b^{-1}xb) = (b^{-1}xb)a$. This implies there is an element c in G such that $a = c^i$ and $b^{-1}xb = c^j$ since a is in R(G). We may write bab^{-1} as $bc^ib^{-1} = (bcb^{-1})^i$. Also $b^{-1}xb = c^j$ implies $x = bc^jb^{-1} = (bcb^{-1})^j$. Hence, there is an element bcb^{-1} in G such that $bab^{-1} = (bcb^{-1})^i$ and $x = (bcb^{-1})^j$, for i and j positive integers, i.e., $bab^{-1} \in R(G)$.

<u>Definition</u>: The set of all finite products of the rim of G is called the <u>anticenter</u> of G, and is denoted by AC(G).

<u>Theorem 1.14</u>: AC(G) is a normal subgroup of G.

<u>Proof</u>: AC(G) contains the identity, e, of G, is closed under multiplication, and contains the inverse of every element a in AC(G). Hence AC(G) is a subgroup. Now, let $b \in G$ and $a \in AC(G)$. Since a is a finite product of rim elements, $a_1, a_2, \ldots, a_n$, we have

$$bab^{-1} = b(a_1 \cdot a_2 \cdots a_n)b^{-1} = (ba_1b^{-1})(ba_2b^{-1})\cdots(ba_nb^{-1}).$$

By the previous theorem, each product ba_ib^{-1} for $i = 1,2,\ldots,n$ is in R(G), hence $bab^{-1} \in AC(G)$, and AC(G) is normal.

<u>Theorem 1.15</u>: AC(AC(G)) = AC(G).

<u>Proof</u>: Since $AC(AC(G)) \equiv \{a \mid a$ is a finite product of the rim of $AC(G)\}$, it suffices to show that $R(G) \subset R(AC(G))$. This implies that AC(G) will be the set of all finite products of the rim of AC(G), hence the theorem is proved.

Let a be in R(G), b be in AC(G) and ab = ba. There exists an element c in G such that $a = c^j$ and $b = c^k$, where j and k are integers. Let s be the least positive integer such that c^s is in AC(G). We assert that j and k are both divisible by s. Otherwise, suppose j is not divisible by s. Then $j = ms + n$, where $0 < n < s$. Now $c^j = c^{ms} \cdot c^n$. Since $c^s \in AC(G)$, it follows that $c^{ms} \in AC(G)$. Also, $c^j = a$

is in AC(G). We, therefore, have that c^n is in AC(G). This contradicts the fact that s is the least positive integer such that $c^s \in AC(G)$, since $n < s$. Thus, j, and similarly k, are divisible by s. Denote c^s by d. Hence $a = c^j = (c^s)^t$ since $j = st$ for some integer t. Also, $b = c^k = (c^s)^p$ since $k = sp$ for some integer p. We therefore have $ab = ba$ implying that there is an element d in AC(G) such that $a = d^t$ and $b = d^p$, i.e., $a \in R(AC(G))$. It follows immediately that $R(G) \subset R(AC(G))$, which gives the desired result.

Theorem 1.16: If H is a subgroup of G, then $R(G) \cap H \subset R(H)$.

Proof: Let $a \in R(G) \cap H$ and $b \in H$ such that $ab = ba$. Since a in in R(G), there is a c in G such that $a = c^j$ and $b = c^k$. Let s be the least positive integer such that $c^s \in H$. As in the proof of the previous theorem, it follows that j and k are divisible by s. Hence $a = c^j = (c^s)^u$ and $b = c^k = (c^s)^v$ for some integers u and v. Thus $a \in R(H)$ and $R(G) \cap H \subset R(H)$.

The concepts introduced by Levine may be extended to observe the behavior of the rim and the anticenter under isomorphism.

Theorem 1.17: If groups G and G' are isomorphic under the mapping f, the $f(R(G)) = R(G')$.

Proof: Let $f(a) \in f(R(G))$ and $b' \in G'$. There is an element b in G such that $f(b) = b'$. Suppose $f(a) \cdot f(b) = f(b) \cdot f(a)$. This implies $f(ab) = f(ba)$, or equivalently $ab = ba$. Since a is in $R(G)$, there is an element c in G where $a = c^i$ and $b = c^j$. Hence, there is an element $f(c)$ in G' such that $f(a) = f(c^i) = [f(c)]^i$ and $f(b) = f(c^j) = [f(c)]^j$, i.e., $f(a) \in R(G')$. It follows that $f(R(G)) \subset R(G')$.

Now, suppose $a' \in R(G')$. There is an element a in G such that $f(a) = a'$. We must show that a is in $R(G)$. Let $ab = ba$ for some b in G.

$f(ab) = f(a)\cdot f(b) = f(ba) = f(b)\cdot f(a)$ implies

there is an element c in G where $f(a) = [f(c)]^i$ and $f(b) = [f(c)]^j$. Hence $a = c^i$ and $b = c^j$, which implies $a \in R(G)$. It follows that $R(G') \subset f(R(G))$, and the equality results.

Theorem 1.18: $AC(G)$ is a characteristic subgroup.

Proof: The proof is immediate from the previous theorem, since an automorphism of G carries rim elements of G into rim elements of G.

Theorem 1.19: If $G \cong G'$ under f, then $AC(G) \cong AC(G')$.

Proof: Let Φ be the mapping: $a \to f(a)$, where $a \in AC(G)$. Since f is well-defined, one-to-one, and product-preserving, so is Φ. Now, suppose $a' \in AC(G')$. Hence $a' = a_1'.a_2'\cdots a_n'$, where each $a_i' \in R(G')$, $i = 1,2,\ldots,n$. By the previous theorem, $a_1' = f(a_1)$, $a_2' = f(a_2)$, ..., $a_n' = f(a_n)$ where each $a_i \in R(G)$. Hence, there is an element $a = a_1\cdot a_2\cdots a_n$ in $AC(G)$ such that $\Phi(a) = f(a) = a'$, and the mapping is onto. Hence $AC(G) \cong AC(G')$.

In the next chapter, we shall characterize ideals of a ring which play the role of normal subgroups of a group.

CHAPTER II

THE ROLE OF IDEALS IN A RING

The concept of normal subgroups in a group has an analogue in the theory of rings, namely the ideals of a ring. We now proceed to describe various ideals as well as to investigate the corresponding manner in which they decompose their respective rings.

<u>Definition</u>: A non-empty subset A of a ring R is called a <u>left ideal</u> (<u>right ideal</u>) of R if and only if:

(i) A is a subring of R, i.e., ab is in A and a-b is in A for all a and b in A.

(ii) For any r in R and a in A, ra (ar) is in A.

If, in (ii) above, both ra and ar are in A, then A is called a <u>two-sided ideal</u> or simply an <u>ideal</u>. Clearly all ideals in a commutative ring are two-sided.

For example, in the ring of all real matrices of order n, the set of all matrices of the form

$A = (a_{ij})_n$ where $a_{ij} = 0$ for $i = 2,\ldots,n$ and $j = 1,2,\ldots,n$

and $a_{ij} \neq 0$ for $i = 1$ and $j = 1,\ldots,n$

constitutes a right ideal, but not a left ideal, whereas the set of all real matrices of the form

$A = (a_{ij})_n$ where $a_{ij} = 0$ for $i \neq j$ and $a_{ij} \neq 0$ for $i = j$

constitutes a two-sided ideal.

<u>Theorem 2.1</u>: The intersection of an arbitrary system of left (right) ideals of a ring R is itself a left (right) ideal of R.

<u>Proof</u>: Let A_i be a system of left ideals of R where i ranges over the set of positive integers, and let D be the intersection of these ideals. D is non-void, since 0 belongs to each ideal, and, hence, 0 is in D. Let a and b $\in$ D. This implies a and b are in each A_i. Since a-b is in each A_i, a-b $\in$ D.

Now, let r $\in$ R and d $\in$ D. rd is in each A_i, hence rd is in D. D is therefore a left ideal. A similar proof holds for right ideals.

We may thus speak of the smallest ideal containing a subset S of R, or the intersection of every ideal containing S.

<u>Definition</u>: Let S be a non-empty subset of the ring R. The left, right, or two-sided <u>ideal generated by</u> S is the smallest left, right, or two-sided ideal, respectively, containing S, and is denoted by (S). If S concists of a single element a, then (a) is called the <u>principal</u> (left, right, or two-sided) <u>ideal</u> generated by a.

Clearly, if R has a unit element e, (e) = R. Also, if b is any element of R having an inverse, (b) = R. Thus the ideal (S) generated by the set of elements S = $\{a,b,\ldots\}$ of the ring R is the set of all elements of R expressible as finite sums of terms, each term being a finite product of elements of R, at least one of which is in the set S. The left ideal generated by S consists of all elements of R expressible a finite sums of terms of the form $rs + ns$ where $r \in R$, $s \in S$ and n is an integer. A similar description can be given for the right ideal generated by S.

The principal left (right) ideal (a) consists of all elements of the form $ra + na$ $(ar + na)$. If R has a unit element e, the principal left (right) ideal (a) consists of all elements of the form ra (ar).

As an example of a principal ideal, it may be verified that in the ring of integers, every ideal is a principal ideal [6, page 56].

Let us now define the center of a ring R.

<u>Definition</u>: The <u>center</u> of a ring R is the set of all elements a of R such that $ar = ra$ for all r in R. We denote the center of ring R by C_R.

<u>Theorem 2.2</u>: The center of a ring R is a commutative subring of R.

<u>Proof</u>: Let a and $b \in C_R$. For any r in R,

$$(a-b)r = ar-br = ra-rb = r(b-a).$$

Hence a-b is in C_R. Also,

$$(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab).$$

This implies $ab \in C_R$, and C_R is a subring of R, which is obviously commutative.

We now proceed to further characterize properties of ideals.

Definition: An ideal M of a ring R is called maximal (divisorless) in R if and only if M is contained in R properly, and for any ideal Q of R, $M \subset Q \subset R$ implies $Q = R$.

Definition: An ideal M of a ring R is called minimal in R if $M \neq (0)$, and for any ideal Q of R, $Q \subset M$ implies $Q = (0)$.

Theorem 2.3: A minimal ideal is a principal ideal.

Proof: Let M be a minimal ideal in ring R. $M \neq (0)$ implies there is an x in M such that x is not the zero element. Consider the ideal generated by x. Since every element of a ring can generate a principal ideal, x generates the ideal (x). Any ideal containing x must contain the ideal (x). Thus M contains (x). However, since M is minimal, it contains no proper ideals except (0). It follows that (x) = M. Since (x) is a principal ideal, M is a principal ideal.

That the converse of this theorem is false may be shown by the following counterexample:

Counterexample: Let I denote the ring of integers. Since every ideal in I is principal, we choose some arbitrary non zero integer n and consider the ideal (n). We wish to show that (n) is not a minimal ideal. Suppose (n) = M is a minimal ideal. Consider the ideal (2n). Clearly, $(2n) \subset (n)$. Let us show this inclusion is proper. The element n is in (n).

Suppose (2n) contained n. Then n could be expressed as $n = 2n \cdot r$ where $r \in I$. Since I is an integral domain and n is non zero, we get $1 = 2r$ which is a contradiction. Thus, (2n) is properly contained in (n). Since (n) is minimal by assumption, this implies (2n) = (0), an obvious contradiction. It follows that the principal ideal (n) is not minimal.

The above example serves to prove the result:

<u>Theorem 2.4</u>: The ring of integers contains no minimal ideals.

In the preceding chapter we investigated various normal subgroups and their corresponding factor groups. Since ideals are normal subgroups of the additive group of a ring R, it follows that an ideal S defines a partition of R into disjoint cosets called residue classes modulo the ideal N.

<u>Definition</u>: The <u>residue</u> <u>class</u> , $\overline{x} = \{r \mid r \equiv x(\mathrm{mod} N)\}$, is the set of all elements r in R congruent to x modulo the ideal N.

It is clear that the set of residue classes of R modulo the ideal N forms a ring under the operations:

$$\overline{a} + \overline{b} = \overline{a + b} \text{ and } \overline{a} \cdot \overline{b} = \overline{ab}.$$

This is called the residue class ring of R modulo N and is denoted by R/N.

<u>Theorem 2.5</u>: Let R be a ring with unity and M an ideal in R. M is maximal if and only if R/M is a field.

Proof: Assume M is maximal. Since R contains the unit element e, R/M contains the residue class $\bar{e}$. Hence R/M is a ring with unity. We must show, for any $\bar{a}$ in R/M where $\bar{a} \neq 0$, there is an inverse element $(\bar{a})^{-1}$ in R/M such that $(\bar{a})^{-1} \cdot \bar{a} = \bar{e}$. Let $\bar{a}$ be a non zero element of R/M. Thus $a \not\equiv 0 (\text{mod } M)$. This implies a is not in M. Consider the ideal N generated by all elements of the form $xa + m$ where $m \in M$ and $x \in R$. Obviously, $M \subset N$. Since M is maximal, the ideal N must generate the ring R. Hence there is an element x' in R and m' in M such that $e = x'a + m'$. This implies $x'a-e = 0 + (-m')$ where $-m'$ is in M. Hence $x'a \equiv e (\text{mod } M)$. It follows that $\bar{x}' \cdot \bar{a} = \bar{e}$ and $\bar{x}' = (\bar{a})^{-1}$ is the inverse of $\bar{a}$ and R/M is a field.

Now, assume R/M is a field. We assert M is maximal. Since R/M is a field, it contains at least two elements. For this reason $M \neq R$. Let Q be an ideal in R that contains M properly. We must show that $Q = R$. Let a belong to Q and not to M, and let b be in R. Since R/M is a field, there is an $\bar{x}$ in R/M such that $\bar{x} \cdot \bar{a} = \bar{b}$. This implies $xa \equiv b (\text{mod } M)$. Hence $xa-b \equiv 0 (\text{mod } M)$, and $xa-b$ belongs to M. Let $xa-b = m_1$. It follows that $b = xa-m_1$. Since a is in Q, xa is in Q. Also $-m_1$ is in Q since $M \subset Q$. Thus b is an element of Q. It follows that $R \subset Q$, or $R = Q$. We therefore have that M is a maximal ideal.

Definition: The ideal P in a commutative ring R is prime if and only if ab belonging to P implies a is in P or b is in P.

Let us observe that this definition implies P is a prime ideal if and only if $ab \equiv 0 (\text{mod } P)$ implies $a \equiv 0 (\text{mod } P)$ or $b \equiv 0 (\text{mod } P)$. In a proof similar to the previous theorem, we may establish the following result:

Theorem 2.6: Let P be an ideal in R such that $P \neq R$. P is a prime ideal if and only if R/P is an integral domain.

From this theorem it follows that in a commutative ring with unity, every maximal ideal is prime. That the converse of this theorem is false is shown by the following counterexample:

Counterexample: Let I[x,y] be the ring R of polynomials with integral coefficients. Since I[x,y] is an integral domain [1, page 67], if a product of two polynomials has x as a factor, then at least one of the polynomials must have x as a factor. Hence (x) is prime in R. The ideal (x), however, is properly contained in (x,y), which is the ideal consisting of all polynomials in two variables with constant term zero. (x,y) is obviously not R itself. Hence (x) is not maximal.

In order to interrelate the concepts of principal, maximal, and prime ideals, we have the following results:

<u>Theorem 2.7</u>: In a principal ideal domain R, i.e., an integral domain in which every ideal is principal, the prime ideals coincide with ideals of the form (p), where p is a prime element.

<u>Proof</u>: Let p be a prime element in R. Consider the ideal (p). Let x and y $\in$ R such that xy belongs to (p). This implies xy = pr for some r in R. Since p is a prime, $p|xy$ implies $p|x$ or $p|y$. Hence x is in (p) or y is in (p). It follows that (p) is a prime ideal.

Now suppose q is not a prime element in R. Consider the ideal (q). Since q is not prime, q = ab, where neither a nor b is a divisor of unity and ab belongs to (q). Suppose a belongs to (q). This implies that there is a c in R such that a = qc. Thus a = qc = abc. Since R is an integral domain, it follows that 1 = bc which implies that b is a divisor of unity, contrary to our initial assumption. Hence b is not in (q). In a similar manner, we may show that a is not in (q). We have shown that (q) is not a prime ideal if q is not a prime element.

<u>Theorem 2.8</u>: Let R be a principal ideal domain. A non zero ideal P is prime if and only if it is maximal.

<u>Proof</u>: Obviously, if P is maximal in R then P is prime. It suffices to show that if P is a prime ideal $\neq$ (0), then P is maximal. By the previous theorem, P = (p) where p is a prime element of R. P $\neq$ R obviously, since R = (1) and 1 is not a prime element of R. Hence P is properly

contained in R. Let Q be an ideal of R such that $P \subset Q$. We must show $Q = R$. Since Q properly contains P, there is an element a in Q that is not in P. It follows that $(a,p) = 1$. This implies $1 = ra + sp$ where r and s belong to R. We have the ideal (a,P) generated by elements of the form $ra + sp$ for r and s in R. Hence, it follows that

$$R = (1) \subset (a,P) \subset Q \subset R.$$

This implies equality between Q and R. Thus $Q = R$, and P is maximal.

We concluded the first chapter by investigating a normal subgroup, the anticenter, derived from integral powers of group elements, with the property that the operation of forming the anticenter is idempotent, i.e., $AC(G) = AC(AC(G))$. Furthermore, we found that the anticenter is invariant under automorphisms of the group. It is therefore fitting to develop an analogous ideal, formed by considering integral powers of ring elements, having similar properties.

<u>Definition</u>: Let R be a commutative ring and $A \neq R$ be an ideal of R. The <u>radical of A</u> is defined as
$\sqrt{A} \equiv \{a \mid a \in R \text{ and } a^i \in A \text{ for some positive integer } i\}$.

Let us note that the radical of R is defined as the set of all elements x such that $x^n \equiv 0 \pmod{R}$ for some positive integer n. This definition is in accordance with the fact that $x^n \equiv 0 \pmod{R}$ implies x^n is in R for some positive integer n.

Theorem 2.9: $\sqrt{A}$ is an ideal of R containing A.

Proof: Let a and b belong to $\sqrt{A}$. This implies a^i and b^j are in A where i and j are positive integers. Consider the expansion of $(a-b)^{i+j-1}$. Since R is commutative, every term in the expansion contains either a^i or b^j as a factor. Hence $(a-b)^{i+j-1}$ is in A, $i+j-1$ is a positive integer and a-b is in $\sqrt{A}$. Moreover, for any r in R, $(ra)^i = r^i a^i$, which is in A. Thus $ra \in \sqrt{A}$ and $\sqrt{A}$ is an ideal of R. That $\sqrt{A}$ contains A is trivial.

Theorem 2.10: If A and B are ideals and $A \subset B$, then $\sqrt{A} \subset \sqrt{B}$.

Proof: Let c belong to $\sqrt{A}$. There is a positive integer m such that c^m is in A. This implies c^m is in B, hence c is in $\sqrt{B}$.

Theorem 2.11: $\sqrt{\sqrt{A}} = \sqrt{A}$.

Proof: Since $A \subset \sqrt{A}$, by the previous theorem we have $\sqrt{A} \subset \sqrt{\sqrt{A}}$. Now, let $c \in \sqrt{\sqrt{A}}$. This implies c^m is in $\sqrt{A}$ for some positive integer m. $(c^m)^n$ is thus in A for $(c^m)^n = c^{mn}$ implies there is some positive integer $k = mn$ such that c^k is in A. Hence c is in $\sqrt{A}$, and it follows that $\sqrt{\sqrt{A}} \subset \sqrt{A}$. We then have the equality $\sqrt{A} = \sqrt{\sqrt{A}}$.

With the preliminary definitions and results we have established, we are now able to compare in an analytical manner various analogous concepts of normal subgroups and ideals.

CHAPTER III

ANALOGOUS CONCEPTS OF NORMAL SUBGROUPS AND IDEALS

We now wish to compare normal subgroups and ideals with respect to set properties, homomorphisms and isomorphisms, direct products and direct sums. Basic to the comparison are the concepts of set theory.

Theorem 3.1: The intersection of an arbitrary set of normal subgroups of a group G is itself a normal subgroup of G.

Proof: Let S_i be a system of normal subgroups of G where i ranges over the set of positive integers, and let D be the intersection of these subgroups. D is non-void, since the group identity, e, belongs to each normal subgroup, and, hence, e is in D. Let a and $b \in D$. This implies a and b are in each S_i. Since ab^{-1} is in each S_i $ab^{-1} \in D$, and D is a subgroup.

Now, let $g \in G$ and $d \in D$. It follows that d is in each S_i, hence gdg^{-1} is in each S_i. This implies gDg^{-1} is in D, and D is normal.

In chapter II, it was proved that the intersection of an arbitrary system of ideals in a ring R is itself an ideal of R.

<u>Definition</u>: Let $\{S_i\}_{i=1}^{n}$ be a finite system of subgroups of a group G. The <u>union</u> of these subgroups, denoted by $\cup S_n$, is the set of all finite products, each factor of the product belonging to some S_i.

<u>Theorem 3.2</u>: The union of a finite system of normal subgroups of a group G is itself normal in G.

<u>Proof</u>: Let $\{S_i\}_{i=1}^{n}$ be a finite system of normal subgroups of G, and let D be the union of these subgroups. Also, let a and b $\in$ D. Thus, $a = a_1 \cdot a_2 \cdots a_m$, where each a_j, $1 \leq j \leq m$, is in some S_i. Likewise $b = b_1 \cdot b_2 \cdots b_k$, where each b_j, $1 \leq j \leq k$, is in some S_i. It follows that

$$ab^{-1} = a_1 \cdot a_2 \cdots a_m \cdot b_k^{-1} \cdot b_{k-1}^{-1} \cdots b_1^{-1}$$

is a finite product, each factor of the product belonging to some S_i. Hence $\cup S_n$ is a subgroup.

Now, let $g \in G$ and $d \in D$. Since d belongs to D, $d = d_1 \cdot d_2 \cdots d_p$ where each d_p is in some S_i.

$$gdg^{-1} = g(d_1 \cdot d_2 \cdots d_p)g^{-1} = (gd_1g^{-1})(gd_2g^{-1}) \cdots (gd_pg^{-1}).$$

Since each S_i is normal, the factors gd_jg^{-1}, $1 \leq j \leq p$, are in some S_i, and hence $gDg^{-1} \subset D$. D is normal, and the proof is completed.

<u>Definition</u>: Let $\{A_i\}_{i=1}^{n}$ be a finite system of subrings

of a ring R. The <u>sum</u> of these subrings, denoted by $A_1 + A_2 + \ldots + A_n$, is the set of all elements r in R such that $r = a_1+a_2+\ldots+a_n$ where each a_i, $1\leq i\leq n$, belongs to A_i.

<u>Theorem 3.3</u>: The sum of a finite system of ideals in a ring R is itself an ideal in R.

<u>Proof</u>: Let $\{A_i\}_{i=1}^{n}$ be a finite system of ideals in R, and let D be the sum of these ideals. Also, let a and b $\in$ D. Thus,

$a = a_1+a_2+\ldots+a_n$, where each $a_i \in A_i$, $1\leq i\leq n$ and

$b = b_1+b_2+\ldots+b_n$, where each $b_i \in B_i$, $1\leq i\leq n$.

It follows that

$$a-b = (a_1+a_2+\ldots+a_n) - (b_1+b_2+\ldots+b_n) = (a_1-b_1)+\ldots+(a_n-b_n).$$

Since each A_i is an ideal, each $a_i-b_i \in A_i$. Hence $a-b \in D$.

Now let r be in R and d be in D. It follows that

$$rd = r(d_1+d_2+\ldots+d_n) = rd_1+rd_2+\ldots rd_n$$

where each rd_i is in A_i. Hence $rd \in D$, and D is an ideal in R.

<u>Definition</u>: Let $\{S_i\}_{i=1}^{n}$ be a finite system of subgroups of a group G. The product of these subgroups, denoted by ΠS_n, is the set of all elements g in G such that $g = s_1\cdot s_2\cdots s_n$ where each s_i belongs to S_i.

Theorem 3.4: The product of a finite system of normal subgroups of a group G is itself normal in G.

Proof: The proof is exactly like the proof of Theorem 3.2.

We observe that in any finite system of subgroups, not necessarily normal, the product of the subgroups is, in general, properly contained in the union of the subgroups. However, we have the following result:

Theorem 3.5: In a finite system of normal subgroups, the product of the subgroups is equal to their union.

Proof: Let $\{S_i\}_{i=1}^{n}$ be a finite system of normal subgroups. It is clear that $\prod S_n \subset \cup S_n$. We wish to show that $\cup S_n \subset \prod S_n$. Let b be in $\cup S_n$. Hence $b = b_1 \cdot b_2 \cdots b_m$ where each b_j, $1 \leq j \leq m$, is in some S_i. Furthermore, suppose one of the factors of b, call it b_k, is in S_1 and no factor b_j where $j<k$ is in S_1. Since we may insert the factor e in the product without altering b, such an element b_k in S_1 exists. Since each S_i is normal, we may permute the factors of b as follows:

$b_{k-1} \cdot b_k = b_k \cdot b'_{k-1}$ where b_{k-1}, b'_{k-1} are in the same S_i,

$b_{k-2} \cdot b_k = b_k \cdot b'_{k-2}$ where b_{k-2}, b'_{k-2} are in the same S_i,

$\cdots$

$b_1 \cdot b_k = b_k \cdot b'_1$, where b_1, b'_1 are in the same S_i.

Hence $b = b_k \cdot b'_1 \cdot b'_2 \cdots b'_{k-1} \cdot b_{k+1} \cdots b_m$. By repeating the same process, we can rearrange the factors of b, inserting the identity element whenever needed, so that

$$b = s_1 \cdot s_2 \cdots s_n \quad \text{where each } s_i \in S_i.$$

It follows that $b \in S_n$, or $\cup S_n \subset \Pi S_n$. This implies equality.

<u>Definition</u>: Let $\{A_i\}_{i=1}^{n}$ be a finite system of subrings of a ring R. The <u>product</u> of these subrings, denoted by ΠA_i, is the set of all finite sums, each term of the sum a product of n factors, each factor of the product belonging to some A_i.

<u>Theorem 3.6</u>: The product of a finite system of ideals of a ring R is itself an ideal.

<u>Proof</u>: Let $\{A_i\}_{i=1}^{n}$ be a finite system of ideals, and let B be their product. Also let b_1 and $b_2 \in B$.

$$b_1 = a_{11} \cdot a_{12} \cdots a_{1n} + \cdots + a_{k1} \cdot a_{k2} \cdots a_{kn} \quad \text{and}$$

$$b_2 = b_{11} \cdot b_{12} \cdots b_{1n} + \cdots + b_{j1} \cdot b_{j2} \cdots b_{jn}.$$

It follows that

$$b_1 - b_2 = \sum_{i=1}^{k} a_{i1} \cdots a_{in} - \sum_{i=1}^{j} b_{j1} \cdots b_{jn} =$$

$$\sum_{i=1}^{k} a_{i1} \cdots a_{in} + \sum_{i=1}^{j} (-b_{j1}) \cdots b_{jn}.$$

Hence $b_1 - b_2 \in \Pi A_i$. Also, for r in R, and b in ΠA_i, it is clear that rb is in ΠA_i. The product, ΠA_i, is therefore an ideal.

We observe that in a ring with unity, the sum of a system of ideals is contained in the product of the ideals.

Let us now consider an illustration of the concept of set theory.

Example: Let I be the ring of integers and let the ideal $A = (9)$ and the ideal $B = (12)$. $A \cap B$ is the set of all integers which are multiples of both 9 and 12, namely, $A \cap B = (36)$. The sum, $A + B$ is the set of all integers which can be expressed in the form $9a+12b$ where a and $b \in I$. From elementary number theory, we know that $A + B = (3)$.

Having seen the parallel thus far between the roles of normal subgroups and ideals in respect to set theory, we naturally wish to see if the parallel extends to the notions of homomorphism and isomorphism.

In the first chapter, we proved the Fundamental Homomorphism Theorem for Groups. We now consider a homomorphism f from a ring R onto a ring R'.

Lemma 1: The kernel of f, K_f, is an ideal.

Proof: Since K_f is a normal subgroup under addition, if a and $b \in K_f$, $a-b \in K_f$. Now let r be in R and a be in K_f.

$$f(ar) = f(a) \cdot f(r) = 0' \cdot f(r) = 0',$$

where $0'$ is the additive identity element of R'. Hence K_f is an ideal.

Lemma 2: $a \equiv b(\text{mod } K_f)$ if and only if $f(a) = f(b)$.

Proof: Suppose $a \equiv b(\text{mod } K_f)$. Then, $a = b+x$ where x is in K_f. Then,

$$f(a) = f(b+x) = f(b) + f(x) = f(b) + 0' = f(b).$$

Now, suppose $f(a) = f(b)$. Since both a and b ϵ R, a-b is in R, and $f(a-b) = f(a) - f(b) = 0$. Hence $a \equiv b(\text{mod } K_f)$.

Theorem 3.7: If f is a homomorphism from ring R onto ring R', then $R/K_f \cong R'$.

Proof: Let us denote the coset of the factor ring R/K_f containing a as $\bar{a}$. Hence $\bar{a}$ is the residue class containing a.

Let the mapping Φ be given by $\Phi: \bar{a} \rightarrow f(a)$. By Lemma 2, the mapping Φ is well-defined and one-to-one. Let a' ϵ R'. Since f is a homomorphism, there is an element a in R such that $f(a) = a'$. Hence there is a residue class $\bar{a}$ containing a in R/K_f such that $\Phi(\bar{a}) = f(a) = a'$, and Φ is onto. Lastly,

$$\Phi(\bar{a}+\bar{b}) = \Phi(\overline{a+b}) = f(a+b) = f(a) + f(b) = \Phi(\bar{a}) + \Phi(\bar{b})$$

and $\Phi(\bar{a}\cdot\bar{b}) = \Phi(\overline{ab}) = f(ab) = f(a)\cdot f(b) = \Phi(\bar{a})\cdot\Phi(\bar{b})$.

Thus, $R/K_f \cong R'$.

The next theorems further develop the relations between normal subgroups and ideals under homomorphisms as well as utilize set properties previously developed.

Theorem 3.8: Let f be a homomorphism mapping the group G onto a group G' with kernel K_f. Let H be the set of all subgroups U of G that contain K_f, and let H' be the set of all subgroups V of G'. Then the following are true:

(i) There is a one-to-one function Φ from H onto H' given by $\Phi(U) = f(U)$.

(ii) If U is normal in G, then $\Phi(U)$ is normal in G', and conversely.

(iii) If U is normal if G, $G/U \cong G'/\Phi(U)$.

<u>Proof of (i)</u>: Let V be in H'. First, we wish to find a subgroup U in H such that $\Phi(U) = V$. This will show that Φ maps H onto H'. Let $U = f^{-1}(V)$. Hence $U = \{x \mid x \in G$ and $f(x) \in V\}$. Since e', the identity element of G', is in V, $f^{-1}(e') = K_f$ is contained in $f^{-1}(V) = U$. Now, let x and $y \in U$.

$$f(x^{-1}y) = f(x^{-1})\cdot f(y) = f^{-1}(x)\cdot f(y)$$

which is in V, since V is a subgroup. Hence $x^{-1}y$ is in U. We now have a subgroup U of G containing K_f, i.e., $U \in H$. $\Phi(U) = f(U) = \{f(g) \mid g \in U\} = \{f[f^{-1}(h)] \mid h \in V\} = \{h \mid h \in V\} = V$. Hence $\Phi(U) = V$ and Φ maps H onto H'. It remains to show that Φ is a one-to-one function.

Suppose $\Phi(U_1) = \Phi(U_2)$. Let x be in U_1. There is a y in U_2 such that $f(x) = f(y)$ since $\Phi(U) = f(U)$ for all U in H.

$$f(x\cdot y^{-1}) = f(x)\cdot f^{-1}(y) = f(x)\cdot f^{-1}(x) = e'.$$

Hence $x\cdot y^{-1}$ is in K_f. Since $U_2 \subset H$, this implies $K_f \subset U_2$ or $x\cdot y^{-1}$ is in U_2. Hence $x = x(y^{-1}y) = (xy^{-1})y$, which is in U_2. It follows that x is in U_2 or $U_1 \subset U_2$. In a similar manner, it can be shown that $U_2 \subset U_1$. As a result $U_1 = U_2$ and the mapping Φ is one-to-one.

<u>Proof of (ii)</u>: Let us assume U is normal in G. Let g' be in G'. There is a g in G such that $f(g) = g'$. Let y be in $\Phi(U)$. There is an x in U such that $f(x) = y$ since

$\Phi(U) = f(U)$. Now,

$g' \cdot y \cdot (g')^{-1} = f(g) \cdot f(x) \cdot [f(g)]^{-1} = f(g)f(x)f(g^{-1}) = f(gxg^{-1})$.

Since U is normal in G, gxg^{-1} is in U and $f(gxg^{-1})$ is in V. Hence $g' \cdot V \cdot (g')^{-1} \subset V$ or $V = \Phi(U)$ is normal in G'.

To prove the converse, let us assume V is normal in G'. We must show U is normal in G. Let $x \in U$ and $g \in G$. $f(x) = y$. Since V is normal in G', there is a z in V such that $f(g) \cdot y \cdot f^{-1}(g) = f(g) \cdot f(x) \cdot f(g^{-1}) = f(gxg^{-1}) = z$. Hence gxg^{-1} is in U or $gUg^{-1} \subset U$. This implies U is normal in G.

<u>Proof of (iii)</u>: We must show if U is normal in G, then $G/U \cong G'/\Phi(U)$. Let us define f_1 as a mapping G' onto $G'/\Phi(U)$. By the Fundamental Theorem, f_1 is a homomorphism of G' onto $G'/\Phi(U)$ with kernel $K_{f_1} = \Phi(U)$ and the identity element of $G'/\Phi(U)$ is the coset $\Phi(U)$ which, of course, is normal since U is normal in G. Now, let f_2 be the mapping: $G \to G'/\Phi(U)$ where for all g in G, $f_2(g) = f_1[f(g)]$. Since the product of two homomorphisms is itself a homomorphism [8, page 36], f_2 is a homomorphism of G onto $G'/\Phi(U)$. K_{f_2} is the set of all elements of G which map onto the identity of $G'/\Phi(U)$, which is the coset $\Phi(U)$. Hence $K_{f_2} = U$. It follows that $G/U \cong G'/\Phi(U)$ and the theorem is proved.

We now state the corresponding theorem for rings which is proved in an almost identical manner.

<u>Theorem 3.9</u>: Let f be a homomorphism from a ring R onto a ring R' with kernel K_f. Let A be the set of all subrings S of R that contain K_f, and let A' be the set of all subrings T of R'. Then the following are true:

(i) There is a one-to-one function Φ from A onto A' given by $\Phi(S) = f(S)$.

(ii) If S is an ideal in R, then $\Phi(S)$ is an ideal in A', and conversely.

(iii) If S is an ideal in R, $R/S \cong R'/\Phi(S)$.

Let us recall that in chapter I we found that if two groups G and G' were isomorphic under the mapping f, then $f(AC(G)) = AC(G')$. As a further analogy between the anti-center of a group and the radical of an ideal, we utilize Theorem 3.9 to establish the following:

<u>Theorem 3.10</u>: If rings R and R' are isomorphic under the mapping f, and A is an ideal of R containing K_f, then $f(\sqrt{A}\,) = \sqrt{f(A)}$.

<u>Proof</u>: Since A is an ideal in R containing K_f, f(A) is an ideal in R' by Theorem 3.9. Suppose $f(x) \in f(\sqrt{A}\,)$. Since x is in $\sqrt{A}$, there is a positive integer i such that x^i is in A. Hence $f(x^i) = [f(x)]^i$ is in f(A) implies $f(x) \in \sqrt{f(A)}$. This shows $f(\sqrt{A}\,) \subset \sqrt{f(A)}$.

Now suppose f(x) is in $\sqrt{f(A)}$. There is a positive integer i such that $[f(x)]^i \in f(A)$. This implies

$f(x^i) \in f(A)$ or $x^i \in A$. Hence x is in $\sqrt{A}$ and $f(x) \in f(\sqrt{A})$. It follows that $\sqrt{f(A)} \subset f(\sqrt{A})$ and the equality ensues.

The next theorems indicate the interrelating concepts of set theory and isomorphism.

Lemma 1: If H is a subgroup of G and N is a normal subgroup of G, HN is a subgroup of G, and N is normal in HN.

Proof: Since N is normal in G, HN = NH. Let h_1n_1 and h_2n_2 be in HN.

$$(h_1n_1)(h_2n_2)^{-1} = (h_1n_1)(n_2^{-1}h_2^{-1}) = (h_1n_1n_2^{-1})(h_2^{-1}) = (h_1n_3)(h_2^{-1})$$

where $n_1n_2^{-1} = n_3$. Since N is normal, $h_1n_3 = n_4h_1$. Hence

$$(h_1n_3)(h_2^{-1}) = (n_4h_1)h_2^{-1} = (n_4)(h_1h_2^{-1}) = n_4h_3 \text{ where } h_1h_2^{-1} = h_3.$$

Now n_4h_3 is in NH which is HN. Hence $(h_1n_1)(h_2n_2)^{-1}$ is in HN, and HN is a subgroup of G. Obviously N is normal in HN since N is normal in G.

Lemma 2: $H \cap N$ is a normal subgroup of H.

Proof: We know $H \cap N$ is a subgroup of H. Now, let x be in $H \cap N$ and h be in H. hxh^{-1} is in H and also in N. Hence hxh^{-1} is in $H \cap N$, or $H \cap N$ is normal in H.

Theorem 3.11: If H is a subgroup of G and N is a normal subgroup of G, then $H/(H \cap N) \cong HN/N$.

Proof: Let us consider the natural homomorphism f of G onto G/N given by $f: g \to gN$. We wish to show that $f(H) = HN/N$ with kernel $H \cap N$. Consider the set $f^{-1}[f(H)]$.

We first must show that $f^{-1}[f(H)] = HN$. Now,

$$f^{-1}[f(H)] = \{g \mid g \in G \text{ and } f(g) \in f(H)\}.$$

Let $x \in f^{-1}[f(H)]$. There is an h in H such that $f(x) = f(h)$. From a previous theorem, $f(x) = f(h)$ implies that the cosets xN and hN are equal, i.e., x is in hN. It follows that there is an element n_1 in N such that $x = hn_1$. This proves that x is in HN, or $f^{-1}[f(H)]$ belongs to HN. Conversely, let $y \in HN$. Then $y = hn$, where h is in H and n is in N. Hence

$$f(y) = f(hn) = f(h) \cdot f(n) = f(h) \cdot e',$$

since N is the kernel of f. Hence $f(y) = f(h)$ implies that $f(y)$ is in $f(H)$ or $y \in f^{-1}[f(H)]$. It follows that HN belongs to $f^{-1}[f(H)]$ and the desired result ensues.

Since HN is a subgroup with N normal in HN, we may form HN/N. Suppose $f(x) \in f(H)$. We have that $x \in f^{-1}[f(H)] = HN$. It follows that $x = h_1n_1$ and $f(x) = f(h_1n_1) = (h_1n_1)N$. This implies $f(x) \in HN/N$, or $f(H) \subset HN/N$. Conversely, let $f(g) \in HN/N$. $f(g) = (h_2n_2)N = h_2N$, which implies $f(g)$ is in $f(H)$ or $HN/N \subset f(H)$. Thus, $f(H) = HN/N$, and f is a homomorphis mapping of H onto HN/N.

Lastly, $f(h) = f(e)$ if and only if $h \in N$. It follows that $H \cap N$ is the kernel of this mapping and $H/(H \cap N) = HN/N$.

<u>Theorem 3.12</u>: If M and N are ideals of the ring R, then $M/(M \cap N) = (M + N)/N$.

<u>Proof</u>: This theorem is proved in a similar manner to

the preceding theorem. We observe that $M + N$ and $M \cap N$ are ideals, and consider the homomorphism f from R onto R/N. We show f induces a homomorphism from N onto $(M + N)/N$ with kernel $M \cap N$.

Using our knowledge of set theory and effects of homomorphism on groups and rings, we consider the possibility of building up a group from normal subgroups and building up a ring from ideals. To this end, we define the direct product of a set of normal subgroups, and the direct sum of a set of ideals.

<u>Definition</u>: The <u>direct product</u> $H = G_1 \times G_2 \times \ldots \times G_n$ of a finite set of normal subgroups, $\{G_1, G_2, \ldots, G_n\}$ is the set $\{(a_1, a_2, \ldots, a_n) \mid a_i \in G_i\}$ and multiplication is defined by: $(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, a_3b_3, \ldots, a_nb_n)$.

We observe that the operation is clearly well-defined, and its associativity follows at once from the associativity of the operations in the groups G_i. The identity of H is $e = (e_1, e_2, \ldots, e_n)$ and the inverse of $a = (a_1, a_2, \ldots, a_n)$ is $(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$. Hence H is a group.

<u>Definition</u>: The <u>direct sum</u> $S = R_1 \oplus R_2 \oplus \ldots \oplus R_n$ of a finite set of ideals $\{R_1, R_2, \ldots, R_n\}$ is the set given by $\{(a_1, a_2, \ldots a_n) \mid a_i \in R_i\}$ and addition and multiplication are defined by:

$(a_1,a_2,\ldots a_n) + (b_1,b_2,\ldots b_n) = (a_1+b_1, a_2+b_2,\ldots,a_n+b_n)$ and

$(a_1,a_2,\ldots a_n)\cdot(b_1,b_2,\ldots,b_n) = (a_1b_1,a_2b_2,\ldots,a_nb_n)$.

Again, we note that this set S has well-defined operations, is an Abelian group under addition, and is associative and distributive with respect to addition under multiplication. Hence S is a ring.

Theorem 3.13: Suppose $\{G_1,G_2,\ldots,G_n\}$ are subgroups of a group G such that:

(i) Each G_i is normal in G.

(ii) $G = \pi G_i$, $i=1,2,\ldots,n$.

(iii) $G_i \cap G'_i = e$, where $G'_i = G_1\cdot G_2\cdots G_{i-1}\cdot G_{i+1}\cdots G_n$,

i.e., $G'_i = \pi G_j$, $j\neq i$.

Then for any g_i in G_i and any g_j in G_j where $i\neq j$, $g_ig_j = g_jg_i$, and for any g in G, g is uniquely expressible in the form $g = g_1\cdot g_2\cdots g_n$, where g_i is in G_i.

Proof: Let $g_i \in G_i$ and $g_j \in G_j$ with $i\neq j$. Since G_i and G_j are both normal, we have

$$(g_i\cdot g_j\cdot g_i^{-1})g_j^{-1} = g_i(g_j\cdot g_i^{-1}\cdot g_j^{-1}) \quad G_i\cap G_j \subset G_i\cap G'_i$$

as defined in (iii) of the hypothesis. Since $G_i\cap G'_i = e$, we have $(g_i\cdot g_j\cdot g_i^{-1})g_j^{-1} = e$ or $g_ig_j = g_jg_i$.

Now suppose $g \in G$ where $g = a_1\cdot a_2\cdots a_n$ and $g = b_1\cdot b_2\cdots b_n$. It follows that $b_1^{-1}a_1 = (b_2\cdots b_n)(a_n^{-1}\cdots a_2^{-1})$. By what we have just established, $b_1^{-1}a_1 = (b_2a_2^{-1})\cdots(b_na_n^{-1})$ and $b_1^{-1}a_1$ is in $G_1 \cap G'_1$ as in hypothesis (iii). Since $G_1 \cap G'_1 = e$, $b_1^{-1}a_1 = e$, and this implies $a_1 = b_1$. In a similar manner, $a_2 = b_2$, $a_3 = b_3, \ldots, a_n = b_n$. Thus the representation of every element in G is unique.

<u>Theorem 3.14</u>: Suppose $\{R_1, R_2, \ldots, R_n\}$ are subrings of a ring R such that:

(i) Each R_i is an ideal of R.

(ii) $R = R_1 \oplus R_2 \oplus \ldots \oplus R_n$.

(iii) $R_i \cap R'_i = 0$ where $R'_i = R_1 \oplus R_2 \oplus \ldots \oplus R_{i-1} \oplus R_{i+1} \oplus \ldots \oplus R_n$.

Then any r in R is uniquely expressible in the form $r = r_1 + r_2 + \ldots + r_n$, where $r_i \in R_i$.

<u>Proof</u>: Since R is an Abelian group under addition, $r_i + r_j = r_j + r_i$. Suppose r G where $r = a_1 + a_2 + \ldots + a_n$ and also, $r = b_1 + b_2 + \ldots + b_n$. It follows that

$$a_1 - b_1 = b_2 + \ldots + b_n + (-a_n) + (-a_{n-1}) + \ldots + (-a_2).$$

Since R is Abelian,

$$a_1 - b_1 = (b_2 - a_2) + (b_3 - a_3) + \ldots + (b_n - a_n).$$

Each $b_j - a_j$ is in the ideal R_j, hence $a_1 - b_1$ $R_1 \cap R'_1$ as defined in (iii) of the hypothesis. This implies $a_1 - b_1 = 0$ or $a_1 = b_1$. Similarly, $a_2 = b_2$, $a_3 = b_3$, $\ldots$, $a_n = b_n$. Each element of R is therefore uniquely represented.

<u>Theorem 3.15</u>: If group G has normal subgroups $G_1, G_2, \ldots, G_n$ such that $G = \prod G_i$ where $i=1,2,\ldots n$ and $G_i \cap G'_i = e$ where $G'_i = \prod G_j$, $j \neq i$, then $G \cong G_1 \times G_2 \times \ldots \times G_n$.

<u>Proof</u>: Let f be the mapping $G \to G_1 \times G_2 \times \ldots \times G_n$ given by $f(g) = f(g_1 \cdot g_2 \cdots g_n) = (g_1, g_2, \ldots, g_n)$. By Theorem 3.13, $g = g_1 \cdot g_2 \cdots g_n$ is a unique expression of g. This uniqueness guarantees that f is one-to-one and the operation is well-defined. f is evidently onto since any product $g_1 \cdot g_2 \cdots g_n$ is an element of G. Now, suppose a and b are in G.

$f(ab) = f(a_1 \cdot a_2 \cdot a_3 \cdots a_n)(b_1 \cdot b_2 \cdots b_n)] = f[(a_1 b_1) \cdots (a_n b_n)]$, since the elements of distinct G_i's commute with each other. We have that

$$f[(a_1 b_1)(a_2 b_2) \cdots (a_n b_n)] = (a_1 b_1, \ldots, a_n b_n) =$$
$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = f(a) \cdot f(b).$$

Hence f preserves the group operation. We have proved that $G \cong G_1 \times G_2 \times \ldots \times G_n$.

It is interesting to note that this property may also be formulated for rings.

<u>Theorem 3.16</u>: If ring R has ideals $R_1, R_2, \ldots, R_n$ such that $R = \sum_{i=1}^{n} R_i$ and $R_i \cap R'_i = 0$, where $R'_i = \Sigma R_j$ for $j \neq i$, then $R \cong R_1 \oplus R_2 \oplus \ldots \oplus R_n$.

Proof: Let f be the mapping $R \to R_1 \oplus R_2 \oplus \cdots \oplus R_n$ given by $f(r) = f(r_1+r_2+\cdots+r_n) = (r_1,r_2,\ldots,r_n)$. By Theorem 3.14, $r = r_1+r_2+\cdots r_n$ is a unique expression of r and guarantees that f is well-defined and one-to-one. f is onto since any sum $r_1+r_2+\cdots+r_n$ is in R. Let us now consider both operations of addition and multiplication under f. Suppose a and b are in R.

$$f(a+b) = f[(a_1+a_2+\cdots+a_n) + (b_1+b_2+\cdots+b_n)] =$$
$$f[(a_1+b_1)+(a_2+b_2)+\cdots+(a_n+b_n)] = (a_1+b_1, a_2+b_2,\ldots,a_n+b_n) =$$
$$(a_1,a_2,\ldots,a_n) + (b_1,b_2,\ldots,b_n) = f(a) + f(b).$$

Also, $f(ab) = f[(a_1+a_2+\cdots+a_n)\cdot(b_1+b_2+\cdots+b_n)] =$

$$f[a_1(b_1+b_2+\cdots+b_n) + \cdots + a_n(b_1+b_2+\cdots+b_n)].$$

Since R is a ring, $a_i(b_1+\cdots+b_n) = a_ib_i + 0 = a_ib_i$, for $b_1+\cdots+b_{i-1}+b_{i+1}+\cdots+b_n$ is in R'_i. Hence

$$f(ab) = f(a_1b_1+a_2b_2+\cdots+a_nb_n) =$$
$$(a_1b_1,a_2b_2,\ldots,a_nb_n) = (a_1,a_2,\ldots,a_n)\cdot(b_1,b_2,\ldots,b_n) =$$
$$f(a)\cdot f(b).$$

Since f preserves both ring operations, it follows that $R \cong R_1 \oplus R_2 \oplus \cdots \oplus R_n$.

As illustrations of the direct product of a group and the direct sum of a ring, let us consider the following examples:

Example: Let G be the group of real numbers under

F, it follows that b is in A. Hence every element of F is in A, or A = F. This suffices to show that every field is a simple ring.

Wedderburn proved perhaps the most important theorem concerning the structure of simple rings, a recent and short proof of which may be found in [3, pages 385-386].

Wedderburn's Theorem: Any simple ring R is isomorphic to the ring of all m square matrices over a field F, where the field F and the integer m are uniquely defined by R. Conversely, for any integer m and any field F, the set of all m square matrices over F is a simple ring.

APPENDIX

ANALOGOUS THEOREMS

Groups	Rings
Theorem 1.4	Theorem 3.7
Theorem 1.14 (anticenter)	Theorem 2.9 (radical)
Theorem 1.15 (anticenter)	Theorem 2.11 (radical)
Theorem 1.16 (anticenter)	Theorem 2.10 (radical)
Theorem 1.19 (anticenter)	Theorem 3.10 (radical)
Theorem 3.1	Theorem 2.1
Theorem 3.2	Theorem 3.3
Theorem 3.4	Theorem 3.6
Theorem 3.8	Theorem 3.9
Theorem 3.11	Theorem 3.12
Theorem 3.13	Theorem 3.14
Theorem 3.15	Theorem 3.16

BIBLIOGRAPHY

1. Birkhoff, Garrett, and Saunders MacLane. _A Survey of Modern Algebra_. New York: Macmillan Co., 1960.

2. Chambers, Herbert. "Elementary Problems for Solution", _Amer. Math. Monthly_, 55(1948), 482.

3. Henderson, D.W. "A Short Proof of Wedderburn's Theorem", _Amer. Math. Monthly_, 72(1965), 385-386.

4. Kurosh, A.G. _General Algebra_. New York: Chelsea Publishing Co., 1963.

5. Levine, Norman. "On the Anticenter of a Group", _Amer. Math. Monthly_, 67(1960), 61-62.

6. McCoy, Neal H. _Rings and Ideals_. Buffalo: Mathematical Association of America, 1948.

7. Van der Waerden, B.L. _Modern Algebra_. New York: Frederick Ungar Publishing Co., 1953.

8. Zassenhaus, Hans J. _The Theory of Groups_. New York: Chelsea Publishing Co., 1958.

VITA

Ellen Joyce Stone

Born in West Chester, Pennsylvania, December 20, 1939. Graduated from Woodrow Wilson High School in Portsmouth, Virginia, 1956, A. B., Old Dominion College, 1960. Teaching Fellow at the University of North Carolina, 1960-61. From September, 1961 until June, 1964, the author was an Instructor at Old Dominion College.

In September, 1964, the author entered the College of William and Mary as an M. A. candidate and Lecturer in the Department of Mathematics.