SOME PROPERTIES OF RINGS AND IDEALS

APPROVED:

Major Professor

Russell G. Bilyeu

Minor Professor

H. C. Parrish

Director of the Department of Mathematics

Robert B. Toulouse

Dean of the Graduate School

SOME PROPERTIES OF RINGS AND IDEALS

THESIS

Presented to the Graduate Council of the
North Texas State University in Partial
Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

By

Jere B. Higgins, B. A.

Denton, Texas
August, 1964

TABLE OF CONTENTS

CHAPTER I

RINGS

The purpose of this paper will be to investigate certain properties of algebraic systems known as rings. The proofs, in most cases, are based on definitions and theorems in this paper. A basic knowledge of the algebra of sets is assumed.

Definition 1-1. A set R will be called a ring if R satisfies the following properties:

PI. R is closed with respect to the binary operations $\oplus$ and $*$. These operations will be called "addition" and "multiplication."

PII. If a, b, $c \in R$, then the following properties are true:

(1) $a \oplus (b \oplus c) = (a \oplus b) \oplus c$

(2) $a*(b*c) = (a*b)*c$

(3) $a \oplus b = b \oplus a$

(4) $a*(b \oplus c) = a*b \oplus a*c$

(5) $(b \oplus c)*a = b*a \oplus c*a$

PIII. There exists an element $o \in R$ such that $0 \oplus a = a$ for every $a \in R$.

PIV. Given $a \in R$, there is an $x \in R$ such that $x \oplus a = 0$.

Note that the $o \in R$ is not necessarily the real number zero.

The following systems are examples of rings.

Example 1-1. Let V denote the set consisting of the totality of ordered n-tuples of real numbers. Let $\alpha = \{\alpha_1, \alpha_2, \dots \alpha_n\}$ and $B = \{B_1, B_2, \dots B_n\}$ be elements of V.

$$\alpha \oplus B = \{\alpha_1 + B_1, \alpha_2 + B_2, \dots \alpha_n + B_n\}$$

$$\alpha * B = \{\alpha_1 B_1, \alpha_2 B_2, \dots \alpha_n B_n\}$$

V is closed under the operations of $\oplus$ and * since the real number system is closed with respect to addition and multiplication. Therefore, PI is satisfied. Due to the corresponding properties of real numbers, PII is satisfied. For PIII let $0 = \{0_1, 0_2, \dots 0_n\}$ where 0_i is the real number zero. Therefore $0 \oplus \alpha = \alpha$. In order to satisfy PIV, let $x = \{-\alpha_1, -\alpha_2, \dots -\alpha_n\}$.

Then $x \oplus \alpha = \{\alpha_1 - \alpha_1, \alpha_2 - \alpha_2, \dots \alpha_n - \alpha_n\} = \{0_1, 0_2 \dots\} = 0$.

Therefore V is a ring with respect to $\oplus$ and *.

Example 1-2. Suppose C is the class of all functions f(x) of the real variable x defined and continuous on the closed interval $[0, 1]$. If $f, g \in C$, let $(f \oplus g)(x) = f(x) + g(x)$ and $(f*g)(x) = f(x).g(x)$. Since f(x) and g(x) are defined and continuous on $[0,1]$, $f(x) + g(x)$ and $f(x)\cdot g(x)$ are also defined and continuous on $[0,1]$. Therefore, $(f \oplus g)(x)$ and $(f*g)(x) \in C$ and PI is satisfied. Again PII is satisfied due to the corresponding properties of real numbers.

Let $e(x) \equiv 0$ for $x \in [0,1]$. Since $e(x)$ is defined and continuous on $[0,1]$, $e(x) \in C$.

$$\begin{aligned}(e \oplus f)(x) &= e(x) + f(x)\\ &= 0 + f(x)\\ &= f(x).\end{aligned}$$

Hence PIII is satisfied. Finally if $f(x) \in C$, $-f(x)$ also belongs to C and PIV follows since $(f \oplus -f)(x) = f(x)-f(x)=0$. Therefore C is a ring.

Example 1-3. Let F denote the set of rational numbers and let x and y be indeterminants. Then the set of polynomials in x and y with coefficients in F is a ring. It is from this ring that an important example will be constructed in Chapter III.

Some basic properties of a ring are stated in the following four lemmas.

Lemma 1-1. Given $a \in R$, the element $x \in R$ such that $x \oplus a = 0$ is unique and will be denoted by the symbol $-a$.

Proof: Let y be any element of R such that $y \oplus a = 0$.

$$\begin{aligned}&x \oplus a = y \oplus a\\ &(x \oplus a) \oplus x = (y \oplus a) \oplus x\\ &x \oplus (a \oplus x) = y \oplus (a \oplus x)\\ &x \oplus 0 = y \oplus 0\\ &x = y.\end{aligned}$$

Lemma 1-2. $0*a = a*0 = 0$ for $a \in R$.

Proof: Let $a,b \in R$. Since $b = b \oplus 0$, $b*a = (b \oplus 0)*a =$ $b*a \oplus 0*a$.

$$-b*a \oplus b*a = -b*a \oplus (b*a \oplus 0*a)$$
$$0 = (-b*a \oplus b*a) \oplus 0*a$$
$$0 = 0 \oplus 0*a$$
$$0 = 0*a$$

In a similar manner it can be shown that $a*0 = 0$.

Lemma 1-3. Suppose R is a ring. If S is the "sum" of any n elements of R, any insertion of parentheses will yield the same "sum" S.

Proof by induction: For $n = 1$ the result is trivial. For $n = 3$ $(a_1 \oplus a_2) \oplus a_3 = a_1 \oplus (a_2 \oplus a_3) =$ $a_1 \oplus a_2 \oplus a_3$ by PII. $\sum_1^k a_i$ is independent of the manner in which parentheses are inserted.

$$\sum_1^k a_i = a_1 \oplus \sum_2^k a_i$$

$$\sum_1^k a_i \oplus a_{k+1} = a_1 \oplus \sum_2^k a_i \oplus a_{k+1}$$
$$= a_1 \oplus \left(\sum_2^k a_i \oplus a_{k+1}\right)$$
$$= \left(a_1 \oplus \sum_2^k a_i\right) \oplus a_{k+1}$$
$$= \sum_1^{k+1} a_i .$$

Since inside each parenthesis there are exactly k elements, parentheses may be inserted in any way desired about these k elements. Therefore $\sum_{1}^{k+1} a_i$ is independent of parentheses; hence this is true for any positive integer n. The proof for * is similar.

<u>Lemma 1-4</u>. If $a,c \in R$. then $-(a*c) = -a*c = a*(-c)$.

Proof: If $c \in R$, then $c \oplus -c = 0$.

But $a*(c \oplus -c) = a*c \oplus a*(-c) = 0$.

By lemma 1-1, $-(a*c)$ is unique. Therefore, $a*(-c) = -(a*c)$. Similarly it can be shown that $-(a*c) = -a*c$.

In certain algebraic systems some of the properties of a ring may be replaced with equivalent properties. It will be assumed that these algebraic systems are non-empty.

<u>Theorem 1-1</u>. Suppose R is an algebraic system with all the properties of a ring except for PIII and PIV. R is a ring if and only if for $a,b \in R$ the equation $a \oplus x = b$ has a solution in R.

Proof: Suppose for $a,b \in R$ the equation $a \oplus x = b$ has a solution in R. In particular, there is $x \in R$ such that $a \oplus x = a$ and there is a $y \in R$ such that $b \oplus y = b$. Furthermore there are elements $y', x' \in R$ such that $a \oplus y' = y$ and $b \oplus x' = x$. But $y = a \oplus y' = a \oplus x \oplus y' = a \oplus y' \oplus x = y \oplus x$ and $x = b \oplus x' = b \oplus y \oplus x' = b \oplus x' \oplus y = x \oplus y = y \oplus x$. Therefore, $x = y$ and the existence of a zero is established.

For $0, a \in R$ the equation $a \oplus x = 0$ also has a solution. This fact establishes PIV. Conversely, if R is a ring for $a, b \in R$ the equation $a \oplus x = b$ has a solution in R. Namely $x = b \oplus -a$.

<u>Theorem 1-2</u>. Let R be an algebraic system which, except for commutativity of $\oplus$ is a ring. If $a*b = a*c$ with $a \neq 0$ implies $b = c$, then R is a ring.

Proof: Let $a, b \in R$. Then $a \oplus b$ and $b \oplus a \in R$. Let c denote any non-zero element of R. $c*(a \oplus b)$ and $-c*(b \oplus a) \in R$.

$$c*(a \oplus b) = c*a \oplus c*b$$

$$-c*(b \oplus a) = -c*b \oplus -c*a$$

$$\begin{aligned}\left[c*(a \oplus b)\right] \oplus \left[-c*(b \oplus a)\right] &= \left[(c*a) \oplus (c*b)\right] \oplus \left[(-c*b) \oplus (-c*a)\right] \\ &= \left[(c*a) \oplus (-c*a)\right] \oplus \left[(c*b) \oplus (-c*b)\right] \\ &= 0 \oplus 0 \\ &= 0\end{aligned}$$

Therefore $c*(a \oplus b) = c*(b \oplus a)$; hence $a \oplus b = b \oplus a$ and R is a ring.

<u>Theorem 1-3</u>. Suppose R and S are two distinct rings. Let $R \times S$ denote the set of all ordered pairs (a,b) where $a \in R$ and $b \in S$. Then $R \times S$ is a ring if "addition" and "multiplication" are defined in the following manner:

$$(a,b) \oplus (c,d) =_d (a \oplus_r c,\ b \oplus_s d)$$

$$(a,b)*(c,d) =_d (a *_r c,\ b *_s d).$$

Proof: Note that PI is satisfied since $a \oplus_r c$, $a *_r c \in R$ and $b \oplus_s d$, $b *_s d \in S$ because both R and S are rings. Let (a,b), (c,d), (h,f) $\in R \times S$. Then $\left[(a,b) \oplus (c,d)\right] \oplus (h,f) = \left[(a \oplus_r c,\ b \oplus_s d)\right] \oplus (h,f) = (a \oplus_r c \oplus_r h,\ b \oplus_s d \oplus_s f)$ and $(a,b) \oplus \left[(c,d) \oplus (h,f)\right] = (a,b) \oplus \left[(c \oplus_r h,\ d \oplus_s f)\right] = (a \oplus_r c \oplus_r h,\ b \oplus_s d \oplus_s f)$.

The remaining properties of PII can be shown in a similar manner. Since both R and S are rings they each contain a zero. Denote these elements as 0 and $\bar{0}$. If $(a,b) \in R \times S$, then $(a,b) \oplus (0,\bar{0}) = (a \oplus_r 0,\ b \oplus_s \bar{0}) = (a,b)$. Hence $(0,\bar{0})$ is the zero for $R \times S$. Finally if $(a,b) \in R \times S$ then $(-a,-b) \in R \times S$. $(a,b) \oplus (-a,-b) = (a \oplus_r -a,\ b \oplus_s -b) = (0,\bar{0})$. Therefore $R \times S$ is a ring.

<u>Definition 1-2</u>. A subset S of a ring R is a subring of R if S is a ring with respect to the operations of $\oplus$ and $*$ in R.

An equivalent definition for subring is the basis for the next theorem.

<u>Theorem 1-4</u>. A non-empty subset S of a ring R is a subring of R if and only if for $a,b \in S$ $a \oplus -b$ and $a*b$ are elements of S.

Proof: For $a,b \in S$ suppose $a*b$ and $a \oplus -b$ are elements of S. Therefore, S is closed with respect to $*$. If $a \in S$

then $a \oplus -a = 0 \in S$. Since $0, b \in S$, $0 \oplus -b \in S$. Therefore $a \oplus -(0 \oplus -b) \in S$.

$$-(0 \oplus -b) \oplus (0 \oplus -b) = 0$$

$$-(0 \oplus -b) \oplus -b = 0$$

$$-(0 \oplus -b) \oplus -b \oplus b = b$$

$$-(0 \oplus -b) = b$$

Therefore, $a \oplus b \in S$ hence S is closed under $\oplus$. All parts of PII hold since $S \subseteq R$. Since the zero of R is an element of S, PIII is satisfied. If a is any element of S, $0 \oplus -a$ is also an element of S. Since $a \oplus -a = 0$ PIV is satisfied and S is a subring of R. Conversely, if S is a subring of R for $a, b \in S$ $a*b \in S$. Furthermore if $b \in S, -b \in S$. Since S is closed $a \oplus -b \in S$ and the proof is complete.

In general, not all rings are commutative with respect to *. Furthermore, it is not necessary for all rings to have what is termed a unity element.

<u>Definition 1-3</u>. A ring R is said to be a commutative ring if $a*b = b*a$ for all $a, b \in R$.

<u>Definition 1-4</u>. An element h of a ring R is said to be a unity element of R if $a*h = h*a = a$ for every element $a \in R$.

Obviously, if R has a unity element it is unique.

<u>Definition 1-5</u>. Let a denote a non-zero element of a ring R. If there exists a $b \in R$, $b \neq 0$, such that either $a*b = 0$ or $b * a = 0$, a will be called a divisor of zero.

In view of the preceding definitions, the following three theorems can now be stated and proved.

<u>Theorem 1-5</u>. Suppose R is a ring with a finite number of elements which has a unity element h, but which has no divisors of 0. Then for $a \in R$, $a \neq 0$, there is an $x \in R$ such that $a*x = h$.

Proof: Let $\{a_1, a_2, a_3, \ldots a_n\} = R$. Since R has a unity element h, h is some a_i. Without loss of generality assume that $a_1 = h$. Now assume that there is an $a \in R$, $a \neq 0$, such that $a*x \neq h$ for any $x \in R$. Again without loss of generality denote this particular element as a_2. Consider the n products of the form a_2*a_j where $j = 1, 2, \ldots n$. None of these products is equal to h. Since n products have been formed and since no product is equal to a_1, there are at most n-1 distinct results. Hence, two of the products formed in this process are identical. Therefore, $a_2*a_r = a_2*a_s$. There exists $-a_s \in R$. Furthermore, since $a_2*(a_s \oplus -a_s) = a_2*0 = 0$, $a_2*a_s \oplus a_2*(-a_s) = 0$. Since $a_2*a_r = a_2*a_s$, $a_2*a_r \oplus a_2*(-a_s) = 0$. But $a_2*a_r \oplus a_2*(-a_s) = a_2*(a_r \oplus - a_s) = 0$, hence either $a_2 = 0$ or $a_r \oplus - a_s = 0$ since R has no divisors of 0. $a_2 \neq 0$ by hypothesis. Therefore, $a_r \oplus -a_s = 0$ hence $a_r = a_s$. At this point a contradiction has been reached since $a_r \neq a_s$. Therefore the assumption that there is no $x \in R$ such that $a_2*x = h$ is false and the proof is complete.

Theorem 1-6. A ring R is free of divisors of zero if, and only if, the following cancellation law holds. The equalities $a*b = a*c$ and $b*a = c*a$ imply that $b = c$, if $a \neq 0$, for otherwise arbitrary elements $a,b,c \in R$.

Proof: Suppose R has no divisor of zero. If $a*b = a*c$, $a*b \oplus (-a*c) = 0$. By lemma 1-4 $-a*c = a*(-c)$. Therefore $a*b \oplus (-a*c) = a*b \oplus a*(-c) = a*(b \oplus -c) = 0$.

Since R has no divisors of zero, either $a = 0$ or $b \oplus -c = 0$. By hypothesis $a \neq 0$. Therefore $b \oplus -c = 0$.

$$b \oplus -c = 0$$
$$b \oplus -c \oplus c = 0 \oplus c$$
$$b \oplus 0 = 0 \oplus c$$
$$b = c.$$

In a similar manner it can be shown that if $b*a = c*a$, $a \neq 0$ then $b = c$. Conversely, if $a*b = a*c$ and $b*a = c*a$ imply $b = c$, suppose $a*b = 0$ with $a \neq 0$. Since $0 = a*0$, $a*b = a*0$. Hence, $b = 0$. In a similar manner it can be shown that if $b*a = 0$, then $b = 0$.

Theorem 1-7. Let a be an element of a ring R which has no divisors of zero. If $a*a = a, a \neq 0$, then a is a unity for R.

Proof: If $b \in R$, then $b*a$ and $b*(a*a)$ are also elements of R. Since $a*a = a$, $b*a = b*(a*a)$. By PII, $b*(a*a) = (b*a)*a = b*a$. Therefore, $b*a = b$ by theorem 1-6. In addition both $a*b$ and $(a*a)*b$ are elements of R. Once again

$a*(a*b) = a*b$. Therefore by theorem 1-6 $a*b = b$. Since $a*b = b*a = b$, a is a unity for R.

<u>Definition 1-6</u>. Suppose $(R, \oplus, *)$ and $(R_1, \oplus_1, *_1)$ are rings. Let ϕ denote a mapping of R into R_1. If $\phi(a \oplus b) = \phi(a) \oplus_1 \phi(b)$ and $\phi(a*b) = \phi(a) *_1 \phi(b)$ for all $a,b \in R$, ϕ is said to be a homomorphism of R into R_1. Furthermore, if ϕ is a one-to-one mapping of R onto R_1, ϕ is called an isomorphism of R onto R_1.

Two basic properties of homomorphisms are stated in the following lemma.

<u>Lemma 1-5</u>. Let ϕ denote a homomorphism of R into R_1. If 0 is the zero of R, then $\phi(0)$ is the zero of R_1. In addition if $a \in R$, $\phi(-a) = -\phi(a)$.

Proof: Given $a \in R$, $\phi(a \oplus 0) = \phi(a) \oplus_1 \phi(0)$. Since $\phi(a \oplus 0) = \phi(a)$, $\phi(a) = \phi(a) \oplus_1 \phi(0)$. Since R_1 is a ring $-\phi(a) \in R$ such that $\phi(a) \oplus (-\phi(a)) = \bar{0}$, where $\bar{0}$ is the zero of R_1. Hence $\bar{0} = \bar{0} \oplus_1 \phi(0) = \phi(0)$. Also given $a \in R$, $\phi(a \oplus -a) = \phi(a) \oplus_1 \phi(-a)$. However, $\phi(a \oplus -a) = \bar{0}$. Therefore, $\bar{0} = \phi(a) \oplus_1 \phi(-a)$.

$$-\phi(a) \oplus_1 \bar{0} = -\phi(a) \oplus_1 \phi(a) \oplus_1 \phi(-a)$$
$$-\phi(a) = \bar{0} \oplus_1 \phi(-a)$$
$$= \phi(-a).$$

In view of lemma 1-5, theorem 1-8 follows immediately.

<u>Theorem 1-8</u>. If ϕ is a homomorphism of R into R_1, $R_1\phi \equiv_d \{\phi(a) / a \in R\}$ is a subring of R_1.

Proof: Suppose $\phi(a)$, $\phi(b) \in R_1\phi$. Since ϕ is a homomorphism, $\phi(a) *_1 \phi(b) = \phi(a*b)$. Hence $\phi(a)*_1\phi(b) \in R_1\phi$. If $\phi(b) \in R_1\phi$, $b \in R$. Hence $-b \in R$ and $\phi(-b) \in R_1\phi$. Due to lemma 1-5 $\phi(a) \oplus_1 \phi(-b) = \phi(a) \oplus_1 -\phi(b)$. Since $\phi(a) \oplus_1 \phi(-b) = \phi(a) \oplus_1 - \phi(b) = \phi(a \oplus -b)$, $\phi(a) \oplus_1 - \phi(b) \in R_1\phi$ and $R_1\phi$ is a subring of R_1 by theorem 1-4.

In theorem 1-3 it was shown that if R and S are two rings, then $R \times S$ is a ring with suitable definitions for $\oplus$ and $*$. The next theorem illustrates a homomorphism of $R \times S$ into $R \times S$.

<u>Theorem 1-9</u>. Let $R \times S$ be the ring of theorem 1-3. Then the mappings ϕ and defined by $\phi\left[(a,b)\right] = (a,\bar{o})$ and $\psi\left[(a,b)\right] = (\bar{o},b)$ are homomorphisms.

Proof: $\phi\left[(a,b) \oplus (c,d)\right] = \phi\left[(a \oplus_r c,\ b \oplus_s d)\right] = (a \oplus_r c,\bar{o})$. $\phi\left[(a,b)\right] \oplus \phi\left[(c,d)\right] = (a,\bar{o}) \oplus (c,\bar{o}) = (a \oplus_r c,\bar{o})$. Therefore, $\phi\left[(a,b) \oplus (c,d)\right] = \phi\left[(a,b)\right] \oplus \phi\left[(c,d)\right]$. In regard to $*$, $\phi\left[(a,b)*(c,d)\right] = \phi\left[(a*_r c, b*_s d)\right] = (a*_r c,\bar{o})$. $\phi\left[(a,b)\right]*\phi\left[(c,d)\right] = (a,o)*(c,\bar{o}) = (a*_r c,\bar{o})$. Hence $\phi\left[(a,b)*(c,d)\right] = \phi\left[(a,b)\right] * \phi\left[(c,d)\right]$. Therefore ϕ is a homomorphism of $R \times S$ into $R \times S$. In the same manner it can be shown that ψ is a homomorphism of $R \times S$ into $R \times S$.

Example 1-4. Consider the ring of 2×2 matricies over the real numbers. The mapping ϕ such that $\phi\left[\begin{pmatrix} a & c \\ b & d \end{pmatrix}\right] = a$ is not a homomorphism into the real numbers since

$\phi\left[\begin{pmatrix} 1 & 2 \\ o & o \end{pmatrix}\begin{pmatrix} o & o \\ 1 & o \end{pmatrix}\right] = \phi\left[\begin{pmatrix} 2 & o \\ o & o \end{pmatrix}\right] = 2$, while $\phi\left[\begin{pmatrix} 1 & 2 \\ o & o \end{pmatrix}\right] * \phi\left[\begin{pmatrix} o & o \\ 1 & o \end{pmatrix}\right] =$ $(1)(o) = o$.

If R is a ring, there are situations in which consideration of a ring which contains a subring isomorphic to R may be of interest.

Theorem 1-10. If S is a ring, and T is a set of elements in a one-to-one correspondence with the elements of S, then $\oplus_1$ and $*_1$ may be defined in T in such a way that T is a ring isomorphic to S (1, p. 83).

Proof: Since S and T are in a one-to-one correspondence ϕ, let $\psi : T \longrightarrow S$ such that if $a \in S$ then $\phi(a) \in S$ and $\psi(\phi(a)) = a$. Define $\oplus_1$ in T to be $\phi(a) \oplus_1 \phi(b) = \phi(a \oplus b)$ and define $*_1$ such that $\phi(a) *_1 \phi(b) = \phi(a*b)$. Properties PI and PII are immediately obvious since S is a ring. Let $x \in T$. There is an $a \in S$ such that $\phi(a) = x$. But $\phi(a) \oplus_1 \phi(o) = \phi(a \oplus o) = \phi(a)$ which satisfies PIII. In addition, $\phi(a) \oplus_1 \phi(-a) = \phi(o)$ which satisfies PIV.

Suppose $x, y \in T$ then $x = \phi(a)$ and $y = \phi(b)$ for some $a, b \in S$. Since $\psi(\phi(a)) \oplus \psi(\phi(b)) = a \oplus b$ and $\psi(\phi(a) \oplus_1 \phi(b)) = \psi(\phi(a \oplus b)) = a \oplus b$, $\psi(\phi(a)) \oplus \psi(\phi(b)) = \psi(\phi(a) \oplus_1 \phi(b))$.

Similarly $\psi(\phi(a)) * \psi(\phi(b)) = a*b$ and $\psi(\phi(a) *_1 \phi(b)) = \psi(\phi(a*b)) = a*b$. Hence $\psi(\phi(a)) * \psi(\phi(b)) = \psi(\phi(a) *_1 \phi(b))$. Therefore T is isomorphic to S since ψ is a one-to-one onto mapping that preserves the operations.

Theorem 1-11. If R and S are rings with no elements in common, and S contains a subring S_1 which is isomorphic to R, there exists a ring T which is isomorphic to S and which contains R as a subring (1, p. 83).

Proof: Let $T = R \cup \left\{ x \in S \mid X \notin S_1 \right\}$ and let ϕ denote the isomorphism between S_1 and R. Suppose $x \in S$. Let $\psi(x) = x$ if $x \in S_1$ and $\psi(x) = \phi(x)$ if $x \in S_1$. The mapping is well defined since R and S are disjoint. Let $x \in T$ then either $x \in R$ or $x \in \left\{ x \in S \mid x \notin S_1 \right\}$. If $x \in R$ then there is an $a \in S$, such that $x = \phi(a)$. Therefore $x = \psi(a)$. If $x \in \left\{ x \in S \mid x \notin S_1 \right\}$ then $\psi(x) = x$. Hence ψ is an onto mapping. Let $x, y \in S$. Suppose $\psi(x) = \psi(y)$. Since $x \in S$, $\psi(x) = x$ or $\psi(x) = \phi(x)$. If $\psi(x) = x$, then $x = \psi(y)$. Since $y \in S$, $\psi(y) = y$ or $\psi(y) = \phi(y)$. Suppose $\psi(y) = \phi(y)$, then $\phi(y) = x$ and $x \in R$. This is impossible since R and S are disjoint. Secondly if $\psi(x) = \phi(x)$, then $\phi(x) = \psi(y)$. Since $y \in S$, $\psi(y) \neq y$. Therefore $\psi(y) = \phi(y)$. Since ϕ is a one-to-one mapping $x=y$. Therefore ψ is a one-to-one onto mapping. All that remains is to observe that S and T are in a one-to-one correspondence and apply theorem 1-10.

R is a subring of T since if $x, y \in R$, $x = \phi(a)$ and $y = \phi(b)$ for some pair $a, b \in S_1$. Since $\phi(a) * \phi(b) = \phi(a *_1 b)$, $x * y \in R$ because $a *_1 b \in S_1$. In addition $\phi(a) \oplus -\phi(b) = \phi(a \oplus_1 -b)$ and since S_1 is a subring $x \oplus -y \in R$. Therefore R is a subring of T.

The remainder of this chapter will deal with a special type of ring known as a Boolean ring.

<u>Definition 1-7.</u> A ring R is said to be a Boolean ring if for every $a \in R$, $a * a = a$.

<u>Example 1-5.</u> Let H denote any set. Suppose $X \equiv \{x/x$ is a subset of $H\}$. If $A \subseteq H$, then $A' \equiv \{x/x \in H \text{ and } x \notin A\}$. Suppose $A, B \in X$. Define $A \oplus B \equiv (A \cup B) \cap (A \cap B)'$ and $A * B \equiv A \cap B$. With these operations X is a Boolean ring.

X is closed since both $A \oplus B$ and $A * B$ are subsets of H. Before proceeding further it will be convenient to develop an equivalent expression for $A \oplus B$.

$$\begin{aligned}(A \cup B) \cap (A \cap B)' &\equiv \left[A \cap (A \cap B)'\right] \cup \left[B \cap (A \cap B)'\right] \\ &= \left[A \cap (A' \cup B')\right] \cup \left[B \cap (A' \cup B')\right] \\ &= \left[(A \cap A') \cup (A \cap B')\right] \cup \left[(B \cap A') \cup (B \cap B')\right] \\ &= (A \cap B') \cup (B \cap A') \quad .\end{aligned}$$

The verification of all parts of PII will now be examined in detail.

$$
\begin{aligned}
(1)\quad A \oplus (B \oplus C) &= \left[A \cap (B \oplus C)'\right] \cup \left[(B \oplus C) \cap A'\right] \\
&= \left[A \cap \left\{(B \cap C') \cup (C \cap B')\right\}'\right] \\
&\qquad \cup \left[\left\{(B \cap C') \cup (C \cap B')\right\} \cap A'\right] \\
&= \left[A \cap \left\{(B \cap C')' \cap (C \cap B')\right\}'\right] \\
&\qquad \cup \left[\left\{(B \cap C') \cap A'\right\} \cup \left\{(C \cap B') \cap A'\right\}\right] \\
&= \left[A \cap \left\{(B' \cup C) \cap (C' \cup B)\right\}\right] \\
&\qquad \cup \left[\left\{(B \cap C') \cap A'\right\} \cup \left\{(C \cap B') \cap A'\right\}\right] \\
&= \left[A \cap (B' \cup C) \cap C' \cup B)\right] \\
&\qquad \cup \left[\left\{(B \cap C') \cap A'\right\} \cup \left\{(C \cap B') \cap A'\right\}\right] \\
&= \left[\left\{(A \cap B') \cup (A \cap C)\right\} \cap (C' \cup B)\right] \\
&\qquad \cup \left[\left\{(B \cap C') \cap A'\right\} \cup \left\{(C \cap B') \cap A'\right\}\right] \\
&= \left(\left[(A \cap B') \cup (A \cap C)\right] \cap C'\right) \\
&\qquad \cup \left(\left[(A \cap B') \cup (A \cap C)\right] \cap B\right) \\
&\qquad \cup \left[\left\{(B \cap C') \cap A'\right\} \cup \left\{(C \cap B')\right\} \cup A'\right] \\
&= (A \cap B' \cap C') \cup (A \cap C \cap C') \cup (A \cap B \cap C) \\
&\qquad \cup \left[\left\{(B \cap C') \cap A'\right\} \cup \left\{(C \cap B') \cap A'\right\}\right] \\
&= (A \cap B' \cap C') \cup (A \cap B \cap C) \cup (B \cap C' \cap A') \\
&\qquad \cup (C \cap B' \cap A').
\end{aligned}
$$

$$
\begin{aligned}
(A \oplus B) \oplus C &= \left[(A \oplus B) \cap C'\right] \cup \left[C \cap (A \oplus B)'\right] \\
&= \left[\{(A \cap B') \cup (B \cap A')\} \cap C'\right] \\
&\qquad \cup \left[C \cap \{(A \cap B') \cup (B \cap A')\}'\right] \\
&= \left[(A \cap B' \cap C') \cup (B \cap A' \cap C')\right] \\
&\qquad \cup \left[C \cap \{(A \cap B')' \cap (B \cap A')'\}\right] \\
&= \left[(A \cap B' \cap C') \cup (B \cap A' \cap C')\right] \\
&\qquad \cup \left[C \cap \{(A' \cup B) \cap (B' \cup A)\}\right] \\
&= \left[(A \cap B' \cap C') \cup (B \cap A' \cap C')\right] \\
&\qquad \cup \left[C \cap (A' \cup B) \cap (B' \cup A)\right] \\
&= \left[(A \cap B' \cap C') \cup (B \cap A' \cap C')\right] \\
&\qquad \cup \left[\{(C \cap A') \cup (C \cap B)\} \cap (B' \cup A)\right. \\
&= \left[(A \cap B' \cap C') \cup (B \cap A' \cap C')\right. \\
&\qquad \cup \left[\{(C \cap A') \cap (B' \cup A)\} \cup \{(C \cap B) \cap (B' \cup A)\}\right] \\
&= \left[(A \cap B' \cap C') \cup (B \cap A' \cap C')\right] \\
&\qquad \cup \left[(C \cap A' \cap B') \cup (C \cap A \cap A') \cup (C \cap B \cap A)\right] \\
&= \left[(A \cap B' \cap C') \cup (B \cap A' \cap C')\right] \\
&\qquad \cup \left[(C \cap A' \cap B') \cup (C \cap B \cap A)\right] \\
&= (A \cap B' \cap C') \cup (B \cap A' \cap C') \cup (C \cap A' \cap B') \\
&\qquad \cup (C \cap B \cap A).
\end{aligned}
$$

Hence $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

(2) $A*(B*C) = A \cap (B \cap C)$.

$(A*B)*C = (A \cap B) \cap C = A \cap (B \cap C)$.

Hence $(A*B)*C = A*(B*C)$.

(3) $A \oplus B = (A \cup B) \cap (A \cap B)'$

$B \oplus A = (B \cup A) \cap (B \cap A)'$

Since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, $A \oplus B = B \oplus A$.

(4) $A*(B \oplus C) = A \cap \left[(B \cup C) \cap (B \cap C)'\right]$

$= A \cap (B \cup C) \cap (B \cap C)'$

$= \left[(A \cap B) \cup (A \cap C)\right] \cap (B' \cup C')$

$= \left[(A \cap B) \cap (B' \cup C')\right] \cup \left[(A \cap C) \cap (B' \cup C')\right]$

$= (A \cap B \cap B') \cup (A \cap B \cap C') \cup (A \cap C \cap B')$

$\cup (A \cap C \cap C')$

$= (A \cap B \cap C') \cup (A \cap C \cap B')$.

$A*B \oplus A*C = (A \cap B) \oplus (A \cap C)$

$= \left[(A \cap B) \cup (A \cap C)\right] \cap \left[(A \cap B) \cap (A \cap C)\right]'$

$= \left[(A \cap B) \cup (A \cap C)\right] \cap \left[(A' \cup B') \cup (A' \cup C')\right]$

$= \left[(A \cap B) \cup (A \cap C)\right] \cap \left[A' \cup B' \cup C'\right]$

$= \left((A \cap B) \cap \left[A' \cup B' \cup C'\right]\right) \cup \left((A \cap C) \cap \left[A' \cup B' \cup C'\right]\right)$

$= (A \cap B \cap A') \cup (A \cap B \cap B') \cup (A \cap B \cap C')$

$\cup (A \cap C \cap A') \cup (A \cap C \cap B') \cup (A \cap C \cap C')$

$= (A \cap B \cap C') \cup (A \cap C \cap B')$.

Therefore $A*(B \oplus C) = A*B \oplus A*C$.

(5) A similar proof holds for $(B \oplus C)* A$.

In the verification of PIII and PIV, $\emptyset$ will denote the empty set.

$$\emptyset \oplus A = (\emptyset \cup A) \cap (A \cap \emptyset)'$$
$$= A \cap \emptyset'$$
$$= A \cap X$$
$$= A.$$

Hence $\emptyset$ is the zero for X.

$$A \oplus A = (A \cup A) \cap (A \cap A)'$$
$$= A \cap A'$$
$$= \emptyset.$$

Therefore A = -A and PIV is satisfied. Furthermore since $A * A = A \cap A = A$, X is a Boolean ring.

Example 1-6. The set $K = \{o, 1, a, b\}$ with $\oplus$ and * defined as follows is a Boolean ring (1, p. 140).

+	o	1	a	b
o	o	1	a	b
1	1	o	b	a
a	a	b	o	1
b	b	a	1	o

*	o	1	a	b
o	o	o	o	o
1	o	1	a	b
a	o	a	a	o
b	o	b	o	b

Theorem 1-12. The Boolean ring K is isomorphic to the ring of all subsets of a two element set.

Proof: Let $\{x,y\}$ denote a two element set. The subsets of $\{x,y\}$ are $\{x\}$, $\{y\}$, $\{x,y\}$ and $\emptyset$. Therefore the ring of subsets X of $\{x,y\}$ has its elements $\{x\}$, $\{y\}$, $\{x,y\}$ and $\emptyset$. Let γ be a mapping of K onto X such that $\gamma(o) = \emptyset$, $\gamma(1) = \{x,y\}$, $\gamma(a) = \{x\}$, and $\gamma(b) = \{y\}$. If P is any element of K $\gamma(o*p) = \gamma(o) = \emptyset$ and $\gamma(o) \cap \gamma(p) = \emptyset$. Likewise $\gamma(p*o) = \gamma(p) \cap \gamma(o) = \emptyset$. Again if P is an element of K, $\gamma(1*p) = \gamma(p) = \gamma(p*1)$. While $\gamma(1) \cap \gamma(p) = \{x,y\} \cap \gamma(p) = \gamma(p)$ since $\gamma(p) \subseteq \{x,y\}$. Finally $\gamma(a*b) = \gamma(b*a)$ since $a*b = b*a = o$. Therefore $\gamma(a*b) = \emptyset$. Since $\gamma(a) \cap \gamma(b) = \{x\} \cap \{y\} = \emptyset$, $\gamma(a*b) = \gamma(a) \cap \gamma(b)$. In a similar manner it can be shown $\gamma(p) \oplus \gamma(q) = \gamma(p \oplus q)$ where $p,q \in K$. Hence K is isomorphic to the ring of subsets of a two element set.

Both example 1-5 and example 1-6 were commutative rings as well as Boolean rings. This is, in fact, true for all Boolean rings.

Lemma 1-6. Let R be a Boolean ring. If $a \in R$, $a \oplus a = o$.

Proof:
$$\begin{aligned}(a \oplus a)*(a \oplus a) &= (a \oplus a)*a \oplus (a \oplus a)*a \\ &= a*a \oplus a*a \oplus a*a \oplus a*a \\ &= a \oplus a \oplus a \oplus a.\end{aligned}$$

Since
$$\begin{aligned} a \oplus a &= a \oplus a \oplus a \oplus a, \\ -a \oplus a \oplus a \oplus -a &= -a \oplus a \oplus a \oplus a \oplus a \oplus -a \\ o \oplus o &= o \oplus a \oplus a \oplus o \\ o &= a \oplus a.\end{aligned}$$

Theorem 1-13. If R is a Boolean ring, then R is a commutative ring.

Proof: Let $a,b \in R$.

$$(a \oplus b)*(a \oplus b) = (a \oplus b)*a \oplus (a \oplus b)*b$$

$$= a*a \oplus b*a \oplus a*b \oplus b*b$$

$$= a \oplus b*a \oplus a*b \oplus b.$$

Therefore $a \oplus b = a \oplus b*a \oplus a*b \oplus b$

$$-a \oplus a \oplus b \oplus -b = a \oplus a \oplus b*a \oplus a*b \oplus b \oplus -b$$

$$o = b*a \oplus a*b.$$

Therefore $b*a = -(a*b)$. By lemma 1-6 $b*a \oplus b*a = 0$. Hence $b*a = -(b*a)$. Then by lemma 1-1, $-(b*a) = -(a*b)$ and $b*a = a*b$ follows.

CHAPTER BIBLIOGRAPHY

1. McCoy, Neal H., *Rings and Ideals*, Baltimore, The Waverly Press, 1948.

CHAPTER II

IDEALS

In the study of rings, a special type of subring plays a prominent role. This chapter will examine this type of subring known as an ideal.

Definition 2-1. A non-empty subset S of a ring R is called an ideal in R if for $a,b \in S$, $a \oplus -b \in S$, and whenever $a \in S$, $a*r$ and $r*a$ belong to S for every $r \in R$.

Theorem 2-1. If S_λ, $\lambda \in \Lambda$, is a collection of ideals in R, then $\bigcap S_\lambda$ is an ideal in R.

Proof: Suppose $a,b \in \bigcap S_\lambda$. Then a and b are elements of each S_λ hence $a \oplus -b$ is an element of each S_λ since each S_λ is an ideal. Therefore $a \oplus -b \in \bigcap S_\lambda$. Since a is an element of each S_λ, $r*a$ and $a*r$ are elements of each S_λ for $r \in R$ because each S_λ is an ideal. Hence $a*r$, $r*a$ $\in \bigcap S_\lambda$ for $r \in R$. Hence $\bigcap S_\lambda$ is an ideal in R. Note that $o \in \bigcap S_\lambda$ so that $\bigcap S_\lambda \neq \emptyset$.

Definition 2-2. Suppose A and B are sets. Let $\oplus$ and $*$ denote binary operations defined on A and B. Define $A \oplus B \equiv \{x \oplus y / x \in A,\ y \in B\}$. If a_1 is a fixed element of A, then $a_1 \oplus B \equiv \{a_1 \oplus b / b \in B\}$ and $A*a \equiv \{a*a_1 / a \in A\}$.

Before proceeding with the study of ideals, it will be necessary to prove the following theorem which deals with subrings in general.

Theorem 2-2. Suppose R is a ring and B is a subring in R. If $(a_1 \oplus B) \cap (c_1 \oplus B) \neq \emptyset$, then $a_1 \oplus B = c_1 \oplus B$.

Proof: Suppose $(a_1 \oplus B) \cap (b_1 \oplus B) \neq \emptyset$. Hence there is a $p \in (a_1 \oplus B) \cap (c_1 \oplus B)$. Therefore $p = a_1 \oplus r$ and $p = c_1 \oplus s$ where $r, s \in B$. Suppose $x \in a_1 \oplus B$, then $x = a_1 \oplus t$ where $t \in B$. Since $p = a_1 \oplus r$, $a_1 = p \oplus -r$, but $a_1 = c_1 \oplus s \oplus (-r)$. Therefore $x = c_1 \oplus s \oplus (-r) \oplus t$ $= c_1 \oplus (s \oplus (-r) \oplus t)$. However B is a subring and is closed hence $s \oplus (-r) \oplus t \in B$. Therefore $x \in c_1 \oplus B$ and $a_1 \oplus B \subseteq c_1 \oplus B$. Conversely suppose $x \in c_1 \oplus B$, then $x = c_1 \oplus h$ where $h \in B$. But $c_1 = p \oplus -s = a_1 \oplus r \oplus (-s)$. Hence $x = a_1 \oplus r \oplus (-s) \oplus h$ $= a_1 \oplus (r \oplus (-s) \oplus h)$. Therefore $x \in a_1 \oplus B$, and $c_1 \oplus B \subseteq a_1 \oplus B$.

If γ is a homomorphism between two rings R and $\overline{R}$, an ideal can be constructed in R with respect to γ.

Theorem 2-3. Let γ be a homomorphism of R onto $\overline{R}$. Then the set of elements $N\gamma$, $N\gamma = \left\{ a \in R / \gamma(a) = \overline{0} \right\}$, is an ideal in R.

Proof: $N\gamma$ is non-empty since $\gamma(0) = \bar{0}$. Suppose $a, b \in N\gamma$. Then $\gamma(a) = \bar{0}$ and $\gamma(b) = \bar{0}$. Since $\gamma(a \oplus -b) = \gamma(a) \oplus \gamma(-b) = \gamma(a) \oplus (-\gamma(b)$ by lemma 1-5, $\gamma(a \oplus -b) = \bar{0} \oplus -\bar{0} = \bar{0} \oplus \bar{0} = \bar{0}$. Therefore $a \oplus -b \in N\gamma$. Suppose $a \in N\gamma$ and let $r \in R$. Then $\gamma(r*a) = \gamma(r)* \gamma(a) = \bar{0}$ and $\gamma(a*r) = \gamma(a)* \gamma(r) = \bar{0}* \gamma(r) = \bar{0}$. Therefore $N\gamma$ is an ideal in R.

In view of theorem 2-2 if B is an ideal in R, an important ring can be constructed with respect to B.

Theorem 2-4. Suppose R is a ring and B is an ideal in R. The set $D \equiv \{a \oplus B / a \in R\}$ with appropriate operations is a ring.

Proof: Suppose $a \oplus B$, $b \oplus B \in D$. Define $(a \oplus B) \oplus (b \oplus B) \equiv (a \oplus b) \oplus B$ and $(a \oplus B)*(b \oplus B) \equiv (a*b) \oplus B$. Since the elements of D are sets, it is necessary to show that $\oplus$ and $*$ are well defined. Suppose $a \oplus B = a' \oplus B$ and $b \oplus B = b' \oplus B$. Let $x \in (a \oplus b) \oplus B$. Then $x = (a \oplus b) \oplus r$ where $r \in B$. Since $a \in a' \oplus B$ and $b \in b' \oplus B$, $a = a' \oplus t$ and $b = b' \oplus s$ where $s, t \in B$. Therefore $x = (a' \oplus t) \oplus (b' \oplus s) \oplus r = (a' \oplus b') \oplus (t \oplus s \oplus r)$. Because B is a subring, $t \oplus s \oplus r \in B$. Hence $x \in (a' \oplus b') \oplus B$. Therefore by theorem 2-2, $(a \oplus b) \oplus B = (a' \oplus b') \oplus B$. Now let $x \in a*b \oplus B$. Hence $x = a*b \oplus r$ where $r \in B$. Since $a = a' \oplus t$ and $b = b' \oplus s$, $a*b = (a' \oplus t)*(b' \oplus s) = a'*b' \oplus a'*s \oplus t*b' \oplus t*s$. But B is an ideal, so $a'*s$, $t*b'$, and $t*s$ are elements of B.

Hence $a'*s \oplus t*b' \oplus t*s \in B$. Therefore $x \in a'*b' \oplus B$ and by theorem 2-2 $a*b \oplus B = a'*b' \oplus B$. Hence $\oplus$ and $*$ are well defined.

Obviously PI is satisfied since R is a ring. A verification of PII will now be given.

$$(1)\quad \left[(a \oplus B) \oplus (b \oplus B)\right] \oplus (c \oplus B) = \left[(a \oplus b) \oplus B\right] \oplus (c \oplus B)$$
$$= \left[(a \oplus b) \oplus c\right] \oplus B$$
$$= \left[a \oplus (b \oplus c)\right] \oplus B$$
$$= (a \oplus B) \oplus \left[(b \oplus c) \oplus B\right]$$
$$= (a \oplus B) \oplus \left[(b \oplus B) \oplus (c \oplus B)\right].$$

$$(2)\quad (a \oplus B) * \left[(b \oplus B)*(c \oplus B)\right] = (a \oplus B)* \left[(b*c) \oplus B\right]$$
$$= \left[a*(b*c)\right] \oplus B$$
$$= \left[(a*b)*c\right] \oplus B$$
$$= \left[(a*b) \oplus B\right] *(c + B)$$
$$= \left[(a \oplus B)*(b \oplus B)\right] *(c \oplus B).$$

$$(3)\quad (a \oplus B) \oplus (b \oplus B) = (a \oplus b) \oplus B$$
$$= (b \oplus a) \oplus B$$
$$= (b \oplus B) \oplus (a \oplus B).$$

$$(4)\quad (a \oplus B)* \left[(b \oplus B) \oplus (c \oplus B)\right] = (a \oplus B)* \left[(b \oplus c) \oplus B\right]$$
$$= \left[a*(b \oplus c)\right] \oplus B$$
$$= \left[a*b \oplus a*c\right] \oplus B$$
$$= \left[(a*b) \oplus B\right] \oplus \left[(a*c) \oplus B\right]$$
$$= (a \oplus B)*(b \oplus B) \oplus (a \oplus B)*(c \oplus B).$$

(5) Verification is similar to (4).

Therefore PII is satisfied. If o is the zero of R, then $(a \oplus B) \oplus (o \oplus B) = (a \oplus o) \oplus B = a \oplus B$. Hence $o \oplus B$ is the zero for D. In conclusion if $a \oplus B \in D$, then $-a \in R$. But $(a \oplus B) \oplus (-a \oplus B) = (a \oplus -a) \oplus B = o \oplus B$, so $-a \oplus B$ is the inverse with respect to $\oplus$ for $a \oplus B \in D$. Therefore D is a ring.

If R is a ring and B is an ideal, the ring D of theorem 2-4 will be denoted as R/B. Recalling the ideal $N\gamma$ of theorem 2-3 furnishes theorem 2-5.

<u>Theorem 2-5</u>. Suppose $(R, \oplus, *)$ and $R_1, \oplus 1, *_1)$ are two rings. Let γ be a homomorphism of R onto R_1. Then the ring $R/N\gamma$ is isomorphic to R_1.

Proof: Let φ be the mapping of $R/N\gamma$ into R_1 defined by $\varphi(a \oplus N\gamma) = \gamma(a)$ for $a \in R$. First it is necessary to show that φ is well defined. Suppose $a \oplus N\gamma = b \oplus N\gamma$, hence $b \in a \oplus N\gamma$. Therefore $b = a \oplus x$ when $x \in N\gamma$. But $\gamma(b) = \gamma(a \oplus x) = \gamma(a) \oplus_1 \gamma(x) = \gamma(a) \oplus_1 0_1 = \gamma(a)$. Hence if $a \oplus N\gamma = b \oplus N\gamma$, $\varphi(a \oplus N\gamma) = \varphi(b \oplus N\gamma)$ and φ is well-defined. Suppose now that $\varphi(a \oplus N\gamma) = \varphi(b \oplus N\gamma)$. Then $\gamma(a) = \gamma(b)$. Hence $\gamma(a) \oplus_1 - \gamma(b) = 0_1 = \gamma(a \oplus -b)$. Therefore $a \oplus -b \in N\gamma$ and since $a = a \oplus b \oplus -b = b \oplus (a \oplus -b)$, $a \oplus N\gamma = b \oplus N\gamma$ by theorem 2-2. Therefore φ is a one-to-one mapping. This mapping is an onto mapping since γ is an onto mapping. All that remains is to show that ψ preserves the operations.

$$\psi\left[(a \oplus N\gamma) \oplus (b \oplus N\gamma)\right] = \psi\left[(a \oplus b) \oplus N\gamma\right]$$
$$= \gamma(a \oplus b)$$
$$= \gamma(a) \oplus_1 \gamma(b)$$
$$= \psi(a \oplus N\gamma) \oplus_1 \psi(b \oplus N\gamma).$$
$$\psi\left[(a \oplus N\gamma)*(b \oplus N\gamma)\right] = \psi\left[(a*b) \oplus N\gamma\right]$$
$$= \gamma(a*b)$$
$$= \gamma(a)*_1 \gamma(b)$$
$$= \psi\left[a \oplus N\gamma\right] *_1 \psi\left[b \oplus N\gamma\right].$$

In the study of ideals, there are a number of different types of ideals. The next two definitions serve as a start for a closer investigation of types of ideals.

<u>Definition 2-3</u>. Let R be a ring and let M be an arbitrary non-empty subset of R. The intersection of all ideals containing M is called the ideal generated by M and is denoted by (M). An ideal generated by a single element is called a principal ideal.

<u>Definition 2-4.</u> Let R be a ring and let B denote an ideal in R. If B has the property that when $a*b$ B, either $a \in B$ or $b \in B$; then B is called a prime ideal.

<u>Theorem 2-6</u>. Suppose R is a ring and (M) is the ideal generated by an arbitrary non-empty set of elements in R; then (M) is the "smallest" ideal in R containing M.

Proof: In order to prove theorem 2-6, it is necessary to show that $(M) \subseteq B$ where B is any ideal containing M. The proof follows immediately from the definition of (M); since if $x \in (M)$, x is an element of every ideal containing M. Hence in particular $x \in B$. Therefore $(M) \subseteq B$ for any ideal B which contains M. Hence (M) is the smallest ideal in R containing M.

<u>Theorem 2-7.</u> Let I denote the ring of integers under + and $\cdot$. Suppose $a \in I$. The set $H \equiv \{x \in I / x = ka, k \in I\}$ is (a).

Proof: Let $x, y \in H$. Then $x = ka$ and $y = k'a$. Since $x-y = (k-k')a$, $x-y \in H$. If $r \in R$ and x H, $rx = xr = rka = kra$ since $x = ka$. Therefore $xr \in H$. Note that $o \in H$, so that H is non-empty. Hence H is an ideal. H contains a since $a = 1.a$. If B is any ideal in I containing a, $ka \in B$ where $k \in I$. Therefore $H \subseteq B$. In particular $H \subseteq (a)$. But $(a) \subseteq H$ since (a) is a subset of any ideal containing a by theorem 2-6. Therefore $(a) = H$.

<u>Theorem 2-8</u>. Suppose I is the ring of integers and let p be a prime integer. If (p) is the principal ideal generated by p, then every non-zero element of I/(p) has an inverse with respect to the multiplication in I/(p).

Proof: Since I contains the unity element 1, it can be easily verified that 1 + (p) is the unity for I/(p).

There are at most p elements in $I/(p)$. This fact can be proved by showing that given any integer i, there is an integer h such that $o \leq h \leq p-1$ and $i + (p) = h + (p)$. If i is a positive integer, the proof is by induction. For $i = 1$, $1 \leq p$ for any prime p. Choose $h = 1$ if $1 < p$. If $p = 1$, choose $h = o$; since $1 + (1) = o + (1)$ because $o \in 1 + (1)$ and $o \in o + (1)$. Therefore $1 + (1) = o + (1)$ by theorem 2-2. Suppose for $i = k$, $k + (p) = h + (p)$ where $o \leq h \leq p-1$. If $k + (p) = h + (p)$, then $[k + (p)] + [1 + (p)] = [h + (p)] + [1 + (p)]$. Hence $[k + 1] + (p) = [h + 1] + (p)$. Since $h \leq p-1$, $h + 1 \leq p$. If $h + 1 < p$, then $h + 1 \leq p-1$ and proof is complete. If $h + 1 = p$, then $[k + 1] + (p) = o + (p)$ since $p \in o + (p)$. Therefore if i is a positive integer, there is an h such that $o \leq h \leq p-1$ and $i + (p) = h + (p)$. If i is a negative integer, $i + (p) = -i[p-1] + (p)$ since $-i[p-1] = -ip + i = i - ip = i + [-ip]$. Therefore $-i[p-1]$ belongs to $i + (p)$ and $-i[p-1] + (p)$. Hence $i + (p) = -i[p-1] + (p)$ by theorem 2-2. Observe $i - ip > o$ except for $p = 1$. If $p = 1$, choose $h = o$; since $i + (1) = o + (1)$. For $i-ip > o$, $[i-ip] + (p) = h + (p)$ for some h $o \leq h \leq p-1$. Hence $i + (p) = h + (p)$ for $o \leq h \leq p-1$. Therefore $I/(p)$ can have at most p elements.

Suppose $a + (p)$, $b + (p)$ $I/(p)$ such that $[a + (p)] \cdot [b + (p)] = o + (p)$. Therefore $ab + (p) = o + (p)$.

Hence $ab = kp$. Since p is a prime integer if $ab = kp$, either $a = rp$ or $b = sp$. If $a = rp$, $a \in o + (p)$ and $a + (p) = o + (p)$. Likewise if $b = sp$, $b + (p) = o + (p)$. Therefore if $\left[a + (p)\right] \cdot \left[b + (p)\right] = o + (p)$, either $a + (p) = o + (p)$ or $b + (p) = o + (p)$. Hence $I/(p)$ has no divisors of zero. Since $I/(p)$ also has only a finite number of elements each non-zero element of $I/(p)$ has an inverse by theorem 1-5.

Ideals in the ring I have many desirable properties. One such property is dealt with in theorem 2-9.

Theorem 2-9. If $\{a_1, a_2, \ldots a_n\}$ is any set of integers in the ring I, there exists an element $a \in I$ such that $(a) = (a_1, a_2, \ldots a_n)$.

Proof: Let the integer a denote the greatest common divisor of the integers $a_1, a_2, \ldots a_n$. Then $(a) = (a_1, a_2, \ldots a_n)$. Since $a \in (a)$ and since by the Euclidean Algorithm, there exist integers $x_1, x_2, \ldots, x_n$ such that $a = x_1 a_1 + x_2 a_2 + \ldots + x_n a_n$. Therefore $a \in (a_1, a_2 \ldots a_n)$. Hence $(a) \subseteq (a_1, a_2, \ldots a_n)$ since (a) is a subset of any ideal containing a by theorem 2-6. Furthermore since a is the greatest common divisor of the integers $a_1, a_2, \ldots a_n$, a divides each integer. Therefore $a_1 = k_1 a$; $a_2 = k_2 a$; . . . $a_n = k_n a$. Hence $a_1, a_2, \ldots a_n$ are all elements of (a) which guarantees $(a_1, a_2, \ldots a_n) \subseteq (a)$.

<u>Definition 2-5</u>. Suppose R is a ring. Let $a \in R$ and n be a positive integer. Then $\underbrace{a*a* \ldots *a}_{n \text{ factors}}$ will be denoted a^n and $\underbrace{a \oplus a \oplus \ldots \oplus a}_{n \text{ factors}}$ will be denoted as na. If n is a negative integer, na will mean $\underbrace{-a \oplus -a \oplus \ldots \oplus -a}_{n \text{ factors}}$. If n = o, na will be o where o is the zero element of R.

<u>Definition 2-6</u>. An ideal B in a ring R is said to be a radical ideal if whenever $a^n \in B$ for some positive integer n, $a \in B$.

<u>Definition 2-7</u>. An ideal B in a ring R is said to be right primary if for $a*b \in B$ with $a \notin B$, implies $b^n \in B$ for some positive integer n. An ideal B in a ring R is said to be left primary if whenever $a*b \in B$ with $b \notin B$, implies $a^n \in B$ for some positive integer n. If B is both left and right primary B is said to be primary.

<u>Definition 2-8</u>. A non-zero element $a \in R$ is called nilpotent if there exists a positive integer n such that $a^n = o$.

The following set of theorems and examples is based on consequences of definition 2-4 through definition 2-8.

<u>Theorem 2-10</u>. Every prime ideal is a radical ideal.

Proof: Let B denote a prime ideal. Suppose $a^n \in B$. Since $a^n = a*(a* \ldots *a)$, either $a \in B$ or $a^{n-1} \in B$. If $a \in B$, the proof is complete. Suppose $a \notin B$, then $a^{n-1} \in B$. Since $a^{n-1} = a*a^{n-2}$, $a^{n-2} \in B$. This process can be continued k times until n-k = 2 at which point $a^2 \in B$. Therefore $a \in B$ and every prime ideal is a radical ideal.

<u>Theorem 2-11</u>. Every prime ideal is a primary ideal.

Proof: Suppose B is a prime ideal. Let $a*b \in B$. If $a \notin B$, then $b \in B$. Hence B is right primary. If $b \notin B$, then $a \in B$. Hence B is left primary. Therefore B is primary.

Theorem 2-10 showed that every prime ideal is a radical ideal and theorem 2-11 showed that every prime ideal is a primary ideal. The following examples will show that a primary ideal is not necessarily a prime ideal or a radical ideal, and a radical ideal need not be a prime ideal or a primary ideal.

<u>Examples 2-1</u>. Every primary ideal is not a prime ideal. Consider the ideal (4) in I. Since $2 \cdot 6 \in (4)$ with neither 2 nor 6 belonging to (4), (4) is not a prime ideal. However if $ab \in (4)$ with $a \notin (4)$ implies $b^2 \in (4)$. If $a \notin (4)$ then a is not a multiple of 4. Hence the largest power of 2 which is a factor of a is 2^1. Since $ab \in (4)$, b must be even. Hence b = 2k. Therefore $b^2 \in (4)$ and (4) is primary.

<u>Example 2-2</u>. Every primary ideal is not a radical ideal since $4 \in (4)$ and $4 = 2^2$, but $2 \notin (4)$.

<u>Example 2-3</u>. Every radical ideal is not a prime ideal. Consider the ideal (6) in I. Let $a^p \in (6)$. Then $a^p = 6k$ by theorem 2-7. Suppose a is not a multiple of 6. Then both

2 and 3 are not factors of a and hence are not factors of a^p. This is a contradiction since $a^p = 6k$. Therefore (6) is a radical ideal. Since $4 \cdot 3 \in (6)$ with neither 4 nor 3 belonging to (6), (6) is not a prime ideal.

Example 2-4. Every radical ideal is not primary since (6) is a radical ideal which is not primary. This can be shown by noting that $2 \cdot 3 \in (6)$ with $2 \notin (6)$ and $3^k \notin (6)$ for any positive integer k.

Theorem 2-12. If B is a radical ideal in R, then R/B has no nilpotent elements.

Proof: Suppose R/B contains a nilpotent element $a \oplus B$. Then there exists a positive integer n such that $(a \oplus B)^n = o \oplus B$. Hence $a^n \oplus B = o \oplus B$. Therefore $a^n \in o \oplus B$. Therefore $a^n \in B$. Since B is a radical ideal $a \in B$. Hence $a \oplus B = o \oplus B$ by theorem 2-2. This contradicts the fact that $a \oplus B$ is nilpotent. Hence R/B has no nilpotent elements.

Theorem 2-13. Suppose B is a primary ideal in a ring R. Then every divisor of zero in R/B is nilpotent.

Proof: Let $a \oplus B$ be a divisor of zero in R/B. Therefore there exists an element $c \oplus B \neq o \oplus B$ such that either $(c \oplus B)*(a \oplus B) = o \oplus B$ or $(a \oplus B)*(c \oplus B) = o \oplus B$. If $(c \oplus B)*(a \oplus B) = o \oplus B$, $c*a \in B$. Since $c \notin B$, $a^n \in B$ for some positive integer n. Therefore $(a \oplus B)^n = o \oplus B$. Similarly if $(a \oplus B)*(c \oplus B) = o \oplus B$ it can be shown that there exists a positive integer n such that $(a \oplus B)^n = o \oplus B$.

Theorem 2-14. The intersection of every set of prime ideals is a radical ideal.

Proof: Suppose B_α, $\alpha \in \Lambda$, is a set of prime ideals. Then $\cap B_\alpha$ is an ideal by theorem 2-1. Suppose $a^n \in \cap B_\alpha$. Then a^n is an element of each B_α. Since each B_α is prime, a is an element of each B_α by theorem 2-10. Therefore $a \in \cap B_\alpha$ and $\cap B_\alpha$ is a radical ideal.

The following lemmas concerning ideals will be of use in Chapter III.

Lemma 2-1. If A and B are ideals in a ring R, $A*B \equiv \{x \mid x$ is a finite sum of the form $a_1^*b_1 \oplus \ldots \oplus a_n*b_n$ where $a_i \in A$ and $b_i \in B\}$ is also an ideal in R.

Proof: If $x,y \in A*B$, $x \oplus -y$ will obviously be a finite sum of the desired form. Let $x \in A*B$. Then $r*x$ and $x*r$ are also elements of $A*B$ since A and B are ideals. Hence $A*B$ is an ideal.

Lemma 2-2. The set $B^r \equiv B*B* \ldots *B$, r factors, is an ideal in R if B is an ideal in R.

Proof by induction: If $r = 1$, $B^1 = B$ is an ideal. Suppose for $r = k$, B^k is an ideal. Hence B^k*B is an ideal by lemma 2-1. Therefore B^{k+1} is an ideal and the proof is complete.

Lemma 2-3. If B is a prime ideal and C and D are ideals such that $C * D = B$, then either $C = B$ or $D = B$.

Proof: Suppose $x \in B$; then $x = c_1 * d_1 \oplus \ldots \oplus c_n * d_n$ since $C * D = B$. Therefore $x \in C$ and $x \in D$. Hence $B \subset C$ and $B \subset D$. Suppose that $B \neq C$; then there is $t \in C$ such that $t \notin B$. Let Y denote any element of D. Since $C * D = B$, $t * Y \in B$. But B is a prime ideal. Therefore $Y \in B$. Hence $B = D$. In a similar fashion it can be shown that if $B \neq D$, then $B = C$.

Lemma 2-4. If A and B are ideals in a commutative ring R, then $\overline{AB} \equiv \{x \in R \mid b * x \in A \text{ for all } b \in B\}$ is an ideal of R.

Proof: Note that $\overline{AB}$ is non-empty since $o \in \overline{AB}$. Let $x, y \in \overline{AB}$. Then $b * x \in A$ and $b * y \in A$ for any $b \in B$. Since A is an ideal, $b * x \oplus -b * y \in A$.

$$\begin{aligned} b * x \oplus -b * y &= b * x \oplus b * (-y) \\ &= b * (x \oplus -y). \end{aligned}$$

Therefore $x \oplus -y \in \overline{AB}$. Let $x \in \overline{AB}$ and let $r \in R$. Since $x * b \in A$ for all $b \in B$ and since R is commutative, $b * (r * x)$ and $(r * x) * b \in A$ for all $b \in R$. Therefore $\overline{AB}$ is an ideal.

CHAPTER III

NOETHERIAN RINGS

Before proceeding with Noetherian rings, a few properties concerning radicals of ideals will be investigated.

<u>Definition 3-1</u>. If B is an ideal in a ring R, the set $H \equiv \{ x \in R \mid x^n \in B \text{ for some positive integer } n \}$ is called the radical of B.

<u>Lemma 3-1</u>. If B is a radical ideal, B = H.

Proof: Obviously $B \subseteq H$. Suppose $x \in H$. Then there exists a positive integer n such that $x^n \in B$. Since B is a radical ideal, $x \in B$. Hence $H \subseteq B$.

<u>Lemma 3-2</u>. If B_1 and B_2 are ideals, then radical $(B_1 \cap B_2)$ = radical $B_1 \cap$ radical B_2.

Proof: Suppose $x \in$ radical $(B_1 \cap B_2)$; then there exists a positive integer n such that $x^n \in (B_1 \cap B_2)$. Hence $x^n \in B_1$ and $x^n \in B_2$. Therefore $x \in$ radical B_1 and $x \in$ radical B_2. Hence $x \in$(radical $B_1 \cap$ radical B_2). Therefore radical $(B_1 \cap B_2) \subseteq$ radical $B_1 \cap$ radical B_2.

Suppose $x \in$ radical $B_1 \cap$ radical B_2. Then there exist positive integers n and k such that $x^n \in B_1$ and $x^k \in B_2$. Let h denote the larger of n and k. Therefore $x^h \in B_1$

and $x^h \in B_2$. Hence $x^h \in B_1 \cap B_2$. Therefore $x \in$ radical $(B_1 \cap B_2)$. It follows that radical $(B_1 \cap B_2) =$ radical $B_1 \cap$ radical B_2.

Lemma 3-3. If B is an ideal, radical (radical B) = radical B.

Proof: Suppose $x \in$ radical (radical B). Then there exists a positive integer n such that $x^n \in$ radical B. If $x^n \in$ radical B, there exists a positive integer r such that $(x^n)^r \in B$. It can be easily verified that $(x^n)^r = x^{nr}$. Obviously radical B $\subseteq$ radical (radical B). Hence the proof is complete.

Theorem 3-1. If B is an ideal in a commutative Ring R, then the radical of B is also an ideal in R.

Proof: Suppose $a, b \in$ radical B. Hence for some positive integers m and n, $a^m \in B$ and $b^n \in B$. Without loss of generality suppose $m \geq n$; then a^{2m} and $b^{2m} \in B$. Consider the product $(a \oplus -b)^{2m}$. Since R is a commutative ring, it is easily verified that the binomial expansion holds for $(a \oplus -b)^{2m}$. In the r^{th} term of $(a \oplus -b)^{2m}$, a is raised to the $2m - r+1$ power and $-b$ is raised to the $r-1$ power. If $r = m$, a is raised to the $m + 1$ power and $ha^{m+1} * (-b)^{m-1} \in B$ where h is a positive integer. If $r > m$, then $r-1 \geq m$. Hence $h_1 a^{2m-r+1} * (-b)^{r-1} \in B$. If $r < m$, $m < 2m-r + 1$. Hence

$h_2a^{2m-r+1}*(-b)^{r-1} \in B$. Therefore every term in the expansion of $(a \oplus -b)^{2m}$ is an element of B and hence $(a \oplus -b)^{2m} \in B$. Therefore $a \oplus -b \in$ radical B. Let $x \in$ radical B. There exists a positive integer n such that $x^n \in B$. Suppose $a \in R$; then $a^n \in R$. Since B is an ideal $a^n*x^n \in B$. But since R is commutative, $a^n*x^n = (a*x)^n = (x*a)^n$. Therefore radical B is an ideal in R.

An immediate consequence of theorem 3-1 is corollary 3-1.

Corollary 3-1. If B is a primary ideal in a commutative ring R, then radical B is a prime ideal in R.

Proof: By theorem 3-1 radical B is an ideal in R. Suppose $a*b \in$ radical B; then there exists a positive integer n such that $(a*b)^n \in B$. Since R is commutative, $(a*b)^n = a^n*b^n$. Suppose $a^n \notin B$. Since B is primary, there exists a positive integer k such that $(b^n)^k \in B$. Since $(b^n)^k = b^{nk}$, $b \in$ radical B. Similarly if $b^n \notin B$, $a \in$ radical B. Hence whenever $a*b \in$ radical B, either $a \in$ radical B or $b \in$ radical B.

Definition 3-2. A ring R is said to satisfy the ascending chain condition for ideals if every sequence of ideals $B_1, B_2, \ldots$ in R such that $B_1 \subset B_2 \subset \ldots$ has only a finite number of terms.

Definition 3-3. A commutative ring which satisfies definition 3-2 is said to be a Noetherian ring.

There are other statements which could also serve as the definition of a Noetherian ring. Theorem 3-2 will give two alternate definitions. The following lemma will aid in the proof of theorem 3-2.

Lemma 3-4. If $B_1 \subset B_2 \subset \ldots$ is an infinite ascending chain of ideals in a ring R, then the union of all the ideals in the chain is an ideal.

Proof: Suppose $a, b \in \cup B_\alpha$; then a belongs to some B_k and b belongs to some B_h. Either $B_k \subset B_h$ or $B_h \subset B_k$. Hence both $a, b \in B_k$ or $a, b \in B_h$. Therefore $a \oplus -b \in B_k$ or $a \oplus -b \in B_h$. Hence $a \oplus -b \in \cup B_\alpha$. If $x \in \cup B_\alpha$, then x is an element of some B_k. Since B_k is an ideal, $r * x$ and $x * r \in B_k$. Therefore $r * x$ and $x * r$ are elements of $\cup B_\alpha$.

Theorem 3-2. In any commutative ring R the following conditions are equivalent.

(1) R satisfies the ascending chain condition.

(2) Every ideal in R is generated by a finite number of elements.

(3) Every non-empty set of ideals in R contains at least one ideal which is not contained in any other ideal of the set (3, p. 20).

Proof: Suppose R satisfies the ascending chain condition. Let B denote an ideal of R and let $b_1 \in B$. Then $(b_1) \subseteq B$ since if $x \in (b_1)$ x is an element of every ideal containing b_1. If $(b_1) = B$, the proof is complete. Suppose $(b_1) \subset B$. Now choose $b_2 \in B$ such that $b_2 \notin (b_1)$. Obviously $(b_1) \subset (b_1, b_2) \subseteq B$. If $(b_1, b_2) = B$, the proof is complete. If not $(b_1, b_2) \subset B$ and again choose an element $b_3 \in B$ such that $b_3 \notin (b_1, b_2)$. Now we have $(b_1) \subset (b_1, b_2) \subset (b_1, b_2, b_3) \subseteq B$. This process can only be done a finite number of times. Otherwise there would exist an infinite ascending chain in R. Therefore for some positive integer k, $(b_1, b_2, \ldots b_k) = B$.

Suppose now every ideal in R is generated by a finite number of elements. Furthermore suppose there exists a set K of ideals in R such that for every $B_\alpha \in K$, B_α is contained in some other ideal in K. Without loss of generality the ideals in K can be arranged in a sequence such that $B_1 \subset B_2 \subset \ldots \subset B_\delta \subset \ldots$. By lemma 3-4 $\cup B_\alpha$ is also an ideal in R and hence is generated by a finite number of elements. Therefore, $\cup B_\alpha = (b_1, b_2, \ldots b_r)$. Now each one of the generators for $\cup B_\alpha$ is an element of some B_α in the chain. Observe now that there is an ideal B_h in the chain such that $b_1, b_2, \ldots b_r \in B_h$.

The contention is that $B_h = \cup B_\alpha$. Obviously, $B_h \subseteq \cup B_\alpha$. Since $\cup B_\alpha = (b_1, b_2, \ldots b_r)$ with each $b_i \in B_h$, $\cup B_\alpha \subseteq B_h$. Hence $\cup B_\alpha = B_h$. Obviously B_h is not contained in any other member of the set K. Therefore every non-empty set of ideals in R contains at least one ideal which is not contained in any other ideal of the set.

Finally suppose every non-empty set of ideals in R contains an ideal which is not contained in any other member of the set. Let $B_1, B_2, \ldots, B_k$ .. be a sequence of ideals in R such that $B_1 \subset B_2 \subset \ldots \subset B_k \subset \ldots$. Consider the set of all ideals in this sequence. There exists an ideal B_m such that $B_m \not\subset B_t$ for any B_t in the set. Since these ideals form a chain, $B_t \subseteq B_m$ for every element in the set. Therefore since this is a sequence of ideals the chain is of finite length.

The next set of lemmas is suggested by the fact that every ideal in a Noetherian ring is generated by a finite number of elements.

<u>Lemma 3-5</u>. If $(x_1, x_2, \ldots x_n)$ is an ideal in a commutative ring R, then $(x_1, x_2, \ldots x_n) = G$ where $G = \left\{ X \,\middle|\, X = \sum_1^n \left[n_i x_i \oplus a_i * x_i \right] \text{ where } n_i \in I \text{ and } a_i \in R \right\}$.

Proof: Suppose $x, y \in G$; then $x = \sum_1^n \left[n_i x_i \oplus a_i * x_i \right]$ and $-y = -\sum_1^n \left[m_i x_i \oplus b_i * x_i \right]$.

$$x \oplus -y = \sum_1^n \left[n_i x_i \oplus a_i * x_i\right] \oplus - \sum_1^n \left[m_i x_i \oplus b_i * x_i\right]$$

$$= \sum_1^n \left\{ \left[n_i - m_i\right] x_i \oplus \left[a_i \oplus -b_i\right] * x_i \right\} .$$

Therefore $x \oplus -y \in G$. Suppose $x \in G$ and $r \in R$.

$$r * x = x * r = r * \sum_1^n \left[n_i x_i \oplus a_i * x_i\right]$$

$$= \sum_1^n \left\{ r * \left[n_i x_i\right] \oplus r * a_i * x_i \right\}$$

$$= \sum_1^n \left\{ \left[n_i r\right] * x_i \oplus r * a_i * x_i \right\}$$

$$= \sum_1^n \left[n_i r \oplus r * a_i\right] * x_i$$

$$= \sum_1^n \left[o_i x_i \oplus c_i * x_i\right] .$$

The o_i is the real number zero and $c_i = n_i r \oplus r * a_i$. Therefore G is an ideal. Since G contains $x_1, x_2, \ldots x_n$, $(x_1, x_2, \ldots x_n) \subseteq G$. Let b denote an element of G. Then $b = \sum_1^n \left[n_i x_i \oplus a_i * x_i\right]$. Hence $b \in (x_1, x_2, \ldots x_n)$ because $(x_1, x_2, \ldots x_n)$ is an ideal. Therefore $(x_1, x_2, \ldots x_n) = G$.

<u>Lemma 3-6</u>. If B is an ideal in a commutative ring R, the ideal B^r is the set P of all finite sums of products with r factors. In set notation $P = \left\{ x \in R \,\middle|\, X = \sum_{i=1}^n a_{i1} * a_{i2} * \ldots * a_{ir} \right.$ where $n \in I$ and $\left. a_{ij} \in B \right\}$.

Proof by induction: For $r = 1$ the result is trivial. For $r = 2$, the lemma is true by lemma 2-2. Suppose lemma is true for $r = k$. Then if $y \in B^k$, $y = \sum_1^n a_{i1} * a_{i2} * \ldots * a_{ik}$ where $a_{ij} \in B$. Now $B^k * B = \left\{ x / x \text{ is a finite sum of the form } y_1 * b_1 \oplus y_2 * b_2 \oplus \ldots y_n * b_n \text{ where } y_j \in B^k \text{ and } b_j \in B \right\}$. Each y_j is expressible as a finite sum of terms with each term consisting of a product of k elements of B. Also each y_j is "multiplied" by b_j B. Upon application of the distributive law each term in the sum is a product of $k + 1$ elements of B. This is also a finite sum since each $y_j * b_j$ is a finite sum and there are only a finite number of these sums. Therefore $B^k * B \subseteq \left\{ x \mid x = \sum_1^n a_{i1} * a_{i2} * \ldots * a_{i\,k+1} \text{ where } n \in I \text{ and } a_{ij} \in B \right\}$. But if $y \in \left\{ x \mid x = \sum_1^n a_{i1} * a_{i2} * \ldots * a_{ik+1} \right\}$, $y = \sum_1^n \left[a_{i1} * a_{i2} * \ldots \right] * a_{ik+1}$. Therefore

$$\left\{ x \mid x = \sum_1^n a_{i1} * \ldots * a_{ik+1} \text{ where } n \in I \text{ and } a_{ij} \in B \right\} \subseteq B^k * B.$$

Hence lemma 3-6 is true.

<u>Lemma 3-7</u>. If R is a commutative ring,

$$(x_1, x_2, \ldots x_n)^r = (\ldots, \underbrace{x_i * x_j * \ldots * x_r}_{r \text{ factors}}, \ldots).$$

Proof: Suppose $a \in (x_1, x_2, \ldots x_n)^r$, then by lemma 3-6 a is expressible as a finite sum of products $a_1 * \ldots * a_r$ with r factors each a_i being an element of $(x_1, x_2, \ldots x_n)$.

$$a_1 = \sum_1^n \left[n_i x_i \oplus d_i * x_i\right]$$

$$a_2 = \sum_1^n \left[m_i x_i \oplus b_i * x_i\right]$$

$$\vdots$$

$$a_r = \sum_1^n \left[P_i x_i \oplus h_i * x_i\right].$$

Hence $a_1 * a_2 * \ldots * a_r = \left[\sum_1^n [h_i x_i \oplus d_i * x_i]\right] * \left[\sum_1^n [m_i x_i \oplus b_i * x_i]\right] * \ldots * \left[\sum_1^n [P_i x_i \oplus h_i * x_i]\right]$. Each term in this product consists of r factors of the form $x_j * x_k * \ldots * x_n$. Since a is a finite sum of factors of this type, a can be written in the form $a = \sum_1^k \left[m_j y_j \oplus \ell_j * y_j\right]$ where $m_j \in I$, $\ell_j \in R$ and y_j is a product of the form $\underbrace{x_i * x_j * \ldots * x_r}_{r \text{ factors}}$. Therefore $a \in (\ldots, x_i * x_j \ldots * x_r, \ldots)$. Obviously any product of the form $\underbrace{x_i * x_j * \ldots * x_r}_{r \text{ factors}}$ will belong to $(x_1, x_2, \ldots x_n)^r$ by lemma 3-6.

The preceding three lemmas have laid the groundwork for theorem 3-3.

<u>Theorem 3-3</u>. If B is an ideal in a Noetherian ring, there exists a positive integer m such that $\left[\text{radical } B\right]^m \subseteq B$ (3, p. 22).

Proof: Since radical B is an ideal in R by theorem 3-1, it is generated by a finite number of elements due to theorem 3-2. Therefore radical B = $(x_1, x_2, \ldots x_n)$. For each x_i, there exists a positive integer m_i such that $x_i^{mi} \in B$. Let $m = m_1 + m_2 + \ldots + m_n$. By lemma 3-7, $(x_1, x_2, \ldots x_n)^m = (\ldots, \underbrace{x_i * x_j * \ldots * x_k}_{m \text{ factors}}, \ldots)$. Since there are only n distinct x_i's and since R is commutative, each $\underbrace{x_i * x_j * \ldots * x_k}_{m \text{ factors}} = \underbrace{x_p^{np} * x_q^{nq} * \ldots * x_k^{nk}}_{r \text{ factors}}$ where $r \leq n$. Observe $n_p + n_p + \ldots + n_k = m_1 + m_2 + \ldots + m_n$. For each x_h in the product of r factors, there corresponds an n_h. Each x_h in the product of r factors is also contained in the product of m factors. Observe for each x_h there is an m_h such that $x_h^{mh} \in B$. Consider the sum $n_p + n_q + \ldots + n_k$ and the sum $m_p + m_q + \ldots + m_k$. It is easily seen that $n_p + n_p + \ldots + n_k \geq m_p + m_q + \ldots + m_k$. Hence there is $n_s \geq m_s$ for some n_s and m_s since if every $n_t < m_t$, then $n_p + n_q + \ldots n_k < m_p + m_q + \ldots m_k$. But this statement cannot be true since $n_p + n_q + \ldots n_k \geq m_p + m_q + \ldots m_k$. Therefore there is an $n_s \geq m_s$. Hence contained in each product $x_i * x_j * \ldots * x_k$ there is an $x_s^{ns} \in B$. This fact guarantees that every element in the set of generators for $[\text{radical } B]^m$ belongs to B. Hence $[\text{radical } B]^m \subseteq B$.

A similar type of proof can be applied to theorem 3-4.

Theorem 3-4. If B_1 and B_2 are ideals in a Noetherian ring R, there exists a positive integer r such that $B_1^r \subseteq B_2$ if and only if radical $B_1 \subseteq$ radical B_2.

Proof: Suppose there is an r such that $B_1^r \subseteq B_2$. Since R is Noetherian, $B = (x_1, x_2, \ldots x_n)$. Therefore $(x_1, x_2, \ldots, x_n)^r \subseteq B_2$. By lemma 3-7 $(\ldots, x_i{*}x_j{*}\ldots{*}x_n) \subseteq B_2$. Therefore for $p = 1, \ldots, n$, $x_p^r \in B_2$. This implies that the set of generators for B_1 is contained in radical B_2. Therefore $B_1 \subseteq$ radical B_2. Since $B_1 \cap$ radical $B_2 = B_1$, by lemma 3-2 and lemma 3-3 radical B_1 = radical $B_1 \cap$ radical B_2. Therefore radical $B_1 \subseteq$ radical B_2. Now suppose radical $B_1 \subseteq$ radical B_2. Since $B_1 \subseteq$ radical B_1, $B_1 \subseteq$ radical B_2. Since R is Noetherian, $B_1 = (x_1, x_2, \ldots x_n)$. For each x_i in the set of generators for B_1 there exists an $r_i \in I$ such that $x_i^{ri} \in B_2$. Let $r = r_1 + r_2 + \ldots + r_n$. The remainder of the proof is identical with that of theorem 3-3. Therefore $B_1^r \subseteq B_2$.

Lemma 3-8. Suppose B is an ideal in R. Let ϕ denote the mapping of R onto R/B defined by $\phi(x) = x \oplus B$ for $x \in R$. If C_i is an ideal in R/B, then $D_i \equiv \{ x \in R \mid \phi(x) \in C_i \}$ is an ideal in R.

Proof: Observe first that ϕ is a homorphism of R onto R/B. Suppose $x, y \in D_i$, then $\phi(x)$, $\phi(y) \in C_i$. But C_i is an ideal. Therefore $\phi(x) \oplus -\phi(y) \in C_i$. Since $\phi(x) \oplus -\phi(y) = \phi(x \oplus -y)$, $x \oplus -y \in D_i$. Suppose $x \in D_i$. Let $r \in R$. Since $\phi(r*x) = \phi(r)*\phi(x)$ and $\phi(x*r) = \phi(x)*\phi(r)$, $r*x$ and $x*r \in D_i$ because C_i is an ideal. Therefore D_i is an ideal.

Lemma 3-9. If C_1 and C_2 are ideals in R/B such that $C_1 \subset C_2$, then $D_1 \subset D_2$.

Proof: Suppose $x \in D_1$; then $\phi(x) \in C_1$. Hence $\phi(x) \in C_2$, so $x \in D_2$. Since $C_1 \subset C_2$, there exists a $y \oplus B \in C_2$ such that $y \oplus B \notin C_1$. Therefore $y \in D_2$ but $y \notin D_1$.

Theorem 3-5 follows from lemma 3-8 and lemma 3-9.

Theorem 3-5. If B is an ideal in a Noetherian ring R, R/B is a Noetherian ring (2, p. 198).

Proof: Suppose R/B is not Noetherian. Then there exists an infinite sequence of ideals in R/B such that $C_1 \subset C_2 \subset . . . .$ according to lemma 3-8 and lemma 3-9 the sequence of ideals D_1, D_2, ... D_n in R is also infinite. But this statement contradicts the fact that R is a Noetherian ring. Therefore R/B is Noetherian.

The remainder of this chapter will be devoted to the decomposition of an ideal in a Noetherian ring.

Definition 3-4. Suppose B is an ideal in a ring R such that $B = B_1 \cap B_2 \cap \ldots \cap B_n$ where each B_i is a primary ideal in R. This intersection will be called a primary decomposition of B.

Definition 3-5. An ideal B is said to be irreducible if whenever $B = B_1 \cap B_2$, either $B = B_1$ or $B = B_2$.

Definition 3-6. A finite intersection of ideals is said to be irredundant if no ideal in the intersection contains the intersection of the remaining ideals.

A fundamental property of Noetherian rings is stated in theorem 3-6.

Theorem 3-6. In a Noetherian ring every ideal can be represented as the intersection of a finite number of irreducible ideals (1, p. 175).

Proof: If B is an ideal in R, either B is irreducible or B is not irreducible. If B is irreducible, B can be expressed in the form $B = B_1 \cap B_2$ where $B = B_1 = B_2$. Obviously $B_1 \cap B_2$ is a finite intersection of irreducible ideals. If B is not irreducible, then there must exist ideals B_1 and B_2 such that $B = B_1 \cap B_2$ with $B \neq B_1$ and $B \neq B_2$. Therefore $B \subset B_1$ and $B \subset B_2$. If both B_1 and B_2 are irreducible, the theorem is proved. Suppose that exactly one of B_1 and B_2 is not irreducible. Without loss of generality assume it is B_2. Then there exist ideals B_4 and B_6 such that $B_2 = B_4 \cap B_6$ with $B_2 \subset B_4$ and $B_2 \subset B_6$. Therefore $B = B_1 \cap B_4 \cap B_6$ with $B \subset B_2 \subset B_6$. Again if B_4 and B_6 are both irreducible the theorem is proved. So suppose B_4 is irreducible and B_6 is not irreducible. Hence $B_6 = B_8 \cap B_{10}$ with $B_6 \subset B_8$ and $B_6 \subset B_{10}$. Now $B = B_1 \cap B_4 \cap B_8 \cap B_{10}$ with $B \subset B_2 \subset B_6 \subset B_{10}$. Once again if B_8 and B_{10} are irreducible the theorem is proved. If not, the same procedure is repeated. This procedure can only be done a finite number of times since the chain $B \subset B_2 \subset B_6 \subset B_{10} \subset \ldots$ can have only finite length. Hence there can be only a finite number of ideals in the intersection and all of these ideals are irreducible.

Theorem 3-7. If R is Noetherian, every irreducible ideal in R is a primary ideal (1, p. 176).

Proof: Suppose there is an irreducible ideal B in R which is not a primary ideal. Since B is not primary, there exist elements $a, b \in R$ such that $a*b \in B$ with $a \notin B$ and $b^n \notin B$ for any positive integer n. Consider the set of ideals $A_i \equiv \left\{ x \in R \mid x*b^i \in B \right\}$. It is easily verified that each A_i is an ideal. Observe also that $A_i \subseteq A_{i+1}$. Therefore the A_i's form a chain in R. Since R is Noetherian, this chain can have only finite length. Therefore there exists a positive integer n such that $A_n = A_{n+1}$. Consider the set $K \equiv \left[B \oplus (a)\right] \cap \left[(B \oplus R*b^n\right]$. It can be easily verified that $B \oplus (a)$, $R*b^n$ and $B \oplus R*b^n$ are ideals in R. If $x \in K$, then $x \in B \oplus (a)$. Hence $x = h \oplus ka \oplus k'*a$ where $h \in B$, $k \in I$ and $k' \in R$. Observe that $x*b = h*b \oplus k(a*b) \oplus k'*a*b$. Since $h*b$, $k(a*b)$, and $k'*a*b \in B$, $x*b \in B$. Since $x \in B \oplus R*b^n$, $x = p \oplus q$ where $p \in B$ and $q \in R*b^n$. If $q \in R*b^n$, then $q = r*b^n$. Hence $x = p \oplus r*b^n$. Therefore $x*b = p*b \oplus r*b^{n+1}$. Since $x*b$ and $-p*b \in B$, $r*b^{n+1} \in B$. Furthermore since $r*b^{n+1} \in B$, $r \in A_{n+1}$. But $A_n = A_{n+1}$. Therefore $r \in A_n$. Hence $r*b^n \in B$. Since $x = p \oplus r*b^n$ with p, $r*b^n \in B$, $x \in B$. Therefore $K \subseteq B$. Obviously $B \subseteq K$. Hence $K = B$. Since $a \notin B$, $B \oplus (a) \nsubseteq B$. Also $B \oplus R*b^n \nsubseteq B$ since $b^{n+1} \notin B$. Therefore $B \subset B \oplus (a)$ and $B \subset B \oplus R*b^n$. This result contradicts the fact that B is irreducible. Hence every irreducible ideal in a Noetherian ring is primary.

Before stating and proving the fundamental decomposition theorem one more lemma is needed.

<u>Lemma 3-10</u>. If B_1 and B_2 are primary ideals with radical B_1 = radical B_2, $B_1 \cap B_2$ is a primary ideal.

Proof: Suppose $a*b \in B_1 \cap B_2$ with $a \notin B_1 \cap B_2$. Hence $a \notin B_1$ or $a \notin B_2$. Without loss of generality suppose $a \notin B_1$. Since $a*b \in B_1 \cap B_2$, $a*b \in B_1$. Hence $b^k \in B_1$ for some positive integer k. Therefore $b \in$ radical B_1. Since radical B_1 = radical B_2, $b \in$ radical B_2.

Hence there exists a positive integer n such that $b^n \in B_2$. Let ℓ denote the larger of k and n. Then $b^\ell \in B_1$ and $b^\ell \in B_2$. Hence $b^\ell \in B_1 \cap B_2$. Therefore $B_1 \cap B_2$ is right primary. Similarly it can be shown that $B_1 \cap B_2$ is left primary.

Theorem 3-8 is the fundamental decomposition theorem for Noetherian rings.

<u>Theorem 3-8</u>. Each ideal in a Noetherian ring R is an irredundent intersection of primary ideals with distinct radicals.

Proof: By theorem 3-6 if B is an ideal in R, B is the intersection of a finite number of irreducible ideals. Each of these irreducible ideals is primary by theorem 3-7. Let $B = B_1 \cap B_2 \cap \ldots \cap B_n$ denote this intersection. Either this intersection is irredundant or it is not irredundant. If it is not irredundant, there exists a B_i such that $B_1 \cap B_2 \cap \ldots \cap B_{i-1} \cap B_{i+1} \ldots \cap B_n \subseteq B_i$. Therefore $B_1 \cap B_2 \cap \ldots \cap B_{i-1} \cap B_{i+1} \cap \ldots \cap B_n = B_1 \cap B_2 \cap \ldots \cap B_n$. Hence $B = B_1 \cap B_2 \cap \ldots \cap B_{i-1} \cap B_{i+1} \cap \ldots \cap B_n$. Clearly this process can be repeated until an irredundant expression is found. Let $B = B_1 \cap B_2 \cap \ldots \cap B_j$ denote the irredundant intersection. If all the $B_{j's}$ have distinct radicals, the proof is complete. Suppose there is a B_k and a B_p with the same radical. By lemma 3-10 $B_k \cap B_p$ is a primary ideal. Clearly this process can also be repeated until there is a representation $B = \cap B_h$ with each B_h having a distinct radical.

This intersection need not be unique as the following example will show.

Example 3-1. Let F denote the set of rational numbers. Consider the polynomial ring F $[x,y]$. It can be verified that F $[x,y]$ is a Noetherian ring. The ideal (x^4, x^2y) in F $[x,y]$ has more than one representation as the intersection of a finite number of primary ideals with distinct radicals.

For example $(x^4, x^2y) = (x^2) \cap (x^4, y)$ and $(x^4, x^2y) = (x^2) \cap (x^4, x^2y, y^2)$. Let f, g, and h denote elements of F $[x,y]$.

First of all (x^2) is primary. Let $f*g \in (x^2)$ with $f \notin (x^2)$. Therefore there is a term in f which has degree less than two in x. Hence each term in g must be of at least degree one in x. Therefore $g^2 \in (x^2)$ and (x^2) is primary.

The ideal (x^4, y) is also primary. Suppose $f*g \in (x^4,y)$ with $f \notin (x^4,y)$. Hence f has a term which does not contain either x^4 or y. This particular term has a degree of less than four in x and of less than one in y. Hence every term in g must be of at least the first degree in x or of the first degree in y since $f*g \in (x^4,y)$. Therefore $g^4 \in (x^4,y)$ and (x^4,y) is primary.

Finally the ideal (x^4, x^2y, y^2) is primary. Suppose $f*g \in (x^4, x^2y, y^2)$ with $f \notin (x^4, x^2y, y^2)$. Then f contains a term which is less than the fourth degree in x, less than the second degree in y, and which is not of the form h_2x^2y.

Therefore every term of g is either of the first degree in x or of the first degree in y. Therefore $g^4 \in (x^4, x^2y, y^2)$; hence (x^4, x^2y, y^2) is primary.

Suppose $f \in (x^4, x^2y)$.

$$\begin{aligned} f &= f_1x^4 + f_2x^2y \\ &= \left[f_1x^2 + f_2y\right] x^2 \\ &= f_1x^4 + \left[f_2x^2\right] y. \end{aligned}$$

Therefore $f \in (x^2)$ and $f \in (x^4, y)$. Hence $(x^4, x^2y) \subseteq (x^2) \cap (x^4, y)$. Suppose $f \in (x^2) \cap (x^4, y)$; then $f = f_1x^2$ and $f = g_1x^4 + g_2y$. Hence $g_2 = gx^2$. Therefore $f = g_1x^4 + gx^2y$ and $(x^4, x^2y) = (x^2) \cap (x^4, y)$. Since radical $(x^2) = (x)$ and radical $(x^4, y) = (x, y)$ with $(x^2) \not\subseteq (x^4, y)$ and $(x^4, y) \not\subseteq (x^2)$, this decomposition satisfies theorem 3-8.

Again suppose $f \in (x^4, x^2y)$.

$$\begin{aligned} f &= f_1x^4 + f_2x^2y \\ &= \left[f_1x^2 + f_2y\right] x^2 \\ &= f_1x^4 + f_2x^2y + oy^2 \end{aligned}$$

Therefore $(x^4, x^2y) \subseteq (x^2) \cap (x^4, x^2y, y^2)$. Suppose $f \in (x^2) \cap (x^4, x^2y, y^2)$; then $f = h_1x^2$ and $f = g_1x^4 + g_2x^2y + g_3y^2$. Since $f = h_1x^2$, $g_3 = gx^2$. Hence

$$\begin{aligned} f &= g_1x^4 + g_2x^2y + gx^2y \\ &= g_1x^4 + \left[g_2 + gy\right] x^2y. \end{aligned}$$

Therefore $(x^4, x^2y) = (x^2) \cap (x^4, x^2y, y^2)$. Note once again that radical $(x^2) = (x)$ while radical $(x^4, x^2y, y^2) = (x, y)$.

Note also that $(x^2) \nsubseteq (x^4, x^2y, y^2)$ and $(x^4, x^2y, y^2) \nsubseteq (x^2)$. Therefore this decomposition also satisfies theorem 3-8. Finally note that $(x^4, y) \neq (x^4, x^2y, y^2)$ because $y \in (x^4, y)$ but $y \notin (x^4, x^2y, y^2)$. Hence these two decompositions are different.

The concluding two theorems in this thesis are consequences of theorem 3-8.

Theorem 3-9. The radical of an ideal in a Noetherian ring R is the intersection of the radicals of the primary ideals in theorem 3-8.

Proof: Let $B = \bigcap B_i$ of theorem 3-8.

$$\text{radical } B = \text{radical } \left[\bigcap B_i\right] = \bigcap \left[\text{radical } B_i\right].$$

The radicals of the primary ideals in theorem 3-8 are known as the associated prime ideals of B.

The final six lemmas prepare the way for theorem 3-10.

Lemma 3-11. If B is a primary ideal such that $a*b \in B$ with $b \notin$ radical B, $a \in B$.

Proof: Suppose $a \notin B$; then since B is primary $b \in$ radical B. But $b \notin$ radical B. Hence $a \in B$.

Lemma 3-12. If $\bigcap B_i$ and C are ideals, $\overline{\left[\bigcap B_i\right] C} = \bigcap \overline{\left[B_i \; C\right]}$.

Proof: Suppose $x \in \cap \overline{[B_i\ C]}$; then x is an element of each $\overline{[B_i\ C]}$. Therefore $x*c$ is an element of each B_i for $c \in C$. Hence $x \in \overline{[\cap B_i]\ C}$. Suppose now $x \in \overline{[\cap B_i]C}$; then for $c \in C$, $x*c \in \cap B_i$. Hence $x*c$ is an element of each B_i for any $c \in C$. Therefore x is in each $\overline{[B_i\ C]}$ and hence $x \in \cap\overline{[B_i\ C]}$.

Lemma 3-13. If B is a primary ideal, and C is an ideal which is not contained in radical B, $\overline{BC} = B$.

Proof: Obviously $B \subseteq \overline{BC}$. So suppose $x \in \overline{BC}$. There exists a $c \in C$ such that $c \notin$ radical B. But $x*c \in B$ for every $c \in C$ since $x \in \overline{BC}$. Hence by lemma 3-11 $x \in B$.

Lemma 3-13. If B and C are ideals in a Noetherian ring R such that $B \subseteq C$, then for any positive integer n $B^n \subseteq C^n$.

Proof: Since R is Noetherian $B = (x_1, x_2, \ldots x_p)$ and $C = (y_1, y_2, \ldots y_k)$. By lemma 3-7

$$B^n = (\ldots, \underbrace{x_i * x_j \ \ldots * x_\ell}_{n \text{ factors}}, \ldots) \text{ and } C^n = (\ldots, \underbrace{y_r * y_s \ \ldots * y_t}_{n \text{ factors}}, \ldots).$$

Each $x_m = \sum_1^n \left[n_i y_i \oplus a_i * y_i\right]$ where $n_i \in I$ and $a_i \in R$. Therefore each term in the product $\underbrace{x_i * x_j \ldots * x_\ell}_{n \text{ factors}}$ will contain a product of the form $\underbrace{y_h * y_f \ \ldots * y_o}_{n \text{ factors}}$. Hence every element of the set of generators for B^n is in C^n. Therefore $B^n \subseteq C^n$.

Lemma 3-14. If B and C are ideals in a Noetherian ring R and $C \subseteq B$, then $\overline{BC} = R$.

Proof: Obviously $\overline{BC} \subseteq R$. Suppose $x \in R$ and let c denote any element of C. Then $x * c \in B$ since $c \in B$. Therefore $x \in \overline{BC}$. Hence $\overline{BC} = R$.

Lemma 3-15. If A and B are ideals such that $\overline{AB} = A$, $\overline{AB^n} = A$ for each positive integer n.

Proof by induction: For $n = 1$, $\overline{AB} = A$ by hypothesis. Suppose for $n = k$ $\overline{AB^k} = A$; then $\overline{\overline{AB^k}B} = \overline{AB} = A$. Hence it will suffice to show that $\overline{\overline{AB^k}B} = \overline{AB^{k+1}}$. Suppose $x \in \overline{\overline{AB^k}B}$. Let g denote any element of B^{k+1}. Then g is a finite sum of terms each term containing k+1 factors. Hence $x*g = x* \sum_1^n c_i * b_i$ where $b_i \in B^k$ and $c_i \in B$. Each $x*c_i \in \overline{AB^k}$ since $x \in \overline{\overline{AB^k}B}$. Since $x\, c_i \in \overline{AB^k}$ $x * c_i * b_i \in A$. Hence $x * \sum_1^n c_i * b_i \in A$. Therefore if $g \in B^{k+1}$, $x * g \in A$. Hence $x \in \overline{AB^{k+1}}$. Now suppose $x \in \overline{AB^{k+1}}$; then $x \in \overline{\overline{AB^k}B}$. Let b denote any element of B^k and let c denote any element of B. Then $x * [c * b] \in A$ for any $b \in B^k$. Hence $x * c \in \overline{AB^k}$ which is true for all $c \in B$. Therefore $x \in \overline{\overline{AB^k}B}$ and proof is complete.

Theorem 3-10. If B and C are ideals in a Noetherian ring R, then $\overline{BC} = B$ if and only if C is not contained in any of the associated primes of B (1, p. 179).

Proof: Suppose C is not contained in any of the associated primes of B. Let $B = \bigcap B_i$ by theorem 3-8.

$$\overline{BC} = \overline{[\bigcap B_i]\, C}$$
$$= \bigcap \overline{B_i C} \quad \text{by lemma 3-12.}$$

For each B_i there is a $c_i \in C$ such that $c_i \notin \text{rad } B_i$. Therefore for each B_i, $\overline{B_iC} = B_i$ by lemma 3-13. Therefore $\bigcap \overline{B_iC} = \bigcap B_i = B$. Hence $\overline{BC} = B$. Suppose now $\overline{BC} = B$. Suppose also that C is contained in one of the associated primes of B. Without loss of generality denote this primary ideal as B_1. Then $C \subseteq \text{radical } B_1$. By theorem 3-3 there exists a positive integer n such that $[\text{radical } B_1]^n \subseteq B_1$. By lemma 3-13 $C^n \subseteq [\text{radical } B_1]^n$. Furthermore $\overline{B_1C^n} = R$ by lemma 3-14. Since $\overline{BC} = B$, $\overline{BC^n} = B$ by lemma 3-15.

$$\begin{aligned} B &= \overline{BC^n} \\ &= \overline{\bigcap B_i C^n} \\ &= \overline{B_1C^n} \cap \overline{B_pC^n} \text{ by lemma 3-12} \\ & \qquad\qquad\quad p \neq 1 \\ &= R \cap \overline{B_pC^n} \\ & \qquad\quad p \neq 1 \\ &= \bigcap_{p \neq 1} \overline{B_pC^n} \end{aligned}$$

But $\bigcap\limits_{p \neq 1} B_p \subseteq \overline{\bigcap\limits_{p \neq 1} B_p C^n}$. By lemma 3-12 $\overline{\bigcap\limits_{p \neq 1} B_p C^n} = \bigcap\limits_{p \neq 1} \overline{B_p C^n}$.

Therefore $\bigcap\limits_{p \neq 1} B_p \subseteq \bigcap\limits_{p \neq 1} \overline{B_p C^n}$. This implies $\bigcap\limits_{p \neq 1} B_p \subseteq B$.

Since $B = \bigcap B_i$ and $\bigcap B_i \subseteq \bigcap\limits_{p \neq 1} B_p$, $B \subseteq \bigcap\limits_{p \neq 1} B_p$. Therefore

$B = \bigcap B_p$. But if $\bigcap B_i = \bigcap\limits_{p \neq 1} B_p$ for $x \in \bigcap\limits_{p \neq 1} B_p$, $x \in \bigcap B_i$.

However if $x \in \bigcap B_i$, $x \in B_1$. Hence $\bigcap\limits_{p \neq 1} B_p \subseteq B_1$. But this result is a contradiction since $\bigcap B_i$ is an irredundant expression. Hence C is not contained in any of the associated primes of B.

CHAPTER BIBLIOGRAPHY

1. Jacobson, Nathan, Lectures in Abstract Algebra (2 Volumes) New York, Van Nostrand, 1951.

2. McCoy, Neal H., Rings and Ideals, Baltimore, The Waverly Press, 1948.

3. Northcott, D.D., Ideal Theory, Cambridge, University Press, 1953.

APPENDIX

BIBLIOGRAPHY

Jacobson, Nathan, Lectures in Abstract Algebra (2 volumes), New York, Van Nostrand, 1951.

McCoy, Neal H., Rings and Ideals, Baltimore, The Waverly Press, 1948.

Miller, Kenneth S., Elements of Modern Abstract Algebra, New York, Harper and Brothers, 1958.

Moore, John T., Elements of Abstract Algebra, New York, Macmillian, 1962.

Northcott, D.D., Ideal Theory, Cambridge, University Press, 1953.