SOME PROPERTIES OF IDEALS IN A COMMUTATIVE RING

APPROVED:

Mike Vaughan

Major Professor

John T. Mohat

Minor Professor

Frank Connor

Director of the Department of Mathematics

Robert B Toulouse

Dean of the Graduate School

Hicks, Gary B., Some Properties of Ideals in a Commutative Ring. Master of Science (Mathematics), August, 1973, 44 pp., bibliography, 1 title.

This thesis exhibits a collection of proofs of theorems on ideals in a commutative ring with and without a unity. Theorems treated involve properties of ideals under certain operations (sum, product, quotient, intersection, and union); properties of homomorphic mappings of ideals; contraction and extension theorems concerning ideals and quotient rings of domains with respect to multiplicative systems; properties of maximal, minimal, prime, semi-prime, and primary ideals; properties of radicals of ideals with relations to quotient rings, semi-prime, and primary ideals.

The thesis is divided into three chapters: "Introductory Concepts," "Properties of Ideals and Their Radicals Under Certain Operations," and "Properties of Maximal, Prime, and Primary Ideals."

In Chapter I, basic definitions and theorems assumed are stated. For proofs of the theorems stated in Chapter I, the reader is referred to Zariski and Samuel, Commutative Algebra, Vol. I and II, 1958. It is assumed that the reader is familiar with basic properties of sets and commutative rings.

Chapter II is sub-divided into four parts: "Some Properties of Quotients of Ideals," "Some Properties of

Ideals Under a Homomorphism," "Some Properties of Radicals of Ideals," and "Some Properties of Extensions and Contractions of Ideals with Respect to a Quotient Ring."

In Chapter III, some properties of maximal, minimal, prime, primary, and semi-prime ideals are presented under various hypotheses. One of the most interesting theorems in this chapter states that, if an ideal $\underline{A}$ of a ring is contained in the intersection of a finite set of prime ideals such that no prime ideal is contained in another, then $\underline{A}$ must be contained in one of the prime ideals. The chapter concludes with a proof that a ring with no divisors of zero such that each of its subrings is an ideal must be a commutative ring.

SOME PROPERTIES OF IDEALS IN A COMMUTATIVE RING

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

Gary B. Hicks, B. S.

Denton, Texas
August, 1973

TABLE OF CONTENTS

CHAPTER I

INTRODUCTORY CONCEPTS

This thesis exhibits a collection of proofs of theorems on ideals in commutative rings with and without a unity. Basic definitions and theorems which are assumed in developing proofs of the theorems in this thesis are stated in this chapter. For proofs of the theorems stated in this chapter see (1).

Theorems treated involve properties of ideals under certain operations (sum, product, quotient, intersection, and union); properties of homomorphic mappings of ideals; contraction and extension theorems concerning ideals and quotient rings of domains with respect to multiplicative systems; properties of maximal, minimal, prime, semi-prime, and primary ideals; properties of radicals of ideals with relations to quotient rings, semi-prime, and primary ideals; a certain ring with the property that every subring is an ideal.

As the title indicates, all rings considered are commutative, and the property of having or not having a unity is specified for each theorem or groups of theorems. It is assumed that the reader is familiar with basic properties of sets and commutative rings. For all rings the additive identity is denoted by 0 and the unity element (if it exists) by 1.

Addition of elements of rings is always denoted by + regardless of its meaning when used in different systems. If an element x of a ring is to be used in a sum n times, the symbol nx will denote this. It is understood that n is not necessarily an element of the ring, and the symbol nx should not be mistaken as a product involving elements of the ring. Multiplication is denoted by $\cdot$, but the symbol is not used unless confusion would, otherwise, result. In cases where it is necessary to raise a binomial sum to a power, binomial coefficients are used to simplify the notation. Set containment is denoted by $\subset$ and proper containment by $<$. J denotes the set of integers, and J_0 denotes the set of positive integers.

A subset A of a given commutative ring R is called an <u>ideal</u> of R if and only if: (1) $x, y \in A$ implies that $x - y \in A$, and (2) $a \in A$ and $r \in R$ implies that $ar = ra \in A$: i.e., the product of any element of A with any element of R remains in A.

<u>For the remainder of this chapter, reference to "the ring R" or simply "R" will be understood to denote a commutative ring</u>.

Notice that the definition of an ideal makes no guarantee that either of the elements of a product are in the ideal just because the product itself is in the ideal; in fact, the foregoing property is reserved for a special class of ideals. If A is an ideal in R, then for $a, b \varepsilon R$ such that $ab \varepsilon A$ and $a \varepsilon A$, it is not necessary that $b \varepsilon A$. However since a ring is a group under addition, if $a + b \varepsilon A$, and $a \varepsilon A$, then b must be an element of A.

An ideal A in a ring R is called a *proper ideal* of R if and only if A is not the *zero ideal* (the ideal whose set contains only the additive identity) and not R itself. A is a *principal ideal* of R if and only if there exists an element x of R so that any element of A is the product of x with some element of R: that is, if

$A = \{ xr \mid r \varepsilon R \}$ (sometimes denoted by (x) or xR).

A is said to be a *prime ideal* of R if and only if $a, b \varepsilon R$, and $ab \varepsilon A$, such that $b \notin A$, implies that $a \varepsilon A$. A is a *primary ideal* of R if and only if $c, d \varepsilon R$, and $cd \varepsilon A$, such that $d \notin A$, implies that $c^n \varepsilon A$ for some positive integer n. Note that if A is a prime ideal in R, then A is a primary ideal of R, but the converse is not always true. A is a *maximal ideal* in R if and only if there is no proper ideal of R which properly contains A: that is, if B is any ideal of R such that $A < B \subset R$, then $B = R$. A is said to be a *minimal ideal* of R if and only if $A \neq (0)$, and there is no ideal B of R such that $(0) < B < A$.

If A is an ideal in R, then C is called the *radical of A* (denoted by $\sqrt{A}$) if and only if

$$C = \{ x \varepsilon R \mid x^n \varepsilon A, n \varepsilon J_o \} .$$

If $A = \sqrt{A}$ then A is called a *semi-prime ideal* of R and conversely. If P is a prime ideal of R, then P is said to be a *minimal prime ideal of A* if and only if $A \subset P$, and there exists no prime ideal P' of R such that $A \subset P' < P$. The minimal prime ideals of the zero ideal are said to be the *minimal primes of R*.

If A and B are ideals in R, the *sum of A and B* is defined in the obvious manner as

$$A + B = \{ a + b \mid a \varepsilon A, \text{ and } b \varepsilon B \} ,$$

and the sum of A and B is also an ideal in R. In order to insure closure for the module, it is necessary to define the *product of A and B* as

$$A \cdot B = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \varepsilon A, b_i \varepsilon B, \text{ and } n \varepsilon J_o \right\}$$

so that A·B is also an ideal in R. The set of products of a single element x in R with elements in an ideal C of R is denoted by xC where

$$xC = \{ xc \mid c \varepsilon C \} .$$

The *quotient of A by B* is defined as

$$A:B = \{ x \varepsilon R \mid xB \subset A \} .$$

A non-zero element a in a ring R is called a *zero-divisor* if and only if there exists a non-zero element b in R such that ab = ba = 0. A commutative ring with a unity and without zero-divisors is called an *integral domain*, or more simply, a *domain*. Note that the requirement that there be no divisors of zero is equivalent to the cancellation law for multiplication: i.e., if a, b, and c are non-zero elements in D (a domain) such that $ab = ac$, then it follows that $b = c$ only if there are no divisors of zero in D. An integral domain D which contains at least two distinct elements (1 and 0) is called a <u>field</u> if for each non-zero element d of D there exists an element c of D such that $cd = dc = 1$.

Let D be a domain and let

$$E = \{ (a,b) \mid a,b \in D, \text{ and } b \neq 0 \} .$$

Define a relation $\sim$ in E by

$$(a,b) \sim (c,d) \text{ if and only if } ad = bc.$$

Now $\sim$ is an equivalence relation in E and defines a partition of E. Denote an equivalence class by $\frac{a}{b}$, where $(a,b) \in E$, and

$$\frac{a}{b} = \{ (x,y) \mid (x,y) \sim (a,b) \} .$$

Now let

$$K = \left\{ \frac{a}{b} \mid (a,b) \in E \right\}$$

and define two binary operations such that if $\frac{a}{b}, \frac{c}{d} \in K$ then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} ,$$

and

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} .$$

Then the algebraic system consisting of K and the operations + and $\cdot$ defined on K is a field which is called the <u>quotient field of D</u>.

A non-empty subset S of a ring R is a <u>multiplicative system in R</u> if and only if $0 \notin S$, and $a, b \in S$ implies that $a \cdot b \in S$. Let S be a multiplicative system in D, then D_S

such that $$D_S = \left\{ \frac{a}{b} \mid a,b \in D, \text{ and } b \in S \right\}$$

is called the quotient ring of D with respect to the multiplicative system S. If P is a proper prime ideal of D, then D\P defined by

$$D \backslash P = \{ x \in D \mid x \notin P \}$$

is a multiplicative system in D, and $D_{D \backslash P}$ is usually denoted simply as D_P so that

$$D_P = \left\{ \frac{a}{b} \mid a,b \in D, \text{ and } b \notin P \right\} .$$

If A is an ideal of D, then AD_S defined by

$$AD_S = \left\{ \sum_{i=1}^{m} a_i b_i \mid a_i \in A,\ b_i \in D_S, \text{ and } m \in J_o \right\}$$

is called the extension of A to D_S (or A extended to D_S). If B is an ideal of D_S, then $B \cap D$ is called the contraction of B in D (or B contracted to D_S).

If A is an ideal in a ring R and $r \in R$, then the set

$$r + A = \{ r + a \mid a \in A \}$$

is called the coset or residue class determined by r and A. Now let R/A be the set of all cosets of A in R and define the binary operations + and • in R/A as follows: for $c,d \in R$

$$(c + A) + (d + A) = (c + d) + A,$$

and $$(c + A) \cdot (d + A) = c \cdot d + A.$$

Then the algebraic system consisting of R/A with the operations + and • is a ring called the quotient ring (or residue class ring) of R modulo A. The zero element of R/A is an element $(z + A)$ such that $z \in A$.

A homomorphism of a ring R onto a ring R' is a function f from R onto R' such that if a, b ε R, then

$$f(a + b) = f(a) + f(b),$$

and $$f(ab) = f(a) \cdot f(b)$$

where f(a), f(b) ε R'. Furthermore if x' ε R', then there exists x ε R such that f(x) = x'. It is easily shown that

(1) f(0) is the additive identity for R'.

(2) f(1) is the unity element for R'.

(3) If x is the inverse of y for a given binary operation in f, then f(x) is the inverse of f(y) for the corresponding operation in R'.

(4) Any properties of the operations in R will be properties of the corresponding operations in R'.

If f(a) = f(b) implies that a = b for a, b ε R, then f is said to be a <u>one-to-one function</u>, and there exists a function denoted by $\underline{f}^{-1}$ called the <u>inverse of f</u> such that $f^{-1}(x') = x$ implies that f(x) = x', where x' ε R', and x ε R. If f is a homomorphism and K is a set of elements in R such that x ε K implies that f(x) = 0, then K is called <u>the kernel of the homomorphism</u> (or <u>the kernel of f</u>), and

$$K = \{ x \in R \mid f(x) = 0 \} .$$

An element a is said to be <u>idempotent</u> if and only if $a^2 = a$. An element b is said to be <u>nilpotent</u> if and only if $b^n = 0$ for some positive integer n.

A set S is said to be <u>partially ordered</u> if and only if there exists a binary relation $\leq$ defined for certain ordered pairs (a,b) of elements of S such that:

(1) $a \leq a$ for all $a \in S$ (reflexive);

(2) if $a \leq b$, and $b \leq a$, then $a = b$ (antisymmetric);

(3) if $a \leq b$, and $b \leq c$, then $a \leq c$ (transitive).

A subset S_1 of a partially ordered set S is called a <u>chain</u> (or <u>totally ordered</u>) if and only if for a, $b \in S_1$, either $a \leq b$, or $b \leq a$. An element u of S is called an <u>upper bound</u> of a subset S_1 of S if and only if $a \leq u$ for all $a \in S_1$. An element m of S is <u>maximal</u> if and only if there is no element $s \in S$ such that $m < s$, or, equivalently, if $m \leq s$ for some $s \in S$, then $m = s$. ($a < b$ means $a \leq b$, and $a \neq b$). S is said to be <u>inductive</u> if and only if every totally ordered subset of S has an upper bound in S, or equivalently, if every chain in S has an upper bound in S.

<u>Theorem 1.1</u>: If A and B are ideals of a commutative ring R, then $A + B$, and $A \cdot B$ are ideals of R such that A and B are contained, respectively, in $A + B$; also $A \cdot B$ is contained in each of A and B.

<u>Theorem 1.2</u>: If A and B are ideals of a commutative ring R, then $A:B$ is an ideal of R.

Theorem 1.3: If $\{I_i\}$ $i = 1,2,\ldots$ such that for any i, I_i is an ideal of a commutative ring R, then $\bigcap_{i=1}^{\infty} I_i$ is an ideal of R.

Theorem 1.4: If $T = \{A_\alpha\}$ is a chain of ideals in a commutative ring R, then $B = \bigcup A_\alpha$ is an ideal in R.

Theorem 1.5: If A is an ideal of a commutative ring R, then $\sqrt{A}$ is an ideal of R, and $\sqrt{A}$ contains A.

Theorem 1.6: Let Q be a primary ideal in a commutative ring R. If $P = \sqrt{Q}$, then P is a prime ideal in R. Moreover if $ab \in Q$, and $a \notin Q$, then $b \in P$. Also if A and B are ideals such that $AB \subset Q$, and $A \not\subset Q$, then $B \subset P$.

Theorem 1.7: Let Q and P be ideals in a ring R. Then Q is primary and P is its radical if and only if the following conditions are satisfied:

(1) $Q \subset P$;

(2) if $b \in P$, then $b^m \in Q$ for some positive integer m;

(3) if $ab \in Q$, and $a \notin Q$, then $b \in P$.

a condition equivalent to (3) is: if $ab \in Q$ and $b \notin P$, then $a \in Q$.

Theorem 1.8: If A is a maximal ideal in a commutative ring R with a unity, then A is a prime ideal in R.

Theorem 1.9: If f is a homomorphism frcm a ring R onto a ring R', and if A is an ideal of R, then f(A) such that

$$f(A) = \{ f(a) \mid a \in A \}$$

is an ideal of R'.

Theorem 1.10: If a partially ordered set S is inductive, then there exists a maximal element in S. (Zorn's Lemma)

CHAPTER II

PROPERTIES OF IDEALS AND THEIR RADICALS UNDER CERTAIN OPERATIONS

Theorems in this chapter involve various properties of ideals under operations of $+$, $\cdot$, $:$, $\cap$, and $\cup$: that is, the sum, product, quotient, intersection, and union of ideals. It can be shown (1) that if A and B are ideals in a commutative ring R, then each of the following are also ideals in R: $A + B$, $A \cdot B$, $A:B$, $A \cap B$, and $A \cup B$ (if either $A \subset B$ or $B \subset A$). Also, for any ideal C in R, $\sqrt{C}$ is an ideal in R.

Some Properties of Quotients of Ideals

The following theorems develop some useful relationships concerning quotients of ideals in a commutative ring with a unity. Each of the theorems in this section has the following general hypothesis: A, B, and C are ideals in a commutative ring R with a unity.

Theorem 2.1: If $A \subset B$, then $A:C \subset B:C$, and $C:A \supset C:B$.

Proof: Let $x \in A:C$ so that $xy \in A$ for any $y \in C$. Now since $A \subset B$, it follows that $xy \in B$ for any $y \in C$, and $x \in B:C$. Thus

$$A:C \subset B:C.$$

If $w \in C:B$, then $wz \in C$ for any $z \in B$. Therefore, since

$A \subset B$, $wh \in C$ for any $h \in A$. Now $w \in C:A$, and

$$C:A \supset C:B.$$

Now the proof is complete.

Theorem 2.2: $A:BC = (A:B):C$.

Proof: If $x \in A:BC$, then $xBC \subset A$. Now, for any $c \in C$, $xcB \subset xCB \subset A$, and hence $xc \in A:B$. Therefore $xC \subset A:B$, and $x \in (A:B):C$,which shows that

$$A:BC \subset (A:B):C.$$

If $y \in (A:B):C$, then $yC \subset A:B$. Now, for any $c \in C$, $yc \in A:B$ so $ycB \subset A$. Any element ycb, with $c \in C$ and $b \in B$, is in A. Thus, if $z \in yCB$, then

$$z = y\left(\sum_{i=1}^{n} c_i b_i\right) = \sum_{i=1}^{n} yc_i b_i; \; c_i \in C, \; b_i \in B, \text{ and } n \in J_o;$$

therefore, $z \in A$, and $yCB \subset A$. It follows that $y \in A:BC$; hence

$$(A:B):C \subset A:BC,$$

which completes the proof.

Theorem 2.3: $A:B^{n+1} = (A:B^n):B = (A:B):B^n$ for any $n \in J_o$.

Proof: Using the results from Theorem 2.2, it follows immediately that

$$A:B^{n+1} = A:B^nB = (A:B^n):B,$$

and

$$A:B^{n+1} = A:BB^n = (A:B):B^n.$$

Now the transitive property of equality completes the proof.

Theorem 2.4: $A:B = R$ if and only if $B \subset A$.

Proof: Let $x \in B$. Now, since $1 \in A:B$, $1 \cdot x \in A$; hence

$x \varepsilon A$, and $$B \subset A.$$

Conversely, suppose that $B \subset A$. It is clear that

$$A:B \subset R.$$

Let $y \varepsilon R$. If $b \varepsilon B$, then $b \varepsilon A$, and $yb \varepsilon A$; thus, $y \varepsilon A:B$, and $$R \subset A:B.$$

Therefore $$A:B = R.$$

Theorem 2.5: $A:B = A:(A + B)$.

Proof: If $x \varepsilon A:B$, then $xp \varepsilon A$ for all $p \varepsilon B$, and $xq \varepsilon A$ for all $q \varepsilon A$; thus $(xq + xp) \varepsilon A$, and $x(q + p) \varepsilon A$. Therefore, $x \varepsilon A:(A + B)$, and

$$A:B \subset A:(A + B).$$

If $y \varepsilon A:(A + B)$, then $(ya + yb) \varepsilon A$ for all $a \varepsilon A$, and $b \varepsilon B$. Now, since $ya \varepsilon A$, it follows that $yb \varepsilon A$; so $y \varepsilon A:B$, and

$$A:(A + B) \subset A:B;$$

therefore $$A:B = A:(A + B).$$

Theorem 2.6: $A: \sum_{i=1}^{m} B_i = \bigcap_{i=1}^{m} (A:B_i)$.

Proof: If $x \varepsilon A: \sum_{i=1}^{m} B_i$, then $x \cdot \left(\sum_{i=1}^{m} B_i \right) \subset A$; hence $x \cdot \left[\sum_{i=1}^{m} (b_i) \right] \varepsilon A$, where $b_i \varepsilon B_i$ for $i = 1,2,\ldots,m$. Now since $(xb_1 + xb_2 + \ldots + xb_m) \varepsilon A$, and $\left[x(0) + x(-b_2) + \ldots + x(-b_m) \right] \varepsilon A$ it follows that $xb_1 \varepsilon A$. It can be shown in a like manner that $xb_i \varepsilon A$ for $i = 1,2,\ldots,m$. Therefore, it is clear that $x \varepsilon \bigcap_{i=1}^{m} (A:B_i)$, and

$$A: \sum_{i=1}^{m} B_i \subset \bigcap_{i=1}^{m} (A:B_i).$$

If $y \in \bigcap_{i=1}^{m} (A:B_i)$, then $yB_i \subset A$ for any $i = 1,2,\ldots,m$; and so $yb_i \in A$ for any $b_i \in B_i$, $i = 1,2,\ldots,m$. Thus $y\left(\sum_{i=1}^{m} b_i\right) \in A$, and $y\left(\sum_{i=1}^{m} B_i\right) \subset A$. It follows that $y \in A: \sum_{i=1}^{m} B_i$; hence

$$\bigcap_{i=1}^{m} (A:B_i) \subset A: \sum_{i=1}^{m} B_i,$$

and therefore $$A: \sum_{i=1}^{m} B_i = \bigcap_{i=1}^{m} (A:B_i).$$

Theorem 2.7: $\left(\bigcap_{i=1}^{m} A_i\right):B = \bigcap_{i=1}^{m} (A_i:B)$.

Proof: Let $x \in \left(\bigcap_{i=1}^{m} A_i\right):B$, then $xB \subset \bigcap_{i=1}^{m} A_i \subset A_i$ for $i = 1,2,\ldots,m$; so that, $x \in A_i:B$ for $i = 1,2,\ldots,m$. Thus, $x \in \bigcap_{i=1}^{m} (A_i:B)$ which shows that

$$\left(\bigcap_{i=1}^{m} A_i\right):B \subset \bigcap_{i=1}^{m} (A_i:B).$$

If $y \in \bigcap_{i=1}^{m} (A_i:B)$, then $yB \subset A_i$ for any $i = 1,2,\ldots,m$; thus $yB \subset \bigcap_{i=1}^{m} A_i$. It follows that $y \in \left(\bigcap_{i=1}^{m} A_i\right):B$, and

$$\bigcap_{i=1}^{m} (A_i:B) \subset \left(\bigcap_{i=1}^{m} A_i\right):B.$$

Therefore $$\left(\bigcap_{i=1}^{m} A_i\right):B = \bigcap_{i=1}^{m} (A_i:B).$$

Some Properties of Ideals Under a Homomorphism

The theorems in this section exhibit some general relationships between ideals in the range of a homomorphism from a commutative ring onto a ring. The general hypothesis is <u>A and B are ideals in a commutative ring R, and f is a homomorphism from R onto a ring R'</u>.

<u>Theorem 2.8</u>: $f(A + B) = f(A) + f(B)$.

<u>Proof</u>: If $x \varepsilon f(A + B)$, then

$$\begin{aligned} x &= f(a + b) \\ &= f(a) + f(b), \end{aligned}$$

where $a \varepsilon A$, and $b \varepsilon B$. Thus, $x \varepsilon f(A) + f(B)$, and

$$f(A + B) \subset f(A) + f(B).$$

If $y \varepsilon f(A) + f(B)$, then

$$y = f(c) + f(d)$$

for some $c \varepsilon A$, and some $d \varepsilon B$; hence,

$$y = f(c + d),$$

and $$y \varepsilon f(A + B).$$

Therefore $$f(A) + f(B) \subset f(A + B),$$

and it follows that

$$f(A + B) = f(A) + f(B).$$

<u>Theorem 2.9</u>: $f(AB) = f(A) \cdot f(B)$.

<u>Proof</u>: If $x \varepsilon f(AB)$, then

$$x = f\left(\sum_{i=1}^{n} c_i d_i\right) \text{ with } c_i \varepsilon A,\ d_i \varepsilon B, \text{ and } n \varepsilon J_o;$$

thus

$$x = f(c_1)\cdot f(d_1) + f(c_2)\cdot f(d_2) + \ldots + f(c_n)\cdot f(d_n)$$
$$= \sum_{i=1}^{n} f(c_i)\cdot f(d_i);$$

so $x \varepsilon f(A)\cdot f(B)$, and it is clear that

$$f(AB) \subset f(A)\cdot f(B).$$

If $y \varepsilon f(A)\cdot f(B)$, then

$$y = \sum_{i=1}^{m} f(a_i)\cdot f(b_i),$$

where $a_i \varepsilon A$, and $b_i \varepsilon B$. It follows that

$$y = \sum_{i=1}^{m} f(a_i\cdot b_i)$$
$$= f\left(\sum_{i=1}^{m} a_i\cdot b_i\right) \varepsilon f(AB);$$

hence, $f(A)\cdot f(B) \subset f(AB)$,

and therefore $f(AB) = f(A)\cdot f(B)$.

Theorem 2.10: $f(A \cap B) \subset f(A) \cap f(B)$ (with equality if either A or B contain the kernel of the homomorphism).

Proof: If $x \varepsilon f(A \cap B)$, then

$$x = f(a), \text{ where } a \varepsilon A, \text{ and } a \varepsilon B.$$

Thus, $f(a) \varepsilon f(A)$, and $f(a) \varepsilon f(B)$; consequently

$$x \varepsilon f(A) \cap f(B),$$

and $f(A \cap B) \subset f(A) \cap f(B)$.

Now suppose $A \subset$ kernel f. If $y \varepsilon f(A) \cap f(B)$, then for some $a \varepsilon A$, and some $b \varepsilon B$

$$y = f(a),$$

and $y = f(b);$

so, $$f(a) - f(b) = 0,$$

and $$f(a - b) = 0.$$

Therefore $(a - b) \in A$, and, since $a \in A$, it follows that $b \in A$; hence, $b \in A \cap B$, and

$$f(b) \in f(A \cap B).$$

Thus, $$f(A) \cap f(B) \subset f(A \cap B),$$

which completes the proof that

$$f(A \cap B) = f(A) \cap f(B), \text{ if } A \supset \text{kernel } f.$$

(Clearly, the same result is obtained if $B \supset$ kernel f.)

Theorem 2.11: $f(A{:}B) \subset f(A){:}f(B)$ (with equality if A contains the kernel of the homomorphism).

Proof: If $x \in f(A{:}B)$, then,for some $c \in A{:}B$, $x = f(c)$. But $c \in A{:}B$ implies that $cB \subset A$; so that $cb \in A$ for any $b \in B$; hence

$$f(cb) = f(c) \cdot f(b) \in f(A),$$

and $$x = f(c) \in f(A){:}f(B).$$

Therefore $$f(A{:}B) \subset f(A){:}f(B).$$

Now suppose $A \supset$ kernel f. If $f(r) \in f(A){:}f(B)$ for some $r \in R$, then

$$f(r) \cdot f(B) \subset f(A),$$

and $f(r) \cdot f(b) = f(a)$ for some $b \in B$, and some $a \in A$; hence,

$$f(r) \cdot f(b) - f(a) = 0,$$

so $$f(rb - a) = 0.$$

Therefore $$rb - a \quad \in A,$$

and, since $a \in A$, $rb \in A$: that is, $r \in A{:}B$ so that

$$f(r) \in f(A{:}B), \text{ and}$$

$$f(A){:}f(B) \subset f(A{:}B).$$

Now, having shown containment both ways, it is clear that if $A \supset$ kernel f, then

$$f(A:B) = f(A):f(B).$$

Some Properties of Radicals of Ideals

The theorems in this section develop some useful relationships concerning radicals of sums, products, and intersections of ideals. Each of the theorems in this section is under the following general hypothesis: A and B are ideals in a commutative ring R.

Theorem 2.12: $\sqrt{AB} = \sqrt{A \cap B} = \sqrt{A} \cap \sqrt{B}$.

Proof: If $x \in \sqrt{AB}$, then

$$x^n = \sum_{i=1}^{k} a_i b_i, \; a_i \in A, \; b_i \in B, \text{ and } n,k \in J_0.$$

Since A and B are ideals,

$$\sum_{i=1}^{k} a_i b_i \in A \cap B;$$

hence $\qquad x \in \sqrt{A \cap B},$

and $\qquad \sqrt{AB} \subset \sqrt{A \cap B}.$

Let $y \in \sqrt{A \cap B}$, then

$$y^m \in A \cap B \text{ for some } m \in J_0;$$

so that $\qquad y^m \in A$, and $y^m \in B$.

Now it follows that $y \in \sqrt{A}$, and $y \in \sqrt{B}$: i.e.,

$$y \in \sqrt{A} \cap \sqrt{B}.$$

Therefore $\qquad \sqrt{A \cap B} \subset \sqrt{A} \cap \sqrt{B}.$

Let $w \in \sqrt{A} \cap \sqrt{B}$, then

$$w^p \in A, \text{ and } w^q \in B \text{ for some } p,q \in J_0.$$

Now, since $w^{p+q} \varepsilon AB$, it follows that

$$w \ \varepsilon \ \sqrt{AB},$$

and

$$\sqrt{A} \cap \sqrt{B} \subset \sqrt{AB}.$$

Now it is clear that

$$\sqrt{AB} \subset \sqrt{A \cap B} \subset \sqrt{A} \quad \sqrt{B} \subset \sqrt{AB};$$

hence

$$\sqrt{AB} = \sqrt{A \cap B} = \sqrt{A} \cap \sqrt{B}.$$

<u>Theorem 2.13</u>: $\sqrt{A + B} = \sqrt{\sqrt{A} + \sqrt{B}} \supset \sqrt{A} + \sqrt{B}$.

<u>Proof</u>: If $x \ \varepsilon \ \sqrt{A + B}$, then

$$x^m = a + b, \text{ for some } a \ \varepsilon \ A,\ b \ \varepsilon \ B, \text{ and } m \ \varepsilon \ J_o.$$

But $(a + b) \ \varepsilon \ \sqrt{A} + \sqrt{B}$, so

$$x^m \ \varepsilon \ \sqrt{A} + \sqrt{B}.$$

Thus

$$x \ \varepsilon \ \sqrt{\sqrt{A} + \sqrt{B}},$$

and therefore

$$\sqrt{A + B} \subset \sqrt{\sqrt{A} + \sqrt{B}}.$$

If $y \ \varepsilon \ \sqrt{\sqrt{A} + \sqrt{B}}$, then

$$y^n = a + b, \text{ where } a^p \ \varepsilon \ A, \text{ and } b^q \ \varepsilon \ B \text{ for some } p,q \ \varepsilon \ J_o.$$

Consequently

$$\left(y^n\right)^{(p+q)} = (a + b)^{(p+q)},$$

and it is easily seen that each term of the expansion of the right member above, up to and including the $(q-1)^{th}$ term, is a member of the ideal A, and, likewise, the sum of the q^{th} thru the $(p+q)^{th}$ terms is a member of B; hence

$$y^{(np+nq)} \ \varepsilon \ A + B,$$

and

$$y \ \varepsilon \ \sqrt{A + B}.$$

Therefore

$$\sqrt{\sqrt{A} + \sqrt{B}} \subset \sqrt{A + B},$$

and so

$$\sqrt{A + B} = \sqrt{\sqrt{A} + \sqrt{B}}.$$

It can be shown (1) that $\sqrt{A}$ and $\sqrt{B}$ are ideals in R, so that

$(\sqrt{A} + \sqrt{B})$ is an ideal in R; therefore, it follows directly from Theorem 1.5 that

$$\sqrt{\sqrt{A} + \sqrt{B}} \supset \sqrt{A} + \sqrt{B}.$$

Theorem 2.14: If $A^k \subset B$ for some positive integer k, then $\sqrt{A} \subset \sqrt{B}$.

Proof: If $x \in \sqrt{A}$, then $x^m \in A$; so

$$(x^m)^k \in A^k.$$

But $$A^k \subset B;$$

therefore $$x^{mk} \in B,$$

and $$x \in \sqrt{B}.$$

Now it follows that $$\sqrt{A} \subset \sqrt{B}.$$

Theorem 2.15: $\sqrt{\sqrt{A}} = \sqrt{A}$.

Proof: If $x \in \sqrt{\sqrt{A}}$, then

$$x^m \in \sqrt{A} \text{ for some } m \in J_o,$$

and $$(x^m)^p \in A \text{ for some } p \in J_o.$$

Therefore $$x \in \sqrt{A},$$

and $$\sqrt{\sqrt{A}} \subset \sqrt{A}.$$

Since the radical of any ideal in R contains that ideal (Theorem 1.5), it follows that

$$\sqrt{A} \subset \sqrt{\sqrt{A}},$$

consequently $$\sqrt{\sqrt{A}} = \sqrt{A}.$$

Some Properties of Extensions and Contractions of Ideals with Respect to a Quotient Ring

Recall from Chapter I that the extension of an ideal A in a domain D to the quotient ring of D with respect to some multiplicative system S (denoted by D_S), is the product of A with D_S: i.e., AD_S. The contraction of an ideal B in D_S, to D_S is the intersection of B with D: i.e., $B \cap D$. Various properties of these contractions and extensions will be constructed in this section. For each of the theorems D is an integral domain with $1 \neq 0$. $D \backslash P$ and S are multiplicative systems in D (P is a proper, prime ideal of D).

Theorem 2.16: Let D be a domain with $1 \neq 0$ and quotient field K. Let S be a multiplicative system in D. Then $D_S = \left\{ \frac{a}{b} \mid a,b \in D, \text{ and } b \in S \right\}$ is an integral domain with $1 \neq 0$, and $D \subset D_S \subset K$.

Proof: For any $d \in D$, $\frac{d}{1}$ is an equivalence class in K, so $D \subset K$. Obviously, D_S is a subset of the field K, so the following properties of a domain are hereditary in D_S: associativity and commutativity of addition and multiplication, distributivity for multiplication over addition, no zero divisors, and $1 \neq 0$.

D_S is a module since, if $\frac{a}{b}, \frac{c}{d} \in D_S$, then it is clear that

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in D_S.$$

That D_S is closed under multiplication follows almost immediately from the definition of D_S. For any $\frac{e}{f}, \frac{g}{h} \in D_S$

$$\frac{e}{f}\cdot\frac{g}{h} = \frac{eg}{fh} \varepsilon D_S.$$

Thus, D_S is an integral domain with $1 \neq 0$, and $D \subset D_S \subset K$.

Theorem 2.17: If A is an ideal of D, then AD_S is an ideal of D_S.

Proof: That AD_S is a subset of D_S can be seen as follows: if $x \varepsilon AD_S$, then

$$x = \sum_{i=1}^{n} a_i b_i;\ a_i \varepsilon A,\ b_i \varepsilon D_S, \text{ and } n \varepsilon J_o.$$

$$x = \sum_{i=1}^{n} a_i \cdot \frac{c_i}{d_i};\ c_i,\ d_i \varepsilon D,\ d_i \varepsilon S.$$

$$x = \frac{a_1c_1d_2d_3\ldots d_n + a_2c_2d_1d_3\ldots d_n + \ldots + a_nc_nd_1d_2\ldots d_{n-1}}{d_1d_2\ldots d_n}.$$

But each $a_ic_i \prod_{j=1}^{n} d_j$, (where $d_i = 1$), ε A, and $\prod_{j=1}^{n} d_j \varepsilon S$; hence

$$x \varepsilon D_S, \text{ and } AD_S \subset D_S.$$

For any $x,y \varepsilon AD_S$, it was shown above that

$$x = \frac{a} {b} \text{ for some } a \varepsilon A,\ b \varepsilon S,$$

$$y = \frac{c}{d} \text{ for some } c \varepsilon A,\ d \varepsilon S.$$

Thus

$$x - y = \frac{ad - bc}{bd}$$

where $ad - bc \varepsilon A$ (since A is an ideal in D), and $bd \varepsilon S$; so

$$x - y \varepsilon AD_S.$$

If $z \varepsilon AD_S$, and $w \varepsilon D_S$, then

$$z = \frac{e}{f} \text{ for some } e \varepsilon A,\ f \varepsilon S,$$

$$w = \frac{g}{h} \text{ for some } g \varepsilon D,\ h \varepsilon S.$$

$$zw = \frac{eg}{fh} \varepsilon AD_S;$$

hence AD_S is an ideal in D_S.

Theorem 2.18: If B is an ideal of D_S, then $B \cap D$ is an ideal of D.

Proof: Obviously, $B \cap D \subset D$. Since B and D are ideals in D_S, $x,y \varepsilon B \cap D$ implies that

$$x - y \varepsilon B \cap D.$$

If $r \varepsilon B \cap D$, and $s \varepsilon D$, then $s \varepsilon D_S$: thus

$$rs \varepsilon B \text{ (since B is an ideal in } D_S).$$

It is clear that $rs \varepsilon D$; therefore

$$rs \varepsilon B \cap D,$$

and $B \cap D$ is an ideal in D.

Theorem 2.19: $A \cap S \neq \emptyset$ if and only if $AD_S = D_S$.

Proof: It was shown in Theorem 2.17 that

$$AD_S \subset D_S.$$

If $x \varepsilon D_S$, then

$$x = \frac{a}{b} \text{ where } a,\ b \varepsilon D,\ b \varepsilon S.$$

Let $y \varepsilon A \cap S$, then

$$x = \frac{a}{b} \cdot \frac{y}{y} = \frac{ay}{by}.$$

But $ay \varepsilon A$, and $by \varepsilon S$; therefore

$$x = ay \cdot \frac{1}{by} \varepsilon AD_S.$$

Thus $D_S \subset AD_S$, and $AD_S = D_S$.

Conversely, if $AD_S = D_S$, then for any $x \varepsilon S$, it is clear that

$$\frac{x}{x} = \frac{a}{s},$$

for some $a \in A$, $s \in S$. Thus

$$xs = xa,$$

which implies that $s = a.$

Therefore $A \cap S \neq \emptyset.$

Theorem 2.20: If A is an ideal in D, and P is a prime, proper ideal of D such that $P \supset A$, then

$$AD_P = \left\{ \frac{a}{b} \mid a,b \in D,\ a \in A,\ b \notin P \right\}.$$

Proof: Recall that $D \backslash P = \{ x \in D \mid x \notin P \}$, and $D_{D\backslash P}$ is denoted by D_P. Since $1 \in D\backslash P$, it follows that $AD_P \neq D_P$ if and only if P contains A. From the first part of Theorem 2.17, it is clear that

$$AD_P \subset \left\{ \frac{a}{b} \mid a,b \in D,\ a \in A,\ b \notin P \right\}.$$

If $y \in \left\{ \frac{a}{b} \mid a,b \in D,\ a \in A,\ b \notin P \right\}$, then

$$y = \frac{r}{s} \text{ where } r,s \in D,\ r \in A,\ s \notin P;$$

so $y = r.\frac{1}{s}$ where $r \in A$, $\frac{1}{s} \in D_P$.

Therefore $y \in AD_P,$

and $\left\{ \frac{a}{b} \mid a,b \in D,\ a \in A,\ b \notin P \right\} \subset AD_P;$

hence $AD_P = \left\{ \frac{a}{b} \mid a,b \in D,\ a \in A, \text{ and } b \notin P \right\}.$

Theorem 2.21: If A and B are ideals of D, then $(A + B)D_S = AD_S + BD_S$.

Proof: If $x \in (A + B)D_S$, then

$$x = \frac{g + h}{f};\ g \in A,\ h \in B, \text{ and } f \in S.$$

Now it follows easily that

$$x = \frac{g}{f} + \frac{h}{f},$$

therefore $x \in AD_S + BD_S$,

and $(A + B)D_S \subset AD_S + BD_S$.

If $y \in AD_S + BD_S$, then

$$y = \frac{a}{b} + \frac{c}{d};\ \text{where } a \in A,\ c \in B, \text{ and } b,d \in S.$$

$$y = \frac{ad + bc}{bd}$$

$$y = (ad + bc)\left(\frac{1}{bd}\right).$$

But $ad \in A$, $bc \in B$, and $\frac{1}{bd} \in D_S$; therefore

$$y \in (A + B)D_S, \text{ and } AD_S + BD_S \subset (A + B)D_S.$$

Now it is clear that

$$(A + B)D_S = AD_S + BD_S.$$

Theorem 2.22: If A and B are ideals of D, then $(AB)D_S = AD_S \cdot BD_S$.

Proof: $a \in (AB)D_S$ implies that

$$a = \frac{x}{s};\ x \in AB, \text{ and } s \in S.$$

But if $x \in AB$, then

$$x = \sum_{i=1}^{n} a_i b_i;\ a_i \in A, \text{ and } b_i \in B.$$

Therefore

$$a = \frac{\sum_{i=1}^{n} a_i b_i}{s} = \frac{a_1}{s}.\frac{b_1 s}{s} + \frac{a_2}{s}.\frac{b_2 s}{s} + \ldots + \frac{a_n}{s}.\frac{b_n s}{s}.$$

Since $\frac{a_i}{s} \varepsilon AD_S$, and because B is an ideal in D with s ε D, it follows that

$$b_i s \; \varepsilon \; B; \text{ so that } \frac{b_i s}{s} \; \varepsilon \; BD_S.$$

Now if $\frac{a_i}{s} = f_i$, and $\frac{b_i s}{s} = g_i$, it is clear that

$$a = \sum_{i=1}^{n} f_i g_i \; \varepsilon \; AD_S \cdot BD_S,$$

and hence $(AB)D_S \subset AD_S \cdot BD_S$.

If $y \; \varepsilon \; AD_S \cdot BD_S$, then

$$y = \sum_{i=1}^{m} c_i d_i; \; c_i \; \varepsilon \; AD_S, \text{ and } d_i \; \varepsilon \; BD_S.$$

Let $c_i = \frac{p_i}{s_i}$; $p_i \; \varepsilon \; A$, and $s_i \; \varepsilon \; S$,

$d_i = \frac{q_i}{t_i}$; $q_i \; \varepsilon \; B$, and $t_i \; \varepsilon \; S$.

Now $c_i d_i = p_i q_i \left(\frac{1}{s_i t_i}\right)$.

Let $z_i = p_i q_i \; \varepsilon \; AB$,

$w_i = \frac{1}{s_i t_i} \; \varepsilon \; D_S$.

Then

$$y = \sum_{i=1}^{m} z_i w_i \; \varepsilon \; (AB)D_S,$$

and it is clear that $AD_S \cdot BD_S \subset (AB)D_S$;

hence $(AB)D_S = AD_S \cdot BD_S$.

<u>Theorem 2.23</u>: If A and B are ideals in D, then $(A \cap B)D_S = AD_S \cap BD_S$.

<u>Proof</u>: If $x \; \varepsilon \; (A \cap B)D_S$, then it follows that

$$x = \sum_{i=1}^{n} r_i s_i;\ r_i \in A \quad B,\ s_i \in D_S.$$

Since $r_i \in A \cap B$, it follows that

$$r_i s_i \in AD_S, \text{ and } r_i s_i \in BD_S.$$

Now, because AD_S and BD_S are ideals in D_S,

$$x \in AD_S, \text{ and } x \in BD_S;$$

hence $$x \in AD_S \cap BD_S,$$

and $$(A \cap B)D_S \subset AD_S \cap BD_S.$$

If $y \in AD_S \cap BD_S$, then

$$y = \sum_{i=1}^{m} p_i q_i;\ p_i \in A \cap B,\ q_i \in D_S.$$

Therefore $$y \in (A \cap B)D_S,$$

and $$AD_S \cap BD_S \subset (A \cap B)D_S.$$

Thus $$(A \cap B)D_S = AD_S \cap BD_S.$$

Theorem 2.24: If A is an ideal in D, then $(\sqrt{A})D_P = \sqrt{AD_P}$.

Proof: If $x \in (\sqrt{A})D_P$, then

$$x = \frac{a}{d};\ a \in \sqrt{A}, \text{ and } d \notin P.$$

Now $a^n \in A$ for some $n \in J_o$. It follows that

$$x^n = \frac{a^n}{d^n};\ a^n \in A,\ d^n \notin P,$$

and therefore $$x^n \in AD_P.$$

This implies that

$$x \in \sqrt{AD_P}; \text{ hence, } (\sqrt{A})D_P \subset \sqrt{AD_P}.$$

If $y \in \sqrt{AD_P}$, then

$$y^m \in AD_P \text{ for some } m \in J_o.$$

Therefore $$y^m = \frac{q}{r};\ q \in A, \text{ and } r \notin P.$$

Now it follows that

$$ry^m = q,$$

$$(ry)^m = qr^{m-1} \varepsilon A,$$

$$ry \varepsilon \sqrt{A},$$

$$ry = z \varepsilon \sqrt{A},$$

$$y = \frac{z}{r}.$$

Therefore $y \varepsilon (\sqrt{A})D_p$, and $\sqrt{AD_p} \subset (\sqrt{A})D_p$,

and it follows that

$$(\sqrt{A})D_p = \sqrt{AD_p}.$$

Theorem 2.25: If A' and B' are ideals of D_p, then $(A' \cap B') \cap D = (A' \cap D) \cap (B' \cap D)$, and $(\sqrt{A'}) \cap D = \sqrt{A' \cap D}$.

Proof: The first part is easily shown as a consequence of properties of sets, but it is important to note that the statement shows that the contraction of the intersection of two ideals in a domain is precisely the intersection of the contractions of those ideals in the domain.

Here is a proof of the second part:

If $x \varepsilon (\sqrt{A'}) \cap D$, then

$$x^m \varepsilon A', \text{ and } x^m \varepsilon D \text{ for some } m \varepsilon J_o;$$

thus $x \varepsilon \sqrt{A' \cap D}$, and $(\sqrt{A'}) \cap D \subset \sqrt{A' \cap D}$.

If $y \varepsilon \sqrt{A' \cap D}$, then

$$y^n \varepsilon A'; n \varepsilon J_o;$$

so that $y \varepsilon \sqrt{A'}$.

But $y \varepsilon D$ (since $A' \cap D$ is an ideal in D); thus

$$y \varepsilon (\sqrt{A'}) \cap D,$$

and $\qquad \sqrt{A' \cap D} \subset \sqrt{A'} \cap D.$

Therefore $\qquad (\sqrt{A'}) \cap D = \sqrt{A' \cap D},$

and the proof is complete.

CHAPTER III

PROPERTIES OF MAXIMAL, PRIME, AND PRIMARY IDEALS

This chapter displays properties of prime, semi-prime, primary, maximal, and minimal ideals under various hypotheses. The last theorem in this chapter shows an interesting relationship between the subrings of a certain ring and the commutativity of that ring. With the exception of the latter theorem, all theorems in this chapter are under the following general hypothesis: R is a commutative ring with a unity.

Theorem 3.1: If A is an ideal in R such that $A \neq R$, then A is contained in a maximal ideal.

Proof: Form a set T such that if I is an element of T then I is an ideal of R which contains A, and $I \neq R$. T is not empty since $A \varepsilon T$. T is partially ordered by the relation of containment. Also any chain in T has an upper bound in T (namely the ideal formed by the union of the ideals in the chain). Now by Zorn's Lemma (see Theorem 1.10) there exists a maximal element M in T. M is also maximal in R because if there exists an ideal Q in R such that $Q \neq R$, and $M < Q$, then $A < Q$ so $Q \varepsilon T$: that is to say, M is not a maximal element in T; hence, a contradiction. Thus, M is maximal in R and M contains A.

Theorem 3.2: If R has exactly one maximal ideal M, then the only idempotent elements in R are 0 and 1.

Proof: Suppose there exists an element b in R such that: $b \neq 0$, $b \neq 1$, and $b^2 = b$. Now, since M is maximal in R, M is prime in R (see Theorem 1.8); so, because $(b - 1) \cdot b = 0$, either b is in M or $(b - 1)$ is in M. However, both of the elements b and $(b - 1)$ cannot be in M because, if they are, then b and $(1 - b)$ are in M which implies that $1 \in M$, and $M = R$; thus contradicting the hypothesis that M is maximal in R.

Let A and B be principal ideals in R such that

$$A = \{ xb \mid x \in R \}$$
$$B = \{ y(b - 1) \mid y \in R \} .$$

$1 \notin A$, since this would imply that $1 = qb$ for some q in R, thus producing the contradiction that $b = 1$. Therefore, $A \neq R$. Now, using the conclusion from Theorem 3.1, A is contained in M (since M is the only maximal ideal in R); and so $b \in M$. Similarly, $1 \notin B$, since this would imply that $1 = p(b - 1)$ for some $p \in R$, producing the contradiction that $b = 0$. Thus $B \neq R$, and, using the same argument as before, B is contained in M; thus $(b - 1) \in M$. Now the fact that both b and $(b - 1)$ are contained in M is a contradiction; thus, b cannot exist.

Theorem 3.3: An ideal A in R is semi-prime if and only if R/A has no non-zero nilpotent elements.

Proof: Assume there exists an element $a \in R$ such that

$a \notin A$, and $(a + A)^k = 0 + A = A$ for some $k \varepsilon J_o$. Then it follows that $a^k \varepsilon A$, so $a \varepsilon \sqrt{A} = A$ which is a contradiction. Therefore, the element a does not exist; hence $(a + A)$ does not exist.

Conversely, if R/A has no non-zero nilpotent elements, let $x^m \varepsilon A$ for some $m \varepsilon J_o$, and suppose $x \notin A$. Then $(x + A)^m = x^m + A = A$; thus, contradicting the hypothesis that R/A has no non-zero nilpotent elements. Therefore, if $x \varepsilon \sqrt{A}$, then $x \varepsilon A$, and $\sqrt{A} \subset A$. It is already known (see Theorem 1.5) that $A \subset \sqrt{A}$. It follows that $A = \sqrt{A}$, and A is semi-prime.

Theorem 3.4: An ideal A in R is primary if and only if every zero divisor in R/A is nilpotent.

Proof: Let $a,b \varepsilon R$ such that $a,b \notin A$. Furthermore, suppose that $(a + A)(b + A) = ab + A = A$; i.e., $ab \varepsilon A$. Then, since A is primary, and $a \notin A$, it follows that $b^n \varepsilon A$ for some $n \varepsilon J_o$. Hence, $(b + A)^n = 0 + A$; thus, $(b + A)$ is nil-potent.

Conversely, suppose every zero divisor in R/A is nilpotent. Let $a,b \varepsilon R$ such that $ab \varepsilon A$, and $b \notin A$. If $a \varepsilon A$, then A is primary, but if $a \notin A$, then $(a + A)$ and $(b + A)$ are zero-divisors in R/A. Therefore, for some $n \varepsilon J_o$, $(a + A)^n = a^n + A = 0 + A$, and, consequently, $a^n \varepsilon A$; thus A is a primary ideal in R.

Theorem 3.5: If $Q_1,\ldots,Q_n$ is a finite set of primary ideals of R such that $\sqrt{Q_i} = P$ for $i = 1,2,\ldots,n$, then $Q = \bigcap_{i=1}^{m} Q_i$ is a primary ideal of R and $\sqrt{Q} = P$.

Proof: It can be shown (1) that if $\{Q_1,\ldots,Q_n\}$ is a set of ideals in R, then $Q = \bigcap_{i=1}^{n} Q_i$ is also an ideal of R. Let $a,b \varepsilon R$ such that $ab \varepsilon Q$, and $b \not\varepsilon Q$. If $ab \varepsilon Q$, then $ab \varepsilon Q_i$ for any $i = 1,2,\ldots,n$, but since $b \not\varepsilon Q$, there must exist some Q_j ($j \varepsilon \{1,2,\ldots,n\}$) such that $b \not\varepsilon Q_j$. Furthermore, since Q_j is primary, $a^{p_j} \varepsilon Q_j$ for some $p_j \varepsilon J_o$; hence $a \varepsilon \sqrt{Q_j}$, and, since $\sqrt{Q_j} = \sqrt{Q_i}$ for any $i = 1,2,\ldots,n$, it is clear that $a \varepsilon \sqrt{Q_i}$, and for any $i = 1,2,\ldots,n$ there exists p_i such that $a^{p_i} \varepsilon Q_i$. Let K be the largest p_i, then $a^K \varepsilon Q_i$ for each $i = 1,2,\ldots,n$. Therefore $a^K \varepsilon Q$, and Q is a primary ideal of R.

Let $x \varepsilon \sqrt{Q}$, then

$$x^r \varepsilon Q \text{ for some } r \varepsilon J_o;$$

thus $x^r \varepsilon Q_i$, and $x \varepsilon \sqrt{Q_i}$ for any $i = 1,2,\ldots,n$, and

$$\sqrt{Q} \subset P.$$

If $y \varepsilon P$, then

$$y \varepsilon \sqrt{Q_i} \text{ for any } i = 1,2,\ldots,m.$$

Let M be an integer such that

$$y^M \varepsilon Q_i \text{ for any } i = 1,2,\ldots,m;$$

then $$y^M \varepsilon \bigcap_{i=1}^{m} Q_i = Q.$$

Thus $$y \varepsilon \sqrt{Q}, \text{ and } P \subset \sqrt{Q};$$

hence $$\sqrt{Q} = P.$$

Theorem 3.6: If P_1 and P_2 are ideals of R such that $P_1 \not\subset P_2$, and $P_2 \not\subset P_1$, then $P_1 \cap P_2$ is not a prime ideal.

Proof: Suppose $a \cdot b \ \varepsilon \ P_1 \cap P_2$ for some a,b ε R such that $a \ \varepsilon \ P_2$ but $a \not\varepsilon P_1$, and $b \ \varepsilon \ P_1$ but $b \not\varepsilon P_2$. Then $a \not\varepsilon P_1 \cap P_2$, and $b \not\varepsilon P_1 \cap P_2$; hence, $P_1 \cap P_2$ is not a prime ideal.

Theorem 3.7: If $\{P_i\}$ i = 1,2,... is a chain of prime ideals of R, then $A = \bigcap_{i=1}^{\infty} P_i$, and $B = \bigcup_{i=1}^{\infty} P_i$ are prime ideals of R.

Proof: A is an ideal in R. If ab ε A, and $b \not\varepsilon A$ then there exists some $P_j \supset A$ such that $b \not\varepsilon P_j$, and, since P_j is prime, $a \ \varepsilon \ P_j$. Furthermore, for any P_k such that $P_k \subset P_j$, $b \not\varepsilon P_k$ so $a \ \varepsilon \ P_k$. For any P_q such that $P_j \subset P_q$, $a \ \varepsilon \ P_q$, since $a \ \varepsilon \ P_j$. Therefore

$$a \ \varepsilon \ \bigcap_{i=1}^{\infty} P_i,$$

and A is a prime ideal of R.

It can be shown (1) that if $B = \bigcup_{i=1}^{\infty} P_i$, then B is an ideal in R. If xy ε B, and $y \not\varepsilon B$, then $y \not\varepsilon P_i$ for any i = 1,2,... . Therefore $a \ \varepsilon \ P_i$ for some i = 1,2,... , and hence, a ε B. Therefore, B is a prime ideal.

Theorem 3.8: If A is an ideal of R, and P is a prime ideal of R containing A, then P contains a minimal prime ideal of A.

Proof: Form a set T such that if I ε T, then I is contained in P, and I is a prime ideal of R containing A.

T is not empty since P is in T. Let T be partially ordered by the relation $\leq$ such that if B and C are elements of T, $B \leq C$ if and only if C is contained in B. Now T is inductive since any chain in T has an upper bound in T (namely, the prime ideal which is the intersection of all the prime ideals of the chain). So T contains a maximal element M, and M is a minimal prime of A, for if $A \subset J < M \subset P$, then $M \leq J$; hence $M = J$, which is a contradiction.

<u>Lemma 3.9</u>: If a prime ideal contains a finite intersection of ideals, then it contains at least one of the ideals.

<u>Proof</u>: The proof is by induction, and the case for $n = 2$ will be shown below.

Let A and B be two ideals such that their intersection is contained in a prime ideal P. Certainly $A \cap B$ contains AB. Now if $P \supset A \cap B$, then $P \supset AB$. Suppose $P \not\supset A$, then there exists $x \in A$ such that $x \notin P$. If $y \in B$, then $xy \in P$ since $P \supset AB$; but P is prime, so $y \in P$. Therefore, $P \supset B$.

<u>Theorem 3.10</u>: Let A be an ideal in R, and let $P_1, P_2, P_3, \ldots, P_m$ be a finite set of prime ideals of R such that if $i \neq j$, then $P_i \not\subset P_j$. If $A \not\subset P_i$ for $i = 1,2,\ldots,m$, then there exists an element $a \in A$ such that $a \notin \bigcup_{i=1}^{m} P_i$; hence $A \not\subset \bigcup_{i=1}^{m} P_i$.

<u>Proof</u>: Consider the set $A \cap \left(\bigcap_{i \neq j} P_j\right)$. Now $A \cap \left(\bigcap_{i \neq j} P_j\right) \not\subset P_i$ for $i = 1,2,\ldots,m$, because if so, then

$P_i \supset A$ (which is a contradiction), or $P_i \supset \left(\bigcap_{i \neq j} P_j\right)$, and hence $P_i \supset P_j$ for some $j \neq i$ (which is also a contradiction). So there exists $a_1 \varepsilon A \cap \left(\bigcap_{i \neq j} P_j\right)$ such that $a_1 \notin P_1$, and in general there exists $a_i \varepsilon A \cap \left(\bigcap_{i \neq j} P_j\right)$, such that $a_i \notin P_i$. Let $a = \sum_{i=1}^{m} a_i$. Certainly $a \varepsilon A$, and $a \notin \bigcup_{i=1}^{m} P_i$ because if $\sum_{i=1}^{m} a_i \varepsilon \bigcup_{i=1}^{m} P_i$, then $\sum_{i=1}^{m} a_i \varepsilon P_j$ for some $j = 1,2,\ldots m$. Hence, $\left(\sum_{i=1}^{m} a_i\right) - a_j \varepsilon P_j$, which implies that $a_j \varepsilon P_j$ resulting in a contradiction. Therefore the element a does exist, and consequently $A \not\subset \bigcup_{i=1}^{m} P_i$.

With the prime ideals under the same hypothesis, the contrapositive of Theorem 3.10 is worth taking note of: that is, if $A \subset \bigcup_{i=1}^{m} P_i$, then $A \subset P_j$ for some j.

Theorem 3.11: A proper ideal of R is maximal if and only if, for every element $r \notin M$, there exists an element $b \varepsilon R$ such that $1 + rb \varepsilon M$.

Proof: If $r \notin M$, consider the ideal $(r) + M$, and denote it by I. I consists of elements of the form $ar + d$, where $a \varepsilon R$, and $d \varepsilon M$. Now since M is maximal, and I contains M, it follows that $I = R$; hence, every element in R is of the form $ar + d$. In particular, there exists $c \varepsilon R$, and $x \varepsilon M$ such that

$$1 = cr + x, \text{ and } 1 + (-cr) = x \varepsilon M.$$

Conversely, suppose there exists an ideal A such that $M \subset A$, and $M \neq A$. Then there exists $x \in A$ such that $x \notin M$, and it follows that $1 + xc \in M$ for some $c \in R$. Therefore, $1 + xc \in A$, and, since $xc \in A$, it follows that $1 \in A$; hence $A = R$, and M is maximal in R.

Lemma 3.12: If f is a homomorphism from R onto a ring R', and I is an ideal in R containing the kernel of f, then $f(a) \in f(I)$ implies that $a \in I$.

Proof: $f(I) = \{ x \in R' \mid x = f(a) \text{ for some } a \in I \}$. If b is any element of R such that $f(b) \in f(I)$, then there exists $a \in I$ such that $f(b) = f(a)$. Therefore, $f(b) - f(a) = 0$, and $f(a - b) = 0$: i.e., $(a - b) \in I$; thus, $b \in I$.

Theorem 3.13: Let f be a homomorphism from R onto a ring R'. If M is a maximal ideal of R containing the kernel of f, then f(M) is a maximal ideal of R'.

Proof: Suppose M is a proper ideal, and let A' be any ideal in R' such that $f(M) < A'$. Then there must exist $a \in R$ with $f(a) \in A'$ so that $f(a) \notin f(M)$, and $a \notin M$. Now it has been shown (see Theorem 3.11) that there exists an element $b \in R$ such that $1 + ba \in M$, and so $f(1 + ba) \in f(M)$. Since f is a homomorphism and f(M) is contained in A', it follows that

$$f(1) + f(b) \cdot f(a) \in A'.$$

Since A' is an ideal, $f(a) \in A'$ implies that

$$f(b) \cdot f(a) \in A',$$

and so it follows that $f(1) \varepsilon A'$ which means that $A' = R$; hence, $f(M)$ is maximal in R'.

If M is the zero ideal, then $f(M)$ contains only the zero of R'. Suppose there exists a proper ideal A' of R'. Then, $f^{-1}(A') = \{ x \varepsilon R \mid f(x) \varepsilon A' \}$ is a proper ideal of R which contradicts the fact that M is maximal in R. Hence, A' cannot exist, and $f(M)$ is maximal in R'.

Theorem 3.14: Let f be a homomorphism from R onto a ring R'. If M' is a maximal ideal of R', then $f^{-1}(M') = \{ x \varepsilon R \mid f(x) \varepsilon M' \}$ is a maximal ideal in R.

Proof: Suppose M' is a proper ideal. If there exists an ideal A in R such that $f^{-1}(M') < A$, then there is some $x \varepsilon A$ such that $x \not\varepsilon f^{-1}(M')$, and $f(x) \not\varepsilon M'$. Therefore, for some $f(b) \varepsilon R'$, it follows that

$$f(1) + f(b)\, f(x) \varepsilon M'$$

so that

$$f(1 + bx) \varepsilon M',$$

and

$$1 + bx \varepsilon f^{-1}(M') < A.$$

Now, since $bx \varepsilon A$, it follows that $1 \varepsilon A$, and $A = R$: that is, $f^{-1}(M')$ is a maximal ideal in R.

If M' is the zero ideal, then $f^{-1}(M')$ is the kernel of the homomorphism. If there exists an ideal B in R such that $f^{-1}(M') < B < R$, then: $f(B)$ is an ideal of R', $f(B) \neq M'$, and $f(B) \neq R'$. So the existence of B contradicts the hypothesis that M' is maximal in R'; hence, B cannot exist, and $f^{-1}(M')$ is a maximal ideal in R.

Theorem 3.15: let f be a homomorphism from R onto a ring R'. Then the mapping $M \rightarrow f(M)$ defines a one-to-one correspondence between the maximal ideals of R which contain the kernel of f and the set of all maximal ideals of R'.

Proof: It was shown in Theorem 3.14 that if M' is any maximal ideal in R', $f^{-1}(M')$ will be a maximal ideal in R containing the kernel of f. So, any maximal ideal in R' is the image of some maximal ideal in R which contains the kernel of f. If $f(M_1) = f(M_2)$, then, for any $x_1 \varepsilon M_1$, $f(x_1) \varepsilon f(M_2)$; so $x_1 \varepsilon M_2$, and $M_1 \subset M_2$. For any $x_2 \varepsilon M_2$, $f(x_2) \varepsilon f(M_1)$; so $x_2 \varepsilon M_1$, and $M_2 \subset M_1$. Hence, $M_1 = M_2$. (The latter argument is based on the conclusion of Lemma 3.12.) Now the one-to-one correspondence is seen.

It will now be shown that each of the theorems above concerning maximal ideals under a homomorphism is valid for prime and primary ideals. For each of the theorems 3.16 - 3.21 below, the following general hypothesis will apply: f is a homomorphism from R onto a ring R'.

Theorem 3.16: If P is a prime ideal of R containing the kernel of f, then f(P) is a prime ideal in R'.

Proof: If $x,y \varepsilon f(R)$, and $xy \varepsilon f(P)$ such that $y \not\varepsilon f(P)$; then $y = f(a)$, and $a \not\varepsilon P$. Let $x = f(b)$ so that

$$xy = f(b) \cdot f(a) = f(ba).$$

It follows that $ba \varepsilon P$; hence, $b \varepsilon P$, and $x = f(b) \varepsilon f(P)$. Thus, f(P) is a prime ideal in R'.

Theorem 3.17: If P' is a prime ideal of R', then $f^{-1}(P') = \{ x \in R \mid f(x) \in P' \}$ is a prime ideal in R.

Proof: If $x,y \in R$, and $xy \in f^{-1}(P')$ such that $y \notin f^{-1}(P')$, then $f(y) \notin P'$. $f(xy) = f(x)\cdot f(y) \in P'$, and, since P' is a prime ideal in R', $f(x) \in P'$. Hence $x \in f^{-1}(P')$, and therefore $f^{-1}(P')$ is a prime ideal of R.

Theorem 3.18: The mapping $P \to f(P)$ defines a one-to-one correspondence between the prime ideals of R which contain the kernel of f and the set of all prime ideals of R'.

Proof: The proof is constructed in the same manner as the proof of Theorem 3.15 and will not be given here.

Theorem 3.19: If Y is a primary ideal of R containing the kernel of f, then $f(Y)$ is a primary ideal of R'.

Proof: For any $x,y \in R'$ such that $xy \in f(Y)$ and $y \notin f(Y)$, let $x = f(a)$, and $y = f(b)$. Since $y \notin f(Y)$, it follows that $b \notin Y$. $f(a)\cdot f(b) \in f(Y)$; hence $ab \in Y$, which implies that $a^n \in Y$ for some $n \in J_0$, and thus $f(a^n) \in f(Y)$. But $f(a^n) = [f(a)]^n = x^n \in f(Y)$. Now it is clear that $f(Y)$ is a primary ideal in R'.

Theorem 3.20: If Y' is a primary ideal of R', then $f^{-1}(Y') = \{ x \in R \mid f(x) \in Y' \}$ is a primary ideal in R.

Proof: Let $r,s \in R'$ such that $rs \in f^{-1}(Y')$, and $s \notin f^{-1}(Y')$. Now $f(s) \notin Y'$, but $f(rs) = f(r):f(s) \in Y'$; so it follows that $[f(r)]^n \in Y'$. Hence $f(r^n) \in Y'$, which implies that $r^n \in f^{-1}(Y')$, thus completing the proof that $f^{-1}(Y')$ is a primary ideal in R.

Theorem 3.21: The mapping $Y \to f(Y)$ defines a one-to-one correspondence between the primary ideals of R which contain the kernel of f and the set of all primary ideals of R'.

Proof: The proof is constructed in the same manner as the proof of Theorem 3.15 and will not be given here.

Theorem 3.22: If M_1 and M_2 are distinct maximal ideals in R, then $M_1M_2 = M_1 \cap M_2$.

Proof: It is clear that $M_1M_2 \subset M_1 \cap M_2$. If $p \varepsilon M_1 \cap M_2$, let $y \varepsilon M_1$ so that $y \notin M_2$. Then there exists $b \varepsilon R$ such that $1 + by \varepsilon M_2$. If $1 + by = q$, then $1 = q - by$. Now $p = pq + p[-(yb)]$ where the product pq is composed of an element p from M_1 and an element q from M_2; and the product $p[-(yb)]$ is composed of an element p from M_2 and an element $-(yb)$ from M_1. So, it follows that $p \varepsilon M_1M_2$; thus, $M_1 \cap M_2 \subset M_1M_2$, and therefore $M_1M_2 = M_1 \cap M_2$.

Theorem 3.23: Let M be a proper ideal of R. M is maximal if and only if, for each ideal A of R, either $A \subset M$ or else $A + M = R$.

Proof: If $A \not\subset M$, then, since M is maximal, $M \not\subset A$; so there exists $x \varepsilon A$ such that $x \notin M$; hence, for some $b \varepsilon R$, $1 + xb \varepsilon M$. Since $xb \varepsilon A$, it follows that $-(xb) \varepsilon A$, and $[-(xb) + (1 + xb)] \varepsilon A + M$. Therefore, $1 \varepsilon A + M$: that is, $A + M = R$.

Conversely, suppose there exists an ideal A' such that

$M < A' < R$. Then it follows that $A' + M = R$, so there exists $a' \varepsilon A'$ and $m \varepsilon M$ such that $1 = a' + m$. But $m \varepsilon A'$, so $1 \varepsilon A'$, and $A' = R$. Hence, the existence of A' produced a contradiction, so A' does not exist and M is maximal in R.

Theorem 3.24: A non-zero ideal B of R is minimal if and only if $bR = B$ for every non-zero element $b \varepsilon B$.

Proof: If $b \varepsilon B$, then $bR = \{ bx \mid x \varepsilon R \}$, and certainly $bR \varepsilon B$. But, since bR is an ideal for any $b \varepsilon B$, it follows that for every non-zero $b \varepsilon B$, $bR = B$ because B is minimal, and no non-zero ideal of R can be properly contained in B.

Conversely, if $bR = B$ for every non-zero element $b \varepsilon B$, suppose there exists an ideal A such that $(0) < A < B$. Any element of B is in the set aR where $a \varepsilon A < B$; hence, any element of B is in A,which contradicts the hypothesis that $A < B$. Therefore, A does not exist, and B is minimal.

Theorem 3.25: If P is a proper ideal of R, then P is a prime ideal of R if and only if $T = R \backslash P = \{ x \varepsilon R \mid x \notin P \}$ is a multiplicative system.

Proof: T is not empty since P is a proper ideal of R. Also $0 \notin T$ since $0 \varepsilon P$. Suppose $a,b \varepsilon T$. Now if $ab \notin T$, then $ab \varepsilon P$,which means either $a \varepsilon P$ or $b \varepsilon P$; thus contradicting the hypothesis that $a,b \varepsilon T$. So $ab \varepsilon T$, and T is a multiplicative system.

Conversely, if T is a multiplicative system, and if

$ab \in P$, then either $a \in P$ or $b \in P$ because, if neither a nor b is in P, then $a,b \in T$, and $ab \in T$. The latter statement contradicts the hypothesis that $ab \in P$; hence, P is a prime ideal.

The following theorem, though not directly related to the theorems of this chapter, is a fitting climax to this study of ideals in a commutative ring.

Theorem 3.26: Let R be a ring with the property that every subring of R is an ideal of R. If R has no divisors of zero, then R is a commutative ring.

Proof: Consider any elements a and b in R. Form the following set:

$$C(a) = \{ r \in R \mid ar = ra \} .$$

To prove that C(a) is a subring of R, it must be shown that:

(1) The collection $\langle C(a), + \rangle$ is an algebraic system and an abelian group.

(2) The set C(a) is closed under multiplication.

Proof of (1): $\langle C(a), + \rangle$ is an algebraic system since the set C(a) contains at least one element, namely a. The operation + is associative in C(a) by heredity. Consider any elements x and y in C(a). It follows that

$$ax = xa$$

$$ay = ya$$

$$ax - ay = xa - ya$$

$$a(x - y) = (x - y)a,$$

and thus, if x and y are in C(a), then (x - y) is in C(a). The operation + is commutative in C(a) by heredity; therefore, the system is an abelian group.

Proof of (2): Consider any elements x,y in C(a). It follows that

$$\begin{aligned} ax &= xa \\ ay &= ya \\ (ax)(ay) &= (xa)(ya) \\ [(ax)a]y &= (ax)(ya) \\ [a(xa)]y &= a[x(ya)] \\ a[(ax)y] &= a[(xy)a] \\ a[a(xy)] &= a[(xy)a], \end{aligned}$$

and, since there are no zero-divisors,

$$a(xy) = (xy)a.$$

Therefore, $xy \varepsilon C(a)$; thus completing the argument that C(a) is a subring of R. Now it must follow, from the hypothesis, that C(a) is an ideal of R; hence, ab is in C(a), and

$$\begin{aligned} a(ab) &= (ab)a \\ a(ab) &= a(ba). \end{aligned}$$

Now it is clear that

$$ab = ba,$$

thus completing the proof that R is a commutative ring.

BIBLIOGRAPHY

Zariski, Oscar and Pierre Samuel, *Commutative Algebra*, Vol. I, (2 volumes), Princeton, New Jersey, D. Van Nostrand Company, Inc., 1958.