PROPERTIES OF EXTENDED AND CONTRACTED IDEALS

APPROVED:

Robert H. Cranford
Major Professor

Russell H. Bilyeu
Minor Professor

John T. Mohat
Director of the Department of Mathematics

Robert B. Toulouse
Dean of the Graduate School

PROPERTIES OF EXTENDED AND CONTRACTED 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

George Chan, B. A.
Denton, Texas
August, 1966

TABLE OF CONTENTS

CHAPTER I

PROPERTIES OF IDEALS

This paper presents an introduction to the theory of ideals in a ring with emphasis on ideals in a commutative ring with identity.

Basic definitions and properties of ideals are given and these properties are studied in the classes of ideals called extended and contracted ideals. The ideal structure in quotient rings is investigated with respect to the ideal structure of the rings over which they lie and theorems are provided to show applications of the theory developed.

Definition 1-1. A set is a collection of objects; these objects are called elements of the set.

Definition 1-2. A binary operation "o" on a set A is a correspondence that associates with each ordered pair (a,b) of elements of A a uniquely determined element a o b of A.

Notation:

Small letters will denote the elements of a set and capital letters will denote sets.

$\in$ means belongs to or is an element of.

$\notin$ means does not belong to or is not an element of.

$\subset$ means is contained in or is included in.

$<$ means proper containment (i.e., $A < B$ means A is a proper subset of B) when used between sets and means less than when used between elements of sets.

$\leq$ means less than or equal to.

$\sum$ means the sum of.

$\equiv$ means the same as.

<u>Definition 1-3</u>. A nonempty set G on which there is defined a binary operation "o" is called a group (with respect to this operation) provided the following properties are satisfied:

(1) The operation "o" is associative. If a, b, c are any elements of G, then $(a \circ b) \circ c = a \circ (b \circ c)$.

(2) There exists in G an identity element e such that $a \circ e = e \circ a = a$ for all elements a in G.

(3) For each element a in G there exists an inverse a^{-1} in G, such that $a \circ a^{-1} = a^{-1} \circ a = e$.

<u>Definition 1-4</u>. If R is a nonempty set on which there are defined binary operations $\oplus$ and $\odot$, which will be called addition and multiplication respectively, such that the following conditions hold, then R is a ring.

(1) Addition in R is associative.

(2) R contains an additive identity element.

(3) For each element a in R, there exists an additive inverse, denoted by $-a$, in the set R.

(4) Addition in R is commutative. If $a, b \in R$, then $a \oplus b = b \oplus a$.

(5) Multiplication in R is associative.

(6) Multiplication in R is left distributive and right distributive with respect to addition, i.e.,
$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ and
$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$ for any elements a, b, c in R.

Operation Notation.

In order to simplify the notation, the product $a \odot b$ for $a, b \in R$ will sometimes be written as ab.

Definition 1-5. A ring is called a commutative ring if and only if the operation of multiplication is commutative.

Definition 1-6. A ring is a ring with unity if and only if there is a multiplicative identity (unity element) in the ring.

Theorem 1-1. A nonempty subset A of a ring R is a subring of R if and only if the following two conditions hold.

(a) A is closed under the operations of addition and multiplication defined on R.

(b) If $a \in A$, then $-a \in A$ (1, P. 26).

Proof:

Conditions (a) and (b) are required of all rings and hence must be satisfied if A is a subring of R.

Conversely, if A is a subset of R satisfying properties (a) and (b), then properties (1), (4), (5), and (6) in the definition of a ring hold in R, hence hold in A also. Condition (b) is identical to property (3) of this definition so only the existence of an additive identity needs to be shown in A. Since A is not empty, it must contain at least one element, say x. Under condition (b), -x is also in A. By condition (a), $x \oplus (-x)$ is an element of A, but $x \oplus (-x)$ is the additive identity of R. A contains an additive identity and is therefore a subring of R.

<u>Definition 1-7</u>. Let A be a nonempty subset of a ring R such that

(1) $a \oplus (-b) \in A$ if a and b are elements of A.

(2) $ra \in A$ if $a \in A$ and $r \in R$.

Then A is called a left ideal in R.

The following statement is an equivalent definition of left ideal in R. A subset A of a ring R is a left ideal in R if and only if it is a subring of R such that ra is in A for every r in R and every a in A.

A subset A of a ring R is a right ideal in R if and only if it is a subring of R such that ar is in A for every a in A and every r in R.

A left ideal is the same as a right ideal in a commutative ring R since $ar = ra$ for every a in A and every r in R. In this case A is simply called an ideal.

Theorem 1-2. If a is an element in a ring R, then the set $A = \{ra \mid r \in R\}$ is a left ideal in R.

Proof:

The set A is not empty by construction. Let ra and sa be any two elements of A. Then $ra \oplus (-sa) = [r \oplus (-s)]a$ by the right distributive law in R. But $r \oplus (-s)$ is in R, hence $ra \oplus (-sa) \in A$. If $r_1 a \in A$ and $r_2 \in R$, then $r_2(r_1 a) = (r_2 r_1)a \in A$ since $r_2 r_1 \in R$. Hence A is a left ideal.

Corollary 1-1. If a is an element in a commutative ring R with unity, then the set $A = \{ra \mid r \in R\}$ is an ideal in R. Further, if B is an ideal in R and $a \in B$, then $A \subset B$.

Proof:

The first part of the corollary follows from theorem 1-2 and the definition of ideal. Now suppose that B is any ideal such that a is an element of B. By the definition of a left ideal, ra is in B for every r in R. But $A = \{ra \mid r \in R\}$, so that $A \subset B$. This means that every ideal of R which contains the element a must contain A.

Definition 1-8. The ideal A of corollary 1-1 is called the principal ideal generated by the element a, denoted by (a). A ring in which every ideal is a principal ideal is called a principal ideal ring.

Note. R will denote a commutative ring with unity throughout the rest of the paper.

Definition 1-9. Let A and B denote ideals in a ring R, define $A + B = \left\{a \oplus b \mid a \in A,\ b \in B\right\}$.

Theorem 1-3. If A and B are ideals in a ring R, then A + B is an ideal in R.

Proof:

The set A + B is not empty since A and B are each contained in A + B.

Let x and y be any two elements of A + B, where $x = a \oplus b$ for some a in A, and b in B; $y = a_o \oplus b_o$ for some a_o in A, and b_o in B. Then $x \oplus (-y) = (a \oplus b) \oplus \left[-(a_o \oplus b_o)\right]$ $= \left[a \oplus (-a_o)\right] \oplus \left[b \oplus (-b_o)\right] \in A + B$, since $\left[a \oplus (-a_o)\right]$ is an element of A and $\left[b \oplus (-b_o)\right]$ is an element of B.

Let r be an arbitrary element of R; then $rx = r(a \oplus b)$ $= ra \oplus rb$ by the left distributive law of R. But $(ra \oplus rb)$ is in A + B, since ra is in A and rb is in B.

Hence A + B is an ideal.

Definition 1-10. If A and B are ideals in a ring R, define the product of A and B as

$$AB = \left\{\sum_{i=1}^{k} a_i b_i \;\middle|\; a_i \in A,\ b_i \in B,\ k \text{ arbitrary positive integer}\right\}.$$

Theorem 1-4. If A and B are ideals in R, then AB is an ideal in R.

Proof:

The set AB is not empty by construction. Let x and y be any two elements of AB such that $x = \sum_{i=1}^{s} a_i b_i$, $y = \sum_{j=1}^{t} a'_j b'_j$ for some a_i, a'_j in A and b_i, b'_j in B, and $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots, t$. Then $x \oplus (-y) = \sum_{i=1}^{s} a_i b_i \oplus (-\sum_{j=1}^{t} a'_j b'_j)$. Let $-a'_j = a_{s+j}$ and $b'_j = b_{s+j}$ for $1 \leq j \leq t$. Hence $x \oplus (-y) = \sum_{j=1}^{s} a_j b_j \oplus \sum_{j=1}^{t} a_{s+j} b_{s+j} = \sum_{j=1}^{s+t} a_j b_j$ in AB since a_j in A and b_j in B for $j = 1, 2, \ldots, s+t$.

Let r be an arbitrary element of R, then $rx = r \sum_{i=1}^{s} a_i b_i = \sum_{i=1}^{s} r a_i b_i = \sum_{i=1}^{s} (r a_i) b_i$ in AB since $r a_i$ in A and b_i in B for $i = 1, 2, \ldots, s$.

Hence AB is an ideal in R.

Lemma 1-1. If A and B are ideals in R, then AB is contained in A and AB is contained in B.

Proof:

Let x be any element of AB such that $x = \sum_{i=1}^{n} a_i b_i$ for some a_i in A and b_i in B. In particular, since B is an ideal, and b_i in B, this implies that b_i in R. Hence $a_i b_i$ in A by definition 1-7. Therefore $x = \sum_{i=1}^{n} a_i b_i \in A$ and $AB \subset A$.

The proof of $AB \subset B$ is similar.

Definition 1-11. If A and B are ideals in R, then the quotient A:B consists of all elements c in R such that $cB \subset A$ (cB means (c)B).

Theorem 1-5. If A and B are ideals in R, then A:B is an ideal in R.

Proof:

Since A and B are ideals, AB is contained in A by lemma 1-1. Let a be any element in A; then aB is contained in A. This implies A is contained in A:B. Hence A:B is not empty.

Let x, y be elements in A:B; then xB is contained in A and xb is in A for every b in B. Also yB is contained in A and yb is in A for every b in B. Fix b arbitrary; then $xb \oplus (-yb)$ is in A. Since the distributive law is valid in R, then $[x \oplus (-y)]b$ is an element of A for every b in B. Then $[x \oplus (-y)]B$ is contained in A. Hence $x \oplus (-y)$ is an element of A:B.

Let z be an element in A:B; this implies that zB is contained in A by definition 1-11. If b is an arbitrary element of B, zb in A implies that r(zb) is in A, $r \in R$, by definition 1-7. Then (rz)b in A, since multiplication is associative in R. This implies $(rz)B$ is contained in A or $rz \in A:B$.

Hence A:B is an ideal in R.

Definition 1-12. If A is an ideal in R, the radical of A, denoted by $\sqrt{A}$, consists of all elements $b \in R$ some power of which is contained in A (i.e., if x is in the radical of A, then there exists a positive integer n such that x^n is in A.)

Theorem 1-6. If A is an ideal in R, then the radical of A is an ideal in R.

Proof:

The radical of A is not empty since A is contained in the radical of A.

Let x and y be any two elements of the radical of A; then there exist positive integers m and n such that x^m is in A and y^n is in A. The term $[x \oplus (-y)]^{m+n}$ expanded yields $\sum_{k=0}^{m+n} c_k x^k y^{(m+n)-k}$ for binomial coefficients c_k, or by the factorial notation $\sum_{k=0}^{m+n} \frac{(m+n)!}{[(m+n)-k]!k!}(-1)^k x^k y^{(m+n)-k}$. Either k is greater than or equal to m, or $(m+n)-k$ is greater than or equal to n. Hence $[x \oplus (-y)]^{m+n}$ is an element of A and $x \oplus (-y)$ is in the radical of A.

Let r be an arbitrary element of R; then $(rx)^m$ is equal to $r^m x^m \in A$ since $r^m \in R$, $x^m \in A$. Then rx is in the radical of

A and the radical of A is an ideal in R.

Lemma 1-2. Every ideal in the ring of integers is principal.

Proof:

Let A be an ideal of ring R. If A = (0), then it is principal ideal. If A contains a number b not equal to 0, then it also contains -b, and one of these numbers is positive. Let a be the least positive element of A, and c an arbitrary element in A. If r is the non-negative remainder when c is divided by a, then $c = qa + r$ for $0 \leq r < a$. Since c and a belong to the ideal, $c - qa = r$ belongs to the ideal also. Since r is less than a, then r is equal to zero because a is the least positive number of the ideal. Hence $c = qa$. Therefore all numbers of the ideal A are multiples of a. Hence A = (a), and A is a principal ideal.

Definition 1-13. Let R be a ring. An ideal A is said to be prime if whenever a product bc in A with b and c in R, then either b in A or c in A.

Let $m > 1$ be an integer and suppose (m) is a prime ideal in the ring of integers. If m is not a prime integer, then $m = ab$, where a and b are integers different from 0, 1, -1. No generality is lost in assuming a and b positive, thus $0 < a < m$ and $0 < b < m$. But since (m) is prime, $ab \in (m)$ implies that either $a \in (m)$ or $b \in (m)$, and from this it follows that either a = ma' or b = mb' for some positive integers a' and b'. This is impossible since both a and b are positive integers less than m. This contradiction implies m must be prime.

Conversely, if m = p is a prime integer and the ideal (p) contains ab, where a and b are integers, it follows that ab = cp for some integer c. Hence p divides ab and so p divides either a or b, whence (p) contains either a or b. It follows from the definition that (p) = (m) is a prime ideal.

Definition 1-14. Let R be a ring. An ideal A is said to be maximal if A is not equal to R and there exists no ideals between A and R. (i.e., If $A \subset K \subset R$, either K = A, or K = R.)

In the ring of integers I, every proper prime ideal is maximal (2, P. 112). For suppose A = (p) is any proper prime ideal in I, with another ideal B such that $A \leqslant B \leqslant I$. Then there exists an element t in B such that t is not in A. This implies t is not equal to jp for any integer j. Hence the greatest common divisor of t and p is 1. Since 1 is the greatest common divisor of t and p, there exist integers x and y such that 1 = tx + py. But tx is in B and py is in B also; this implies that 1 is in B. If 1 is in B, then B = I, and this is a contradition. Hence A is maximal.

Definition 1-15. Let R be an arbitrary ring and let A be an ideal in R. Then A is said to be primary if the conditions a, b in R, ab in A, a is not in A imply the existence of a positive integer m such that b^m is in A.

Theorem 1-7. Let Q be a primary ideal in R. If P is the radical of Q, then P is prime. Moreover if $ab \in Q$, $a \notin Q$, then $b \in P$. Also if A and B are ideals in R such that AB is contained in Q and A is not contained in Q, then B is contained in P.

Proof:

Let $\sqrt{Q} = P$, and $a, b \in R$ such that $ab \in P$. Suppose $a \notin P$; then $a^n \notin Q$ for any integer n. There exists an integer t, such that $(ab)^t \in Q$, or $a^t b^t \in Q$, and $a^t \notin Q$ implies $(b^t)^m \in Q$ for some integer m. Hence $b^{tm} \in Q$ implies $b \in \sqrt{Q} = P$. Therefore P is a prime ideal.

Now if $ab \in Q$ with $a \notin Q$, then $b^m \in Q$ for some positive integer m; hence $b \in \sqrt{Q} = P$.

Also, if A is not contained in Q, there exists an element $a_o \in A$ such that $a_o \notin Q$, $a_o b \in Q$ for every $b \in B$. But $a_o \notin Q$ implies $b \in P$ for every $b \in B$; hence $B \subset P$.

Definition 1-16. Let Q denote a primary ideal and let $P = \sqrt{Q}$. Then Q is said to be a primary ideal belonging to P or that Q is primary for P.

Theorem 1-8. Let Q and P are ideals in a ring R such that

(1) $Q \subset P$.

(2) If $b \in P$, then $b^n \in Q$ for some integer n. (n may depend on b)

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

Then Q is primary with radical P if and only if these conditions hold.

Proof:

Suppose Q is primary with radical P; then $Q \subset P$ by definition 1-16. If $b \in P = \sqrt{Q}$, then $b^n \in Q$ for some integer n. If $ab \in Q$, $a \notin Q$, then $b^k \in Q$ for some integer k since Q is a primary ideal. Hence $b \in \sqrt{Q} = P$.

Assume (1), (2), and (3), if $ab \in Q$, $a \notin Q$, then $b \in P$ by (3). By (2) $b \in P$ implies $b^n \in Q$ for some integer n; hence Q is primary. To show $P = \sqrt{Q}$, show $P \subset \sqrt{Q}$ and $\sqrt{Q} \subset P$. Let $b \in P$, by (2) $b^n \in Q$ implies $b \in \sqrt{Q}$ or $P \subset \sqrt{Q}$. Now if $x \in \sqrt{Q}$, then $x^t \in Q$ where t is the least exponent such that $x^t \in Q$. If $t = 1$, then $x \in Q \subset P$ by (1). If $t \neq 1$, then $x^{t-1} \notin Q$ implies $x \in P$ by (3). Hence $\sqrt{Q} \subset P$.

The following statement is an equivalent form of condition (3).

If $ab \in Q$, $b \notin P$, then $a \in Q$.

<u>Corollary 1-2</u>. Let R be a ring with unity, and let Q, P be ideals in R such that

(1) $Q \subset P$.

(2) If $b \in P$, then $b^n \in Q$ for some integer n.

(3) P is a maximal ideal.

Then Q is primary belonging to P.

Proof:

Let $ab \in Q$, $b \notin P$; it is necessary to show that $a \in Q$. Consider the ideal $P + (b)$; then $P < P + (b) \subset R$. Since P is a maximal ideal, it follows that $P + (b) = R$ and $p + rb = e$ for some $p \in P$, $r \in R$, where e denotes the identity in R. By (2), there exists a positive integer k such that $p^k \in Q$ and also $(p + rb)^k = e$. The expansion of this equation gives
$p^k + kp^{k-1}(rb) + \ldots + (rb)^k = e$, and
$p^k + b(kp^k r + \ldots + r^k b^{k-1}) = e$. Let t denote
$(kp^k r + \ldots + r^k b^{k-1})$; then $ap^k + abt = a$ by multiplying this equation by a. Then $ap^k \in Q$ since $p^k \in Q$, and $abt \in Q$ since $ab \in Q$; hence $a \in Q$.

CHAPTER BIBLIOGRAPHY

1. McCoy, Neal H., Introduction to Modern Algebra, Boston, Allyn and Bacon, Inc., 1960.

2. Moore, John T., Elements of Abstract Algebra, New York, Macmillan Company, 1962.

CHAPTER II

EXTENDED AND CONTRACTED IDEALS

Definition 2-1. Let R be a ring. A ring R' is said to contain a homomorphic image of R if there exists a mapping $\overline{f}$ of R into R' such that the operations of addition and multiplication are preserved. Then $\overline{f}(a \oplus b) = \overline{f}(a) \boxplus \overline{f}(b)$ and $\overline{f}(a \odot b) = \overline{f}(a) \boxdot \overline{f}(b)$ where addition is denoted by $\oplus$ and $\boxplus$ and multiplication is denoted by $\odot$ and $\boxdot$ in rings R and R' respectively. This mapping is called a homomorphism of R into R'.

Throughout this chapter R and S will denote rings with unity, and $\overline{f}$ will denote a homomorphism of R into S such that $\overline{f}(e) = e'$ where e denotes the identity in R and e' the identity in S. The relations between ideals in R and ideals in S will be discussed with ideals in R being denoted by capital letters with subscript r, and ideals in S by capital letters with subscript s. The operations of addition and multiplication will be denoted by $\oplus$, $\odot$ and $\boxplus$, $\boxdot$ in R and S respectively.

<u>Theorem</u> <u>2-1</u>. Let A_s be an arbitrary ideal in S. Then $\overline{f}^{-1}(A_s) = \{x \mid x \in R, \overline{f}(x) \in A_s\}$ is an ideal in R.

Proof:

Let x, y $\overline{f}^{-1}(A_s)$; then $\overline{f}(x \oplus (-y)) = \overline{f}(x) \boxplus \overline{f}(-y)$. Since $\overline{f}(x), \overline{f}(y) \in A_s$ and A_s is an ideal it follows that $\overline{f}(-y) = -\overline{f}(y) \in A_s$ (2, p. 17). Therefore $\overline{f}(x \oplus (-y)) = \overline{f}(x) \boxplus \overline{f}(-y) \in A_s$; hence $x \oplus (-y) \in \overline{f}^{-1}(A_s)$. If $r \in R$, then $\overline{f}(rx) = \overline{f}(r)\overline{f}(x) \in A_s$ since $\overline{f}(x) \in A_s$ and $\overline{f}(r) \in S$. Hence $rx \in \overline{f}^{-1}(A_s)$ for any $x \in \overline{f}^{-1}(A_s)$ and $r \in R$ and therefore $\overline{f}^{-1}(A_s)$ is an ideal in R.

<u>Theorem</u> <u>2-2</u>. Let A_r be an arbitrary ideal in R. Then $S(\overline{f}(A_r)) = \{y' \mid y' = \sum_{i=1}^{n} s_i a_i$ where $s_i \in S$, $a_i \in \overline{f}(A_r)$, n a positive integer$\}$ is an ideal in S.

Proof:

Let $x', y' \in S(\overline{f}(A_r))$ such that $x' = \sum_{i=1}^{n} s_i a_i$, $y' = \sum_{j=1}^{m} s'_j b_j$ where $s_i, s'_j \in S$, $a_i, b_j \in \overline{f}(A_r)$, n and m positive integers and $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$. Then $x' \boxplus (-y') = \sum_{i=1}^{n} s_i a_i \boxplus (-\sum_{j=1}^{m} s'_j b_j) = \sum_{i=1}^{n} s_i a_i \boxplus \sum_{i=n+1}^{m+n} s_i a_i$ where $s_{n+j} = -s'_j$ for $j = 1, 2, \ldots, m$, and $b_j = a_{j+n}$. Thus $x' \boxplus (-y') = \sum_{i=1}^{m+n} s_i a_i$. Since $a_i \in \overline{f}(A_r)$, this implies that $\sum_{i=1}^{m+n} s_i a_i \in S\overline{f}(A_r)$ and $x' \boxplus (-y') \in S(\overline{f}(A_r))$.

If $r \in S$, then $rx' = r(\sum_{i=1}^{n} s_i a_i) = \sum_{i=1}^{n} r(s_i a_i) = \sum_{i=1}^{n} (rs_i)a_i$ is the element of $S(\overline{f}(A_r))$.

Therefore $S(\overline{f}(A_r))$ is an ideal in S.

Definition 2-2. If A_s is an ideal in S, the ideal $\overline{f}^{-1}(A_s)$ is called the contracted ideal, denoted by $A_s{}^c$, or the contraction, of A_s in R. If A_r is an ideal in R, the ideal $S\overline{f}(A_r)$ generated by $\overline{f}(A_r)$ in S is called the extended ideal, denoted by $A_r{}^e$, or the extension, of A_r in S.

Theorem 2-3. If $A_s \subset B_s$ then $A_s{}^c \subset B_s{}^c$; and if $A_r \subset B_r$ then $A_r{}^e \subset B_r{}^e$.

Proof:

First, assume $A_s \subset B_s$, and let x be an arbitrary element of $A_s{}^c$. Then $\overline{f}(x) \in A_s \subset B_s$ by definition, hence $x \in B_s{}^c$. Since x is an arbitrary element of $A_s{}^c$, it follows that $A_s{}^c \subset B_s{}^c$.

Now, assume $A_r \subset B_r$, and let $y' \in A_r{}^e$, then $y' = \sum_{i=1}^{n} s_i \overline{f}(a_i)$ for some positive integer n, i = 1, 2, ..., n, $s_i \in S$, $a_i \in A_r$. Since $a_i \in A_r \subset B_r$, this implies $a_i \in B_r$ or $\overline{f}(a_i) \in B_r{}^e$ for each i. Also, $s_i \overline{f}(a_i) \in B_r{}^e$ by definition, hence $y' = \sum_{i=1}^{n} s_i \overline{f}(a_i) \in B_r{}^e$ since $B_r{}^e$ is an ideal in S.

Therefore $A_r{}^e \subset B_r{}^e$.

<u>Theorem 2-4</u>. $(A_s{}^c)^e \subset A_s$; and $A_r \subset (A_r{}^e)^c$.

Proof:

First, let $y' \in (A_s{}^c)^e$, then by definition $y' = \sum_{i=1}^{n} s_i\bar{f}(a_i)$, for some n, $i = 1, 2, \ldots, n$, $s_i \in S$, $a_i \in A_s{}^c$. Since each $a_i \in A_s{}^c$, it follows by theorem 2-1 that $\bar{f}(a_i) \in A_s$. Also $s_i\bar{f}(a_i) \in SA_s = A_s$; hence $y' = \sum_{i=1}^{n} s_i\bar{f}(a_i) \in A_s$ and therefore $(A_s{}^c)^e \subset A_s$.

Now, let $x \in A_r$, then $\bar{f}(x) \in A_r{}^e$ by theorem 2-2. This implies $x \in (A_r{}^e)^c$ by definition 2-2. Therefore $A_r \subset (A_r{}^e)^c$.

<u>Notation</u>.

$A_r{}^{ec}$ means $(A_r{}^e)^c$, and $A_s{}^{ce}$ means $(A_s{}^c)^e$.

$\bar{f}(x^n)$ means $(\bar{f}(x))^n$.

<u>Theorem 2-5</u>. $A_s{}^{cec} = A_s{}^c$; and $A_r{}^{ece} = A_r{}^e$.

Proof:

First, $A_s{}^{ce} \subset A_s$ by theorem 2-4, hence $(A_s{}^{ce})^c \subset A_s{}^c$ by theorem 2-3. Also $A_s{}^c \subset (A_s{}^c)^{ec}$ by theorem 2-4; therefore $A_s{}^{cec} = A_s{}^c$.

Now, $(A_r{}^e)^{ce} \subset A_r{}^e$ by theorem 2-4. Also $A_r \subset A_r{}^{ec}$ by theorem 2-4; therefore $A_r{}^e \subset (A_r{}^{ec})^e$ follows by theorem 2-3. Hence $A_r{}^{ece} = A_r{}^e$.

<u>Theorem 2-6</u>. $A_s{}^c + B_s{}^c \subset (A_s + B_s)^c$, and $(A_r + B_r)^e = A_r{}^e + B_r{}^e$.

Proof:

First, $A_s \subset A_s + B_s$ for A_s and B_s in S; then $A_s{}^c \subset (A_s + B_s)^c$ by theorem 2-3, and $B_s \subset A_s + B_s$ implies $B_s{}^c \subset (A_s + B_s)^c$. Hence $A_s{}^c + B_s{}^c \subset (A_s + B_s)^c$.

Now, $A_r \subset A_r + B_r$ for A_r and B_r in R, then $A_r{}^e \subset (A_r + B_r)^e$ by theorem 2-3, and $B_r \subset A_r + B_r$ implies $B_r{}^e \subset (A_r + B_r)^e$. Hence $A_r{}^e + B_r{}^e \subset (A_r + B_r)^e$. Also, let $y' \in (A_r + B_r)^e$, then by definition, $y' = \sum_{i=1}^{n} s_i \overline{f}(a_i \oplus b_i) = \sum_{i=1}^{n} s_i \overline{f}(a_i) \boxplus \sum_{i=1}^{n} s_i \overline{f}(b_i)$ for n a positive integer, $i = 1, 2, \ldots, n$, $a_i \in A_r$, $b_i \in B_r$, $s_i \in S$. Since $a_i \in A_r$, then $\overline{f}(a_i) \in A_r{}^e$ and $s_i \overline{f}(a_i) \in A_r{}^e$ by theorem 2-1, this implies that $s_i \overline{f}(a_i) \in A_r{}^e + B_r{}^e$. Since $b_i \in B_r$, then $\overline{f}(b_i) \in B_r{}^e$ and $s_i \overline{f}(b_i) \in B_r{}^e$ by theorem 2-1, this implies $s_i \overline{f}(b_i) \in A_r{}^e + B_r{}^e$. Hence
$y' = \sum_{i=1}^{n} s_i \overline{f}(a_i) \boxplus \sum_{i=1}^{n} s_i \overline{f}(b_i) \in A_r{}^e + B_r{}^e$ or
$(A_r + B_r)^e \subset A_r{}^e + B_r{}^e$. Therefore $(A_r + B_r)^e = A_r{}^e + B_r{}^e$.

Theorem 2-7. $(A_s \cap B_s)^c = A_s{}^c \cap B_s{}^c$, and $(A_r \cap B_r)^e \subset A_r{}^e \cap B_r{}^e$.

Proof:

First, $(A_s \cap B_s) \subset A_s$ for A_s and B_s in S, then $(A_s \cap B_s)^c \subset A_s{}^c$ by theorem 2-3, and $(A_s \cap B_s) \subset B_s$ implies $(A_s \cap B_s)^c \subset B_s{}^c$. Hence $(A_s \cap B_s)^c \subset A_s{}^c \cap B_s{}^c$. Let $x \in A_s{}^c \cap B_s{}^c$, then $x \in A_s{}^c$ and $x \in B_s{}^c$. This implies $\overline{f}(x) \in A_s$ and $\overline{f}(x) \in B_s$

by theorem 2-1. Then $\overline{f}(x) \in A_s \cap B_s$ by the definition of intersection. Hence $x \in (A_s \cap B_s)^c$ or $A_s{}^c \cap B_s{}^c \subset (A_s \cap B_s)^c$. Therefore $(A_s \cap B_s)^c = A_s{}^c \cap B_s{}^c$.

Now, $(A_r \cap B_r) \subset A_r$ by the definition of intersection; this implies $(A_r \cap B_r)^e \subset A_r{}^e$. Also $A_r \cap B_r \subset B_r$ implies $(A_r \cap B_r)^e \subset B_r{}^e$. Hence $(A_r \cap B_r)^e \subset A_r{}^e \cap B_r{}^e$.

<u>Theorem</u> <u>2-8</u>. $A_s{}^c B_s{}^c \subset (A_s B_s)^c$, and $(A_r B_r)^e = A_r{}^e B_r{}^e$.

Proof:

First, let z be an arbitrary element of $A_s{}^c B_s{}^c$ where $z = \sum_{i=1}^{n} x_i y_i$ for $x_i \in A_s{}^c$ and $y_i \in B_s{}^c$, $i = 1, 2, \ldots, n$, for some positive integer n. This implies that $\overline{f}(x_i) \in A_s{}^{ce} \subset A_s$ and $\overline{f}(y_i) \in B_s{}^{ce} \subset B_s$ for each $i = 1, 2, \ldots, n$. Then $\overline{f}(x_i)\overline{f}(y_i) = \overline{f}(x_i y_i) \in A_s B_s$ for each $i = 1, 2, \ldots, n$. Therefore $\sum_{i=1}^{n} \overline{f}(x_i y_i) = \overline{f}(\sum_{i=1}^{n} x_i y_i) = \overline{f}(z) \in A_s B_s$. Hence $z \in (A_s B_s)^c$ and $A_s{}^c B_s{}^c \subset (A_s B_s)^c$.

Now, let $z' \in (A_r B_r)^e$. Then $z' = \sum_{i=1}^{k} s_i \overline{f}(c_i)$ where

$$c_i = \sum_{j_i=1}^{n_i} a_{j_i} b_{j_i} \text{ for } a_{j_i} \in A_r,\ b_{j_i} \in B_r,\ s_i \in S,\ i = 1, 2, \ldots, k$$

and $j_i = 1, 2, \ldots, n_i$, for some positive integer k. Hence, $\overline{f}(a_{j_i}) \in A_r{}^e$, $\overline{f}(b_{j_i}) \in B_r{}^e$, and $\overline{f}(a_{j_i})\overline{f}(b_{j_i}) = \overline{f}(a_{j_i} b_{j_i}) \in A_r{}^e B_r{}^e$

for each j_i. Therefore $\sum_{j_i=1}^{n_i} \overline{f}(a_{j_i} b_{j_i}) = \overline{f}(\sum_{j_i=1}^{n_i} a_{j_i} b_{j_i})$

$= \overline{f}(c_i) \in A_r{}^e B_r{}^e$. Since $s_i \in S$, this implies that

$s_i\bar{f}(c_i) \in A_r^e B_r^e$ and $\sum_{i=1}^{k} s_i\bar{f}(c_i) \in A_r^e B_r^e$. Therefore $(A_r B_r)^e \subset A_r^e B_r^e$.

Also, let w' be an arbitrary element of $A_r^e B_r^e$ where $w' = \sum_{i=1}^{k} x'_i y'_i$ for $x'_i \in A_r^e$ and $y'_i \in B_r^e$. Let

$x'_i = \sum_{j_i=1}^{m_i} s_{j_i}\bar{f}(a_{j_i})$ and $y'_i = \sum_{j_i=1}^{n_i} t_{j_i}\bar{f}(b_{j_i})$ for $s_{j_i}, t_{j_i} \in S$, $a_{j_i} \in A_r$ and $b_{j_i} \in B_r$, for some positive integers m_i and n_i.

Then
$$
\begin{aligned}
x'_i y'_i &= \Big(\sum_{j_i=1}^{m_i} s_{j_i}\bar{f}(a_{j_i})\Big)\Big(\sum_{j_i=1}^{n_i} t_{j_i}\bar{f}(b_{j_i})\Big) \\
&= (s_1\bar{f}(a_1))(t_1\bar{f}(b_1)) \boxplus (s_1\bar{f}(a_1))(t_2\bar{f}(b_2)) \boxplus \cdots \\
&\quad \boxplus (s_{m_i}\bar{f}(a_{m_i}))(t_{n_i-1}\bar{f}(b_{n_i-1})) \boxplus (s_{m_i}\bar{f}(a_{m_i}))(t_{n_i}\bar{f}(b_{n_i})) \\
&= s_1 t_1\bar{f}(a_1 b_1) \boxplus s_1 t_2\bar{f}(a_1 b_2) \boxplus \cdots \boxplus \\
&\quad s_{m_i} t_{n_i-1}\bar{f}(a_{m_i} b_{n_i-1}) \boxplus s_{m_i} t_{n_i}\bar{f}(a_{m_i} b_{n_i}).
\end{aligned}
$$

Since $a_1 \in A_r$ and $b_1 \in B_r$, this implies that $a_1 b_1 \in A_r B_r$, and $\bar{f}(a_1 b_1) \in (A_r B_r)^e$. Also, $s_1 t_1 \in S$, hence $s_1 t_1\bar{f}(a_1 b_1) \in (A_r B_r)^e$. Using the same argument, $s_1 t_2\bar{f}(a_1 b_2) \in (A_r B_r)^e$, ..., $s_{m_i} t_{n_i}\bar{f}(a_{m_i} b_{n_i}) \in (A_r B_r)^e$ follows. Since the sum of all these terms is contained in $(A_r B_r)^e$, it follows that $x'_i y'_i \in (A_r B_r)^e$ and $w' = \sum_{i=1}^{k} x'_i y'_i \in (A_r B_r)^e$. Hence $A_r^e B_r^e \subset (A_r B_r)^e$ and therefore $(A_r B_r)^e = A_r^e B_r^e$.

Theorem 2-9. $(A_s : B_s)^c \subset A_s^c : B_s^c$, and $(A_r : B_r)^e \subset A_r^e : B_r^e$.

Proof:

First, since $A_s : B_s = A_s : B_s$, then $(A_s : B_s)B_s \subset A_s$ by the definition of quotient ideal. This implies $((A_s : B_s)B_s)^c \subset A_s^c$ by theorem 2-3, and $(A_s : B_s)^c B_s^c \subset A_s^c$ by theorem 2-8. Hence $(A_s : B_s)^c \subset A_s^c : B_s^c$.

Now, since $(A_r : B_r)B_r \subset A_r$, it follows that $((A_r : B_r)B_r)^e \subset A_r^e$ by theorem 2-3, and $(A_r : B_r)^e B_r^e \subset A_r^e$ by theorem 2-8. Hence $(A_r : B_r)^e \subset A_r^e : B_r^e$.

Theorem 2-10. $(\sqrt{A_s})^c = \sqrt{A_s^c}$, and $(\sqrt{A_r})^e \subset \sqrt{A_r^e}$.

Proof:

If $x \in \sqrt{A_s^c}$, then $x^n \in A_s^c$ for some positive integer n by definition 1-12. Then by definition 2-2, $(\overline{f}(x))^n \in A_s$. By definition 1-12 again, $\overline{f}(x) \in \sqrt{A_s}$, and $x \in (\sqrt{A_s})^c$. Hence $\sqrt{A_s^c} \subset (\sqrt{A_s})^c$. Now if $y \in (\sqrt{A_s})^c$, it follows that $\overline{f}(y) \in \sqrt{A_s}$. This implies $(\overline{f}(y))^n = \overline{f}(y^n) \in A_s$ for some positive integer n, and $y^n \in A_s^c$ by definition 2-2, so $y \in \sqrt{A_s^c}$. Hence $(\sqrt{A_s})^c \subset \sqrt{A_s^c}$ and therefore $(\sqrt{A_s})^c = \sqrt{A_s^c}$.

Now, if $x' \in (\sqrt{A_r})^e$, then $x' = \sum_{i=1}^{k} s_i \overline{f}(a_i)$ for $a_i \in \sqrt{A_r}$, $s_i \in S$, k a positive integer, and $i = 1, 2, \ldots, k$. Since $a_i \in \sqrt{A_r}$, this implies $(a_i)^{n_i} \in A_r$ for some positive integer n_i, for each i. Also $\overline{f}(a_i)^{n_i} = (\overline{f}(a_i))^{n_i}$; thus

$(s_i)^{n_i}\bar{f}(a_i)^{n_i} = (s_i\bar{f}(a_i))^{n_i} \in A_r^e$ for each i. Hence $s_i\bar{f}(a_i) \in \sqrt{A_r^e}$ for each i = 1, 2, ..., k and therefore $x' = \sum_{i=1}^{k} s_i\bar{f}(a_i) \in \sqrt{A_r^e}$ or $(\sqrt{A_r})^e \subset \sqrt{A_r^e}$.

In the comparison between theorems 2-4 and 2-5, the containments in theorem 2-4 become equalities when A_s is an extended ideal and A_r a contracted ideal. However, an ideal in S need not be an extended ideal, and need not be the extension of its contraction; this implies that $A_s^{ce} < A_s$ is possible. Also, an ideal in R need not be a contracted ideal nor need it be the contraction of its extension; hence $A_r^{ec} > A_r$ is possible. Theorem 2-5 implies that if an ideal in S is an extended ideal, it is the extension of its contraction, and that if an ideal in R is a contracted ideal, it is the contraction of its extension. These results are stated in the following theorems.

Notation.

Denote by (C) the set of all ideals in R which are contracted ideals, and by (E) the set of all ideals in S which are extended ideals.

An ideal A_r in (C) means there exists an ideal $A_s \subset S$ such that $A_r = A_s^c$. Likewise an ideal A'_s in (E) means there exists an ideal $A'_r \subset R$ such that $(A'_r)^e = A'_s$.

Theorem 2-11. If A_r is a contracted ideal, then $(A_r{}^e)^c = A_r$.

Proof:

Since $A_r \subset (C)$, then $A_r = A_s{}^c$ for some ideal $A_s \subset S$, hence $A_r{}^{ec} = (A_s{}^c)^{ec} = A_s{}^c$ by theorem 2-5. Therefore $A_r{}^{ec} = A_r$.

Theorem 2-12. If A_s is an extended ideal, then $(A_s{}^c)^e = A_s$.

Proof:

Let $A_s \subset (E)$, then there exists an ideal $A_r \subset R$ such that $A_s = A_r{}^e$, thus $A_s{}^{ce} = (A_r{}^e)^{ce} = A_r{}^e$ by theorem 2-5. Therefore $A_s{}^{ce} = A_s$.

Definition 2-3. Let two sets A and $\bar{A}$ be given. If there exists a mapping of A onto $\bar{A}$ such that each element of $\bar{A}$ appears only once as an image, then the mapping is called biunique, and is referred to as a one-to-one correspondence. In this case there exists an "inverse" mapping which associates with each element b of $\bar{A}$ that element of A which has b as its image. This mapping is denoted by $A \longleftrightarrow \bar{A}$.

Lemma 2-1. The mapping of the set of extended ideals in S onto their respective contracted ideals in R is a one-to-one mapping.

Proof:

Let A_s and B_s be any two ideals in (E), such that A_s is not equal to B_s. Now, if $A_s^c = B_s^c$, then $(A_s^c)^e = (B_s^c)^e$ by theorem 2-5. Hence $A_s = B_s$ by theorem 2-12, but this is a contradiction to the assumption. Therefore this is a one-to-one mapping.

Lemma 2-2. The mapping of the set of contracted ideals in R onto their respective extended ideals in S is a one-to-one mapping.

Proof:

Let A_r and B_r be any two ideals in (C), such that A_r is not equal to B_r. Now, if $A_r^e = B_r^e$, it follows that $(A_r^e)^c = (B_r^e)^c$ by theorem 2-5. Hence $A_r = B_r$ by theorem 2-11, but this is a contradiction to the assumption. Therefore this is a one-to-one mapping.

Theorem 2-13. There exists a one-to-one correspondence between the set of all contracted ideals in R and the set of all extended ideals in S.

Proof:

The proof follows directly from lemma 2-1 and lemma 2-2.

Definition 2-4. Let two sets A and $\bar{A}$ be given. If it is possible to place the two sets into one-to-one correspondence such that the mapping preserves the relations, i.e., if with every element a of A there can be associated an element a' of $\bar{A}$ in a biunique manner so that the relations existing between any elements a, b, ... of A also exist between the associated elements a', b', ... and vice versa, then the two sets are called isomorphic (with respect to the relations in question). The mapping itself is called an isomorphism (1, pp. 24-25).

Lemma 2-3. The set of all contracted ideals in R is closed under ideal quotient formation.

Proof:

Let A_r and B_r denote arbitrary contracted ideals in R. Then $A_r = A_r^{ec}$ and $B_r = B_r^{ec}$. Let $A_r^e = A_s$ and $B_r^e = B_s$, then $(A_s : B_s)^c \subset A_s^c : B_s^c$ by theorem 2-9. Also, $(A_s^c : B_s^c)^e B_s = (A_s^c : B_s^c)^e B_s^{ce}$ by theorem 2-12 since B_s is an extended ideal. Then $(A_s^c : B_s^c)^e B_s = ((A_s^c : B_s^c)B_s^c)^e \subset A_s^{ce} = A_s$. From $(A_s^c : B_s^c)^e B_s \subset A_s$ follows $(A_s^c : B_s^c)^e \subset A_s : B_s$ by the definition of a quotient ideal; this implies $(A_s^c : B_s^c)^{ec} \subset (A_s : B_s)^c$ by theorem 2-3, and $(A_s^c : B_s^c) \subset (A_s^c : B_s^c)^{ec}$ by theorem 2-4. Hence $(A_s^c : B_s^c) \subset (A_s : B_s)^c$. Therefore $A_s^c : B_s^c = (A_s : B_s)^c$.

Let $\overline{f}$ denote a homomorphic mapping of a ring R into a ring S such that the identity of S is the image of the identity of R. Consider the set of contracted ideals in R and the set of extended ideals in S where the contractions and extensions are performed with respect to the function $\overline{f}$. Let ϕ denote the one-to-one correspondence between the set of contracted ideals in R and the set of extended ideals in S. The following results are then valid.

Theorem 2-14. If (C) is closed with respect to addition, then the sum of two contracted ideals is the contraction of the extension of their sum and the sets (C) and (E) are isomorphic with respect to addition.

Proof:

Let A_r, B_r be elements of (C). Since $(A_r + B_r)$ is in (C), there exists an ideal $D_s \in (E)$ such that $D_s{}^c = A_r + B_r$. Then $A_r + B_r = D_s{}^c = (D_s{}^c)^{ec} = (A_r + B_r)^{ec}$ by theorem 2-5.

Since $\phi(A_r) = A_r{}^e$ and $\phi(B_r) = B_r{}^e$ by lemma 2-2, then $\phi(A_r + B_r) = (A_r + B_r)^e = A_r{}^e + B_r{}^e = \phi(A_r) + \phi(B_r)$ by theorem 2-6. Therefore (C) and (E) are isomorphic with respect to addition.

Theorem 2-15. If (E) is closed with respect to the operation of intersection, then the intersection of two extended ideals is the extension of the contraction of their intersection and the sets (C) and (E) are isomorphic with respect to the operation of intersection.

Proof:

Let A_s, B_s be ideals of (E). Since $A_s \cap B_s \in (E)$, there exists an ideal $D_r \in (C)$ such that $D_r{}^e = A_s \cap B_s$. Then $A_s \cap B_s = D_r{}^e = (D_r{}^e)^{ce} = (A_s \cap B_s)^{ce}$ by theorem 2-5.

Since $\phi^{-1}(A_s) = A_s{}^c$ and $\phi^{-1}(B_s) = B_s{}^c$ by lemma 2-1, then $\emptyset^{-1}(A_s \cap B_s) = (A_s \cap B_s)^c = A_s{}^c \cap B_s{}^c = \emptyset^{-1}(A_s) \cap \emptyset^{-1}(B_s)$ by theorem 2-7. Hence (C) and (E) are isomorphic with respect to the operation of intersection.

<u>Theorem</u> <u>2-16</u>. If (C) is closed with respect to the operation of multiplication, then the product of two contracted ideals is the contraction of the extension of their product and the sets (C) and (E) are isomorphic with respect to the operation of multiplication.

Proof:

Let A_r, B_r be ideals of (C). Since $A_rB_r \in (C)$, there exists an ideal $D_s \in (E)$ such that $D_s{}^c = A_rB_r$. Then $A_rB_r = D_s{}^c = (D_s{}^c)^{ec} = (A_rB_r)^{ec}$ by theorem 2-5.

Now, since $\emptyset(A_r) = A_r{}^e$ and $\emptyset(B_r) = B_r{}^e$ by lemma 2-2, then $\emptyset(A_rB_r) = (A_rB_r)^e = A_r{}^eB_r{}^e = \emptyset(A_r)\emptyset(B_r)$ by theorem 2-8. Hence (C) and (E) are isomorphic with respect to the operation of multiplication.

<u>Theorem</u> <u>2-17</u>. If (E) is closed with respect to the operation of quotient formation, then the quotient of two extended ideals is the extension of the contraction of their quotient formation and the sets (C) and (E) are isomorphic with respect to the operation of quotient formation.

Proof:

Let A_s, B_s be ideals of (E). Since $(A_s : B_s) \in (E)$, there exists an ideal $D_r \in (C)$ such that $D_r{}^e = A_s : B_s$.

Then $(A_s : B_s) = D_r{}^e = (D_r{}^e)^{ce} = (A_s : B_s)^{ce}$ by theorem 2-5.

Since $\phi^{-1}(A_s) = A_s{}^c$ and $\phi^{-1}(B_s) = B_s{}^c$ by lemma 2-1, then $\phi^{-1}(A_s : B_s) = (A_s : B_s)^c = A_s{}^c : B_s{}^c = \phi^{-1}(A_s) : \phi^{-1}(B_s)$ by lemma 2-3. Hence (C) and (E) are isomorphic with respect to ideal quotient formation.

Theorem 2-18. If (E) is closed with respect to the operation of radical formation, then the radical of an extended ideal is the extension of the contraction of its radical formation and the sets (C) and (E) are isomorphic with respect to the operation of radical formation.

Proof:

Let A_s be an ideal of (E). Since $\sqrt{A_s} \in (E)$, there exists an ideal $D_r \in (C)$ such that $D_r{}^e = \sqrt{A_s}$. Then $D_r{}^{ec} = (\sqrt{A_s})^c$ by theorem 2-5, and $D_r = D_r{}^{ec} = (\sqrt{A_s})^c = \sqrt{A_s{}^c}$ by theorem 2-11 and theorem 2-10. Hence $\sqrt{A_s} = D_r{}^e = (\sqrt{A_s{}^c})^e = (\sqrt{A_s})^{ce}$.

The sets (C) and (E) are isomorphic with respect to radical formation since $\phi^{-1}(\sqrt{A_s}) = (\sqrt{A_s})^c = \sqrt{A_s{}^c} = \sqrt{\phi^{-1}(A_s)}$.

Theorem 2-19. If P_s is a prime ideal in S and Q_s an ideal in S which is primary for P_s, then $P_s{}^c$ is prime and $Q_s{}^c$ primary for $P_s{}^c$ in R.

Proof:

Suppose a, $b \in R$ such that $ab \in P_s{}^c$ and $a \notin P_s{}^c$. This implies that $\bar{f}(ab) \in P_s{}^{ce} \subset P_s$ or $\bar{f}(a)\bar{f}(b) \in P_s$, where P_s is a prime ideal. But $\bar{f}(a) \notin P_s$, since otherwise $a \in P_s{}^c$. Hence

$\overline{f}(b) \in P_s$ and $b \in P_s{}^c$. Therefore $P_s{}^c$ is a prime ideal.

Since Q_s is primary for P_s, then $Q_s \subset P_s$, hence $Q_s{}^c \subset P_s{}^c$ by theorem 2-3.

Suppose a, $b \in R$ such that $ab \in Q_s{}^c$ and $a \notin Q_s{}^c$. This implies that $\overline{f}(ab) \in Q_s{}^{ce} \subset Q_s$ or $\overline{f}(a)\overline{f}(b) \in Q_s$, where Q_s is primary for P_s. But $\overline{f}(a) \notin Q_s$ otherwise $a \in Q_s{}^c$. Hence $\overline{f}(b) \in P_s$ and $b \in P_s{}^c$ by theorem 1-8.

If $b \in P_s{}^c$, then $\overline{f}(b) \in P_s{}^{ce} \subset P_s = \sqrt{Q_s}$ by theorem 2-4. Then $(\overline{f}(b))^n = \overline{f}(b^n) \in Q_s$ for some positive integer n. Therefore $b^n \in Q_s{}^c$ and hence $Q_s{}^c$ primary for $P_s{}^c$ by theorem 1-8.

CHAPTER BIBLIOGRAPHY

1. Van der Waerden, B. L., Modern Algebra, Volume I, translated by Fred Blum, New York, Frederick Ungar Publishing Company, 1950.

2. Zariski, Oscar and Pierre Samuel, Commutative Algebra, Volume I, Princeton, N. J., D. Van Nostrand Company, Inc., 1958.

CHAPTER III

RELATIONS BETWEEN IDEALS IN INTEGRAL DOMAINS D AND D_M

Definition 3-1. A commutative ring R with more than one element and having a unity is called an integral domain if the following additional property holds.

If $r, s \in R$ such that $rs = 0$, then $r = 0$, or $s = 0$ (3, p. 36).

Definition 3-2. A nonempty set F is a field if F is a commutative ring with unity, having the property that every non-zero element in F has a multiplicative inverse. (i.e., If e is the unit, there exists a^{-1} for each non-zero a in F such that $a \odot a^{-1} = e$.)

Definition 3-3. The set of all elements of a ring R which map into the zero of a ring S under a homomorphism $\overline{F}$ is called the kernel of the homomorphism. The kernel is denoted by N.

Definition 3-4. A multiplicative system (abbreviation m.s.) in an integral domain D is a nonempty subset M of D which does not contain the zero of D and which is closed under multiplication--that is, if $m_1 \in M$, $m_2 \in M$, then $m_1 m_2 \in M$.

The set of all quotients a/m, where $a \in D$, $m \in M$, is a subring of the field F containing the domain D. It will be denoted by D_M and will be called the quotient ring of D with respect to the multiplicative system M. There are two extreme cases.

(1) If D is the set of all units in D, then $D_M = D$.

(2) If M is the set of all non-zero elements of D, then $D_M = F$.

The following theorem (4, pp. 221-222) is quoted without proof for the case of an integral domain D.

Theorem 3-1. Let D denote an integral domain and M a multiplicative system in D. There exists a homomorphism $\bar{h}$ of D into D_M such that

(a) The kernel N of $\bar{h}$ is the zero element in D.

(b) The elements of $\bar{h}(M)$ are units in D_M.

(c) Every element of D_M may be written as a quotient $\bar{h}(x)/\bar{h}(m)$ for some $x \in R$ and $m \in M$.

This homomorphism is called the canonical or natural mapping of D into D_M and will be used throughout the remainder of this chapter when refering to a homomorphism of D into D_M.

Definition 3-5. An element x of a ring R is said to be prime to an ideal A_r of R if $(A_r : (x)) = A_r$ (that is, if its residue class modulo A_r is not a zero divisor in R/A_r).

A subset G of R is said to be prime to A_r if each one of its elements is prime to A_r.

Theorem 3-2. Let M be a multiplicative system in an integral domain D, and let D_M be the quotient ring of D with respect to M. If A_r is an ideal in D, then A_r^{ec} consists of all elements b in D such that $bm \in A_r$ for some m in M.

Proof:

Let $J = \{x \mid x \in D,\ xm \in A_r \text{ for some } m \in M\}$. An arbitrary element b of A_r^{ec} is such that $\overline{h}(b) \in A_r^{e}$, and by property (c) of theorem 3-1, an element of A_r^{e} may be written in the form $\sum_{i=1}^{k}((\overline{h}(x_i)/\overline{h}(m_i))\overline{h}(a_i)$, $x_i \in D$, $m_i \in M$, $a_i \in A_r$, and k a positive integer. Since M is closed under multiplication, the elements of A_r^{e} may be reduced to the form $\overline{h}(a)/\overline{h}(m)$ for $a \in A_r$, $m \in M$. Thus $b \in A_r^{ec}$ implies $\overline{h}(b) = \overline{h}(a)/\overline{h}(m)$ for some $a \in A_r$, $m \in M$. This implies $\overline{h}(b)\overline{h}(m) = \overline{h}(a)$ or $\overline{h}(bm) = \overline{h}(a)$. Thus $\overline{h}(bm \oplus (-a))$ is the zero in D_M, and therefore $bm \oplus (-a) \in N$. From property (a) of theorem 3-1, it follows that $bm = a \in A_r$, hence $b \in J$ and $A_r^{ec} \subset J$.

Now suppose $b \in J$. There exists an element m in M such that $bm \in A_r$, hence $\overline{h}(b)\overline{h}(m) \in \overline{h}(A_r)$. Then $\overline{h}(b) \in A_r^{e}$ since $\overline{h}(m)$ is a unit in D_M by property (b) of theorem 3-1. Therefore $b \in A_r^{ec}$ implies $J \subset A_r^{ec}$.

The equality $A_r^{ec} = J$ follows from these containments.

Theorem 3-3. Let M be a multiplicative system in an integral domain D, and let D_M be the quotient ring of D with respect to M. Then an ideal A_r in D is a contracted ideal (that is, $A_r = A_r^{ec}$) if and only if M is prime to A_r.

Proof:

First, $A_r \subset A_r^{ec}$ by theorem 2-4. Assume M is prime to A_r and let $b \in A_r^{ec}$, then $bm \in A_r$ for some m in M by theorem 3-2. By the definition of M is prime to A_r, $bm \in A_r$ implies that $b \in A_r$. Hence $A_r^{ec} \subset A_r$. Therefore $A_r = A_r^{ec}$.

Conversely, suppose $A_r = A_r^{ec}$ and let m be any element of M and $x \in D$ such that $x \in A_r : (m)$, this implies that $xm \in A_r$. Then $\overline{h}(xm) \in A_r^e$, whence $\overline{h}(x)\overline{h}(m) \in A_r^e$. By property (b) of theorem 3-1, $\overline{h}(m)$ is a unit, hence $\overline{h}(x) \in A_r^e$, this implies $x \in A_r^{ec}$. Since $A_r = A_r^{ec}$, this implies that $x \in A_r$, and therefore $(A_r : (m)) \subset A_r$. The containment $A_r \subset A_r : (m)$ is valid for any $m \in D$, hence $A_r = A_r : (m)$. Therefore M is prime to A_r since m is arbitrary element of M.

Theorem 3-4. Let M be a multiplicative system in an integral domain D, and let D_M be the quotient ring of D with respect to M; then every ideal in D_M is an extended ideal.

Proof:

Let A_s be any ideal in D_M, and let x' be an arbitrary element of A_s. Then $x' = \overline{h}(x)/\overline{h}(m)$ for some $x \in D$, $m \in M$, thus $\overline{h}(x) \in A_s$ implies that $x \in A_s^c$. Now $\overline{h}(x) \in A_s^{ce}$ implies $x' = \overline{h}(x) \boxdot e'/\overline{h}(m)$ in A_s^{ce} where e' denotes the multiplicative identity in D_M, hence $A_s \subset A_s^{ce}$. Also $A_s^{ce} \subset A_s$ by theorem 2-4, whence $A_s = A_s^{ce}$ and every ideal in D_M is an extended ideal.

Theorem 3-5. Let M be a multiplicative system in an integral domain D, and let D_M be the quotient ring of D with respect to M. Then the mapping $A_r \longrightarrow A_r^e$ is a one-to-one mapping of the set of contracted ideals in D onto the set of all ideals in D_M, and this mapping is an isomorphism with respect to the ideal theoretic operations of forming intersections, quotients, and radicals.

Proof:

Since every ideal in D_M is an extended ideal by the previous theorem, it follows from theorem 2-13 that the mapping $A_r \longrightarrow A_r^e$, of the set of contracted ideals in D into the set of ideals in D_M is a one-to-one onto mapping. This mapping is an isomorphism with respect to the ideal theoretic operations of forming intersections, quotients, and radicals by theorem 2-15, theorem 2-17, and theorem 2-18, respectively.

Theorem 3-6. Let Q_r be a primary ideal of an integral domain D disjoint from a multiplicative system M, and let P_r be its (prime) radical. Then P_r is disjoint from M, and P_r and Q_r are contracted ideals with respect to D_M.

Proof:

Suppose $x \in D$ such that $x \in P_r$ and $x \in M$. Then there exists a positive integer n such that $x^n \in Q_r$ since Q_r is primary for P_r. Since x is an element of M, then any power of x belongs to M, in particular $x^n \in M$. This contradicts the disjointness of Q_r and M. Therefore P_r and M have no elements in common; hence P_r is disjoint from M.

Let m be any element of M and $x \in D$ such that $x \in P_r : (m)$, then $xm \in P_r$. Since P_r is disjoint from M, $x \in P_r$ by the definition of a prime ideal. Hence $P_r : (m) \subset P_r$. The containment $P_r \subset (P_r : (m))$ is valid for any m in D, hence $P_r = P_r : (m)$. Since m is an arbitrary element of M, then P_r is prime to M and hence P_r is a contracted ideal by theorem 3-3.

Let m be any element of M and $x \in D$ such that $x \in Q_r : (m)$, then $xm \in Q_r$. Since $m \notin P_r$, then $x \in Q_r$ by theorem 1-8. Hence $Q_r : (m) \subset Q_r$. The containment $Q_r \subset (Q_r : (m))$ is valid for any $m \in D$, hence $Q_r = Q_r : (m)$. Since m is an arbitrary element of M, then Q_r is prime to M and hence Q_r is a contracted ideal by theorem 3-3.

<u>Theorem 3-7</u>. Let Q_r be a primary ideal of an integral domain D disjoint from a multiplicative system M, and let P_r be its prime radical. Then Q_r^e is a primary ideal and P_r^e is its associated prime in D_M.

Proof:

Let x' and y' be elements of D_M such that $x' \notin P_r^e$ and $x'y' \in P_r^e$, by property (c) of theorem 3-1, it follows that

$x' = \overline{h}(x)/\overline{h}(m)$ for $x \in D$, $x \notin P_r$, $m \in M$, $y' = \overline{h}(y)/\overline{h}(m')$ for $y \in D$, $m' \in M$, and $x'y' = \overline{h}(z)/\overline{h}(m'')$ for $z \in P_r$ and $m'' \in M$. By substitution $\dfrac{\overline{h}(x)}{\overline{h}(m)} \boxdot \dfrac{\overline{h}(y)}{\overline{h}(m')} = \dfrac{\overline{h}(z)}{\overline{h}(m'')}$, hence $\overline{h}(xym'' \oplus (-mm'z))$ is the zero element of D_M. Therefore $(xym'' \oplus (-mm'z)) \in N$, hence $xym'' = mm'z$ by property (a) of theorem 3-1. Now $xym'' \in P_r$ since $z \in P_r$ and thus $x \notin P_r$ implies $ym'' \in P_r$. But $m'' \notin P_r$ since M is disjoint from P_r, whence $y \in P_r$ and $\overline{h}(y) = y' \in {P_r}^e$. Therefore ${P_r}^e$ is a prime ideal.

Let a' and b' be elements of D_M such that $a' \notin {Q_r}^e$ and $a'b' \in {Q_r}^e$. According to property (c) of theorem 3-1, it follows that $a' = \overline{h}(a)/\overline{h}(m)$ for $a \in D$, $a \notin Q_r$, $m \in M$, $b' = \overline{h}(b)/\overline{h}(m')$ for $b \in D$, $m' \in M$, and $a'b' = \overline{h}(c)/\overline{h}(m'')$ for $c \in Q_r$ and $m'' \in M$. It follows that $\overline{h}(abm'' \oplus (-mm'c))$ is the zero element of D_M, hence $abm'' = mm'c$ by property (a) of theorem 3-1. Since $c \in Q_r$ it follows that $abm'' \in Q_r$ and $am'' \notin Q_r$ because $a \notin Q_r$ and $m'' \in M$. Then $b \in P_r$ since Q_r is primary for P_r and $\overline{h}(b) \in {P_r}^e$ by theorem 1-8. Since the elements of $\overline{h}(M)$ are units in D_M, then $b' = \overline{h}(b) \in {P_r}^e$.

Since Q_r is primary for P_r, then $Q_r \subset P_r$, and hence ${Q_r}^e \subset {P_r}^e$ by theorem 2-3.

Let x' be an arbitrary element in ${P_r}^e$. By property (c) of theorem 3-1, ${P_r}^e$ may be written in the form $\left\{ \sum_{i=1}^{k} (\overline{h}(x_i)/\overline{h}(m_i))\overline{h}(p_i) \,\middle|\, x_i \in D,\ m_i \in M,\ p_i \in P_r, \text{ and k a positive integer} \right\}$. Since M is closed under multiplication, the elements of P_r^e may be reduced to the form $\bar{h}(p)/\bar{h}(m)$ for some $p \in P_r$, $m \in M$. Thus $x' = \bar{h}(p)/\bar{h}(m)$. There exists a positive integer n such that $p^n \in Q_r$ since Q_r is primary for P_r. This implies that $\bar{h}(p^n) \in Q_r^e$. Also, since m is an element of M, then any power of m belongs to M, in particular $m^n \in M$. Thus $x'^n = (\bar{h}(p)/\bar{h}(m))^n = \bar{h}(p^n)/\bar{h}(m^n) = \bar{h}(p^n) \boxdot e'/\bar{h}(m^n) \in Q_r^e$ where e' denotes the multiplicative identity in D_M, and hence $x'^n \in Q_r^e$ as desired.

Therefore Q_r^e is primary for P_r^e by theorem 1-8.

Corollary 3-1. The mapping $P_r \longrightarrow P_r^e$ is a one-to-one mapping of the set of all contracted prime ideals in D onto the set of all prime ideals in D_M.

Proof:

Every ideal in D_M is an extended ideal by theorem 3-4. In particular, every prime ideal in D_M is an extended prime ideal by the previous theorem. Also, the contraction of a prime ideal is a prime ideal by theorem 2-19. Hence it follows from theorem 2-13 that the mapping $P_r \longrightarrow P_r^e$ of the set of contracted prime ideals in D onto the set of prime ideals in D_M is a one-to-one mapping.

Definition 3-6. A ring R is called noetherian if it has an identity and if it satisfies the following equivalent conditions (1), (2), and (3).

(1) Every strictly ascending chain $A_{r_1} < A_{r_2} < \ldots$

of ideals of R is finite. (Ascending chain condition).

(2) In every non-empty family of ideals of R, there exists a maximal element, that is, an ideal not contained in any other ideal of the family. (Maximum condition).

(3) Every ideal A_r of R has a finite basis; this means, that A_r contains a finite set of elements a_1, a_2, ..., a_n such that $A_r = Ra_1 + Ra_2 + \ldots + Ra_n$. (Finite basis condition).

<u>Theorem 3-8</u>. If D is a noetherian domain and M is a multiplicative system in D, then D_M is a noetherian domain.
Proof:

Let $A_{s_1} < A_{s_2} < A_{s_3} < \ldots$ be a strictly ascending chain of ideals in D_M. Since every ideal in D_M is an extended ideal, there exists ideals $A_{r_1} < A_{r_2} < A_{r_3} < \ldots$ such that $(A_{r_i})^e = A_{s_i}$ for $i = 1, 2, 3, \ldots$. Then $(A_{r_1})^{ec} \subset (A_{r_2})^{ec} \subset (A_{r_3})^{ec} \subset \ldots$ by theorem 2-3. In particular, if $(A_{r_i})^e < (A_{r_{i+1}})^e$ then $(A_{r_i})^{ec} < (A_{r_{i+1}})^{ec}$, since $(A_{r_i})^{ec} = (A_{r_{i+1}})^{ec}$ for some i implies $(A_{r_i})^e = (A_{r_i})^{ece}$ $= (A_{r_{i+1}})^{ece} = (A_{r_{i+1}})^e$. Therefore the chain $(A_{r_1})^{ec} < (A_{r_2})^{ec} < (A_{r_3})^{ec} < \ldots$ is a strictly ascending chain of ideals in R, hence must be finite. Thus the chain $(A_{r_1})^e < (A_{r_2})^e < (A_{r_3})^e < \ldots$ must be finite, otherwise an infinite strictly ascending chain of ideals in D is obtained. Therefore D_M is a noetherian ring. Since the kernel of the homomorphism of D into D_M is the zero element of D, it follows that D_M is a domain.

Theorem 3-9. If each ideal with prime radical in a domain D is a prime power, then ideals in D_M with prime radicals are also prime powers.

Proof:

Let A_s be an ideal in D_M. There exists an ideal A_r in D such that $A_r^e = A_s$. Suppose $\sqrt{A_s} = P_s$ is prime, then there exists a prime ideal P_r in D such that $P_r^e = P_s$. In particular, $\sqrt{A_s} = \sqrt{A_r^e}$ implies that $(\sqrt{A_s})^c = (\sqrt{A_r^e})^c = \sqrt{A_r^{ec}}$ by theorem 2-8, and $P_s^c = (\sqrt{A_s})^c = \sqrt{A_r^{ec}}$ is prime by theorem 2-19. Moreover, $(\sqrt{A_s})^c = \sqrt{A_s^c} = \sqrt{A_r^{ec}}$ by theorem 2-10. Since each ideal with prime radical in D is a prime power, there exists a positive integer n such that $(P_s^c)^n = A_s^c = (A_r^e)^c = P_r^n$. This implies that $A_r^e = (A_r^{ec})^e = (P_r^n)^e$ by theorem 2-5 and $A_r^e = (P_r^e)^n$ by theorem 2-6. Therefore $A_s = P_s^n$ as desired, whence ideals in D_M with prime radicals are prime powers.

Definition 3-7. If c is an element of a ring R with identity and A an ideal in R, define
$((c),A) = \left\{\sum_{i=1}^{n} r_i c \oplus \sum_{j=1}^{k} r_j a_j \middle| r_i, r_j \in R,\ a_j \in A,\ n, k \text{ positive integers}\right\}$.

It is easy to see from the definition of an ideal that $((c),A)$ in the above definition is an ideal in R.

Lemma 3-1. If b, c are elements of a ring R with identity and A an ideal in R, then $((b),A)((c),A) \subset ((bc),A)$.
Proof:

Let b, $c \in R$ and A be an ideal in R, then
$((b),A) = \left\{\sum_{i=1}^{n} r_i b \oplus \sum_{j=1}^{k} r_j a_j \middle| r_i,\ r_j \in R,\ a_j \in A,\ n, k \text{ positive integers}\right\}$, and $((c),A) = \left\{\sum_{i=1}^{n'} r'_i c \oplus \sum_{j=1}^{k'} r'_j a'_j \middle| r'_i,\ r'_j \in R,\ a'_j \in A,\ n', k' \text{ positive integers}\right\}$. By definition 1-10, $((b),A)((c),A) = \left\{\sum_{i=1}^{m} x_i y_i \middle| x_i \in ((b),A),\ y_i \in ((c),A),\ m \text{ a positive integer}\right\}$. Let z be an arbitrary element of $((b),A)((c),A)$. Then $z = \sum_{i=1}^{m} x_i y_i$ for $x_i \in ((b),A)$, $y_i \in ((c),A)$ and m a positive integer. Suppose $x_k y_k$ is an arbitrary term in this sum, then $x_k = \sum_{i=1}^{n} r_i b \oplus \sum_{j=1}^{k} r_j a_j$ for r_i, $r_j \in R$, n, k positive integers, and $y_k = \sum_{i=1}^{n'} r'_i c \oplus \sum_{j=1}^{k'} r'_j a'_j$ for r'_i, $r'_j \in R$, n', k' positive integers. Then

$$x_k y_k = \left(\sum_{i=1}^{n} r_i b\right)\left(\sum_{i=1}^{n'} r'_i c\right) \oplus \left(\sum_{j=1}^{k} r_j a_j\right)\left(\sum_{i=1}^{n'} r'_i c\right)$$

$$\oplus \left(\sum_{i=1}^{n} r_i b\right)\left(\sum_{j=1}^{k'} r'_j a'_j\right) \oplus \left(\sum_{j=1}^{k} r_j a_j\right)\left(\sum_{j=1}^{k'} r'_j a'_j\right).$$ It is easy to see that $\left(\sum_{i=1}^{n} r_i b\right)\left(\sum_{i=1}^{n'} r'_i c\right) \in (bc)$ and the other three terms in this sum are elements of A. Hence $x_k y_k \in ((bc),A)$. Since $x_k y_k$ is an arbitrary term in the sum $\sum_{i=1}^{m} x_i y_i$, then every term in this sum is contained in $((bc),A)$. Hence $z = \sum_{i=1}^{m} x_i y_i$ is contained in $((bc),A)$ since $((bc),A)$ is an ideal. Therefore $((b),A)((c),A) \subset ((bc),A)$.

Theorem 3-10. Maximal ideals of an integral domain D are prime.

Proof:

Let M be a maximal ideal in D and suppose $b \notin M$, $c \notin M$, and $bc \in M$. Then the ideals $((b),M)$ and $((c),M)$ each contain M properly and since M is maximal, this implies that $((b),M) = D$, and $((c),M) = D$. Hence $((b),M)((c),M) = DD = D$. Since $bc \in M$, then $((bc),M) \subset M$. Hence $D = ((b),M)((c),M) \subset ((bc),M) \subset M$ is a contradiction to the assumption that M is a maximal ideal. Therefore if $bc \in M$, either $b \in M$ or $c \in M$, whence M is a prime ideal.

Definition 3-8. A ring R is said to be a Dedekind domain if it is an integral domain and if every ideal in R is a product of prime ideals (4, p. 270).

Notation. If J is an integral domain and P is a prime ideal in J, the set of elements in J and not in P forms a multiplicative system M. In this case the quotient ring J_M is denoted by J_P.

Definition 3-9. An integral domain J will be said to be almost Dedekind if, given any maximal ideal P of J, J_P is a Dedekind domain (2, p. 813).

Theorem 3-11. If J is an almost Dedekind domain, then proper prime ideals of J are maximal.

Proof:

Let M be a maximal ideal in J. Since a maximal ideal in an integral domain is prime, this implies that M^e, the extension of M in J_M, is a prime ideal in J_M by theorem 3-7. Also, by theorem 3-3, $M^{ec} = M \neq J$, hence M^e is a proper prime in J_M, and thus M^e is maximal in J_M since J_M is a Dedekind domain. Suppose $Q \subset M$ is a proper prime ideal in J, then Q^e is a prime ideal in J_M by theorem 3-7. But Q^e is not properly contained in M^e since prime ideals are maximal in J_M. In particular, every prime ideal contained in M is a contracted ideal in J by theorem 3-3, and there is a one-to-one correspondence between prime ideals contained in M and all prime ideals in J_M by corollary 3-1. Hence Q in J is not properly contained in M. Since every ideal in a domain J is contained in a maximal ideal (4, p. 151), and each maximal ideal M contains no proper prime ideal except itself, it follows that proper prime ideals in J are maximal.

Theorem 3-12. The powers of a proper ideal in an almost Dedekind domain J intersect in (0) (1, p. 269).

Proof:

Let A be a proper ideal in J and P a maximal ideal in J such that $A \subset P \subset J$. Then $A^e \subset P^e \subset J^e = J_M$ by theorem 2-3. Since J_M is Dedekind domain $\bigcap_{n=1}^{\infty} (P^e)^n =$ (zero ideal in J_M) (4, p. 217). Moreover, $\bigcap_{n=1}^{\infty} (A^e)^n \subset \bigcap_{n=1}^{\infty} (P^e)^n$ implies $\bigcap_{n=1}^{\infty} (A^n)^e = \bigcap_{n=1}^{\infty} (A^e)^n =$ (zero ideal in J_M) by theorem 2-8. Therefore $\bigcap_{n=1}^{\infty} A^n \subset (\bigcap_{n=1}^{\infty} (A^n))^{ec} =$ (zero ideal in $J_M)^c = (0) \subset J$. Hence $\bigcap_{n=1}^{\infty} A^n = (0)$.

Theorem 3-13. Each proper primary ideal of an almost Dedekind domain J is a power of a maximal ideal (2, p. 813).

Proof:

If Q is primary for a maximal ideal P in J, then Q^e is primary for P^e in J_p by theorem 3-7. Since J_p is a Dedekind domain, $Q^e = (P^e)^k = (P^k)^e$ for some positive integer k since J_P has only one proper prime ideal. Since Q is primary for P, $Q = Q^{ec}$ by theorem 3-3. But because P is maximal in D, P^k is also primary for P by corollary 3-1. Therefore $P^k = (P^k)^{ec}$ and hence $Q = P^k$.

Corollary 3-2. Each ideal with prime radical of an almost Dedekind domain is a prime power (1, p. 268).

Proof:

The proof follows from the above theorem since prime ideals are maximal in an almost Dedekind domain.

The conditions of either theorem 3-13 or corollary 3-2 are actually necessary and sufficient for a domain to be an almost Dedekind domain.

CHAPTER BIBLIOGRAPHY

1. Butts, H. S. and R. C. Phillips, "Almost Multiplication Rings," *Canadian Journal of Mathematics*, XVII (April, 1965), 267-277.

2. Gilmer, Robert W. Jr., "Integral Domains which Are Almost Dedekind," *Proceedings of the American Mathematical Society*, XV (October, 1964), 813-818.

3. McCoy, Neal H., *Introduction to Modern Algebra*, Boston, Allyn and Bacon, Inc., 1960.

4. Zariski, Oscar and Pierre Samuel, *Commutative Algebra*, Volume I, Princeton, N. J., D. Van Nostrand Company, Inc., 1958.

BIBLIOGRAPHY

Books

McCoy, Neal H., Introduction to Modern Algebra, Boston, Allyn and Bacon, Inc., 1960.

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

Van der Waerden, B. L., Modern Algebra, Volume I, translated by Fred Blum, New York, Frederick Ungar Publishing Company, 1950.

Zariski, Oscar and Pierre Samuel, Commutative Algebra, Volume I, Princeton, N. J., D. Van Nostrand Company, Inc., 1958.

Articles

Butts, H. S. and R. C. Phillips, "Almost Multiplication Rings," Canadian Journal of Mathematics, XVII (April, 1965), 267-277.

Gilmer, Robert W. Jr., "Integral Domains which Are Almost Dedekind," Proceedings of the American Mathematical Society, XV (October, 1964), 813-818.