PRIME IDEALS AND THE PRIME RADICAL

A Thesis

Presented to

the Faculty of the Department of Mathematics

Kansas State Teachers College

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

---

by

Andrew Grant Borden Jr.

December 1964

Approved for the Major Department

Marion P. Emerson

Approved for the Graduate Council

Laurence C. Boylan

This thesis is dedicated to my four children, who always seem to have a hand in my work.

I also wish to thank Dr. Marion P. Emerson for his encouragement and for his helpful suggestions.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

1.1 THE BACKGROUND OF MODERN RING THEORY

The discovery by Gauss, Bolyai and Lobachevski of a consistent non-Euclidean geometry in the first half of the nineteenth century was the first great step in the liberation of mathematics. Since Euclid, geometry had been thought to be merely an attempt to give an accurate description of local two and three dimensional space. The discovery that there could be more than one consistent geometry led to the study of geometry as an abstract structure and forever destroyed the idea that mathematics is the study of absolute truths.

In 1843, William Rowan Hamilton took another great step forward when he created the first non-commutative algebra, the algebra of quaternions. This discovery was to algebra what non-Euclidean geometry was to traditional geometry. It was the first step in the study of abstract algebraic structures. The mathematician was now a creator of new things and not merely an explorer in a realm of fixed and immutable truths.

The motivation for the definition of the structure known as a ring comes from the familiar properties of the system of integers. The deletion of some of the defining properties of the ring of integers yields new algebraic structures which are interesting in their own right, just as the deletion of Euclid's fifth postulate yields new geometries.

The earliest important work on prime ideals and the prime radical in commutative rings was by Krull [3] in 1929. This paper was not published in English, however. The first extensive treatment of these ideas in English was by Jacobson [2] and McCoy [5] in the late 1940's. The first Rigorous Treatment of prime ideals in general rings was in a paper by McCoy [4] in 1949. The subject is treated more recently in Jacobson's <u>Structure of Rings</u> [1] and McCoy's <u>Theory of Rings</u> [6].

1.2 EXAMPLES OF RINGS

The ring of integers will be used most often to illustrate the properties of prime ideals and associated structures in commutative rings with unity. Other useful examples of such rings are the rings of polynomials over a field. These rings, designated by $F[x]$, consist of all polynomials $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ where a_i is an element of the specified field F, x is an indeterminate and n is the degree of the polynomial. If $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$, addition is defined as : $f(x) + g(x) =$

$= \sum_{i=0}^{k} (a_i + b_i)x^i$ where k is the maximum of m and n. Multiplication is defined as $f(x)g(x) = \sum_{k=0}^{m+n} (\sum_{i=0}^{k} a_i b_k)x^k$. The unity of this ring is the unity of the field. This ring is an integral domain.

The following eight matrices over the field of integers modulo 2 form an interesting example of a finite non-commutative ring with a unity:

$$0=\begin{bmatrix}0&0\\0&0\end{bmatrix}\quad 1=\begin{bmatrix}1&0\\0&1\end{bmatrix}\quad 2=\begin{bmatrix}0&1\\1&0\end{bmatrix}\quad 3=\begin{bmatrix}1&1\\0&0\end{bmatrix}\quad 4=\begin{bmatrix}1&0\\1&0\end{bmatrix}\quad 5=\begin{bmatrix}0&1\\0&1\end{bmatrix}$$

$$6=\begin{bmatrix}0&0\\1&1\end{bmatrix}\quad 7=\begin{bmatrix}1&1\\1&1\end{bmatrix}$$

The matrices $\begin{bmatrix}0&0\\0&0\end{bmatrix}$ and $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ are the zero and the unity of the ring respectively and will be called '0' and '1'. The other elements of the ring have been named 2,3,4,5,6,7 for convenience. Addition and multiplication in this ring are ordinary matrix addition and multiplication. Each element is its own additive inverse and some, but not all, elements have multiplicative inverses and there are proper divisors of zero. This ring illustrates most of the important properties of prime ideals in non-commutative rings very well. This ring will be referred to as 'M_2' and the addition tables are presented in Tables I and II respectively.

1.3 ORGANIZATION OF THE THESIS

Chapter II of this thesis will include a definition and discussion of principal and maximal ideals with examples

TABLE I

ADDITION TABLE FOR THE RING 'M_2'

0	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	7	5	6	3	4	2
2	2	7	0	4	3	6	5	1
3	3	5	4	0	2	1	7	6
4	4	6	3	2	0	7	1	5
5	5	3	6	1	7	0	2	4
6	6	4	5	7	1	2	0	3
7	7	2	1	6	5	4	3	0

TABLE II

MULTIPLICATION TABLE FOR THE RING 'M_2'

0	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	1	6	4	5	3	7
3	0	3	3	3	0	0	3	0
4	0	4	5	7	4	5	0	7
5	0	5	4	0	4	5	7	7
6	0	6	6	6	0	0	6	0
7	0	7	7	7	0	0	7	0

taken from the three rings mentioned above. Ideal products and residue class rings are discussed in Chapter III. The main topic of the thesis, prime ideals, will be introduced in Chapter IV. The most important part of this chapter will be a thorough proof of a theorem by McCoy on the five equivalent conditions for an ideal in a ring to be prime. An attempt will be made to illustrate all the important ideas by reference to appropriate examples. Chapter V will contain a development of the important theorems concerning m-systems and the prime radical. In Chapter VI, the results on prime ideals in arbitrary rings will be extended to complete matrix rings. Zorn's Lemma, which is tacitly assumed in some of the proofs, will be discussed in Chapter VII.

1.4 DEFINITION OF IDEAL

Definition 1.1 A subset of the elements of a ring is called a <u>right</u> (<u>left</u>) <u>ideal</u> if, and only if, it is closed under subtraction and closed under multiplication by elements of the ring from the right (left).

Definition 1.2 A subset of the elements of a ring is called an <u>ideal</u> if, and only if, it is closed under subtraction and closed under multiplication by elements of the ring from the right and from the left.

CHAPTER II

PRINCIPAL AND MAXIMAL IDEALS

2.1 PRINCIPAL RIGHT IDEALS

An ideal in a non-commutative ring may be a right ideal without being a left ideal, i.e. it may be closed under multiplication by elements of the ring from the right and not from the left. Ideals in commutative rings are necessarily two-sided. In this paper, 'ideal' will mean two-sided ideal. All the results concerning right ideals apply equally to left ideals.

A principal right ideal is an ideal generated by one element, that is it consists of all multiples of the element and all products of multiplications of the element by elements of the ring from the right. A principal ideal always contains the generating element. The definition of principal right ideal is stated formally as follows:

Definition 2.1 $(a)_r$ is a <u>principal right ideal</u> in a ring R if and only if $(a)_r = \{na + at; n \in I,\ t \in R\}$.

It may be verified from Table II that $\{0,3\}$ is a principal right ideal generated by the element 3 in the non-commutative ring M_2. Another right principal ideal in this ring is $(6)_r = \{0,6\}$. The left principal ideals are $(4)_l$ and $(5)_l$ and the two-sided ideals are $(7)=\{0,7\}$, $(3)=$

$=\{0,3,6,7\}$ and $(4)=\{0,4,5,7\}$. The two trivial ideals, the zero of the ring and the ring itself, are generated by the zero and the unity of the ring respectively.

If any element of an ideal (right ideal) has an inverse (right inverse), the property of being closed under multiplication with other elements of the ring requires that the ideal also contain the unity of the ring and, hence, the entire ring.

2.2 TWO-SIDED PRINCIPAL IDEALS IN ARBITRARY RINGS

To construct a two-sided principal ideal in an arbitrary ring, the generating element is multiplied by all elements of the ring from the right, from the left, and from both right and left. The following is a formal definition:

Definition 2.2 (a) is a <u>principal</u> <u>ideal</u> in a ring R generated by the element a if and only if:

$$(a)=\{na + s_i a + a t_j + \Sigma s_i a t_j\}$$

where s_i and t_j are elements of the ring and n is an integer. The summation symbol represents an arbitrary finite sum of the products $s_i a t_j$.

If the ring R has a unity, this definition reduces to: $(a)=\{s_i a t_j;\ s_i, t_j \in R\}$.

The integer 2 generates a principal ideal in the ring of integers. In fact, every ideal in this ring has the form

(n) where n is some integer. Rings in which every ideal is principal are called 'principal ideal rings'.

In the ring of polynomials over a field, the set of all polynomials which are multiples of one given polynomial is closed under multiplication by any other polynomial, so this set is an ideal in $F[x]$. McCoy ([5], P. 56) presents a proof that this ring and the ring of integers are principal ideal rings.

2.3 MAXIMAL IDEALS

Definition 2.3 An ideal (right ideal) is a <u>maximal ideal</u> (<u>right ideal</u>) in a ring R if and only if it is not properly contained in any non-trivial ideal (right ideal) in the ring.

Consider the principal ideal (n) in the ring of integers where n is a positive integer. If n is not prime, there exists a decomposition into prime factors:

$$n=p_1p_2p_3\cdots p_r.$$

Every element of (n) is a multiple of n and, therefore, a multiple of p_i, $i=1,2,3,\ldots r$. Thus every element of (n) is an element of every principal ideal (p_i). Each ideal (p_i) contains elements which are not elements of (n) because p_i itself is such an element, so $(n)\subset(p_i)$ for each i and (n) is not a maximal ideal in I when n is composite.

Suppose the integer n is prime and that (n) is properly contained in another ideal A in the ring. If m is an element of A, ($m \notin (n)$) then $an + bm$ is also an element of A for every pair of integers a and b. Since m and n are relatively prime, the unity can be expressed in this manner and must also be contained in A. If the unity is in A, then $A = R$ and (n) is not properly contained in any non-trivial ideal. The following theorem has been established:

Theorem 2.4 In the ring of integers, an ideal is maximal if and only if it generated by a prime integer.

With little modification of the previous proof, it can be shown that the principal ideal generated by a polynomial in $F[x]$ is a maximal ideal if and only if the generating element is an irreducible or prime polynomial over the field.

In the ring M_2, only the ideals (3) and (4) are maximal.

The existence of maximal elements in sets ordered by set inclusion cannot be proved and must be assumed. The formal statement of this assumption is known as Zorn's Lemma. It is logically equivalent to the axiom of choice ([7], p. 245) and it will be used as an axiom in this paper. A more complete discussion of Zorn's Lemma will be given in Chapter VII.

CHAPTER III

RESIDUE CLASS RINGS AND IDEAL SUMS AND PRODUCTS

3.1 CONGRUENCE AND RESIDUE CLASS RINGS

Congruence modulo n is an equivalence relation defined on the integers and this relation partitions the integers into n residue classes. The proof that these residue classes form a ring with the operations of addition and multiplication suitably defined can be found in McCoy. ([6], p. 41) The zero of this ring is the residue class [n]. The elements of this residue class are precisely the same elements as those contained in the principal ideal generated by n. It is convenient, therefore, to consider the ring of integers modulo n to be the ring of integers modulo the ideal (n), denoted I/(n). This ring contains proper divisors of zero if and only if n is composite and it was proved in Chapter II that the principal ideal generated by an element n is maximal when n is prime. The following theorem has been proved:

Theorem 3.1 The principal ideal (n) is maximal if and only if the ring of integers modulo (n) contains no proper divisors of zero.

The ring of polynomials over a field modulo a given polynomial is discussed thoroughly in McCoy ([5], p. 66) and the ring of polynomials modulo a principal ideal, $F[x]/(s(x))$, can be developed in a manner strictly analogous to the way $I/(n)$ was developed above. It is also true that $(s(x))$ is maximal and $F[x]/(s(x))$ has no proper divisors of zero if and only if $s(x)$ is irreducible over the field.

The above results will be used to prove an important theorem concerning proper divisors of zero in commutative rings modulo a prime ideal.

The idea of a ring modulo an ideal is not restricted to rings in which every ideal is principal nor even to commutative rings. If B is a two-sided ideal in an arbitrary ring, an element x is said to be congruent to an element k modulo B if and only if $x - k$ is contained in B. That is, $x \equiv k \bmod B$ if and only if $x = k + b$ where b is some element of B. This relation of congruence is an equivalence relation which partitions the ring into disjoint residue classes. Addition and multiplication are defined as in the ring of integers modulo an ideal and the residue classes form a ring.

3.2 IDEAL PRODUCTS

The definition of prime ideal that will be given in the next chapter involves the product of two ideals:

Definition 3.2 If A and B are ideals in a ring R, the <u>ideal product</u> of A and B is defined as follows:

$AB = \{\sum a_i b_j; a \in A, b \in B\}$.

Since the set of all products $\{a_i b_j; a \in A, b \in B\}$ may not be closed under addition, the definition includes all finite sums of these products.

If A and B are two-sided ideals, they are closed under multiplication by all elements of the ring from the right and left and, therefore, $AB \subseteq A$ and $AB \subseteq B$. If A and B are right ideals, they are closed under multiplication from the right and $AB \subseteq A$, but it is not necessarily true that $AB \subseteq B$.

Suppose B is a right ideal in R. Then B is closed under multiplication by elements of the ring from the right. It is important to show that the ideal product RB is a two-sided ideal in R. (RB)R=R(BR) because multiplication of ideals is associative and R(BR)=RB because B is a right ideal. RB is also a left ideal because R(RB)=(RR)B= =RB so that RB is closed under multiplication by elements of the ring from the left.

It is also true that for any a in R, RaR is a two-sided ideal in R and RaR=(a) if R has a unity. McCoy ([6], p. 31) proves the statements above and also shows that aR is a right ideal in R and Ra is a left ideal in R. The proofs are simple and will not be presented here.

3.3 THE SUM OF TWO IDEALS

Definition 3.3 If A and B are ideals in a ring R, the <u>sum</u> <u>A + B</u> is defined as follows:

$$A + B = \{a + b;\ a \in A,\ b \in B\}.$$

It is easy to prove that the sum of two ideals is an ideal. If a_1 and a_2 are elements of A and b_1 and b_2 are contained in B, then

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$$

and this is contained in the sum A + B so A + B is closed under subtraction. If r is any element of R, then

$$(a + b)r = (ar + br) \text{ and } r(a + b) = (ra + rb)$$

and these are contained in the sum A + B so A + B is closed under multiplication by elements of the ring from the right and left and is an ideal in the ring. The fact that the sum of two right (left) ideals is a right (left) ideal is proved in the same manner.

If M is a maximal ideal in R and A is any ideal not contained in M, then M + A must be the entire ring, because M is certainly contained in M + A.

The results presented in the first three chapters in an informal manner have prepared the way for the definitions and theorems concerning prime ideals in the next chapter.

CHAPTER IV

PRIME AND COMPLETELY PRIME IDEALS

4.1 DEFINITION OF COMPLETELY PRIME IDEAL

Krull's results [3] on rings and ideals are the earliest mention of prime ideals and the prime radical in the literature and these results apply only to commutative rings. The first Formal Discussion of prime ideals in arbitrary rings is in a paper by McCoy in 1949 [4]. McCoy found that the definition of prime ideal given by Krull was too restrictive to be useful in arbitrary rings and he proposed a new definition which would apply to non-commutative rings and which would be equivalent to Krull's definition in the case of commutative rings.

In this paper, ideals which satisfy the more restrictive definition will be called 'completely prime'. The purpose of the present chapter is to define, give examples of and prove some of the basic theorems concerning prime and completely prime ideals.

Definition 4.1 An ideal P in a ring R is <u>completely prime</u> if and only if for any a and b in R such that ab is contained in P, then a is contained in P or b is contained in P.

The reader can recall the discussion in the previous chapter about divisors of zero in residue class rings and verify that Definition 4.1 is equivalent to:

Definition 4.2 An ideal P in a ring R is completely prime if and only if for any a and b contained in R such that $ab \equiv 0 \bmod P$, then $a \equiv 0 \bmod P$ or $b \equiv 0 \bmod P$.

4.2 PROPERTIES OF COMPLETELY PRIME IDEALS

If P is an ideal in an arbitrary commutative ring R, the elements of the zero residue class ring R/P are precisely those contained in P. The residue class ring contains proper divisors of zero if and only if there exist a and b in R such that a and b are not contained in P but ab is contained in P. This fact and Definition 4.1 establish the following theorem:

Theorem 4.3 In an arbitrary commutative ring R, an ideal P is completely prime if the residue class ring R/P has no proper divisors of Zero.

Two corollaries follow directly from Theorem 4.3.

Corollary 4.4 The principal ideal (n) is completely prime in I if and only if n is prime.

The reader will recall the result in Chapter III that I/(n) contains no proper divisors of zero if and only if n is a prime integer.

The analogous result in Chapter III concerning the polynomial ring establishes the following:

Corollary 4.5 The principal ideal $(s(x))$ is completely prime in the ring of polynomials over a field if and only if $s(x)$ is irreducible over the field.

Since ideals in I and $F[x]$ are maximal if and only if the generating element is prime or irreducible, the following is true:

Theorem 4.6 In the ring of Integers and the ring of polynomials over a field, an ideal is completely prime if and only if it is maximal or the entire ring.

Theorem 4.7 In any ring R, the ring itself is always completely prime and the principal ideal generated by the zero element is completely prime if and only if the ring has no proper divisors of zero.

The first part of this theorem is immediate from the definition of completely prime ideal. The zero ideal, denoted (0), consists of the zero of the ring alone. The ring fails to have proper divisors of zero if and only if $ab=0$ implies $a=0$ or $b=0$.

Theorem 4.6 does not apply to commutative rings which do not have a unity. For example, the principal ideal (4) is a maximal ideal in the ring of even integers, but it is not completely prime because the product of any two elements of this ring is a multiple of 4 and, hence, an element of (4).

The following theorem concerns the relationship between completely prime ideals and other ideals in the ring:

Theorem 4.8 If A is an ideal in a ring R and P a completely prime ideal in R, $A \cap P$ is a completely prime ideal in the ring A.

Proof: Let $A \cap P = P'$. If $ab \equiv 0 \mod P'$ for $a, b \in A$, then $ab \equiv 0 \mod P$ and either $a \equiv 0 \mod P$ or $b \equiv 0 \mod P$. Since a and b are contained in A, it follows that either a or b is contained in $A \cap P = P'$, so $a \equiv 0 \mod P'$ or $b \equiv 0 \mod P'$ and P' is a completely prime ideal in the ring A.

As a simple illustration of the above theorem, consider the ideal E of even integers and the completely prime ideal (3) in the ring of integers. $E \cap (3) = (6)$ and the integer 6 is prime in the ring of even integers, so (6) is a completely prime ideal in E.

4.3 DEFINITION OF PRIME IDEAL

The following definition of prime ideal is less restrictive than Definition 4.1 and more useful in the study of non-commutative rings.

Definition 4.9 An ideal P in a ring R is said to be a <u>prime ideal</u> if and only if it has the following property: If A and B are ideals in R such that $AB \subseteq P$, then $A \subseteq P$ or $B \subseteq P$, where AB is the ideal product of A and B.

The reader should keep in mind that prime ideals are always two-sided, even in non-commutative rings.

The following theorem, McCoy's five equivalent properties of prime ideals, is the principal result of this chapter.

Theorem 4.10 If P is an ideal in the ring R, all of the following definitions are equivalent:

i. P is a prime ideal according to definition 4.9.

ii. If a,b are elements of R such that $aRb \subseteq P$, then a is contained in P or b is contained in P.

iii. If (a) and (b) are principal ideals in R such that $(a)(b) \subseteq P$, then a is contained in P or b is contained in P.

iv. If U and V are right ideals in R such that $UV \subseteq P$, then $U \subseteq P$ or $V \subseteq P$.

v. If U and V are left ideals in R such that $UV \subseteq P$, the $U \subseteq P$ or $V \subseteq P$. ([6], p. 62).

Proof: The first step in the proof of this theorem is to assume that the first property holds and prove the second. Suppose a and b are elements of R such that $aRb \subseteq P$ and P is a prime ideal. The set aRb is the set of all ordered triples $\{axb;\ x \in R\}$. It follows that $R(aRb)R \subseteq P$ because P is a two-sided ideal, closed under multiplication by elements of the ring from the right and left. Then $(Ra)R(bR) \subseteq P$ because multiplication is associative and

$(RaR)(RbR) \subseteq P$ because $RR \subseteq R$. It was proved in Chapter III that RaR and RbR are ideals in R. Since P is a prime ideal, either $RaR \subseteq P$ or $RbR \subseteq P$. Suppose $RaR \subseteq P$. Let $A=(a)$. Now $A^3=(a^3) \subseteq RaR \subseteq P$. Since $A^3 \subseteq P$, $AA^2 \subseteq P$ and $A \subseteq P$ because P is a prime ideal. Since a is contained in A, then a is contained in P and the second property is proved. If $RbR \subseteq P$, the proof is the same.

The third property follows directly from the definition, but it can also be proved from the second. It is first necessary to show that $aRb \subseteq (a)(b)$ where $(a)(b)$ is the ideal product of the principal ideals generated by a and b. Every element of aRb has 'a' as a left hand factor and 'b' as a right hand factor. It follows from the definition of principal ideal and the definition of ideal product that every such element is contained in $(a)(b)$. Since $aRb \subseteq P$ implies $a \subseteq P$ or $b \subseteq P$, the third property is proved.

To illustrate the definition and the equivalent properties ii and iii, let E be the prime ideal of even integers in the ring of integers I. If A and B are ideals such that $AB \subseteq E$, it follows that $A \subseteq E$ or $B \subseteq E$, because if A and B each contained an odd integer, their product would contain an odd integer and the condition in the definition would not hold, so E satisfies the definition of prime ideal.

If a and b are integers such that $aIb \subseteq E$, it is immediately evident that either a or b is an even integer so property ii is satisfied.

If $(a)(b) \subseteq E$, then ab is contained in E and either a or b is an even integer, so property iii holds.

The next step in the proof of the five equivalent properties is to prove iv from iii.

Suppose the condition holds in iv and that U is not contained in P. Let u and v be arbitrary elements of U and V respectively with u not an element of P. Since

$$(u) = \{(u)_r + su + \sum s_i u t_i;\ s, t \in R\},$$
$$(u)(v) = \{UV + RUV\} \subset P$$

and property iii implies that v is contained in P. Since v was an arbitrary element of V, then $V \subseteq P$ so property iv is established. The last property is proved in the same manner. The last two properties imply the definition directly, so the equivalence of the five properties of prime ideals is established.

4.4 EXAMPLES OF PRIME IDEALS IN A NON-COMMUTATIVE RING

Properties iv and v are illustrated in the multiplication table of the ideals in M_2 (Table III). Of the three two-sided ideals, only (7) is not prime, because $(4)_1(3) \subseteq (7)$ and neither of the factors is contained in (7). The other two-sided ideals, (4) and (3) satisfy the five parts of the definition. Table IV shows how the ideals

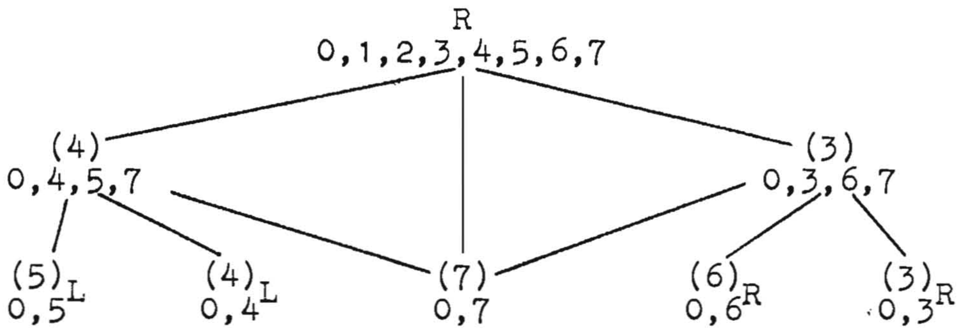
TABLE III

MULTIPLICATION OF IDEALS IN THE RING 'M_2'

	(0)	$(3)_R$	$(6)_R$	$(4)_L$	$(5)_L$	(3)	(4)	(7)
(0)	(0)	(0)	(0)	(0)	(0)	(0)	(0)	(0)
$(3)_R$	(0)	$(3)_R$	$(3)_R$	X	X	$(3)_R$	(0)	(0)
$(6)_R$	(0)	$(6)_R$	$(6)_R$	X	X	$(6)_R$	(0)	(0)
$(4)_L$	(0)	X	X	$(4)_L$	$(5)_L$	(7)	(4)	(7)
$(5)_L$	(0)	X	X	$(4)_L$	$(5)_L$	(7)	(4)	(7)
(3)	(0)	(3)	(3)	(0)	(0)	(3)	(0)	(0)
(4)	(0)	(7)	(7)	$(4)_L$	$(5)_L$	(7)	(4)	(0)
(7)	(0)	(7)	(7)	(0)	(0)	(7)	(0)	(0)

TABLE IV

LATTICE OF IDEALS IN THE RING 'M_2'



in M_2 are partially ordered by set inclusion. This table is useful in verifying that all the properties of prime ideals apply to the prime ideals in this ring. An array like Table IV is called a 'lattice' and will be discussed further in Chapter VII.

4.5 A THEOREM ON PRIME IDEALS

The following theorem is an example of the relationship between prime and maximal ideals in arbitrary rings with a unity:

Theorem 4.11 If a ring R has a unity, every maximal ideal is prime.

Proof: Suppose M is a maximal ideal in a ring R which has a unity and that $AB \subseteq M$ where A and B are ideals in R, but neither A nor B is contained in M. Since M is maximal, $M + A = R$ and $M + B = R$. Since in a ring with unity $R^2 = R$, $(M + A)(M + B) = R$. Then

$$(M^2 + AM + MB + AB) = (M + AB) = R.$$

Since AB is contained in M, $M = R$ and M is not maximal, contrary to hypothesis. Therefore, either $A \subseteq M$ or $B \subseteq M$ and M is a prime ideal.

CHAPTER V

M-SYSTEMS AND THE PRIME RADICAL

5.1 DEFINITION OF MULTIPLICATIVE SYSTEM

Now that the important theorems on prime and completely prime ideals have been discussed, it seems natural to investigate the characteristics of the elements of a ring which are not contained in a prime ideal in the ring, that is, the complement of a prime ideal in a ring. Just as the definition of completely prime ideal is too restrictive to be useful in non-commutative rings, the definition associated with the complement of a completely prime ideal in a ring are too restrictive and must be modified to be useful in non-commutative rings.

Definition 5.1 A set M of elements of a ring R is said to be a <u>multiplicative system</u> if and only if M is closed under multiplication.

5.2 MULTIPLICATIVE SYSTEMS AND COMPLETELY PRIME IDEALS

In the ring of integers, the following subsets are multiplicative systems: the positive integers, odd integers, ideals and the complements of maximal ideals. The first three are obviously closed under multiplication and are, therefore, multiplicative systems. The fact that the complement of every maximal ideal in the ring of integers is a multiplicative system is easily proved. Every maximal ideal in the ring has the form (p) where p is a prime integer. The complement of (p) is denoted C((p)) and contains all and only elements which are not multiples of p. If a and b are elements of C((p)), then p is not a factor of a or b and, since p is prime, p is not a factor of their product ab. Therefore, ab is an element of C((p)) and C((p)) is closed under multiplication and is a multiplicative system. Since it was proved earlier that an ideal in the ring of integers is maximal if and only if it is completely prime, it is also true that the complement of every prime ideal in I is a multiplicative system.

The next theorem generalizes the preceding result to arbitrary commutative rings.

Theorem 5.2 An ideal P in a commutative ring R is completely prime if and only if C(P) is a multiplicative system.

Proof: The proof follows from the definitions of ideal, completely prime ideal and multiplicative system. If P is an ideal in a commutative ring R and a and b are elements of R and either a or b is an element of P, then the product ab is contained in P because P is an ideal. Now suppose there exist a and b in R such that a and b are contained in C(P) and such that ab is an element of P. Then C(P) is not a multiplicative system and P is not a prime ideal. If, on the other hand, for every a and b in

R such that a and b are contained in C(P), ab is contained in C(P), then C(P) is a multiplicative system and P is completely prime by Definition 4.1.

5.3 M-SYSTEMS AND PRIME IDEALS

One more definition is required before proceeding to the main topic of this chapter.

Definition 5.3 A set M of elements in a ring R is an m-system if and only if it has the following property:

If a and b are elements of M, there exists an x in R such that the product axb is contained in M.

It is immediate that every multiplicative system is also an m-system, because if M is a multiplicative system and a and b are elements of M, then x=a or x=b satisfies the requirement that axb is contained in M.

Suppose M is an m-system in a commutative ring R and M=C(A) where A is an ideal in R. It would be useful to know whether M is also a multiplicative system. For every a and b in M, Definition 5.3 requires that there exist an x in the ring such that axb is also contained in M. Since multiplication is commutative, (ab)x is also contained in M. Now ab cannot be an element of A because A is an ideal and (ab)x is not an element of A. It follows that ab is contained in C(A)=M. Since a and b were arbitrary elements of M, then M is closed under multiplication and is a multiplicative system.

Since there can be no distinction between m-systems and multiplicative systems when they are the complements of ideals in commutative rings and since m-systems are so useful in non-commutative rings, multiplicative systems will not be mentioned again in this paper.

If A is a two-sided ideal in a non-commutative ring and if a and b are elements of A, then axb is an element of A for any x in the ring, so every such ideal is an m-system.

Theorem 5.4 An ideal P in a ring R is a prime ideal if and only if C(P) is an m-system.

Proof: The proof of this theorem follows from the first two parts of theorem 4.10. Suppose P is a prime ideal and a and b are elements of C(P). Then axb is an element of C(P) for some x in R by theorem 4.10ii, so C(P) is an m-system. Suppose, on the other hand, that P is an ideal in R but not a prime ideal. Then for some a and b in C(P), $aRb \subseteq P$ (theorem 4.10ii) so $axb \in C(P)$ has no solution for x and C(P) is not an m-system.

5.4 DEFINITION OF PRIME RADICAL

Definition 5.5 The <u>radical</u> of an ideal A in a commutative ring R consists of all elements r of R such that r^n is contained in A for some positive integer n.

Every element of the radical of an ideal is, in a sense, the nth root of an element of the ideal. In non-commutative rings, this definition is too restrictive to be useful and the following is used instead:

Definition 5.6 The prime radical $\mathcal{R}(A)$ of the ideal A in the ring R is the set consisting of those elements r of R with the property that every m-system in R which contains r has a non-empty intersection with A.

5.5 THE PRIME RADICAL IN COMMUTATIVE RINGS

Theorem 5.7 In a commutative ring R, the prime radical of an ideal A coincides with the radical of A.

Proof: If r is an element of the prime radical of an ideal A in the commutative ring R, then by definition, every m-system containing r has non-empty intersection with A. The set $\{r^n; n \text{ is a positive integer}\}$ is certainly an m-system containing r, so there must exist some n such that r^n is contained in A and r is an element of the radical of A. Since r is any element of the prime radical of A, the prime radical is contained in the radical. It remains to be proved that the radical of A is contained in the prime radical of A in the commutative ring R.

Suppose r is an element of the radical of A and that r is contained in any m-system M. This is not an unreasonable assumption because r is contained in at least one m-system by Definition 5.5. By definition of m-system, there exists an x in R such that $rxr=r^2x$ is contained in M. There also exists a y in R such that $(r^2x)y(r)=r^3xy$ is contained in M.

By induction, it follows that for each positive integer n, there exists a t in R such that $r^n t$ is contained in M. Since r is an element of the radical of A, there exists an integer n such that r^n is contained in A. If r^n is contained in A, then $r^n t$ is contained in A because A is an ideal, and M has non-empty intersection with A. Since M is any m-system in R containing r, and r is any element of the radical of A, then every m-system containing r has non-empty intersection with A and the radical of A is contained in the prime radical of A.

Since the prime radical of an ideal is so useful in non-commutative rings, and since the two ideas coincide in commutative rings, prime radicals will be used instead of radicals throughout the remainder of this paper.

5.6 THE PRIME RADICAL IN GENERAL RINGS

In the ring M_2, the sets $\{1,2,3,6\}$, $\{1,2,4,5\}$ and $\{0,7\}$ are m-systems as the reader can quickly verify from Table II. The two-sided ideals $\{0,4,5,7\}$ and $\{0,3,6,7\}$ are also m-systems. In general, any subset of a ring which contains the zero of the ring is an m-system and the complement of every prime ideal in M_2 is an m-system. What, then, is the prime radical of the ideal $(3)=\{0,3,6,7\}$? Clearly, any m-system which contains 0,3,6, or 7 has non-empty intersection with (3), so these elements are contained in $\mathcal{R}((3))$. Consider the elements 1,2,4 and 5.

These are contained in the m-system $\{1,2,4,5\}$ which is disjoint from (3), so none of these elements are contained in $\mathcal{R}(3)$. The prime ideal (3), then, coincides with its prime radical in the ring M_2.

The following theorems extend these results to arbitrary rings:

Theorem 5.8 Every ideal is contained in its prime radical.

Proof: If A is an ideal in the ring R and r is any element of A, then every m-system containing r certainly has non-empty intersection with A, so r is contained in $\mathcal{R}(A)$ by Definition 5.6.

Theorem 5.9 If A is an ideal in the ring R, then the prime radical of A coincides with the intersection of all the prime ideals in R which contain A.

Proof: By theorem 5.8, $A \subseteq \mathcal{R}(A)$, so if any prime ideal contains $\mathcal{R}(A)$, it must contain A.

Suppose P is a prime ideal in R which contains A and a is any element of $\mathcal{R}(A)$. The complement of P is an m-system which does not intersect P and hence, $C(P) \cap A = \emptyset$, so a cannot be contained in C(P). It follows that a is contained in P and $\mathcal{R}(A) \subseteq P$. Since any prime ideal containing A must also contain $\mathcal{R}(A)$, A and its prime radical are contained in exactly the same prime ideals.

It remains to be proved that if some element r is not contained in $\mathcal{R}(A)$, then there exists a prime ideal P containing A such that r is not contained in P.

If r is not an element of $\mathcal{R}(A)$, then there exists an m-system M containing r which is disjoint from A. Define a set of ideals in R as follows:

$$\{K; K \text{ is an ideal in } R,\ A \subseteq K,\ K \cap M = \emptyset$$

where M is the m-system disjoint from A. This set is not empty because A is in the set. It is necessary to use Zorn's Lemma to establish that there is a maximal ideal P in this set. If the ideal P is prime, the proof of this theorem is complete. The proof that this ideal must be prime follows:

Suppose P is not a prime ideal and $(a)(b) \subseteq P$, but a and b are not elements of P (contrary to Theorem 4.10ii). Then P is properly contained in the ideal P + (a). Since P is maximal in C(M), then P + (a) contains an element m_1 which is also an element of M. Similarly, P + (b) contains an element m_2 which is also contained in M. Now M is an m-system so there exists an x in M such that $m_1 x m_2$ is contained in M, but $m_1 x m_2$ is also in the ideal (P + (a))(P + (b). If $(a)(b) \subseteq P$ as the hypothesis states, then

$$(P + (a))(P + (b)) \subseteq P$$

and $m_1 x m_2$ is contained in P, but this is impossible because $M \cap P = \emptyset$. It follows that P is a prime ideal and the theorem is proved.

An immediate consequence of this theorem is that a prime ideal coincides with its prime radical since a prime ideal is clearly the intersection of all the ideals which contain it.

CHAPTER VI

COMPLETE MATRIX RINGS

6.1 DEFINITION OF COMPLETE MATRIX RING

For simplicity, the only example of non-commutative rings used in this paper has been our ring M_2 which is a subset of the complete matrix ring of two by two matrices with elements taken from the ring of integers modulo two.

Definition 6.1 A <u>complete</u> <u>matrix</u> <u>ring</u> R_n is the set of all n by n matrices with elements taken from a ring R.

These matrices are designated $[a_{ij}]$ where the a_{ij}'s are the scalar elements taken from the ring R. It is easily verified that these elements form a ring with addition and multiplication defined as ordinary matrix addition and multiplication. The purpose of this chapter is to present some results about prime ideals in complete matrix rings.

6.2 IDEALS IN COMPLETE MATRIX RINGS

Consider the set of n by n matrices with elements taken from an ideal A in a ring R. These matrices are certainly closed under subtraction and under multiplication by the other matrices in the complete matrix ring R_n from the right and left. They form an ideal in the ring R_n. McCoy proves that if the ring R has a unity, these are the only ideals in R_n ([6], p. 37).

6.3 PRIME IDEALS IN COMPLETE MATRIX RINGS

Results analogous to McCoy's theorems on ideals in complete matrix rings can be stated for prime ideals in these rings.

Theorem 6.2 If P is a prime ideal in a ring R, which has a unity, the complete matrix ring P_n is a prime ideal in the complete matrix ring R_n.

Proof: Let P be a prime ideal in the ring R. The complete matrix ring P_n is an ideal in the complete matrix ring R_n. Let A_n and B_n be ideals in R_n such that

$$A_nB_n \subseteq P_n.$$

P_n is a prime ideal if and only if $A_n \subseteq P_n$ or $B_n \subseteq P_n$ by Definition 4.9 of prime ideal.

Every matrix in the complete matrix ring A_n has the form $[a_{ij}]$ where the a_{ij}'s are elements of an ideal A in R. Similarly, every matrix in B_n has the form $[b_{ij}]$ where the b_{ij}'s come from an ideal B in R. Every matrix in the ideal product A_nB_n has the form $\left[\sum_{j=1}^{n} a_{ij}b_{jk}\right]$. Since $A_nB_n \subseteq P_n$, all matrices with elements from the set $\{\sum ab; a \in A, b \in B\}$ are contained in P_n, but these elements are precisely those of the ideal product AB. Then $AB \subseteq P$ and $A \subseteq P$ or $B \subseteq P$ because P is a prime ideal in R. It follows from Definition 6.1 that $A_n \subseteq P_n$ or $B_n \subseteq P_n$.

Theorem 6.3 If the ring R has a unity, every prime ideal in the complete matrix ring R_n is of the form P_n where P is a prime ideal in R.

Proof: Suppose P_n is a prime ideal in R_n. Since P_n is an ideal in R_n, P is an ideal in R. It must be proved that P is a prime ideal in R. Suppose A and B are ideals in R such that $AB \subseteq P$. It was shown in the proof of the previous theorem that this is equivalent to the condition that $A_n B_n \subseteq P_n$. Since P_n is a prime ideal in R_n, $A_n \subseteq P_n$ or $B_n \subseteq P_n$. It follows from the definition of complete matrix ring that $A \subseteq P$ or $B \subseteq P$ so P is a prime ideal in R and the theorem is proved.

Complete matrix rings are good examples of rings which have prime ideals but no completely prime ideals.

Theorem 6.4 The complete matrix ring R_n has no non-trivial completely prime ideals if the ring R has a unity.

Proof: Since every ideal in R_n has the form M_n where M is an ideal in R, it is sufficient for the proof of this theorem to show that in every such ideal M_n there exists at least one matrix that can be factored into two matrices, neither of which could possibly be contained in M_n. The following is such an example:

$$\begin{bmatrix} a & 0 & \cdots & 0 \\ 0 & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & 0 \\ 0 & \cdots & 0 & I \end{bmatrix} \cdot \begin{bmatrix} I & 0 & \cdots & 0 \\ 0 & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & 0 \\ 0 & \cdots & 0 & a \end{bmatrix} = \begin{bmatrix} a & 0 & \cdots & 0 \\ 0 & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & 0 \\ 0 & \cdots & 0 & a \end{bmatrix}$$

In the above product, a is any element of an ideal M in R, and I is the unity of the ring R. The product is contained in the ideal M_n in R_n, but neither of the factors could be contained in any non-trivial ideal whatsoever because the unity of R is in each one. Since M_n is any ideal in R_n and a is any element in M, every ideal in R_n has at least one element which can be factored in this way, so there are no completely prime ideals in R_n.

CHAPTER VII

ZORN'S LEMMA

7.1 PARTIALLY ORDERED SETS

Zorn's Lemma, or the maximum principle, was used to prove the existence of a maximal ideal in the discussion of Theorem 5.9. The purpose of this chapter is to explain and justify its use. Some preliminary definitions are required.

Definition 7.1 A set S is <u>partially</u> <u>ordered</u> by the binary relation F if and only if:

i. For any x in S, xFx.

ii. For any x and y in S, if xFy and yFx, then x=y.

iii. For any x,y and z in S, if xFy and yFz, then xFz.

The relation $\leq$ is an example of an order relation defined on the integers.

Note that the two elements x and y need not be related at all. An important example of a partial order relation is the relation $\subseteq$ defined on subsets of a given set. If L_i, i=1,2,3..., are subsets of a given set, then

i. $L_i \subseteq L_i$

ii. If $L_i \subseteq L_j$ and $L_j \subseteq L_i$, then $L_i = L_j$.

iii. If $L_i \subseteq L_j$ and $L_j \subseteq L_k$, then $L_i \subseteq L_k$.

It is not necessarily true that $L_i \subseteq L_j$ or $L_j \subseteq L_i$ for every i and j.

7.2 CHAINS IN PARTIALLY ORDERED SETS

Definition 7.2 A chain or linear system is a system M of subsets of a set S such that for any L_i, L_j in M, either $L_i \subseteq L_j$ or $L_j \subseteq L_i$.

The union of such a chain is simply the union of all the L_i in M. If the chain has a finite number of links, then there exists a maximal element L_n not properly contained in any L_i. The least upper bound of a chain M is the union of all the L_i in M. McCoy presents three instructive examples of these ideas in Rings and Ideals ([5], p. 101). All three examples make use of a certain class of subsets of the set N of natural numbers.

In the first example, let M_a be the set of all non-empty subsets of N which contain at most three elements. In this case, every set containing three elements is maximal in M_a. Chains in M_a can contain no more than three distinct elements, for example $\{i\}$, $\{i,j\}$, $\{i,j,k\}$ where i,j,k are three distinct natural numbers. The union of the elements of this chain is the maximal element $\{i,j,k\}$ and this element is contained in M_a.

In the second example, let M_b be the set of all finite subsets of N. There is no maximal element in M_b. Consider a chain in M_b consisting of all sets $\{1,2,3...i\}$

where i is a natural number. The union of all the elements of the chain is not a finite set and the chain has no least upper bound. M_b has no maximal element and, most important, the union of the elements of the chain is not an element of the chain.

In the third example, M_c is the set of all subsets L_i of N such that if k contained in L_i, then every integer less than K is also contained in L_i. The set N itself is certainly an element of M_c and it is necessarily the maximal element. Moreover, the union of each chain in M_c is an element of M_c.

7.3 ZORN'S LEMMA

In each of the above cases, the set under consideration contained a maximal element only when the union of each chain in the set was also contained in the set. This condition can be stated formally as follows:

Zorn's Lemma: If a partially ordered set S has the property that every chain in S has an upper bound in S, then S contains one or more maximal elements.

If the partial order relation is set inclusion, Zorn's Lemma can be stated as follows:

Zorn's Lemma: Let M be a non-empty collection of subsets of a given set S. If the union of each chain in M is an element of M, then M contains one or more maximal elements.

7.4 APPLICATIONS OF ZORN' LEMMA

Now consider the set M consisting of all the ideals in any ring R. Let U be the union of the ideals in a chain in M and let a and b be any elements of U. Suppose a is contained in L_1 and b in L_2 where L_1 and L_2 are ideals in the chain. Then either $L_1 \subseteq L_2$ or $L_2 \subseteq L_1$, so a and b are both contained in at least one ideal L_n. By the definition of ideal, a - b is an element of L_n and aR, Ra, bR and rB are contained in L_n. Since $L_n \subseteq U$ and a and b were arbitrary elements of U, then the set U is closed under subtraction and under multiplication by the other elements of the ring and U is an ideal. Since the union of each chain of ideals in M is also an ideal, then M contains one or more maximal ideals by Zorn's Lemma.

In the ring of integers, the following is an example of a chain of ideals: $(24) \subset (12) \subset (6) \subset (3)$. The union of the chain is the maximal element or least upper bound (3). Since every composite integer has a prime factor and the principal ideal generated by a prime integer is maximal in the ring, every such chain in I has a maximal element as Zorn's Lemma requires.

Zorn's Lemma is logically equivalent to the axiom of choice, but the proof of that equivalence is beyond the scope of this paper. ([8], p. 245).

CHAPTER VIII

CONCLUSION

8.1 SUMMARY

The first three chapters of this thesis include an informal survey of the basic facts concerning integral domains, principal and maximal ideals, residue class rings, the ring of integers, the ring of polynomials over a field and a special example of a finite non-commutative ring.

Chapter IV is an introduction to completely prime and prime ideals with proofs of the important theorems and illustrations taken from the rings mentioned above.

Chapter V includes a discussion of multiplicative systems, m-systems, the radical and the prime radical of an ideal.

The conditions for prime and completely prime ideals to exist in complete matrix rings were discussed in Chapter VI and three new theorems were presented.

Chapter VII contained an explanation of how Zorn's Lemma is used in certain proofs in the theory of rings.

8.2 SUGGESTIONS FOR FURTHER STUDY

Professor McCoy's new book contains a great many topics which would make excellent theses [5]. Some possibilities are the following:

1. What is the relationship between the prime radical of an ideal, the radical of an ideal, the radical of a ring and the Baer, Jacobson and lower radicals of a ring?

2. An ideal Q in a ring R is semi-prime if and only if it has the property that for any ideal A in R, $A \subseteq Q$ if $A^2 \subseteq Q$. A set N of elements of a Ring R is said to be an n-system if and only if it has the property that for any a in N, there exists an x in R such that axa is contained in N.

Semi-prime ideals and n-systems parallel prime ideals and m-systems very closely and a comparison of completely prime, prime and semi-prime ideals and multiplicative, m- and m-systems would make an interesting thesis.

3. What kind of structure is formed by congruence modulo a two-sided ideal in complete matrix rings and in other non-commutative rings?

4. Do there exist right ideals which otherwise satisfy the definition of prime ideal?

The theory of rings is a lively area of mathematical research and there are enough unanswered questions to provide fertile ground for thesis material.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Jacobson, Nathan. Structure of Rings. Providence: American Mathematical Society, 1956.

2. Jacobson, Nathan. Theory of Rings. New York: American Mathematical Society, 1943.

3. Krull, Wolfgang. "Idealtheorie in Ringen ohne Endlichkeitsbedingung," Mathematische Annalen, 101:729-744, 1929.

4. McCoy, Neal H. "Prime Ideals in General Rings," American Journal of Mathematics, 71:823-833, 1949.

5. McCoy, Neal H. Rings and Ideals. Buffalo: Mathematical Association of America, 1948.

6. McCoy, Neal H. The Theory of Rings. New York: The MacMillan Company, 1964.

7. Samuel, Pierre and Oscar Zariski. Commutative Algebra. Vol. 1. Princeton: D. Van Nostrand Company, 1958.

8. Suppes, Patrick C. Axiomatic Set Theory. Princeton: D. Van Nostrand Company, 1960.