IDEALS IN A RING

by

RAYMOND CARL SMITH

B. S., Nebraska State Teachers College, 1962
Kearney, Nebraska

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

1965

Approved by:

R. L. Yates

Major Professor

TABLE OF CONTENTS

I. INTRODUCTION

The purpose of this report is to discuss some of the elementary concepts of the theory of ideals in a ring. Some emphasis is given to a consideration of the properties of and relationships among minimal and maximal prime ideals, the radical of an ideal, and primary ideals.

The theory discussed in this report is based, of course, on the theory of groups and the theory of rings. Thus the primary purpose of this section is to list the basic definitions and theorems from group and ring theory which will be needed.

Definition 1.1.[1] Let G be a non-empty set of elements such that for any two elements $a,b \in G$ a sum $a + b \in G$ is uniquely defined. Let a, b and c be arbitrary elements of G not necessarily distinct. Then the set G (together with the operation of addition) is said to be an additive abelian group if addition has the following three properties:

(i) $(a + b) + c = a + (b + c)$

(ii) $a + b = b + a$

(iii) There is at least one $x \in G$ such that $a + x = b$.

It is shown in elementary group theory that Definition 1.1

[1] This denotes the first definition in the first section. The notation, a.b, where a is the number of the section and b is the number of the theorem, lemma, or definition in that section, is used throughout this report.

implies the existence of a unique additive identity, $0 \in G$, and the existence for each element $a \in G$ of a unique additive inverse, $-a \in G$.

Definition 1.2. Let G be an additive abelian group. Let H be a non-empty subset of G. Then H is called a subgroup of G if H is itself an additive abelian group with respect to the operation of addition in G.

Definition 1.3. Let H_i $(i = 1,2,\ldots)$ be a set of subsets of a set S. Then the set K of elements common to the H_i is called the intersection of the subsets H_i.

Theorem 1.1. The intersection of subgroups of an additive abelian group G is a subgroup of G.

Definition 1.4. Let R be a non-empty set of elements such that for any two elements $a,b \in R$ a sum $a + b \in R$ and a product $ab \in R$ are uniquely defined. Let a, b and c be arbitrary elements of R not necessarily distinct. Then the set R (together with the operations of addition and multiplication) is said to be a ring if addition and multiplication have the following three properties:

(i) With respect to addition R is an additive abelian group.

(ii) $a(bc) = (ab)c$

(iii) $a(b + c) = ab + ac, \quad (b + c)a = ba + ca$

If multiplication in a ring R has the additional property:

(iv) $ab = ba$

then R is called a commutative ring. If multiplication in R does not satisfy property (iv), then R is said to be non-commutative.

Definition 1.5. Let R be a ring. Let S be a non-empty subset of R. Then S is called a subring of R is S is itself a ring with respect to the operations of addition and multiplication in R.

If a non-empty subset M of a ring R is closed under addition and subtraction, then M is called a module. Note that any subgroup H of the additive group of R is a module since $a + b \in H$ and $a + (-b) = a - b \in H$ for every pair $a,b \in H$.

II. THE CONCEPT OF AN IDEAL

To begin this section, it is necessary to make the following definition:

Definition 2.1. A non-empty subset A of a ring R is called an ideal in R if it satisfies the following postulates:

(1) With respect to the operation of addition, A is a subgroup of the additive group of R.

(2) $ar, ra \in A$ for each $a \in A$ and $r \in R$.

There are other useful, equivalent definitions of an ideal in a ring R. This fact is stated as the following theorem:

Theorem 2.1. If A is a non-empty subset of a ring R such that $ar, ra \in A$ for each $a \in A$ and $r \in R$, then all of the following statements are equivalent:

(i) A is an ideal.

(ii) With respect to the operation of addition, A is a subgroup of the additive group of R.

(iii) A is a module.

(iv) If $a, b \in A$, then $a - b \in A$.

Proof: Assume that (i) is true. Then (ii) is true by Definition 2.1, and (i) implies (ii).

Next, assume that (ii) is true. Then for any $a \in A$ and any $b \in A$; $a + b \in A$ by closure under addition. Since each element $b \in A$ has an additive inverse $-b \in A$, then $a - b \in A$, A is a module by definition, and (ii) implies (iii).

By the definition of a module in a ring R, it follows, trivially, that (iii) implies (iv).

Finally, assume that (iv) is true, then for any $a \in A$, $a - a = 0$ is in A and, hence, $0 - a = -a$ is in A. Thus, if A contains any element a, it also contains its additive inverse. It is obvious then that if $a \in A$ and $b \in A$, $a-(-b) = a + b$ is in A. This establishes the fact that A is an additive subgroup of R, and it follows that A is an ideal in R. Therefore, (iv) implies (i), and the proof is complete.

An ideal A in a ring R is, then, by the preceding definitions, simply a "special" subring of R with the property that it contains the product of any element of the ring R by any element of the subring A. It is readily seen that every ring has two trivial ideals--the whole ring, which is called the unit ideal, and the single element zero, which is called the zero ideal. These two ideals are called improper ideals. Any other ideal in a ring is said to be proper. Any ring which contains only the two improper ideals is said to be simple.

Theorem 2.2. If A is an ideal in a ring R, then A is a subring of R.

Proof: Since A is a non-empty subset of R, it is only necessary to show that multiplication is closed. Consider any two elements $a \in A$ and $b \in A$. Because A is a subset of R, $a \in R$ and $b \in R$. Hence, by the definition of an ideal, $ab \in A$.

Of course, a subring A of a ring R is not necessarily an ideal in R. For example, let A be the set of all integers, and let R be the set of all rationals. Then $3 \in A$ and $1/2 \in R$, but $(1/2)3 = 3/2 \in A$.

It should be noted that the case often arises in which A does satisfy postulate (1) of Definition 2.1, but either $ar \in A$ for $a \in A$, $r \in R$ or $ra \in A$ for $a \in A$, $r \in R$ is not satisfied. If A satisfies postulate (1) of Definition 2.1, and is closed under multiplication on the right by elements of R, A is called a right ideal. If A satisfies postulate (1) of Definition 2.1 and is closed under multiplication on the left by elements of R, A is called a left ideal. If A is closed under multiplication on both the right and the left by elements of R, it is called a two-sided ideal or simply an ideal. Note that a two-sided ideal is a left (right) ideal, but a left (right) ideal may or may not be a two-sided ideal.

Throughout this report, statements made about an ideal will hold equally well for right or left ideals provided appropriate changes are made simply in the notation, or in the wording of the statement. It will be convenient, with this understanding, to limit the discussion to two-sided ideals.

III. ELEMENTARY CALCULUS OF IDEALS

In this section, three basic ways of combining ideals are discussed. These are known as addition, multiplication, and intersection.

First, consider addition of ideals.

Definition 3.1. If A and B are given ideals in a ring R, the set C of all elements of the form $a + b$ for $a \in A$ and $b \in B$ is called the sum of A and B and is denoted by $A + B$.

Theorem 3.1. The set $C = A + B$ is an ideal.

Proof: Suppose $x_1, x_2 \in C$ and $r \in R$

Then, $x_1 = a_1 + b_1$ and $x_2 = a_2 + b_2$

in which $a_1, a_2 \in A$ and $b_1, b_2 \in B$, and $$x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)$$

$$x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2)$$

$$rx_1 = ra_1 + rb_1$$

$$x_1r = a_1r + b_1r.$$

However, $a_1 + a_2, a_1 - a_2, ra_1, a_1r \in A$

$$b_1 + b_2, b_1 - b_2, rb_1, b_1r \in B.$$

Hence by Definition 3.1

$$x_1 + x_2, x_1 - x_2, rx_1, x_1r \in C$$

and therefore C is an ideal.

From Definition 3.1, it is readily seen that $A + B = B + A$. Also, if A_1, A_2, and A_3 are any three ideals in R, then $A_1 + (A_2 + A_3) = (A_1 + A_2) + A_3$ because $A_1 + (A_2 + A_3)$ and $(A_1 + A_2) + A_3$ both consist of elements of the form $a_1 + a_2 + a_3$ for $a_i \in A_i$ $(i = 1,2,3)$.

<u>Definition 3.2</u>. If A and B are given ideals in R, the set C of all elements of the form $\sum a_ib_i$[2] with $a_i \in A$ and $b_i \in B$ is called the product of A and B and is denoted by AB.

[2] It is to be understood that $\sum$ represents an arbitrary finite sum with one or more terms.

Theorem 3.2. The set $C = AB$ is an ideal.

Proof: Suppose $x_1, x_2 \in C$ and $r \in R$.

Then, $x_1 = a_1b_1 + a_2b_2 + \dots + a_nb_n$

$x_2 = a_1'b_1' + a_2'b_2' + \dots + a_m'b_m'$

in which $a_i, a_i' \in A$ and $b_k, b_k' \in B$,

and
$$x_1 + x_2 = a_1b_1 + a_2b_2 + \dots + a_nb_n + a_1'b_1' + \dots + a_m'b_m'$$

$$x_1 - x_2 = a_1b_1 + a_2b_2 + \dots + a_nb_n + (-a_1')b_1' + \dots + (-a_m')b_m'$$

$$rx_1 = (ra_1)b_1 + \dots + (ra_n)b_n$$

$$x_1r = a_1(b_1r) + \dots + a_n(b_nr).$$

However, $-a_i', ra_i \in A$ and $b_ir \in B$.

Hence by Definition 3.2,

$$x_1 + x_2,\ x_1 - x_2,\ rx_1, \text{ and } x_1r \in C,$$

and C is an ideal.

Since R is not necessarily commutative, the statement $AB = BA$ is not generally true. However, if A_1, A_2, and A_3 are any three ideals in R, $A_1(A_2A_3) = (A_1A_2)A_3$ because $A_1(A_2A_3)$ and $(A_1A_2)A_3$ both consist of elements of the form $a_{1i}a_{2i}a_{3i}$ in which $a_{ji} \in A_j$ for $j = 1,2,3$.

Consider next the intersection of a set of ideals in a ring R.

Theorem 3.3. The intersection of any non-empty set S of ideals in a ring R is an ideal in R.

Proof: Since the zero ideal is contained in every ideal, the intersection is non-empty. Each of the ideals in S is a subgroup of the additive group of R. By Theorem 1.1, the intersection is a subgroup of the additive group of R, and postulate (1) of Definition 2.1 is satisfied. Postulate (2) of the same definition is satisfied because the elements of the intersection are necessarily contained in each of the ideals of the given set.

A given non-empty set K of elements in a ring R determines uniquely an ideal in R which is the intersection of all ideals in R containing the set K.

Definition 3.3. The intersection of all ideals in a ring R which contain a given non-empty set K of elements of R is called the ideal generated by K.

Definition 3.4. Let K be a non-empty set of elements of R which generates an ideal A. Then K is said to be a basis of the ideal A.

The special case in which the basis K consists of a single element of R will be considered in the following section.

IV. PRINCIPAL IDEALS

Definition 4.1. An ideal in R generated by one element a of R is called a principal ideal. It is denoted by (a).

Consider in detail the set E of elements which make up the ideal (a) in the ring R. Because $a \in (a)$, $a - a = 0 \in (a)$, and it follows that $0 - a = -a \in (a)$. Since (a) is closed under addition:

$$a + a + a + \dots + a = na \; (n = 1,2,\dots) \in (a),$$

$$[-a] + [-a] + \dots + [-a] = n[-a] \; (n = 1,2,\dots) \in (a)$$

$$= na \; (n = -1,-2,\dots) \in (a),$$

$$0 = na \; (n = 0) \in (a).$$

Thus, $na \in (a)$ for all $n \in I$. (The set of all integers).

By Definition 2.1, $a \in (a)$ and $r \in R$ implies that $ra, ar \in (a)$, but note that "a" denotes a particular single element of R. It follows that elements of the form ras, with $r, s \in R$ and a, the generator of (a), are contained in (a).

Hence, (a) is made up of a set E of elements such that if $e \in E$ then:

$$e = na + ra + as + \sum r_i a s_i \; (n \in I, \text{ and } r,s,r_i,s_i \in R).$$

Because the difference,

$$\left[n_1a + r_1a + as_1 + \sum r_ias_i\right] - \left[n_2a + r_2a + as_2 + \sum r_jas_j\right]$$
$$= (n_1 - n_2)a + (r_1 - r_2)a + a(s_1 - s_2) + \sum r_kas_k,$$

is a member of the set E,E is closed under subtraction.

If any member of the set E is multiplied on the right by any $u \in R$, the product is a member of the set E as the following lemma shows.

<u>Lemma 4.1</u>. $\left[na + ra + as + \sum r_ias_i\right]u =$

$$(1) \quad \left[nau + rau + asu + \sum r_ias_iu\right] =$$
$$\left[at + \sum v_iaw_i\right] \in E$$

<u>Proof</u>: Consider each of the terms of (1). If $n > 0$,

then $nau = au + au + \ldots + au$ to n terms,

but $au + au + \ldots + au = a(u + u + \ldots + u)$.

Hence, $nau = a(nu)$ for $n > 0$. If $n < 0$,

then $nau = (-n)(-a)u = (-au) + (-au) + \ldots + (-au)$ to $-n$ terms,

but $(-au) + (-au) + \ldots + (-au) =$
$a(-u) + a(-u) + \ldots + a(-u) = a(-n)(-u)$.

Hence, $nau = a(nu)$ for $n < 0$. If $n = 0$, then $nau = 0(au) = 0 = a(0)$. Thus all terms of the form nau can be written in the form at_1. Because $asu = a(su)$, terms of this form can be written in the form at_2. Finally, it is obvious that elements of the form rau and $r_1as_1u = r_1a(s_1u)$ can be written in the form v_1aw_1.

If a member of the set E is multiplied on the left by any $u \in R$, the product is a member of the set E as the following lemma shows.

Lemma 4.2.

$$u\left[na + ra + as + \sum r_1as_1\right] =$$

$$(2) \quad \left[una + ura + uas + \sum ur_1as_1\right] =$$

$$\left[va + \sum v_1aw_1\right] \in E$$

Proof: Consider each of the terms of (2). Any $una = (nu)a$ and any $ura = (ur)a$ can obviously be written in the form va. Any uas and any $(ur_1)as_1$ can be written in the form v_1aw_1.

Therefore, the set E generated by the element $a \in R$ is an ideal in R, and the following theorem holds.

Theorem 4.1. In an arbitrary ring R:

$$(a) = \left\{na + ra + as + \sum r_1as_1 \;\middle|\; n \in I \text{ and } r,s,r_1,s_1 \in R\right\}.$$

If the ring R is commutative, the set E reduces to a much simpler form.

Theorem 4.2. In a commutative ring R_c:

$$(a) = \left\{na + at \;\middle|\; n \in I \text{ and } t \in R_c\right\}..$$

Proof: This follows easily from Theorem 4.1. Because multiplication of elements of R_c is commutative, all finite sums of the form $\sum r_i a s_i = \sum a r_i s_i$ and all expressions of the form $ra + as = a(r + s)$ can be reduced to a single term.

It is convenient at this point to introduce some concepts and notations which will be needed in later sections.

Consider the ideal A + B which is the sum of the two ideals A and B in a ring R_c. A + B contains A and B, and any ideal in R_c which contains both A and B obviously contains the ideal A + B. It follows that A + B is the intersection of all ideals which contain both A and B. For this reason, the sum A + B is sometimes denoted (A,B).

If $K = \{a_1, a_2, \ldots, a_m\}$ is a basis of an ideal A in R_c, then A is just the sum of the principle ideals (a_i) $(i = 1,2,\ldots,m)$. However, instead of writing $((a_1), (a_2), \ldots, (a_m))$, the more common notation $(a_1, a_2, \ldots, a_m)$ will be used. Similarly, if M is an ideal in R_c and $a \in R_c$ then M + (a) will be denoted by (M,a). Note that from the above and Theorem 4.2 it follows that in R_c the elements of (M,a) are of the form

$$b + na + at \quad (b \in M,\ n \in I, \text{ and } t \in R_c) .$$

Certain commutative rings have the interesting property that every ideal that they contain is a principal ideal.

Theorem 4.3. In the commutative ring I of integers every ideal is a principal ideal.

Proof: Let A be any ideal in I. If A is the zero ideal, then $A = (0)$ is a principal ideal. Assume $A \neq (0)$. Then A contains some integer $m \neq 0$. If A contains m, then A contains $-m$ and it follows that A contains at least one positive integer. Let d be the smallest positive integer in A. If n is any integer, then $n = qd + r$ for $q, r \in I$ and $d > r \geq 0$. If $n \in A$, then $n - qd = r \in A$, and $r = 0$ because $d > r > 0$ contradicts the assumption that d is the smallest positive integer in A. Hence, any $n \in A$ is of the form qd and $A = \{qd \mid q \in I\}$. But by Theorem 4.2, $\{qd \mid q \in I\} = (d)$, and the proof is complete.

In the commutative ring I of integers it has been shown that every ideal is principal. Suppose (m) is an ideal in I, then all elements in (m) are of the form km for $k \in I$. If $a, b \in (m)$, then $a - b \in (m)$, since (m) is closed under subtraction. Hence, $a - b = km$, but this is the familiar definition of congruence modulo m. This is a specific case of the concept of congruence modulo an ideal which will be needed in the next section.

Definition 4.2. Let M be any ideal in a ring R_c. If $a - b \in M$, then a is said to be congruent to b modulo the ideal M. This is denoted by $a \equiv b(M)$.

It follows that $a \equiv 0(M)$ is simply another way of expressing $a \in M$.

V. PRIME IDEALS AND THE RADICAL OF AN IDEAL

For the purposes of the rest of this report, the rings under consideration will all be commutative rings. To avoid possible confusion, however, commutative rings will continue to be denoted by R_c.

Before a definition of a prime ideal is given it is necessary to define divisibility.

Definition 5.1. Let B be an ideal in a ring R_c. If a is an element of B, then $a - 0 \in B$ which implies $a \equiv 0(B)$, and a is said to be divisible by the ideal B. This is denoted by $B \mid a$. If all the elements of an ideal A are divisible by B, then the ideal A is said to be divisible by the ideal B. Moreover, if $A \subset B$, then B is called a proper divisor of A.

Definition 5.2. An ideal P in a ring R_c is a prime ideal if and only if:

$$P \mid ab \text{ implies } P \mid a \text{ or } P \mid b.$$

This definition of a prime ideal is somewhat analogous to one of the properties of a prime integer. Thus, the ideals (p) for p a prime integer are prime ideals in the ring I of integers.

There are, however, other equivalent definitions which are sometimes more useful. These are stated as the following theorem.

Theorem 5.1. The following necessary and sufficient conditions that an ideal P be a prime ideal are equivalent:

(i) $P \mid ab$ implies $P \mid a$ or $P \mid b$.

(ii) $ab \equiv 0(P)$ implies $a \equiv 0(P)$ or $b \equiv 0(P)$.

(iii) $ab \in P$ implies $a \in P$ or $b \in P$.

Proof: This follows trivially from definitions 5.1 and 5.2.

It should be noted that the above conditions can be stated in other logically equivalent forms. For example, (iii) could be stated as: $a \notin P$ and $b \notin P$ implies $ab \notin P$.

Definition 5.3. A set M is called a multiplicative system if the product of elements of M is always an element of M.

Since the null set satisfies Definition 5.3 vacuously, it will be considered as a multiplicative system.

Throughout this report the set of elements of R_c not in the ideal P, the complement of P, will be denoted by C(P).

Theorem 5.2. The ideal P is a prime ideal in R_c if and only if C(P) is a multiplicative system.

Proof: Let P be a prime ideal. Then by the logical equivalent of part (iii) of Theorem 5.1, $a \notin P$ and $b \notin P$ imply $ab \notin P$. However ($a \notin P$ and $b \notin P$ imply $ab \notin P$) is equivalent to ($a,b \in C(P)$ implies $ab \in C(P)$), and ($a,b \in C(P)$ implies $ab \in C(P)$) implies that C(P) is a multiplicative system. Hence, if P is a prime ideal then C(P) is a multiplicative system. The converse can be shown by simply reversing these steps.

Definition 5.4. Let A be any ideal in R_c. Then RadA is the set of all elements $z \in R_c$ for which there exists a positive integer r (possibly depending on z) such that $z^r \in A$. RadA is called the radical of the ideal A.

Theorem 5.3. RadA is an ideal in R_c.

Proof: Let $z_1, z_2 \in$ RadA. Then $z_1^{r_1}, z_2^{r_2} \in A$ for r_1, r_2 positive integers. Let $r = r_1 + r_2$ then $(z_1 - z_2)^r = \sum m_{ij} z_1^i z_2^j$ in which $i \geq 0$, $j \geq 0$, $i + j = r$ for i,j, and m_{ij} integers. In each term of $\sum m_{ij} z_1^i z_2^j$, either $i \geq r_1$ or $j \geq r_2$. If $i \geq r_1$ then of course $i = r_1 + k$, where k is some non-negative integer, and $z_1^i = z_1^{r_1 + k} = z_1^{r_1} z_1^k \in A$. Similarly, if $j \geq r_2$ then $z_2^j \in A$. In either case $z_1^i z_2^j \in A$. Hence, $\sum m_{ij} z_1^i z_2^j = (z_1 - z_2)^r \in A$, and it follows that $z_1 - z_2 \in$ RadA.

Also, for any $a \in R_c$, $(az_1)^r = a^r z_1^r \in A$ which implies $az_1 \in$ RadA.

Since $z_1 - z_2$, $az_1 \in$ RadA, RadA is an ideal in R_c.

Suppose P is a prime ideal such that $A \subseteq P$, then it can be shown that $a \subseteq \text{RadA} \subseteq P$. It is obvious from Definition 5.4 that $A \subseteq$ RadA. If $z \in$ RadA, then $z^1 \in A$ and $z^1 \in P$. However, if $z^1 \in P$, by the definition of a prime ideal, $z \in P$, and Rada $\subseteq P$. Consider the special case, $A = P$, then $P \subseteq \text{RadP} \subseteq P$, and it follows that a prime ideal is its own radical.

The primary purpose of the rest of this section is to prove the important fact that in a commutative ring R_c the radical of an ideal A is the intersection of all prime ideals containing A. It is necessary at this point to introduce some material which will be needed later.

Definition 5.5. Let $\mathcal{L}$ be a system consisting of one or more subsets of an arbitrary set $\mathcal{S}$ with the property that for any two subsets L_1 and L_2 either $L_1 \subseteq L_2$ or $L_2 \subseteq L_1$. Then $\mathcal{L}$ is called a linear system. Moreover, if all subsets of $\mathcal{L}$ are also subsets of a system $\mathcal{T}$ then $\mathcal{L}$ is said to be a linear subsystem of $\mathcal{T}$.

For the purposes of this section, $\mathcal{T}$ will generally be either a set of ideals in R_c or a set of multiplicative systems in R_c.

Theorem 5.4. The union U of any linear system $\mathcal{L}$ of ideals in R_c is an ideal in R_c.

Proof: Let $a, b \in U$, then $a \in L_1$ and $b \in L_2$ where L_1 and L_2 are ideals not necessarily distinct in $\mathcal{L}$. Since $\mathcal{L}$ is a linear system, either $L_1 \subseteq L_2$ or $L_2 \subseteq L_1$. Assume, for the purposes of argument, that $L_1 \subseteq L_2$. Then $a \in L_2$ and $b \in L_2$. Thus, because L_2 is an ideal, $a - b \in L_2$ and for any $r \in R_c$, $ar \in L_2$. But $L_2 \subseteq U$. Therefore $a - b \in U$, $ar \in U$, and U is an ideal.

Theorem 5.5. The union U of any linear system $\mathcal{L}$ of multiplicative systems of elements of R_c is a multiplicative system of elements of R_c.

Proof: Let $c,d \in U$. Then $c \in M_1$ and $d \in M_2$ where M_1 and M_2 are multiplicative systems not necessarily distinct in $\mathcal{L}$. Since $\mathcal{L}$ is a linear system, either $M_1 \subseteq M_2$ or $M_2 \subseteq M_1$. Assume $M_1 \subseteq M_2$. Then $c \in M_2$, $d \in M_2$ and $cd \in M_2$ since M_2 is a multiplicative system. Now $M_2 \subseteq U$; therefore $cd \in U$, and U is a multiplicative system.

Definition 5.6. Let $\mathcal{T}$ be a system of one or more subsets of $\mathcal{S}$. A subset M of $\mathcal{T}$ is said to be maximal in $\mathcal{T}$ if $M \subseteq A$ for any subset A of $\mathcal{T}$ implies that $M = A$.

In other words M is maximal in $\mathcal{T}$ if M is in $\mathcal{T}$ and there is no subset of $\mathcal{T}$ which contains M as a proper subset.

The following statement, which will be called the Maximum Principle, is logically equivalent to the Axiom of Choice, and is sometimes called Zorn's Lemma.[3]

Maximum Principle. If the union of each linear subsystem of $\mathcal{S}$ is a subset of $\mathcal{S}$, then $\mathcal{S}$ has a maximal subset.

Throughout the rest of this report the Maximum Principle will be considered as an axiom.

[3] J. Barkley Rosser, Logic for Mathematicians, p. 507.

Definition 5.7. Let A be any ideal in R_c. A prime ideal P in R_c is said to be a minimal prime ideal belonging to A if $A \subseteq P$ and there is no prime ideal P' such that $A \subseteq P' \subset P$.

This completes the statement of the necessary preliminary material. At this point it is necessary to prove three lemmas which will lead to the proof of the following theorem:

Theorem 5.6. RadA in R_c is the intersection of all minimal prime ideals belonging to A.

Lemma 5.1. Let A be an ideal in R_c, and M a multiplicative system of elements of R_c such that $M \cap A = \emptyset$.[4] Then $M \subseteq M^*$ where M^* is a maximal multiplicative system such that $M^* \cap A = \emptyset$ and if N is a multiplicative system such that $M^* \subset N$, then $N \cap A \neq \emptyset$.

Proof: Let $\mathfrak{A}$ be the set of all multiplicative systems M_1 in R_c such that $M \subseteq M_1$ and $M_1 \cap A = \emptyset$. Let $\mathcal{L}$ be any linear subsystem of $\mathfrak{A}$. Then by Theorem 5.5 the union U of $\mathcal{L}$ is a multiplicative system. Obviously $M \subseteq U$ and $U \cap A = \emptyset$; hence $U \in \mathfrak{A}$. By the Maximum Principle, it follows that $\mathfrak{A}$ has a maximal multiplicative system M^*. Since $M^* \in \mathfrak{A}$, $M \subseteq M^*$ and $M^* \cap A = \emptyset$. Suppose N is a multiplicative system such that $M^* \subset N$, then $N \notin \mathfrak{A}$; hence $N \cap A \neq \emptyset$.

Lemma 5.2. Let A be an ideal in R_c, and M a multiplicative system of elements of R_c such that $M \cap A = \emptyset$. Then $A \subseteq P^*$ where

[4] Throughout this report the null set is denoted by $\emptyset$.

P^* is a maximal ideal such that $M \cap P^* = \emptyset$, and if B is an ideal such that $P^* \subset B$, then $B \cap M \neq \emptyset$. Also, P^* is necessarily prime.

Proof: Let $\mathfrak{a}$ be the set of all ideals A_i in R_c such that $A \subseteq A_i$ and $A_i \cap M = \emptyset$. Let $\mathcal{L}$ be any linear subsystem of $\mathfrak{a}$. Then by Theorem 5.4, the union U of $\mathcal{L}$ is an ideal. Obviously $A \subseteq U$ and $U \cap M = \emptyset$. Hence, $U \in \mathfrak{a}$. By the Maximum Principle, it follows that $\mathfrak{a}$ has a maximal ideal P^*. Since $P^* \in \mathfrak{a}$, $M \cap P^* = \emptyset$. Suppose B is an ideal such that $P^* \subset B$. Then $B \notin \mathfrak{a}$ and hence $B \cap M \neq \emptyset$.

To show that P^* is necessarily prime, assume that $a \notin P^*$, $b \notin P^*$, and show that $ab \notin P^*$ for $a, b \in R$. Consider the ideal $(P^*, a) = P^* + (a)$. Because $a \notin P^*$, it follows that $P^* \subset (P, a)$ which implies that there exists at least one element $m_1 \in M$ such that $m_1 \in (P^*, a) \cap M$.

$$\text{Let } m_1 = p_1 + r_1 a + i_1 a \quad (p_1 \in P^*,\ r_1 \in R_c,\ i_1 \in I)$$

since all elements of (P^*, a) are expressible in this form. Similarly, it can be shown that (P^*, b) contains an element $m_2 \in M$ which can be expressed in the following form:

$$m_2 = p_2 + r_2 b + i_2 b \quad (p_2 \in P^*,\ r_2 \in R_c,\ i_2 \in I).$$

The product,

$$\begin{aligned} m_1m_2 &= \left[p_1 + r_1a + i_1a\right] \left[p_2 + r_2b + i_2b\right] \\ &= p_1p_2 + p_1r_2b + p_1i_2b + r_1p_2a + r_1r_2ab + r_1i_2ab + \\ &\quad + i_1p_2a + i_1r_2ab + i_1i_2ab \\ &= p_1p_2 + (r_2b + i_2b)p_1 + (r_1a + i_1a)p_2 + \\ &\quad + (r_1r_2 + r_1i_2 + i_1r_2)ab + i_1i_2ab. \end{aligned}$$

Since $p_1, p_2 \in P^*$, $m_1m_2 \in P^*$ if $ab \in P^*$. However $m_1m_2 \notin P^*$ since $m_1m_2 \in M$. Therefore, it follows that $ab \notin P^*$.

Lemma 5.3. A set P of elements of R_c is a minimal prime ideal belonging to the ideal A in R_c if and only if C(P) is a maximal multiplicative system such that $C(P) \cap A = \emptyset$.

Proof: First, let P be a set of elements in R_c such that $C(P) = M$ where M is a maximal multiplicative system such that $M \cap A = \emptyset$. Then by Lemma 5.2 there exists a prime ideal P^* such that $A \subseteq P^*$ and $P^* \cap M = \emptyset$. Hence, $C(P^*) \cap A = \emptyset$ and $M \subseteq C(P^*)$. By Theorem 5.2, $C(P^*)$ is a multiplicative system, and since M is a maximal multiplicative system, it follows that $C(P^*) = M = C(P)$. Therefore, $p = P^*$ and hence P is a prime ideal such that $A \subseteq P$. Now suppose P_1 is a prime ideal such that $A \subseteq P_1 \subset P$. Then $C(P_1)$ is a multiplicative system such that $C(P_1) \cap A = \emptyset$ and $M \subset C(P_1)$. This, however, is a contradiction since M is maximal, and it follows that P is a minimal prime ideal belonging to A.

To prove the converse, let P be a minimal prime ideal belonging to A, that is, $A \subseteq P$. Then $C(P) = M$ is a multiplicative system such that $C(P) \cap A = \emptyset$. By Lemma 5.1, there exists a maximal multiplicative system M' such that $C(P) \subseteq M'$ and $M' \cap A = \emptyset$. By the first part of this proof, $C(M') = P'$ is a minimal prime ideal belonging to A. Because $M' \supseteq C(P)$, $P' \subseteq P$, but P is minimal, and it follows that $P = P'$. Hence, $C(P) = M'$ which implies that C(P) is a maximal multiplicative system such that $C(P) \cap A = \emptyset$.

Now Theorem 5.6 can be established. It has been shown that if $A \subseteq P$ then $\text{Rad}A \subseteq P$. Hence, RadA is contained in the intersection of all minimal prime ideals belonging to A. To complète the proof, it is necessary to show that RadA contains the intersection of all minimal prime ideals belonging to A. Suppose $a \in R_c$ but $a \notin \text{Rad}A$, and let M be the set of all elements of the form a^i $(i = 1,2, \ldots)$. Then M is a multiplicative system such that $M \cap A = \emptyset$. By Lemma 5.1, $M \subseteq M^*$ where M^* is a maximal multiplicative system such that $M^* \cap A = \emptyset$. Now $a \in M$ implies $a \in M^*$ which in turn implies that $a \notin C(M^*)$. However by Lemma 5.3, $C(M^*)$ is a minimal prime ideal belonging to A, and it follows that a is not in the intersection of all prime ideals belonging to A. This completes the proof.

Note that for any ideal A in R_c there exists at least one minimal prime ideal belonging to A since RadA is the intersection of all minimal prime ideals belonging to A.

Theorem 5.7. Any prime ideal containing the ideal A contains a minimal prime ideal belonging to A.

Proof: Let P be any prime ideal such that $A \subseteq P$. Then $C(P) \cap A = \emptyset$. By Theorem 5.2, C(P) is a multiplicative system, and by Lemma 5.1 there exists a maximal multiplicative system M^* such that $C(P) \subseteq M^*$ and $M^* \cap A = \emptyset$. It follows from Lemma 5.3 that $C(M^*)$ is a minimal prime ideal belonging to A. Also, since $C(P) \subseteq M^*$, $C(M^*) \subseteq P$.

VI. MAXIMAL PRIME IDEALS BELONGING TO AN IDEAL

In this section another system of prime ideals, maximal prime ideals, associated with a given ideal A in a commutative ring R_c will be considered.

It is necessary to consider first the concept "is related to".

Definition 6.1. An element b of R_c is said to be related to the ideal A if there exists an element $r \in C(A)$ such that $br \in A$. If no such element exists, b is unrelated to A.

In other words, an element b of R_c is unrelated to A if and only if $bx \in A$ implies that $x \in A$.

It follows from Definition 6.1 that if A is a proper subset of R_c, then every element of A is related to A. Since $A \subset R_c$, $C(A) \neq \emptyset$, and there is at least one element $r \in C(A)$.

Let $a \in A$. Then certainly $ar \in A$ since A is an ideal in R_c. To insure that $C(A) \neq \emptyset$, throughout this section it will be assumed that $A \neq R_c$.

<u>Definition 6.2</u>. An ideal B is said to be related to A if every element of B is related to A; otherwise B is unrelated to A.

Obviously A is related to A and if $B \subset A$, then B is related to A.

<u>Theorem 6.1</u>. Rad A is related to A.

<u>Proof</u>: Let $d \in \text{Rad } A$. Then $d^i \in A$ for some positive integer i. If $i = 1$, d is an element of A and hence is related to A. If $i > 1$, let $j \leq i$ be the least positive integer such that $d^j \in A$. Then $d^{j-1} \notin A$, and $d\ (d^{j-1}) \in A$ implies d is related to A. Thus every element of RadA is related to A, and it follows that Rad A is related to A.

<u>Theorem 6.2</u>. Let M be the set of all elements of R_c which are unrelated to A. Then M is a multiplicative system.

<u>Proof</u>: Let $c,d \in M$, that is, let c,d be unrelated to A. Suppose $cd\ x \in A$. Then $c(dx) \in A$, but c unrelated to A implies $dx \in A$. Similarly, $d(x) \in A$ and d unrelated to A implies $x \in A$. Hence by the equivalent of Definition 6.1, cd is unrelated to A and is an element of M.

A maximal ideal belonging to A can now be defined.

Definition 6.3. An ideal which is maximal in the set of all ideals related to A is called a maximal prime ideal belonging to A.

Theorem 6.3. An ideal P is a maximal prime ideal belonging to A if and only if P is related to A but any ideal N such that $N \supset P$ is unrelated to A.

Proof: Let M be the set of all elements of R_c unrelated to A. Then, since A is related to A, $M \cap A = \emptyset$. If P is related to A, then $P \cap M = \emptyset$. Also, if N is unrelated to A, then $N \cap M \neq \emptyset$. Thus if P is related to A and N is an ideal unrelated to A such that $N \supset P$, by Lemma 5.2 P is a maximal ideal belonging to A and P is necessarily prime.

If P is a maximal prime ideal belonging to A then by Lemma 5.2 $M \cap P = \emptyset$ and if N is an ideal such that $N \supset P$ then $N \cap M \neq \emptyset$. Hence P is related to A and N is unrelated to A.

Theorem 6.4. A is contained in every maximal prime ideal P belonging to A.

Proof: Let $a + p \in (A,P)$ with $a \in A$ and $p \in P$. Since P is related to A, $pr \in A$ for some $r \in C(A)$. Hence, because $(a + p) r = ar + pr \in A$, $a + p$ is related to A. Since $a + p$ is any element of (A,P), (A,P) is related to A. Obviously, $P \subseteq (A,P)$. But P is maximal. Hence $P = (A,P)$ which implies $A \subseteq P$. Thus the proof is complete.

Theorem 6.5. Every element or ideal which is related to A is contained in a maximal prime ideal belonging to A.

To prove this theorem it is necessary to state and prove the following lemma:

Lemma 6.1. If an element b of R_c is related to an ideal A, then the ideal (b) is related to A.

Proof: Let b be related to A. Then there exists $r \in (A)$ such that $br \in A$. Consider any element of (b). It has been shown that such an element can be expressed in the form $nb + bt$ $(n \in I,\ t \in R_c)$. Obviously, the product $(nb + bt)r = nbr + btr = nbr + tbr \in A$. Hence every element of (b) is related to A, and it follows that (b) is related to A.

Therefore, for the proof of Theorem 6.5, only the case of an ideal which is related to A need be considered.

Let B be an ideal related to A. Also, let M be the set of all elements of R_c unrelated to A. Then $M \cap B = \emptyset$, and since A is related to A, $M \cap A = \emptyset$. By Lemma 5.2 there exists a maximal prime ideal P belonging to A, that is $A \subseteq P$, such that $M \cap P = \emptyset$. Now $M \cap P = \emptyset$ implies that P is related to A. Hence P is maximal in the set of all ideals related to A, and $B \subseteq P$.

Theorem 6.6. Every minimal prime ideal belonging to A is contained in a maximal prime ideal belonging to A.

Proof: To prove this theorem it is only necessary to show that a minimal prime ideal belonging to A is necessarily related to A. Then this theorem follows immediately from Theorem 6.5.

Let P be a minimal prime ideal belonging to A. Let b be any element of R_c unrelated to A. Then if it can be shown that $b \in C(P)$, it will follow that all elements of P are related to A. By Lemma 5.3, C(P) is a maximal multiplicative system such that $C(P) \cap A = \emptyset$. Let M be a multiplicative system such that $M = \{b^i, s, b^i s \ (s \in C(P), i = 1, 2, \ldots)\}$.

Since $A \subseteq P$, $C(P) \subseteq C(A)$. Hence, $s \in C(P)$ implies $s \notin A$. Suppose $b^i \in A$. Then $b \in$ Rad A. This is a contradiction since Rad A is related to A. Therefore $b^i \notin A$. Now suppose $b^j s \in A$. Let j be the smallest positive integer such that $b^j s \in A$ and $b^{j-1}s \in A$ for some fixed $s \in C(P)$. Obviously $j \neq 1$ because b is unrelated to A. Hence $j > 1$ and we can write $b(b^{j-1}s) \in A$. However, since $b^{j-1}s \notin A$, $b(b^{j-1}s) \in A$ implies b is related to A which is a contradiction. Thus $b^j s \notin A$ and it follows that $M \cap A = \emptyset$. Because $C(P) \subseteq M$, the maximal property of C(P) implies $C(P) = M$. Hence $b \in C(P)$, and the proof is complete.

VII. PRIMARY IDEALS

<u>Definition 7.1</u>. An ideal Q in the ring R_c is said to be primary if $ab \in Q$ and $a \notin Q$ imply that $b^i \in Q$ for some positive integer i.

A useful equivalent to Definition 7.1 is the following: An ideal Q in R_c is primary if $ab \in Q$ and $b^k \notin Q$ for all positive integers k imply $a \in Q$.

Note that every prime ideal is a primary ideal. Let P be any prime ideal. Then by definition $ab \in P$ and $a \notin P$ imply $b \in P$. Thus P satisfies the definition of a primary ideal with $i = 1$.

Theorem 7.1. The radical of a primary ideal is a prime ideal.

Proof: Let Q be a primary ideal. Suppose $ab \in$ RadQ but $a \notin$ Rad Q. Now $a \notin$ RadQ implies no integral power of a is in Q, but $ab \in$ RadQ implies $(ab)^j = a^j b^j \in Q$ for some positive integer j. Since $a^j \notin Q$, $(b^j)^i \in Q$ by Definition 7.1 and it follows that $b \in$ Rad Q. Hence RadQ is a prime ideal.

In section V it was shown that an ideal and its radical are contained in exactly the same prime ideals. This fact and Theorem 7.1 leads to the following statement.

Theorem 7.2. RadQ is the only minimal prime ideal belonging to Q if Q is a primary ideal.

Proof: Since every ideal has at least one minimal prime ideal belonging to it, let P be a minimal prime ideal belonging to Q. Then by Definition 5.7, $Q \subseteq P$ and there is no prime ideal P' such that $Q \subseteq P' \subset P$. This is a contradiction unless $P =$ RadQ since $Q \subseteq P$ implies $Q \subseteq$ RadQ $\subseteq P$, and RadQ is a prime ideal. Hence RadQ is the only minimal prime ideal belonging to Q.

Theorem 7.3. If $Q \neq R_c$ and Q is any primary ideal in R_c, then RadQ is the only maximal prime ideal belonging to Q.

Proof: Because RadQ is a minimal prime ideal belonging to Q and because $Q \neq R_c$, there exists a maximal prime ideal P^* belonging to Q such that $\mathrm{RadQ} \subseteq P^*$ by Theorem 6.6. Assume $\mathrm{RadQ} \neq P^*$. Then there exists $a \in R_c$ such that $a \notin \mathrm{RadQ}$ and $a \in P^*$. Let $ax \in Q$. Since $a \notin \mathrm{RadQ}$ no positive integral power of a is in Q, and it follows from the definition of a primary ideal that $x \in Q$. Therefore a is unrelated to Q. Since $a \in P^*$, P^* is unrelated to Q. This, however, is a contradiction because Theorem 6.3 holds since $Q \neq R_c$, and it would follow that P^* is not a maximal prime ideal belonging to Q. Therefore the assumption that $\mathrm{RadQ} \neq P^*$ is false, $\mathrm{RadQ} = P^*$, and the proof is complete.

Theorem 7.4. An ideal $Q \neq R_c$ is a primary ideal if and only if there exists a prime ideal P which is the unique minimal prime ideal belonging to Q and the unique maximal prime ideal belonging to Q.

Proof: If Q is a primary ideal then by Theorems 7.2 and 7.3 there does exist such a prime ideal. It is RadQ. To complete the proof, it is only necessary to show that if the prime ideal P is the unique minimal and maximal prime ideal belonging to Q, then Q is primary. Suppose that $ab \in Q$ and that $a^i \in Q$ for all positive integers i. Then $a \notin \mathrm{RadQ}$, which by Theorem 5.6 is P. Hence by Theorem 6.5 a is unrelated to Q. That is, $ab \in Q$ and $a \notin Q$ imply $b \in Q$. Hence Q is primary.

ACKNOWLEDGMENT

The author wishes to express his sincere appreciation to Dr. Richard L. Yates for his patient assistance in the preparation of this report.

BIBLIOGRAPHY

McCoy, Neal Henry.
Rings and Ideals. Menasha, Wisconsin: Mathematical Association of America, 1948.

_______.
The Theory of Rings. New York: Macmillan Company, 1964.

Northcott, D.G.
Ideal Theory. London: Cambridge University Press, 1953.

Rosser, J. Barkley.
Logic for Mathematicians. New York: Mcgraw-Hill, 1953.

Van Der Waerden, B.L.
Modern Algebra (Volume I). New York: Fredrick Ungar Publishing Company, 1953.

IDEALS IN A RING

by

RAYMOND CARL SMITH

B. S., Nebraska State Teachers College, 1962
Kearney, Nebraska

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1965

The purpose of this report is to discuss some of the elementary concepts of the theory of ideals in a ring.

An ideal in an arbitrary ring R is defined and some elementary operations on ideals -- addition, multiplication, and intersection -- are considered.

A principal ideal (a) in an arbitrary ring R is defined. It is shown to consist of elements of the form:

$$na + ra + as + \sum r_i a s_i \quad (n \in I, \text{ and } r, s, r_i, s_i \in R).$$

Throughout the remainder of the report the discussion is limited to commutative rings. A principal ideal (a) in a commutative ring R_c is shown to consist of elements of the form: $na + at \quad (n \in I,\ t \in R_c)$.

Prime ideals and the radical of an ideal are considered next. A prime ideal P is shown to coincide with its radical, RadP.

A discussion of minimal prime ideals belonging to an ideal leads to the important result that the radical of an ideal A is the intersection of all minimal prime ideals belonging to A.

Next, the concept "is related to" is discussed and a maximal prime ideal belonging to an ideal is defined. Some properties of maximal prime ideals are discussed. An important result of this discussion is that every minimal prime ideal belonging to A is contained in a maximal prime ideal belonging to A.

Finally, a primary ideal Q is defined and an important relationship among minimal and maximal prime ideals belonging to Q, RadQ, and Q is established. That is, an ideal $Q \neq R_c$ is a primary ideal if and only if there exists a prime ideal P = RadQ which is the unique minimal and maximal prime ideal belonging to Q.