IDEALS AND BOOLEAN RINGS: SOME PROPERTIES

APPROVED:

David R. Cecil
Major Professor

Miles E. Anderson
Minor Professor

John T. Mohat
Director of the Department of Mathematics

Robert B. Toulouse
Dean of the Graduate School

IDEALS AND BOOLEAN RINGS : SOME PROPERTIES

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

Grace Min-Ying Chin Hu, B. A.

Denton, Texas
May, 1968

TABLE OF CONTENTS

CHAPTER I

GENERAL PROPERTIES OF RINGS AND IDEALS

The purpose of this thesis is to investigate certain properties of rings, ideals, and a special type of ring called a Boolean ring.

Definition 1-1. Let A be a given set. A binary operation $\oplus$ on A is a correspondence that associates with each ordered pair (a,b) of elements of A a uniquely determined element $a \oplus b$ of A.

Definition 1-2. A non-empty set G on which there is defined a binary operation $\oplus$ is called a group (with respect to this operation) if G satisfies the following conditions:

G1. The operation $\oplus$ is associative.

If $a,b,c \in G$, then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

G2. There exists in G a unique zero element 0 such that $a \oplus 0 = 0 \oplus a = a$ for every element a in G.

G3. For each element a in G, there exists a unique element -a in G such that $a \oplus (-a) = (-a) \oplus a = 0$.

Operation notation. In order to simplify the notation we write $a \oplus (-b)$ as $a-b$ for $a,b \in R$

Definition 1-3. A group $(G,\oplus)$ is an abelian group if $a \oplus b = b \oplus a$ for every $a,b \in G$.

Definition 1-4. A non-empty set R, in which two binary operations $\oplus$ and $\odot$ are defined, is called a ring if the following conditions are satisfied:

R1. $(R,\oplus)$ is an abelian group.

R2. The operation $\odot$ is associative.

If $a,b,c \in R$, then $(a \odot b) \odot c = a \odot (b \odot c)$.

R3. If $a,b,c \in R$, then

(1) $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ (left distributive law), and

(2) $(b \oplus c) \odot a = b \odot a \oplus c \odot a$ (right distributive law).

Some basic properties of a ring are stated and proved in theorem 1-1.

Theorem 1-1. If $(R,\oplus,\odot)$ is a ring, then the following properties hold for any $a,b,c \in R$:

(1a) $a \odot (b-c) = a \odot b - a \odot c$

(1b) $(b-c) \odot a = b \odot a - c \odot a$

(2) $a \odot 0 = 0 \odot a = 0$

(3) $-(-a) = a$

(4) $(-a) \odot c = a \odot (-c) = -(a \odot c)$

(5) $(-a) \odot (-c) = a \odot c$

Proof: (1) $$\begin{aligned}[a \odot (b-c)] \oplus (a \odot c) &= a \odot [(b-c) \oplus c] \\ &= a \odot [b \oplus (-c \oplus c)] \\ &= a \odot (b \oplus 0) \\ &= a \odot b.\end{aligned}$$

Hence $[a \odot (b-c)] \oplus (a \odot c) = a \odot b$. Now $-(a \odot c)$ is in R for $a \odot c$ in R. Therefore,

$$\{[a \odot (b-c)] \oplus (a \odot c)\} \oplus [-(a \odot c)] = [(a \odot b)] \oplus [-(a \odot c)]$$

$$a \odot (b-c) \oplus \{(a \odot c) \oplus [-(a \odot c)]\} = (a \odot b) \oplus [-(a \odot c)]$$

$$a \odot (b-c) \oplus [(a \odot c) - (a \odot c)] = (a \odot b) - (a \odot c)$$

$$a \odot (b-c) = a \odot b - a \odot c$$

In similar manner, $(b-c) \odot a = b \odot a - c \odot a$ can be shown.

(2) From (1) we have for every $a,b,c \in R$,

$a \odot (b-c) = a \odot b - a \odot c$ and

$(b-c) \odot a = b \odot a - c \odot a$.

Now, let $b = c$, we see that

$$a \odot (c-c) = a \odot c - a \odot c = 0$$

$$a \odot 0 = 0 \text{, and}$$

$$(c-c) \odot a = c \odot a - c \odot a = 0$$

$$0 \odot a = 0.$$

Therefore, $a \odot 0 = 0 \odot a = 0$

(3) If $a = 0$, the proof is trivial.

If $a \neq 0$, then

$$\begin{aligned} a = a \oplus 0 &= a \oplus \{(-a) \oplus [-(-a)]\} \\ &= [a \oplus (-a)] \oplus [-(-a)] \\ &= 0 \oplus [-(-a)] \\ &= -(-a) \end{aligned}$$

(4) From (1a), let $b = 0$, then

$$a \odot (0 - c) = a \odot 0 - (a \odot c)$$

$$\begin{aligned} a \odot (-c) &= 0 - (a \odot c) \\ &= -(a \odot c). \end{aligned}$$

Therefore, $a \odot (-c) = -(a \odot c)$.

From (1b), let $b=0$, then

$(0-c) \odot a = 0 \odot a - c \odot a$,

$(-c) \odot a = 0 - (c \odot a)$.

Therefore, $(-c) \odot a = -(c \odot a) = a \odot (-c)$.

(5) If $a \in R$, then $-a \in R$.

From (1a), let $b = 0$, then

$(-a) \odot (0-c) = (-a) \odot 0 - [(-a) \odot c]$,

$(-a) \odot (-c) = -[(-a) \odot c]$

$= [-(-a) \odot c]$

$= a \odot c$.

Therefore, $(-a) \odot (-c) = a \odot c$.

Before stating and proving theorem 1-2, the following definitions are needed:

Definition 1-5. A ring $(R,\oplus,\odot)$ is a commutative ring if $a \odot b = b \odot a$ for every a,b in R.

Definition 1-6. A ring $(R,\oplus,\odot)$ is a ring with identity if there exists an element e in R such that $a \odot e = e \odot a = a$ for every a in R.

Definition 1-7. If $(R,\oplus,\odot)$ is a ring with identity and there exists an element a^{-1} in R such that $a \odot a^{-1} = a^{-1} \odot a = e$ for $a \in R$, then a^{-1} is called the inverse of a under $\odot$.

Definition 1-8. If an element a in R is such that its inverse a^{-1} is also in R, then a is called a unit in R.

In the ring of integers $(I,+,x)$ the only units are 1 and -1.

The set of units in a ring with identity is denoted by $U = \{a \in R \mid a^{-1} \in R\}$.

With the preceding definitions, theorem 1-2 can now be stated and proved.

Theorem 1-2. Let $(R, \oplus, \odot)$ be a ring with identity; and R has at least two elements. Then

(1) $(R, \odot)$ is not necessarily a group, but $(U, \odot)$ is a group.

(2) The identity e of R is distinct from the zero element of R and there exists no inverse for the zero element of R under $\odot$.

Proof: (1) Consider $U \equiv \{a \in R / a^{-1} \in R\}$; $U \neq \emptyset$ since $e \in U$ for $e \in R$ and $e \odot e = e$ so $e^{-1} = e \in R$. Clearly, $a \in U$ implies that $a^{-1} \in U$. For any $a, b \in U$, we have $a^{-1}, b^{-1} \in R$ and $b^{-1} \odot a^{-1} \in R$. The inverse of $a \odot b$ is $b^{-1} \odot a^{-1}$, since

$$\begin{aligned}(a \odot b) \odot (b^{-1} \odot a^{-1}) &= [(a \odot b) \odot b^{-1}] \odot a^{-1} \\ &= [a \odot (b \odot b^{-1})] \odot a^{-1} \\ &= (a \odot e) \odot a^{-1} \\ &= a \odot a^{-1} \\ &= e \in R.\end{aligned}$$

Since $b^{-1} \odot a^{-1} \in R$, we conclude that $a \odot b \in U$. $U \subseteq R$ so the associative property holds in U. Hence, $(U, \odot)$ forms a group.

(2) Let $a \in R$ such that $a \neq 0$, then $a \odot 0 = 0 \odot a = 0$ and $a \odot e = e \odot a = a$. Therefore, $e \neq 0$. Since $a \odot 0 = 0 \odot a = 0 \neq e$, it follows that 0 has no inverse under $\odot$.

The terms zero divisors and free of zero divisors are introduced in definition 1-9.

Definition 1-9. An element a not equal to the zero element of a ring $(R,\oplus,\odot)$ is called a left (right) zero divisor if there exists in R an element b not equal to the zero element of R such that $a \odot b = 0$ $(b \odot a = 0)$. An element a is called a zero divisor if it is a left and right zero divisor. An element a not equal to the zero element of R is called free of left (right) zero divisors if $a \odot b = 0$ $(b \odot a = 0)$ implies b=0. The element a is called free of zero divisors if it is free of left and right zero divisors.

Theorem 1-3. If $a \in U \equiv \{a \in R / a^{-1} \in R\}$, then a is free of zero divisors.

Proof: From theorem 1-2(2), $a \neq 0$ if $a \in U$. From theorem 1-2(1), if $a \in U$, then $a^{-1} \in U$. If $a \odot b = 0$ for $b \in R$, then $a^{-1} \odot (a \odot b) = (a^{-1} \odot a) \odot b = e \odot b = b$. On the other hand, $a^{-1} \odot (a \odot b) = a^{-1} \odot 0 = 0$ implies that $b = 0$. Hence, a is free of left zero divisors. If $c \odot a = 0$ for $c \in R$, then $(c \odot a) \odot a^{-1} = c \odot (a \odot a^{-1}) = c \odot e = c$. On the other hand, $(c \odot a) \odot a^{-1} = 0 \odot a^{-1} = 0$ implies that $c = 0$. Hence, a is free of right zero divisors. Since a is free of left and right zero divisors, therefore, a is free of zero divisors.

The following two theorems deal with generalized properties of a ring.

Theorem 1-4. If a and b are elements of a ring $(R,\oplus,\odot)$, then the following relations are true:

(1) $b \odot \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} (b \odot a_i)$, and

(2) $(\sum_{i=1}^{n} a_i) \odot b = \sum_{i=1}^{n} (a_i \odot b)$.

Proof: This theorem can be easily proved by mathematical induction.

(1) The relation is true for $n = 1$, since

$$b \odot \sum_{i=1}^{1} a_i = b \odot a_i = \sum_{i=1}^{1} b \odot a_i \ .$$

Let us now assume that the relation is true for $n = k$, that is

$$b \odot \sum_{i=k}^{k} a_i = \sum_{i=k}^{k} b \odot a_i \ .$$

Then,

$$\begin{aligned} b \odot \sum_{i=1}^{k+1} a_i &= b \odot (\sum_{i=1}^{k} a_i \oplus a_{k+1}) \\ &= \left[b \odot \sum_{i=1}^{k} a_i\right] \oplus \left[b \odot a_{k+1}\right] \\ &= \left[\sum_{i=1}^{k} (b \odot a_i)\right] \oplus (b \odot a_{k+1}) \\ &= \sum_{i=1}^{k+1} (b \odot a_i) \ . \end{aligned}$$

The above result shows that it is true for $n = k+1$. This completes the proof.

(2) In the similar manner the relation (2) can be proved. For $n = 1$, the relation (2) is true.

$$(\sum_{i=1}^{1} a_i) \odot b = a_1 \odot b = \sum_{i=1}^{1} a_i \odot b \ .$$

Assume that it is true for $n = k$, that is

$$(\sum_{i=1}^{k} a_i) \odot b = \sum_{i=1}^{k} (a_i \odot b).$$

Then we obtain the following result :

$$(\sum_{i=1}^{k+1} a_i) \odot b = (\sum_{i=1}^{k} a_i \oplus a_{k+1}) \odot b$$

$$= \left[(\sum_{i=1}^{k} a_i) \odot b\right] \oplus \left[a_{k+1} \odot b\right]$$

$$= \left[\sum_{i=1}^{k} (a_i \odot b)\right] \oplus \left[a_{k+1} \odot b\right]$$

$$= \sum_{i=1}^{k+1} (a_i \odot b) .$$

The result shows that $n = k+1$ is true, and hence we have verified theorem 1-4(2).

<u>Theorem</u> <u>1-5</u>. If a and b are elements of a ring $(R,\oplus,\odot)$, then the following property is true, where n is an arbitrary positive integer:

$$n(a \odot b) = (na) \odot b = a \odot (nb) .$$

Proof: Let $b_1=b_2=b_3= \cdots\cdot=b_k=b_{k+1}=\cdots=b_n=b$. Then it is easy to verify $\sum_{i=1}^{n} b_i = nb$ by mathematical induction. If $n=1$, then $\sum_{i=1}^{n} b_i = nb$ obviously holds, since $b_1=b=1b$. If the same holds for $n=k$, then for $n=k+1$,

$$\sum_{i=1}^{k+1} b_i = \sum_{i=1}^{k} b_i \oplus b_{k+1} = kb \oplus b_{k+1} = kb \oplus b = (k+1)b .$$

Hence, by induction, for any positive integers n, $\sum_{i=1}^{n} b_i=nb$.

Now we obtain the following results:

$$a \odot \sum_{i=1}^{n} b_i = a \odot nb, \text{ and}$$

$$\sum_{i=1}^{n} (a \odot b_i) = n(a \odot b), \text{ if } a \odot b_1 = \cdots = a \odot b_n = a \odot b.$$

From theorem 1-4(1), hence we have $a \odot (nb) = n(a \odot b)$.

Similarly, we have

$$\sum_{i=1}^{n} (a_i \odot b) = n(a \odot b) \quad \text{and} \quad \left(\sum_{i=1}^{n} a_i\right) \odot b = (na) \odot b,$$

if $a_1 \odot b = a_2 \odot b = \cdots = a_n \odot b = a \odot b$, and $a_1 = a_2 = \cdots = a_n = a$.

From theorem 1-4(2), hence we have $n(a \odot b) = (na) \odot b$.

Therefore, $n(a \odot b) = (na) \odot b = a \odot (nb)$.

The commutative property under $\oplus$ is necessary for a ring with identity. This is discussed in the next theorem.

<u>Theorem</u> <u>1-6</u>. If $(R, \oplus, \odot)$ is an algebraic system satisfying all the conditions for a ring with identity with the exception of $a \oplus b = b \oplus a$, then the relation $a \oplus b = b \oplus a$ must hold in R and R is thus a ring.

Proof: Let e be the identity of R, and $(a \oplus b) \in R$ and $(e \oplus e) \in R$ for every a,b in R. Then

$$\begin{aligned}(a \oplus b) \odot (e \oplus e) &= [(a \oplus b) \odot e] \oplus [(a \oplus b) \odot e] \\ &= [(a \odot e) \oplus (b \odot e)] \oplus [(a \odot e) \oplus (b \odot e)] \\ &= (a \oplus b) \oplus (a \oplus b),\end{aligned}$$

and also

$$\begin{aligned}(a \oplus b) \odot (e \oplus e) &= [a \odot (e \oplus e)] \oplus [b \odot (e \oplus e)] \\ &= [(a \odot e) \oplus (a \odot e)] \oplus [(b \odot e) \oplus (b \odot e)] \\ &= (a \oplus a) \oplus (b \oplus b).\end{aligned}$$

Hence, $(a \oplus b) \oplus (a \oplus b) = (a \oplus a) \oplus (b \oplus b)$.

Now, since $a,b \in R$ implies $-a,-b \in R$, then

$$-a \oplus [(a \oplus b) \oplus (a \oplus b)] \oplus (-b) = -a \oplus [(a \oplus a) \oplus (b \oplus b)] \oplus (-b),$$

$$[(-a) \oplus a] \oplus [(b \oplus a)] \oplus [b \oplus (-b)] = [(-a) \oplus a] \oplus [(a \oplus b)] \oplus [b \oplus (-b)],$$

$$0 \oplus (b \oplus a) \oplus 0 = 0 \oplus (a \oplus b) \oplus 0 ,$$

hence $b \oplus a = a \oplus b$.

Therefore, $a \oplus b = b \oplus a$ holds and R is a ring, and the proof is completed.

The necessary and sufficient conditions for a subgroup and a subring are discussed in the following definitions.

Definition 1-10. A non-empty subset S of a group $(G,+)$ is a subgroup if $(S,+)$ itself is a group.

If $(S,+)$ is a group, then for any element c in S there exists $-c$ in S such that $a + (-c) = a - c \in S$ whenever $a \in S$.

If S is a non-empty subset of G such that $a - c \in S$, then $a-a = 0 \in S$ and $0 - c = -c \in S$. Now $-(-c) = c$ by theorem 1-1(3), we therefore see that $a-(-c) = a+c \in S$. Since $S \subseteq R$, hence S is a group. Therefore, for any $a,c \in S$, $a-c \in S$ is a necessary and sufficient condition for a non-empty subset S to be a subgroup in G.

Definition 1-11. A non-empty subset B of a ring $(R,\oplus,\odot)$ is a subring of R if $(B,\oplus,\odot)$ itself is a ring.

If $(B,\oplus,\odot)$ is a ring, then $(B,\oplus)$ must be a subgroup of $(R,\oplus)$ which implies $a-c \in B$ for any $a,c \in B$. Furthermore, $a \odot c \in B$. If B is a non-empty subset of R and $a-c \in B$ for any $a, c \in B$, then $(B, \oplus)$ is a subgroup of $(R, \oplus)$. The condition $a \odot c \in B$ assures us of all conditions necessary for $(B, \oplus, \odot)$ to be a ring. Therefore, for any $a, c \in B$, $a - c \in B$ and $a \odot c \in B$ are necessary and sufficient conditions for a subring B in R.

The identity of a ring and the identity of its subring are of great interest. They are discussed in theorem 1-7.

Theorem 1-7. Let S be a subring of $(R, +, \cdot)$. The following statements are true:

(1) If R has identity e, then S may not have one. But if e is in S, then e is an identity in S,

(2) If e is an identity of R and e' is an identity of S and $e \notin S$, then $e \neq e'$,

(3) If S has the identity e' and R does not have one, then e' is necessarily a zero divisor of R.

Proof: (1) Consider the ring of integers I and let S be the set of all even integers in I. For any $a, c \in S$, $a - c \in S$ and $a \times c \in S$, S is a subring of I. I has the identity 1 where $1 \in I$ but $1 \notin S$. Hence $(S, +, x)$ forms a subring in I without an identity. However, if $e \in S$ such that e is the identity of R, then $a \odot e = e \odot a = a$ for any $a \in R$. Suppose there exists an element b in S such that $b \odot e \neq b$, and $S \subseteq R$ implies that $b \in R$. This leads to a contradiction. Therefore, e is the identity of S.

(2) Consider the set $R \equiv \{(a, b) / a \in A \text{ and } b \in B\}$ where $(A, \underset{a}{+}, \underset{a}{\cdot})$ and $(B, \underset{b}{+}, \underset{b}{\cdot})$ are two rings. Define

$$+ \equiv \left\{\left[(a,b),(c,d)\right], (a \underset{a}{+} c,\ b \underset{b}{+} d) / \ a,c \in A \text{ and } b,d \in B\right\}, \text{ and}$$

$$\cdot \equiv \left\{\left[(a,b),(c,d)\right], (a \underset{a}{\cdot} c,\ b \underset{b}{\cdot} d) / \ a,c \in A \text{ and } b,d \in B\right\},$$

where $(a,b) = (c,d)$ if and only if $a = c$ and $b = d$.

$(R,+,\cdot)$ is a ring and the proof is as follows. Let $r_1 = (a,b)$, $r_2 = (c,d)$, $r_3 = (a',b')$ and $r_4 = (c',d')$. If $r_1 = r_3$ and $r_2 = r_4$, then $a=a'$, $b=b'$, $c=c'$ and $d=d'$. It follows that $a \underset{a}{+} c = a' \underset{a}{+} c'$, $b \underset{b}{+} d = b' \underset{b}{+} d'$ and $(a \underset{a}{+} c,\ b \underset{b}{+} d) = (a' \underset{a}{+} c', b' \underset{b}{+} d')$. Hence $(a,b) + (c,d) = (a',b') + (c',d')$, that is,

$$r_1 + r_2 = r_3 + r_4 .$$

Therefore, $+$ is a binary operation. Since $a \underset{a}{\cdot} c = a' \underset{a}{\cdot} c'$ and $b \underset{b}{\cdot} d = b' \underset{b}{\cdot} d'$, then

$$\begin{aligned} r_1 \cdot r_2 &= (a,b) \cdot (c,d) \\ &= (a \underset{a}{\cdot} c,\ b \underset{b}{\cdot} d) \\ &= (a' \underset{a}{\cdot} c',\ b' \underset{b}{\cdot} d') \\ &= (a',b') \cdot (c',d') \\ &= r_3 \cdot r_4 . \end{aligned}$$

Hence $r_1 \cdot r_2 = r_3 \cdot r_4$. Therefore, $\cdot$ is a binary operation.

For $(a,b),(c,d),(e,f) \in R$, we have

$$\begin{aligned} \left[(a,b) + (c,d)\right] + (e,f) &= (a \underset{a}{+} c,\ e \underset{b}{+} d) + (e,f) \\ &= \left[(a \underset{a}{+} c) \underset{a}{+} e, (b \underset{b}{+} d) \underset{b}{+} f\right] \\ &= \left[a \underset{a}{+} (c \underset{a}{+} b),\ b \underset{b}{+} (d \underset{b}{+} f)\right] \\ &= (a,b) + (c \underset{a}{+} e,\ d \underset{b}{+} f) \\ &= (a,b) + \left[(c,d) + (e,f)\right] . \end{aligned}$$

Since A and B are rings for any $a \in A$ and $b \in B$, there exists $-a \in A$ and $-b \in B$. For any $(a,b) \in R$, we have

$$(a,b) + (-a,-b) = (a-a, b-b) = (0_a, 0_b) \in R ,$$

$$(0_a, 0_b) + (a,b) = (0_a \underset{a}{+} a,\ 0_b \underset{b}{+} b) = (a,b) , \quad \text{and}$$

$$(a,b) + (c,d) = (a \underset{a}{+} c,\ b \underset{b}{+} d) = (c \underset{a}{+} a,\ d \underset{b}{+} b) = (c,d) + (a,b).$$

Therefore, $(R,+)$ is an abelian group.

$$\begin{aligned}
(a,b) \cdot \left[(c,d) \cdot (e,f)\right] &= (a,b) \cdot (c \underset{a}{\cdot} e,\ d \underset{b}{\cdot} f) \\
&= \left[a \underset{a}{\cdot} (c \underset{a}{\cdot} e),\ b \underset{b}{\cdot} (d \underset{b}{\cdot} f)\right] \\
&= \left[(a \underset{a}{+} c) \underset{a}{\cdot} e,\ (b \underset{b}{\cdot} d) \underset{b}{\cdot} f\right] \\
&= \left[(a \underset{a}{\cdot} c,\ b \underset{b}{\cdot} d) \cdot (e,f)\right] \\
&= \left[(a,b) \cdot (c,d)\right] \cdot (e,f) .
\end{aligned}$$

$$\begin{aligned}
(a,b) \cdot \left[(c,d) + (e,f)\right] &= (a,b) \cdot (c \underset{a}{+} e,\ d \underset{b}{+} f) \\
&= \left[a \underset{a}{\cdot} (c \underset{a}{+} e),\ b \underset{b}{\cdot} (d \underset{b}{+} f)\right] \\
&= \left[(a \underset{a}{\cdot} c) \underset{a}{+} (a \underset{a}{\cdot} e), (b \underset{b}{\cdot} d) \underset{b}{+} (b \underset{b}{\cdot} f)\right] \\
&= (a \underset{a}{\cdot} c,\ b \underset{b}{\cdot} d) + (a \underset{a}{\cdot} e,\ b \underset{b}{\cdot} f) \\
&= \left[(a,b) \cdot (c,d)\right] + \left[(a,b) \cdot (e,f)\right] .
\end{aligned}$$

A similar proof holds for right distributive law. Hence $(R,+,\cdot)$ is a ring.

Let $S \equiv \{(a,0) \,/\, a \in A$ and 0 is zero element in $B\}$. $A \neq \emptyset$ and $B \neq \emptyset$ imply that $S \neq \emptyset$. For any $(a,0),(b,0) \in S$, we have

$$(a,0) + (b,0) = (a \underset{a}{+} b,\ 0 \underset{b}{+} 0) = (a \underset{a}{+} b, 0) \in S$$

$$(a,0) \cdot (b,0) = (a \underset{a}{\cdot} b,\ 0 \underset{b}{\cdot} 0) = (a \underset{a}{\cdot} b, 0) \in S$$

$-b \in A$ for $b \in A$ implies $(-b,0) = -(b,0) \in S$,
hence, $(a,0) - (b,0) = (a-b, 0 \underset{b}{+} 0) = (a-b,0) \in S$. Therefore, $(S,+,\cdot)$ forms a subring of $(R,+,\cdot)$.

Since $(a,0) \cdot (e_a,0) = (a \underset{aa}{\cdot} e, 0 \underset{b}{\cdot} 0) = (a,0)$ for any $(a,0) \in S$, if A is a ring with identity, then S is a ring with identity. Since $(a,b) \cdot (e_a,e_b) = (a \underset{aa}{\cdot} e, b \underset{bb}{\cdot} e) = (a,b)$ for any $(a,b) \in R$, if B is also a ring with identity, then R is a ring with identity.

Let $e = (e_a,e_b)$ and $e' = (e_a,0)$. The ring R has an identity if and only if A and B both are rings with identities. From theorem 1-2(2), it follows that $0_b \neq e_b$. Hence , we have $e = (e_a,e_b) \neq (e_a,0) = e'$ and $e = (e_a,e_b) \notin S$. Therefore, we conclude that identity e of a ring may be different from the identity e' of its subring, if e is not an element of the subring.

(3) Let e' be the identity of S. From theorem 1-2(2), we have $e' \neq 0' \in S$. Suppose $e' \cdot a = b \neq a$ for some $a \in R$, then $e' \cdot b = e' \cdot (e' \cdot a) = (e' \cdot e') \cdot a = e' \cdot a$ which implies $e' \cdot b = e' \cdot a$. Since $-(e' \cdot a) \in R$, then $(e' \cdot b) + [-(e' \cdot a)] = (e' \cdot a) + [-(e' \cdot a)] = 0$. By theorem 1-1(4), it follows

$$\begin{aligned} (e' \cdot b) + [e' \cdot (-a)] &= e' \cdot [b + (-a)] \\ &= e' \cdot (b-a) \\ &= 0 \end{aligned}$$

Since $b \neq a$ implies $b-a \neq 0$, hence e' is a left zero divisor.

A similar proof holds for e' being a right zero divisor. Therefore, e' of S in this case is a zero divisor.

Ideals are non-empty subsets of a ring. They play important roles in the study of rings.

Definition 1-12. A non-empty subset I of a ring R is said to be a left (right) ideal of R if

(1) $(I,\oplus)$ is a subgroup of $(R,\oplus)$, and

(2) $i \in I$, $r \in R$ implies that $r \odot i \in I$ ($i \odot r \in I$).

If I is a left ideal and is also a right ideal, then I is called an ideal.

Some important properties of ideals are stated and proved in the following set of theorems.

Theorem 1-8. If R is a commutative ring and $a \in R$, then $T = a \odot R$ is an ideal, where $a \odot R = \{a \odot r \mid r \in R\}$.

Proof: Since $R \neq \emptyset$, it follows that $T \neq \emptyset$. If $a \odot r_1$ and $a \odot r_2$ are two elements in T, then

$$\begin{aligned}(a \odot r_1) \oplus [-(a \odot r_2)] &= (a \odot r_1) \oplus [a \odot -(r_2)] \\ &= a \odot [r_1 + (-r_2)] \\ &= a \odot (r_1 - r_2) \in T\end{aligned}$$

for $(r_1-r_2) \in R$. Hence, $(T,\oplus)$ is a subgroup of $(R,\oplus)$.

For any $a \odot r_1 \in T$ and $r_2 \in R$, $(a \odot r_1) \odot r_2 = a \odot (r_1 \odot r_2) \in T$. Hence, T is a right ideal in R. Since $T \subseteq R$ for any $a \odot r \in T$, therefore, $a \odot r = r \odot a \in T$ which proves that T is an ideal in R.

Theorem 1-9. If R is a ring and $a \in R$, and let $r(a) \equiv \{x \in R \mid a \odot x = 0\}$, then $r(a)$ is a right ideal in R.

Proof: It is trivial that $r(a) \neq \emptyset$. For every $x,y \in r(a) \subseteq R$, by hypothesis, $a \odot x = 0$ and $a \odot y = 0$. This implies that $a \odot x - a \odot y = 0$ and $a \odot (x-y) = 0$. Hence, $x-y \in r(a)$.

Therefore, $(r(a),\oplus)$ is a subgroup of $(R,\oplus)$. If $y \in r(a)$ and $b \in R$, then $a \odot (y \odot b) = (a \odot y) \odot b = 0 \odot b = 0$. Hence $y \odot b \in r(a)$ and the proof is completed.

Theorem 1-10. Let I_{l1} and I_{l2} be two left ideals in R and suppose $(I_{l1} \cap I_{l2}) \neq \emptyset$, then the intersection of two left ideals is a left ideal.

Proof: Since $(I_{l1} \cap I_{l2}) \subseteq I_{l1}$, $(I_{l1} \cap I_{l2}) \subseteq I_{l2}$ and $b \in (I_{l1} \cap I_{l2})$ implies that $-b \in I_{l1}$ and $-b \in I_{l2}$. By the uniqueness of the inverse of b under $\oplus$, it follows $-b \in (I_{l1} \cap I_{l2})$. Furthermore, $a \oplus (-b) = a - b \in (I_{l1} \cap I_{l2})$ for any a,b in $(I_{l1} \cap I_{l2})$. Hence $(I_{l1} \cap I_{l2}, \oplus)$ is a subgroup of $(R,\oplus)$. For $r_1 \in R$, $r_1 \odot a \in I_{l1}$ and $r_1 \odot a \in I_{l2}$ which imply that $r_1 \odot a \in (I_{l1} \cap I_{l2})$ for $a \in (I_{l1} \cap I_{l2})$. Therefore, $(I_{l1} \cap I_{l2})$ is a left ideal of R.

A similar proof can be shown that the intersection of two right ideals is a right ideal.

Now consider the intersection of a right and a left ideal of R and $(I_l \cap I_r) \neq \emptyset$. Since $(I_l \cap I_r) \subseteq I_l$ and $(I_l \cap I_r) \subseteq I_r$ for any $a,b \in (I_l \cap I_r)$, then $(a-b) \in (I_l \cap I_r)$. Hence $(I_l \cap I_r, \oplus)$ is a subgroup of $(R,\oplus)$. If R is a commutative ring, and $r_1 \in R$, $r_1 \odot a \in I_l$ and $a \odot r_1 \in I_r$ where $a \in (I_l \cap I_r)$, then $r_1 \odot a = a \odot r_1 \in I_r$ and $r_1 \odot a \in I_l$. This implies $r_1 \odot a = a \odot r_1 \in (I_l \cap I_r)$ and $(I_l \cap I_r)$ is an ideal. If R is not a commutative ring, then $(I_l \cap I_r)$ is not an ideal.

A ring R has at least two ideals; the entire ring R and the set (0) consisting of the zero element only. An ideal of R distinct from (0) and R will be called a proper ideal.

A special type of ideal known as principal ideal is introduced and discussed in the following definition and theorem 1-11.

Definition 1-13. An ideal I_p is called a principal ideal of a ring R if every element of I_p is some multiple of a. Denote I_p by (a) for such an ideal, that is, $(a) \equiv \{x \cdot a \mid x \in R\}$.

Theorem 1-11. Every ideal in the ring of integers is principal.

Proof: (1) If I= (0), then I is a principal ideal.

(2) If $I \neq (0)$, then $c \neq 0$ for some $c \in I$. Since $c \in I$ and $-c \in I$, it follows $c > 0$ or $-c > 0$. Let a be the smallest positive integer in I, then there exists $b \in I$ such that

$$b = qxa + r \quad , \text{ where } q \in R \text{ and } 0 \leq r < a.$$

Since $qxa \in I$ and $-(qxa) \in I$, it follows $b-(qxa)=(qxa+r)-(qxa)$ $=(qxa) - (qxa) + r = 0 + r = r$ and $b-(qxa)=r \in I$, a being the smallest positive integer such that $0 \leq r < a$. Hence $b-(qxa) = r = 0$ and $b = qxa$. Therefore I= (a).

A sfield and a field can not have proper ideals. This will be shown in the next two theorems.

Definition 1-14. A ring D^* is called a sfield if it contains more than one element, and for every $a \in D^*$, $a \neq 0$, the equation $a \cdot x = b$ has a solution for any $b \in D^*$.

<u>Theorem 1-12</u>. A sfield $(D^*, +^*, \cdot^*)$ has no proper ideals.

Proof: Let I^* be an ideal in D^* such that $I^* \neq (0)$, $I^* \neq \emptyset$, and $I^* \subseteq D^*$. Suppose that $a, b \in D^*$, where $a \neq 0$, $b \neq 0$; then, by the definition of sfield, there exists $x \in D^*$ such that $a \cdot^* x = b$ and also $y \in D^*$ such that $x = b \cdot^* y$, that is,

$$a \cdot^* x = a \cdot^* (b \cdot^* y) = (a \cdot^* b) \cdot^* y = b \neq 0$$

which implies, by definition of sfield, $a \neq 0$ and $b \neq 0$. It follows $a \cdot^* b \neq 0$. Therefore, D^* has no proper zero divisors. Let $a, e \in D^*$ such that $a \neq 0$, $e \neq 0$ and $a \cdot^* e = a$. Then,

$$\begin{aligned} a \cdot^* e^2 &= a \cdot^* (e \cdot^* e) \\ &= (a \cdot^* e) \cdot^* e \\ &= a \cdot^* e \quad . \end{aligned}$$

It follows

$$\begin{aligned} (a \cdot^* e^2) - (a \cdot^* e) &= 0 \\ a \cdot^* (e^2 - e) &= 0 \quad . \end{aligned}$$

Therefore, $e^2 = e$. Furthermore, for any $c \in D^*$, we have $c \cdot^* e^2 = c \cdot^* e$ and $(c \cdot^* e - c) \cdot^* e = 0$. Since $e \neq 0$, we obtain $c \cdot^* e = c$. Similarly, we also obtain $e \cdot^* c = c$. For any $c \in D^*$, $c \cdot^* e = c = e \cdot^* c$. Therefore, e is the identity in D^*.

By the same definition, $a \cdot^* x = e$ has a solution in D^* which implies $a^{-1} \in D^*$. If $b \in I^*$ and $b^{-1} \in D^*$, then $b \cdot^* b^{-1} = e \in I^*$. Since $e \cdot^* y = y \cdot^* e = y \in I^*$ and $D^* \subseteq I^*$ and $I^* \subseteq D^*$, therefore, $I^* = D^*$.

<u>Definition 1-15</u>. A commutative ring F is called a field if the following conditions are satified :

F_1. F has at least two elements.

F_2. F has an identity.

F_3. Every $a \in F$ such that $a \neq 0$ has an inverse a^{-1} in F.

Theorem 1-13. A commutative ring R with identity is a field if and only if R has no proper ideals.

Proof: If R is a field and if I is an ideal of R such that $I \neq (0)$, then there exists an element $a \neq 0$ such that $a \in I$. For R to be a field, a^{-1} must be in R. Hence, by definition of ideal, $a \cdot a^{-1} = e \in I$. Let $y \in R$, then $e \cdot y \in I$. Since $R \subset I$ and $I \subset R$, therefore, $I = R$. Conversely, if R ia a commutative ring with identity and R has no proper ideals, and also if $a \in R$ and $a \neq 0$, then consider the set $R_a = \{ r \cdot a \mid r \in R \}$. By theorem 1-8, R_a is an ideal in R. Since $R_a \neq (0)$ implies $R_a = R$, and $e \in R = R_a$ implies $e = x \cdot a$ for some $x \in R$, hence R is a field.

The following definitions concern certain important mappings between rings, and some basic properties of homomorphisms are stated and proved in theorem 1-14 through theorem 1-16.

Definition 1-16. (1) A mapping from a ring R into a ring R' is a correspondence that associates with each element $r \in R$ a unique $r' \in R'$.

(2) A mapping T from a ring $(R,+,\cdot)$ into a ring $(R',+',\cdot')$ is a homomorphism if

$$(a+b)T = aT +' bT \quad , \text{ and}$$

$$(a \cdot b)T = aT \cdot' bT \quad \text{for all } a.b \in R.$$

(3) A mapping T is said to be from a ring R onto a ring R' if for any $b' \in R'$ there exists at least one element $a \in R$ such that $aT = b'$.

(4) A mapping T is said to be a one to one mapping of a ring R into R' if for any $a, b \in R$ with $a \neq b$, then $aT \neq bT$.

(5) If T is a one to one homomorphic mapping from ring R onto ring R', then T is called an isomorphism.

Definition 1-17. If T is a homomorphic mapping from a ring R into a ring R', then the kernal of T (denoted by $\ker(T)$) is the set of all elements of R which are mapped into the zero element of R'.

Theorem 1-14. If T is a homomorphism of a ring $(R,+,\cdot)$ into a ring $(R',+',\cdot')$, then

(1) $0T = 0'$

(2) $(-a)T = -(aT)$

(3) $\text{Ker}(T)$ is a subring of R.

Proof: (1)

$$0 = 0 + 0$$
$$0T = (0 + 0)T$$
$$= 0T +' 0T$$

Since $0T = 0' +' 0T$, then $0' +' 0T = 0T = 0T +' 0T$. Now $-(0T) \in R'$ if $0T \in R'$. It follows that

$$(0' +' 0T) - (0T) = (0T +' 0T) - (0T)$$
$$0' +' (0T - 0T) = 0T +' (0T - 0T)$$
$$0' = 0T$$

(2)

$$0 = (a + (-a))$$
$$0T = ((a + (-a))T = aT +' (-a)T$$

From (1) we have $0' = 0T$, hence $0' = aT +' (-a)T$. Since $aT +' (-(aT)) = 0'$, thus we obtain the relation

$$aT +' (-a)T = aT +' (-(aT)) = 0'$$

R' is a ring, hence if $aT \in R'$, then $-(aT) \in R'$. Therefore, we have

$$-(aT) +' [aT +' (-a)T] = -(aT) +' [aT +' (-(aT))]$$

$$[-(aT) +' aT] +' (-a)T = [-(aT) +' aT] +' [-(aT)]$$

$$(-a)T = -(aT)$$

(3) Let $0'$ be the zero element of R' and for any $a,b \in Ker(T)$, then

$$\begin{aligned}(a-b)T &= [a + (-b)]T \\ &= aT +' (-b)T \\ &= aT - bT \\ &= 0' - 0' \\ &= 0'\end{aligned}$$

Hence $(a-b) \in Ker(T)$, and $(Ker(T),+)$ is a subgroup of $(R,+)$. Also $(a \cdot b)T = aT \cdot' bT = 0' \cdot' 0' = 0'$. Hence $a \cdot b \in Ker(T)$, and $(Ker(T),+,\cdot)$ is a subring of the ring $(R,+,\cdot)$.

Theorem 1-15. A homomorphism T from ring $(R,+,\cdot)$ onto ring $(R',+',\cdot')$ is an isomorphism if and only if $Ker(T)$ consists of zero element of R only.

Proof: Suppose T is a isomorphism. For $a,b \in R$, $aT = a'$ and $bT = b'$ with $a',b' \in R'$, and if c is any element in $Ker(T)$, then $(c+a)T = (a+c)T = aT +' cT = aT +' 0' = aT = a'$ and $(a+c)T = aT +' cT = aT +' 0'$. Since T is isomorphism and

$OT = 0'$, hence $CT = OT = 0'$ and $c = 0 \in R$. If Ker(T)=(0), then let r_1, r_2 R such that $r_1T = r_2T$. Since

$$\begin{aligned}(r_1 - r_2)T &= r_1T + (-r_2)T \\ &= r_1T - r_2T \\ &= 0' ,\end{aligned}$$

hence $r_1 - r_2 \in$ Ker(T). Since Ker(T) = (0), it follows that $r_1 - r_2 = 0$ and $r_1 = r_2$. So we have shown that T is a one to one mapping. Therefore, with hypothesis, T is an isomorphism.

<u>Definition 1-18</u>. A commutative ring with identity and having no zero divisors is called an integral domain.

<u>Theorem 1-16</u>. Let ϕ be a homomorphic mapping from a ring $(R,+,\cdot)$ with identity e into a ring $(R',+',\cdot')$ with identity e', then $e\phi$ is the identity of

$$R\phi = \{ r' \in R' / \exists\, r \in R \ni r0 = r' \}$$

where $e\phi$ is not necessarily equal to $e' \in R'$. If R' is an integral domain or R' is any ring with ϕ an onto mapping, then $e\phi = e'$.

Proof: Since $e\phi \cdot' a\phi = (e \cdot a)\phi = a\phi$ and $a\phi \cdot' e\phi = (a \cdot e)\phi = a\phi$ for any $a\phi \in R\phi$, hence $e\phi$ is identity of $R\phi$. If $a \cdot b \in R$, $a+b \in R$, and $a\phi, b\phi \in R\phi$, then

$$a\phi \cdot' b\phi = (a \cdot b)\phi \in R\phi$$
$$a\phi +' b\phi = (a+b)\phi \in R\phi .$$

For $a-b \in R$, we have $a\phi - b\phi = a\phi +' (-(b\phi)) = (a + (-b))\phi = (a-b)\phi \in R\phi$. Therefore, $(R\phi,+',\cdot')$ is a subring of $(R',+',\cdot')$.

By theorem 1-7, we see that $e\phi = e'' \in R\phi$ is not necessarily equal to e' of R'. If R' is an integral domain and suppose $e' \neq e\phi$ for $e' \in R'$ and $e\phi \in R\phi$, then $e\phi \cdot' a' = b' \neq a'$ for some $a' \in R'$. Now we have

$$\begin{aligned} e\phi \cdot' b' &= e\phi \cdot' (e\phi \cdot' a') \\ &= (e\phi \cdot' e\phi) \cdot' a' \\ &= e\phi \cdot' a' , \end{aligned}$$

hence $e\phi \cdot' b' = e\phi \cdot' a'$. Since $e\phi \cdot' (b'-a') = 0'$, by hypothesis, R' is an integral domain and $e\phi \neq 0'$. Hence $b' = a'$. This leads to a contradiction. Therefore, $e' = e\phi$. If ϕ is a homomorphic mapping from R onto R', then for any $a' \in R'$ there exists at least an element $a \in R$ such that $a\phi = a'$. Since $e\phi \in R\phi \subseteq R'$, and also

$$e\phi \cdot' a\phi = (e \cdot a)\phi = a\phi = a' \quad \text{and}$$

$$a\phi = (a \cdot e)\phi = a\phi \cdot e\phi ,$$

hence we obtain $e\phi \cdot' a\phi = a\phi \cdot' e\phi = a\phi = a'$. Therefore $e\phi$ is the identity of R' for any $a' \in R'$.

With the aid of the definition of ideal, a special type of ring called quotient ring can be constructed. Some basic properties of the quotient ring will be examined in the remainder of this chapter.

Definition 1-19. If R is a ring and I is an ideal of R, then the set $Q = I + r = \{ i+r \mid i \in I \}$, where $r \in R$, is called a residue class in R.

If $I+r_1 \neq I+r_2$, and if there exists an element $c \in I+r_1$

and $c \in I+r_2$, then there exists $i_1, i_2 \in I$ such that $c=i_1+r_1$ and $c=i_2+r_2$. Since I is an ideal and $-i_1 \in I$ for $i_1 \in I$, then

$$\begin{aligned} i_1 + r_1 &= i_2 + r_2 \\ (-i_1)+(i_1+r_1) &= (-i_1) + (i_2+r_2) \\ (-i_1+i_1) + r_1 &= (-i_1+i_2) + r_2 \end{aligned}$$

Let $-i_1+i_2=i_3$; hence $r_1=i_3+r_2$ and $I+r_1=I+(i_3+r_2)=(I+i_3)+r_2 =I+r_2$. We conclude that for any $I+r_1, I+r_2 \in Q$, if $I+r_1 \neq I+r_2$, then $I+r_1$ and $I+r_2$ have no elements in common.

<u>Theorem 1-17</u>. The set Q of residue classes of an ideal I in a ring $(R,+,\cdot)$ is itself a ring.

Proof: Define $\boxplus$ and $\boxdot$ in the set Q as follows:

$$\boxplus \equiv \{ (I+a, I+b), \ I+(a+b) \mid I+a, I+b \in Q \}$$

$$\boxdot \equiv \{ (I+a, I+b), \ I+(a\cdot b) \mid I+a, I+b \in Q \}.$$

For $x,y,w,z \in Q$, suppose $x=I+a_1$, $y=I+a_2$, $z=I+a_3$, $w=I+a_4$ such that $x=z$ and $y=w$. Let $s \in I+(a_1+a_2)$, then there exists $i_1 \in I$ such that $s=i_1+(a_1+a_2) =(i_1+a_1)+a_2$. Since $I+a_1=I+a_3$, there exists $i_2 \in I$ such that $i_1+a_1=i_2+a_3$; hence

$$\begin{aligned} s &= (i_2+a_3) + a_2 \\ &= i_2 + (a_3+a_2) \\ &= (i_2+a_2) + a_3 \end{aligned}$$

Since $I+a_2=I+a_4$, then there exists $i_3 \in I$ such that $i_2+a_2=i_3+a_4$. Hence $s=(i_3+a_4)+a_3= i_3+(a_4+a_3) = i_3+(a_3+a_4)$ which is an element of $I+(a_3+a_4)$. This implies that

$I+(a_1+a_2) \subseteq I+(a_3+a_4)$. If $t \in I+(a_3+a_4)$, then there exists $i_4 \in I$ such that $t=i_4+(a_3+a_4)=(i_4+a_3)+a_4$. Since $I+a_1=I+a_3$, there exists $i_5 \in I$ such that $i_5+a_1=i_4+a_3$

$$\begin{aligned} t &= (i_5+a_1) + a_4 \\ &= i_5 + (a_1+a_4) \\ &= i_5 + (a_4+a_1) \\ &= (i_5+a_4) + a_1 \end{aligned}$$

Since $I+a_2=I+a_4$, there exists $i_6 \in I$ such that $i_6+a_2=i_5+a_4$. Hence $t=(i_6+a_2)+a_1 = i_6+(a_2+a_1) = i_6+(a_1+a_2) \quad I+(a_1+a_2)$. Therefore $I+(a_3+a_4) \quad I+(a_1+a_2)$ and $I+(a_1+a_2)=I+(a_3+a_4)$. Therefore $\boxplus$ is a binary operation.

Suppose $s' \in I+a_1 \cdot a_2$; then there exists $i_1' \in I$ such that $i' = i_1' + a_1 \cdot a_2$. Since $I+a_1=I+a_3$, there exists $i_2', i_3' \in I$ such that $i_2'+a_1=i_3'+a_3$. Since $(I,+)$ is a subgroup of $(R,+)$, then there exists $-i_2' \in I$ such that $-i_2'+(i_2'+a_1)= -i_2'+(i_3'+a_3)$. It follows that $(-i_2'+i_2')+a_1= (-i_2'+i_3')+a_3$. Let $i_3'-i_2'=i_4' \in I$, then $a_1=i_4'+a_3$. Since $I+a_2=I+a_4$, there exists $i_5', i_6' \in I$ such that $i_5'+a_2=i_6'+a_4$ and $-i_5' \in I$. Now

$$\begin{aligned} -i_5' + (i_5'+a_2) &= -i_5' + (i_6'+a_4) \\ (-i_5'+i_5') + a_2 &= (-i_5'+i_6') + a_4 \end{aligned}$$

Let $i_7'=-i_5'+i_6'$, then $a_2=i_7'+a_4$.

$$s' = i_1' + a_1 \cdot a_2$$

$$s' = i_1' + a_1 \cdot a_2$$
$$= i_1' + (i_4' + a_3) \cdot (i_7' + a_4)$$
$$= i_1' + (i_4' + a_3) \cdot i_7' + (i_4' + a_3) \cdot a_4$$
$$= i_1' + (i_4' \cdot i_7' + a_3 \cdot i_7') + (i_4' \cdot a_4 + a_3 \cdot a_4)$$
$$= (i_1' + i_4' \cdot i_7' + a_3 \cdot i_7' + i_4' \cdot a_4) + a_3 \cdot a_4$$

Let $(i_1' + i_4' \cdot i_7' + a_3 \cdot i_7' + i_4' \cdot a_4) = i_0' \in I$, then $i_0' + a_3 \cdot a_4 \in I + a_3 \cdot a_4$.

Therefore $I + a_1 \cdot a_2 \subseteq I + a_3 \cdot a_4$.

In a similar manner it can be shown that $I + a_3 \cdot a_4 \subseteq I + a_1 \cdot a_2$. Hence $I + a_1 \cdot a_2 = I + a_3 \cdot a_4$. Therefore, $\boxdot$ is a binary operation.

For any $I+a_1$, $I+a_2$, $I+a_3 \in Q$,

1. $(I+a_1) \boxplus [(I+a_2) \boxplus (I+a_3)] = (I+a_1) \boxplus [I+(a_2+a_3)]$
$$= I + a_1 + (a_2 + a_3)$$
$$= I + (a_1 + a_2) + a_3$$
$$= (I + a_1 + a_2) \boxplus (I + a_3)$$
$$= [(I+a_1) \boxplus (I+a_2)] \boxplus (I+a_3)$$

2. $(I+0) \boxplus (I+a_1) = I+(0+a_1) = I+a_1$

3. $[I+(-a_1)] \boxplus (I+a_1) = I+ [(-a_1)+a_1] = I+0$

4. $(I+a_1) \boxplus (I+a_2) = I+(a_1+a_2) = I+(a_2+a_1) = (I+a_2) \boxplus (I+a_1)$

   Hence, $(R/I, \boxplus)$ is an abelian group.

5. $(I+a_1) \boxdot [(I+a_2) \boxdot (I+a_3)] = (I+a_1) \boxdot (I+a_2 \cdot a_3)$
$$= I + a_1 \cdot (a_2 \cdot a_3)$$
$$= (I + a_1 \cdot a_2) \boxdot (I + a_3)$$
$$= [(I+a_1) \boxdot (I+a_3)] \boxdot (I+a_3)$$

$$6.\quad (I+a_1) \boxdot [(I+a_3) \boxplus (I+a_3)] = (I+a_1) \boxdot [I+(a_2+a_3)]$$
$$= I + a_1\cdot(a_2+a_3)$$
$$= I + (a_1\cdot a_2 + a_1\cdot a_3)$$
$$= (I+a_1\cdot a_2) \boxplus (I+a_1\cdot a_3)$$
$$= (I+a_1)\boxdot(I+a_2)\boxplus(I+a_1)\boxdot(I+a_3)$$

A similar proof holds for right distributive law.

Therefore $(Q,\boxplus,\boxdot)$ is a ring.

Definition 1-20. The set of residue class Q defined in definition 1-19 is a ring and is called the quotient ring of R by I (denoted by R/I).

Theorem 1-18. Let T be a homomorphic mapping from a ring $(R,+,\cdot)$ onto a ring $(R',+',\cdot')$ and let I be the set of elements in R which map onto the zero element $0'$ of R', then I is an ideal and the quotient ring R/I is isomorphic to R'.

Proof: Since T is isomorphic onto mapping, then by theorem 1-14, the set $(I,+,\cdot)$ is a subring of $(R,+,\cdot)$. For any $a \in R$ and $i \in I$, $(i\cdot a)T = iT\cdot' aT = 0' \cdot' aT = 0'$ and $(a\cdot i)T = aT \cdot' iT = aT \cdot' 0' = 0'$, which implies that $i\cdot a \in I$ and $a\cdot i \in I$. Hence I is an ideal of R. If $x_1 \in R/I$, then there exists $a_1 \in R$ such that $x_1=I+a_1$. Define ϕ by $x_1\phi=a_1T$. Let $x_1, x_2 \in R/I$ and $x_1\phi=x_1'$, $x_2\phi=x_2'$. If $x_1' \neq x_2'$, then there exists $a_1, a_2 \in R$ such that $x_1=I+a_1$ and $x_2=I+a_2$. Now

$$(I+a_1)\phi = x_1\phi = a_1T = x_1' \quad \text{, and}$$
$$(I+a_2)\phi = x_2\phi = a_2T = x_2' \ .$$

Since $x_1' \neq x_2'$, it follows that $a_1T \neq a_2T$. Suppose $x_1 = x_2$, then

$$I + a_1 = I + a_2$$

$$(I+a_1)T = (I+a_2)T$$

$$0' +' a_1T = 0' +' a_2T$$

$$a_1T = a_2T \quad .$$

This leads to a contradiction. Therefore ϕ is a mapping.

Now let $x_1, x_2 \in R/I$, $I+a_1 = x_1$ and $I+a_2 = x_2$, then

$$\begin{aligned}(x_1 \boxplus x_2)\phi &= [(I+a_1) \boxplus (I+a_2)]\phi \\ &= [I + (a_1+a_2)]\phi \\ &= (a_1+a_2)T \\ &= a_1T +' a_2T \\ &= x_1\phi +' x_2\phi \quad \text{, and}\end{aligned}$$

$$\begin{aligned}(x_1 \boxdot x_2)\phi &= [(I+a_1) \boxdot (I+a_2)]\phi \\ &= [I + (a_1 \cdot a_2)]\phi \\ &= (a_1 \cdot a_2)T \\ &= a_1T \cdot' a_2T \\ &= x_1\phi \cdot' x_2\phi \ .\end{aligned}$$

Therefore ϕ is a homomorphic mapping.

Now if $x_1 \neq x_2$ for $x_1, x_2 \in R/I$, then $I+a_1 \neq I+a_2$ implies $a_1 \neq a_2$. Suppose $x_1\phi = x_2\phi$, then $x_1\phi = a_1T = a_2T = x_2\phi$. Hence $a_1T = a_2T$. Since $-(a_1T) \in R'$ implies

$$(a_1T) +' (-a_1T) = a_2T +' (-a_1T)$$
$$0' = a_2T - a_1T$$
$$0' = (a_2-a_1)T \quad ,$$

and $a_2-a_1 \in I$. Therefore, $I+(a_2-a_1)=I+0$. Now

$$(I+a_2) \boxplus (I-a_1) = I + 0$$
$$[(I+a_2) \boxplus (I-a_1)] \boxplus (I+a_1) = (I+0) \boxplus (I+a_1)$$
$$(I+a_2) \boxplus [(I-a_1) \boxplus (I+a_1)] = I + (0+a_1)$$
$$I + a_2 = I + a_1$$

The above result implies that $x_1=x_2$, which is then contrary to the assumption. Therefore, if $x_1 \neq x_2$ implies $x_1\phi \neq x_2\phi$, then ϕ is one to one.

For every $x_1' \in R'$ there exists at least one $a_1 \in R$ such that $a_1T=x_1'$. Since $x_1\phi=(I+a_1)\phi= a_1T = x_1'$ for any $x_1' \in R'$, so ϕ is onto.

Therefore, ϕ is an isomorphic mapping from R/I onto R'.

<u>Theorem</u> <u>1-19</u>. If R is a commutative ring with identity, then R/I is also a commutative ring with identity, and moreover, if R is an integral domain, then R/I is an integral domain.

Proof: For $x_1,x_2 \in R/I$ there exists $a_1,a_2 \in R$ such that $x_1=I+a_1$ and $x_2=I+a_2$. Now

$$x_1 \boxdot x_2 = (I+a_1) \boxdot (I+a_2)$$
$$= I + (a_1 \cdot a_2)$$
$$= I + (a_2 \cdot a_1)$$

$$x_1 \boxdot x_2 = I + (a_2 \cdot a_1)$$
$$= (I+a_2) \boxdot (I+a_1)$$
$$= x_2 \boxdot x_1 \quad .$$

Hence, R/I is a commutative ring.

For $I+a_1=x_1 \in R/I$, then $I+e \in R/I$ where $e \in R$, hence $(I+e) \boxdot (I+a_1)= (I+e \cdot a_1)= (I+a_1)$. Therefore, R/I has the identity $I+e$.

If R is an integral domain, then for $a,b \in R$ such that $a \neq 0$, $a \cdot b=0$. Then $b=0$. Consider $x_1,x_2 \in R/I$ such that $x_1=I+a_1 \neq I+0$ which implies $a_1 \neq 0$. If $x_1 \boxdot x_2 = I+0$ and $(I+a_1) \boxdot (I+a_2) = I + a_1 \cdot a_2 = I+0$, then $a_1 \cdot a_2=0$. But R is an integral domain and $a_1 \neq 0$, so $a_2=0$ leads to $x_2= I+a_2= I+0$. Therefore, R/I is an integral domain.

CHAPTER BIBLIOGRAPHY

1. Herstein, I. N., Topics in Algebra, New York, Blaisdell Publishing Company, 1964.

2. Waerder, B. L., Modern Algebra, Vol. I, translated by Fred Blum, New York, Frederick Ungar Publishing Co., 1949.

3. Zariski, Oscar and Pierre Samuel, Commutative Algebra, Vol. I, New York, D. Van Nostrand Company, 1958.

CHAPTER II

SPECIAL TYPES OF IDEALS

In the preceding chapter, some general properties of ideals have been discussed. Prime ideals and maximal ideals are special types of ideals which have many interesting properties. This chapter will investigate some properties of these special types of ideals.

<u>Definition 2-1</u>. The product of two ideals A and B in a ring R is the set

$$AxB = \left\{ \sum_{k=1}^{n} a_k \cdot b_k \,\middle|\, a_k \in A \text{ and } b_k \in B,\ n \text{ is any arbitrary positive integer} \right\}$$

<u>Theorem 2-1</u>. The product of two ideals in a ring R is itself an ideal of R.

Proof: Let $x, y, \in AxB$, then $x = \sum_{k=1}^{n} a_k \cdot b_k$ and $y = \sum_{k'=1}^{m} a_{k'} \cdot b_{k'}$ where $k=1,2,3,\cdots,n$ and $k'=1,2,3,\cdots,m$. Note that $-y = -\sum_{k'=1}^{m} a_{k'} \cdot b_{k'} = \sum_{k'=1}^{m} (-a_{k'}) \cdot b_{k'}$. Let $-a_{k'} = a_{n+k'}$ and $b_{k'} = b_{m+k'}$, then

$$x - y = \left(\sum_{k=1}^{n} a_k \cdot b_k\right) - \left(\sum_{k'=1}^{m} a_{k'} \cdot b_{k'}\right)$$

$$x - y = \sum_{k=1}^{n} a_k \cdot b_k + \sum_{k'=1}^{m} (-a_{k'}) \cdot b_{k'}$$

$$= \sum_{k=1}^{n} a_k \cdot b_k + \sum_{k'=1}^{m} a_{n+k'} \cdot b_{m+k'}$$

$$= \sum_{k=1}^{m} a_k \cdot b_k \in AxB$$

where $a_k \in A$ and $b_k \in B$. For $r \in R$, then

$$r \cdot x = r \cdot \sum_{k=1}^{n} a_k \cdot b_k = \sum_{k=1}^{n} (r \cdot a_k) \cdot b_k$$

where $r \cdot a_k \in A$ and $b_k \in B$. Therefore, $r \cdot x \in AxB$ for $x \in AxB$. Similarly, $x \cdot r \in AxB$ for $x \in AxB$. Therefore, AxB is an ideal of R.

<u>Definition 2-2</u>. Let I be an ideal in R. I is prime if for any b,c in R such that $b \cdot c \in I$, then at least one of them is an element of I.

<u>Definition 2-3</u>. An ideal I_m of R is maximal if $I_m \neq R$, and if there is no ideal properly contained between R and I_m.

Examples of prime ideals and maximal ideals are given in the following:

<u>Example 2-1</u>. The ring of integers J itself is a prime ideal, since by definition of prime ideal, if $b \cdot c \in J$, then $b \in J$ or $c \in J$. Also the principal ideal (0) of J is a prime ideal, since J is free of zero divisors. If $b \cdot c \in (0)$, then $b \cdot c = 0$. So if $b \neq 0$, then $c = 0$ and $c \in (0)$. Therefore, (0) is a prime ideal of J.

Example 2-2. If J is the ring of integers and $n > 1$ such that $n \in J$, then the principle ideal (n) is prime if and only if n is a prime number. If n is a prime number and if $a \cdot b \in (n)$ then $a \cdot b = kn$ so either $a = k_1 n$ or $b = k_2 n$ for $k_1, k_2 \in J$. Hence $a \in (n)$ or $b \in (n)$. Therefore, (n) is a prime ideal in J. Suppose n is not a prime number. By definition, there exists $a, b \in J$ such that $a \cdot b = n$ with $0 < a < n$ and $0 < b < n$ so $a \notin (n)$ and $b \notin (n)$. Hence, if (n) is a prime ideal, then n is a prime number in J. Moreover, every prime ideal (n) in J is maximal. If I is an ideal in J such that $(n) \subset I \subset J$, then there exists $m \in I$ such that $m \notin (n)$. It follows that (m, n) is relative prime. There exists no common divisors between m and n except ± 1. Then there exists $a, b \in J$ such that $m \cdot a + n \cdot b = 1 \in I$. Since $n \cdot b \in (n) \subset I$ and $m \in I$, so $1 \in I$ implies that any $x \in J$, then $x \cdot 1 \in I$. It follows that $J \subset I$ and $I \subset J$. Hence $I = J$. Therefore (n) is a maximal ideal of J.

Theorem 2-2. If I is a prime ideal in R and I_1 and I_2 are ideals in R such that $I_1 x I_2 \subset I$, then $I_1 \subset I$ or $I_2 \subset I$. If I is not prime, then there exists I_1 and I_2 such that

$$I \subset I_1 \ , \ I \subset I_2 \ , \ I_1 x I_2 \subset I \ .$$

Proof: Suppose $I_1 \not\subset I$ and $I_2 \not\subset I$ and let I be a prime ideal in R such that $I_1 x I_2 \subset I$, then there exists $a_1 \in I_1$, $a_2 \in I_2$ such that $a_1 \cdot a_2 \notin I$. Since I is a prime ideal in R, then $a_1 \cdot a_2 \notin I$ implies $I_1 x I_2 \not\subset I$. This leads to a contradiction. If I is not a prime ideal in R, then there exists

b_1 and b_2 such that $b_1, b_2 \notin I$ and $b_1 \cdot b_2 \in I$. Now let

$$I_1 = I + (b_1) \equiv \{ i + (b_1) \mid i \in I \}$$

$$I_2 = I + (b_2) \equiv \{ i + (b_2) \mid i \in I \}.$$

For $x, y \in I+(b_1)$, there exists $i_1, i_2 \in I$ and $p, q \in R$ such that $x = i_1 + pb_1$ and $y = i_2 + qb_1$. But

$$\begin{aligned} x - y &= (i_1 + pb_1) - (i_2 + qb_1) \\ &= (i_1 + pb_1 - i_2) - qb_1 \\ &= (i_1 - i_2 + pb_1) - qb_1 \\ &= (i_1 - i_2) + (p - q)b_1 \in I + (b_1) \ , \end{aligned}$$

and for $r \in R$,

$$\begin{aligned} r \cdot x &= r \cdot (i_1 + pb_1) \\ &= r \cdot i_1 + r \cdot (pb_1) \\ &= r \cdot i_1 + (r \cdot p)b_1 \in I+(b_1) \ . \end{aligned}$$

Similarly, $x \cdot r \in I+(b_1)$ for $r \in R$ and $x \in I$. Therefore, $I_1 = I+(b_1)$ is an ideal of R . A similar proof holds for $I_2 = I+(b_2)$ being an ideal of R.

For any $i_1 \in I$, since $0 \in R$ and $i_1 = i_1 + 0 \cdot b_1 \in I+(b_1)$, hence $I \subset I_1 = I+(b_1)$. Likewise, $I \subset I+(b_2)$. For any $r_1, r_2 \in R$ and $x \in I_1 x I_2 = I+(b_1) \ x \ I+(b_2)$, there exist $i_1, i_2 \in I$ such that

$$\begin{aligned}
x &= (i_1+r_1\cdot b_1)\cdot(i_2+b_2\cdot r_2)\\
&= (i_1+r_1\cdot b_1)\cdot i_2 + (i_1+r_1\cdot b_1)\cdot(b_2\cdot r_2)\\
&= i_1\cdot i_2 + (r_1\cdot b_1)\cdot i_2 + i_1\cdot(b_2\cdot r_2) + (r_1\cdot b_1)\cdot(b_2\cdot r_2)\\
&= i_1\cdot i_2 + (r_1\cdot b_1)\cdot i_2 + i_1\cdot(b_2\cdot r_2) + r_1\cdot(b_1\cdot b_2)\cdot r_2
\end{aligned}$$

Since $b_1\cdot b_2 \in I$ and , by definition of ideal, hence $x \in I$. Therefore, $I_1 x I_2 \subset I$.

The next lemma concerns a homomorphic mapping of a ring onto its quotient ring.

Lemma 2-1. There exists a homomorphic mapping f from a ring R onto its quotient ring R/I such that $b\cdot c \in I$ if and only if $bf \boxdot cf = I+0$.

Proof: Let $x_1 \in R/I$, then there exists $a_1 \in R$ such that $x_1 = I+a_1$. Define f such that $a_1 f = I+a_1$ for $a_1 \in R$ and $I+a_1 \in R/I$. Suppose $I+a_1 \neq I+a_2$ and $a_1 = a_2$, then there exists $i_1 \in I$ such that $i_1+a_1 = i_1+a_2$ which leads to a contradiction. Therefore, f is a mapping. For any $x_1 \in R/I$ there exists $a_1 \in R$ such that $a_1 f = I+a_1 = x_1$. Hence f is onto. For $a_1, a_2 \in R$, then

$$\begin{aligned}
(a_1+a_2)f &= I+(a_1+a_2)\\
&= (I+a_1) \boxplus (I+a_2)\\
&= a_1 f \boxplus a_2 f \quad \text{, and}\\
(a_1\cdot a_2)f &= I+(a_1\cdot a_2)\\
&= (I+a_1) \boxdot (I+a_2)\\
&= a_1 f \boxdot a_2 f
\end{aligned}$$

Hence f is a homomorphism. The homomorphism f is called the natural homomorphism from ring R onto its quotient ring R/I. Since $b \cdot c \in I \subset R$, then

$$\begin{aligned} bf \boxdot cf &= (b \cdot c)f \\ &= I + b \cdot c \\ &= I + 0 \ . \end{aligned}$$

On the other hand, if $bf \boxdot cf = I+0$, then

$$\begin{aligned} bf \boxdot cf &= (I+b) \boxdot (I+c) \\ &= I + (b \cdot c) \\ &= I + 0 \\ &= I \ . \end{aligned}$$

Therefore, $b \cdot c \in I$.

The preceding lemma prepares the way for theorem 2-3.

Theorem 2-3. Let I be an ideal such that $I \neq R$. Then I is a prime ideal if and only if R/I has no zero divisors.

Proof: $R \neq \phi$ implies $R/I \neq \phi$. If R/I has no zero divisors, then for $x_1, x_2 \in R/I$ such that $x_1 \neq I+0$, $x_1 \boxdot x_2 = I+0$ and $x_2 = I+0$. By lemma 2-1, there exists a natural homomorphism f from R onto R/I. Then $a_1 f = I+a_1 = x_1$ and $a_2 f = I+a_2 = x_2$ such that $a_1 - a_2 \in I$ for some $a_1, a_2 \in R$. Also $a_2 f = I+a_2 = x_2 = I+0$ and $I+a_2 = I+0$, then there exists $i_1, i_2 \in I$ such that $i_1 + a_2 = i_2 + 0 = i_2 \in I$. Since $(I,+)$ is a subgroup of $(R,+)$, then $i_2 - i_1 = a_2 \in I$. Therefore, I is a prime ideal of R.

If I is a prime ideal of R and $i_1 \cdot i_2 \in I$, then there exists at least one of i_1 or i_2, say i_1, that is in I.

By lemma 2-1, for $i_1 \cdot i_2 \in I$, if $i_1 f \circledcirc i_2 f = (I+i_1) \circledcirc (I+i_2) = I+0$, then $i_1 f = I+0$. Hence, if $i_1 f \circledcirc i_2 f = I+0$, then $i_1 f = I+0$.

Definition 2-4. The inverse transformation T^{-1} at $\bar{a}$ of a ring $\bar{R}$ into a ring R is the set of all elements of R having $\bar{a}$ as T-image, where $\bar{a} \in \bar{R}$.

The following lemma is rather important and has frequent application in the remainder of the chapter.

Lemma 2-2. Let T be a homomorphism of a ring R onto a ring $\bar{R}$, with kernel N. Then there exists a one to one inclusion preserving mapping between the ideals of $\bar{R}$ and the ideals of R which contain kernel N, such that if I and $\bar{I}$ correspond, then $IT = \bar{I}$ and $\bar{I}T^{-1} = I$, and R/I is isomorphic to $\overline{R/I}$.

Proof: If I is an ideal containing N, then $IT = \bar{I}$ is an ideal. If $x_1, x_2 \in I$ such that $x_1 T = x_1'$ and $x_2 T = x_2'$ where $x_1', x_2' \in IT$, then

$$\begin{aligned} x_1' - x_2' &= x_1 T - x_2 T \\ &= (x_1 - x_2)T \in IT \ . \end{aligned}$$

This implies that $x_1 - x_2 \in I$. For any $x_1' \in IT$ and $r' \in \bar{R}$ such that $rT = r'$, then

$$\begin{aligned} r' \cdot x_1' &= rT \cdot x_1 T \\ &= (r \cdot x_1)T \in IT \ , \end{aligned}$$

which implies $r \cdot x_1 \in I$. Likewise, $x_1' \cdot r' \in IT$. Hence $\bar{I} = IT$ is an ideal in $\bar{R}$. Every ideal I of R has its image IT being an ideal of $\bar{R}$.

Before proving that T is one to one from ideals of R onto ideals of $\bar{R}$, one must show that $(IT)T^{-1} = I$. For any $x_1 \in I \subset R$ such that $x_1T = x_1' \in IT$, then $x_1 \in (IT)T^{-1}$. Therefore $I \subset (IT)T^{-1}$. If $x_1 \in (IT)T^{-1}$, then $x_1T \in IT$, so $x_1T = y_1T$ with $y_1 \in I$. Hence $(x_1-y_1) \in N \subset I$. Let $x_1-y_1=z_1 \in I$ with $y_1, z_1 \in I$, then $x_1=z_1+y_1 \in I$. Hence $(IT)T^{-1} \subset I$. Since $(IT)T^{-1} \subset I$ and also $I \subset (IT)T^{-1}$, then $(IT)T^{-1} = I$.

If $I_1 \neq I_2$, then without loss of generality there exists some $x_1 \in I_1$ and $x_2 \in I_2$ such that $x_1 \neq x_2$. Since $(IT)T^{-1} = I$, then $x_1 \in (I_1T)T^{-1}$, $x_2 \in (I_2T)T^{-1}$, $x_1T \in I_1T$ and $x_2T \in I_2T$. Suppose $I_1T=I_2T$, then $x_2T \in I_2T=I_1T$. Hence $x_2T \in I_1T$ and $x_2 \in (I_1T)T^{-1} = I_1$. It follows that $x_2 \in I_1$ which is a contradiction. Therefore, T is one to one between I_1 of R and $\bar{I}_1$ of $\bar{R}$.

If $x_1, x_2 \in \bar{I}T^{-1}$, then $x_1T, x_2T \in \bar{I}$, by definition of T^{-1}. Since $(x_1-x_2)T = x_1T - x_2T \in \bar{I}$, then $x_1-x_2 \in \bar{I}T^{-1}$. If $x_1 \in \bar{I}T^{-1}$ and $r \in R$, then $x_1T \in \bar{I}$ and $rT \in R'$. Hence $(x_1 \cdot r)T=x_1T \cdot rT \in \bar{I}$ and $x_1 \cdot r \in \bar{I}T^{-1}$. Likewise, $r \cdot x_1 \in \bar{I}T^{-1}$ for any $r \in R$ and $x_1 \in \bar{I}T^{-1}$.

From the above discussion, it can be concluded that for every ideal $\bar{I}$ of $\bar{R}$, $\bar{I}T^{-1}$ is an ideal of R. Suppose this preimage $\bar{I}T^{-1}$ of $\bar{I}$ does not contain N, then there exists $x \in N$ such that $x \notin \bar{I}T^{-1}$ and $xT=0 \notin \bar{I}$. But $\bar{I}$ is an ideal of R and this leads to a contradiction. Therefore, every preimage $\bar{I}$ of $\bar{R}$ is an ideal of R containing N. Since T is an onto mapping, then for every $\bar{I}$ of $\bar{R}$ there exists $\bar{I}T^{-1}$ of R such that $(\bar{I}T^{-1})T = \bar{I}$. If $I_1T=\bar{I}_1$ and $I_2T=\bar{I}_2$ such that $I_1 \subset I_2$, then $\bar{I}_1 \subseteq \bar{I}_2$ because for every $i_2 \in I_2$ and $i_2 \notin I_1$, then there exists $i_2T=i_2' \in \bar{I}_2$ such that $i_2T=i_2' \notin \bar{I}_1$. If $i_2' \in \bar{I}_1$, since $I_1T=\bar{I}_1$ and $(I_1T)T^{-1}= I_1$, then $i_2'T^{-1} \subseteq I_1$. But $i_2'T^{-1}=i_2$ implies $i_2 \in I_1$ which is a contradiction. Since for $i_1' \in \bar{I}_1$ and $(i_1')T^{-1} \subseteq I_1 \subset I_2$, then $i_1'T^{-1} \subseteq I_2$. Note that $(i_1'T^{-1})T \in I_2T = \bar{I}_2$ and $(\bar{I}T^{-1})T=\bar{I}$, then $(i_1'T^{-1})T=i_1' \in \bar{I}_2$. Therefore, $\bar{I}_1 \subset \bar{I}_2$.

T is a homomorphism from R onto $\bar{R}$. By lemma 2-1, there exists a natural homomorphic mapping f_2 from $\bar{R}$ onto $\overline{R/I}$. Define a mapping $T_1=T\cdot f_2$ such that T_1 is a homomorphism from R onto $\overline{R/I}$. Also define $xT_1=\bar{x}f_2=\bar{\bar{x}} \in \overline{R/I}$, where $xT=\bar{x}$ and $x \in R$. Suppose $\bar{\bar{x}}_1 \neq \bar{\bar{x}}_2$ for $\bar{\bar{x}}_1,\bar{\bar{x}}_2 \in \overline{R/I}$. Since f_2 is a function, then $\bar{x}_1 \neq \bar{x}_2$. Since T is also a function, hence $x_1 \neq x_2$. Therefore, T_1 is a function. For any $\bar{\bar{x}} \in \overline{R/I}$, there exists $\bar{x} \in \bar{R}$ such that $\bar{x}f_2=\bar{\bar{x}}$ and there exists $x \in R$ such that $xT=\bar{x}$. Therefore, T_1 is onto. For $x,y \in R$, then

$$\begin{aligned}
(x+y)T_1 &= (\overline{x+y})f_2 \\
&= [(x+y)T]f_2 \\
&= (xT+yT)f_2 \\
&= (\bar{x}+\bar{y})f_2 \\
&= \bar{x}f_2 + \bar{y}f_2 \\
&= xT_1 + yT_1
\end{aligned}$$

$$
\begin{aligned}
(x\cdot y)T_1 &= (\overline{x\cdot y})f_2 \\
&= (x\cdot y)T\ f_2 \\
&= (xT\cdot yT)f_2 \\
&= (\bar{x}\cdot\bar{y})f_2 \\
&= \bar{x}f_2\cdot\bar{y}f_2 \\
&= xT_1\cdot yT_1\ .
\end{aligned}
$$

Therefore, T_1 is a homomorphism from R onto $\overline{R/I}$. By theorem 1-17, $\overline{R/I}$ is a ring. Now let N be $\in$ Ker(T_1). If $x \in N$, $xT \in \bar{R}$ and $(xT)f_2=\bar{\bar{0}} \in \overline{R/I}$, then $xT \in$ Ker(f_2) and $xT+\bar{I} = \bar{I}$. Since $xT \in \bar{I}$ and $x \in (\bar{I})T^{-1} = (IT)T^{-1} = I$, hence $N \subset I$. If $x \in I=(IT)T^{-1}$, $xT \in IT=\bar{I} \subset \bar{R}$ and $xT+\bar{I}=\bar{I}$, then $xT \in$ Ker(f_2), $(xT)f_2=\bar{\bar{0}} \in \overline{R/I}$ and $x \in$ Ker(T_1)=N. Hence $I \subset N$. Therefore, I = N. By theorem 1-18, T_1 is a homomorphism from a ring R onto a ring $\overline{R/I}$ and I is the Ker(T_1) and an ideal of R. Therefore, the quotient ring R/I is isomorphic to $\overline{R/I}$.

<u>Theorem</u> <u>2-4</u>. I_m is a maximal ideal of R if and only if R/I_m has no ideals but itself and (0).

Proof: By lemma 2-1, there exists a natural homomorphism f from R onto its quotient ring R/I_m. By lemma 2-2, there exists a one to one inclusion preserving mapping between ideals of R/I_m and ideals of R. If I_m is a maximal ideal of R and if there exists I_1' in R/I_m such that $I_1' \neq R/I_m$ and $I_1' \neq (0)$, then because T is onto there exists I_1 in R such that $I_1T = I_1'$. Since $I_mT = I_m/I_m = (0)$, $RT = R/I_m$, $I_1'\neq(0)$, and $I_1' \neq R/I_m$, and also T is an inclusion preserving mapping, $I_1 \neq (0)$ and $I_1 \neq R$, hence $I_m \subset I_1 \subset R$. But I_m is a maximal ideal in R; therefore, I_1 does not exist. Conversely, if R/I has only two ideals (0) and R/I and suppose I is not maximal, then there exists I_1 in R such that $I \subset I_1 \subset R$. Since I is a one to one inclusion preserving mapping from R onto R/I, then there exists I_1' in R/I such that $I_1T=I'$. Since R/I has only ideals (0) and R/I, then $I_1'=(0)$ or $I_1' = R/I$. If $I_1T= I_1/I_1 = (0)$, then $I_1=I$ which leads to a contradiction. If $I_1T = I_1' = R/I_1$, then $I_1=R$, which also leads to a contradiction. Therefore, I is a maximal ideal of R.

<u>Theorem 2-5</u>. If R is a commutative ring with identity, then I is maximal if and only if R/I is a field.

Proof: By theorem 1-13, R/I is a field if and only if R/I has no proper ideals. By theorem 2-4, I_m is maximal if and only if R/I_m has no proper ideals. If R has an identity, then by theorem 1-19, R/I has an identity. Therefore, the proof is completed.

<u>Theorem 2-6</u>. In a ring with identity, any maximal ideal is prime.

Proof: If I_m is a maximal ideal of R, then R/I_m has, by theorem 2-4, no proper ideals. By theorem 1-13, if R/I_m has no proper ideals, then R/I_m is a field. If R/I_m is a field, then R/I_m has no zero divisors. Then, by theorem 2-3, I_m is a prime ideal of R.

<u>Theorem 2-7</u>. Let T be a homomorphism of a ring R onto a ring $\bar{R}$ with kernel N. If I is an ideal in R containing N, then I is respectively prime or maximal if and only if IT is respectively prime or maximal. If $\bar{I}$ is an ideal in $\bar{R}$, then $\bar{I}$ is respectively prime or maximal if and only if $\bar{I}T^{-1}$ is respectively prime or maximal.

Proof: Since $I=R$ if and only if $IT=\bar{R}$ and T is a one to one inclusion preserving mapping from ideals of R onto ideals of $\bar{R}$, then I is prime if and only if IT is prime.

If $I \neq R$, by theorem 2-3, I is prime if and only if R/I has no zero divisors, and $\overline{R/IT}$ has no zero divisors if and only if IT is prime. By lemma 2-2, there exists an isomorphism g from R/I into $\overline{R/IT}$, and R/I has no zero divisors if and only if $\overline{R/IT}$ has no zero divisors. If $(I+r_1) \boxdot (I+r_2)$ and $I+r_1 \neq I+0$ for $I+r_1, I+r_2 \in R/I$, $(I+r_1)g=\bar{I}+r_1'$ and $(I+r_2)g=\bar{I}+r_2'$, then

$$[(I+r_1) \boxdot (I+r_2)]g = (I+0)g$$
$$(\bar{I}+r_1') \boxdot (\bar{I}+r_2') = \bar{I}+0' \ .$$

But $(I+r_1)g \neq (I+0)g$ implies $\bar{I}+r_1' = \bar{I}+0'$, and $(I+r_2)g=(I+0)g$ implies $\bar{I}+r_2' = \bar{I}+0'$. Hence, if $(\bar{I}+r_1') \boxdot (\bar{I}+r_2')=\bar{I}+0'$ and $\bar{I}+r_1' \neq \bar{I}+0'$, then $\bar{I}+r_2' = \bar{I}+0'$. Since g is one to one and if $(\bar{I}+r_1') \boxdot (\bar{I}+r_2')=\bar{I}+0'$, $(I+r_1) \boxdot (I+r_2)=I+0$ and $\bar{I}+r_1' \neq \bar{I}+0'$, then $I+r_1 \neq I+0$. Since g is a mapping and $\bar{I}+r_2' = \bar{I}+0'$, it follows that $I+r_2 = I+0$. Therefore, I is prime if and only if IT is prime.

By theorem 2-5, if $I \neq R$, then I is maximal if and only if R/I is a field. Since g is an isomorphism, it follows that R/I is a field if and only if R/IT is a field, and $\overline{R}/\overline{IT}$ is a field if and only if IT is a maximal ideal of $\overline{R}$. Since T is inclusion preserving, then there exist no ideals between IT and $\overline{R}$ if and only if there exist no ideals between I and R. By lemma 2-2, it follows that $\overline{I}T^{-1}$ is an ideal containing N, and $(\overline{I}T^{-1})T = \overline{I}$. Therefore, $(\overline{I}T^{-1})T = \overline{I}$ is respectively prime or maximal if and only if $\overline{I}T^{-1}$ is respectively prime or maximal.

CHAPTER BIBLIOGRAPHY

1. Zariski, Oscar and Pierre Samuel, Commutative Algebra, Vol. I, New York, D. Van Nostrand Company, 1958.

CHAPTER III

BOOLEAN RINGS

Boolean rings are special types of rings which are of great interest. This chapter will investigate some interesting properties of these special types of rings.

<u>Definition 3-1</u>. An element a of a ring R is idempotent if $a^2=a$ for $a \in R$.

<u>Definition 3-2</u>. A Boolean ring B is a ring such that all of its elements are idempotent, that is, $a^2=a$ for every $a \in B$.

The following systems are examples of Boolean rings.

<u>Example 3-1</u>. A simple Boolean ring is a ring with only two elements, that is a zero element 0 and an identity e, because $e \cdot e=e$ and $0 \cdot 0=0$. As another example, consider the set $S=\{a,b,c,d\}$ with addition and multiplication defined by the following tables.

+	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

·	a	b	c	d
a	a	d	a	d
b	d	b	b	d
a	a	b	c	d
d	d	d	d	d

.

Note that c is an identity for $(S,\cdot)$ and d is a zero element for $(S,+)$. By construction, we know the set S is a Boolean ring.

<u>Example 3-2</u>. Let R be a commutative ring $(R,+,\cdot)$ with identity and $B \equiv \{a \in R \mid a^2=a\}$. B is the set consisting of all idempotent elements of R.

Define operations $\oplus$ and $\odot$ as follows:

$$\oplus \equiv \{(a,b),(a+b-2a\cdot b) \mid a,b \in R \text{ and } a^2=a,\ b^2=b\}$$

$$\odot \equiv \{(a,b),(a\cdot b) \mid a,b \in R \text{ and } a^2=a,\ b^2=b\} .$$

If $a_1=a_2$ and $b_1=b_2$ for $a_1,a_2,b_1,b_2 \in B$, then

$$\begin{aligned} a_1 \oplus b_1 &= a_1 + b_1 - 2a_1\cdot b_1 \\ &= a_2 + b_2 - 2\, a_2\cdot b_2 \\ &= a_2 \oplus b_2 \quad , \text{ and} \end{aligned}$$

$$\begin{aligned} a_1 \odot b_1 &= a_1 \cdot b_1 \\ &= a_2 \cdot b_2 \\ &= a_2 \odot b_2 \quad . \end{aligned}$$

Hence $\oplus$ and $\odot$ are binary operations.

$$\begin{aligned} (a \oplus b) \oplus c &= (a+b-2a\cdot b) \oplus c \\ &= (a+b-2a\cdot b)+c- 2(a+b-2a\cdot b)\cdot c \\ &= (a+b-2a\cdot b+c) - 2[a\cdot c+b\cdot c-2(a\cdot b)\cdot c] \\ &= (a+b-2a\cdot b+c) -[2a\cdot c+2b\cdot c-4(a\cdot b)\cdot c] \\ &= (a+b+c-2a\cdot b) -[2b\cdot c+2a\cdot c-4(a\cdot b)\cdot c] \\ &= (a+b+c)-[2a\cdot b+2b\cdot c+2a\cdot c-4a\cdot (b\cdot c)] \\ &= a +(b+c)-[2b\cdot c+2a\cdot b+2a\cdot c-4a\cdot (b\cdot c)] \end{aligned}$$

$$
\begin{aligned}
&= a + (b+c-2b\cdot c) - 2a\cdot(b+c-2b\cdot c) \\
&= a \oplus (b+c-2b\cdot c) \\
&= a \oplus (b \oplus c) \\
a \oplus a &= a+a-2a\cdot a \\
&= a+a-2a^2 \\
&= a+a-2a \\
&= (a+a)-(a+a) \\
&= (a+a-a)-a \\
&= a+0-a \\
&= 0 \\
a \oplus 0 &= a+0-2a\cdot 0 \\
&= a+0-0 \\
&= a \\
a \oplus b &= a+b-2a\cdot b \\
&= b+a-2b\cdot a \\
&= b \oplus a \\
(a \odot b) \odot c &= (a\cdot b) \odot c \\
&= (a\cdot b)\cdot c \\
&= a\cdot(b\cdot c) \\
&= a \odot (b \odot c) \\
a \odot (b \oplus c) &= a \odot (b+c-2b\cdot c) \\
&= a\cdot(b+c-2b\cdot c) \\
&= a\cdot b+a\cdot c-a\cdot(2b\cdot c) \\
&= a\cdot b+a\cdot c-2a\cdot(b\cdot c) \\
&= a\cdot b+a\cdot c-2a^2\cdot(b\cdot c)
\end{aligned}
$$

$$= a\cdot b+a\cdot c-2a\cdot a\cdot(b\cdot c)$$

$$= a\cdot b+a\cdot c-2(a\cdot b\cdot a)\cdot c$$

$$= a\cdot b+a\cdot c-2(a\cdot b)\cdot(a\cdot c)$$

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

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

$$a \odot b = a\cdot b$$

$$= b\cdot a$$

$$= b \odot a$$

Therefore, B is a commutative ring with the property that every $a \in B$ is such that $a^2=a$. Hence B is a Boolean ring.

Some basic properties of a Boolean ring are stated in the following theorems.

Theorem 3-1. Let $(B,+,\cdot)$ be a Boolean ring; then if $a \in B$, the inverse of a under + is a itself, that is, $a+a=0$.

Proof: If $a,b \in B$, then $a^2=a\cdot a=a$, $b^2=b\cdot b=b$.

$$(a+b)^2 = (a+b)\cdot(a+b)$$

$$= (a+b)\cdot a + (a+b)\cdot b$$

$$= (a\cdot a+b\cdot a) + (a\cdot b+b\cdot b)$$

$$= (a+b\cdot a) + (a\cdot b+b).$$

On the other hand, $(a+b)^2=(a+b)\cdot(a+b)=(a+b)$ for $(a+b) \in B$, hence $(a+b)=(a+b\ a)+(a\cdot b+b)$.

$$(a+b) = (a+b\cdot a)+(a\cdot b+b)$$

$$= (a+b\cdot a+a.b+b)$$

$$= (a+b\cdot a+b+a\cdot b)$$

$$= (a+b+b\cdot a+a\cdot b)$$

$$= (a+b)+(b\cdot a+a\cdot b) \; .$$

Since B is a ring and $-(a+b) \in B$, then

$$-(a+b)+(a+b) = -(a+b)+[(a+b)+(b\cdot a+a\cdot b)]$$

$$0 = [-(a+b)+(a+b)]+ (b\cdot a)+(a\cdot b)$$

$$0 = b\cdot a + a\cdot b \; .$$

Let $b=a$, then $0=a\cdot a+a\cdot a$. Therefore, $0=a+a$.

Theorem 3-2. Every Boolean ring is commutative.

Proof: Let $a,b \in B$ and $b\cdot a \in B$. By theorem 3-1, $b\cdot a+a\cdot b=0$ and $(b\cdot a)+(b\cdot a)=0$. Hence $(b\cdot a)+(a\cdot b)=(b\cdot a)+(b\cdot a)$.

$$(b\cdot a)+(a\cdot b) = (b\cdot a)+(b\cdot a)$$

$$(b\cdot a)+[(b\cdot a)+(a\cdot b)] = (b\cdot a)+[(b\cdot a)+(b\cdot a)]$$

$$(b\cdot a+b\cdot a) + (a\cdot b) = (b\cdot a+b\cdot a) + b\cdot a$$

$$0 + a\cdot b = 0 + b\cdot a$$

$$a\cdot b = b\cdot a \quad \text{for any } a,b \in B.$$

Definition 3-3. If there exists a positive integer n such that na=0 for every a in R, then the smallest such positive integer is called the characteristic of R.

Definition 3-4. An element a of R is said to be nilpotent if there exists a positive integer n such that $a^n=0$.

Theorem 3-3. If B is a Boolean ring, then

(1) B has characteristic 2

(2) If B contains at least three elements, then every element of B except an identity (if B has one) is a zero divisor.

Proof: (1) By theorem 3-1, for every a in B, $a+a=2a=0$. Hence 2 is the least positive integer which satisfies $2a=0$.

(2) B contains at least three elements, then there exists $a,b \in B$ such that $a \neq b$. Suppose $a \neq b \neq 0$ and $a+b=0$, then $a+0=a+(b+b)=0+b$ which implies that $a=b$. This leads to a contradiction. Therefore, if $a \neq b \neq 0$, then $a+b \neq 0$. But B is a ring ; hence $(a+b) \in B$ and $a \cdot b \in B$. Then

$$\begin{aligned}(a \cdot b) \cdot (a+b) &= (a \cdot b) \cdot a + (a \cdot b) \cdot b \\ &= a \cdot (b \cdot a) + a \cdot (b \cdot b) \\ &= a \cdot (a \cdot b) + a \cdot (b \cdot b) \\ &= (a \cdot a) \cdot b + a \cdot (b \cdot b) \\ &= a \cdot b + a \cdot b \\ &= 0 .\end{aligned}$$

If $a \cdot b=0$, then a,b are zero divisors. If $a \cdot b \neq 0$, then for $(a+b) \neq 0$, $(a+b)$ and $(a \cdot b)$ are zero divisors in B.

<u>Theorem</u> 3-4. If B is a Boolean ring, then it has the following properties :

(1) $a+b=0$ if and only if $a=b$, where $a,b \in B$.

(2) $a+b=a-b$ if and only if $a,b \in B$.

(3) If $a+b=c$, then $a=c+b$ for $a,b,c \in B$.

Proof: (1) By theorem 3-1, then $a+a=0$ for every $a \in B$. If $a+b=0$, then

$$\begin{aligned} a + b &= a + a \\ a + (a + b) &= a + (a + a) \\ (a + a) + b &= (a + a) + a \\ 0 + b &= 0 + a \end{aligned}$$

Hence, $a=b$. By theorem 3-1, it follows that $a+b=a+a=0$.

(2) By theorem 3-1, $b+b=0$. Since b is an element of the ring B and $-b$ is in B such that $b-b=0$, then by uniqueness of the additive inverse in the Boolean ring, hence $b=-b$. Therefore, $a-b=a+b$ for $a \in B$.

(3)
$$\begin{aligned} a + b &= c \\ (a + b) + b &= c + b \\ a + (b + b) &= c + b \\ a + 0 &= c + b \\ a &= c + b\ . \end{aligned}$$

Definition 3-5. A ring R_1 is said to be embedded in a ring R_2 if there exists a subring R_2' of R_2 such that R_1 is isomorphic to R_2'.

The embedding theorem describes an algebraic structure with prescribed properties which contains a substructure isomorphic to a given structure.

Theorem 3-5. A Boolean ring $(B_1,+,\cdot)$ without identity can be embedded in a Boolean ring $(B_2,+,\cdot)$ with an identity.

Proof: Let B_1 be a Boolean ring and B_2 be the set of $B_1 x I/(2)$, that is, $B_1 x I/(2) \equiv \{(a,i) / a \in B_1 \text{ and } i \in I/(2)\}$, and $(a_1,i_1)=(a_2,i_2)$ if and only if $a_1=a_2$ and $i_1=i_2$. Define addition and multiplication in B_2 as follows:

$$+_2 \equiv \{((a_1,i_1),(a_2,i_2)),(a_1+a_2,i_1+i_2) \quad a_1,a_2 \in B_1 \text{ and } i_1,i_2 \in I/(2)\}$$

$$\cdot_2 \equiv \left\{((a_1,i_1),(a_2,i_2)),(a_1 \cdot a_2+i_1a_2+i_2a_1,i_1 \cdot i_2) \quad \begin{array}{r} a_1,a_2 \in B_1 \\ \text{and } i_1,i_2 \in I/(2) \end{array}\right\}$$

If $x_1=(a_1,i_1)$, $x_2=(a_2,i_2)$, $x_3=(a_3,i_3)$ and $x_4=(a_4,i_4)$ where $x_1,x_2,x_3,x_4 \in B_2$ such that $x_1=x_3$ and $x_2=x_4$, then by definition $(a_1,i_1)=(a_3,i_3)$ and $(a_2,i_2)=(a_4,i_4)$ if and only if $a_1=a_3$, $i_1=i_3, a_2=a_4$ and $i_2=i_4$. Since $a_1+a_2=a_3+a_4$ and $i_1+i_2=i_3+i_4$, then

$$\begin{aligned} x_1 +_2 x_2 &= (a_1,i_1) +_2 (a_2,i_2) \\ &= (a_1+a_2, i_1+i_2) \\ &= (a_3+a_4, i_3+i_4) \\ &= (a_3,i_3) +_2 (a_4,i_4) \\ &= x_3 +_2 x_4 . \end{aligned}$$

Since $a_1 \cdot a_2 = a_3 \cdot a_4$ and $i_1 \cdot i_2 = i_3 \cdot i_4$, then

$$\begin{aligned} x_1 \cdot_2 x_2 &= (a_1,i_1) \cdot_2 (a_2,i_2) \\ &= (a_1 \cdot a_2 + i_1 a_2 + i_2 a_1,\ i_1 \cdot i_2) \\ &= (a_3 \cdot a_4 + i_3 a_4 + i_4 a_3, i_3 \cdot i_4) \\ &= (a_3,i_3) \cdot_2 (a_4,i_4) \\ &= x_3 \cdot_2 x_4 . \end{aligned}$$

Therefore, $+_2$ and $\cdot_2$ are binary operations. Other properties are then found as follows:

(1) $$\begin{aligned} (a_1,i_1) +_2 [(a_2,i_2)+(a_3,i_3)] &= (a_1,i_1) +_2 [(a_2+a_3, i_2+i_3)] \\ &= [a_1+(a_2+a_3),\ i_1+(i_2+i_3)] \\ &= [(a_1+a_2)+a_3,\ (i_1+i_2)+i_3] \\ &= (a_1+a_2, i_1+i_2) +_2 (a_3,i_3) \\ &= [(a_1,i_1)+\ (a_2,i_2)] +_2 (a_3,i_3) \end{aligned}$$

$$(2) \qquad (a_1,i_1) +_2 (0,0) = (a_1+0, i_1+0)$$
$$= (a_1,i_1)$$

$$(3) \qquad (a_1,i_1) +_2 (-a_1,-i_1) = (a_1-a_1, i_1-i_1)$$
$$= (0,0)$$

$$(4) \qquad (a_1,i_1) +_2 (a_2,i_2) = (a_1+a_2, i_1+i_2)$$
$$= (a_2+a_1, i_2+i_1)$$
$$= (a_2,i_2) +_2 (a_1,i_1)$$

$$(5) \qquad (a_1,i_1) \cdot_2 [(a_2,i_2) \cdot_2 (a_3,i_3)]$$
$$\begin{aligned}
&= (a_1,i_1) \cdot_2 [(a_2\cdot a_3+i_2a_3+i_3a_2,\ i_2\cdot i_3)] \\
&= [a_1\cdot(a_2\cdot a_3+i_2a_3+i_3a_2) + i_1(a_2a_3+i_2a_3+i_3a_2) \\
&\qquad +(i_2\cdot i_3)a_1,\ i_1\cdot(i_2\cdot i_3)] \\
&= [a_1\cdot(i_2a_3)+a_1\cdot(i_2a_3)+a_1\cdot(i_3a_2)+i_1(a_2\cdot a_3) \\
&\qquad +i_1(i_2a_3)+i_1(i_3a_2)+(i_2\cdot i_1)a_1, i_1\cdot(i_2\cdot i_3)] \\
&= [a_1\cdot a_2\cdot a_3+i_2a_1\cdot a_3+i_3a_1\cdot a_2+i_1a_2\cdot a_3 \\
&\qquad +i_1\cdot i_2a_3+i_3\cdot i_1a_2+i_3\cdot i_2a_1, (i_1\cdot i_2)\cdot i_3] \\
&= [a_1\cdot a_2\cdot a_3+i_1a_2\cdot a_3+i_2a_1\cdot a_3+i_1\cdot i_2a_3+i_3a_1\cdot a_2 \\
&\qquad +i_3\cdot i_1a_2+i_3\cdot i_2a_1,\ (i_1\cdot i_2)\cdot i_3] \\
&= [(a_1\cdot a_2+i_1a_2+i_2a_1)a_3+(i_1\cdot i_2)a_3 \\
&\qquad +i_3(a_1\cdot a_2+i_1a_2+i_2a_1),\ (i_1\cdot i_2)\cdot i_3] \\
&= (a_1\cdot a_2+i_1a_2+i_2a_1,\ i_1\cdot i_2) \cdot_2 (a_3,i_3) \\
&= [(a_1,i_1) \cdot_2 (a_2,i_2)] \cdot_2 (a_3,i_3)
\end{aligned}$$

where the associative law has been used repeatedly.

$$(6) \quad (a_1,i_1) \cdot_2 [(a_2,i_2) +_2 (a_3,i_3)]$$
$$= (a_1,i_1) \cdot_2 [(a_2+a_3, i_2+i_3)]$$
$$= [a_1\cdot(a_2+a_3)+i_1(a_2+a_3)+(i_2+i_3)a_1, i_1\cdot(i_2+i_3)]$$
$$= [(a_1\cdot a_2+a_1\cdot a_3)+(i_1a_2+i_1a_3)+(i_2a_1+i_3a_1),$$
$$(i_1\cdot i_2)+(i_1\cdot i_3)]$$
$$= [(a_1\cdot a_2+i_1a_2+i_2a_1)+(a_1\cdot a_3+i_1a_3+i_3a_1),$$
$$(i_1\cdot i_2)+(i_1\cdot i_3)]$$
$$= [(a_1\cdot a_2+i_1a_2+i_2a_1, i_1\cdot i_2) +_2 (a_1\cdot a_3+i_1a_3+i_3a_1),$$
$$(i_1\cdot i_3)]$$
$$= [(a_1,i_1) \cdot_2 (a_2,i_2)] +_2 [(a_1,i_1) \cdot_2 (a_3,i_3)]$$

$$(7) \quad (a_1,i_1) \cdot_2 (0,1) = (a_1\cdot 0+i_1 0+1a_1, i_1\cdot 1)$$
$$= (a_1,i_1)$$

Hence, B_2 is a ring with identity. If $(a_1,i_1) \in B_2$, then

$$(a_1,i_1) \cdot_2 (a_1,i_1) = (a_1\cdot a_1+i_1a_1+i_1a_1,\ i_1\cdot i_1)$$
$$= (a_1,i_1)$$

Hence every element in B_2 is idempotent. Therefore, B_2 is a Boolean ring with identity $(0,1)$.

Now consider the subset B_2' of B_2 such that $B_2' \equiv \{(a_1,0) | a_1 \in B_1$ and 0 is the zero element of $I/(2)\}$. For any $(a_1,0)$ and $(b_1,0) \in B_2'$, then $(a_1,0)+_2(-b_1,0)=(a_1-b_1,0) \in B_2'$ and $(a_1,0)\cdot_2(b_1,0)=(a_1\cdot b_1+0b_1+0a_1,0) = (a_1\cdot b_1,0) \in B_2'$. Hence B_2' is a subring of B_2.

There remains to be shown that there exists an isomorphism π from $(B_1,+,\cdot)$ to $(B_2',+\ ,\cdot\ )$. Define π by $a_1\pi = (a_1,0)$ for all $a_1 \in B_1$. Now π is a mapping for suppose there exists $a_1,a_2 \in B_1$ such that $a_1\pi = (a_1,0)$, $a_2\pi = (a_2,0)$ and $(a_1,0) \neq (a_2,0)$. If $a_1=a_2$, then $(a_1,0)=(a_2,0)$ which leads to a contradiction. Hence, $(a_1,0) \neq (a_2,0)$ implies $a_1 \neq a_2$ which shows that π is a mapping. Now

$$\begin{aligned}
(a_1+a_2)\pi &= (a_1+a_2,0) \\
&= (a_1,0) +_2 (a_2,0) \\
&= a_1\pi +_2 a_2\pi \qquad , \text{ and} \\
(a_1\cdot a_2)\pi &= (a_1\cdot a_2,0) \\
&= (a_1,0) \cdot_2 (a_2,0) \\
&= a_1\pi \cdot_2 a_2\pi \quad .
\end{aligned}$$

Therefore, π is a homomorphism. If $a_1\pi =(a_1,0)$ and $a_2\pi =(a_2,0)$ with $a_1 \neq a_2$ and if $(a_1,0)=(a_2,0)$, then $a_1=a_2$ which contradicts the definition. Hence $a_1 \neq a_2$ implies $(a_1,0) = (a_2,0)$. Thus π is one to one. For any $(a_1,0) \in B_2'$ there exists $a_1 \in B_1$ such that $a_1\pi = (a_1,0)$, then by the construction of the set B_2', π is an isomorphism. Therefore, every Boolean ring without an identity can be embedded in a Boolean ring with identity.

In certain algebraic systems, the conditions required for a Boolean ring as stated in definition 3-2 may be replaced by other properties which are stated and proved in theorem 3-6.

Theorem 3-6. If $(A,+,\cdot)$ is an algebraic structure such that A has at least two elements, there is an identity element for multiplication, and for all $x,y,z,w \in A$ such that

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

(b) $[x\cdot(y\cdot y)]\cdot z = (z\cdot y)\cdot x$,

(c) $x\cdot[(y+z)+w] = x\cdot(w+z) + x\cdot y$,

then $(A,+,\cdot)$ is a Boolean ring with identity.

Proof: By (a), every x in A has y+y as a zero element on the right. Let $x=e \in A$. By (c) then

$$e\cdot[(y+z)+w] = e\cdot(w+z)+e\cdot y$$
$$(y+z)+w = (w+z)+y \quad .$$

Let z=y+y, then

$$[y+(y+y)]+w = y+w \quad \text{and}$$
$$[w+(y+y)]+y = w+y \quad .$$

Since $(y+z)+w = (w+z)+y$, then $y+w = w+y$ for all $w,y \in A$. Therefore, $(A,+)$ is commutative. By (a), $x+(y+y)=(y+y)+x=x$. Hence x in A has a zero element on the left. If there exists $z \in A$ such that $z+x=x+z=x$ for all $x \in A$, then

$$z = z+(y+y) = (y+y)+z = y+y \quad .$$

Hence y+y is unique. Denote y+y=0 and let w=0 in (c), then

$$\begin{aligned} x\cdot[(y+z)+0] &= x\cdot(0+z)+x\cdot y \\ &= x\cdot z + x\cdot y \\ &= x\cdot y + x\cdot z \quad . \end{aligned}$$

Hence $x\cdot(y+z) = x\cdot y + x\cdot z$, and $(A,+,\cdot)$ is distributive. Let $x=z=e \in A$ in (b), then

$$\begin{aligned} [e\cdot(y\cdot y)]\cdot e &= (e\cdot y)\cdot e \\ (y\cdot y)\cdot e &= y\cdot e \\ y\cdot y &= y \quad \text{for every } y \in A. \end{aligned}$$

Therefore, every element in A is idempotent. Now consider (b). Let $z=e \in A$, then

$$[x\cdot(y\cdot y)]\cdot e = (e\cdot y)\cdot x$$
$$x\cdot(y\cdot y) = y\cdot x$$
$$x\cdot y = y\cdot x$$

for $x,y \in A$. Also

$$[x\cdot(y\cdot y)]\cdot z = (z\cdot y)\cdot x$$
$$(x\cdot y)\cdot z = x\cdot(z\cdot y)$$
$$(x\cdot y)\cdot z = x\cdot(y\cdot z) \quad .$$

Therefore, $(A,+,\cdot)$ is a Boolean ring with identity.

With the following definition of the complete direct sum S of the rings S_i where $i=1,2,\cdots,k$, S can then be shown to be a ring.

<u>Definition 3-6</u>. Let S_i be a given family of rings, where $i \in N$ and $N= 1,2,3,\cdots,k$. Let $S=\{(a_1,a_2,\cdots,a_k)/a_i \in S_i\}$ and define operations $+_s$ and $\cdot_s$ as follows:

$$+_s = \{((a_1,a_2,\cdots,a_k),(b_1,b_2,\cdots,b_k)),(a_1+b_1,a_2+b_2,\cdots,a_k+b_k) \text{ such that } a_i,b_i \in S_i\}$$

$$\cdot_s = \{((a_1,a_2,\cdots,a_k),(b_1,b_2,\cdots,b_k)), (a_1\cdot b_1,a_2\cdot b_2,\cdots,a_k\cdot b_k) \text{ such that } a_i,b_i \in S_i\}$$

For simplicity, the same notations of operations for the family of rings $(S_i,+,\cdot)$ are used. S so defined is called a complete direct sum of the rings S_i, where $i \in N$ and $(a_1,a_2,\cdots,a_k) = (b_1,b_2,\cdots,b_k)$ if and only if $a_i = b_i$.

Let $x_1,x_2,x_3,x_4 \epsilon$ S and $x_1=(a_1,a_2,\cdots,a_k)$, $x_2=(b_1,b_2,\cdots,b_k)$ $x_3=(c_1,c_2,\cdots,c_k)$, $x_4=(d_1,d_2,\cdots,d_k)$ such that $x_1=x_3$ and $x_2=x_4$, that is, $(a_1,a_2,\cdots,a_k)=(c_1,c_2,\cdots,c_k)$ and $(b_1,b_2,\cdots,b_k)=(d_1,d_2,\cdots,d_k)$. By definition, $a_i=c_i$ and $b_i=d_i$ where $a_i,b_i,c_i,d_i \epsilon S_i$. Then

$$\begin{aligned} x_1 +_s x_2 &= (a_1,a_2,\cdots,a_k) +_s (b_1,b_2,\cdots,b_k) \\ &= (a_1+b_1,a_2+b_2,\cdots,a_k+b_k) \\ &= (c_1+d_1,c_2+d_2,\cdots,c_k+d_k) \\ &= (c_1,c_2,\cdots,c_k) +_s (d_1,d_2,\cdots,d_k) \\ &= x_3 +_s x_4 \quad , \text{ and} \end{aligned}$$

$$\begin{aligned} x_1 \cdot_s x_2 &= (a_1,a_2,\cdots,a_k) \cdot_s (b_1,b_2,\cdots,b_k) \\ &= (a_1 \cdot b_1,a_2 \cdot b_2,\cdots,a_k \cdot b_k) \\ &= (c_1 \cdot d_1,c_2 \cdot d_2,\cdots,c_k \cdot d_k) \\ &= (c_1,c_2,\cdots,c_k) \cdot_s (d_1,d_2,\cdots,d_k) \\ &= x_3 \cdot_s x_4 \quad . \end{aligned}$$

Therefore, $+_s$ and $\cdot_s$ are binary operations. Other properties are shown as follows.

(1) $$\begin{aligned} x_1 +_s 0 &= (a_1,a_2,\cdots,a_k) +_s (0_1,0_2,\cdots,0_k) \\ &= (a_1+0_1,a_2+0_2,\cdots,a_k+0_k) \\ &= (a_1,a_2,\cdots,a_k) \\ &= x_1 \end{aligned}$$

(2) $$\begin{aligned} x_1 +_s (x_2 +_s x_3) &= x_1 +_s \{(b_1,b_2,\cdots,b_k) +_s (c_1,c_2,\cdots,c_k)\} \\ &= (a_1,a_2,\cdots,a_k) +_s (b_1+c_1,b_2+c_2,\cdots,b_k+c_k) \\ &= [a_1+(b_1+c_1),a_2+(b_2+c_2),\cdots,a_k+(b_k+c_k)] \\ &= [(a_1+b_1)+c_1,(a_2+b_2)+c_2,\cdots,(a_k+b_k)+c_k] \\ &= (a_1+b_1,a_2+b_2,\cdots,a_k+b_k) +_s (c_1,c_2,\cdots,c_k) \\ &= [(a_1,a_2,\cdots,a_k) +_s (b_1,b_2,\cdots,b_k)] \\ &\qquad +_s (c_1,c_2,\cdots,c_k) \\ &= (x_1 +_s x_2) +_s x_3 \quad . \end{aligned}$$

(3) $$\begin{aligned} x_1 +_s (-x_1) &= (a_1,a_2,\cdots,a_k) +_s (-a_1,-a_2,\cdots,-a_k) \\ &= (a_1-a_1,a_2-a_2,\cdots,a_k-a_k) \\ &= (0_1,0_2,\cdots,0_k) \\ &= 0 \quad . \end{aligned}$$

(4) $$\begin{aligned} x_1 +_s x_2 &= (a_1,a_2,\cdots,a_k) +_s (b_1,b_2,\cdots,b_k) \\ &= (a_1+b_1,a_2+b_2,\cdots,a_k+b_k) \\ &= (b_1+a_1,b_2+a_2,\cdots,b_k+a_k) \\ &= (b_1,b_2,\cdots,b_k) +_s (a_1,a_2,\cdots,a_k) \\ &= x_2 +_s x_1 \quad . \end{aligned}$$

(5) $$\begin{aligned} x_1 \cdot_s (x_2 \cdot_s x_3) &= (a_1,a_2,\cdots,a_k) \cdot_s [(b_1,b_2,\cdots,b_k) \cdot_s \\ &\qquad (c_1,c_2,\cdots,c_k)] \\ &= (a_1,a_2,\cdots,a_k) \cdot_s [(b_1+c_1,\cdots,b_k+c_k)] \\ &= [a_1\cdot(b_1\cdot c_1),a_2\cdot(b_2\cdot c_2),\cdots,a_k\cdot(b_k\cdot c_k)] \\ &= [(a_1\cdot b_1)\cdot c_1,(a_2\cdot b_2)\cdot c_2,\cdots,(a_k\cdot b_k)\cdot c_k] \\ &= (a_1\cdot b_1,a_2\cdot b_2,\cdots,a_k\cdot b_k) \cdot_s (c_1,c_2,\cdots,c_k) \end{aligned}$$

$$x_1 \cdot_s (x_2 \cdot_s x_3) = [(a_1,a_2,\cdots,a_k) \cdot_s (b_1,b_2,\cdots,b_k)] \cdot_s (c_1,c_2,\cdots,c_k)$$

$$= (x_1 \cdot_s x_2) \cdot_s x_3$$

(6) $$x_1 \cdot_s (x_2 +_s x_3) = (a_1,a_2,\cdots,a_k) \cdot_s [(b_1,b_2,\cdots,b_k) +_s (c_1,c_2,\cdots,c_k)]$$

$$= (a_1,a_2,\cdots,a_k) \cdot_s (b_1+c_1,b_2+c_2,\cdots,b_k+c_k)$$

$$= [a_1\cdot(b_1+c_1),a_2\cdot(b_2+c_2),\cdots,a_k\cdot(b_k+c_k)]$$

$$= [(a_1\cdot b_1+a_1\cdot c_1),(a_2\cdot b_2+a_2\cdot c_2),\cdots,(a_k\cdot b_k+a_k\cdot c_k)]$$

$$= (a_1\cdot b_1,a_2\cdot b_2,\cdots,a_k\cdot b_k) +_s (a_1\cdot c_1,a_2\cdot c_2,\cdots,a_k\cdot c_k)$$

$$= (a_1,a_2,\cdots,a_k) \cdot_s (b_1,b_2,\cdots,b_k) +_s [(a_1,a_2,\cdots,a_k) \cdot_s (c_1,c_2,\cdots,c_k)]$$

$$= (x_1 \cdot_s x_2) +_s (x_1 \cdot_s x_3)$$

Therefore, S is a ring and S has an identity if and only if S_i has an identity for every $i \in N$.

There remains to be shown that there exists an onto homomorphism θ_i between S and S_i where $i \in N$. Define θ_i as follows: $(a_1,a_2,\cdots,a_k)\theta_i = a_i$ for $(a_1,a_2,\cdots,a_k) \in S$. Let $x_1=(a_1,a_2,\cdots,a_k)$ and $x_2=(b_1,b_2,\cdots,b_k)$ be in S such that

$$(a_1,a_2,\cdots,a_k)\theta_i = a_i$$
$$(b_1,b_2,\cdots,b_k)\theta_i = b_i$$

where $a_i,b_i \in S_i$. If $a_i \neq b_i$, then $(a_1,a_2,\cdots,a_k) \neq (b_1,b_2,\cdots,b_k)$.

Hence θ_i is a mapping. For every $a_i \in S_i$ there exists $x_1 \in S$ such that $x_1=(a_1,a_2,\cdots,a_k)$ and $x_1\theta_i=a_i \in S_i$. Then

$$\begin{aligned}
(x_1 +_s x_2)\theta_i &= [(a_1,a_2,\cdots,a_k) +_s (b_1,b_2,\cdots,b_k)]\,\theta_i \\
&= (a_1+b_1,a_2+b_2,\cdots,a_k+b_k)\ \theta_i \\
&= a_i + b_i \\
&= (a_1,a_2,\cdots,a_k)\theta_i +_s (b_1,b_2,\cdots,b_k)\theta_i \\
&= x_1\theta_i +_s x_2\theta_i \quad \text{, and} \\
(x_1 \cdot_s x_2)\theta_i &= [(a_1,a_2,\cdots,a_k) \cdot_s (b_1,b_2,\cdots,b_k)]\,\theta_i \\
&= (a_1\cdot b_1,a_2\cdot b_2,\cdots,a_k\cdot b_k)\theta_i \\
&= a_i\cdot b_i \\
&= (a_1,a_2,\cdots,a_k)\theta_i \cdot_s (b_1,b_2,\cdots,b_k)\theta_i \\
&= x_1\theta_i \cdot_s x_2\theta_i \quad .
\end{aligned}$$

Hence θ_i is an onto homomorphism.

<u>Definition</u> <u>3-7</u>. Let T be the subring of the complete direct sum S of rings S_i where $i \in N$. Let θ_i be the homomorphism from S onto S_i. If $T\theta_i=S_i, i \in N$, then T is a subdirect sum of the rings S_i, $i \in N$.

Before proving the next theorem, two more lemmas will be stated without proof.

<u>Definition</u>. A ring is said to be subdirectly irreducible if it has no non-trivial representation as a subdirect sum of any rings.

<u>Definition</u> <u>3-8</u>. If a ring R is isomorphic to a subdirect

sum T of rings S_i, $i \in N$, then T is said to be a representation of R as a subdirect sum of the rings S_i, $i \in N$.

Lemma 3-1. Every ring R is isomorphic to a subdirect sum of subdirectly irreducible rings.

Lemma 3-2. A subdirectly irreducible commutative ring with more than one element and with no non-zero nilpotent elements is a field.

Theorem 3-7. A ring is isomorphic to a subdirect sum of fields I/(2) if and only if it is a Boolean ring.

Proof: Clearly, I/(2) is a commutative ring. Since I/(2) satisfies the conditions of a field, I/(2) is a field. Moreover, every element of I/(2) is idempotent, since $0^2 = 0$ and $1^2 = 1$. Let S be the complete direct sum of these fields I/(2) and T be any subdirect sum of the fields I/(2). It follows that T is a subring of S. For any $x_1 = (a_1, a_2, \cdots, a_k)$ $x_2 = (b_1, b_2, \cdots, b_k) \in T$, $i \in N$, and $a_i, b_i \in S_i$, then

$$\begin{aligned} x_1^2 &= (a_1, a_2, \cdots, a_k)^2 \\ &= (a_1, a_2, \cdots, a_k) \cdot_s (a_1, a_2, \cdots, a_k) \\ &= (a_1 \cdot a_1, a_2 \cdot a_2, \cdots, a_k \cdot a_k) \\ &= (a_1^2, a_2{}^2, \cdots, a_k^2) \end{aligned}$$

where $a_i = 0$ or $a_i = 1$. But $0^2 = 0$ and $1^2 = 1$, so $x_1^2 = (a_1, a_2, \cdots, a_k)$ for any $x_1 \in T$. Thus, T is a Boolean ring. If a ring B is isomorphic to T, then there exists an isomorphism ρ such that $a\rho = x \in T$. Now $(a \cdot a)\rho = a\rho \cdot_s a \quad = x \cdot_s x = x \in T$ with

$a\xi=x$, hence $(a\cdot a)\xi=a\xi$. Since ξ is one to one, then $a\cdot a=a$ for every $a\in B$. Therefore, B is a Boolean ring.

Now one must show that if B is a Boolean ring, then B is isomorphic to a subdirect sum of fields $I/(2)$. By lemma 3-1, B is isomorphic to a subdirect sum of subdirectly irreducible rings. By definition of the subdirect sum T of rings, there exist homomorphisms θ_i such that $T\theta_i=S_i$, $i\in N$. B is isomorphic to T, then for any $x\in T$ there exists $a\in B$ such that $a\xi=x$ and $(a\cdot a)\xi=a\xi\cdot_s a\xi=x\cdot_s x=x^2$. But $a\cdot a=a\in B$ implies $(a\cdot a)\xi=a\xi$, and hence $x^2=x$ for every $x\in T$. Hence T is a Boolean ring. Therefore, if B_1 is a Boolean ring and also is homomorphic onto B_2, then B_2 is a Boolean ring. Now there exist homomorphisms θ_i such that T is homomorphic onto S_i. Being homomorphic onto images of a Boolean ring T, the S_i are Boolean rings. For every $i\in N$, a Boolean ring contains no non-zero nilpotent elements. By theorem 3-3, a Boolean ring has characteristic 2. Furthermore, by theorem 3-2, a Boolean ring is commutative. Thus by lemma 3-2, each S_i is a field. Since each S_i is a Boolean ring and a field, it contains at least two elements, and every element a_i in S_i satisfies $a_i^2=a_i$. Hence, at least the zero element 0_i and the identity e_i must be in every S_i. Now if there exists $c_i\in S_i$ such that $c_i\neq 0_i$ and $c_i\neq e_i$, then $c_i\cdot c_i=c_i^2=c_i=c_i\cdot e_i$. Since S_i is a ring for every $i\in N$, $c_i\cdot(c_i-e_i)=0_i$. $c_i\neq 0$ so $c_i=e_i$. Hence, there exist no elements in S_i except 0_i and e_i.

Define g_2 by $0_i g_2 = 0$ and $e_i g_2 = 1$. By the tables below, g_2 is a one to one mapping and is also an onto mapping. Hence S_i is isomorphic to $I/(2)$.

$+$	0_i	e_i
0_i	0_i	e_i
e_i	e_i	0_i

$\cdot$	0_i	e_i
0_i	0_i	0_i
e_i	0_i	e_i

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Define θ_i' as follows: $x_1\theta_i' = (x_1\theta_i)g_2 = x_{1i}'g_2 = x_{1i}''$ where $x_1, x_2 \in T$, $x_{1i}' \in S_i$ and $x_{1i}'' \in I/(2)$. If $x_1\theta_i' = x_{1i}''$, $x_2\theta_i' = x_{2i}''$ and $x_{1i}'' \neq x_{2i}''$, then $x_{1i}' \neq x_{2i}'$ and $x_1 \neq x_2$. Hence θ_i is a mapping. For every x_{2i}'' there exists a x_{1i}' in S_i such that $x_{1i}'g_2 = x_{2i}''$ and for every $x_{1i}' \in S_i$ there exists at least one $x_1 \in T$ such that $x_1\theta_i = x_{1i}'$. Also

$$
\begin{aligned}
(x_1 +_s x_2)\theta_i' &= (x_1 +_s x_2)\theta_i \; g_2 \\
&= (x_1\theta_i + x_2\theta_i)g_2 \\
&= (x_{1i}' + x_{2i}')g_2 \\
&= x_{1i}'g_2 + x_{2i}'g_2 \\
&= x_{1i}'' + x_{2i}'' \\
&= x_1\theta_i' + x_2\theta_i'
\end{aligned}
$$

$$
\begin{aligned}
(x_1 \cdot_s x_2)\theta_i' &= [(x_1 \cdot_s x_2)\theta_i] g_2 \\
&= (x_1\theta_i \cdot x_2\theta_i) g_2 \\
&= x_{1i}' g_2 \cdot x_{2i}' g_2 \\
&= x_{1i}'' \cdot x_{2i}'' \\
&= x_1\theta_i' \cdot x_2\theta_i' \quad .
\end{aligned}
$$

Hence θ_i' is a homomorphism from T onto I/(2). Therefore, B is a Boolean ring isomorphic to the subdirect sum T of the fields I/(2). This completes the proof of the theorem.

A Boolean ring is sometimes called the ring of all subsets of a set. This will be examined in theorem 3-8. Let B be the set of all subsets of a given non-empty set A where B includes the empty set ϕ and the universal set A. If $a,b \in B$, define the operations + and $\cdot$ as follows:

$$+ \equiv \{(a,b),(a\cap b')\cup(a'\cap b) \mid a,b \in B \text{ and } a'=\{x/x \notin a\}\}$$

$$\cdot \equiv \{(a,b),(a\cap b) \mid a,b \in B\}$$

where $(a\cap b')\cup(a'\cap b)=\{x \mid x \in a \text{ and } x \notin b \text{ or } x \notin a \text{ and } x \in b\}$.

<u>Theorem 3-8</u>. The class of all subsets of a non-empty set is a Boolean ring with the above operations.

Proof: For every $a,b \in B$, $a+b=(a\cap b')\cup(a'\cap b) \in B$ and $a\cdot b=a\cap b \in B$.

(1) $$
\begin{aligned}
(a+b)+c &= [(a+b)\cap c'] \cup [(a+b)'\cap c] \\
&= \{[(a\cap b')\cup(a'\cap b)]\cap c'\} \cup \{[(a\cap b')\cup(a'\cap b)]'\cap c\} \\
&= \{[(a\cap b'\cap c')\cup(a'\cap b\cap c')]\} \cup \{[(a\cap b')'\cap(a'\cap b)']\cap c\} \\
&= \{[(a\cap b'\cap c')\cup(a'\cap b\cap c')]\} \cup \{[(a'\cup b)\cap(a\cup b')]\cap c\}
\end{aligned}
$$

$$= \{[(a\cap b'\cap c')\cup(a'\cap b\cap c')]\}\cup\{(a'\cup b)\cap[(a\cap c)\cup(b'\cap c)]\}$$

$$= \{[(a\cap b'\cap c')\cup(a'\cap b\cap c')]\}\cup\{(a'\cap b)\cap(a\cap c)\cup[(a'\cap b)\cap(b'\cap c)]\}$$

$$= \{[(a\cap b'\cap c)\cup(a'\cap b\cap c')]\}\cup\{a'\cap(a\cap c)\cup[b\cap(a\cap c)]$$
$$\cup[(a'\cap b\cap c)\cup(b\cap b'\cap c)]\}$$

$$= \{[(a\cap b'\cap c')\cup(a'\cap b\cap c')]\}\cup\{[b\cap(a\cap c)]\cup(a'\cap b'\cap c)\}$$

$$= \{[b\cap(a\cap c)]\cup[a'\cap b'\cap c]\}\cup\{[(a\cap b'\cap c')\cup(a'\cap b\cap c')]\}$$

$$= [(a\cap b\cap c)\cup(a\cap b'\cap c')]\cup[(a'\cap b\cap c')\cup(a'\cap b'\cap c)]$$

$$= [(\phi)\cup(a\cap c\cap b)\cup(a\cap b'\cap c')\cup(\phi)]\cup[(a'\cap b\cap c')\cup(a'\cap b'\cap c)]$$

$$= [(a\cap b'\cap b)\cup(a\cap c\cap b)\cup(a\cap b'\cap c')\cup(a\cap c\cap c')]$$
$$\cup[(a'\cap b\cap c')\cup(a'\cap b'\cap c)]$$

$$= \{[(a\cap b')\cup(a\cap c)]\cap b\}\cup\{[(a\cap b')\cup(a\cap c)]\cap c'\}\cup\{[a'\cap(b\cap c')]\}$$
$$\cup\{[(a'\cap b'\cap c)]\}$$

$$= [(a\cap b')\cup(a\cap c)\cap(b\cap c')]\cup[(a'\cap(b\cap c')\cup(a'\cap(b'\cap c)$$

$$= \{a\cap[(b'\cap c)\cap(b\cap c')]\}\cup\{[a'\cap(b\cap c')]\cup[a'\cap(b'\cap c)]\}$$

$$= \{a\cap[(b\cap c')'\cap(b'\cap c)']\}\cup\{[a'\cap(b\cap c')]\cup[a'\cap(b'\cap c)]\}$$

$$= \{a\cap[(b\cap c')\cup(b'\cap c)]'\}\cup\{a'\cap[(b\cap c')\cup(b'\cap c)]\}$$

$$= [a\cap(b+c)']\cup[a'\cap(b+c)]$$

$$= a + (b + c)\ .$$

(2) $a + \phi = (a\cap\phi')\cup(a'\cap\phi) = a\cup\phi = a$

(3) $a + a = (a\cap a')\cup(a'\cap a) = \phi\cup\phi = \phi$

(4) $a + b = (a\cap b')\cup(a'\cap b)$

$$= (b'\cap a)\cup(b\cap a')$$

$$= (b\cap a')\cup(b'\cap a)$$

$$= b + a$$

(5) $(a\cdot b)\cdot c = (a\cap b)\cap c = a\cap(b\cap c) = a\cdot(b\cdot c)$

(6) $$\begin{aligned} a\cdot(b+c) &= a\cap[(b\cap c')\cup(b'\cap c)] \\ &= (a\cap b\cap c')\cup(a\cap b'\cap c) \\ &= (a\cap b\cap c')\cup(a\cap c\cap b') \\ &= [(\phi)\cup(a\cap b\cap c')]\cup[(\phi)\cup(a\cap c\cap b')] \\ &= [(a\cap b\cap a')\cup(a\cap b\cap c')]\cup[(a'\cap a\cap c)\cup(b'\cap a\cap c)] \\ &= [(a\cap b)\cap(a'\cup c')]\cup[(a'\cup b')\cap(a\cap c)] \\ &= [(a\cap b)\cap(a\cap c)']\cup[(a\cap b)'\cap(a\ c)] \\ &= (a\cap b) + (a\cap c) \\ &= a\cdot b + a\cdot c \end{aligned}$$

(7) $a\cdot A = a\cap A = a$. Hence A is the identity of B.

(8) $a\cdot b = a\cap b = b\cap a = b\cdot a$.

(9) $a^2 = a\cdot a = a\cap a = a$.

Therefore, B is a Boolean ring.

Lemma 3-3. If a ring R has a representation as a subdirect sum T of rings S_i, $i \in N$, then for each $i \in N$ there exists a homomorphism ϕ_i of R onto S_i such that if $r \in R$ and $r \neq 0 \in R$, then $r\phi_i \neq 0 \in S_i$ for at least one $i \in N$.

Proof: Let $\S$ be the isomorphism from R to T. By definition of subdirect sum, there exists a homomorphism θ_i such that $T\theta_i = S_i$ for every $i \in N$. Define ϕ_i by $r_1\phi_i = r_1'\theta_i = r_1''$ where $r_1' = r_1\S$, $r_1'' \in S_i$ and $r_1 \in R$ for $i \in N$. If $r_1'' \neq r_2''$, then $r_1' \neq r_2'$. But θ_i is a mapping and $\S$ is an isomorphism, then $r_1 \neq r_2$. Hence ϕ_i is a mapping. For any $r_1'' \in S_i$ there exists at least one $r_1' \in T$ such that $r_1'\theta_i = r_1''$. But θ_i is onto and $\mathcal{S}$ is an isomorphism for every r_1' in T, thus there exists a r_1 in R such that $r_1\mathcal{S} = r_1'$. Hence for every $r_1'' \in S_i$ there exists at least one $r_1 \in R$ such that ϕ_i is an onto mapping. Let $r_1, r_2 \in R$ such that $r_1\phi_i = r_1''$ and $r_2\phi_i = r_2''$. Then

$$\begin{aligned}
(r_1+r_2)\phi_i &= (r_1+r_2)'\,\theta_i \\
&= [(r_1+r_2)\mathcal{S}]\,\theta_i \\
&= (r_1\mathcal{S} +_s r_2\mathcal{S})\theta_i \\
&= (r_1' +_s r_2')\theta_i \\
&= r_1'\theta_i + r_2'\theta_i \\
&= r_1\phi_i + r_2\phi_i \quad , \quad \text{and} \\
(r_1\cdot r_2)\phi_i &= (r_1\cdot r_2)'\,\theta_i \\
&= [(r_1\cdot r_2)\mathcal{S}]\theta_i \\
&= (r_1\mathcal{S} \cdot_s r_2\mathcal{S})\theta_i \\
&= (r_1' \cdot_s r_2')\theta_i \\
&= r_1'\theta_i \cdot r_2'\theta_i \\
&= r_1\phi_i \cdot r_2\phi_i \quad .
\end{aligned}$$

Hence ϕ_i is a homomorphism from R onto S_i for $i \in N$. If $r_1 \in R$ and $r_1 \neq 0$, and since $\mathcal{S}$ is an isomorphism and $r_1\mathcal{S} = r_1' \in T$, where $r_1' \neq 0 \in T$, then for some $i \in N$ $r_1\phi_i \neq 0_i \in S_i$. This completes the proof of the lemma.

Theorem 3-9. Every Boolean ring B is isomorphic to a ring of subsets of some non-empty set.

Proof: If B is a Boolean ring, by theorem 3-7, B is isomorphic to the subdirect sum T of fields I/(2). By lemma 3-3, since B has a representation as a subdirect sum of fields I/(2), then there exist homomorphisms ϕ_i of B onto I/(2) such that if $r \in B$ and $r \neq 0 \in R$, then $r\phi_i \neq 0 \in I/(2)$ for at least one $i \in N$. Let H be the set of homomorphisms of B onto I/(2), that is

$$H \equiv \{\phi_i / i \in N\} .$$

By lemma 3-3, if $a \in B$ and $a \neq 0 \in B$, then $a\phi_i \neq 0$ for at least one $i \in N$. For every $a \in B$ there must be either $a\phi_i = 0_i$ or $a\phi_i = 1_i$. Let

$$H_a \equiv \{\phi_i / a\phi_i = 1_i \text{ and } i \in N\} .$$

Suppose $H_a \neq H_b$. Then by definition, $a\phi_i \neq b\phi_i$ which implies that $a \neq b$ for ϕ_i is a mapping. Hence $a \rightarrow H_a$ is a mapping from B to a certain subset H_a of H. Since ϕ_i is an onto mapping from B onto I/(2), $i \in N$, then for any subset of H there exists at least one element in B such that the mapping from B to the subsets of H is onto. Suppose $H_a = H_b$. By definition, $a\phi_i = b\phi_i$ and $a\phi_i - b\phi_i = 0_i$. Since ϕ_i are homomorphisms, then

$$(a-b)\phi_i = 0_i$$

$$a-b = 0_i$$

$$a = b$$

Therefore, the mapping from B onto $I/(2)$ is one to one. Since $(a\cdot b)\phi_i = a\phi_i\cdot b\phi_i$ and $(a\cdot b)\phi_i = 1_i$, then $a\phi_i=1_i$ and $b\phi_i=1_i$. It follows that $\phi_i \in H_a$ and $\phi_i \in H_b$ if $\phi_i \in H_{ab}$. Hence $H_{ab} = H_a \cap H_b = H_a \cdot H_b$. For $(a+b)\phi_i = a\phi_i + b\phi_i$ and $(a+b)\phi_i=1_i$, either $a\phi_i=1_i$ and $b\phi_i=0_i$ or $a\phi_i=0_i$ and $b\phi_i=1_i$ can be obtained. It follows that $\phi_i \in H_a$, $\phi_i \notin H_b$ or $\phi_i \notin H_a$, $\phi_i \in H_b$. Define

$$\phi_i \equiv_b \{x / x \in H_a \text{ and } x \notin H_b \text{ or } x \notin H_a \text{ and } x \in H_b\} ,$$

then $\phi_i \in H_a + H_b$ which implies that

$$H_{a+b} = (H_a \cap H_b') \cup (H_a' \cap H_b) = H_a + H_b .$$

Therefore, the mapping from B to the subsets of H is homomorphic, and the mapping $a \rightarrow H_a$ is an isomorphism.

CHAPTER BIBLIOGRAPHY

1. Halmos, Paul R., Lectures on Boolean Algebras, New York, D. Van Nostrand Company, 1963.

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

3. Warner, Seth, Modern Algebra, Vol. I, Englewood Cliffs, Prentice-Hall, 1965.

BIBLIOGRAPHY

Halmos, Paul R., _Lectures on Boolean Algebras_, New York, D. Van Nostrand Company, 1963.

Herstein, I. N., _Topics in Algebra_, New York, Blaisdell Publishing Company, 1964.

McCoy, Neal H., _The Theory of Rings_, New York, MacMillan Company, 1964.

Waerder, B. L., _Modern Algebra_, Vol. I, translated by Fred Blum, New York, Frederick Ungar Publishing Co., 1949.

Warner, Seth, _Modern Algebra_, Vol. I, Englewood Cliffs, Prentice-Hall, 1965.

Zariski, Oscar and Pierre Samuel, _Commutative Algebra_, Vol. I, New York, D. Van Nostrand Company, 1958.