$R_1 \cap R_2 \subseteq R$ and it is non-empty since $0 \in R_1$ and $0 \in R_2$.

Let $a, b \in R_1 \cap R_2$, then

$a \in R_1, b \in R_1$ and

$a \in R_2, b \in R_2$.

Since $(R_1 +, .)$ and $(R_2, +, .)$ are subrings, then $a - b \in R_1$

$a . b \in R_1$

and $a - b \in R_2$

$a . b \in R_2$

Therefore,

$a - b \in R_1 \cap R_2$

and $a, b \in R_1 \cap R_2$.

This proves that $(R_1 \cap R_2 +, .)$ is a subring.

COROLLARY. 1 : The intersection of any collection of subrings under the operations of addition and multiplication of the parent ring $(R, +, .)$ is a subring.

N **Definition 6.40 :** Let $(R, +, .)$ be a ring such that $a . a = a$ for all $a \in R$, then the ring $(R, +, .)$ is said to be Boolean ring.

Example 6.41 : (1) The ring $(P(S), \Delta, \cap)$ of power set of S is a Boolean ring.

Since

$A \cap A = A$, for all $A \in P(S)$.

THEOREM 6.42 : If $(R, +, .)$ is a Boolean ring, then

$a + a = 0, \forall a \in R$.

PROOF : Since $a \in R$, then $a + a \in R$.

Since $(R, + , .)$ is a Boolean ring, then

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

By cancellation law we have

$a + a = 0$

That is, each element of the Boolean ring is the additive inverse of itself.

N ***Example 6.43 :*** Let a and b be the elements of a Boolean ring $(R, +, .)$ with $a + b = 0$. Prove that $a = b$.

Solution: Since $a \in R$, then

$a + a \in R$.

Since $(R, +, .)$ is a Boolean ring, then

$a + a = 0$, by the theorem 6.42

and we have $a + a = 0$

So $a + a = 0 = a + b$.

By cancellation law we obtain

$a = b$.

N ***THEOREM 6.44 :*** Every Boolean ring $(R, +, .)$ is commutative.

PROOF. Let $a, b \in R$, then

$a + b \in R$.

Since $(R, +, .)$ is a Boolean ring, then

$(a + b) = (a + b)^2 = (a + b) . (a + b)$.

or $= a . (a + b) + b . (a + b)$.

or $= a . a + a . b + b . a + b . b$

or $= a^2 + a . b + b . a + b^2$

or $= (a + b) + (a . b + b . a)$.

Thus $a + b + 0 = a + b + (b . a + a . b)$

By cancellation law we obtain

$0 = b . a + a . b$.

By the example 6.43 we have

$b . a = a . b$.

N **Definition 6.45 :** Let $(R, +, .)$ be a ring. The set $\{c \in R \mid c . x = x . c, \forall x \in R\}$, denoted by Cent R, is called the centre of the ring $(R, +, .)$. In other words, Cent R is the set of all those elements of R which commute with every element of R with respect to multiplication.

N ***THEOREM 6.46 :*** (Cent R, +, .) is a subring of $(R, +, .)$.

PROOF : Let $a, b \in$ Cent R, then

$a . x = x . a, \forall x \in R$,

$b . x = x . b, \forall x \in R$.

$$\begin{aligned}\text{Now } (a - b) . x &= a . x - b . x, && \forall x \in R\\ &= x . a - x . b, && \forall x \in R\\ &= x . (a - b), && \forall x \in R\end{aligned}$$

which shows $a - b \in$ Cent R.

Again

$$\begin{aligned}(a . b) . x &= a . (b . x)\\ &= a . (x . b)\\ &= (a . x) . b\\ &= (x . a) . b\\ &= x . (a . b).\end{aligned}$$

and it shows that

$a . b \in$ Cent R

This proves the theorem.

Exercises 4.3

1. Let $(\{m, n, p, q\}, +, .)$ be a ring and addition and multiplication be defined by the following tables :

+	m	n	p	q
m	m	n	p	q
n	n	m	q	p
p	p	q	m	n
q	q	p	n	m

.	m	n	p	q
m	m	m	m	m
n	m	n	m	n
p	m	p	m	p
q	m	q	m	q

Check associative law, distributive law, and commutative law.
Does the relation $(p+q)^2 = p^2 + 2\,p\,.\,q + q^2$ hold ?

2. Prove that $(P(S), \cup, \cap)$ is not ring, where addition and multiplication are defined by set union and set intersection.
3. Find the characteristic of each of the following rings :
   (a) The ring of integers of modulo 7, with addition and multiplication modulo 7.
   (b) The ring of real numbers, with ordinary addition and multiplication.
   (c) The ring of even integers, with ordinary addition and multiplication.
   (d) The ring of all 2×2 matrices with addition and multiplication of matrices.
4. Let $(R, +, .)$ be a ring. Then show that $(S, +, .)$ is a subring of $(R, +, .)$ if and only if :
   (i) S is a non-empty subset of R,
   (ii) $a, b \in S \Rightarrow a - b \in S$,
   (iii) $a, b \in S \Rightarrow a\,.\,b \in S$.
5. Prove that the system $(\{0, 3, 6, 9\}, +_{12}, \odot_{12})$ is a subring of $(Z_{12}, +_{12}, \odot_{12})$, the ring of integers modulo 12.
6. Let $(R, +, .)$ be a ring such that $x^2 = x$, $\forall x \in R$. The prove that
   (1) $(R, +, .)$ is commutative.
   (2) $(R, +, .)$ has characteristic 2.
   (3) $(a+b)^2 = a^2 + b^2 = (a-b)^2$
7. Let $(R, +, .)$ be a ring with identity. Then prove that $(R, +, .)$ has characteristic $n > o$ if and only if n is the least positive integers for which $n\,.\,1 = 0$.
8. Prove that the set of (2×2) matrices over the integers with addition and multiplication of matrices is a non-commutative ring.
9. Define the characteristic of a ring and deduce the characteristic of $(Z/(4), +_4\, \odot_4)$.

6.5. IDEALS AND QUOTIENT RINGS

In this section we introduce an important class of subrings which are more special than subrings, known as ideals.

N **Definition 6.47** : $(R, +, .)$ be a ring and $\phi \neq I \subseteq R$. Then the triple $(I, +, .)$ is an ideal of the ring $(R, +, .)$ if, and only if :

(1) $a, b \in I \Rightarrow a - b \in I$,
(2) $a \in I$, $r \in R \Rightarrow a\,.\,r \in I$ and $r\,.\,a \in I$.
In a commutative ring we need only $r\,.\,a \in I$.

N **Definition 6.48 :** If $a, b \in I$, $a - b \in I$ and if $a \in I$, $r \in R$, $a\,.\,r \in I$, then $(I, +, .)$ is called right ideal of the Ring $(R, +, .)$.

Definition 6.49 : If $a, b \in I$, $a - b \in I$, and if $a \in I$, $r \in R$, $r\,.\,a \in I$, then $(I, +, .)$ is called left ideal of the ring $(R, +, .)$.

THEOREM 6.50 : Let $(R, +, .)$ be a ring and $(I, +, .)$ be an ideal in $(R, +, .)$ then $(I, +, .)$ is a subring of $(R, +, .)$.

PROOF : Let $(I, +, .)$ be an ideal. Then by the definition of an ideal, I is non-empty set, and if $a, b \in I$, then $a - b \in I$. Thus, $(I, +, .)$ is subgroup of the additive group $(R, +, .)$.

Let $a, b \in I$, then $b \in R$ since $I \subset R$. By the definition of an ideal $a\,.\,b \in I$, which implies I is closed under multiplication, this completes the proof of the theorem.

But the converse of the theorem is not true, that is, some rings have subrings which are not ideals. Some examples are given below :

Example 6.51 : Let $(Q, +, .)$ be a ring of rational numbers with the usual operation of addition and multiplication. The system $(Z, +, .)$ is subring of integers of the ring $(Q, +, .)$. In order to establish the fact, it is sufficient to find an integer a and one rational number r such that $a\,.\,r \notin Z$, we observe that $1 \in Z$, $1/2 \in Q$ but $1\,.\,1/2 \notin Z$, which shows $(Z, +, .)$ is not an ideal.

Example 6.52 : Let $(Q, +, .)$ be a subring of the ring $(R, +, .)$ of real numbers. We see that $1/2 \in Q$, $\sqrt{2} \in R$ but $1/2$, $\sqrt{2} \notin Q$, which shows that the subring $(Q, +, .)$ of rational numbers of the ring $(R, +, .)$ of real numbers is not an ideal.

Example 6.53 : In any ring $(R, +, .)$ the trivial subrings $(R, +, .)$ and $(\{0\}, +, .)$ are both ideals.

Definition 6.54 : A ring $(R, +, .)$ is called a simple ring if it does not contain proper ideals.

Example 6.55 : $(\{0, 3, 6, 9\}, +_{12}, \odot_{12})$ is an ideal of the ring $(Z_{12}, +_{12}, \odot_{12})$ the ring of integers modulo 12.

Example 6.56 : For a fixed integer $a \in Z$, the set $(a) = \{na \mid n \in Z\}$. We see that the triple $((a), +, .)$ is an ideal of the ring $(Z, +, .)$. For, if $na \in (a)$, $m\,a \in (a)$ then $na - ma = (n - m)\,.\,a \in (a)$ and $(m)\,(na) = (mn)\,a \in (a)$.

In particular $a = 2$, the ring of even integers $(E, +, .)$ is an ideal of $(Z, +, .)$, the ring of integers.

Example 6.57 : Let $(K_2, +, .)$ be a ring of all matrices of order 2 over the real numbers. Let U be the set of all matrices of K_2 of the form

$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, then $(U, +, .)$ is right ideal.

For, if $\begin{bmatrix} c & d \\ p & q \end{bmatrix} \in K_2$, then

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c & d \\ p & q \end{bmatrix} = \begin{bmatrix} ac+dp & ad+bq \\ 0+0 & 0+0 \end{bmatrix}$$

which belongs to U.

Let V be the set of all matrices of K_2 of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ then $(V, +, .)$ is a left ideal. For, if $\begin{bmatrix} c & d \\ p & q \end{bmatrix} \in K_2$, then

$$\begin{bmatrix} c & d \\ p & q \end{bmatrix} \cdot \begin{bmatrix} a & o \\ b & o \end{bmatrix} = \begin{bmatrix} ac+db & o+o \\ ap+bq & o+o \end{bmatrix} \in V.$$

And let W be the set of all matrices of K_2 of the form $\begin{bmatrix} a & b \\ o & c \end{bmatrix}$, then $(W, +, .)$ is a subring of $(K_2, +, .)$ but neither a right ideal nor a left ideal.

N ***THEOREM 6.58 :*** Let $(I_1, +, .)$ and $(I_2, +, .)$ be two ideals of the ring $(R, +, .)$, then $(I_1 \cap I_2, +, .)$ is also an ideal.

PROOF : We observe that $I_1 \cap I_2$ is non-empty since $0 \in I_1$, and $0 \in I_2$.

Let $a, b \in I_1 \cap I_2$, then

$a, b \in I_1$ and $a, b \in I_2$.

Since $(I_1, +, .)$ and $(I_2, +, .)$ are ideals,

$a, b \in I_1 \Rightarrow a - b \in I_1$ and $a . r \in I_1, b . r \in I_1$.

$a . r \in I_1, b . r \in I_1 \Rightarrow a . r - b . r \in I_1$, thus, if $a - b \in I_1$, then $(a - b) . r \in I_1$.

Again, $a, b \in I_2 \Rightarrow a - b \in I_2, a . r$ and $b . r \in I_2$

Thus $(a - b) . r \in I_2$.

Therefore $a - b \in I_1 \cap I_2$ and

$ar, b . r \in I_1 \cap I_2$.

Hence $(I_1 \cap I_2 +, .)$ is an ideal.

COROLLARY : If $(I_i, +, .)$ is an arbitrary indexed collection of ideals of the ring $(R, +, .)$ then so is also $(\cap I_i, +, .)$.

N ***THEOREM 6.59 :*** If $(I, +, .)$ is a proper ideal of the ring $(R, +, .)$ with identity, then no element of I has a multiplicate inverse.

PROOF : Let $a \in I$ such that there exists $a^{-1} \in R$. Since I is closed under multiplication by the elements of R, then

$a . a^{-1} = 1 \in I.$

Let $r \in R$, then

$1 . r = r \in I,$

which shows that $R \subseteq I$ and we have $I \subseteq R$. This proves $R = I$ which is contradicting the hypothesis that I is a proper subset of R. This proves the theorem.

N **Definition 6.60 :** The intersection of all ideals in a ring $(R, +, .)$ which contain a given non-empty set K of elements of R is called the ideal generated by K.

Now have a special case, if $K = \{a\}$.

Definition 6.61 : An ideal in a commutative ring $(R, +, .)$ with identity generated by one element of R is called a Principle ideal. The ideal generated by the element a is denoted by $((a), +, .)$.

Definition 6.62 : A commutative ring $(R, +, .)$ with identity is called a Principal ideal ring if every ideal in the ring $(R, +, .)$ is a principal ideal.

N ***THEOREM 6.63 :*** The ring $(Z, +, .)$ of integers is a principal ideal ring.

PROOF : Let $(A, +, .)$ be an ideal of the ring $(Z, +, .)$ of integers. If $A = (0)$, then $(\{0\}, +, .)$ is a principal ideal generated by the element 0. If $A \neq (0)$, A contains positive integers, and let us assume that n is the smallest positive integer such that $n \in A$. Certainly, $(n) \subseteq A$, and we only need to prove that $A \subseteq (n)$. Let $a \in A$, then there exist integers q and r such that

$a = q\,n + r, 0 \leq r < n.$

Since $a \in A$, $n \in A$, and $qn \in A$, and $r = a - qn \in A$.

If $r > 0$, we have a contradiction to the assumption that n is the smallest positive integer. That is, $r = 0$ and $a = qn$. It follow, that $a \in (n)$, so $A \subseteq (n)$ which implies $(n) = A$.

Thus the proof is completed.

There are many rings which have ideals that are not principal ideals. The ring $(K_2, +, .)$ of all matrices of order 2 has the ideal $(U, +, .)$ of all matrices of K_2 of the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ which is not a principal ideal.

N ***THEOREM 6.64 :*** Let $a_1, a_2, \ldots, a_n$ be non-zero elements of a principal ideal of ring $(R, +, .)$. Then

$(\cap (a_i), +, .) = ((a), +, .),$

where a is the least common multiple of $a_1, a_2, \ldots a_n$.

PROOF : Let $a_1, a_2, \ldots, a_n$ be the elements of the ring $(R, +, .)$. By the common multiple a of $a_1, a_2, \ldots a_n$ we mean that a is common multiple of $a_1, a_2, \ldots a_n$ under the operation of ring multiplication. Thus $a \in R$. Now the element a is called the least common multiple of $a_1, a_2, \ldots, a_n$ if a is common multiple of $a_1, a_2, \ldots, a_n$ and every other common multiple of $a_1, a_2, \ldots a_n$ is a multiple of a as well.

Since the ring $(R, +, .)$ is a principal ideal ring, then the principal ideal $((a), +, .)$ generated by the least common multiple a of $a_1, a_2, \ldots a_n$ exists, and we have the principal ideals $((a_i), +, .)$ $i = 1, 2, \ldots n$. Therefore $(\cap (a_i), +, .)$

is an ideal of $(R, +, .)$ by cordlary of theorem 6.58. But the ideal $(\cap (a_i), +, .)$ is a principal ideal because $(R, +, .)$ is the principal ideal ring. Therefore there exists an element $a \in R$ such that $(a) = \cap (a_i)$ which implies $(a) \subseteq (a_i)$, $i = 1, 2, \ldots, n$. Therefore for some $r_i \in R$, $a = r_i a_i \Rightarrow a$ is common multiple of $a_1, a_2, \ldots a_n$.

Now we assume that b is common multiple of $a_1, a_2, \ldots a_n$. Then $b = s_i . a_i$, $i = 1, 2, \ldots, n$, for some $s_i \in R$.

If $r \in R$, then

$r . b . = r . (s_i . q_i) = (r . s_i) . a_i \in (a_i)$, $i = 1, 2, \ldots n$.

Which implies $(b) \subseteq (a_i)$ for all i, that is,

$$(b) \subseteq \cap (a_i) = (a).$$

Since a is the least common multiple, b must be a multiple of a.

Example 6.65 : The ring of integers $(Z, +, .)$ is a principal ideal ring. We consider two principal ideal $((2), +, .)$ and $((3), +, .)$ generated by 2 and 3 respectively. Then we see that

$$(2) \cap (3) = (6)$$

and $((2) \cap (3), +, .) = ((6), +, .)$.

6.6. COSETS OF A RING

Now we study the cosets in a ring. The ideals play the same role in ring theory as the normal subgroups do in the group theory. If $(U, +, .)$ is an ideal of the ring $(R, +, .)$ then since addition is commutative, the system $(U, +)$ is a normal subgroup of the additive group $(R, +)$ of the ring $(R, +, .)$. Thus we can construct quotient group of R by U. Thus cosets of U assume the form $a + U = \{a + i \mid i \in U\}$, when $a \in R$.

We have seen that cosets of a normal subgroup in a group are identical or disjoint. Two cosets $a + U$ and $b + U$ are equal if $a - b \in U$. The set of cosets is denoted by R/U, where $(U, +)$ is the normal subgroup of $(R, +)$. We see that with two operations R/U forms a ring.

First, we have to define sum and product of two cosets of U in R, so that the operation of addition and multiplication are well defined.

Let addition and multiplication of cosets be defined by

$(a + U) + (b + U) = (a + b) + U$, and

$(a + U) . (b + U) = (a . b) + U$

To see that the addition and multiplication are well defined in the sense that they are independent of the representative of cosets of U. To obtain the sum and product of the cosets,

let $a + U = a' + U$, where $a, a' \notin U$,

and $b + U = b' + U$, where $b, b' \notin U$.

Then we shall show that

$(a + b) + U = (a' + b') + U$,

and $(a . b) + U = (a' . b') + U$.

If

$a + U = a' + U \Rightarrow a - a' \in U$,

$b + U = b' + U \Rightarrow b - b' \in U$.

Since $(U, +, .)$ is an ideal, then.

$$\begin{aligned}(a - a') \in U, b - b' \in U &\Rightarrow (a - a') + (b - b') \in U \\ &\Rightarrow (a + a) - (a' + b') \in U \\ &\Rightarrow (a + b) + U = (a' + b') + U.\end{aligned}$$

Again, $a - a' \in U$, $b - b' \in U$, then there exist two elements $x \in U$, $y \in U$ such that

$a - a' = x$ and $b - b' = y$

or $a = a' + x$, $b = b' + y$.

Now $\quad a . b = (a' + x) . (b' + y)$

$\quad = a' . b' + a' y + x . b' + xy.$

Since $(U, +, .)$ is an ideal, then

$a' . y + x . b' + x . y \in U$

which follows that

$ab - a'. b' = a' . y + x . b' + x . y \in U$

which implies

$a . b + U = a' . b' + U$.

Now we proceed to obtain that the system $(R/I, +, .)$ is a ring.

THEOREM 6.65 : Let $(I, +, .)$ be an ideal of the ring $(R, +, .)$ then the system $(R/I, +, .)$ is a ring, known as the quotient ring of R by I.

(1) (*Closure*). We have seen that the sum of two cosets of I is again a coset of I, that is, $(a + I) + (b + I) = (a + b) + I \in R/I$.

(2) (*Associativity*). Let $a + I, b + 1, c + I \in R/I$,

$$\begin{aligned}[(a + I) + (b + I)] + (c + I) &= [(a + b) + I] + (c + I) \\ &= ((a + b) + c) + I \\ &= (a + (b + c)) + I \\ &= (a + I) + (b + c) + I \\ &= (a + I) + [(b + I) + (c + I)].\end{aligned}$$

(3) (*Commutativity*). Let $a + I, b + I \in R/I$

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

(4) (*Existence of additive identity*). For all $a + I \in R/I$, $\exists\, 0 + I \in R/I$ such that

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

Thus $0 + I = I$ is the identity in R/I.

(5) (*Existence of additive inverse*). For $a + I$, there exists $-a + I$ such that

$$\begin{aligned}(a + 1) + (-a + I) &= a + (-a)) + I \\ &= 0 + I \\ &= ((-a) + a) + I \\ &= (-a + I) + (a + I).\end{aligned}$$

Which proves that R/I is an abelian group with addition. Now we prove that $(R/I, .)$ is a semi-group.

(6) (*Closure*). We have defined that if $a + I \in R/I$, $b + I \in R/I$, then $(a + I) . (b + I) = a . b + I \in R/I$

(7) (Associativity). Let $a + I$, $b + I$, $c + I \in R/I$,

$$\begin{aligned}[(a + I) . (b + I)] . (c + I) &= (a . b + I) . (c + I)\\ &= (a . b) . c + I\\ &= a . (b . c) + I\\ &= (a + I) . ((b . c) + I)\\ &= (a + I) . [(b + I) . (c + I)].\end{aligned}$$

(8) (*Distributivity*). $(a + I) . [(b + I) + (c + I)] = (a + I) . [b + c + I] = a . (b + c) + I = (a . b + I) + (a . c + I)$.

Thus, we have seen that $(R/I, +, .)$ is a ring, called factor ring or residue classes ring modulo I or quotient ring.

Example 6.65 **:** (1) In the ring (Z, +, .) of integers, we consider the principal ideal $((n), +, .)$, where n is a non-negative integer. The cosets of (n) in Z will assume the form

$$a + (n) = \{a + nk \mid k \in Z\} = [a]$$

Thus the cosets are precisely the congruence classes modulo n. It is clear from the definition of addition and multiplication of cosets, $(Z/(n), +, .)$ is a ring, which is merely the ring of integers modulo n.

$$(Z_n, +_n, (\cdot)_n) = (Z/(n), +, .).$$

(i) Let (Z, +, .) be the ring of integers and let (5 Z, +, .) be an ideal generated by 5. Then the system (Z/ 5 Z, +, .) is a quotient ring.

The quotient set Z/ 5 Z contains the elements 5Z, 5Z + 1, 5Z + 2, 5Z + 3, 5Z + 4.

from the operation tables it is quite obvious that (Z/5 (Z), +, .) is a ring.

+	5Z	5Z + 1	5Z + 2	5Z + 3	5Z + 4
5Z	5Z	5Z + 1	5Z + 2	5Z + 3	5Z + 4
5Z + 1	5Z + 1	5Z + 2	5Z + 3	5Z + 4	5Z
5Z + 2	5Z + 2	5Z + 3	5Z + 4	5Z	5Z + 1
5Z + 3	5Z + 3	5Z + 4	5Z	5Z + 1	5Z + 2
5Z + 4	5Z + 4	5Z	5Z + 1	5Z + 2	5Z + 3

(·)	5Z	5Z + 1	5Z + 2	5Z + 3	6Z + 4
5Z	5Z	5Z	5Z	5Z	5Z
5Z + 1	5Z	5Z + 1	5Z + 2	5Z + 3	5Z + 4
5Z + 2	5Z	5Z + 2	5Z + 4	5Z + 1	5Z + 3
5Z + 3	5Z	5Z + 3	5Z + 1	5Z + 4	5Z + 2
5Z + 4	5Z	5Z + 4	5Z + 3	5Z + 2	5Z + 1

Example 6.67: Given $(I_1, +, .)$ and $(I_2, +, .)$ are ideals of the ring $(R, +, .)$

Let $I_1 + I_2 = \{(a + b) \mid a \in I_1, b \in I_2\}$

Show that $(I_1 + I_2, +, .)$ is also an ideal of $(R, +, .)$.

Solution : Let $a + b \in I_1 + I_2$, then $a \in I_1, b \in I_2$ and $a_1 + b_1 \in I_1 + I_2$, then $a_1 \in I_1$, $b_1 \in I_2$. Since $(I_1, +, .)$ and $(I_2, +, .)$ are ideals,

$a \in I_1, a_1 \in I_1 \Rightarrow a - a_1 \in I_1$

and $r \in R, a \in I_1 \Rightarrow ar \in I_1$ and $ra \in I_1$,

again $b \in I_2, b_1 \in I_2 \Rightarrow b - b_1 \in I_2$,

and $r \in R, b \in I_2 \Rightarrow rb \in I_2$ and $br \in I_2$.

$a - a_1 \in I_1$ and $b - b_1 \in I_2$,

$\Rightarrow a - a_1 + b - b_1 \in I_1 + I_2$,

$\Rightarrow (a + b) - (a_1 + b_1) \in I_1 + I_2$,

and $ra \in I_1$, $rb \in I_2$,

$\Rightarrow ra + rb \in I_1 + I_2$.

$\Rightarrow r(a + b) \in I_1 + I_2$.

Hence $(I_1 + I_2, +, .)$ is an ideal.

Exercise 6.68: Show by example that if $(I_1, +, .)$ and $(I_2, +, .)$ are both ideals of the ring $(R +, .)$, then $(I_1 \cup I_2, +,)$ is not necessarily an ideal.

Solution: Let (Z, +, .) be a ring of integers and ((2) . +, .) and ((3), +, .) be ideals. We observe that (2) U (3) contain all integers which are multiples of 2 or 3. Thus $2 \in (2)$ and $3 \in (3)$. We see that $2 + 3 \notin (2)\, U\, (3)$. For ((2) U (3), +, .) to be an ideal it should be additive subgroup. But the sum of 2, $3 \in (2)\, U\, (3)$ does not belong to (2) U (3).

Hence ((2) U (3), +, .) is not an ideal.

But we observe that $(2) + (3) = \{a + b \mid a) \in (2)$ and $b \in (3)\}$, contains the sum of all elements of (2) and (3) which is clearly the set generated by {(2) U (3)}.

Hence ((2) + (3), + .) is an ideal.

Exercise 6.69: Let $(I_1, + .)$ and $(I_2, +, .)$ be two ideals of the ring $(R, +, .)$ such that $I_1 \cap I_2 = \{0\}$. Prove that $a.b = 0$ for every $a \in I_1, b \in I_2$.

Solution: Since $(I_1, +, .)$ and $(I_2, +, .)$ are ideals, then, If $a \in I_1$, $b \in I_2$ C R.,

then $a.b \in I_1$

and $b \in I_2$, $a \in I_1 \subseteq R$.

then $a.b \in I_2$.

That is, $a.b \in I_1 \cap I_2 = \{0\}$

Hence $a.b = 0$, for all $a \in I_1, b \in I_2$.

Exercise 6.70: Let $(R, +, .)$ be a commutative ring and $a \in R$, the set I is defined by

$$I = \{x \in R \mid x.a = 0\}.$$

Prove that $(I, +, .)$ is an ideal of $(R, +, .)$.

Solution : Let $x, y \in I$. By the definition of I, we have $x.a = 0$, $y.a = 0$

or $x.a - y.a = 0 - 0 = 0 \Rightarrow (x - y).\ a = o \Rightarrow x - y \in I$ Again, if $r \in R, x \in I$, then $x.a = 0$

and $(x \cdot r).\ a = (r.x).\ a = r\,(x.a) = 0 \Rightarrow x \cdot r \in I$ and $r.x \in I$.

since $(R, +, .)$ is commutative,

Hence $(I, +, .)$ is an ideal of $(R, +, .)$.

N

(N → notes)

PROBLEMS

1. Is the subring $(\{0, 2\}, +_4, \cdot_4)$ an ideal of the integers modulo 4?
2. Is the subring $(\{0, 3, 6\}, +_4, \cdot_4)$ an ideal of the integers modulo 9?
3. Prove that every subring of the integers is an ideal.
4. Prove that every subring of the integers modulo n is an ideal.
5. Determine the quotient rings for the ideals in question nos. 1 and 2.
6. Suppose that $(I, +, .)$ is an ideal of the ring $(R, +, .)$ Prove that if $(R, +, .)$ is commutative, then the quotient ring $(R/I, +, .)$ is commutative.
7. Let $(S, +, .)$ be an ideal and $(T, +, .)$ be a subring of the ring $(R, +, .)$. Then prove that $(S, +, .)$ is an ideal of $(S + I, +, .)$.
8. Determine all ideals of $(Z_{12}, +_{12}, \odot_{12})$, the ring of integers modulo 12.
9. Let $(I, +, .)$ be an ideal of the ring $(R, +, .)$ and let $C\,(I)$ be the set defined by
   $C\,(I) = \{r \in R \mid r.a - a.r \in I, \forall a \in R\}$.
   Determine whether $(C\,(I), +, .)$ forms a subing of $(R, +, .)$
10. Show that the ring $(R, +, .)$ of real number is a simple ring.
11. Show that the ring $(Z_n, +_n, \odot_n)$ of integers modulo n is *a* principal ideal ring.
12. Let $(I, +, .)$ be an ideal of the ring $(R, +, .)$ and define
    $ann\ I = \{r \in R \mid r.a = 0, a \in I\}$
    Prove that the system $(a_{nn}\ I, +, .)$ is an ideal of $(R, +, .)$, called *annihilator ideal of I.*
13. Let $(I, +, .)$ be an ideal of $(R, +, .)$, a commutative ring with identity. For an arbitrary element $a \in R$, the ideal generated by $I\ U\ \{a\}$ is denoted by $((I, a), +, .)$. Assuming $a \notin I$, show that
    $(I, a) = \{i + r.a \mid i \in I, r \in R\}$.
    [Hint: The set generated by $I\ U\ \{a\}$ is the set of all elements of I and of those elements which are of the forms $i + a$ or $j.a$ for all $j \in I$. So the set (I, a) generated by $I\ U\ \{a\}$ is
    $(I, a) = \{j + a \mid j \in I\}$
    $= \{\, r(j + a) \mid j \in I, r \in R\}$, Since $((I, a), +, .)$ is an ideal
    $= \{i + ra \mid i \in I, r \in R\}$, where $i = r.j \in I$.]
14. In the ring of integers, let us consider two principal ideals $((n), +, .)$ and $((m), +, .)$ generated by two non negative integers n and m respectively. Then show that
    $((n), m) = ((m), n) = (n) + (m) = (\{m, n\}) = (d)$,
    where d is the greatest common divisor of n and m.

15. Let $(I_1, +, .)$ and $(I_2, +, .)$ be two ideals of the ring $(R, +, .)$. Define the set $I_1 . I_2$ by
    $I_1 . I_2 = \{\sum a_i\, b_i \mid a_i \in I_1, b_i \in I_2\}$,
    where $\sum$ denotes a finite sum with one or more terms. Prove that $(I_1 . I_2, +, .)$ is an ideal of $(R, +, .)$
16. Let $(I, +, .)$ be an ideal of the ring $(R, +, .)$, show that
    (a) the ring $(R/I, +, .)$ may have divisor of zeros, even though $(R, +, .)$ does not have any.
    (b) If $(R, +, .)$ is a principal ideal ring, then so is the quotient ring $(R/I, +, .)$
17. Let $(R, +, .)$ be a commutative ring with identity, and Let N denote the set of all nilpotent elements of R.
    (a) Prove that $(N, +, .)$ is an ideal of $(R, +, .)$
    (b) Show that the quotient ring $(R/N, +, .)$ has no nilpotent elements. The set N is non-empty for $0^n = 0, 0 \in N$.
    [Hint: Let a and b be two nilpotent elements of R. Then there exist positive integers m and n such that $a^m = 0, b^n = 0$
    Now we consider $(a - b)^{m+n}$. By bionomial theorem we have $(a - b)^{m+n} =$
    $a^{m+n} - {}^{m+n}C_1\, a^{m+n-1}\, b + \ldots + (-1)^{m+n}\ m + n\ C_{m+n-1}\, a.b^{m+n-1}$
    $+ (-1)^{m+n}\, b^{m+n}$
    $= a^m.\ a^n - m{+}n\ C_1,\ a^m.\ a^{n-1}.\ b + \ldots + (-1)^{m+n-1}\ C_{m+n-1}\, a.b^{m-1}.\ b^n$
    $+ (-1)^{m+n}\, b^m.\ b^n$
    $= 0$ Since every term contains either a^m or b^n,
    Thus $(a - b) \in N$
    Hence the pair $(N, +)$ is subgroup of the additive group $(R, +)$ of the ring $(R, +, .)$.
    Now for every $r \in R$, we have
    $= (r.a)^m$, where m is the positive integer for which $a^m = 0$
    $= r^m.\ a^m$ Since $(R, +, .)$. is commutative
    $= 0$, Since $a^m = 0$.
    Similarly, $a.r = 0$. This shows
    $(N, +, .)$ is an ideal of the ring $(R, +, .)$
    (b) The set R/N is the set of cosets $a + N$ of N, the ideal of nil-potent elements. If $a \in N$, then $a + N = N$, so we consider $a \notin N$, that is, there does not exist any positive integer n for which $a^n = 0$.
    So $a^n \neq 0$, for any integer $n > 0$.
    Now $(a + n)^n = a^n + N \neq N$ for any integer,
    Since $a^n \notin N$. Hence the result.]
19. Let $(R, +, .)$ be a ring with the property $a^2 + a \in$ cent R for every $a \in R$. Show that $(R, +, .)$ is commutative.
20. For two ideals $(A, +, .)$ and $(B, +, .)$ of a ring $(R, +, .)$, $(A \cup B, +, .)$ is an ideal if any only if either $A \subseteq B$ or $B \subseteq A$.