Chapter 2

Subrings and Ideals

2.1 INTRODUCTION

In this chapter, we discuss, subrings, sub fields. Ideals and quotient ring. We begin our study by defining a subring. If $(R, +, \cdot)$ is a ring and S is a non-empty subset of R, then '+' and '$\cdot$', may induce binary operations '+' and '$\cdot$' respectively on S. If S is a ring with respect to these induced operations, then we call S, a subring of R.

2.2 SUBRING

Definition 2.1 Let $(R, +, \cdot)$ be a ring and let S be a non-empty subset of R. If $(S, +, \cdot)$ is a ring, then S is called a subring of R.

Every non-zero ring R has two trivial subrings, viz. the ring itself and the zero ring consisting of the zero element of the ring R.

$\{0\}$ and R are called the improper subrings of R.

If S is a subring of R, then

(i) S is a subgroup of additive group R.
i.e., $(S, +)$ is a subgroup of $(R, +)$.

(ii) S is closed with respect to multiplication.

Example 1: The set S of all 2×2 matrices of the type $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ where a, b, c are integers is subring of the ring M_2 of all $2 \times$ matrices over Z.

Example 2: The set of integers Z is a subring of the ring of real numbers.

Theorem 2.1: A non-empty subset S of a ring R is a subring of R if and only if
$a - b \in S$ and $ab \in S$ for all $a, b \in S$

Proof: Let S be a subring of R and let $a, b \in S$.

Then S is a subgroup of R under addition.

Hence, $b \in S \Rightarrow -b \in S$

and, $a \in S, b \in S \Rightarrow a \in S, -b \in S$

$\Rightarrow a + (-b) \in S$

$\Rightarrow a - b + S$

Hence, S is a subring of R.

Example 2: Show that $S = \{0, 3\}$ is a subring of $(z_6, +_6, x_6)$ under the operations $+_6$ and x_6.

Solution: We construct the composition tables as follows:

$+_6$	0	3
0	0	3
3	3	0

$\times_6$	0	3
0	0	0
3	0	3

From the above composition tables

$$a \in S, b \in S \Rightarrow a +_6 (-b) = a - b \in S$$

$$a \times_6 b \in S \quad \forall\ a, b \in S$$

Hence, S is a subring of R.

Example 3: Let m be any fixed integer and let S be any subset of Z, the set of integers, such that

$$S = \{..., -3m, -2m, -m, 0, m, 2m, 3m, ...\}$$

show that S is a subring of $(z, +, \cdot)$

Solution: Let $rm, s\ m \in S$, then $r, s \in Z$

now $rm - sm = (r - s)m \in Z \qquad (\because \quad r - s \in Z \quad \forall\ r, s \in Z)$

and, $(rm)\ (sm) = (rsm)\ m \in Z \qquad (\because \quad r\ s\ m \in Z \quad \forall\ r, s, m \in Z)$

$\therefore$ S is a subring of $(Z, +, \cdot)$

Theorem 2.2: The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are: (i) $S + (-S) = S$ and (ii) $SS \subseteq S$

Solution: Let S be a subring of R

Then $(S, +)$ is a subgroup of $(R, +)$

let $a + (-b) \in S + (-S)$, then

$$a + (-b) \in S + (-S) \Rightarrow a \in S, -b \in -S$$

$$\Rightarrow a \in S, b \in S$$

$$\Rightarrow a - b \in S$$

$$\Rightarrow a + (-b) \in S$$

Thus, $$S + (-S) \subseteq S \qquad (1)$$

$$0 \in S \Rightarrow 0 \in -S$$

Now $$a \in S, 0 \in -S \Rightarrow a + 0 \in ST\ (-S)$$

Hence, $$S \subseteq S + (-S) \qquad (2)$$

From (1) and (2), we have

$$S + (-S) = S$$

Again, S is a subring of $R \Rightarrow S$ is closed under multiplication.

Thus, $a \in S, b \in S \Rightarrow ab \in S$

but $ab \in SS$

Now $ab \in SS \Rightarrow a \in S, b \in S$

$$\Rightarrow ab \in S$$

$$\Rightarrow SS \subseteq S$$

Hence, proved.

Conversely, let $S + (-S) = S$ and $SS \subseteq S$

$\forall\ a, b \in S$, we have $ab \in SS \Rightarrow ab \in S$ $(\because \quad SS \subseteq S)$

Again $S + (-S) = S \Rightarrow S + (-S) \subseteq S$

we have $a + (-b) \in S + (-S) \subseteq S$

Thus, $\Rightarrow a + (-b) \in S \quad \forall\ a, b \in S$

$\Rightarrow a - b \in S \quad \forall\ a, b \in S$

Thus, $a - b \in S, ab \in S \quad \forall\ a, b \in S$

Hence, S is a subring of R.

Theorem 2.3: The intersection of two subrings of a ring R is a subring of R.

Proof: Let S_1 and S_2 be two subrings of a ring R.

$0 \in S_1$, $0 \in S_2$, therefore, $0 \in S_1 \cap S_2$

Thus, $S_1 \cap S_2 \neq \phi$

Now let $a, b \in S_1 \cap S_2$, then

$$a \in S_1 \cap S_2 \Rightarrow a \in S_1, a \in S_2$$

$$b \in S_1 \cap S_2 \Rightarrow b \in S_1, b \in S_2$$

But S_1, S_2 are subrings of R, therefore,

$$a \in S, b \in S_1 \Rightarrow a - b \in S_1, ab \in S_1$$

and, $a \in S_2, b \in S_2 \Rightarrow a - b \in S_2, ab \in S_2$

$$a - b \in S_1, a - b \in S_2 \Rightarrow a - b \in S_1 \cap S_2$$

$$ab \in S_1, ab \in S_2 \Rightarrow ab \in S_1 \cap S_2$$

Consequently, $a - b \in S_1 \cap S_2, ab \in S_1 \cap S_2 \quad \forall\ a, b \in S_1 \cap S_2$

Hence, $S_1 \cap S_2$ is a subring of R.

Theorem 2.4: Let R be a ring and S_1, S_2 be two subrings. Then $S_1 \cup S_2$ is a subring of R if and only if $S_1 \subseteq S_2$ or $S_2 \subseteq 1$.

3. Prove that the z of integers is a subring of R, the set real numbers under addition and multiplication.
4. Show that the set of $n \times n$ matrices over the rational numbers is a subring of $n \times n$ matrices over the real numbers under addition and multiplication matrices.
5. Show that $(\{0, 2, 4\}, +_6, \times_6)$ is a subring of $(Z_6, +_6, \times_6)$

   where, $Z_6 = \{0, 1, 2, 3, 4, 5\}$.
6. R is an integral domain. Show that the set

   $S = \{mx : x \in R, m \text{ is a fixed integer}\}$ is a subring of R.
7. If R is a ring, then show that the set

   $N(a) = \{x \in R; ax = xa\}$ is a subring of R.

2.3 IDEALS

2.3.1 Left Ideal

Definition 2.2: A non-empty subset U of a ring R is called a left ideal if

(i) $a \in U, b \in U \Rightarrow a - b \in U$

(ii) $a \in U, r \in R \Rightarrow r\,a \in U$

Example: In the ring M of 2×2 matrices over integers consider the set $U = \left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathrm{Z}\right\}$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in U \Rightarrow U \neq \phi$$

Let

$$A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix},\ B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \in U, \text{ then}$$

$$A - B = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in U$$

Also

$$P = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in M, \quad A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \in U$$

$\Rightarrow$

$$PA = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha a + \beta b & 0 \\ \gamma a + \delta b & 0 \end{bmatrix} \in U$$

This shows that U is a left ideal of M

2.3.2 Right Ideal

Definition 2.3: A non-empty set U of a ring R is called a right ideal of R if
(i) $a \in U, b \in U \Rightarrow a - b \in U$, and
(ii) $a \in U, r \in R \Rightarrow ar \in U$.

Example: Let M be the ring of 2×2 matrices one integers. Consider

$$U = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in z \right\}$$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in U \Rightarrow U \neq \phi$$

$$A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \in U B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \in U \Rightarrow A - B = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in 0$$

and, $$P = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \in U$$

we have $$AP = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

$$= \begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ 0 & 0 \end{bmatrix} \in U$$

Hence, U is a right ideal of M.

2.3.3 Ideal

Definition 2.4: A non-empty set U of a ring R is called an ideal (two-sided ideal) of R if
(i) $a \in U, b \in U \Rightarrow a - b \in U$, and
(ii) $a \in U, r \in R \Rightarrow a\, r \in U$ and $r\, a \in U$

Example: The set E of even integers is an ideal of the ring Z of integers.

$a, b \in E \Rightarrow a = 2m, b = 2n$ for some integers m and n

we have $a - b = 2m - 2n = 2(m - n) \in E$

also $r \in Z, a \in E \Rightarrow ra = r(2m) = 2(rm) \in E$

and, $ar = (2m)\, r = 2(mr) \in E$

Hence, E is an ideal of Z.

Consider $a(xr)$

$$a(xr) = (ax)\ r = 0 \cdot r = 0$$

$$\Rightarrow x\ r \in S \quad \forall\ r \in R_1\ x \in S$$

Thus, S is a right ideal of R.

Example 3: If R is a commutative ring with unity, then the ideal Ra is the smallest ideal containing a.

Proof: Let $< a > = \cap \{U: U$ is a ideal of R and $a \in U\}$

Clearly, $< a >$ is the smallest ideal which contains a.

We shall show that $< a > = Ra$.

Since Ra is an ideal and $a \in Ra$, we have

$$< a > \subset Ra$$

Let U be any ideal of R such that $a \in U$

For any $r \in R$, $r\ a \in U$ by the definition of an ideal. Hence, $Ra \subset U$. Since U is an arbitrary ideal containing a it follows that

$R\ a \subset \cap \{U: U$ is an ideal and $a \in U\}$

i.e., $Ra \subset < a >$

Hence, $$Ra = < a >$$

Theorem 2.6: If R is a ring with unity and U is an ideal of R such that $1 \in U$, then $U = R$.

Proof: U is an ideal of $R \Rightarrow U \subseteq R$ (1)

Let $x \in R$

Now $x \in R, 1 \in U \Rightarrow n \cdot 1 \in U$ (since U is a ideal of R)

$\Rightarrow$ $x \in U$

Hence, $R \subseteq U$ (2)

From (1) and (2), we have

$$U = R$$

Theorem 2.7: A field has no proper ideals.

Proof: Let F be a field and U be an ideal of R. Then we will prove that either $U = \{0\}$ or $U = F$.

From the definition of an ideal, we have $U \subseteq F$. (1)

Let $U \neq \{0\}$, $a \in U$ and $a \neq 0$

$$a \in U \Rightarrow a \in F \qquad \text{(since } U \subset F\text{)}$$

$\Rightarrow$ $a^{-1} \in F$ (since F is a field)

Now $a \in U, a^{-1} \in F \Rightarrow aa^{-1} = 1 \in U$

Let $x \in F$: then $x = x \cdot 1 \in F$

$$x \in F, 1 \in U \Rightarrow x \cdot 1 \in U \qquad \text{(since } U \text{ is an ideal)}$$

$$\Rightarrow x \in U$$

Thus, $$F \subseteq U \qquad (2)$$

From (1) and (2), we have

$$U = F$$

Therefore, $\{0\}$ and F are the only ideals of F.

Theorem 2.8: A non-zero commutative ring with unity is a field if it has no proper ideals.

Proof: Let R be a commutative ring with unity such that R has no proper ideals. In order to prove that every non-zero element in R has a multiplicative inverse, let $a \neq 0 \in R$, then the set

$$Ra = \{ra : r \in R\}$$

is an ideal of R.

R is with unity; therefore, $1 \in R$, such

$$1 \cdot a = a \in Ra$$

i.e., $a \neq 0 \in Ra \Rightarrow Ra$ is not a zero ideal

R has no proper ideals and $Ra \neq \{0\}$, therefore, it follows that

$$Ra = R$$

Now $$1 \in R \Rightarrow 1 \in Ra$$

$\Rightarrow$ there exists an element $b \in R$

such that $$1 = ba$$

$\Rightarrow$ $$a^{-1} = b$$

Thus, every non-zero element of R has a multiplicative inverse. Accordingly R is a field.

Theorem 2.9: The intersection of two ideals of a ring R is an ideal of R.

Solution: Let U_1 and U_2 be two ideals of a ring R. Then $0 \in U_1$, $0 \in U_2$ where 0 is zero element of the ring R.

We have $$0 \in U_1 \cap U_2$$

and, $$0 \in U_1 \cap U_2 \Rightarrow U_1 \cap U_2 \neq \phi$$

Let $$a, b \in U_1 \cap U_2, \quad \text{and } r \in R$$

$$a, b \in U_1 \cap U_2 \Rightarrow a, b \in U_1 \text{ and } a, b \in U_2$$

Now $$a, b \in U_1, r \in R \Rightarrow a - b \in U_1, ar, ra \in U_1 \qquad (1)$$

(since U_1 is an ideal of R)

and, $$a, b \in U_2, r \in R \Rightarrow a - b \in U_2, ar, ra \in U_2 \qquad (2)$$

(since U_2 is an ideal of R)

$$a \in U_1, b \in U_2 \Rightarrow a, b \in U_1 \cup U_2$$
$$\Rightarrow a, b \in U_1 \text{ or } a, b \in U_2$$
$$\Rightarrow a - b \in U_1 \text{ or } a - b \in U_2$$

If $a - b \in U_1$, then $a - (a - b) = b \in U_1$ ($\because$ U_1 is an ideal of R)

a contradiction

and if$a - b \in U_2$, then $b + (a - b) = a \in U_2$ ($\because$ U_2 is an ideal of R)

a contradiction

Our assumption that $U_1 \not\subset U_2$ and $U_2 \not\subset U_1$ leads to a contradiction.

Hence, $U_1 \subseteq U_2$ or $U_2 \subseteq U_1$

2.3.5 Sum of Ideals

Definition 2.6: Let U_1 and U_2 be two ideals of a ring R, then the set $U_1 + U_2 = \{a + b: a \in U_1, b \in U_2\}$ is called the sum of ideals U_1 and U_2.

Theorem 2.12: If U_1 and U_2 are any two ideals of a ring R, then $U_1 + U_2$ is an ideal of R containing both A and B.

Proof: Clearly $0 = 0 + 0 \in U_1 + U_2$; therefore, $U_1 + U_2 \neq \phi$.

Consider $\alpha = a_1 + b_1, \beta = a_2 + b_2$; $a_1, a_2 \in U_1$, and $b_1, b_2 \in U_2$

Then, we have $\alpha - \beta = (a_1 - a_2) + (b_1 - b_2) \in U_1 + U_2$

(since $a_1 - a_1 \in U_1$; $b_1 - b_2 \in U_2$ for all $a_1, a_2 \in U_1, b_1, b_2 \in U_2$)

further, for any $r \in R$,

$$\alpha r = a_1 r + b_1 r \in U_1 + U_2$$
$$r\alpha = ra_1 + rb_1 \in U_1 + U_2$$

since $a_1 r, ra_1 \in N_1$, and $b_1 r, rb_1 \in U_2$

Hence, $U_1 + U_2$ is an ideal of R.

Now $a \in U_1 \Rightarrow a = a + 0 \in U_1 + U_2$

$\Rightarrow U_1 \subseteq U_1 + U_2$ ($\because$ $0 \in U_2$)

$b \in U_2 \Rightarrow b = 0 + b \in U_1 + U_2$ ($\because$ $0 \in U_1$)

$\Rightarrow U_2 \subseteq U_1 + U_2$

This proves the theorem.

Definition 2.7: Let S be any subset of a ring R and U be an ideal of R. Then U is said be generated by S if

(i) $S \subseteq U$; and

(ii) for any ideal V of R

$$S \subseteq V \Rightarrow U \subseteq V$$

If the ideal U is generated by a subset S of a ring R, then we denote U by the symbol $< S >$. From the definition, $< S >$ is the intersection of all those ideals of R which contain S.

Theorem 2.13: If U_1 and U_2 are any two ideals of a ring R, then $U_1 + U_2 = < U_1 \cup U_2 >$.

Proof: If U_1, U_2 are ideals of R, then by the previous theorem $U_1 + U_2$ is also an ideal of R, such that $U_1 \subseteq U_1 + U_2$ and $U_2 \subseteq U_1 + U_2$.

We have $U_1 \subseteq U_1 + U_2$, $U_2 \subseteq U_1 + U_2 \Rightarrow U_1 \cup U_2 \subseteq U_1 + U_2$

Let V be any ideal of R such that

$$U_1 \cup U_2 \subseteq V$$

If $x \in U_1 + U_2$, then $x = a + b$, $a \in U_1$, $b \in U_2$

now
$$a \in U_1 \cup U_2, \quad b \in U_1 \cup U_2$$
$$\Rightarrow a, b \in V$$
$$\Rightarrow a + b \in V$$
$$\Rightarrow x \in V$$

Hence, $U_1 + U_2 \subseteq V$, consequently, by definition

$$U_1 + U_2 = < U_1 \cup U_2 >.$$

Example: If R is a ring with an R has no right ideals except R and $\{0\}$, show that R is a divisor ring.

Solution: Let $x \neq 0 \in R$

Consider $$x R = \{xr: r \in R\}$$

$$x \in R \Rightarrow x = x \cdot 1 \in xR, \text{ so } xR \neq \phi$$

Also $$xy - xz = x(y - z) \in xR \quad \forall\ xy, xz \in xR$$

and for any $S \in R$, $(xr)\, s = x\,(rs) \in x\, R$.

Thus, xR is a right ideal of R.

Since $$x \neq 0 \in xR, \quad xR = R.$$

Since R is a ring with unity, there exists $y \in R$ such that $xy = 1$.

Thus, $R - \{0\}$ is a semigroup with unity and every non-zero element of $R - \{0\}$ is right invertible. Hence, $R - \{0\}$ is a group under multiplication. Consequently, R is a divisor ring.

2.4 SIMPLE RING

Definition 2.8 A ring R is said to be simple, if

(i) there exist $a, b \in R$ such that $ab \neq 0$, and,

(ii) R has no proper ideals.

Theorem 2.14: A divisor ring is a simple ring.

$\Rightarrow r_1\, a \in V$ (Since U is an ideal)

$\Rightarrow x \in V$

Thus, $U \subset V$

Hence, U is an ideal of R generated by a, i.e., U is a principal ideal.

Example: $(Z, +, \cdot)$ is a commutative ring with unity.

$E = <2> = \{2n : n \in z\}$ is an ideal of Z generated by 2

Thus E is a principal ideal of Z.

2.6 PRINCIPAL IDEAL RING

Definition 2.10: A ring for which every ideal is a principal ideal is called a principal ideal ring.

Example: The ring $(Z_5, +_5, x_5)$ is a principal ideal ring.

Theorem 2.16: Every field is a principal ideal ring.

Proof: Let F be a field.

We know, that a field has no proper zero divisor, i.e., the null ideal and the unit ideal are the only ideals of F.

The null ideal $U = \{0\} = <0>$ is generated by 0 and the unit ideal $F = <1>$ is generated by, therefore $U = <0>$ and F are the principal ideals of F.

i.e., every ideal of F, is a principal ideal.

Hence, F is a principal ideal ring.

Example: Find the principal ideals of the ring $(Z_6, +_6, \times_6)$

Solution: We have $Z_6 = \{0, 1, 2, 3, 4, 5\}$

Clearly $(Z_6, +_6, \times_6)$ is a commutative ring with unity and it is not a field. ($\because$ Z_6 is a ring with zero divisor)

$(0) = \{0\}$ the null ideal is a principal ideal of Z_6

$(1) = z_6$, the unit ideal is a principal ideal of the ring

$(2) = \{0, 2, 4\}$ is a principal ideal of the ring

$(3) = \{0, 3\}$ is a principal ideal of the ring

$(4) = (2)$ is a principal ideal

$(5) = (1)$ is a principal ideal

Hence, the principal ideals of $(Z_6, +_6, \times_6)$ are (0), (1), {0, 3}, {0, 2, 4}

Theorem 2.17: The ring of integers Z is a principal ideal ring.

Proof: The ring of integers (Z, + , ·) is a commutative ring with unity and without zero divisors; therefore, $(Z, +, \cdot)$ is an integral domain.

Let U be an ideal of Z.

If $U = \{0\} = <0>$, then U is a principal ideal

Let us suppose that $U \neq (0)$.

U contains at least one non-zero integer say a.

Since U is a subgroup Z under addition; $a \in U \Rightarrow -a \in U$, where one of the integers, a, $-a$ is positive.

Hence, we conclude that U contains at least one positive integer. Let U^+ denote the set of all positive integers of U.

From the well ordering principle, U^+ must have at least element. Let b denote least element in U^+.

We now show that $U = (b)$; i.e., U is a principal ideal generated by b.

Let $x \in U$, then x, b are integers where $b \neq 0$. There exist integers q, r such that

$$x = bq + r,\ 0 \leq r < b$$

U is an ideal, therefore,

$$b \in U,\ q \in Z \Rightarrow bq \in U$$

also $x \in U,\ bq \in U \Rightarrow x - bq = r \in U$(Since U is a subgroup of $(Z, +)$)

but $0 \leq r < b$ and b is the least positive integer such that $b \in U$ implies that $r < b$ and $r \in U$, which is a contradiction. Therefore, r must be zero.

Hence, $x = bq$

Therefore, $U = \{bq : q \in z\} = (b)$

i.e., U is a principal ideal of Z, generated by b.

Thus, every ideal of Z is a principal ideal.

Hence, the ring of integers is a principal ideal ring.

Example: If R is a commutative ring and $a \in R$, then the principal ideal (a) is equal to the set

$$\{ar + na : r \in R, n \in Z\}$$

Solution: Let $U = \{ar + na : r \in R, n \in Z)\}$
We shall prove that U is the ideal generated by a.

Clearly $a = a0 + 1a \in U$ so that $U \neq \phi$

Let $ar + na, as + ma \in U$, where $r, s \in R$, $n, m \in Z$

Then $(ar + na) - (as + ma) = a(r - s) + (n - m)\, a \in U$

Further, if $s \in R$, then $(ar + na)s = a(rs) + a(ns)$

$$= a(rs + ns) + 0a \in U$$

which shows that U is a right ideal of R. Since R is commutative, U is also a left ideal of R.

Hence, U is an ideal of R such that $(a) \subset U$.

Let V be another ideal of R, containing (a).

Since $a \in V$ and V is an ideal of R, $ar \in V$, $n\, a \in V$ for all $r \in R$ and $n \in Z$.

Therefore, $ar + na \in V$ for all $r \in R$ and for all $n \in Z$.

Hence, $U \subseteq V$

consequently, $U = (a)$

$$= [r + U] + [(s + t) + U]$$
$$= (r + U) + [(s + U) + (t + U)$$

Thus, addition is associative in R/U

Existence of Identity: $U = 0 + U \in R/U$ such that

$$(r + U) + (0 + U) = (r + 0) + U = r + U$$

and, $(0 + U) + (r + U) = (0 + r) + U = r + U$

for all $r + U \in R/U$

Hence, $U = 0 + U$ is the identity with respect to addition.

Existence of inverse: $r + U \in R/U \Rightarrow - r + U \in R/U$ such that

$$(r + U) + (- r + U) = (r + (- r)) + U$$
$$= 0 + U = U$$

and, $(- r + U) + (r + r) = (- r + r) + U$
$$= 0 + U = U$$

Thus, each element is invertible under addition.

Commutative Property: $r + U, s + U \in R/U$

$\Rightarrow$ $(r + U) + (s + U) = (r + s) + U$
$$= (s + r) + U = (s + U) + (r + U)$$

(Since $(R, +)$ is abelian $\Rightarrow r + s = s + r \ \forall \ r, s \in R$)

Hence, $(R/U, +)$ is an abelian group.

I. R/U is closed with respect to multiplication (by def.)

Association axiom:

$$r + U, s + U, t + U \in R/U$$
$$\Rightarrow [(r + U)] (s + U) (t + U)$$
$$= (rs + U) (t + U)$$
$$= (rs)t + U$$
$$= r (st) + U \qquad (\because \quad r, s, t \in R \Rightarrow (rs)\, t = r\, (st)$$
$$= (r + U) (st + U)$$
$$= (r + U) [(s + U) (t + U)]$$

Thus, multiplication is associative in R/U.

II. Distributive Laws: We have

$$(r + U) [(s + U) + (t + U)]$$
$$= (r + U) [(s + t) + U] = (r + (s + t)] + U$$
$$= (rs + rt) + U = (rs + U) + (rt + U)$$
$$= (r + U) (s + U) + (r + U) (t + U)$$

for all $r + U, s + U, t + U \in R/U$

Similarly, we can prove that

$$[(s + U) + (t + U)] (r + U) = (s + U) (r + U) + (t + U) (r + U)$$

Hence, $(R/U, +, \cdot)$ is a ring.

Definition 2.11: Let R be a ring and U be any ideal of R, then the system $(R/U, +, \cdot)$ where $R/U = \{r + U: r \in R\}$ and '+' '·' are the binary operations on R/U defined by

$$(r + U) + (s + U) = (r + s) + U$$

$(r + U) + (s + U) = rs + U$ for all $r, s \in R$ (i.e., for all $r + U, S + U \in R/U$)

is a ring called the quotient ring of R with respect to the ideal U.

Example: Let $U = \{6n: n \in Z\}$, U is an ideal of Z and

$$Z/U = \{U, 1 + U, 2 + U, 3 + U, 4 + U, 5 + U\}$$

is the quotient ring under the operations '*' and ',', Addition modulo 6 and multiplication modulo 6.

Remarks 1: If R is commutative then R/U is also commutative, since

$$\begin{aligned}(r + U) (s + U) &= rs + U \\ &= sr + U \\ &= (s + U) (r + U)\end{aligned}$$

$(\because rs \equiv sr \ \forall \ r, s \in R)$

2. If R has unity element, then R/U also has unity element:

   Let 1 be the unity element in R, then

   $1 + U \in R/U$ such that

$$\begin{aligned}(1 + U) \cdot (r + U) &= 1 \cdot r + U \\ &= r + U\end{aligned}$$

for all $r + U \in R/U$

$(\because 1 \cdot r = r$ for all $r \in R)$

Therefore, $1 + U$ is the unity element in R/U.

2.8 PRIME IDEAL

Definition 2.12: Let R be a commutative ring. An ideal P of R is called a prime ideal if

$$ab \in P \Rightarrow a \in P \text{ or } b \in P \text{ for all } a, b \in R$$

Example 1: The ideal $(3) = \{3n : n \in z\}$ is a prime ideal in z, since

$$3 \mid ab \Rightarrow 3 \mid a \text{ or } 3 \mid b \Rightarrow a \in (3) \text{ or } b \in (3)$$

In general, $P = \{pr; r \in Z, p \text{ is a prime}\}$ is a prime ideal of Z.

$$= \{... -21, -14, -7, 0, 7, 14, 21, ...\}$$

is maximal ideal in z.

Alternative definition:

A proper ideal M of a ring R is called a maximal ideal if there does not exist an ideal U of R such that $M \subseteq U \subseteq R$.

Theorem 2.20: An ideal ring Z of integers is a maximal ideal if and only if it is generated by some prime number.

Proof: Let M be an ideal of Z generated by a prime number p, and let

$$M = \{pn: n \in z\} = < p >$$

Let U be any ideal of Z, such that

$$M \subset U \subset Z$$

Every ideal of Z is a principal ideal

Thus, $U = < q >$, q is an integer

Now $M \subset U \subset Z \Rightarrow < p > \subset < q > \subset Z$

$\Rightarrow$ $p \in < q >$

$\Rightarrow$ $p = qm$ for some $m \in Z$

but p is prime $\Rightarrow q = 1$ or $m = 1$

$m = 1 \Rightarrow p = q \Rightarrow < p > = < q >$

$\Rightarrow$ $M = U$

$q = 1 \Rightarrow < q > = z \Rightarrow U = Z$

Hence, M is maximal ideal.

Conversely, let M be a maximal ideal in Z and let $M = (p)$.

Let us assume that p is not a prime, then p must be a composite number. There exist integers a and b such that

$$p = ab.$$

Let a, b be prime numbers, then $U = < a >$ and $U \supset M$

Thus $M \subset U \subset Z$

but M is a maximal ideal

Hence, $M = U$ or $U = Z$

Case (i) When $U = z$

we have $U = < a > = < 1 >$

$\Rightarrow$ $a = 1$

Therefore, $p = ab \Rightarrow p = b$

$\Rightarrow$ p is a prime number.

Case (ii) when, $U = M$

We have $U = < a > = M$

$\Rightarrow$ $a \in M$

$\Rightarrow$ $a \in rp, r \in Z$

Therefore, $p = ab = (rp)\, b = p(rb)$

$\Rightarrow$ $1 = rb$

$\Rightarrow$ $r = 1, b = 1$

Thus, $p = a \cdot 1 = a \Rightarrow p$ is prime

Hence, M is generated by the prime p.

Theorem 2.21: An ideal $M \neq R$ of a commutative ring R with unity is maximal if and only if R/M is a field.

Proof: Let R be a commutative ring with unity and let M be a maximal ideal of the ring R. The R/M is also a commutative with unity. $1 + M$ is the unity of the ring R/M. R/M is a field, if we show that every non-zero element of R/M has a multiplicative inverse.

M is a maximal ideal of R, therefore

$$a \in R, a \notin M \Rightarrow < a > + M = R(1)$$

there exist elements $b \in R, x \in M$ such that

$$x + ab = 1$$

or $$ab - 1 = x \in M$$

If $ab - 1 \in M$, then we have

$$ab + M = 1 + M \Rightarrow (a + M)\,(b + M) = 1 + M$$

i.e., to each non-zero element $a + M \in R/M$, there exists $b + M \in R/M$

such that $(a + M)\,(b + M) = 1 + M$

Thus, $a + M \in R/M$ is invertible.

Hence, R/M is a field.

Conversely, let R/M be a field and U be an ideal of $U \neq M$ and $M \subset U$

We now show that $U = R$

Since $U \supset M$, $U \neq M$ there exists an element

$$a \in U \text{ such that } a \notin M$$

$a \notin M \Rightarrow a + M$ is a non-zero element of R/M.

R/M is a field and $a + M$ is a non-zero element in R/M.

Hence, $a + M$ is invertible

Solution: Let $a + U = b + U$

$$0 \in U \Rightarrow a = a + 0 \in a + U = b + U$$

now at $b + U \Rightarrow a = b + x$ for some $x \in U$

$\Rightarrow$ $a - b = x \in U$

Conversely, let $a - b \in U$; and $a - b = c$, then

$$a - b = c \in U \Rightarrow a = b + c$$

we have $x \in a + U \Rightarrow x = a + d$ for some $d \in U$

Hence, $x = (b + c) + d = b + (c + d) \in b + 0 \quad (\because \ c + d \in U)$

Thus, $a + U \subset b + U$

Similarly, $b + U \subset a + U$

Therefore, $a + U = b + U$