Outline of Presentation

- **Definition of Rings, Commutative & Non-commutative Rings**
- **Examples from Number Systems**
- **Ring of Integers Modulo n**
- **Ring of Quaternions**
- **Ring of Matrices**
- **Polynomial Rings**
- **Rings of Continuous functions**
- **Properties of Ring**

Definition: Let R be a non-empty set having two operations, addition '**+**' and multiplication '**.**' Then the algebraic structure **(R, +, .)** is called a R**ing** if the following properties are satisfied:

1. **R is an Abelian group under addition**

(i) If $a, b \in R \; then \; a + b \;\; \in R$.

(ii) If $a, b, c \;\in R \; then \;\; a + (b + c) = (a + b) + c$. (Associativity)

(iii) If $a, b \;\in R, \;\; then \; a + b = b + a$. (Commutativity)

(iv)If $a \;\in R, \exists \, 0 \;\in R \; such \; that \;\; a + 0 = a = 0 + a$.

(v) If $a \;\in R, 0 \;\in R, \exists - a \in R \; such \; that \; a + (-a) = 0 = (-a) + a$.

2. **R is semi-group under multiplication.**

(i) If $a, b \;\in R \; then \; a.b \;\in R$.

(ii) If $a, b, c \;\in R \; then \;\; a(b.c) = (a.b).c$ (Associativity)

3. **Distributive laws hold.**

(i) If $a, b, c \;\in R, then \; a.(b + c) = a.b + a.c$

(ii) If $a, b, c \;\in R, then \; (b + c)a = ba + ca$.

Definition: A ring R is said to be **commutative ring** if $a.b = b.a \quad \forall\, a, b \in R$.

Definition: A ring R is said to be **non-commutative ring** if $a.b \neq b.a \quad \forall\, a, b \in R$.

Definition: A ring R is said to be **ring with unity** if there exists

$$1 \in R \text{ such that } a.1 = a = 1.a \text{ for all } a \in R.$$

<u>Examples:</u>

1. R = Z, the set of integers is a ring for the usual addition and multiplication. It is commutative ring and has 1 as unit element.
2. R = 2Z, the set of even integers is a commutative ring for the usual addition and multiplication. It has no unit element.
3. R = Q, the set of rational numbers, R = R, the set of real numbers and R = C, the set of complex numbers are commutative rings with unity under usual addition and multiplication.

4. Let $R = \{ p + q\sqrt{2} : p, q \in Q\}$. Then R is a ring w.r.t. addition and multiplication of real numbers.

Solution: Let $p_1 + q_1\sqrt{2}$, $p_2 + q_2\sqrt{2} \in R$, $p_1, q_1, p_2, q_2 \in Q$.

Now $(p_1 + q_1\sqrt{2}) + (p_2 + q_2\sqrt{2}) = (p_1 + p_2) + (q_1 + q_2)\sqrt{2} \in R$

for $p_1 + p_2, q_1 + q_2 \in Q$

and

$$(p_1 + q_1\sqrt{2})(p_2 + q_2\sqrt{2}) = (p_1p_2 + 2q_1q_2) + (p_1q_2 + p_2q_1)\sqrt{2} \in R$$

as $p_1 p_2 + 2q_1q_2$, $p_1q_2 + p_2q_1 \in Q$.

Thus, R is closed with respect to addition and multiplication, R is commutative and associative. $0 + 0\sqrt{2}$ is the additive identity of R.

If $p + q\sqrt{2} \in R$, then $(-p) + (-q)\sqrt{2} \in R$ and $[(-p) + (-q)\sqrt{2}] + (p + q\sqrt{2}) = 0 + 0\sqrt{2}$

$1 = 1 + 0\sqrt{2}$ is the unit element of R. Hence R is commutative ring with unity.

5. The set $G = \{ a + ib : a, b \in Z\}$ of **Gaussian integers** forms a commutative ring with unity under addition and multiplication of complex numbers.

6. Let R = Z_n = {0,1,2,3,……….(n-1)} and addition modulo n and multiplication modulo n are the operation on Z_n. Then Z_n is a commutative ring with unity. It is called the ring of residue classes modulo n. (the proof is same as next example)

e.g. The set R = {0,1,2,3,4,5} is a commutative ring with unity w. r.t. operation of $+_6$ (addition modulo 6) and $\times_6$ (multiplication modulo 6) .

Sol: The composition table for $+_6$ is as under

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

From the table it is clear that all possible sum belong to R, therefore R is closed w.r.t. $+_6$. Associative and commutative laws hold under $+_6$. 0 is additive identity for all a in R. Inverse of each element exists, as 0 + **0** = 0, 1+**5** =0, 2 + **4** = 0, 3+**3** = 0, 4+ **2** = 0, 5 +**1** = 0.

The composition table for $\times_6$ as under

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0

1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

From the table, it is clear that R is closed w.r.t. multiplication(mod.6). Associative and commutative laws hold in R under $\times_6$..

Further $\times_6$ is distributive in R w.r.t. $+_6$. If a,b,c are any elements of R, then

$a\times_6 (b +_6 c)$ = $a\times_6 (b +_6 c)$

= least non-negative remainder when ab + ac is divided by 6

= $(ab) +_6 (ac)$

= $(a\times_6 b) +_6 (a \times_6 c)$

Similarly, we have $(b +_6 c)\times_6 a$ = $(b\times_6 a) + (c\times_6 a)$.

Also 1is the identity for $\times_6$. Therefore, R is a commutative ring with unity.

7. Example: Let R = {a +bi + cj + dk / a,b,c,d are real numbers}.

Define + in R as

$(ai +bj + ck + dj) + (a' + b' + c' + d') = (a + a') + (b +b')i +(c + c')j + (d +d')k.$

Define × in R by the rule

$i^2 = j^2 = k^2 = -1, \; ij = k = -ji, \; jk = i = -kj, \; ki = j = -ik.$

Then R is an abelian group with $0 = 0i + 0j + 0k$ as zero element and $-a - bi - cj - dk$ as the inverse of $a + bi + cj + dk$. Also, R is a semigroup under multiplication and distributive property holds good.

Thus, R is a ring with $1 = 1 + 0i + 0j + 0k$ as unit element of R. R is not commutative as i.j is not equal to j.i. This ring is called **ring of quaternions**.

8. **Example:** The set of R of all nxn matrices with their entries as real numbers is a **non-commutative ring** with unity w.r.t. matrix addition and multiplication.

Solution: As the sum and product of two n×n matrices is again a n×n matrices. Thus, R is closed w.r.t. addition and multiplication of matrices. R has the following properties.

(i) $(A + B) + C = A + (B + C)$ for all $A,B,C \in R$

(ii) $A + B = B + A$ for all $A, B \in R$

(iii) If $0 \in R$ is a null matrix, then

$$0 + A = A = A + 0 \quad \text{for all } A \in R$$

(iv) For each $A \in R$, there exist $-A \in R$ s.t.

$$A + (-A) = 0 = (-A) + A$$

(v) A (BC) = (AB)C for all A,B,C $\in$ R

(vi) A (B + C) = (AB)C for all A,B,C $\in$ R

(B+C)A = BA + CA for all A,B,C $\in$ R

(vi)If I R is a unit matrix, then AI = A = IA for all A $\in$ R.

Since the multiplication of matrix is not commutative in general, t+ herefore R is a non-commutative ring with unity as unit matrix.

Example 8: The set P of all polynomial over a ring R forms a ring under addition and multiplication defined as follows:

$$f + g = (a_0 b_0 + a_1 b_1 + a_2 b_2 + \cdots .)$$

$$f . g = (c_0 + c_1 + c_2 + \ldots)$$

where $c_k = (a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2+} \ldots \ldots) = \sum_{i+j=k} a_i b_j$ for $k \geq 0$.

Then P is ring of polynomials over R.

Example 9: The set C[0,1] of all real valued continuous functions defined in the closed interval [0,1] is a commutative ring with unity w.r.t. the addition and multiplication of functions defined as follows:

$$\boldsymbol{(f + g)(x) = f(x) + g(x)}$$

$$\boldsymbol{(f . g)(x) = f(x) g(x)}$$

where $f, g \in C[0,1]$.

Properties of Ring

Theorem : If (R, +, ×) is a ring, then for all a,b,c ∈ R. Then

(i) a.0 = 0 = 0.a for all a ∈ R

(ii) a(-b) = -(ab) = (-a)b for all a,b ∈ R

(iii) (-a)(-b) = ab for all a,b ∈ R

(iv) a(b-c) = ab – ac for all a,b,c ∈ R

(v) b(c-a) = bc – ba for all a,b,c ∈ R

Proof : (i) We have 0 = 0 + 0

a.0 = a.(0 + 0) = a.0 +a.0 (by distributive property of R). Also, 0 + a.0 = a.0 = a.0 + a.0 (as 0 is additive identity of R). By cancellation law for addition in R, 0 = a.0. Similarly, we have 0.a = a

(ii) Suppose b ∈ R, then there exist –b ∈ R s.t. b + (-b) = 0.

a(-b + b) = a.0. Then, by using distributive property of R and (i), we have

a(-b) + ab = 0 , which implies that a(-b) = -ab.

Similarly, we have (-a)b = -ab.

(iii) L.H.S. (-a)(-b) = -[(-a)b] = -[-(ab)] = ab = R.H.S , using (ii)
(iii) L.H.S a(b-c) = a[b +(-c)] = ab + a(-c) = ab –ac,
using distributive property and (ii).
(v)Similar to part (iv).

Exercise: If R is a ring such that $a^2 = a \; \forall \; a \in R$, then
(i) $a + a = 0 \; \forall \; a \in R$
(ii) $a + b = 0 \; \Rightarrow a = b$
(iii) R is commutative.
Solu: (i) a ∈ R ⇒ a + a ∈ R. By using given condition,

$$(a + a)^2 = a + a$$
$$\Rightarrow (a + a)(a + a) = a + a$$
$$\Rightarrow a(a + a) + a(a + a) = a + a$$
$$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a$$
$$\Rightarrow (a + a) + (a + a) = (a + a) + 0$$

$\Rightarrow a + a = 0,$ by using Left Cancellation Laws.

(**ii**) Given a + b = 0, also by (i) a + a= 0
Therefore, a + b = a + a. Hence, a = 0, using Left Cancellation laws.

(iv) For all $a, b \in R \Rightarrow a + b \in R$. Then by given condition,

$$(a+b)^2 = a+b$$
$$\Rightarrow (a+b)(a+b) = a+b$$
$$\Rightarrow a(a+b) + b(a+b) = a+b$$
$$\Rightarrow (a^2 + ab) + (ba + b^2) = a+b$$
$$\Rightarrow (a + ab) + (ba + b) = a+b$$
$$\Rightarrow a + b + ab + ba = a+b$$

$\Rightarrow ab + ba = 0$, by using left cancellation law

$\Rightarrow ab = ba$, using (ii).

Hence, R is commutative.