TOPIC:11- Rings and fields

Algebraic Systems with two Binary operations.

Define Ring and give an example of a ring with zero-divisor:

An algebraic System $(R, +, \cdot)$ is called a ring if the binary operations + and $\cdot$ on S satisfy the following properties.

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

(2) $(R, \cdot)$ is a Semigroup.

(3) The operation $\cdot$ is distributive over +

(ie) for any $a, b, c \in R$.

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \&$$
$$(b+c) \cdot a = b \cdot a + c \cdot a$$

Eg: The ring $(Z_{10}, +_{10}, \times_{10})$ is not an integral domain since $5 \times_{10} 2 = 0$, yet $5 \neq 0, 2 \neq 0$ in Z_{10}.

zero divisor:

An element 'a' in a ring $(R, +, \cdot)$ is said to zero divisor if $a \neq 0$ & $\exists b \neq 0$ in R such that $a \cdot b = 0$.

Without zero divisor:

Let $(R,+,\cdot)$ be a ring. Then for any $a,b \in R$ such that $a \neq 0$ & $b \neq 0$, $a \cdot b \neq 0$ and we call $(R,+,\cdot)$ is a ring without divisors of zero.

(or)

$$a \cdot b = 0 \Rightarrow (a=0 \text{ (or) } b=0).$$

Commutative ring:

If $(R,\cdot)$ is commutative, then the ring $(R,+,\cdot)$ is called a commutative ring.

Integral domain

A commutative ring $(R,+,\cdot)$ with identity and without divisors of zero is called an integral domain.

Field:

A commutative ring $(R,+,\cdot)$ which has more than one element such that every non-zero element of S has a multiplicative inverse in R called a field.

Subring :

A subset $S \subseteq R$ where $(R, +, \cdot)$ is a ring is called a subring if $(S, +, \cdot)$ is itself a ring with the operation + and $\cdot$

Eg: The ring of even integers is a subring of the ring of integers.

Ring homomorphism :

Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings. A mapping $g : R \to S$ is called a ring homomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$ if for any $a, b \in R$

$$g(a+b) = g(a) \oplus g(b) \quad \&$$

$$g(a \cdot b) = g(a) \odot g(b)$$

.

Prove that the set $Z_4 = \{[0],[1],[2],[3]\}$ is a commutative ring with respect to the binary operation addition modulo and multiplication modulo $+_4$, $\times_4$.

Proof:

The composition tables for addition modulo 4 and multiplication modulo 4 are given in table.

$+_4$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

$\times_4$	[0]	[1]	[2]	[3]
[0]	0	0	0	0
[1]	0	1	2	3
[2]	0	2	0	2
[3]	0	3	2	1

$\times$ Table

(i) All the entries in both the tables belong to Z_4.

Hence Z_4 is closed under $+_4$ and $\times_4$

(ii) In both the tables,

Entries in the first row = Entries in the 1st column.

Entries in the 2nd row = Entries in the 2nd column.

Entries in the 3rd row = Entries in the 3rd column.

Entries in the 4th row = Entries in the 4th column

$\therefore$ The operations $+_4$ and $\times_4$ are commutative in Z_4.

Hence Z_4 is closed under $+_4$ and $\times_4$

(ii) In both the tables.

Entries in the first row = Entries in the 1st column.

Entries in the 2nd row = Entries in the 2nd column.

Entries in the 3rd row = Entries in the 3rd column.

Entries in the 4th row = Entries in the 4th column.

$\therefore$ The operations $+_4$ and $\times_4$ are commutative in Z_4.

(iii) Also, for any $a, b, c \in Z_4$, we have

$$a +_4 (b +_4 c) = (a +_4 b) +_4 c.$$

$$\& \quad a \times_4 (b \times_4 c) = (a \times_4 b) \times_4 c.$$

For Eg: consider $a = 1, b = 2, c = 3$

Now $(1 +_4 2) +_4 3 = 3 +_4 3 = 2$ | & $(1 \times_4 2) \times_4 3 = 2 \times_4 3 = 2$

$1 +_4 (2 +_4 3) = 1 +_4 1 = 2$ | $1 \times_4 (2 \times_4 3) = 1 \times_4 2 = 2$

Thus the operations $+_4$ & $\times_4$ are associative in Z_4.

(iv) 0 is the additive identity of Z_4 and ~~$\times_4$ are~~ 1 is the multiplicative identity of Z_4.

(v) Additive inverse of 0, 1, 2, 3 are respectively 0, 3, 2, 1. Multiplicative inverse of the non-zero elements 1, 2 and 3 are 1, 2 and 3. respectively.

(vi) If $a, b, c \in Z_4$, then

$$a \times_4 (b +_4 c) = (a \times_4 b) +_4 (a \times_4 c)$$

Thus, the operation $\times_4$ is distributed over $+_4$ in Z_4.

Hence, $(Z_4, +_4, \times_4)$ is a commutative ring with unity.