Sri SAI RAM ENGINEERING COLLEGE
INSTITUTE OF TECHNOLOGY
West Tambaram, Chennai - 44

SAIRAM DIGITAL RESOURCES

YEAR II

SEM III

MA8351

DISCRETE MATHEMATICS
(Common to CSE & IT)

UNIT IV

ALGEBRA STRUCTURES

4.6 Definition and examples of Rings and Fields

SCIENCE & HUMANITIES

UNIT IV

4.6 Definition and examples of Rings and Fields

Definition: Ring

A non-empty set R with two binary operations denoted by $+$ and ., called addition and multiplication, is called a ring if the following axioms are satisfied

(i) (R, +) is an abelian group, with 0 as identity.

(ii) (R, .) is a semi group

(iii) The operation . is distributive over +

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

and $(b+c).a = b.a + c.a \; \forall \, a, b, c \in R.$

Note:

(R, +) is an abelian group means the following axioms

(i) $a + b \in R, \ \forall a, b \in R$ - closure

(ii $a + b = b + a \ \forall a, b \in R$ -commutativity

(iii) $a + (b + c) = (a + b) + c \forall a, b, c \in R$ –associativity

(iv) there is an element $0 \in R$ such that

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

(v) for every $a \in R$, there is $-a$ is R such that

$$a + (-a) = (-a) + a = 0$$

(R, .) is a semi group means

(vi) $a, b \in R$ and $a.(b.c) = (a.b).c$

Definition :

A ring $(R,+,.)$ is said to be commutative if $a.b = b.a \ \forall \ a,b \in R$

Examples:

1. $(Z,+,.)$, $(Q,+,.)$, $(R,+,.)$ and $(C,+,.)$ and all rings.

If $(R,+,.)$ is a ring , then the singleton set $\{0\} \subset R$ is itself a ring, called the null ring or zero ring.

SOME SPECIAL RINGS

If $(R, +, .)$ is a commutative ring, then $a \neq 0 \in R$ is said to be a zero-divisor if there exists a non-zero $b \in R$ such that $ab = 0$.

Zero divisor is also known as divisor of zero. All number rings are without divisors.

Definition:

If in a commutative ring, $(R, +, .)$ if for any $a, b \in R$ such that $a \neq 0$, $b \neq 0 \implies ab \neq 0$, then the ring is without zero-divisors.

Note:

In a without zero-divisors $a.b = 0$
$\implies a = 0 \text{ or } b = 0$.

Definition : Integral domain

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

Example

$Z_5 = \{[0], [1], [2], [3], [4]\}$ under $+_5$ and $._5$ is an integral domain

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\cdot_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

We can easily verify $(Z_5, +_5, \cdot_5)$ is a commutative ring without identity [1]. From the table for $\cdot_5$ we see product of non-zero elements is non-zero and so the ring is without zero-divisors. Hence it is an integral domain.

Note

$(Z_n, +_n, \cdot_n)$ is an integral domain if n is a prime number

The definition requires the ring has more than one element.
$(Z_n, +_n, \cdot_n)$ is an integral domain if n is a prime number.

Definition : Field

A commutative ring $(R, +, .)$ with identity and which every non-zero element has multiplicative inverse is called a field.

Examples:

1. $(Q, +, .)$ is a field.
2. $(R, +, .)$ and $(C, +, .)$ are field.
3. $(Z, +, .)$ is an integral domain but not a field.

Theorem 1:

A commutative ring R with identity is an integral domain iff the cancellation laws hold in R.

Proof:

The R be an integral domain.

Let $a.b = a.c, where\ a \neq 0$

$$\therefore a.(b - c) = 0$$

$\Rightarrow b - c = 0 \quad \Rightarrow b = c \quad [\because R\ is\ without\ zero\ divisors]$

So cancellation law holds.

Conversely, let R be a commutative ring with identity in which cancellation law holds.

To prove R is an integral domain, we have to prove that R has no *zero divisors.*

Suppose $a.b = 0\ and\ a \neq 0$

Then $a.b = a.0 \quad [\because 0 = a.0]$

$\Rightarrow \quad b = 0$ [by cancellation law]

$\therefore\ R$ is an integral domain.

Theorem 2:

Every field is an integral domain

Proof:

$(F,+,.)$ be a field. Then it is a commutative ring with identity.

To prove F is an integral domain, it is enough to prove that it has no zero divisors.

Suppose $a, b \in F$ with $a.b = 0, a \neq 0$

Since a is is non-zero element, its multiplicative inverse a^{-1} exists.

Therefore $a^{-1}.(a.b) = a^{-1}.0$

$$\Rightarrow (a^{-1}.a).b = 0$$

$$\Rightarrow 1.b = 0 \Rightarrow b = 0$$

Thus

$$\Rightarrow ab = 0, a \neq 0 \Rightarrow b = 0$$

F has no zero divisors

Hence $(F,+,.)$ is an integral domain.

Example 1:

Let $R = \{a, b, c\}$ Define $+$ and . on R by the tables here

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

.	a	b	c	d
a	a	a	a	a
b	a	a	b	a
c	a	b	c	d
d	a	a	d	a

Show that $(R, +, .)$ is a ring. Is it commutative? Does it have an identity? What is the zero of the ring?

Solution:

Given $R = \{a, b, c\}$ and $+$ *and* $.$ are defined by the given tables, we shall now verify the axioms of a ring.

1. We have to prove that $(R, +)$ is an abelian group.

   Since the body of the table (1) contain only all the elements of R, R is closed under $+$. Since elements of each row and each column are different and for $\forall\, x \in R$ we have $x + a = a + x = x$, a is the zero element.

   $(R, +)$ is a group with a as additive identity.

   The additive inverse of a *is* a, inverse of b *is* b, inverse of c *is* d, and inverse of d *is* c, since $a + a = a, b + b = b, c + d = d + c = a$ from the table.

Further, the elements equidistant from the main diagonal are same and $+$ is commutative.

$\therefore (R, +)$ is an abelian group.

2. Now we shall prove that $(R, .)$ is a semi-group.

The body of the table (2) contains only the elements of R and hence R is closed under.

Associativity:

For $b, c, d \in R$, we have

$b.(c.d) = b.d = a$ [from table (2)]

$(b.c).d = b.d = a$ [from table (2)]

$$\therefore\ b.(c.d) = (b.c).d$$

Similarly we can prove for other element in R.

$\therefore$ Associative axiom is satisfied.

Hence $(R, .)$ is a semi-group.

3. From tables (1) and (2)

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

and $a.b + a.c = a + a = a$

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

Similarly we can verify for each triplets.

$\therefore (R, +, .)$ is a ring.

In table (2) the elements equidistant from the main diagonal are same and so . is commutative.

Hence R is commutative ring.

Since $a.a. = a,\ a.b = b.a = a,\ a.c = c.a = a,\ a.d = d.a = a\ etc,$ there is no identity element.

4. The additive identity a is the zero of the ring.

Example 2:

Show that $(Z, +, \times)$ is an integral domain where Z is the set of all integers.

Solution:

We know a commutative ring with identity and without zero-divisors is called an integral domain.

If Z is the set of integers, then $(i)(Z,+)$ is an abelian group.

(ii) $(Z, \times)$ is a semi-group.

(ii) $a \times b = b \times a \quad \forall\, a, b \in Z$

$(iii) a \times (b + c) = (a \times b) + (a \times c) \quad \forall\, a, b, c \in Z$

Hence $(Z, +, \times)$ is a commutative ring with identity.

If $a \neq 0, b \neq 0$ in Z then we know $ab \neq 0$. So Z is without zero divisors.

Hence $(Z, +, \times)$ is an integral domain.

4.6.1: Boolean ring

Definition:

In a ring $(R, +, .)$ if $a^2 = a \;\forall a \in R$, then the ring is called a Boolean ring.

Definition: Subring

Let $(R,+,.)$ be a ring. A non empty subset S of R is said to be a subring of R if S itself is a ring with respect to the same operations $+$ and $.$ of R.

Note:

In other words S is a subgroup of R if (i) $(S,+)$ is a subgroup of $(R,+)$ and (ii) S is closed under .

i.e $a, b \in S, a-b \in S$ and $a.b \in S$

Definition: Ring Homomorphism

Let $(R,+,.)$ and $(S,\oplus.\odot)$ be rings. A mapping $f: R \longrightarrow S$ is called a ring homomorphism if $f(a+b) = f(a) \oplus f(b)$ and $f(a.b) = f(a) \odot f(b)\ \forall a,b \in R$

Example:

Prove that in the ring of integers $(Z, +, .)$ the subset of even integers $2Z$ is a sub ring.

Solution:

Let $a, b \in 2Z$, then $a = 2x, b = 2y$

$$\therefore a - b = 2x - 2y = 2(x - y) \in 2Z$$

$$and\ a.b = 2x.2y = 2(2xy) \in 2Z$$

Hence $(2Z, +, .)$ is a sub ring of Z.

1. For any m, prove that the set $\{mx/x \in Z\}$ is a subring of $(Z,+,.)$

Solution:

Let $S = \{mx/x \in Z\}$

If $x = 0$ $then\ m0 = 0 \in S$

$\therefore$ S is non-empty.

Let $a, b \in S$ be any two elements.

then $a = mx, b = my$

$$\therefore a - b = m(x - y) \in S$$

$$and\ a.b = mx.my = 2(mxy) \in S$$

Hence $(S,+,.)$ is a sub ring of $(Z,+,.)$.