Ring Theory

Defⁿ: Associative Ring

A nonempty set R on which two binary operations '$+$' (called addition) and '$\cdot$' (called multiplication) are defined is said to be an associative ring if the following axioms are satisfied –

R_1 : $(R, +)$ is an abelian group.

R_2 : '$\cdot$' is associative

R_3 : '$\cdot$' is distributive over '$+$'

i.e. for all $a, b, c \in R$,

$a \cdot (b+c) = a \cdot b + a \cdot c$, Left distributivity

and $(b+c) \cdot a = b \cdot a + c \cdot a$, Right distributivity

Remarks: (1) Ring (always mean associative ring) is denoted by algebraic structure $(R, +, \cdot)$ or simply by R.

(2) Additive identity is denoted by 0 (this 0 is not our integer zero).

(3) Additive inverse of $a \in R$ is denoted by $-a$.

Defⁿ: Ring with unit element

Let R be the ring. If there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$, then R is called a ring with unit element.

Note: This 1 is called multiplicative identity and it is not the integer 1.

Defⁿ: Commutative Ring

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

Ex.1: If R is the set of integers, '+' is the usual addition and '.' is the usual multiplication of integers, then R is a commutative ring with unit element.

Ex.2: If R is the set of even integers under the usual operations of addition and multiplication, then R is a commutative ring but has no unit element.

Ex.3: If R is the set of rational numbers under the usual addition and multiplication of rational numbers, then R is a commutative ring with unit element.

Ex.4: Show that the set R of integers mod 7 under addition and multiplication mod 7 is a commutative ring with unity.

Sol^n: Let $R = \{0, 1, 2, 3, 4, 5, 6\}$ be the set of integers mod 7.

Defined addition and multiplication mod 7 on R as

$a +_7 b = c$, remainder when $a+b$ is divided by 7.

$a \cdot_7 b = d$, remainder when $a \cdot b$ is divided by 7.

from the definition of the operations $+_7$ and $\cdot_7$, it is clear that $0 \le c < 7$ and $0 \le d < 7$ $\forall a, b \in R$.

$\Rightarrow$ Both $+_7$ and $\cdot_7$ are binary operations on R.

Now, consider the composition tables for the operations $+_7$ and $\cdot_7$ as below

Table 1 for $+_7$ Table 2 for $\cdot_7$

From Table 1, it is clear that

G_1 : R is closed under $+_7$

G_2 : Associativity holds for $+_7$

G_3 : Additive identity exists in R and it is 0.

G_4 : Additive inverses of 0, 1, 2, 3, 4, 5, 6 are 0, 6, 5, 4, 3, 2, 1 respectively and all these belongs to R.

G_5 : commutativity holds for $+_7$.

$\Rightarrow (R, +_7)$ is an abelian group, i.e., R_1 holds.

From Table 2, we observe that

$(a \cdot_7 b) \cdot_7 c = a \cdot_7 (b \cdot_7 c) \quad \forall a, b, c \in R$.

$\Rightarrow \cdot_7$ is associative, i.e., R_2 holds.

Also we can verify that $\cdot_7$ is distributive over $+_7$.

$\Rightarrow R_3$ holds.

Since R_1, R_2, R_3 holds,

$\therefore (R, +_7, \cdot_7)$ is a ring.

Again from Table 2, we see that

$a \cdot_7 b = b \cdot_7 a \quad \forall a, b \in R$

$\Rightarrow$ R is a commutative ring

And $\exists\ 1 \in R$ s.t. $a \cdot_7 1 = 1 \cdot_7 a = a \quad \forall a \in R$.

$\Rightarrow$ 1 is the multiplicative identity i.e. unity.

Hence $(R, +_7, \cdot_7)$ is a commutative ring with unity.

—o—

Ex.5: If R is the set of integers mod 6 under addition and multiplication mod 6, then R is a commutative ring with unit element.

Note: for Ex.5, we have $2, 3 \in R \Rightarrow 2 \cdot_6 3 = 0$, identity w.r.t. $+_6$.

Thus in a ring, it is possible that $a \cdot b = 0$ with neither $a = 0$ nor $b = 0$.

Ex.6: If R is the set of nxn rational matrices under usual matrix addition and matrix multiplication, then R is a non-commutative ring with unity.

Ex.7: Let R be a ring and $a, b, c, d \in R$. Evaluate $(a+b)(c+d)$.

Soln: Denote $c+d = x \in R$

Then $(a+b)(c+d) = (a+b)x$

$= ax + bx$ - by right distributivity

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

$= ac + ad + bc + bd$

- by left distributivity

Thus $(a+b)(c+d) = ac + ad + bc + bd$.

Ex.8: Prove that if $a, b \in R$ then $(a+b)^2 = a^2 + ba + ab + b^2$, where by x^2 we mean xx.

Soln: Data: $x^2 = xx$

$\therefore$ for $a, b \in R$, $a+b \in R$

L.H.S. $= (a+b)^2 = (a+b)(a+b)$

$= a(a+b) + b(a+b)$ - by left distributive

$= aa + ab + ba + bb$ - " -

$= a^2 + ab + ba + b^2$ - by data

$= a^2 + ba + ab + b^2$ $\{\because (R, +)$ is abelian gp.

$=$ R.H.S.

Ex.9: If every $x \in R$ satisfies $x^2 = x$, prove that R must be commutative.

Soln: Given $x^2 = x \quad \forall x \in R$ — (1)

Let $a \in R$, ring. $\Rightarrow -a \in R$ where $-a$ is additive inverse of a.

Then $-a = (-a)^2$ — by (1)

$= (-a)(-a)$

$= aa$ — by a result $(-a)(-b) = ab$, $\forall a, b \in R$.

$= a^2$

$= a$ — by (1)

Thus $-a = a$ — (2)

Now, $a, b \in R \Rightarrow a+b \in R$ — by Closure Prop. of $(R, +)$

Then $a+b = (a+b)^2$ — by (1)

$= a^2 + ab + ba + b^2$ — by Ex.8.

$= a + ab + ba + b$ — by (1)

$\Rightarrow 0 = ab + ba$ — by cancellation laws

$\Rightarrow ba = -(ab)$

(i.e. ba is additive inverse of ab)

$\Rightarrow ba = ab$ — by (1)

$\therefore \forall a, b \in R, \quad ba = ab$ or $ab = ba$.

$\Rightarrow R$ is commutative.

Note: A ring R in which $x^2 = x \ \forall x \in R$, is called as a Boolean ring.

Thus Boolean rings are commutative.

Ex.10: If $a, b \in R$ and n, m are integers, where R is a ring, then prove that

$$(na)(mb) = (nm)(ab).$$

Soln: Given: $a, b \in R$ ring and m, n are integers.

Then by na we mean $a+a+a+\dots$ n-times.

L.H.S $= (na)(mb) = (a+a+\dots \text{ n times})(b+b+\dots m\text{-times})$

$= a(b+b+\dots m\text{-times})$

$+ a(b+b+\dots m\text{-times})$

$+ \dots\dots n\text{-times}$ — by left dist.

$= (ab+ab+\dots m\text{-times})$

$+ (ab+ab+\dots m\text{-times})$

$+ \dots + n\text{-times}.$

— by left distributivity

$= ab+ab+\dots\dots nm\text{-times}$

$= (nm)(ab)$

$= R.H.S.$

Ex.11: If R is a system satisfying all the conditions for a ring with unit element with the possible exception of $a+b = b+a$, prove that the axiom $a+b = b+a$ must hold in R and that R is thus a ring.

Soln: As unit element $1 \in R$, we have $1 \cdot a = a \cdot 1 = a \ \forall a \in R$ —— (1)

Let $a, b \in R \Rightarrow a+b \in R$.

Now $(a+b)(1+1) = a(1+1) + b(1+1)$ — by left distributive

$= a \cdot 1 + a \cdot 1 + b \cdot 1 + b \cdot 1$ — " —

$= a+a+b+b$ — by (1) — (2)

Also $(a+b)(1+1) = (a+b)1 + (a+b)1$ — by right distributive

$= a \cdot 1 + b \cdot 1 + a \cdot 1 + b \cdot 1$ — " —

$= a+b+a+b$ — by (1) — (3)

from (2) & (3), we have $a+a+b+b = a+b+a+b \ \forall a, b \in R$

$\Rightarrow a+b = b+a \ \forall a, b \in R$ — by cancellation laws

$\therefore$ Commutativity holds for $+ \Rightarrow (R, +)$ is an abelian gp $\because R_2$ & R_3 holds (i.e. R is a ring).

Some Special Classes of Rings :

Def^n: Zero Divisor

Let R be a commutative ring. An element $a(\neq 0) \in R$ is called a zero divisor if there exists $b(\neq 0) \in R$ such that $a \cdot b = 0$.

Remark: When the ring is not commutative, we have a left zero divisor and a right zero divisor as below :

$a \cdot b = 0$ for $a \neq 0, b \neq 0$

gives (i) a as left zero divisor

(ii) b as right zero divisor.

Def^n: Integral Domain

A commutative ring which has no zero divisor is called an integral domain.

eg. The set of integers with ordinary addition and multiplication is an integral domain.

Note: An integral domain must have more than one element. This means that it has at least one nonzero element.

Def^n: Division ring

A ring whose non-zero elements form a group under multiplication is called a division ring.

Defⁿ: Field

A commutative division ring is called as field.
i.e. ring R is a field if its non-zero elements form an abelian group under multiplication.

Theorem 1: If R is a ring, then for all $a, b \in R$

(1) $a0 = 0a = 0$

(2) $a(-b) = (-a)b = -(ab)$

(3) $(-a)(-b) = ab$

Proof: Given that R is a ring.

(1) We know that additive identity $0 \in R$ and

$0 = 0 + 0$

$\therefore a0 = a(0+0) \quad \forall a \in R$

$\Rightarrow a0 = a0 + a0$ — By left distributivity

$\Rightarrow a0 + 0 = a0 + a0$ $\because$ 0 is additive identity

$\Rightarrow 0 = a0$ — By left cancellation law

Hence $a0 = 0 \quad \forall a \in R$.

Similarly $0a = (0+0)a \quad \forall a \in R$

$\Rightarrow 0a + 0 = 0a + 0a$

$\Rightarrow 0 = 0a$

Thus $a0 = 0a = 0 \quad \forall a \in R$.

(2) By the property of additive inverse, $\forall a, b \in R$

we have $a + (-a) = 0$ and $b + (-b) = 0$

$\Rightarrow [a + (-a)]b = 0b$ $\Rightarrow a[b + (-b)] = a0$

$\Rightarrow ab + (-a)b = 0$ by(1) $\Rightarrow ab + a(-b) = 0$ by(1)

These shows that $(-a)b$ and $a(-b)$ are additive inverse of ab. But the additive inverse of ab is $-(ab)$,

which is unique in R. Therefore we obtain

$(-a)b = a(-b) = -(ab) \quad \forall a, b \in R$.

(3) $(-a)(-b) = -((-a)b)$ by (2)

$= -(-(ab))$ by (2)

$= ab$ — As additive inverse of ab is -ab and that of -ab is ab.

Theorem 2: If R is a ring with unit element, 1, then (1) $(-1)a = -a$

(2) $(-1)(-1) = 1$.

Proof: Since R is a ring with unit element, 1,

$\therefore a1 = 1a = a \quad \forall a \in R$.

By a theorem, we have

$a(-b) = (-a)b = -(ab) \quad \forall a, b \in R$,

$\therefore (-b)a = -(ba) \quad \forall a, b \in R$.

Hence for $b = 1 \in R$ we obtain

$(-1)a = -(1a)$

i.e. $(-1)a = -a$ $\because$ 1 is unity

Further, by the same theorem, we have

$(-a)(-b) = ab \quad \forall a, b \in R$

$\therefore$ for $a = b = 1 \in R$, we obtain

$(-1)(-1) = 1 \cdot 1$

$\Rightarrow (-1)(-1) = 1$.

The Pigeon - Hole Principle :

If n objects are distributed over m places and if $n > m$ then some place receives at least two objects.

An equivalent statement of this principle in very useful form is stated as :

If n objects are distributed over n places in such a way that no place receives more than one object then each place receives exactly one object.

Theorem 3: A finite integral domain is a field.

Proof: Let $D = \{x_1, x_2, \ldots, x_n\}$ be a finite integral domain.

$\Rightarrow$ D is a commutative ring having no zero divisors. — By definition.

$\Rightarrow$ (i) $xy = yx \quad \forall x, y \in D$

(ii) $x, y \in D$ and $xy = 0 \Rightarrow x = 0$ or $y = 0$, where 0 is the additive identity of D.

Now, D will be a field, if in addition to commutative ring it is a division ring.

For this we show that non-zero elements of D form a group under multiplication.

Step I: Let $a (\neq 0) \in D$.

Since D is closed under multiplication, we obtain $ax_1, ax_2, \ldots, ax_n \in D$.

We show that all these elements are distinct.

On the contrary, assume that

$ax_i = ax_j$ for some $i \neq j$

$\Rightarrow ax_i + (-ax_j) = ax_j + (-ax_j)$

$\Rightarrow ax_i - ax_j = 0$ {As $-ax_j$ is additive inverse of ax_j

$\Rightarrow a(x_i - x_j) = 0$ — By distributivity

$\Rightarrow x_i - x_j = 0$ $\because a \neq 0$ — by (ii)

$\Rightarrow x_i = x_j$

This contradicts $i \neq j$.

Thus $ax_1, ax_2, \ldots\ldots, ax_n$ are n distinct elements lying in D which already has exactly n elements.

Step II: Therefore, by the Pigeon-hole principle, these must account for all the elements of D.

In other words, every element $y \in D$ can be written as

$y = ax_i$ for some $x_i \in D$. — (iii)

In particular, $a \in D$ can be written as

$a = ax_p$ for some $x_p \in D$.

$\Rightarrow a = ax_p = x_p a$ — by (i) — (iv)

Step III: G_1: Clearly D is closed under multiplication, being a binary operation on D.

G_2: Also multiplication is associative. — by R_2 of D.

G_3: Let y be any element in D.

Then $yx_p = (ax_i)x_p$ — by (iii)

$= (x_i a)x_p$ — by (i)

$= x_i(ax_p)$ — by R_2

$= x_i a$ — by (iv)

$= ax_i$ — by (i)

$= y$ — by (iii)

Thus $y x_p = y$ for $x_p \in D$.

Similarly we can show that $x_p y = y$

Hence $\exists\ x_p \in D$ s.t. $y x_p = y = x_p y\ \forall y \in D$.

$\Rightarrow x_p$ is multiplicative identity in D which is denoted by 1, unit element of D.

i.e. unit element 1 exists in D.

G_4: $1 \in D$ can be written as

$1 = ab$ for some $b \in D$.

$\therefore$ for every non-zero element $a \in D$ $\exists$ some $b \in D$ s.t. $ab = 1 = ba$ — by (i)

$\Rightarrow$ b is multiplicative inverse of a.

i.e. Multiplicative inverse exists in D for each non-zero element of D.

Thus G_1, G_2, G_3, G_4 holds with G_5 viz. (i).

$\Rightarrow$ Non-zero elements of D forms an abelian group under multiplication.

$\Rightarrow$ D is a field. — By definition.

Hence, a finite integral domain is a field.

Corollary: If p is a prime number then J_p, the ring of integers mod p, is a field.

Proof: Let p be a prime number.

Then $p > 1$ and it has exactly four divisors $\pm 1, \pm p$.

$\therefore$ J_p, the ring of integers mod p contains finite number of elements which also commutes under multiplication mod p.

$\Rightarrow$ J_p is a finite commutative ring.

Now, let $a, b \in J_p$ and $ab = 0$, additive identity

i.e. $ab \equiv 0 \pmod{p}$

$\Rightarrow p \mid ab$ where p is a prime

$\Rightarrow p \mid a$ or $p \mid b$ — By a result

$\Rightarrow a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

i.e. $a = 0$ or $b = 0$

$\therefore \forall\, a, b \in J_p$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

$\Rightarrow J_p$ has no zero divisor.

Thus J_p is a commutative ring without zero divisor.

$\Rightarrow J_p$ is an integral domain.

Also J_p is finite.

Hence by a theorem, J_p is a field.

Ex. Prove that every field is an integral domain. Does its converse hold?

Sol^{n}: Let $(F, +, \cdot)$ be a field

$\Rightarrow F$ is a commutative division ring.

$\Rightarrow$ (i) $(F, +)$ is an abelian group

and (ii) The non-zero elements of F form an abelian group under multiplication.

$\therefore$ for $a \neq 0$ in F $\exists\, a^{-1} \in F$.

Let $a (\neq 0), b \in F$ such that $ab = 0$.

Then $a^{-1}(ab) = a^{-1}0$

$\Rightarrow (a^{-1}a)b = 0$ — By R_2 and th^{m} 1

$\Rightarrow 1\,b = 0$ { $\because$ Multiplicative identity $1 \in F$ $\therefore$ By inverse prop. for $(\cdot)$ $\because a1 = 1 \cdot a = a\ \forall a \in F$

$\Rightarrow b = 0$

Thus $a \neq 0$ and $ab = 0 \Rightarrow b = 0$

Similarly for $b \neq 0$ and $ab = 0 \Rightarrow a = 0$.

Hence $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$ $\forall a, b \in F$

$\Rightarrow$ F has no zero divisors.

Thus F is a commutative ring with no zero divisors.

$\Rightarrow$ F is an integral domain.

$\therefore$ Every field is an integral domain.

But its converse is not true.

for example, consider a set Z of integers.

It is a commutative ring with no zero divisors.

$\therefore$ It is an integral domain.

But non-zero elements of Z do not form a group under multiplication ($2 (\neq 0) \in Z \Rightarrow 2^{-1} = \frac{1}{2} \notin Z$).

$\Rightarrow$ Z is not a divison ring.

Hence Z is not a field.

Thus every integral domain need not be a field.

Ex. Show that the commutative ring D is an integral domain iff for $a, b, c \in D$ with $a \neq 0$ the relation $ab = ac \Rightarrow b = c$.

Proof: Let D be a commutative ring.

Necessary Part: Suppose D be an integral domain

$\Rightarrow$ D has no zero divisors.

$\therefore$ $a, b \in D$ and $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Now, $ab = ac \Rightarrow ab - ac = 0$

$\Rightarrow a(b - c) = 0$

$\Rightarrow a = 0$ or $b - c = 0$.

$\therefore$ for $a, b, c \in D$ with $a \neq 0$ we obtain

$ab = ac \Rightarrow b - c = 0$ i.e. $b = c$.

Sufficient Part: Suppose that for $a, b, c \in D$ with $a \neq 0$ the relation $ab = ac \Rightarrow b = c$.

Then $b = c \Rightarrow b - c = 0$.

Also, $ab = ac \Rightarrow ab - ac = 0$.

$\Rightarrow a(b-c) = 0$

$\Rightarrow a \neq 0$ and $b - c = 0$.

Hence D has no zero divisors.

But D is a commutative ring.

$\Rightarrow$ D is an integral domain.

This completes the solution.

—— o ——