

1 S-IV

Rings

Defⁿ — A ring is an algebraic system containing of a non-empty set R and two binary operations '+' and ' \circ ' respectively satisfying the following postulates.

R₁. Associative axiom

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

R₂. Existence of identity

There exists an element denoted by the symbol 0 (called the additive identity) such as

$$0+a = a \quad \forall a \in R \quad [\text{left additive identity}]$$

$$a+0 = a \quad \forall a \in R \quad [\text{Right additive identity}]$$

R₃. Existence of inverse

To each element a in R there exists an element $-a$ in R such that $(-a)+a = 0$; $a+(-a) = 0$

R₄. Commutative axiom (addition is commutative)

$$a+b = b+a \quad \forall a, b \in R.$$

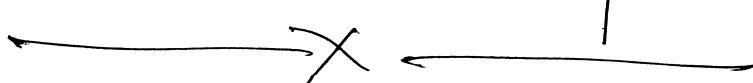
R₅. Associative axiom (Multiplication is associative)

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

R₆. Multiplication is distributive with respect to addition
i.e. for all a, b, c in R

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad [\text{left distributive law}]$$

$$(b+c) \cdot a = b \cdot a + c \cdot a \quad [\text{Right distributive law}]$$



Q. The zero of a ring R is unique.

Proof- We assume if possible 0 and $0'$ be the two zeros of a ring R.

Then from the definition we have for every element

$$a+0 = a \text{ and } 0+a = a \quad \text{--- (1)}$$

$$\text{Again } a+0' = a \text{ and } 0'+a = a \quad \text{--- (2)}$$

Now from (1) & (2) we get

$$a+0 = a+0'$$

By cancellation law $0 = 0'$

Otherwise in (1) we put $a=0'$

$$\therefore 0'+0 = 0' \quad \text{--- (3)}$$

Similarly in putting $a=0$ in (2)

$$\text{i.e. } 0'+0 = 0 \quad \text{--- (4)}$$

From (3) & (4) we get $0 = 0'$

Thus the zero of a ring is unique. Proved

Q. Prove that the inverse of a ring is unique.

Proof- we assume if possible x and y be two inverses of an element a in R

such that $a+x=0$ and $x+a=0$ $\quad \text{--- (1)}$

Again $a+y=0$ and $y+a=0 \quad \text{--- (2)}$

from (1) & (2) we get

$$a+x = a+y$$

By left cancellation law we get

$$x = y$$

Again $x+a = y+a$

$\therefore x = y$ By right cancellation law

Hence we find that $x = y$.

i.e. the inverse of a ring is unique.

Proved

Property 4) Prove that $a(b-c) = ab - ac$

$$\begin{aligned} \text{LHS} &= a(b-c) = a.b + a(-c) \quad [\text{By left distributive law}] \\ &= ab - ac \quad \text{as } a(-c) = -ac \\ &= \text{RHS.} \end{aligned}$$

Proved //

5) Prove that $(b-c)a = ba - ca$

$$\begin{aligned} \text{LHS} &= (b-c)a = ba + (-c)a \quad [\text{By Right distributive law}] \\ &= ba - ca \quad \text{as } (-c)a = -ca \\ \therefore (b-c)a &= ba - ca \quad \text{RHS.} \end{aligned}$$

Proved //

Q/ If a, b, c, d are elements of a ring R , then evaluate $(a+b)(c+d)$

Ans. - We have

$$\begin{aligned} (a+b)(c+d) &= a(c+d) + b(c+d) \quad \text{Right distributive law} \\ &= ac + ad + bc + bd \quad \text{left distributive law} \\ \therefore (a+b)(c+d) &= ac + ad + bc + bd. \end{aligned}$$

//

Q/ Prove that if $a, b \in R$ then $(a+b)^2 = a^2 + ab + ba + b^2$ where x^2 we mean $x \cdot x$.

Sol. - we have $(a+b)^2 = (a+b)(a+b)$ [as x^2 we mean $x \cdot x$]

$$\begin{aligned} &= a(a+b) + b(a+b) \quad \text{Right distributive law} \\ &= aa + ab + ba + bb \quad \text{left distributive law} \\ &= a^2 + ab + ba + b^2 \end{aligned}$$

Hence the result.

Q/ If a, b, c, d are elements of a ring R . Prove that

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

Sol. - $(a-b)(c-d) = \{a+(-b)\}\{c+(-d)\} = a\{c+(-d)\} + b\{c+(-d)\}$

$$\begin{aligned} &\stackrel{\text{Right distributive law.}}{=} ac + a(-d) + (-b)c + (-b)(-d) \quad \text{left distributive law} \\ &\Rightarrow ac - ad - bc + bd = (ac+bd) - (ad+bc) \quad \text{since addition is commutative.} \end{aligned}$$

Proved //

Field — Defⁿ —

A Ring R with at least two elements is called the field if the non zero elements of R form an abelian group under multiplication.

i.e. A Ring R is a field if it has two elements and

(i) is commutative

(ii) has a unity element

(iii) is such that each non zero element has a multiplicative inverse.

Example — The Ring of real nos. and complex nos. are the examples of a field.

Integral Domain — Defⁿ —

A Ring R is said to be an Integral domain if it

(i) is commutative

(ii) has a unity element

(iii) is without zero divisors.

Division Ring or Skew field. —

Defⁿ — A ring $(R, +, \cdot)$ having at least two elements is called a Division ring if it is a ring with unity and is such that every non-zero element has a multiplicative inverse belonging to it.

By definition of division ring it is clear that every division ring is not a field but a ~~com~~ only a commutative division ring is a field whereas every field is a division ring.

In short, An integral domain is a commutative ring with unity and without zero-divisor.

A Field is a commutative ring with unity and every non-zero element has a multiplicative inverse.

Theorem - A finite Integral Domain is a field.
or

A finite commutative ring without zero-divisors is a field.

Proof - Let D be a finite commutative ring without zero divisors having elements $a_1, a_2, a_3, \dots, a_n$. — (1)

Now to show that D is a field we have to show that multiplicative inverse exists in D .

Let $a \neq 0 \in D$

We consider n product $aa_1, aa_2, aa_3, \dots, aa_n$ — (2)

Now all these elements belong to D .

Now no two elements of D be equal, ~~for $aa_i = aa_j$ for some $i \neq j$~~
 $\because a(a_i - a_j) = 0$ since $a \neq 0$

$\therefore a_i - a_j = 0 \Rightarrow a_i = a_j$

which is contradiction for $i \neq j$

Therefore the n elements D are all distinct in some order,

So one of these elements must be equal to a .
 Therefore there exists the identity element $e \in D$ such that

$a e = a = e a$,

we shall prove that e is the multiplicative identity of D .

if $ax = b = xb$

Now $eb = e(ax) = (ea)x = ax = b = be$

Hence e is the identity of D .

Again since $e \in D$, one of the elements of the list (1) must be

equal to e such that $a'a = e = aa'$

$\therefore a'$ is the inverse of a .

So every non zero element has its own inverse.

It follows that D is a field.

Ring with unity — If in a ring R there exists an element denoted by 1 such that $1 \cdot a = a = a \cdot 1 \quad \forall a \in R$. Then R is called a ring with unit element. The element $1 \in R$ is called the unit element of the ring.

Commutative Ring — If in a ring R, the multiplication composition is also commutative i.e. if we have $a \cdot b = b \cdot a \quad \forall a, b \in R$, then R is called a commutative ring.

Zero Divisors — (Ring with zero divisors)

A Ring $(R, +, \cdot)$ is said to be a ring with zero divisors if for $a, b \in R$ we have $ab = 0$ when neither $a = 0$ nor $b = 0$. Then a and b are called the zero divisors.

Example —

$$\text{If } \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

2) We can easily show that $R = \{0, 1, 2, 3, 4, 5\}$ of modulo 6. is a ring with zero divisor.

$$3 \cdot 2 \equiv 6 \pmod{6} = 0$$

$$4 \cdot 3 \equiv 12 \equiv 0 \pmod{6}$$

i.e. $3 \cdot 2$ or $4 \cdot 3 = 0$ or $ab = 0 \quad a \neq 0, b \neq 0$

Hence the ~~the~~ ring $(R + 6, \times 6)$ is also a ring with zero divisors.

Ring with out zero divisors — A ring R is without zero divisors if the product of no two non-zero elements of R is zero. i.e. if $ab = 0 \Rightarrow a = 0$ or $b = 0$ or $a = 0$ and $b = 0$.

Commutative ring with unity —

If $1 \cdot a = a \cdot 1 = a, \forall a \in R$; Then R is called Commutative ring with unity.

Properties of Ring

1). $a \cdot 0 = 0, a = 0 \forall a \in R$

Proof - By the existence of identity

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

$$0 + a = a$$

$$\therefore 0 + 0 = 0$$

$$\therefore a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \quad [\text{By left distributive law}]$$

$$\text{as } a \cdot 0 \in R \therefore 0 + a \cdot 0 = a \cdot 0 + a \cdot 0$$

$$\text{Now by cancellation law we get } 0 = a \cdot 0 \quad \text{--- (1)}$$

$$\text{Again we have } 0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \quad [\text{By Right distributive law}]$$

$$\text{But } 0 \cdot a \in R \therefore 0 + 0 \cdot a \in R \therefore 0 + 0 \cdot a = 0 \cdot a + 0 \cdot a$$

Applying the cancellation law we get $0 = 0 \cdot a$

$$\text{Hence from (1) \& (2) we get } a \cdot 0 = 0, a = 0 \quad \text{--- (2)}$$

2). Prove that $a(-b) = -[ab] = (-a)b$ Proved

Proof - $a \cdot 0 = a \cdot (-b+b) = a \cdot (-b) + a \cdot b$ [by left distributive law]

$$\text{But } a \cdot 0 = 0 \therefore 0 = a \cdot (-b) + a \cdot b \therefore -[ab] = a \cdot (-b) \quad \text{--- (1)}$$

$$\therefore a \cdot b = (-a) \cdot b + a \cdot b \quad \text{[using Right distributive law]}$$

$$\therefore 0 = +[-ab] + ab \quad \text{as } 0 \cdot b = 0 \neq b \in R$$

$$\therefore -[ab] = (-a)b$$

Hence from (1) \& (2) we have

$$a(-b) = -[ab] = -ab$$

3). Prove that $(-a)(-b) = ab$ Proved

Proof - $a \cdot 0 = -a(b-b) = (-a)b + (-a)(-b)$

$$= (-a)b + (-a)(-b) = -[ab] + (-a)(-b)$$

Since a is the inverse of $-a$ $\therefore -a \in R$

$$\therefore 0 = -[ab] + (-a)(-b)$$

$$\therefore ab = (-a)(-b)$$

Hence $(-a)(-b) = ab$ Proved

Cancellation laws in a Ring —

We say that the cancellation law holds in a ring R if

$$ab = ac \quad [a \neq 0] \Rightarrow b = c \quad \text{Left cancellation law}$$

$$ba = ca \quad [a \neq 0] \Rightarrow b = c \quad \text{Right cancellation law}$$

$$\text{for } ab = 0 = a = 0 \quad [a \neq 0] \Rightarrow b = 0 \text{ by left cancellation law}$$

But this is a contradiction if the ring is with zero divisors.

Thus it is not possible for us to define the cancellation law in a ring with zero divisors.

Theorem — A ring R has no zero divisors if and only if the cancellation laws hold in R .

Proof —

We first suppose that R has no zero divisors.

Let $a, b, c \in R$ such that $ab = ac \quad [a \neq 0]$

$$\therefore ab = ac \Rightarrow a(b - c) = 0$$

Since R has no zero divisors and $a \neq 0$.

$$\therefore \cancel{a(b - c) = 0} \Rightarrow b - c = 0$$

Thus the left cancellation law hold in R .

Again let $a, b, c \in R \therefore ba = ca \quad [a \neq 0] \Rightarrow (b - c)a = 0$

But R has no zero divisor. $\therefore a \neq 0 \therefore (b - c)a \neq 0 \Rightarrow b - c = 0$

$$\therefore b = c \quad \text{Right cancellation law hold in } R.$$

Conversely —

Let the cancellation law holds in R . We have to prove that it has no zero divisors.

Let $ab = 0$; $a \neq 0, b \neq 0$ with zero divisor

Then $ab = a \cdot 0$ hence by cancellation law we get
 $b = 0$

which is a contradiction

Hence R is without zero ~~too~~ divisors.



Theorem - Prove that Every field is an integral domain.

Proof - Since a field F is a commutative ring with unity, we have only to prove that it has no zero divisors.

Let $a, b \in F$ with $a \neq 0$, such that $ab = 0$. Since \bar{a}^{-1} exists in a field, we have

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

$$\Rightarrow (\bar{a}^{-1}a)b = \bar{a}^{-1}0 \Rightarrow b = 0 \quad [\because \bar{a}^{-1}a = 1 \text{ & } 1b = b]$$

Similarly we may say that

$$b \neq 0, b^{-1} \text{ exists } ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1} \Rightarrow a(bb^{-1}) = 0 \\ \Rightarrow a = 0$$

Thus in a field $ab = 0 \Rightarrow a = 0$ or $b = 0$

Therefore a field has no zero divisors.

Hence we can conclude that every field is an integral domain,
But the converse is not true i.e. every integral domain
is not a field.

For example, The ring of integers is an integral domain but not a field.

Theorem - A skewfield (division ring) has no divisors of zero.

Proof - Let D be a division ring. Then D is a ring with unit element 1 and every non-zero element of D has a multiplicative inverse.

Let $a, b \in D$ with $a \neq 0$ such that $ab = 0$. Since $a \neq 0$ and \bar{a}^{-1} exists in D we have

$$ab = 0 \Rightarrow \bar{a}^{-1}(ab) = \bar{a}^{-1}0 \Rightarrow (\bar{a}^{-1}a)b = 0 \Rightarrow 1(b) = 0 \\ \Rightarrow b = 0 \quad [\because \bar{a}^{-1}a = 1 \text{ & } 1b = b]$$

Similarly let $ab = 0$ with $b \neq 0$ and b^{-1} exists we have

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

Therefore a (skewfield) division ring has no-zero divisors.

Boolean Ring — An element a of a ring R is said to be idempotent if $a^2 = a$. A ring R is called a Boolean Ring if all its elements are idempotent i.e. $a^2 = a \forall a \in R$.

S./ If R is a ring such that $a^2 = a \forall a \in R$. Prove that
 (i) $a + a = 0 \forall a \in R$

- (i) $a+a=0 \forall a \in R$. i.e. each element of R is its own additive inverse.
 - (ii) $a+b=0 \Rightarrow a=-b$,
 - (iii) R is a commutative ring.

Sol: i) As $a \in R \Rightarrow a+a \in R$; $a^2 = a$ (given)
Hence $(a+a)^2$

$$\text{Hence } (a+a)^2 = a+a$$

$$\Rightarrow (a+a)(a+a) = a+a$$

$$\Rightarrow (a+a)a + (a+a)a = a+a \quad \text{By left distributive law.}$$

$$\Rightarrow (a, a+a \cdot a) + (a, a+a \cdot a) = a+a \quad \text{By Right distributive law.}$$

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

$$\Rightarrow (a+a) + (a+a) = a+a \quad [\text{given } a^2=a]$$

$$\Rightarrow (a+a) + (a+a) = (a+a) + 0 \quad [\because a+0 = a]$$

$\Rightarrow a+a = 0$ [By left cancellation law for addition in R]
 Proved $\underline{\underline{\rightarrow}}$

$$\text{(ii)} \quad a + b = 0 \Rightarrow a = -b \quad \text{arrow}$$

We have just proved that $a + a = 0$

$$a+b=0 \Rightarrow (a+b) = (a+a) \Rightarrow a+b = a+a \rightarrow b=a$$

By left cancellation law for addition in \mathbb{R}

(iii) R is a commutative ring.
We have a 1?

We have $(a+b)^2 = a+b$ [given $a^2 = a$]

$$\Rightarrow (a+b)(a+b) = (a+b)$$

$$\Rightarrow (a+b)a + (a+b)b = a+b \quad \text{By left distributive law}$$

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

By right distributive law

$$\Rightarrow (a+b-a) + (ab+ba) = a+b \quad [\because a^2=a]$$

$$\Rightarrow ba + ab = 0 \quad [\text{By left cancellation}]$$

$$\Rightarrow ab = ba \quad [\text{From part (ii) of s.t. by left cancellation law}]$$

$\therefore R$ is commutative. [From part (ii) as $a+b=0 \Rightarrow a=-b$]

Proved //