RINGS Set-VII

*** Defn:**

An algebraic structure $(R,+,\cdot)$ where R is a non-empty set and $+^n, x^n$ are two binary operations on R, is called a ring if it satisfies the following properties:

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

(i) Closure prop:
$\forall a,b \in R \Rightarrow a+b \in R$

(ii) Associative prop:
$\forall a,b,c \in R$
$\Rightarrow (a+b)+c = a+(b+c)$

(iii) Existence of identity:
$\exists\ 0 \in R$ s.t $a+0=0+a=a\ \forall a \in R$
Here '0' is the identity elt in R.

(iv) Existence of inverse:
for each $a \in R$, $\exists\ -a \in R$ s.t
$a+(-a)=(-a)+a=0$
Here $-a$ is the inverse of a in R

(v) Commutative prop:
$\forall a,b \in R \Rightarrow a+b=b+a$

II. $(R,*)$ is a semigroup.

(i) closure prop:
$\forall a,b \in R \Rightarrow a.b \in R$.

(ii) Asso. prop:
$\forall a,b,c \in R \Rightarrow (ab)c = a(bc)$

III. Distributive laws:
$\forall a,b,c \in R$
(i) $a\cdot(b+c) = a\cdot b + a\cdot c$ (LDL)
(ii) $(b+c)\cdot a = b\cdot a + c\cdot a$ (RDL)

*** Ring with unity ***

A ring R which contains the multiplicative identity (called unity) is called a ring with unity
i.e, if $1 \in R$ s.t $a\cdot 1 = 1\cdot a = a\ \forall a \in R$
then the ring R is called a ring with unity

*** Ring without unity:**

A ring R which doesnot contain multiplicative identity is called a ring without unity.

*** Commutative Ring:**

If in a ring R, the Commutative property w.r.t x^n is satisfied then the ring R is called commutative ring.
i.e, if $\forall a,b \in R \Rightarrow a\cdot b = b\cdot a$
then the ring R is called a commutative ring.

Defn → A ring is called finite or infinite according as it contains finite or infinite number of elements.

Division ring (or) Skew field

If in a ring 'R', the non-zero elts form a group w.r.t x^n, a ring R is called a Division ring

(or)

A ring R is a division ring if

(i) R has atleast two elts

(ii) R has unity

(iii) Each non-zero elt of R has multiplicative inverse.

* Zero Divisor of a ring:

Let $(R,+,\cdot)$ be a ring.

If there exist $a,b \in R$, where $a \neq 0$, $b \neq 0$ and $ab = 0$ then R is called ring with zero divisors

(or) a, b are called zero divisors.

Here 'a' is called the left zero divisor and 'b' is called the right-zero divisors.

(or)

A non-zero elt of a ring R is called a zero divisor (or) a divisor of zero if $\exists$ an elt $b \neq 0 (\in R)$ s.t either $ab = 0$ or $ba = 0$

* Ring without zero divisors:-

A ring which is not with zero divisor is called ring without zero divisor.

i.e, if $a \neq 0, b \neq 0$ then $ab \neq 0$

(or)

A ring R is said to have no zero divisors if $a, b \in R$ and $ab = 0 \Rightarrow a = 0$ (or) $b = 0$

Ex: (1) The ring of integers has no zero divisors.

for $a, b \in \mathbb{Z}$ and $ab = 0$

$\Rightarrow a = 0$ or $b = 0$

(2) The ring $(R,+,\cdot)$ where $R = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ has zero divisors.

i.e, $\bar{2}, \bar{3} \in R \Rightarrow \bar{2}\cdot\bar{3} = \bar{0}$ (mod 6)

(3) The ring $(R,+,\cdot)$ where R = set of 2x2 matrices whose elts are real numbers has zero divisors.

Since $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq 0$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \neq 0$ $\in R$

$\Rightarrow AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$

* Integral Domain

A Commutative ring with unity and without zero divisors is called an I.D.

i.e, A ring R is an Integral domain if (i) R is Commutative

(ii) R has unity

(iii) R is without zero divisors

* Field:

A commutative division ring is called field.

i.e, A ring R is said to be a field if it has atleast two elts and (i) is commutative

(ii) has unity

(iii) every non-zero elt of R is invertible w.r.t x^n.

* Some elementary properties of Rings:

Theorem If R is a ring and $0, a, b \in R$ then (i) $0a = a0 = 0$

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

(iii) $(-a)(-b) = ab$ and

(iv) $a(b-c) = ab - ac$

Proof

(i) $0a = (0+0)a$

$0 + 0a = 0a + 0a$ (By RDL)

$\Rightarrow 0 = 0a$ (By RCL)

Similarly we can prove that $a0 = 0$

$\therefore 0a = a0 = 0$

(ii) To prove that $a(-b) = -(ab)$

Now we have

$a0 = a(-b+b)$

$\Rightarrow a(-b+b) = a0$

$\Rightarrow a(-b) + ab = 0$ (by (i) & LDL)

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

Similarly we can prove that

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

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

(iii) $(-a)(-b) = -[(-a)b]$ [by (ii)]

$= -[-(ab)]$ (by (ii))

$= ab$

(iv) $a(b-c) = a[b+(-c)]$

$= ab + a(-c)$ (by LDL)

$= ab - ac$ (by (ii))

Theorem If R is a ring with unit elt and $a \in R$ then (i) $(-1)a = -a$

(ii) $(-1)(-1) = 1$

Proof (i) Now we have

$0a = (-1+1)a$

$\Rightarrow (-1+1)a = 0a$

$\Rightarrow (-1)a + (1)a = 0$

$\Rightarrow (-1)a + a = 0$

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

(ii) for $a \in R$, we have $(-1)a = -a$

Taking $a = -1$

$\therefore (-1)(-1) = -(-1)$

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

Examples:-

(1) Let $R = \{0\}$ and $+, \cdot$ be the binary operations defined by $0+0=0$ and $0 \cdot 0 = 0$ then $(R, +, \cdot)$ is clearly a ring, called the null ring or zero ring.

(4)

(2) → I = the set of integers

I. (i) $\forall a, b \in I \Rightarrow a+b \in I$

∴ Closure property is satisfied.

(ii) $\forall a, b, c \in I$

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

∴ Asso. prop. is satisfied

(iii) $\exists\, 0 \in I$ s.t $a+0 = 0+a = a \ \forall a \in R$

Identity elt $= 0 \in I$

∴ Identity prop. is satisfied

(iv) For each $a \in I$ $\exists\, -a \in I$ s.t $a+(-a) = (-a)+a = 0$

∴ '$-a$' is the inverse of 'a' in I

Inverse prop. is satisfied.

(v) $\forall a, b \in I \Rightarrow a+b = b+a$

∴ Commutative property is satisfied.

∴ $(I, +)$ is an abelian group.

II. (i) $\forall a, b \in I \Rightarrow a.b \in I$

Closure prop. is satisfied

(ii) $\forall a, b, c \in I$

$\Rightarrow (a.b).c = a.(b.c)$

∴ $(I, \cdot)$ is a semigroup.

III. $\forall a, b, c \in I$

(i) $a.(b+c) = ab+ac$ (LDL)

(ii) $(b+c).a = ba+ca$ (RDL)

∴ Distributive laws are satisfied.

∴ $(I, +, \cdot)$ is a ring.

IV. $\exists\, 1 \in I$ s.t $a.1 = 1.a = a \ \forall a \in I$

∴ Identity elt $= 1 \in I$

∴ $(I, +, \cdot)$ is a ring with unity.

V. $\forall a, b \in I \Rightarrow a.b = b.a$

∴ Comm. prop. is satisfied.

∴ $(I, +, \cdot)$ is a Comm. ring with unity.

VI. $\forall a, b \in I$

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

∴ I doesnot Contain zero divisors.

∴ $(I, +, \cdot)$ is an integral domain.

VII. $\forall a \neq 0 \in I$ $\exists\, \frac{1}{a} \notin I$ s.t

$a.\frac{1}{a} = \frac{1}{a}.a = 1$

Inverse prop. is not satisfied. w.r.t x^n.

∴ $(I, +, \cdot)$ is not a field.

(3) → The set N of natural numbers is not a ring w.r.t. $+^n$ & x^n. because $(N, +)$ is not group.

(4) → I_E = The set of even integers including zero is a commutative ring

(5) → The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

(6) → The set of irrational numbers under $+^n$ & x^n is not a ring.

(6) The set M of all $n \times n$ matrices with their elts as real numbers (rational numbers, complex numbers, integers) is a non-commutative ring with unity w.r.t. $+^n$ & $\times^n$.

Soln

I. (i) $\forall A, B \in M \Rightarrow A+B \in M$

Closure prop. is satisfied.

(ii) $\forall A, B, C \in M$

$(A+B)+C = A+(B+C)$

$\therefore$ Asso. prop. is satisfied.

(iii) $\exists B = O_{n\times n} \in M$ s.t

$A+B = B+A = A \quad \forall A \in M$

Identity elt $= O_{n\times n} \in M$

$\therefore$ Identity prop is satisfied.

(iv) for each $A \in M \exists -A \in M$

s.t $A+(-A) = (-A)+A = O$

$\therefore$ Inverse of A is '$-A$'.

$\therefore$ Inverse prop. is satisfied.

(v) $\forall A, B \in M \Rightarrow A+B = B+A$

$\therefore$ commutative prop. is satisfied.

II. (i) $\forall A, B \in M \Rightarrow A \cdot B \in M$

$\therefore$ Closure prop. is satisfied.

(ii) $\forall A, B, C \in M$

$\Rightarrow (A \cdot B)C = A(BC)$.

$\therefore$ Asso. prop. is satisfied.

III. $\forall A, B, C \in M$

(i) $A \cdot (B+C) = AB + AC$

(ii) $(B+C) \cdot A = BA + CA$.

$\therefore$ Distributive laws satisfied.

$\therefore (M, +, \cdot)$ is a ring.

IV. $\exists B = I$ (unit Matrix) $\in M$

s.t $A \cdot B = B \cdot A = A, \forall A \in M$

$\therefore$ Identity elt $= I$ (Identity matrix)

$\therefore (M, +, \cdot)$ is a ring with unity.

V. $\forall A, B \in M$

$\Rightarrow A \cdot B \neq B \cdot A$.

$\therefore$ commutative prop. is not satisfied w.r.t $\times^n$.

$\therefore (M, +, \cdot)$ is non-commutative ring with unity.

---

(7) $\rightarrow F = \{ b\sqrt{2} \mid b$ is a rational number$\}$

Soln Let $a\sqrt{2}, b\sqrt{2} \in F$ where $a, b \in \mathbb{Q}$

$\Rightarrow a\sqrt{2} + b\sqrt{2} = (a+b)\sqrt{2} \in F$

$(\because a+b \in \mathbb{Q})$

Closure prop. is satisfied w.r.t $+^n$.

$\therefore +^n$ is a binary operation on F.

(ii) Let $a\sqrt{2}, b\sqrt{2} \in F$; $a, b \in \mathbb{Q}$

$\Rightarrow a\sqrt{2} \cdot b\sqrt{2} = ab(2) \notin F$.

$\therefore \times^n$ is not b-o. on F.

(8) $Q[\sqrt{2}] = \{a+b\sqrt{2} / a,b \in Q\} \subseteq R$.
$+^n$ & $\times^n$ b-O's on F.

Sol: I. (i) Closure prop:
Let $a+b\sqrt{2}, c+d\sqrt{2} \in F$ $a,b,c,d \in Q$
$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in F$
$(\because a+c, b+d \in Q)$
$\therefore$ Closure prop. is satisfied.

(ii) Asso. prop:
Let $x,y,z \in F \subseteq R$.
Choosing $x = a+b\sqrt{2}, y = c+d\sqrt{2}, z = e+f\sqrt{2}$ where $a,b,c,d,e,f \in Q$
$\therefore (x+y)+z = x+(y+z)$ (by Asso. prop. of R)
$\therefore$ Asso. prop. is satisfied.

(iii) Existence of Left Identity
$\forall x = a+b\sqrt{2} \in F$, where $a,b \in Q$ $\exists\ y = 0+0\sqrt{2} \in F$; $0 \in Q$
s.t $y+x = (0+0\sqrt{2}) + (a+b\sqrt{2})$
$= (0+a) + (0+b)\sqrt{2}$ $\quad 0+a \in Q$, $0+b \in Q$
$= a+b\sqrt{2}$
$= x$.
$\therefore$ the identity elt $= 0+0\sqrt{2} = 0$ is in F.

(iv) Existence of left inverse:
for each $a+b\sqrt{2} \in F$ $a,b \in Q$ $\exists\ -a-b\sqrt{2} \in F$ $-a,-b \in Q$
s.t $(-a-b\sqrt{2}) + (a+b\sqrt{2}) = (-a+a) + (-b+b)\sqrt{2}$
$= 0+0\sqrt{2} = 0$
$(\because -a+a = 0,\ -b+b = 0)$
$\therefore$ Inverse of $a+b\sqrt{2} = -a-b\sqrt{2} \in F$.

(v) commutative property:
$\forall x,y \in F \subseteq R$.
$\Rightarrow x+y = y+x$ (by comm. prop. of R)
$\therefore$ Comm. prop. is satisfied.
$\therefore (F,+)$ is an abelian group.

II. (i) Closure prop:
Let $x = a+b\sqrt{2}, y = c+d\sqrt{2} \in F$; $a,b,c,d \in Q$
then $x \cdot y = (a+b\sqrt{2})(c+d\sqrt{2})$
$= (ac+2bd) + (ad+bc)\sqrt{2}$
$\in F$ $(\because ac+2bd, ad+bc \in Q)$
$\therefore$ Closure prop. is satisfied.

(ii) Let $x,y,z \in F \subseteq R$
Choosing $x = a+b\sqrt{2}, y = c+d\sqrt{2}$, $z = e+f\sqrt{2}$; $a,b,c,d,e,f \in Q$
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (by Asso. prop. of R)
$\therefore$ Asso. prop. is satisfied.
$\therefore (F,\cdot)$ is a semi group.

III. Let $x,y,z \in F \subseteq R$
$x \cdot (y+z) = x \cdot y + x \cdot z$ (by LDL of R)
$(y+z) \cdot x = y \cdot x + z \cdot x$ (by RDL of R)
$\therefore$ Distributive laws are satisfied.
$\therefore (F,+,\cdot)$ is a ring.

IV. Identity prop:
$\exists\ 1+0\sqrt{2} = 1 \in F$; $0,1 \in Q$
s.t $(1+0\sqrt{2})(a+b\sqrt{2}) = a+b\sqrt{2}$
$\forall a+b\sqrt{2} \in F$; $a,b \in Q$
$\therefore$ Identity elt w.r.t $\times^n$ is 1.
$= 1+0\sqrt{2} \in F$
$\therefore$ Identity prop. is satisfied.
$\therefore (F,+,\cdot)$ is a ring with unity.

V. Commutative prop:
Let $x,y \in F \subseteq R$
Choosing $x = a+b\sqrt{2}, y = c+d\sqrt{2}$, $a,b,c,d \in Q$

$\therefore x.y = y.x$ (by comm. prop. of R)

$\therefore$ Comm. prop. is satisfied in F.

$\therefore (F,+,\cdot)$ is a commutative ring with unity.

VI. Let $x, y \in F \subseteq R$

Choosing $x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$ $a,b,c,d \in \mathbb{Q}$

$\therefore x.y = 0 \Rightarrow x = 0$ or $y = 0$

$\therefore$ F doesnot contain zero divisors.

$\therefore (F,+,\cdot)$ is an integral domain.

VII. Let $a+b\sqrt{2} \neq 0 \in F$, $a \neq 0$, or $b \neq 0 \in \mathbb{Q}$

s.t $(c+d\sqrt{2})(a+b\sqrt{2}) = 1$

$\Rightarrow c+d\sqrt{2} = \frac{1}{a+b\sqrt{2}}$

$= \frac{a-b\sqrt{2}}{a^2-2b^2}$

$= \frac{a}{a^2-2b^2} - \frac{b(\sqrt{2})}{a^2-2b^2}$

$= \frac{a}{a^2-2b^2} + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in F$

$\left(\because \frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}\right.$ & $\left. a^2-2b^2 \neq 0\right)$

$\therefore \exists \frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2} \in F \subseteq R.$

s.t $\left(\frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2}\right)(a+b\sqrt{2}) = 1$ $\forall a+b\sqrt{2} \in F$

$\therefore$ Inverse of $a+b\sqrt{2}$ is $\frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2} \in F$.

$\therefore$ Every non-zero elt of F has inverse w.r.t $\times$.

$\therefore$ Inverse prop. is satisfied.

$\therefore (F,+,\cdot)$ is a field.

H.W $\rightarrow F = \mathbb{Z}(\sqrt{2}) = \{a+b\sqrt{2} / a, b \text{ are integers}\} \subseteq R.$

$(F,+,\cdot)$ is an I.D. but not field.

H.W $\rightarrow F = J[i]$ = the set of Gaussian integers $= \{a+bi / a,b \in I\} \subseteq \mathbb{C}$

$(F,+,\cdot)$ is an ID but not field.

$\rightarrow$ Show that the set I of integers with two binary operations '$*$' and '$\circ$' defined by $a*b = a+b-1$, $a \circ b = a+b-ab$ $\forall a,b \in I$ is comm. ring.

Soln $\forall a,b \in I$

$a*b = a+b-1$ — (1)

and $a \circ b = a+b-ab$ — (2)

I. from (1)

(i) we have $a*b = a+b-1 \in I$

$\therefore *$ is closed in I.

(ii) $\forall a,b,c \in I$

$(a*b)*c = a*(b*c)$.

Since $(a*b)*c = (a+b-1)*c$
$= (a+b-1)+c-1$
$= a+b+c-2$
$a*(b*c) = a*(b+c-1)$
$= a+(b+c-1)-1$
$= a+b+c-2$
$\therefore$ Asso. prop. is satisfied.

(iii) Existence of left identity:
$\forall a \in I \ \exists\, b \in I$ s.t $b*a = a$
$\rightarrow b+a-1 = a$
$\Rightarrow b = 1$
$\therefore \forall a \in I \ \exists\, 1 \in I$ s.t $1*a = a$
$\therefore$ 1 is the identity in I w.r.t *

(iv) Existence of left inverse.
for each $a \in I \ \exists\, b \in I$ s.t $b*a = 1$
$\Rightarrow b+a-1 = 1$
$\Rightarrow b = 2-a \in I$
$\therefore$ For each $a \in I \ \exists\, b = 2-a \in I$
s.t $(2-a)*a = 1$
$\therefore b = 2-a$ is the inverse of 'a' in I w.r.t *

(v) Comm. prop:
$\forall a,b \in I$, $a*b = b*a$
Since $a*b = a+b-1$
$= b+a-1$
$= b*a$.
$\therefore$ * is commutative in I.
$\therefore (I,*)$ is abelian group.

II. from (2) (ii) Closure prop:
$\forall a,b \in I$; $aob = a+b-ab \in I$
$\therefore$ 'o' is closed in I

(ii) $\forall a,b,c \in I$.
$ao(boc) = (aob)oc$.
Since $(aob)oc = (a+b-ab)oc$
$= (a+b-ab)+c-(a+b-ab)c$
$= a+b+c-ab-ac-bc+abc$
and $ao(boc) = ao(b+c-bc)$
$= a+(b+c-bc)-a(b+c-bc)$
$= a+b+c-ab-bc-ac+abc$.
$\therefore$ 'o' is associative in I.
$\therefore (I,o)$ is a semigroup.

III. Left distributive law (8)
$\forall a,b,c \in I \Rightarrow ao(b*c) = ao[b+c-1]$
$= a+(b+c-1) - a(b+c-1)$
$= a+b+c-1-ab-ac+a$
$= (a+b-ab)+(a+c-ac)-1$
$= (aob)+(aoc)-1$
$= (aob)*(aoc)$.
$\therefore$ Distributive law is satisfied.
$\therefore (I,*,o)$ is a ring.

IV. Comm. prop
$\forall a,b \in I$
$\rightarrow aob = a+b-ab$
$= b+a-ba$
$= boa$
$\therefore$ 'o' is commutative in I.
$\therefore (I,*,o)$ is a commutative ring.

H.W $\rightarrow$ If $(R,+,\cdot)$ is a ring with unit elt. show that $(R,\oplus,\otimes)$ is also a ring with unit elt, where $a \oplus b = a+b+1$ & $a \otimes b = ab+a+b$ $\forall a,b \in R$.

H.W $\rightarrow$ If E denotes the set of even integers, then prove that $(E,+,*)$ is a commutative ring. where $a*b = \frac{ab}{2}$ and '+' is usual addition.

H.W $\rightarrow$ P.T the set 'S' of all ordered pairs (a,b) of real numbers is a commutative ring under $+^n$ & $\times^n$ Compositions defined as
$(a,b)+(c,d) = (a+c, b+d)$ and
$(a,b)(c,d) = (ac, bd)$

Defn: Cancellation laws in a Ring:

In a ring R, for $a, b, c \in R$ if $a \neq 0$, $ab = ac \Rightarrow b = c$ (LCL)

and $a \neq 0$, $ba = ca \Rightarrow b = c$ (RCL)

then we say that cancellation laws hold in R.

Theorem: (2004) A ring R is without zero divisors iff the cancellation laws hold in R.

Proof: Let the ring R will have no zero divisors

To prove that the cancellation laws hold in R.

Let $a, b, c \in R$ and $a \neq 0$,

we have $ab = ac$

$\Rightarrow ab + (-ac) = 0$

$\Rightarrow ab + a(-c) = 0$

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

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

$\Rightarrow a = 0$ or $b - c = 0$ ($\because R$ has no zero divisors)

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

$\Rightarrow b = c$.

Similarly we prove that $a, b, c \in R$ and $a \neq 0$,

$ba = ca \Rightarrow b = c$

Conversely suppose that the cancellation laws hold in R. we have to prove that R has no zero divisors.

If possible suppose that R has zero divisors then $\exists\ a, b \in R$ such that $a \neq 0$, $b \neq 0$ and $ab = 0$.

Now we have $a \neq 0$, $ab = 0$

$\Rightarrow a \neq 0$, $ab = a0$

$\Rightarrow b = 0$ (by LCL)

which is a contradiction.

$\therefore R$ has no zero divisors.

→ R is a ring with unit element and $x \neq 0$ in R and a unique $y \in R$ exists so that $xyx = x$; Show that $xy = yx = 1$.

(or)

Let R be a ring with unity $1 \in R$. Suppose for $x \neq 0 \in R$, there exists a unique $y \in R$ such that $xyx = x$. Prove that $xy = yx = 1$ i.e.,

Soln: Let $xa = 0$, where $a \in R$

Then $x(y+a)x = xyx + xax$

$= x + 0x = x$. ($\because xa = 0$)

By the uniqueness of y in the relation $xyx = x$, it follows that

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

$\Rightarrow a = 0$.

Hence $xa = 0 \Rightarrow a = 0$ for each $a \in R$. ①

Again $xyx = x \Rightarrow xyx - x \cdot 1 = 0$

$\Rightarrow x(yx - 1) = 0$

$\Rightarrow yx - 1 = 0$, (by ①)

$\Rightarrow \boxed{yx = 1}$

Similarly, we can show that

$ax = 0 \Rightarrow x(a+y)x = x \Rightarrow a+y = y \Rightarrow a = 0$ ②

and therefore $xyx = x \Rightarrow (xy-1)x = 0 \Rightarrow xy - 1 = 0$

$\Rightarrow \boxed{xy = 1}$ (by ②)

$\therefore xy = yx = 1$

→ Let R be a commutative ring with unity. Then R is an ID iff $ab = ac \Rightarrow b = c$ where $a, b, c \in R$ and $a \neq 0$.

(or)

A commutative ring R with unity is an ID iff the cancellation laws hold in R.

Proof: Suppose R is an ID then we have to show that the cancellation laws hold in R.

Let $a, b, c \in R$ and $a \neq 0$

we have $ab = ac$

$\Rightarrow a(b-c) = 0$ ——— ①

Since R is ID.

i.e., R is a commutative ring with unity and has no zero divisors.

$\therefore$ from ①, either $a=0$ or $b-c=0$

but it is given that $a \neq 0$.

$\therefore b-c=0$

$\Rightarrow b=c$

Similarly we prove that $a, b, c \in R$, $a \neq 0$,

$ba = ca \Rightarrow b=c$

$\therefore$ The cancellation laws hold in R.

Conversely suppose that the cancellation laws hold in R.

we prove that R is an ID.

for this we are enough to prove that R has no zero divisors.

If possible let R has zero divisors. then

$\exists\, a, b \in R$ such that $a \neq 0$, $b \neq 0$ and $ab=0$

Now we have $a \neq 0$, $ab=0$

$\Rightarrow a \neq 0$, $ab = a0$

$\Rightarrow b=0$ (By LCL)

which is contradiction

$\therefore$ R has no zero divisors.

$\therefore$ R is an ID.

Note: The cancellation laws may not hold in an arbitrary ring.

Let $A=\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$, $B=\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}$ and $C=\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}$ be three elements in the ring M_2 of all 2×2 matrices over the integers. Then $AC=\begin{bmatrix}2 & 0\\ 2 & 0\end{bmatrix}=BC$ but $A \neq B$.

Theorem A divison ring has no zero divisors.

proof: Let $(R,+,\cdot)$ be a divison ring.

i.e, in a ring R, the non-zero elements form a group w.r.t x^n.

Let $a,b \in R$ and $a \neq 0$.

Since R is a divison ring.

for $a \neq 0 \in R \Rightarrow a^{-1}$ exists in R.

$\therefore a a^{-1} = a^{-1} a = 1$.

Now we have $ab = 0$

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

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

$\Rightarrow 1b = 0$

$\Rightarrow b = 0$

$\therefore a,b \in R, a \neq 0$ and $ab = 0 \Rightarrow b = 0$.

Similarly we can prove that $a,b \in R, b \neq 0$ and

$ab = 0 \Rightarrow a = 0$

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

$\therefore R$ has no zero divisors.

Theorem A field has no zero divisors.

proof: Same as the proof of the above theorem

Defn: The pigeon-Hole principle: If 'n' objects are distributed over x places in such a way that no place receives more than one object then each place receives exactly one object.

Theorem Every field is an I.D.

proof: Let F be a field then by defn F is a commutative ring with unity and every non-zero elt. is invertible w.r.t x^n.

In order to prove that a field is an I.D.

we have to prove that a field F has no zero divisors.

Let $a, b \in F$ and $a \neq 0$.

since F is a field.

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

$\therefore a a^{-1} = a^{-1} a = 1$

Now we have

$ab = 0$

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

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

$\Rightarrow 1b = 0$

$\Rightarrow b = 0$

Similarly we can prove that $a, b \in F$, $b \neq 0$ and $ab = 0 \Rightarrow a = 0$.

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

$\therefore$ F has no zero divisors.

$\therefore$ A field is an ID.

Note: The converse of the above need not be true.

i.e, every ID need not be a field.

Eg: The ring of integers $(\mathbb{Z}, +, \cdot)$ is an ID but not field. because $2 (\neq 0) \in \mathbb{Z}$ has no x^{ve} inverse.

Theorem 2002: A finite integral domain is a field.

proof: Let F be the finite ID.

Let $F = \{a_1, a_2, \ldots\ldots a_n\}$ and F contains 'n' distinct elements.

TO prove that F is a field.

for this we are enough to prove that the non-zero elements of F have x^ve inverse.

Let $a \neq 0 \in F$

$\therefore aa_1, aa_2, \ldots\ldots aa_n \in F$ (by Closure prop.)

All these elements are distinct.

because: If possible

Let $aa_i = aa_j$; $a_i, a_j \in F$

$\Rightarrow a(a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$ ($\because a \neq 0$ & F is an ID i.e., F doesnot contain zero divisors)

$\Rightarrow a_i = a_j$

This is a contradiction to hypothesis that F contains n distinct elements.

$\therefore$ our assumption that $aa_i = aa_j$ is wrong.

$\therefore aa_1, aa_2, \ldots\ldots aa_n$ are all distinct elements in F which has exactly 'n' elements.

By the pigeon-hole prineiple, one of these products must be equal to one. ($\because$ F is an ID)

Let $aa_r = 1$ for some $a_r \in F$.

$\therefore a^{-1} = a_r$.

$\therefore$ Every non-zero element of F has x^ve inverse.

$\therefore$ F is a field.

Theorem 2000 A finite commutative ring with out zero divisors is a field.

proof: Let F be a finite commutative ring with out zero divisors.

Let $F = \{a_1, a_2, \ldots\ldots a_n\}$ and F contains 'n' distinct elements.

To prove that F is a field.

for this we ale enough to prove that an element $1 \in F$ such that $1 \cdot a = a \cdot 1 = a \ \forall a \in F$ and also for every element $a \neq 0 \in F$, there exists an element $b \in F$ such that $ab = ba = 1$.

Let $a \neq 0 \in F$.

$\therefore aa_1, aa_2 \ldots aa_n \in F$ (by closure prop of F)

All these elts are distinct.

because, If possible

let $aa_i = aa_j$; $a_i, a_j \in R$

$\Rightarrow a(a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$ ($\because a \neq 0$ & F is without zero divisors)

$\Rightarrow a_i = a_j$

which is contradiction to hyp. that f contains n distinct elts.

$\therefore aa_1, aa_2 \ldots aa_n$ are all distinct elts of R of which has exactly n elts.

$\therefore$ By the pigeon-hole principle, every element of F can be written as aa_i for some $a_i \in F$.

since $a \neq 0 \in F$, we have $a = aa_i$ for some $a_i \in F$.

Since F is commutative.

$\therefore a = aa_i = a_i a$.

we now prove that a_i is unit element.

Let $y \in F$ then $y = aa_j$ for some $a_j \in F$.

$$\Rightarrow a_i y = a_i(aa_j)$$
$$= (a_i a)a_j$$
$$= aa_j$$
$$= y$$

$\Rightarrow a_i y = 1 \cdot y \Rightarrow a_i = 1$ (by RCL)

$\therefore a \in F \ \exists\ 1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$.

$\therefore$ 1 is the unit element in F.

since $1 \in F$

$1 = aa_k$ for some $a_k \in F$.

$\therefore$ for $a \neq 0 \in F$, $\exists\ a_k \in F$ such that $aa_k = 1 = a_k a$ ($\because$ F is comm.)

$\therefore a \neq 0 \in D$ has x^{ve} inverse in F.

$\therefore$ F is a field.

2005 → $(F = \{\{0, 1, 2, 3, 4, 5\}, +_6, \times_6)$

Sol^n Form the composition tables for F w.r.t $+_6$ & $\times_6$.

table (i)

$+_6$	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

table (ii)

$\times_6$	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

(I) From table (i)

(i) Closure prop: All the elements of the composition table are elements of set F.

$\therefore$ Closure prop., is satisfied.

(ii) Asso. prop:

$2, 4, 5 \in F \Rightarrow (2 +_6 4) +_6 5 = 2 +_6 (4 +_6 5)$.

Since $(2 +_6 4) +_6 5 = 0 +_6 5 = 5$

and $2 +_6 (4 +_6 5) = 2 +_6 3 = 5$.

$\therefore \forall a, b, c \in F \Rightarrow (a +_6 b) +_6 c = a +_6 (b +_6 c)$.

$\therefore$ Asso. prop is satisfied.

(iii) The first row of table (i) coincides with the top row.
∴ The element in the extreme left column of the first row i.e, '0' is the identity element.
∴ Identity prop. is satisfied.

(iv) Every row & column contains the identity element '0'.
∴ Inverse prop is satisfied.
Here $0 +_6 0 = 0$, inverse of 0 is 0
$1 +_6 5 = 5 +_6 1 = 0$, inverse of 5 is 1
" " 1 is 5
$2 +_6 4 = 4 +_6 2 = 0$, inverse of 4 is 2
" " 2 is 4.
$3 +_6 3 = 3 +_6 3 = 0$ inverse of 3 is 3.

(v) Interchanging the rows and columns. There is no change in the table.
∴ Comm. prop is satisfied.
∴ (F, +) is an abelian group.

(II) From the table (ii).

(i) Closure prop: All the entries of the composition table are the elements of the set F.
∴ Closure prop is satisfied.

(ii) $2, 3, 5 \in F$
$(2 \times_6 3) \times_6 5 = 2 \times_6 (3 \times_6 5)$
Since $(2 \times_6 3) \times_6 5 = 0 \times_6 5 = 0$
and $2 \times_6 (3 \times_6 5) = 2 \times_6 3 = 0$
∴ $\forall a, b, c \in F \Rightarrow (a \times_6 b) \times_6 c = a \times_6 (b \times_6 c)$.
∴ Asso. prop. is satisfied.

(III) Distributive laws:

$2, 3, 5 \in F$.

$\Rightarrow 2 \times_6 (3 +_6 5) = (2 \times_6 3) +_6 (2 \times_6 5)$.

since $2 \times_6 (3 +_6 5) = 2 \times_6 (2) = 4$

and $(2 \times_6 3) +_6 (2 \times_6 5) = 0 +_6 4 = 4$

Similarly $(3 +_6 5) \times_6 2 = (3 \times_6 2) +_6 (5 \times_6 2)$

$\therefore \forall a, b, c \in F$

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

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

$\therefore$ Distributive laws are satisfied.

$(F, +_6, \times_6)$ is a ring.

(IV) Identity property:

From the table (ii), the second row coincides with the top row.

$\therefore$ The element in extreme left column of second row i.e, 1 is the identity element.

$\therefore$ Identity prop. is satisfied.

$\therefore (F, +_6, \times_6)$ is a ring with unity.

(V) from table (ii),

interchanging rows and columns, there is no change in the table.

$\therefore$ comm. prop is satisfied w.r.t $\times_6$.

(VI) From table (ii),

$2 \neq 0, 3 \neq 0$, but $2 \times_6 3 = 0$

$3 \neq 0, 4 \neq 0$ but $3 \times_6 4 = 0$

$\therefore a \neq 0, b \neq 0 \in F \Rightarrow a \times_6 b = 0$.

$\therefore$ F contains zero divisors.

$\therefore (F, +_6, \times_6)$ is not an ID.

(vii) from the table (ii),

$3^{rd}, 4^{th}, 5^{th}$ rows & columns donot contain Identity element 1.

$\therefore$ Inverses 2, 3, 4 donot exist.

$\therefore$ Inverse prop is satisfied.

$\therefore (F, +_6, \times_6)$ is not a field.

Theorem → Let p be a prime number. prove that the set of integers I_p, $I_p = \{0, 1, 2, 3, \ldots\ldots p-1\}$ forms a field w.r.t $+^n$ & $\times^n$ modulo p.

Proof:

(I) If $a, b \in I_p$ and p is +ve integer then $a +_p b = r$, where r is the remainder when $a+b$ is divided by P.

Clearly $0 \leq r \leq p-1 < p$.

(i) Closure prop:

$\forall a, b \in I_p \Rightarrow a +_p b \in I_p$

Since $a +_p b = r$; $0 \leq r < p$.

$\therefore +_p$ is closed in I_p.

(ii) Asso. prop:

$\forall a, b, c \in I_p$

$\Rightarrow a +_p (b +_p c) = (a +_p b) +_p c$.

Since $a +_p (b +_p c) = a +_p (b + c)$ $(\because b +_p c \equiv b + c \pmod p)$

= remainder when $a+(b+c)$ is divided by p.

= remainder when $(a+b)+c$ is divided by p.

$= (a+b)+_p c$ (by def of $+_p$)

$= (a+_p b)+_p c$ $\because a+b \equiv a+_p b \pmod p$.

$\therefore +_p$ is associative in I_p.

(iii) Existence of identity:

Let $a \in I_p$ $\exists\, 0 \in I_p$ such that $0+_p a = a+_p 0 = a$.

$\therefore 0$ is the identity element in I_p.

(iv) Existence of inverse:

Since $0+_p 0 = 0$.

$\therefore$ The inverse of 0 is 0 itself.

If $r(\neq 0) \in I_p$ then $p-r \in I_p$

$\therefore (p-r)+_p r$ = remainder 0 when $(p-r)+r$ is divided by p.

$= r+_p (p-r)$.

$\therefore p-r$ is the inverse of 'r'.

i.e, every element in I_p has inverse

$\therefore$ Inverse prop. is satisfied w.r.t $+_p$.

(v) Comm. prop:

$\forall a, b \in I_p \Rightarrow a+_p b = b+_p a$.

Since $a+_p b$ = remainder when $a+b$ is divided by p.

= remainder when $b+a$ is divided by p.

$= b+_p a$.

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

(vi) Let $a, b \in I_p$ then $a \times_p b = r$ where 'r' is the remainder when ab is divided by p. and $0 \le r < p$.

(i) $\forall a, b \in I_p$

$\Rightarrow a \times_p b \in I_p$

Since $a \times_p b = r$; $0 \le r < p$.

$\therefore \times_p$ is closed on I_p.

(ii) $\forall a, b, c \in I_p$

$\Rightarrow a \times_p (b \times_p c) = (a \times_p b) \times_p c$

Since $a \times_p (b \times_p c) = a \times_p (bc)$

$(\because b \times_p c \equiv bc \pmod p)$

= remainder when $a(bc)$ is divided by p.

= remainder when $(ab)c$ is divided by p.

$= (ab) \times_p c$.

$= (a \times_p b) \times_p c$.

$\therefore \times_p$ is associative on I_p.

$\therefore (I_p, \times_p)$ is a semigroup.

(iii) Let $a, b, c \in I_p$ then

$a \times_p (b +_p c) = a \times_p (b + c)$

$(\because b +_p c \equiv b + c \pmod p)$

= remainder when $a(b+c)$ is divided by p.

= remainder when $(ab + ac)$ is divided by p.

$= (ab) +_p (ac)$

$= (a \times_p b) +_p (a \times_p c)$ $(\because ab \equiv a \times_p b \pmod p)$

$\therefore a \times_p (b +_p c) = (a \times_p b) +_p (a \times_p c)$

Similarly $(b +_p c) \times_p a = (b \times_p a) +_p (c \times_p a)$.

$\therefore$ Distributive Laws are satisfied.

i.e, $\times_p$ is distributive w.r.t $+_p$ on P.

$\therefore (I_p, +_p, \times_p)$ is a ring.

(IV) Let $\forall a, b \in I_p$; then $a \times_p b = b \times_p a$

Since $a \times_p b$ = remainder when ab is divided by p.

= remainder when ba is divided by p.

$= b \times_p a$

$\therefore \times_p$ is Comm. on I_p.

$\therefore (I_p, +_p, \times_p)$ is a comm. ring with unity.

(V) $\exists\ 1 \in I_p$ such that $a \times_p 1 = 1 \times_p a = a$ $\forall a \in I_p$.

$\therefore$ 1 is the identity element w.r.t $\times_p$.

(VI) Let $a, b \in I_p$. then $a \times_p b = 0$

$\Rightarrow$ ab is divided by p. i.e, $\frac{ab}{p}$

$\Rightarrow \frac{a}{p}$ or $\frac{b}{p}$. ($\because$ if a, b are integers and p is prime number then $\frac{ab}{p} \Rightarrow \frac{a}{p}$ or $\frac{b}{p}$)

$\Rightarrow a = 0$ or $b = 0$

$\therefore I_p$ is without zero divisors.

$\therefore (I_p, +_p, \times_p)$ is an ID.

(VII) Let $s \neq 0 \in I_p$ then $1 \leq s \leq p-1 < p$.

Consider the following $(p-1)$ products.

$1 \times_p s,\ 2 \times_p s,\ \ldots\ldots\ldots\ (p-1) \times_p s$.

All these are elements of I_p by Closure prop.

Also these elements are distinct.

because:

Let i, j be two integers such that

$1 \le i \le (p-1)$, $1 \le j \le (p-1)$ and $i > j$.

$\therefore 0 < (i-j) < p-1$

Now if possible that $i \times_p s = j \times_p s$.

$\Rightarrow$ is and js leave the same remainder when each is divided by p.

$\Rightarrow (i-j)s$ is divided by p.

$\Rightarrow \frac{i-j}{p}$ or $\frac{s}{p}$

which is contradiction.

$\therefore i \times_p s \neq j \times_p s$

$\therefore 1 \times_p s, 2 \times_p s, \ldots\ldots (p-1) \times_p s$ are all distinct.

One of these elements must be equal to 1.

Let $s' \times_p s = 1$

$\Rightarrow s'$ is the inverse of s.

i.e, each non-zero element of I_p has inverse.

$\therefore$ Inverse is satisfied w.r.t x^n.

$\therefore (I_p, +_p, \times_p)$ is a field.

Note: If 'p' is not prime then this is not a field. (Because this ring has zero divisors as well as every non-zero element possess doesnot +ve inverse.)

→ Prove that the set of residue classes modulo 'p' is a commutative ring with respect to $+^n$ and $\times^n$ of residue classes. Further show that the ring of residue classes modulo 'p' is a field iff 'p' is a prime.

Soln: Let I_p be the set of residue classes modulo p. Then the set I_p has distinct elements.

Let $I_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ldots (\overline{p-1})\}$

(I) (i) Closure prop:

$\forall\ \bar{a}, \bar{b} \in I_p$

$\Rightarrow \bar{a} + \bar{b} = \overline{a+b} \in I_p$

$\therefore I_p$ is closed w.r.t $+^n$.

$\because \overline{a+b} = \bar{r}$ where r is the remainder when $a+b$ is divided by p. Clearly $0 \le r < p$.

(ii) Asso. prop:

$\forall\ \bar{a}, \bar{b}, \bar{c} \in I_p$.

$\Rightarrow (\bar{a}+\bar{b})+\bar{c} = \overline{(a+b)} + \bar{c}$

$= \overline{(a+b)+c}$

$= \overline{a+(b+c)}$ ($\because +^n$ of integers is asso.)

$= \bar{a} + \overline{(b+c)}$

$= \bar{a} + (\bar{b}+\bar{c})$.

(iii) Existence of additive identity:

$\exists\ \bar{0} \in I_p$ such that $\bar{0}+\bar{a} = \bar{a} = \bar{a}+\bar{0}$ $\forall\ \bar{a} \in I_p$.

Since $\bar{0}+\bar{a} = \overline{0+a}$

$= \bar{a}$

and $\bar{a}+\bar{0} = \overline{a+0} = \bar{a}$

$\therefore \bar{0}$ is the identity element in I_p.

(iv) Existence of additive inverse:

Let $\bar{a} \in I_p$ then $-\bar{a} \in I_p$.

We have $(-\bar{a})+\bar{a} = \overline{(-a)+a}$

$= \bar{0}$.

Similarly $\bar{a}+(-\bar{a}) = \overline{a+(-a)} = \bar{0}$.

$\therefore (-\bar{a})+\bar{a} = \bar{a}+(-\bar{a}) = \bar{0}$.

$\therefore -\bar{a}$ is the inverse of $\bar{a}$ in I_p w.r.t $+^n$.

(v) Comm. prop. of $+^n$:

$\forall \bar{a}, \bar{b} \in I_p \Rightarrow \bar{a}+\bar{b} = \overline{a+b}$
$= \overline{b+a}$ ($+^n$ of integers is comm.)
$= \bar{b}+\bar{a}$.

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

(II) (i) Closure prop. of $\times^n$:

$\forall \bar{a}, \bar{b} \in I_p \Rightarrow \bar{a}\cdot\bar{b} = \overline{a\cdot b} \in I_p$.

$\therefore I_p$ is closed w.r.t $\times^n$.

(ii) Asso. prop. of $\times^n$:

$\forall \bar{a}, \bar{b}, \bar{c} \in I_p$.

$\Rightarrow (\bar{a}\cdot\bar{b})\bar{c} = \overline{(ab)}\,\bar{c}$
$= \overline{(ab)c}$
$= \overline{a(bc)}$
$= \bar{a}\,\overline{(bc)}$
$= \bar{a}(\bar{b}\bar{c})$

$\therefore (I_p, \cdot)$ is a semi group.

(III) Distributive laws:

$\forall \bar{a}, \bar{b}, \bar{c} \in I_p \Rightarrow \bar{a}\cdot(\bar{b}+\bar{c}) = \overline{a\cdot(b+c)}$
$= \overline{a(b+c)}$
$= \overline{ab+ac}$ ($\because \times^n$ is distributive w.r.t $+^n$ in $\mathbb{Z}$)
$= \overline{ab}+\overline{ac}$
$= \bar{a}\bar{b}+\bar{a}\bar{c}$. (LDL)

Similarly $(\bar{b}+\bar{c})\cdot\bar{a} = \bar{b}\bar{a} + \bar{c}\cdot\bar{a}$

$\therefore (I_p, +, \cdot)$ is a ring.

(IV) Comm. prop of x^n:

$\forall\ \bar{a}, \bar{b} \in I_p$

$\Rightarrow \bar{a}\cdot\bar{b} = \overline{ab}$
$= \overline{ba}$ ($\because$ x^n in integers is comm.)
$= \bar{b}\bar{a}$.

$\therefore (I_p, +, \cdot)$ is a commutative ring.

$\therefore (I_p, +, \cdot)$ is a finite comm. ring and it contains p elements.

Now suppose p is prime number.
we have to prove that I_p is a field.

(V) Let $\bar{a}, \bar{b} \in I_p$.
then $\bar{a}\cdot\bar{b} = 0$
$\Rightarrow \overline{a\cdot b} = 0$
$\Rightarrow p$ is divisor of ab. i.e, p/ab (or $\frac{ab}{p}$).
$\Rightarrow \frac{a}{p}$ or $\frac{b}{p}$. ($\because a, b \in \mathbb{Z}$ and p is prime then $\frac{ab}{p} \Rightarrow \frac{a}{p}$ or $\frac{b}{p}$)
$\Rightarrow \bar{a} = 0$ or $\bar{b} = 0$
$\therefore I_p$ is without zero divisors.

$\therefore I_p$ is a commutative ring without zero divisors. and I_p is finite.

But every finite commutative ring without zero divisors is a field.

$\therefore I_p$ is a field.

Conversely, suppose that I_p is a field.

$\therefore I_p$ is an ID.

$\therefore I_p$ is without zero divisors.

Now we are to prove that p is prime number.

If possible suppose that 'p' is not prime number then p is composite number.

Let $p = mn$ where $1<m<p$, & $1<n<p$.

$\Rightarrow \bar{p} = \overline{mn}$

$\Rightarrow \overline{mn} = \bar{p}$

$\Rightarrow \bar{m}\bar{n} = \bar{p}$

$\Rightarrow \bar{m}.\bar{n} = \bar{0}$ $(\because \bar{p} = \bar{0})$

Also $\bar{m} \neq \bar{0}$, $(\because 1<m<p)$

Similarly $\bar{n} \neq \bar{0}$. $(\because 1<n<p)$

$\therefore \bar{m}.\bar{n} = \bar{0}$

$\Rightarrow$ neither $\bar{m} = \bar{0}$ nor $\bar{n} = \bar{0}$.

$\mathbb{I}_p$ has zero divisors which is contradiction.

$\therefore p$ is prime.

Note: The collection of residue classes mod p is not a field if p is Composite number.

→ $F = \{0, 2, 4, 6, 8\}$ (mod 10)

→ $F = \{0, 1, 3, 5, 7, 8\}$ (mod 11)

→ $F = \{0, 1, 3, 4, 5, 9\}$ (mod 11).

2004. Prove that the ring Z_p or $\mathbb{Z}_p$ or $I/(p)$ of integers mod p is a field iff p is prime.

Proof: Let $\mathbb{I}_p$ be a field.

$\therefore I_p$ is an ID $\Rightarrow I_p$ is without zero divisors.

To poove that p is prime.

if possible let p be not prime,

Then p is composite number.

Let $p = mn$ where $1 < m < p$, $1 < n < p$; $m, n \in I$.

$\Rightarrow mn = p$

$\Rightarrow mn \equiv 0 \pmod p$ $(\because p \equiv 0 \pmod p)$.

$\Rightarrow mn = 0$ in Z_p where $m \neq 0$, $n \neq 0$.

$(\because 1 < m < p, 1 < n < p.)$

$\therefore m \neq 0, n \neq 0 \in I_p \Rightarrow mn = 0$

$\therefore I_p$ has zero divisors.

which is contradiction.

$\therefore$ p is prime.

Conversely, suppose that p is a prime number.

we are to prove that I_p is a field.

W.K.T I_p is a finite comm. ring with unity p elements.

Now we have to show that I_p has no zero divisors.

Let $m, n \in I_p$ such that $mn = 0$ in I_p.

Then $p \mid mn \Rightarrow p \mid m$ or $p \mid n$ $(\because$ p is prime$)$

$\Rightarrow m = 0$ or $n = 0$ in I_p.

$\therefore mn = 0$ in $I_p \Rightarrow m = 0$ or $n = 0$ in I_p

I_p has no zero divisors.

$\therefore I_p$ is a finite comm. ring without zero divisors.

$\therefore I_p$ is a field.

$\therefore I_p$ has no zero divisors.

$\therefore I_p$ is a finite comm. ring without zero divisors.

$\therefore I_p$ is a field.

Note: $I_2 = \{0, 1\}$, $I_3 = \{0, 1, 2\}$ $I_5 = \{0, 1, 2, 3, 4\}$ etc are all fields (finite).

Def: **Boolean Ring:**

→ Let R be a ring. If for $a \in R$, we have $a^2 = a$ then a is an idempotent element.

→ A ring R is said to be a Boolean ring if for every element of it is an idempotent element.

i.e, In a ring R, if $a^2 = a \ \forall a \in R$ then R is called a Boolean ring.

12M 20 of

Theorem If R is Boolean ring then (i) $a + a = 0 \ \forall a \in R$.

(ii) $a + b = 0 \Rightarrow a = b$ and (iii) R is commutative under $\times^n$.

Proof: Given that R is Boolean ring.

$\forall a \in R \Rightarrow a + a \in R$

Since $a^2 = a \ \forall a \in R$.

we have

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

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

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

$$\Rightarrow (a^2+a^2) + (a^2+a^2) = a+a \quad (\because a^2 = a \ \forall a \in R)$$

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

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

$$\Rightarrow a + a = 0 \quad (\text{By LCL})$$

(ii) For $a, b \in R$, $a + b = 0$

$$\Rightarrow a + b = a + a \quad (\because a + a = 0 \text{ i.e, by (i)})$$

$$\Rightarrow b = a \quad (\text{By LCL})$$

$$\Rightarrow a = b$$

(iii) $a, b \in R \Rightarrow a + b \in R$

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

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

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

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

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

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

$\Rightarrow (a+b)+(ab+ba) = (a+b)+0$

$\Rightarrow ab+ba = 0$ (by LCL)

$\Rightarrow ab = ba$ (by (ii))

Note: The above theorem can be stated as follows.

"every Boolean ring is abelian".

→ If $a \neq 0$ is an idempotent element of an ID then $a=1$.

Soln: Let $(R, +, \cdot)$ be an ID.

$a \neq 0 \in R$ is an idempotent element.

$\therefore a^2 = a$

$\Rightarrow a^2 = a \cdot 1$ ($\because a \cdot 1 = a$)

$\Rightarrow a^2 - a \cdot 1 = 0$

$\Rightarrow a(a-1) = 0$

$\Rightarrow a-1 = 0$ ($\because R$ has no zero divisors & $a \neq 0$)

$\Rightarrow a = 1$

Note: [1]. An ID contains only two idempotent elements 0 & 1.

[2]. The only idempotent elements in a field are 0 & 1.

Nilpotent Element:

Let R be a ring and $a \in R$. If there exists $n \in N$ such that $a^n = 0$ then 'a' is called nilpotent element of R.

Note: 0 is always nilpotent element of ring R.

Theorem An ID has no nilpotent other than zero.

Soln: Let R be an ID and $a \neq 0 \in R$.

we have $a^1 = a \neq 0$, $a^2 = a \cdot a \neq 0$ ($\because$ R has no zero divisors)

Let $a^n \neq 0$ for $n \in N$

then $a^{n+1} = a^n \cdot a \neq 0$ ($\because$ R has no zero divisors)

$\therefore$ By induction $a^n \neq 0$ ~~$\forall n \in N$~~.

$\therefore a \neq 0 \in R$ is not a nilpotent element.

Examples:

(1) For the ring R_2 of all 2×2 matrices over integers.

$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are idempotent.

Since $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$,

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ etc.

and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ are nilpotent elements

since $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(2) In the ring $Z_4 = \{0, 1, 2, 3\}$ of integers mod 4;
0 and 1 are the only idempotent elements and
0 & 2 are the only nilpotent elements.
($\because 2^2 = 0$ in Z_4)

(3) For the ring $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ of integers modulo 10;
0, 1, 5, 6 are the idempotent elements.
and 0 is the only nilpotent element.

(4) If a, b are nilpotent elements in a commutative ring R then $a+b$, $a \cdot b$ are nilpotent elements.

(5) In a ring R, a non-zero idempotent element cannot be nilpotent.

(6) If a, b are nilpotent elements in a non-commutative ring R then a+b, a.b are not nilpotent elements.

Ex: The ring M_2 of all 2×2 matrices over the integers is non-commutative.

where $A=\begin{pmatrix}0&0\\1&0\end{pmatrix}$, $B=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ are nilpotent (since $A^2=B^2=0$)

$A+B=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ is not nilpotent.

Since $(A+B)^2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$

$(A+B)^3=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ so on.

we get $(A+B)^n=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ or $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\forall n\in N$.

and $A\cdot B=\begin{pmatrix}0&0\\0&1\end{pmatrix}$ is not nilpotent.

Since $(AB)^2=\begin{pmatrix}0&0\\0&1\end{pmatrix}$; $(AB)^3=\begin{pmatrix}0&0\\0&1\end{pmatrix}$ and so on.

we get $(AB)^n=\begin{pmatrix}0&0\\0&1\end{pmatrix}$ $\forall n\in N$.

→ Let R be a commutative ring and $a\in R$ if a is nilpotent then ab is nilpotent for each $b\in R$.

Soln: Since a is nilpotent.

$\therefore a^n=0$ for some $n\in N$.

Since R is commutative.

$\therefore (ab)^n=a^n.b^n$ $\forall a,b\in R$.

$=0.b^n$

$=0$

$\therefore$ ab is nilpotent $\forall b\in R$.

→ Let R be ring and $a, b \in R$ if ab is nilpotent then ba is nilpotent.

Sol^n: Since ab is nilpotent.

$\therefore (ab)^n = 0$ for some $n \in N$.

Now consider

$$(ba)^{n+1} = ba.ba.\ldots\ldots ba.ba \quad (n+1 \text{ times})$$
$$= b(ab).(ab)\ldots\ldots(ab)a.$$
$$= b(ab)^n a$$
$$= b(0)a \quad (\because (ab)^n = 0)$$
$$= 0$$

$\therefore ba$ is nilpotent.

Problems:

→ The set of all 2×2 matrices over the ring $Z_2 = \{0,1\}$ of integers modulo 2 is a finite non-commutative ring.

Sol^n: Hint:

the ring S has $2^4 = 16$ elements.

2×2 . 2 mat. i.e. 2

$$\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\0&0\end{pmatrix},$$
$$\begin{pmatrix}0&0\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&1\end{pmatrix}.$$

→ The set $M = \left\{\begin{bmatrix}0&a\\0&b\end{bmatrix} / a,b \in R\right\}$ is a non-commutative ring without unity under matrix $+^n$ & matrix $\times^n$.

Note: $\begin{pmatrix}0&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix}$; $\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&1\end{pmatrix} = \begin{pmatrix}0&1\\0&0\end{pmatrix}$.

$\therefore \begin{pmatrix}0&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} \neq \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&1\end{pmatrix}$.

→ If R is a ring with unity satisfying $(xy)^2 = x^2y^2 \ \forall x,y \in R$ then R is commutative.

Sol^n: we have $(xy)^2 = x^2y^2 \ \forall x,y \in R$. ——— (1)

Replacing y by $y+1 \in R$ in (1), we get

$[x(y+1)]^2 = x^2(y+1)^2$

$\Rightarrow (xy+x)^2 = x^2(y^2+2y+1)$

$\Rightarrow (xy+x)(xy+x) = x^2(y^2+2y+1)$

$\Rightarrow (xy)^2+(xy)x+x(xy)+x^2 = x^2y^2+2x^2y+x^2$ ——— (2)

$\Rightarrow (xy)^2+(xy)x+x(xy)+x^2 = (xy)^2+2x^2y+x^2$

$\Rightarrow (xy)x+x(xy) = 2x^2y$ ($\because$ LCL & RCL in $(R,+)$)

$\Rightarrow xyx+x^2y = 2x^2y$

$\Rightarrow xyx = x^2y \quad \forall x,y \in R$ ——— (3) ($\because$ RCL)

Replacing x by $x+1 \in R$ in (3),

$(x+1)y(x+1) = (x+1)^2y$

$\Rightarrow (x+1)(yx+y) = (x+1)(xy+y)$.

$\Rightarrow xyx+xy+yx+y = x^2y+xy+xy+y$

$\Rightarrow yx = xy \quad \forall x,y \in R$

($\because$ LCL & RCL in $(R,+)$)

$\therefore$ R is a comm. ring.

——

→ Give an example of a non-commutative ring R without unity such that $(xy)^2 = x^2y^2 \ \forall x,y \in R$.

Sol^n: Consider the ring R of 2×2 matrices

$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a,b \in I \right\}$.

Clearly, R is non-commutative.

since $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

$\therefore \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

[Note: the possible unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin R$]

Let $x = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, $y = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in R$

then $xy = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$; $x^2 = \begin{pmatrix} a^2 & ab \\ 0 & 0 \end{pmatrix}$; $y^2 = \begin{pmatrix} c^2 & cd \\ 0 & 0 \end{pmatrix}$

$(xy)^2 = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}\begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a^2c^2 & a^2cd \\ 0 & 0 \end{pmatrix} = x^2y^2$.

→ A ring R is commutative iff $a^2-b^2=(a+b)(a-b)$ $\forall a,b\in R$.

Sol: Let R be commutative.

Then $ab=ba$ $\forall a,b\in R$

R.H.S $(a+b)(a-b) = a(a-b)+b(a-b)$

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

$= a^2-b^2$ $(\because ab=ba)$.

Conversely suppose that

$(a^2-b^2)=(a+b)(a-b)$

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

$\Rightarrow 0 = -ab+ba$ $(\because$ RCL & LCL in $(R,+))$

$\Rightarrow ab=ba$. $\forall a,b\in R$

Hence R is a Commutative ring.

→ The set of all 2×2 matrices over the finite field $Z_3=\{0,1,2\}$ is a finite non-commutative ring of order $3^4=81$, under matrix addition and matrix multiplication.

→ The set of all 3×3 matrices over a finite field is a finite non-commutative ring under matrix $+^n$ and matrix $\times^n$.

(Hint: If a field having n elements then the required ring R has n^9 elements.)

further R is non-commutative.

Since $AB\neq BA$; where $A=\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix}$ $B=\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}$

→ Let $(R,+,\cdot)$ be a ring. Then the system $(R,+,o)$ is also a ring where $x\,o\,y=y\cdot x$ $\forall x,y\in R$.

Note: The ring $(R,+,o)$ is called the opposite ring of R written as R^{op}.

Subrings

Defn: Let R be a ring. S be a non-empty subset of R (i.e, $S \subseteq R$), if S is a ring w.r.t binary operations defined in R then S is called a subring of R.

Note: [1] If $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ then $(S,+)$ is a subgroup of the group $(R,+)$.

Defn: Let $(F,+,\cdot)$ be a field. and $(S,+,\cdot)$ be a subring of F. If $(S,+,\cdot)$ is a field then we say that 'S' is a subfield of F.

(Or)

Let F be a field and S is a non-empty subset of F. If S is field w.r.t binary operations defined in F then S is called a subfield of F.

Note: [1] If $(S,+,\cdot)$ is subfield of $(F,+,\cdot)$ then

a) $(S,+)$ is a subgroup of $(F,+)$.

b) $(S-\{0\},\cdot)$ is a subgroup of $(F-\{0\},\cdot)$

[2] If $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$, then

a) $(S,+)$ is a subgroup of $(R,+)$

b) $(S,\cdot)$ is a subsemigroup of $(R,\cdot)$

and c) Distributive laws hold.

Examples:

→ The set of even integers is a subring of the ring of integers under $+^n$ and $\times^n$.

→ $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ are subrings of the ring of real numbers $(R,+,\cdot)$.

→ Let $(\mathbb{Q},+,\cdot)$ be the ring of rational numbers.
If $S=\{\frac{a}{2} / a\in\mathbb{Z}\}$ then S is a non-empty subset of $\mathbb{Q}$ and $(S,+)$ is a subgroup of $(\mathbb{Q},+)$.

but for $\frac{1}{2}\in S$
we have
$\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}\notin S$.
$\therefore x^n$ is not a b-o on S.
$\therefore (S,+,\cdot)$ is not a Subring of $(\mathbb{Q},+,\cdot)$

→ Let $(R,+,\cdot)$ be a ring. and $0\in R$ then $S=\{0\}$. is a non-empty subset of R and $(S,+,\cdot)$ is itself a ring.
$\therefore (S,+,\cdot)$ is a Subring of R.
∴ If R is any ring then $\{0\}$ and R itself are always subrings of R.
These are known as improper subrings of R.
Other rings, if any, of R called proper subrings of R.

Theorem. Let S be a non-empty subset of a ring R. Then S is a subring of R iff $\forall a,b\in S \Rightarrow a-b\in S$ and $ab\in S$.

Proof: N.C :-
Let S be a subring of R.
By the defn 'S' is a ring w.r.t the b-o's of R.
(1) $\forall a,b\in S \Rightarrow a\in S, -b\in S$ (inverse prop. of S)
$\Rightarrow a+(-b)\in S$ (by closure prop)
$\Rightarrow a-b\in S$.
(2) $\forall a,b\in S \Rightarrow a\cdot b\in S$ (by closure prop. of S)
$\therefore \forall a,b\in S \Rightarrow a-b\in S$ & $ab\in S$.

S.C :- Let $S\subseteq R$.
$\forall a,b\in S \Rightarrow a-b\in S$ & $ab\in S$ ——(2).
——(1)

(I). (i) $a, a \in S \subseteq R$.

$\Rightarrow a-a \in S \subseteq R$ (by ①)

$\Rightarrow 0 \in S \subseteq R$.

$\therefore \forall a \in S \subseteq R \ \exists\ 0 \in S \subseteq R$ such that $0+a=a+0=a$.

$\therefore 0$ is the identity element in S.

$\therefore$ Identity prop. is satisfied.

(ii) $0 \in S, a \in S \Rightarrow 0-a \in S$ (hyp ①)

$\Rightarrow -a \in S$

$\therefore$ For each $a \in S, \exists -a \in S$ such that $a+(-a)=(-a)+a=0$ (by inverse of R)

$\therefore$ Inverse prop is satisfied in S.

Inverse of a is $-a$ in S.

(iii) $\forall b \in S \Rightarrow -b \in S$

$\therefore \forall a, -b \in S \Rightarrow a-(-b) \in S$ (hyp)

$\Rightarrow a+b \in S$

$\therefore a, b \in S \Rightarrow a+b \in S$.

$\therefore$ closure prop. in S is satisfied.

(iv) $\forall a, b, c \in S \subseteq R$.

$\Rightarrow a+(b+c)=(a+b)+c$ (by asso. prop. of R)

$\therefore$ Asso. property in S is satisfied.

(v) $a, b \in S \subseteq R \Rightarrow a+b=b+a$ (by comm. prop. of R)

$\therefore$ Comm. prop in S is satisfied.

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

(II) (i) $\forall a, b \in S \Rightarrow ab \in S$ (by hyp (2))

Closure prop. in S is satisfied.

(ii) $\forall\ a, b, c \in S \subseteq R \Rightarrow (ab)c=a(bc)$ (by asso. prop. of R)

$\therefore x^n$ is asso. in S.

$\therefore (S,\cdot)$ is a semigroup.

(III) $a, b, c \in S \subseteq R \Rightarrow a\cdot(b+c)=a\cdot b+a\cdot c$ & $(b+c)\cdot a=ba+ca$ } x^n is distributive w.r.t. $+^n$ in R

$\therefore$ Distributive laws are satisfied.

$\therefore (S,+,\cdot)$ is a ring.

$(S,+,\cdot)$ is a subring of $(R,+,\cdot)$.

Note: Let R be a ring and S is a non-empty subset of R.

S is a subring of R iff (i) $S+(-S)=S$
(ii) $SS \subseteq S$.

Theorem → Let F be a field. Let K be a non-empty subset of F. Then K is a subfield of F iff

$$\forall a,b \in K \Rightarrow a-b \in K \ \& \ ab^{-1} \in K.$$

Proof

N.C:

Let K be a subfield of F, Then by defn, K is a field w.r.t. b-o's defined in F.

(i) $\forall a,b \in K \Rightarrow a \in K, -b \in K$ (by inverse of K)
$\Rightarrow a+(-b) \in K$ (by Closure of K)
$\Rightarrow a-b \in K$

(ii) $b \neq 0 \in K \Rightarrow b^{-1}$ exists in K. ($\because$ $\times^{ve}$ inverse in K)
$\therefore \forall a \in K, b^{-1} \in K \Rightarrow ab^{-1} \in K$ (By Closure prop. of K)

S.C:

$K \subseteq F$.

Let $a,b \in K \Rightarrow a-b \in K$. & $ab^{-1} \in K$.

(I). To show $(K,+)$ is an abelian group.

(II) (i) $a, a \in K \subseteq F \Rightarrow a\bar{a}^{-1} \in K$ (by ②)

$\Rightarrow e \in K$. (by inverse prop. of F)

$\therefore \forall a \in K \subseteq F$, $\exists e \in K \subseteq F$ such that $a.e = e.a = a$. (by identity prop. in F)

$\therefore$ Identity prop. in K is satisfied.

and e is the identity element in K.

(ii) $e \in K \subseteq F$, $b \neq 0 \in K \subseteq F$.

$\Rightarrow eb^{-1} \in K \subseteq F$ (by hypo)

$\Rightarrow b^{-1} \in K \subseteq F$

$\therefore b \neq 0 \in K \Rightarrow b^{-1} \in K$ such that $bb^{-1} = b^{-1}b = e$ (by inverse of F)

$\therefore$ inverse of b is b^{-1} in K.

$\therefore$ Inverse prop. is satisfied.

(iii) $b \neq 0 \in K \Rightarrow b^{-1} \in K$

$\therefore \forall a, b^{-1} \in K \subseteq F \Rightarrow a(b^{-1})^{-1} \in K$ (by ①)

$\Rightarrow ab \in K$

$\therefore$ K is closed w.r.t x^n.

(iv) $\forall a, b, c \in K \subseteq F \Rightarrow (ab)c = a(bc)$ (by asso prop in F)

$\therefore$ K is asso. under x^n.

(v) $\forall a, b \in K \subseteq F \Rightarrow ab = ba$ (by comm. of F)

$\therefore$ comm. in K is satisfied w.r.t x^n.

(vi) $\forall a, b, c \in K \subseteq F \Rightarrow a.(b+c) = ab + ac$ & $(b+c)a = ba + ca$ } x^n is distributive w.r.t $+^n$ in F

$\therefore$ Distributive laws are satisfied.

$\therefore (K,+,\cdot)$ is a field.

$\therefore (K,+,\cdot)$ is a subfield of $(F,+,\cdot)$

Examples:

→ P.T $S_1 = \{\bar{0}, \bar{3}\}$, $S_2 = \{\bar{0}, \bar{2}, \bar{4}\}$ are subrings of $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ w.r.t $+^n$ & $\times^n$ of residue classes.

Soln: Since $(Z_6,+,\cdot)$ is a ring.

from the additive inverse of Z_6: $-\bar{0}=\bar{0}$, $-\bar{2}=\bar{4}$, $-\bar{3}=\bar{3}$, $-\bar{2}=\bar{4}$, $-\bar{1}=\bar{5}$.

and $S_1 = \{\bar{0}, \bar{3}\} \subseteq Z_6$.

+	$\bar{0}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	0

·	$\bar{0}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{3}$	$\bar{0}$	$\bar{3}$

from the above tables

$\forall \bar{a}, \bar{b} \in S_1 \Rightarrow \bar{a}-\bar{b} \in S_1$

since $\bar{0}, \bar{3} \in S_1$

$\Rightarrow \bar{0}-\bar{3} = \overline{0-3}$

$= -\bar{3} \in S_1$

$= \bar{3} \in S_1$ etc.

and $\bar{a}, \bar{b} \Rightarrow \bar{a}\bar{b} \in S_1$

since $\bar{0}, \bar{3} \in S_1 \Rightarrow \bar{0}\cdot\bar{3} = \bar{0} \in S_1$ etc

$\therefore S_1$ is a subring of Z_6.

NOW $S_2 = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq Z_6$

+	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

·	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

From the above tables

$\forall \bar{a}, \bar{b} \in S_2 \Rightarrow \bar{a}-\bar{b} \in S_2$

since $\bar{0}, \bar{2} \Rightarrow \bar{0}-\bar{2} = \overline{0-2}$

$= -\bar{2}$

$= \bar{4} \in S_2$ etc.

$\forall \bar{a}, \bar{b} \in S_2 \Rightarrow \bar{a}\cdot\bar{b} \in S_2$

since $\bar{0}, \bar{2} \in S_2 \Rightarrow \bar{0}\cdot\bar{2} = \bar{0} \in S_2$.

$\therefore$ S_2 is a subring of Z_6.

Now we see that $S_1 \cap S_2 = \{\bar{0}\}$ is a trivial subring of Z_6.

But $S_1 \cup S_2 = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$ is not a subring of Z_6 because $\bar{2}, \bar{3} \in S_1 \cup S_2 \Rightarrow \bar{2}+\bar{3} = \bar{5} \notin S_1 \cup S_2$

- **Theorem** The intersection of two subrings of a ring R is a subring of R.

Proof: Let S_1 & S_2 are two subrings of a ring R.

Let $S = S_1 \cap S_2$

$a, b \in S \Rightarrow a, b \in S_1 \cap S_2$

$\Rightarrow a, b \in S_1$ and $a, b \in S_2$

$\Rightarrow a-b \in S_1$ and $a-b \in S_2$ ($\because$ S_1 & S_2 are two subrings of R)
$ab \in S_1$ $ab \in S_2$

$\Rightarrow a-b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$

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

$\therefore$ $S_1 \cap S_2$ is a subring of R.

Theorem Intersection of arbitrary number of subrings a subring of R.

proof: Let $S_1, S_2, \ldots\ldots S_n$ are subrings of R.

Let $S = S_1 \cap S_2 \cap \ldots\ldots \cap S_n \ldots\ldots$

$= \bigcap_{i \in N} S_i$

Let $a, b \in S \Rightarrow a, b \in S_1 \cap S_2 \cap \ldots\ldots$

$\Rightarrow a, b \in \bigcap_{i \in N} S_i$

$\Rightarrow a, b \in S_i \quad \forall\, i \in N$

$\Rightarrow a-b \in S_i$ and $ab \in S_i$ $\forall i \in N$.
($\because S_i$ is a subring).

$\Rightarrow a-b \in \bigcap_{i\in N} S_i$ & $ab \in \bigcap_{i\in N} S_i$.

$\Rightarrow a-b \in S$ & $ab \in S$

$\because S_1 \cap S_2 \cap \dots \cap S_n \dots$ is a subring of R.

$\therefore$ Intersection of arbitrary no. of subrings is a subring.

Theorem: Union of two subrings of R need not be a subring of R.

Soln:

Let $R = I$ (if the ring of integers)

Let $S_1 = \{2n / n \in I\}$

$= \{\dots -6, -4, -2, 0, 2, 4, 6, \dots\}$

$S_2 = \{3n / n \in I\}$

$= \{\dots -9, -6, -3, 0, 3, 6, 9, \dots\}$ be two subrings of R.

$2 \in S_1,\ 3 \in S_2 \Rightarrow 2, 3 \in S_1 \cup S_2$

$\Rightarrow 2+3 = 5 \notin S_1 \cup S_2$

$\therefore S_1 \cup S_2$ is not closed under $+^n$.

$\therefore S_1 \cup S_2$ is not a subring of R.

Theorem: If S_1 and S_2 are two subrings of a ring R then $S_1 \cup S_2$ is a subring of R iff $S_1 \subset S_2$ or $S_2 \subset S_1$

Proof: Let $S_1 \cup S_2$ be a subring of R.

Now we prove that $S_1 \subset S_2$ or $S_2 \subset S_1$.

If possible suppose that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$

Since $S_1 \not\subset S_2$.

Let $a \in S_1$ but $a \notin S_2$.

Since $S_2 \not\subset S_1$

Let $b \in S_2$ but $b \notin S_1$

NOW we have

$a \in S_1, b \in S_2 \Rightarrow a, b \in S_1 \cup S_2$

$\Rightarrow a+b \in S_1 \cup S_2$ ($\because S_1 \cup S_2$ is ring)

$\Rightarrow a+b \in S_1$ or $a+b \in S_2$

NOW we have

$a \in S_1, a+b \in S_1$

$\Rightarrow (a+b)-a \in S_1$ ($\because S_1$ is subring of R)

$\Rightarrow b \in S_1$

which is contradiction.

NOW we have

$b \in S_2, a+b \in S_2$

$\Rightarrow (a+b)-b \in S_2$ ($\because S_2$ is subring of R)

$\Rightarrow a \in S_2$

which is contradiction.

$\therefore$ our assumption that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$ is wrong.

$\therefore S_1 \subset S_2$ or $S_2 \subset S_1$

Conversely suppose that $S_1 \subset S_2$ or $S_2 \subset S_1$ prove that $S_1 \cup S_2$ is a subring

Since $S_1 \subset S_2 \Rightarrow S_1 \cup S_2 = S_2$

$\therefore S_1 \cup S_2$ is a subring of R.

($\because S_2$ is subring of R)

Since $S_2 \subset S_1 \Rightarrow S_1 \cup S_2 = S_1$

$\therefore S_1 \cup S_2$ is a subring of R.

($\because S_1$ is subring of R)

→ The centre of a ring R is a subring of R.

Sol^{n}: Let Z(R) be the centre of Ring R then

$Z(R) = \{ a \in R / xa = ax \ \forall x \in R \}$

Clearly Z(R) is non-empty.

Since $0x = x0 \ \forall x \in R$

$\Rightarrow 0 \in Z(R)$

Let $a, b \in Z(R)$

where $xa = ax$; $xb = bx$ $\forall x \in R$ ——①

Now $(a-b)x = ax - bx$

$= xa - xb$

$= x(a-b)$

$\therefore (a-b)x = x(a-b) \ \forall x \in R$

$\therefore a-b \in Z(R)$

Now $(ab)x = a(bx)$

$= a(xb)$ (by ①)

$= (ax)b$

$= (xa)b$ (by ①)

$= x(ab)$

$\therefore (ab)x = x(ab) \ \forall x \in R.$

$\therefore ab \in Z(R)$

$\therefore$ Z(R) is a subring of R.

→ The centre of a division ring is a field.

Sol^{n}: Let Z(R) be the centre of the division ring R.

then $Z(R) = \{ a \in R / xa = ax \ \forall x \in R \}$ ——①

Now we shall show that Z(R) is a field

W.K.T Z(R) is a subring of R.

$\therefore$ Z(R) is a ring

Let $a, b \in Z(R)$

then $ax = xa$, $\forall x \in R$ & $bx = xb \ \forall x \in R$.

In particular $ab = ba \ \forall a, b \in Z(R)$

$\therefore$ Z(R) is a commutative ring.

Since R is division ring,

$\therefore 1 \in R$ and $1 \cdot x = x \cdot 1 = x \quad \forall x \in R$

$\therefore 1 \in Z(R)$

$\therefore Z(R)$ has unity.

Finally we show that each non-zero element of $Z(R)$ has a multiplicative inverse in $Z(R)$.

Let $a \neq 0 \in Z(R)$ then $a \neq 0 \in R$

$\Rightarrow a^{-1} \in R$ exists

($\because$ R is a division ring)

Let $x \neq 0 \in R$ then $x^{-1} \in R$ exists.

we have $xa^{-1} = (ax^{-1})^{-1}$

$= (x^{-1}a)^{-1}$ ($\because a \in Z(R) \Rightarrow ax^{-1} = x^{-1}a$)

$= a^{-1}x$

$\therefore xa^{-1} = a^{-1}x \quad \forall x \neq 0 \in R.$

and $0a^{-1} = a^{-1}0$

$\therefore a^{-1}x = a^{-1}x \quad \forall x \in R.$

$\therefore a^{-1} \in Z(R) \quad \forall a \neq 0 \in Z(R)$

$\therefore Z(R)$ is a field.

→ Show by means of an example that a subring of a ring with unity may fail to be a ring with unity.

Ex: The ring I of integers is a ring with unity. But the set E of even integers is a subring of I without unity.

→ The subring of a non-commutative ring may or may not commutative.

Sol^n: The ring M_2 of 2×2 matrices over integers is non-commutative.

Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$; $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

$\therefore \begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} \neq \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}$

The set $S=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix} / a\in I\right\}$ is a subring of M_2 which is commutative.

Since $\begin{pmatrix}a&0\\0&0\end{pmatrix}\begin{pmatrix}b&0\\0&0\end{pmatrix} = \begin{pmatrix}ab&0\\0&0\end{pmatrix}$

$= \begin{pmatrix}b&0\\0&0\end{pmatrix}\begin{pmatrix}a&0\\0&0\end{pmatrix}$

→ (i) Ring which is not commutative but has a subring which is commutative.

(ii) Ring which has no unity but subring which has unity.

Soln (ii) $R=\left\{\begin{bmatrix}a&b\\0&0\end{bmatrix} / a,b\in I\right\}$ is a ring which has no unity.

(Note: the possible unity $\begin{pmatrix}1&0\\0&1\end{pmatrix}\notin R$)

It can be verified that none of $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $\begin{pmatrix}0&1\\0&0\end{pmatrix}$, $\begin{pmatrix}1&1\\0&0\end{pmatrix}$ unity of R.

However, $S=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix} / a\in I\right\}$ is a subring of R, which has $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ as the unity of S.

→ Show that $S=\{0,2,4,6,8\}$ is a subring of Z_{10} with unity different from that Z_{10}, the ring of integers mod 10.

Sol^n

$+_{10}$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

$\times_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

From the above tables:

$\forall a,b\in S \Rightarrow a-b\in S$ and $a\times b\in S$.

Since $0, 4 \in S \Rightarrow 0-4 = -4 = 6 \in S$ etc.

and $0 \times 4 = 0 \in S$ etc.

$\therefore$ S is a subring of Z_{10} where the unity '6'.

→ The sum of two subrings of a ring need not be a subring.

Eg:- Let $S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z \right\}$; $T = \left\{ \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} / c \in Z \right\}$ be two subrings of ring M_2 of 2×2 matrices over integers.

Now the sum of S & T is $S+T = \left\{ \begin{pmatrix} a & c \\ b & 0 \end{pmatrix} / a, b, c \in Z \right\}$

Let $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} \in S+T$

but $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \notin S+T$

$\therefore$ S+T is not a subring of M_2.

→ Let R be the ring of 2×2 matrices over reals then $S = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} / x \in \mathbb{R} \right\}$ is a subring of R and has a unity different from the unity of R.

Soln: Let $A = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$, $B = \begin{pmatrix} y & y \\ y & y \end{pmatrix} \in S$; $x, y \in \mathbb{R}$

then $A-B = \begin{pmatrix} x-y & x-y \\ x-y & x-y \end{pmatrix} \in S$ $(\because x, y \in \mathbb{R} \Rightarrow x-y \in \mathbb{R})$

and $A \cdot B = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in S$ $(\because xy \in \mathbb{R})$

$\therefore$ S is a subring of R.

Here the unity of S is $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

and the unity of R is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Problems:

→ Show that the set $S=\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z\right\}$ is a subring of the ring M_2 of 2×2 matrices over integers.

Sol^n: Clearly S is a non-empty subset of M_2 $(\because \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S)$

Let $A=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \in S$ and $B=\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \in S$ where $a, b, c, d \in Z$

Then $A-B=\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in S$ $(\because a-c, b-d \in Z)$

and $A\cdot B=\begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \in S$ $(\because ac, bc \in Z)$

$\therefore S$ is a subring of the ring of 2×2 matrices over integers.

H.W → Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2×2 matrices with integral elements.

→ Let R be the ring of integers. Let m be any fixed integer and let 'S' be any subset of R such that

$S=\{\ldots\ldots -3m, -2m, -m, 0, m, 2m, \ldots\ldots\}$.

Then S is a subring of R.

Sol^n: Let $S=\{rm / r \in I, m \text{ is fixed integer}\}$.

Clearly S is non-empty subset of R. $(\because \{0\} \subseteq R)$

Let $a=rm$, $b=sm$ be two elements of S, $r, s \in I$.

we have

$$a-b = rm-sm = (r-s)m \in S \quad (\because r-s \in I)$$

and $$ab = (rm)(sm) = (rsm)m \in S \quad (\because rsm \in I)$$

$\therefore S$ is a subring of R.

→ If 'a' is a fixed element of a ring R, show that $I_a=\{x \in R / ax=0\}$ is a subring of R.

Sol^n: Since $a0 = 0$

$\therefore 0 \in I_a$

$\Rightarrow I_a$ is a non-empty subset of R

Let $x, y \in I_a$ then $ax = 0$ & $ay = 0$

Now $a(x-y) = ax - ay$
$= 0 - 0$
$= 0$

$\therefore x - y \in I_a$

Again $a(xy) = (ax)y$
$= 0y$
$= 0$

$\therefore xy \in I_a$

$\therefore I_a$ is a subring of R.

Characteristic of a ring:

→ A ring R is said to be of finite characteristic, if there exists a +ve integer 'n' such that $na = 0$ for all $a \in R$.

→ If a ring R is of finite characteristic, then the characteristic of R is defined as the smallest +ve integer 'p' such that $pa = 0$ $\forall a \in R$.
we write it as $\text{Char } R = p$.

→ A ring R is said to be of characteristic zero or infinite if there exists no +ve integer 'n' such that $na = 0$ $\forall a \in R$.

Examples

→ $\text{Char } \mathbb{Z} = 0$, $\text{Char } \mathbb{Q} = 0$, $\text{Char } \mathbb{R} = 0$

→ $\text{Char } \mathbb{Z}_2 = 2$ where $\mathbb{Z}_2 = \{0, 1\}$

Since $1 \times_2 0 = 0$ $1 \times_2 1 = 1$
$2 \times_2 0 = 0$ $2 \times_2 1 = 0$
$3 \times_2 1 = 1$
$4 \times_2 1 = 0$
⋮

Here 2 is the smallest +ve integer such that
$2 \times_2 0 = 0$ & $2 \times_2 1 = 0$.

→ Char $Z_3 = 3$, where $Z_3 = \{0, 1, 2\}$.

In general Char $Z_n = n$.
where $Z_n = \{0, 1, 2, 3, \ldots\ldots (n-1)\}$
is the ring of integers modulo 'n'.

Theorem If R is a ring with unity element, then R has Characteristic $p > 0$ iff p is the least +ve integer such that $p.1 = 0$.

proof: Let the Char. of the ring $R = p$. $(p > 0)$.

By defn $pa = 0$ $\forall a \in R$
where p is the least +ve integer.

In particular, $p1 = 0$

Conversely Suppose that p is the least +ve integer such that $p1 = 0$

Now for any $a \in R$, we have

$$pa = a + a + \ldots\ldots + a \ (p \text{ times})$$
$$= a(1 + 1 + \ldots\ldots + 1 \ (p \text{ times}))$$
$$= a(p1)$$
$$= a(0) \qquad (\because p1 = 0 \text{ where } p \text{ is the least +ve integer})$$

$\therefore pa = 0$ $\forall a \in R$
where p is the least +ve integer.

$\therefore$ Char. of the ring $R = p$.

Theorem If any element of a ring R is of order zero when regarded as an element of $(R, +)$ group then Characteristic of R is zero.

proof: Let $a \in R$
when 'a' is considered as an element of the group $(R, +)$.

Let $O(a) = 0$ i.e, order of $a = 0$.

By the defn of the order of an element of a group there exists no +ve integer 'n' such that $na = 0$

$\therefore$ Char. of $R = 0$

Theorem The Characteristic of a ring with unit element is the order of the unit element regarded as a member of the additive group.

proof:

Let $(R, +, \cdot)$ be a ring.

So that $(R, +)$ is its additive group.

Case(i): Let $O(1) = 0$ when the unit element 1 is regarded as an element of $(R, +)$

By the defn of order of an element in a group, there exists no +ve integer 'n' such that $n \cdot 1 = 0$

$\therefore$ There exists no +ve integer 'n' such that

$na = 0 \ \forall a \in R$.

$(\because ka = a(k1))$

$\therefore$ Char. of $R = 0$

Case(ii): Let $O(1) = p \ (\neq 0)$ when the unit element 1 is regarded as an element of $(R, +)$.

By the defn of order of an element in a group, 'p' is the least +ve integer such that $p \cdot (1) = 0$.

Now $m \in N$ (or I^+)

$m < p \Rightarrow m(1) \neq 0$

$\forall a \in R$, $pa = a + a + \cdots + a$ (p times)

$= a(1 + 1 + \cdots + 1)$

$= a(p \cdot 1)$

$= a(0)$

$= 0$

Further $m \in N$, $m < p \Rightarrow ma \neq 0 \ \forall a \in R$.

$\therefore$ p is the least +ve integer such that $pa = 0 \ \forall a \in R$.

$\therefore$ Char. of $R = p$.

Theorem → The Characteristic of an integral domain is either a prime or zero.

proof: Let $(R,+,\cdot)$ be an ID.

If Char. of $R=0$ then there is nothing to prove.

Let Char $R=p$ $(p\neq 0)$. then 'p' is the least +ve integer such that $pa=0 \ \forall\, a\in R$. ——— (1)

Now we prove that 'p' is prime.

If possible suppose that p is not prime then

$p=mn$; $1<m,n<p$.

(1) $\equiv$ $\forall a\in R$, $pa=0$

$\Rightarrow (mn)a=0$

$\Rightarrow (mn)ab=0b$, $b\in R$

$\Rightarrow ab+ab+\cdots+ab$ (mn times) $=0$ $\forall a,b\in R$.

$\Rightarrow (a+a+\cdots+a)(b+b+\cdots+b)=0$ (m times, n times) $\forall a,b\in R$

$\Rightarrow (ma)(nb)=0$ $\forall a,b\in R$. ——— (2)

Since R is an ID.

$\therefore$ R is without zero divisors

$\therefore$ (1) $\equiv$ either $ma=0$ $\forall a\in R$ or $nb=0$ $\forall b\in R$

where $1<m<p$, $1<n<p$.

$\therefore$ the above two statements contradict the fact that 'p' is the least +ve integer such that $pa=0$ $\forall a\in R$.

$\therefore$ p must be a prime number.

Theorem → The Characteristic of a field is either zero or a prime number.

proof: Since every field is an ID.

by the above theorem, the Characteristic of a field is either zero or prime.

(where we must provide the above theorem proof).

Theorem The characteristic of a division ring is either zero or prime.

proof: (The division ring has no zero divisors, with this help we can easily prove, the above theorem, total proof is applicable)

Problems:

→ If R is a non-zero ring so that $a^2=a \ \forall a \in R$ prove that Characteristic of $R=2$

Soln: Since $a^2=a \ \forall a \in R$

we have $(a+a)^2 = a+a$

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

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

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

$\Rightarrow (a+a)+(a+a) = a+a. \quad (\because a^2=a)$

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

$\Rightarrow a+a=0 \quad (\because$ LCL in $(R,+,\cdot)$ i.e., $(R,+)$

$\Rightarrow 2a=0$

$\therefore$ for every $a \in R$ we have $2a=0$

further $a \neq 0$, $1a=a \neq 0$ i.e., $1a \neq 0$

$\therefore$ 2 is the least +ve integer such that $2a=0 \ \forall a \in R$.

$\therefore$ Char $R=2$.

Note: The Char. of a Boolean ring $=2$.

→ If the characteristic of a ring R is '2' and the elements a, b of the ring commute. Prove that $(a+b)^2 = a^2+b^2 = (a-b)^2$.

Soln: Since the Char of $R=2$.

$\therefore 2x=0 \ \forall x \in R$

$a, b \in R$ commute $\Rightarrow ab = ba$.

Now we have

$$(a+b)^2 = (a+b)(a+b)$$
$$= a(a+b) + b(a+b)$$
$$= (a^2+ab) + (ba+b^2)$$
$$= a^2 + ab + ba + b^2$$
$$= a^2 + ab + ab + b^2 \quad (\because ab = ba)$$
$$= a^2 + 2ab + b^2 \quad \text{---} (1)$$

Since for all $a, b \in R \Rightarrow ab \in R$

$$\Rightarrow 2(ab) = 0 \quad (\because 2x = 0 \ \forall x \in R)$$

$\therefore (1) \Rightarrow (a+b)^2 = a^2 + 0 + b^2$

$$= a^2 + b^2$$

Similarly we can prove that $(a-b)^2 = a^2 + b^2$

→ If F is a field of characteristic p, p is a prime. then $(a+b)^p = a^p + b^p \ \forall a, b \in F$

Soln: Since F is a field,

Char. $F = p$; p is a prime.

$\therefore px = 0 \ \forall x \in F$. ---(1) where p is the least +ve integer

Now we have

$$(a+b)^p = a^p + pa^{p-1}b + \frac{1}{2!}p(p-1)a^{p-2}b^2 + \cdots + pab^{p-1} + b^p$$
$$= a^p + (pb)a^{p-1} + \frac{1}{2!}(p-1)a^{p-2}b(pb) + \cdots \cdots + (pa)b^{p-1} + b^p.$$
$$= a^p + b^p \quad (\text{by } (1))$$

2000 → Prove that order of a finite field F is p^n, for some prime p and some +ve integer n.

Soln: Given that F is a field. (finite)

Now we prove that Char $F \neq 0$

If possible let Char $F = 0$

$\therefore$ By def $\exists$ no +ve integer n such that

$na = 0 \ \forall a \neq 0 \in F$

i.e., $na \neq 0 \ \forall a \neq 0 \in F$ & $\forall n \in N$. ---(1)

It follows that $a, 2a, 3a, \ldots\ldots$ belong to F.

Since F is finite
we must have $ia = ja$ for some +ve integers. i & j; $i > j$

$\Rightarrow (i-j)a = 0$
$\Rightarrow a = 0$ $(\because i-j > 0)$
which is contradiction.

$\therefore$ Char $F \neq 0$.

W.K.T the characteristic of a field F is either zero or prime.

Since Char $F \neq 0$
$\therefore$ Char $F = p$ where p is prime number.

Here p is the smallest +ve integer such that $pa = 0$ $\forall a \in F$.

$\Rightarrow O(a) = p$; treating $(F, +)$ as a group

Since $(F, +)$ is a finite group.

$\therefore$ By Lagrange's theorem $O(a)$ divides $O(F)$.
i.e, p divides $O(F)$; where p is prime.

$\therefore O(F) = p^n$ for some $n \in \mathbb{N}$.

Note: If R is finite (non-zero) integral domain then $O(R) = p^n$ where p is prime number and n is +ve integer.

⟶ If F is a finite field, its Characteristic must be a prime number 'p' and F contains p^n elements for some integer 'n'. Further P.T. if $a \in F$ then $a^{p^n} = a$.

Sol^n: W.K.T $O(F) = p^n$
Since the non-zero elements of F (which are $p^n - 1$ in number) form a x^{ve} group.

$\therefore$ By Lagrange's theorem

$a \in F \Rightarrow a^{p^n - 1} = e$ (multiplicative identity of F)
$a \neq 0$

Hence $a \cdot a^{p^n - 1} = ae$
$\Rightarrow a^{p^n} = a$; $a \in F$.

If G is a finite group and $a \in G$ then $O(a) \mid O(G)$ i.e.