Ring (Notes)

by

Prof. M. Dabeer Mughal

Federal Directorate of Education

Islamabad, PAKISTAN

Partial Contents

1. Rings, commutative ring, ring with unity (identity), examples **1**
2. Consequences from the definition **3**
3. Unit element of ring **4**
4. Division ring or skew field, field, zero divisor **5**
5. Integral domain **7**
6. Characteristic of ring, Boolean ring **8**
7. Sub-ring and related theorem **9**
8. Centre of ring and related theorem **11**
9. Ring homomorphism **16**
10. Isomorphism, kernel of ϕ and related theorems **17**
11. Ideal, left ideal **20**
12. Right ideal, two sided ideal, examples and theorems **21**
13. Principal ideal, principal ideal ring and related theorem **28**
14. Quotient ring and related theorem **37**
15. Ist fundamental theorem **42**
16. Maximal ideal and related theorem **44**
17. Prime ideal and related theorem **49**
18. The field of quotients of an integral domain **52**
19. Prime field **63**

Dated: September 15, 2010

Ring:-

A nonempty set R is called a ring if the binary operations addition "+" and multiplication "." are defined in R and

(i) R is an abelian Group under multiplication.
(ii) R is semi Group under multiplication.
(iii) Both left and right distributive laws hold in it; i.e $\forall\, a, b, c \in R$

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

Commutative Ring:-

If R is a ring and Commutative law w.r.t multiplication hold in it then R is called commutative ring.

OR

R is called commutive ring if $\forall\, a, b \in R$

$$ab = ba$$

Ring with unity (identity)

If R is a ring and it contain the multiplicative identity "1" then R is called ring with unity.

Examples:-

(1) The set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$ is commutative ring with unity. (Ring of integers)

(2) The Set of all even numbers $\{0, \pm 2, \pm 4, \pm 6, ---\}$ is a Commutative ring without unity.

(3) The set of rational numbers $\mathbb{Q}$; Set of real numbers $\mathbb{R}$, Set of Complex numbers $\mathbb{C}$ are all examples of Commutative ring with unity.

(4) The Set $M_{n\times n}(\mathbb{R})$ of all $n\times n$ matrices over the field of real numbers is non-Commutative ring with unity.

(5) The Set $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ is a Commutative ring with unity.
In general $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ---, \overline{(n-1)}\}$ is a Commutative ring with unity.

(6) The Set $R = \{a_0 + a_1 i + a_2 j + a_3 K\}$ wher a_i are real numbers and

$i^2 = j^2 = K^2 = ijK = -1$ and

$ij = -ji = K$ etc

R is a non-Commutative ring with unity; this ring is Called the ring of real quatorineis.

(7) Let X be a non-empty set and let $P(X)$ be the Set of all subsets of X. Let addition and multiplication in $P(X)$ is defined as ; $\forall\ A, B \in P(X)$

$A+B = (A-B) \cup (B-A)$

$AB = A \cap B$ then X is Commutative ring with unity; where X is the identity element:

$\because AX = A \cap X = A \quad \forall A \in P(X)$

Consequences from the definition

C_1:-
If "0" is the additive identity of R then
$$a\cdot 0 = 0\cdot a = 0 \quad \forall\ a\in R.$$

Proof:-

$a\cdot 0 = a\cdot(0+0)$ $\quad \because 0$ is additive identity.
$a\cdot 0 = a\cdot 0 + a\cdot 0$ $\quad$ Left distributive law.
$\Rightarrow\ a\cdot 0 + 0 = a\cdot 0 + a\cdot 0$ $\quad \because 0$ is additive identity.
$\Rightarrow\ 0 = a\cdot 0$ $\quad$ Cancellation law holds in group.
$\Rightarrow\ a\cdot 0 = 0$

Now

$0\cdot a = (0+0)a$ $\quad \because 0$ is additive identity.
$0\cdot a = 0a + 0a$ $\quad$ Right distributive law.
$0\cdot a + 0 = 0\cdot a + 0\cdot a$ $\quad$ 0 is additive identity.
$0 = 0\cdot a$ $\quad$ Cancellation law holds in group.
$\Rightarrow\ 0\cdot a = 0$

thus $a\cdot 0 = 0\cdot a = 0$

C_2:-
$$a(-b) = (-a)b = -(ab) \quad \forall\ a, b\in R.$$

Proof:-

$\because\ a\cdot 0 = 0$
$\Rightarrow\ a\cdot(b+(-b)) = 0$
$\Rightarrow\ a\cdot b + a\cdot(-b) = 0$ $\quad$ (Left distributive law)

This shows that ab is additive inverse of $a(-b)$
i.e $a(-b) = -ab$

Now

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

Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

$\Rightarrow \quad ab + (-a)b = 0$ (Right distributive law)

this shows that ab is the additive inverse of $(-a)b$; i.e $\quad (-a)b = -(ab)$

thus $\quad a(-b) = (-a)b = -(ab)$

C_3:- $\quad (-a)(-b) = ab$

Proof:-

$$\begin{aligned} \because \quad (-a)(-b) &= -(a(-b)) && \because (-a)b = -(ab) \\ &= -(-(ab)) && \because a(-b) = -(ab) \\ &= ab \end{aligned}$$

In particular

$(-1)a = -a \quad$ (if $1 \in R$)

$$\begin{aligned} \because \quad (-1)a + a &= (-1)a + 1\cdot a \\ (-1)a + a &= (-1+1)a && \text{right distributive law.} \\ (-1)a + a &= 0\cdot a \\ (-1)a + a &= 0 \end{aligned}$$

This shows that a is additive inverse of $(-1)a$

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

Unit element of Ring:-

A nonzero element of R is called a unit if it has multiplicative inverse in R.

Note:-

Unity (multiplicative identity) is also a unit but every unit need not to be unity.

Division Ring OR Skew Field:-

A ring R is called division ring if all the non-zero elements of R has its multiplicative inverse in R; i.e each non-zero elements of R is a unit.

Field:-

A ring R is called a field if all the non-zero elements of R form an abelian group under multiplication.

OR.

A Commutative division ring is called a field.

Zero divisor:-

If R is a Commutative ring then a non-zero element $a \in R$ is called zero divisor if there is non-zero element $b \in R$ such that $ab = 0$

e.g;

(1) For $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{2}$ and $\bar{3}$ are zero divisors.

Since $\bar{2} \cdot \bar{3} = 0$ and $\bar{3} \cdot \bar{2} = 0$

(2) For $A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}$; $B = \begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix}$

$$AB = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 2-2 & 4-4 \\ 6-6 & 12-12 \end{bmatrix}$$

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

thus A and B are zero divisors.

Theorem:-

A ring $(R;+,\cdot)$ has no zero divisor if and only if Cancellation law holds in R.

<u>Proof:</u> Suppose Cancellation law holds in R

i.e $a \cdot b = a \cdot c \Rightarrow b = c$

take $a \neq 0$ such that $ab = 0$ for $a, b \in R$

since $a \cdot 0 = 0$

thus $a \cdot 0 = ab$

by Cancellation law we have

$b = 0$.

thus R has no zero divisor.

<u>Conversely:</u> let R has no zero divisor; i.e

for $ab = 0$; either $a = 0$ or $b = 0$.

for $a \neq 0$

as $ab = ac \Rightarrow ab - ac = 0$

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

Since R has no zero divisor; and $a \neq 0$; thus

$b - c = 0$

$\Rightarrow b = c$

this Shows that Cancellation law holds in R.

Note:-

If p is Prime; then Z_p does not have a zero divisor.

Integral Domain.

A Commutative Ring R is called an integral domain if it has no zero divisor; i.e for $a, b \in R$ if
$ab = 0$ then either $a = 0$ or $b = 0$.

The set of integers $\mathbb{Z}$ is an integral domain.

Lemma:-

A Commutative ring R is an integral domain if and only if Cancellation law holds in it w.r.t multiplication.

Proof:

Suppose Cancellation law holds in R w.r.t multiplication.

Now for $a, b \in R$, let
$a \cdot b = 0$ where $a \neq 0$.
also $a \cdot 0 = 0$
thus $a \cdot b = a \cdot 0$
by Cancellation law we have
$b = 0$
thus R has no zero divisor,
therefore R is an integral Domain.

Conversely:-

Suppose R is an integral domain.
i.e R has no zero divisor.

Let $ab = ac$ for $a, b, c \in R$ with $a \neq 0$
$\Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$
Since R has no zero divisor
thus $b - c = 0$ $(\because a \neq 0)$
$\Rightarrow b = c$ i.e Cancellation law holds in R

Charactristic Of a Ring:-

If for a ring $(R,+,\cdot)$ there exists a least +ve integer "n" such that
$na = a+a+a+ \cdots +a = 0$ (n times)
i.e $na = 0 \quad \forall\ a \in R$ then n is called the charactristic of R.

If no such integer Exists then R is of charactristic zero.

Definition:-

An element $x \in R$ (where R is ring) is called an idempotent if $x^2 = x$.

Boolean Ring:-

If each element of a ring is idempotent then the ring is called Boolean ring.

Lemma:-

If R is a Boolean ring then

(i) $2a = 0 \quad \forall\ a \in R$

(ii) $ab = ba$ i.e R is Commutative.

Proof:-

(i) $\because \quad 2a = a+a$

$= (a+a)^2 \qquad \because R$ is Boolean; $\therefore x^2 = x \ \forall x \in R$

$= (a+a)(a+a)$

$= a^2+a^2+a^2+a^2$

$= 4a^2$

$2a = 4a \qquad \because a^2 = a$ (R is Boolean)

$\Rightarrow 4a - 2a = 0$

$\Rightarrow 2a = 0$

(ii) Now $(a+b)^2 = a+b$ $\quad$ $\because$ R is Boolean.

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

$\Rightarrow a(a+b)+b(a+b) = a+b$ $\quad$ distributive law.

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

$\Rightarrow a+ab+ba+b = a+b$ $\quad$ $\because a^2=a$ & $b^2=b$.

$\Rightarrow ab+ba = 0$

$\Rightarrow \boxed{ab = -ba}$

Now

$ab-ba = ab+(-ba)$

$= ab+ab$ $\quad$ $\because ab=-ba$

$= 2(ab)$

$= 0$ $\quad$ $\because 2a = 0 \; \forall \, a \in R$ by (i)

$\Rightarrow ab = ba$

This shows that Boolean Ring is Commutative.

Sub-Ring:-

Let S be a non-empty subset of a ring $(R,+,\cdot)$, then S is said to be a subring of R if S satisfied all the axioms of ring under the induced binary operations.

i.e

S is called a subring of R if

(i) $a-b \in S \quad \forall \, a,b \in S$

(ii) $ab \in S \quad \forall \, a,b \in S$.

e.g Set of even integers $\{0, \pm 2, \pm 4, \pm 6, ---\}$ is a subring of Ring of integers $\{0, \pm 1, \pm 2, \pm 3, ---\}$.

Theorem:-

Let S be a non-empty subset of a ring $(R,+,\cdot)$ then S is a subring of R iff

(i) $a-b \in S \quad \forall\, a,b \in S$
(ii) $ab \in S \quad \forall\, a,b \in S$.

Proof:-

Suppose that S is a subring of R, i.e. S satisfies all the axioms of a ring.

Let $a,b \in S$

Since S is abelian group under addition; thus for $b \in S$; $-b \in S$ (additive inverse).

$\therefore \quad a,-b \in S$

$\Rightarrow a+(-b) \in S \Rightarrow a-b \in S$

hence Condition (i) is proved.

Also S is semigroup under multiplication, Thus for $a,b \in S$

$ab \in S$

Condition (ii) is proved.

Conversely

Suppose Condition (i) and (ii) holds in S. We have to show that S satisfies all the axioms of a ring.

Let $a,b \in S$

by Condition (i) $a-b \in S$

Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

this shows that S is subgroup of R under addition.

also $S \subseteq R$ and commutative law holds in R under addition; thus it also holds in S.

thus S is an abelian subgroup of R under addition.

Also for $a, b \in S \Rightarrow ab \in S$ (by condition (ii))

thus S is closed under multiplication.

Since $S \subseteq R$ and associative law holds in R; thus it also holds in S.

Thus S is a semi-group under multiplication

Again

Since $S \subseteq R$ and distributive laws holds in R, thus they also holds in S.

From above we have proved that

(i) S is abelian subgroup of R under addition.
(ii) S is semigroup under multiplication.
(iii) distributive laws holds in S

Hence S is a subring of R.

Centre Of Ring

If $(R, +, \cdot)$ is a ring, then the set of elements of R which commute with every element of R forms the centre of R, i.e

$$\text{Centre of } R = \{x \in R : ax = xa \ \forall a \in R\}$$

Theorem:- The Centre of R is a subring of R.

Proof:- Centre of R is always non-empty, since at least it contains the identity element which commute with every element of R.

Now suppose

$$x_1, x_2 \in \text{Centre of } R.$$

i.e $ax_1 = x_1 a$ and $ax_2 = x_2 a \quad \forall a \in R.$

then

$$\begin{aligned} (x_1 - x_2)a &= x_1 a - x_2 a && \text{distributive law} \\ &= ax_1 - ax_2 \\ &= a(x_1 - x_2) && \text{distributive law.} \end{aligned}$$

$\Rightarrow \quad x_1 - x_2 \in$ Centre of R

also

$$\begin{aligned} (x_1 x_2)a &= x_1(x_2 a) && \text{associative law.} \\ &= x_1(ax_2) \\ &= (x_1 a)x_2 && \text{associative law.} \\ &= (ax_1)x_2 \\ &= a(x_1 x_2) && \text{associative law.} \end{aligned}$$

$\Rightarrow \quad x_1 x_2 \in$ Centre of R.

$\because$ for $x_1, x_2 \in$ Centre of R

$x_1 - x_2 \in$ Centre of R

and $x_1 x_2 \in$ Centre of R

thus Centre of R is a subring of R.

Theorem:-

Every finite integral domain is a field.

Proof:- Let $D = \{x_1, x_2, x_3, \ldots, x_n\}$ be a finite integral domain. To show that D is a field we have to show that

(i) $1 \in D$ and

(ii) Every non-zero element of D has its multiplicative inverse in D.

Let $0 \neq a \in D$; Now form the product

$\{x_1a, x_2a, x_3a, \ldots, x_na\}$.

Since D is closed under multiplication thus

$x_1a, x_2a, x_3a, \ldots x_na$ all belongs to D i.e

$\{x_1a, x_2a, x_3a, \ldots x_na\} \subseteq D$.

Now we will show that all these elements are distinct.

If possible let $x_ia = x_ja$ where $i \neq j$

$\Rightarrow x_ia - x_ja = 0$

$\Rightarrow (x_i - x_j)a = 0$

$\because$ D is an integral domain thus have no zero divisor.

therefor either $x_i - x_j = 0$ or $a = 0$

Since $a \neq 0$; so $x_i - x_j = 0$

$\Rightarrow x_i = x_j$

This shows that all the elements are distinct.

$\therefore$ $\{x_1a, x_2a, x_3a, \ldots x_na\} = D$

Now let $0 \neq y \in D$; then

$$y = x_i a \text{ for some } i$$

but $a \in D$ then $a = x_j a$ for some j

$$\therefore \quad y = x_i(x_j a)$$
$$= x_i(a x_j) \quad \because D \text{ is an integral domain is Commutative ring.}$$
$$= (x_i a) x_j$$
$$y = y x_j$$

this is possible only when $x_j = 1$
thus $1 \in D$.

Since $1 \in D$ then there exists a non-zero element $b \in D$ such that

$$b \cdot a = 1$$

$\Rightarrow$ b is the multiplicative inverse of a.

Hence D is a field.

Corollary:-

If p is prime then the set Z_p is a field.

Proof:-

As $Z_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$.
to show that Z_p is a field we have to show that Z_p is an integral domain i.e it has no zero divisor.

For this take $\bar{a}, \bar{b} \in Z_p$
and let $\bar{a} \cdot \bar{b} = 0$

$$\Rightarrow \quad p \mid \bar{a} \cdot \bar{b}$$

Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

Since p is prime; so
either $p|\bar{a}$ or $p|\bar{b}$

If $p|\bar{a}$ then $\bar{a} = 0 \pmod{p}$.
If $p|\bar{b}$ then $\bar{b} = 0 \pmod{p}$.

thus Z_p has no zero divisor.
$\therefore Z_p$ is an integral domain.
Since Z_p is finite; therefor Z_p is a field.

Theorem:-
Intersection of two subrings of a ring R is a subring of R.

Proof:-
Let S and T be two subrings of a ring R.
Take $a, b \in S \cap T$
$\Rightarrow a, b \in S$ and $a, b \in T$

$\Rightarrow a-b \in S$ and $a-b \in T$ (since S and T are subrings)
$ab \in S$ $\qquad ab \in T$

$\Rightarrow a-b \in S \cap T$
and $ab \in S \cap T$

thus $S \cap T$ is also a subring of R.

Note:-
Intersection of any number of subrings of a ring R is a subring of R.

Ring Homomorphism:-

Let R and R' be two rings. A mapping $\phi: R \to R'$ is said to be ring Homomorphism if $\forall\ a, b \in R$

(i) $\phi(a+b) = \phi(a) + \phi(b)$

(ii) $\phi(ab) = \phi(a)\phi(b)$

Example:-

① Let $R = C$ (the set of Complex numbers) then the mapping $\phi: C \to C$ defined by

$$\phi(z) = \bar{z} \text{ is ring Homomorphism;}$$

Since

$$\phi(z_1+z_2) = \overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2 = \phi(z_1) + \phi(z_2)$$

and $\phi(z_1 z_2) = \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 = \phi(z_1)\phi(z_2)$.

②

Let $R = \{a + b\sqrt{2} : a, b \in Z\}$

the mapping $\phi: R \to R$ defined as

$\phi(a+b\sqrt{2}) = a - b\sqrt{2}$ is ring Homomorphism

Since.

$$\phi\left((a_1+b_1\sqrt{2}) + (a_2+b_2\sqrt{2})\right) = \phi\left((a_1+a_2) + (b_1+b_2)\sqrt{2}\right)$$

$$= (a_1+a_2) - (b_1+b_2)\sqrt{2}$$

$$= (a_1 - b_1\sqrt{2}) + (a_2 - b_2\sqrt{2})$$

$$= \phi(a_1+b_1\sqrt{2}) + \phi(a_2+b_2\sqrt{2})$$

and

$$\phi\left((a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})\right)=\phi\left(a_1a_2+a_1b_2\sqrt{2}+a_2b_1\sqrt{2}+2b_1b_2\right)$$

$$=\phi\left((a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}\right)$$

$$=(a_1a_2+2b_1b_2)-(a_1b_2+a_2b_1)\sqrt{2}$$

$$=a_1a_2+2b_1b_2-a_1b_2\sqrt{2}-a_2b_1\sqrt{2}$$

$$=(a_1a_2-a_1b_2\sqrt{2})-(a_2b_1\sqrt{2}-2b_1b_2)$$

$$=a_1(a_2-b_2\sqrt{2})-b_1\sqrt{2}(a_2-b_2\sqrt{2})$$

$$=(a_1-b_1\sqrt{2})(a_2-b_2\sqrt{2})$$

$$=\phi(a_1+b_1\sqrt{2})\,\phi(a_2+b_2\sqrt{2})$$

Hence ϕ is ring Homomorphism.

Isomorphism:-

A ring Homomorphism $\phi: R \rightarrow R'$ is Called isomorphism if ϕ is

(i) one-one

(ii) onto

Kernal Of ϕ:-

If ϕ is a ring Homomorphism from R to R' i.e $\phi: R \rightarrow R'$; then $Ker\phi$ is the set of all the elements $a \in R$ such that $\phi(a)=0'$ ($0'$ is additive identity of R')

i.e

$$Ker\,\phi=\{a\in R:\phi(a)=0'\}$$

Theorem:-

Let $\phi : R \to R'$ be a ring Homomorphism, then ϕ is one-one if and only if $\operatorname{Ker}\phi = \{0\}$.

Proof:-

Suppose ϕ is one-one, we have to show that $\operatorname{Ker}\phi = \{0\}$.

Suppose on contrary that $\operatorname{Ker}\phi \neq \{0\}$, then there exists non-zero element $r \in \operatorname{Ker}\phi$

$\therefore \quad \phi(r) = 0'$

but $\phi(0) = 0'$

$\Rightarrow \quad \phi(r) = \phi(0)$

$\Rightarrow \quad r = 0 \qquad$ Since ϕ is one-one.

which is a Contradiction thus $\operatorname{Ker}\phi = \{0\}$.

Conversely

Let $\operatorname{Ker}\phi = \{0\}$, we have to show that ϕ is one-one. For this let

$$\phi(r_1) = \phi(r_2)$$

$\Rightarrow \quad \phi(r_1) - \phi(r_2) = 0'$

$\Rightarrow \quad \phi(r_1 - r_2) = 0' \qquad$ since ϕ is Homomorphism.

$\Rightarrow \quad (r_1 - r_2) \in \operatorname{Ker}\phi$

since $\operatorname{Ker}\phi = \{0\}$

thus

$$r_1 - r_2 = 0$$

$\Rightarrow \quad r_1 = r_2$

this shows that ϕ is one-one.

Theorem:-

Let $\phi : R \to R'$ be a ring Homomorphism, then

(i) Image of ϕ is a subring of R'

(ii) $Ker\phi$ is a subring of R

Proof

(i)

Let $r_1', r_2' \in$ Image of ϕ i.e $r_1', r_2' \in R'$ then there exists $r_1, r_2 \in R$ such that

$$\phi(r_1) = r_1' \quad \text{and} \quad \phi(r_2) = r_2'$$

Now

$$r_1' - r_2' = \phi(r_1) - \phi(r_2)$$
$$= \phi(r_1 - r_2) \quad \because \phi \text{ is Homomorphism.}$$

Since $r_1 - r_2 \in R$ ($\because R$ is ring).

$\therefore$ $\phi(r_1 - r_2) \in$ Image of ϕ

i.e $r_1' - r_2' \in$ Image of ϕ.

also $r_1' r_2' = \phi(r_1)\phi(r_2)$

$$= \phi(r_1 r_2) \quad \because \phi \text{ is Homomorphism.}$$

Since $r_1 r_2 \in R$ ($\because R$ is ring)

$\therefore$ $\phi(r_1 r_2) \in$ Image of ϕ

i.e $r_1' r_2' \in$ Image of ϕ

Hence Image of ϕ is a subring of R'.

(ii) P.T.O.

Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

$Ker\phi = \{r \in R : \phi(r) = 0'\}$, we have to show that $Ker\phi$ is a subring of R.

Obviously $Ker\phi \subseteq R$ and $Ker\phi$ is always non-empty; since at least $0 \in Ker\phi$ such that $\phi(0) = 0'$.

Let $r_1, r_2 \in Ker\phi$

then

$$\phi(r_1) = 0' \text{ and } \phi(r_2) = 0'$$

Now

$$\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) \quad \because \phi \text{ is Homomorphism.}$$
$$= 0' - 0'$$
$$= 0'$$

$$\Rightarrow r_1 - r_2 \in Ker\phi$$

and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2) = 0' \cdot 0' = 0'$

$$\Rightarrow r_1 r_2 \in Ker\phi.$$

Hence $Ker\phi$ is a subring of R.

Ideals

Left Ideal:- Let I be a non-empty subset of a ring R; then I is said to be left ideal of R if

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

(ii) $\forall a \in I, r \in R \Rightarrow ra \in I$

Right Ideal:-

Let I be a non-empty subset of a ring R; then I is called right ideal of R if

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

(ii) $\forall\, a \in I, r \in R \Rightarrow ar \in I$

Two Sided Ideal

A non-empty subset I of R is called two sided ideal of R if it is both left and right ideal of R; i.e

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

(ii) $\forall\, a \in I, r \in R \Rightarrow ar, ra \in I$.

If the ring R is commutative then there is no distinction between the left ideal and the right ideal.

Two sided ideal is simply called ideal of the ring R.

Note:-

① Every ideal is a subring of R but every subring need not to be ideal of R.

② The trivial subring $\{0\}$ and the ring R itself are the improper ideals of R.

BY: Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

Examples:-

① The set $Z = \{0, \pm 1, \pm 2, \pm 3, ---\}$ is a ring of integers.

$2Z = \{0, \pm 2, \pm 4, \pm 6, ---\}$ is a sub ring of Z and also the ideal of Z.

②

Let R be the ring of all 2×2 matrices.

ie $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ (set of real nos.)} \right\}$.

R is non-commutative ring.

A subset U of R such that

$$U = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} : a, c \text{ are real nos.} \right\}$$

is left ideal of R but it is not right ideal.

Since for $A_1, A_2 \in U$

$$\text{Let } A_1 = \begin{pmatrix} a_1 & 0 \\ c_1 & 0 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} a_2 & 0 \\ c_2 & 0 \end{pmatrix}$$

$$A_1 - A_2 = \begin{pmatrix} a_1 & 0 \\ c_1 & 0 \end{pmatrix} - \begin{pmatrix} a_2 & 0 \\ c_2 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 - a_2 & 0 \\ c_1 - c_2 & 0 \end{pmatrix}$$

$\Rightarrow A_1 - A_2 \in U$

Take $r \in R$; let $r = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

and

$$rA_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ c_1 & 0 \end{pmatrix}$$

$$r A_1 = \begin{pmatrix} aa_1 + bc_1 & 0 \\ a_1c + c_1d & 0 \end{pmatrix}$$

$\Rightarrow \quad r A_1 \in U$

Hence U is left ideal of R.

$$\because \quad A_1 r = \begin{pmatrix} a_1 & 0 \\ c_1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \begin{pmatrix} aa_1 & a_1b \\ ac_1 & bc_1 \end{pmatrix}$$

$\Rightarrow A_1 r \notin U$

thus U is not the right ideal of R.

Similarly we can show that the subset S of R such that

$S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \text{ are reals} \right\}$ is right ideal of R but not the left ideal.

Theorem:-

Let $\phi : R \to R'$ be a ring Homomorphism then $\operatorname{Ker}\phi$ is an ideal of R.

Proof:-

$$\because \operatorname{Ker}\phi = \{ r \in R : \phi(r) = 0' \}$$

Let $r_1, r_2 \in \operatorname{Ker}\phi$

thus $\phi(r_1) = 0'$ and $\phi(r_2) = 0'$

Now

$\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) \qquad \because \phi$ is Homomorphism.

$= 0' - 0' = 0'$

$\Rightarrow r_1 - r_2 \in \text{Ker}\phi$

Now

let $r \in R$ and $r_1 \in \text{Ker}\phi$.

$$\Rightarrow \phi(rr_1) = \phi(r)\phi(r_1)$$
$$= \phi(r)\,0' = 0'$$

$\Rightarrow rr_1 \in \text{Ker}\phi$

also $\phi(r_1 r) = \phi(r_1)\phi(r) = 0'\phi(r) = 0'$

$\Rightarrow r_1 r \in \text{Ker}\phi$

This shows that $\text{Ker}\phi$ is an ideal of R.

Theorem:- If I and J are ideals of a ring R then

(i) $I \cap J$ is an ideal of R

(ii) $I+J = \{(a+b) : a \in I \text{ and } b \in J\}$ is an ideal of R.

(iii) $IJ = \{a_1b_1 + a_2b_2 + \dots + a_nb_n : a_i \in I, b_i \in J\}$ is an ideal of R.

Proof:-

(i) To show that $I \cap J$ is an ideal of R

let $a, b \in I \cap J$

$\Rightarrow a, b \in I$ and $a, b \in J$

since I and J are ideals of R

thus $a - b \in I$ and $a - b \in J$

Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

$\Rightarrow \quad a-b \in I \cap J$

also for $r \in R$ and $a \in I \cap J$

$\Rightarrow \; r \in R$ and $a \in I$ and $a \in J$

Since I and J are ideals of R thus

$ra, ar \in I$ and $ra, ar \in J$

$\Rightarrow \; ra, ar \in I \cap J$

Hence $I \cap J$ is also an ideal of R.

(ii)

$I+J = \{(a+b) : a \in I \text{ and } b \in J\}$.

Take $x, y \in I+J$ then

$x = a_1+b_1$, $y = a_2+b_2$ where $a_1, a_2 \in I$, $b_1, b_2 \in J$.

Now

$x-y = (a_1+b_1)-(a_2+b_2)$

$= (a_1-a_2)+(b_1-b_2)$

$\because$ I is an ideal thus $a_1-a_2 \in I$

J " " " " $b_1-b_2 \in J$

$\Rightarrow \; x-y \in I+J$

Also for $r \in R$ and $x \in I+J$

$rx = r(a_1+b_1) = ra_1 + rb_1$

$\because$ I is an ideal of R thus $ra_1 \in I$

J " " " " " " $rb_1 \in J$

$\Rightarrow \; rx \in I+J$

similarly $xr \in I+J$

Hence $I+J$ is an ideal of R.

(iii) $IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_i \in I \text{ and } b_i \in J\}$

let $x, y \in IJ$

where

$$x = a_1b_1 + a_2b_2 + \cdots + a_nb_n \qquad a_i \in I,\ b_i \in J$$
$$y = a_1'b_1' + a_2'b_2' + \cdots + a_n'b_n' \qquad a_i' \in I,\ b_i' \in J$$

Now

$$x - y = (a_1b_1 + a_2b_2 + \cdots + a_nb_n) - (a_1'b_1' + a_2'b_2' + \cdots + a_n'b_n')$$

$$= a_1b_1 + a_2b_2 + \cdots + a_nb_n + (-a_1')b_1' + (-a_2')b_2' + \cdots + (-a_n')b_n'$$

$\Rightarrow \quad x - y \in IJ$

Now for $r \in R$ and $x \in IJ$

$$rx = r(a_1b_1 + a_2b_2 + \cdots + a_nb_n)$$
$$= r(a_1b_1) + r(a_2b_2) + \cdots + r(a_nb_n)$$
$$= (ra_1)b_1 + (ra_2)b_2 + \cdots + (ra_n)b_n$$

Since I is an ideal of R thus

$(ra_1), (ra_2), \ldots, (ra_n) \in I$

Consequently $\quad rx \in IJ$

Similarly $\quad xr \in IJ$

Hence IJ is an ideal of R.

By:. Prof. M. Dabeer Mughal.
Federal Directarate Of Education
Islamabad.

Exercise:-

Let R be a Commutative ring with unity. If I is an ideal of R and $1 \in I$ then $I = R$

Sol:-

By definition of ideal

$$I \subseteq R \quad \text{——} \ (1)$$

Now

let $r \in R$ and $1 \in I$

Then $r \cdot 1 = r \in I$ Since I is ideal of R.

also $1 \cdot r = r \in I$ " " " " " R

$\Rightarrow$ $R \subseteq I$ —— (2)

from (1) and (2)

$$I = R.$$

Theorem:-

A field has no proper ideal.

OR Every field is a simple Group.

Proof:-

Let R be a field. we have to show that R has no proper ideal.

If Possible let I be a proper ideal of field R.

Take $0 \neq a \in I$

Since R is a field thus $a^{-1} \in R$.

$\therefore$ $aa^{-1} \in I$ $\because$ I is an ideal of R.

$\Rightarrow$ $1 \in I$

$\Rightarrow$ $I = R$ (from above Exercise).

Which is a Contradiction.

Hence the field R has no proper ideal.

Principal Ideal:-

An ideal I of a ring R is Called principal ideal if $I = aR$ for some $a \in R$.

It is Called principal ideal generated by "a" and is denoted by $\langle a \rangle$.

Principol Ideal Ring:-

A ring R in which every ideal of R is a principal ideal is Called principal ideal Ring.

e.g

for the ring of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ---\}$ then

$2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, ----\}$ is a principal ideal generated by "2".

$3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, ----\}$ is a principal ideal generated by "3".

Theorem:-

The ring of integers is a principal ideal ring.

Proof:-

The ring of integers is $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ----\}$.

Let I be an ideal of $\mathbb{Z}$.

Let n be the least +ve integer in I (i.e $n \in I$); and let $K \in I$ be any element of I.

By division algorithm we can find integers q and r such that

$$K = nq + r \quad \text{where } 0 \leq r < n$$

$$\Rightarrow \quad r = K - nq$$

Since I is an ideal of $\mathbb{Z}$ so for $n \in I$ and $q \in \mathbb{Z} \Rightarrow nq \in I$. also $K \in I$

$$\therefore \quad K - nq \in I \quad \because I \text{ is an ideal.}$$

$$\Rightarrow \quad r \in I \qquad \text{where } 0 \leq r < n$$

but n is the least +ve integer in I.

only possibility is $r = 0$

thus $K = nq$

this shows that any arbitrary element $K \in I$ is a multiple of n.

Hence I is principal ideal generated by "n".

Since n is arbitrary; so every ideal of $\mathbb{Z}$ is a principal ideal.

Consequently $\mathbb{Z}$ is a principal ideal ring.

Theorem:-

If $\{0\}$ and R are the only ideals of a Commutative ring R with unity then R is a field.
(OR a field has no proper ideal.)

Proof:-

Given that R is a Commutative ring with unity and only ideals of R are $\{0\}$ and R.

To show that R is a field we have to show that every no-zero element a of R has its multiplicative inverse in R. For this

Let $0 \neq a \in R$ then aR is an ideal of R.
(there is no Confusion that $aR = Ra$; since R is Commutative).
but the only ideals of R are $\{0\}$ and R.

$\therefore$ either $aR = \{0\}$ or $aR = R$.
since $a \neq 0$ thus $aR \neq \{0\}$; only possibility
is $R = aR$ where $aR = \{ar : r \in R \wedge a \in R\}$.
Since $1 \in R \Rightarrow 1 \in aR$
$\therefore$ $1 = ab$ where $b \in R$.
this Shows that b is the multiplicative inverse
of "a" in R.
Since "a" is arbitrary, So each non-zero
element of R has its multiplicative inverse in R.
Hence R is a field.

Exercise:-
If I is the right ideal and J is
the left ideal of a ring R and $I \cap J = \{0\}$
then $ab = 0$ $\forall$ $a \in I$ and $b \in J$.

Sol:-
Let $a \in I$ and $r \in R$
$\Rightarrow$ $ar \in I$ $\because$ I is the right ideal.
and let $b \in J$ and $r \in R$
$\Rightarrow$ $rb \in J$ $\because$ J is the left ideal.
Now
$a \in I \subset R \Rightarrow a \in R$ and $b \in J$
$\Rightarrow$ $ab \in J$ $\because$ J is the left ideal.
also $b \in J \subset R \Rightarrow b \in R$ and $a \in I$
$\Rightarrow$ $ab \in I$ $\because$ I is the right ideal.

$\because\ ab \in I$ and $ab \in J$

$\Rightarrow\ ab \in I \cap J$

But Given that $I \cap J = \{0\}$

So $\quad ab = 0 \qquad \forall a \in I$ and $b \in J$.

Question:-

If I is an ideal of a ring R then $C(I) = \{r \in I : ar - ra \in I \ \forall a \in R\}$ is a subring of R.

Sol:-

let $r_1, r_2 \in C(I)$

$\Rightarrow\ ar_1 - r_1 a \in I$ and $ar_2 - r_2 a \in I$

Now

$$a(r_1 - r_2) - (r_1 - r_2)a = ar_1 - ar_2 - r_1 a + r_2 a$$
$$= (ar_1 - r_1 a) - (ar_2 - r_2 a)$$

Since $ar_1 - r_1 a \in I$ and $ar_2 - r_2 a \in I$

also I is an ideal so $(ar_1 - r_1 a) - (ar_2 - r_2 a) \in I$

thus

$a(r_1 - r_2) - (r_1 - r_2)a \in I$

$\Rightarrow\ (r_1 - r_2) \in C(I)$

Now

$$a(r_1 r_2) - (r_1 r_2)a = (ar_1)r_2 - r_1(r_2 a)$$

Since I is an ideal of R so $ar_1, r_2 a \in I$

$\therefore\ (ar_1)r_2,\ r_1(r_2 a) \in I \qquad \because$ I is an ideal

$\Rightarrow\ (ar_1)r_2 - r_1(r_2 a) \in I \qquad$ " " " ".

$\Rightarrow\ a(r_1 r_2) - (r_2 r_2) \in I$

$\Rightarrow\ r_1 r_2 \in I$

Hence $C(I)$ is a subring of R.

Question:-

For any element $a \in R$, let $Ra = \{ ra : r \in R \}$. Show that Ra is a left ideal of R.

Sol:-

Let $x, y \in Ra$

$\Rightarrow \quad x = r_1 a \;,\; y = r_2 a \quad$ where $r_1, r_2 \in R$.

Now

$$x - y = r_1 a - r_2 a$$
$$= (r_1 - r_2)a \qquad \text{distributive law.}$$

Since $r_1 - r_2 \in R$; thus $(r_1 - r_2)a \in Ra$

$\Rightarrow \quad x - y \in Ra$

Also for $r \in R$

$$rx = r(r_1 a)$$
$$= (r r_1)a$$

Since $(r r_1) \in R$ thus $(r r_1)a \in Ra$

$\Rightarrow \; rx \in Ra$

Hence Ra is a left ideal of R.

Question:-

Let $a \in R$ be any element of R and $R(a) = \{ x \in R : ax = 0 \}$. Show that $R(a)$ is right ideal of R.

Sol:-

Let $x_1, x_2 \in R(a)$;

thus $\quad ax_1 = 0 \;,\; ax_2 = 0 \quad$ where $x_1, x_2 \in R$

Now

$$ax_1 - ax_2 = 0 - 0$$

$\Rightarrow \quad a(x_1 - x_2) = 0$

$\because x_1, x_2 \in R \Rightarrow x_1 - x_2 \in R$ ($\because R$ is ring).

$\therefore a(x_1 - x_2) \in R(a)$

Now for $r \in R$ and $x_1 \in R(a)$.

$\Rightarrow ax_1 = 0$

$(ax_1)r = 0r$

$\Rightarrow a(x_1 r) = 0$

$\because x_1 \in R, r \in R \Rightarrow x_1 r \in R$ ($\because R$ is ring)

$\Rightarrow a(x_1 r) \in R(a)$

Hence $R(a)$ is a right ideal of R.

Question:-

Prove that intersection of family of left ideals of a ring R is a left ideal of R.

Sol:-

Let A_α (where $\alpha \in$ indexing set I) be a family of left ideals of a ring R.

we have to show that $\bigcap_{\alpha \in I} A_\alpha$ is a left ideal of R.

let $x, y \in \bigcap_{\alpha \in I} A_\alpha$

$\Rightarrow x, y \in A_\alpha$ for each $\alpha \in I$.

Since each A_α is a left ideal of R; thus

$x - y \in A_\alpha$ for each α

$\Rightarrow x - y \in \bigcap_{\alpha \in I} A_\alpha$

also Let $r \in R$ and $x \in \bigcap_{\alpha \in I} A_\alpha$

$\Rightarrow x \in A_\alpha$ for each α

Since each A_α is a left ideal of R

$\therefore$ $rx \in A_\alpha$ for each α

$\Rightarrow$ $rx \in \bigcap_{\alpha \in I} A_\alpha$

Hence $\bigcap_{\alpha \in I} A_\alpha$ is a left ideal of R.

Question:-

If I is an ideal of R and A is a subring of R then show that $I \cap A$ is an ideal of A.

Sol:-

Let $x, y \in I \cap A$

$\Rightarrow$ $x, y \in I$ and $x, y \in A$

$\Rightarrow$ $x - y \in I$ since I is an ideal of R

and $x - y \in A$ " A is a subring of R

$\Rightarrow$ $x - y \in I \cap A$.

Let $x \in I \cap A$ and $a \in A \subseteq R$.

$\Rightarrow$ $x \in I$ and $x \in A$.

thus $ax \in I$ since I is an ideal of R.

also $ax \in A$ " A is a subring.

$\Rightarrow$ $ax \in I \cap A$.

similarly we can show that $xa \in I \cap A$.

Hence $I \cap A$ is an ideal of A.

BY: Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

Question:-

If R is a Commutative Ring and $a \in R$.
Prove that $L(a) = \{x \in R : xa = 0\}$ is an ideal of R.

Sol:-

Let $t_1, t_2 \in L(a)$

$\therefore \quad t_1 = x_1 a = 0 \quad$ and $\quad t_2 = x_2 a = 0 \quad$ for $x_1, x_2 \in R$

Now

$$t_1 - t_2 = x_1 a - x_2 a = 0 - 0$$

$$\Rightarrow (x_1 - x_2) a = 0$$

$\therefore \quad t_1 - t_2 \in L(a)$

Now for $r \in R$ and $t_1 \in L(a)$

$$r t_1 = r(x_1 a) = r(0)$$

$$\Rightarrow (r x_1) a = 0$$

$\because r \in R$ and $x_1 \in R \Rightarrow r x_1 \in R$

thus $(r x_1) a = 0 \Rightarrow r t_1 \in L(a)$

i.e $L(a)$ is a left ideal of R.

Again

for $r \in R$ and $t_1 \in L(a)$

$$t_1 r = (x_1 a) r = 0 r$$

$$\Rightarrow x_1 (a r) = 0$$

$$\Rightarrow x_1 (r a) = 0 \qquad \because R \text{ is Commutative.}$$

$$\Rightarrow (x_1 r) a = 0$$

$\because x_1 r \in R$

$\therefore (x_1 r) a \in L(a)$

i.e $t_1 r \in L(a)$

thus $L(a)$ is a right ideal of R.

Hence $L(a)$ is an ideal of R.

Question:-

Let I be an ideal of a ring R, then Show that $\{R:I\} = \{x \in R : rx \in I \ \forall r \in R\}$ is an ideal of R Containing I.

Sol:-

Let $x_1, x_2 \in \{R:I\}$

i.e $rx_1 \in I$ and $rx_2 \in I \quad \forall r \in R$.

Now

$$rx_1 - rx_2 = r(x_1 - x_2)$$

$\because x_1 - x_2 \in R \Rightarrow r(x_1 - x_2) \in I$ (I is ideal)

$\Rightarrow$ for $x_1 - x_2 \in R$, $r(x_1 - x_2) \in I$

$\Rightarrow \quad x_1 - x_2 \in \{R:I\}$

Now for $r_1 \in R$ and $x_1 \in \{R:I\}$.

$\Rightarrow rx_1 \in I \quad \forall r \in R.$

$\therefore \quad r_1(rx_1) = (r_1 r)x_1$

$\because r_1 r \in R \Rightarrow (r_1 r)x_1 \in I$ (I is ideal)

$\therefore \quad r_1 x_1 \in \{R:I\}$

Similarly $x_1 r_1 \in \{R:I\}$

Hence $\{R:I\}$ is an ideal of R Containing I.

i.e $I \subset \{R:I\}$.

Quotient Ring:-

Let I be an ideal of a ring R then the Set $R/I = \{a+I : a \in R\}$ is Called Cosets of I in R is a ring Called Quotient ring, where addition and multiplication are defined as

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

Note:-

(i) If R is a Commutative ring with unity then R/I is also a Commutative ring with unity

(ii) $1+I$ is the multiplicative identity of R/I and $0+I = I$ is the additive identity of R/I

Theorem:-

If I is an ideal of a ring R, then R/I is a ring.

Proof:-

First we show that R/I is an abelian group under addition.

$\because R/I = \{a+I : a \in R\}$

let $a+I, b+I \in R/I$ where $a,b \in R$

$(a+I)+(b+I) = (a+b)+I$

$\because a,b \in R \Rightarrow a+b \in R$

$\Rightarrow (a+b)+I \in R/I$

i.e $(a+I)+(b+I) \in R/I$

clouser law holds in R/I under addition.

Now let $(a+I), (b+I), (c+I) \in R/I$; $a, b, c \in R$

$$
\begin{aligned}
(a+I)+[(b+I)+(c+I)] &= (a+I)+(b+c)+I \\
&= [a+(b+c)]+I \\
&= [(a+b)+c]+I \\
&= (a+b)+I+(c+I) \\
&= [(a+I)+(b+I)]+(c+I)
\end{aligned}
$$

thus associative law holds in R/I under addition.

Since $0 \in R$; thus $0+I \in R/I$

$0+I$ is the additive identity of R/I; Since $\forall\ a+I \in R/I$

$$(0+I)+(a+I) = (0+a)+I = a+I$$

and $$(a+I)+(0+I) = (a+0)+I = a+I$$

$\forall\ a \in R$; $-a \in R$ ($\because R$ is ring).

thus $a+I \in R/I$ and $(-a)+I \in R/I$

$(a+I)$ and $(-a)+I$ are the additive inverses of eachother, Since

$$
\begin{aligned}
(a+I)+((-a)+I) &= (a+(-a))+I \\
&= 0+I
\end{aligned}
$$

thus each element of R/I has its additive inverse in R/I.

For $(a+I), (b+I) \in R/I$ $\quad a, b \in R$.

$$
\begin{aligned}
(a+I)+(b+I) &= (a+b)+I \\
&= (b+a)+I \qquad \because R \text{ is Commutative under addition.} \\
&= (b+I)+(a+I)
\end{aligned}
$$

thus R/I is Commutative under addition.

Hence R/I is abelian group under addition.

Now we show that R/I is semi-group under multiplication.

Let $(a+I), (b+I) \in R/I$ $\quad a, b \in R.$

$(a+I)(b+I) = ab+I$

Since $a, b \in R \Rightarrow ab \in R.$

thus $ab+I \in R/I$

i.e $(a+I)(b+I) \in R/I$

clouser law holds in R/I under multiplication

For $(a+I), (b+I), (c+I) \in R/I$ $\quad a, b, c \in R$

$$\begin{aligned}(a+I)[(b+I)(c+I)] &= (a+I)(bc+I)\\ &= a(bc)+I\\ &= (ab)c+I\\ &= (ab+I)(c+I)\\ &= [(a+I)(b+I)](c+I)\end{aligned}$$

thus associative law holds in R/I under multiplication.

Hence R/I is semi group under multiplication.

Now we show that both left and right distributive laws holds in R/I.

Let $(a+I), (b+I), (c+I) \in R/I$ for $a, b, c \in R$.

and

$$\begin{aligned}(a+I)[(b+I)+(c+I)] &= (a+I)[(b+c)+I]\\ &= a(b+c)+I\end{aligned}$$

$$(a+I)[(b+I)+(c+I)] = (ab+ac)+I$$
$$= (ab+I)+(ac+I)$$
$$= (a+I)(b+I)+(a+I)(c+I)$$

i.e left distributive law holds in R/I

also

$$[(b+I)+(c+I)](a+I) = ((b+c)+I)(a+I)$$
$$= (b+c)a+I$$
$$= (ba+ca)+I$$
$$= (ba+I)+(ca+I)$$
$$= (b+I)(a+I)+(c+I)(a+I)$$

i.e right distributive law holds in R/I.

Hence R/I is a Ring.

Lemma:-

If I is an ideal of a ring R; then the mapping $\phi: R \to R/I$ defined by

$$\phi(a) = a+I \qquad \forall a \in R$$

is a Homomorphism.

Proof:-

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

$$\phi(a+b) = (a+b)+I$$
$$= (a+I)+(b+I)$$
$$= \phi(a)+\phi(b)$$

and

$$\phi(ab) = ab+I$$
$$= (a+I)(b+I)$$
$$= \phi(a)\phi(b)$$

hence ϕ is a Homomorphism.

Theorem:-

Let I be an ideal of a ring R; then there always exists an epimorphism $\phi : R \to R/I$ with $Ker\,\phi = I$.

Proof:-

Define a mapping $\phi : R \to R/I$ defined by $\phi(a) = a + I \quad \forall\, a \in R$.

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

$$\therefore \quad \phi(a+b) = (a+b) + I$$
$$= (a+I) + (b+I)$$
$$= \phi(a) + \phi(b)$$

also

$$\phi(ab) = ab + I$$
$$= (a+I)(b+I)$$
$$= \phi(a)\phi(b)$$

this shows that ϕ is a Homomorphism.

Now we show that ϕ is onto.

for each $a + I \in R/I$, there exists an element $a \in R$ such that $\phi(a) = a + I$

Hence ϕ is an onto mapping.

thus ϕ is an epimorphism.

Now we have to show that $Ker\,\phi = I$.

Let $a \in Ker\,\phi \Rightarrow \phi(a) = I$ ($\because$ I is additive identity of R/I)

but $\phi(a) = a + I$

$\Rightarrow a + I = I \Rightarrow a \in I$

$\therefore \quad Ker\,\phi \subseteq I$ —— ①

Now Let $b \in I$

$\Rightarrow b + I = I \Rightarrow \phi(b) = I$

$\Rightarrow b \in Ker\,\phi$

$\therefore \quad I \subseteq Ker\,\phi$ —— ②

from ① and ② $Ker\,\phi = I$

Theorem:- (Ist Fundamental Theorem)

Let I be an ideal of a ring R and $\psi : R \to R'$ be an epimorphism with $\operatorname{Ker}\psi = I$ then $R/I \cong R'$

Proof:-

Define a mapping $\phi : R/I \to R'$ by

$$\phi(a+I) = \psi(a) \qquad \forall a \in R$$

First we show that ϕ is well defined. For this Let

$$a+I = b+I$$
$$\Rightarrow \quad a-b \in I$$
$$\Rightarrow \quad a-b \in \operatorname{Ker}\psi \qquad \because I = \operatorname{Ker}\psi$$
$$\Rightarrow \quad \psi(a-b) = 0' \quad \text{where } 0' \in R'$$
$$\Rightarrow \quad \psi(a)-\psi(b) = 0'$$
$$\Rightarrow \quad \psi(a) = \psi(b)$$
$$\Rightarrow \quad \phi(a+I) = \phi(b+I)$$

Hence ϕ is well defined.

To Show that ϕ is Homomorphism, let

$$\begin{aligned}\phi[(a+I)+(b+I)] &= \phi[(a+b)+I] \\ &= \psi(a+b) \\ &= \psi(a)+\psi(b) \qquad \because \psi \text{ is epimorphism} \\ &= \phi(a+I)+\phi(b+I)\end{aligned}$$

also

$$\begin{aligned}\phi[(a+I)(b+I)] &= \phi[ab+I] \\ &= \psi(ab) \\ &= \psi(a)\psi(b) \\ &= \phi(a+I)\phi(b+I)\end{aligned}$$

thus ϕ is a Homomorphism.

To show that ϕ is onto,

Let $r' \in R'$ be any element of R'.
Since ψ is onto (epimorphism). there exists an element $r \in R$ such that $\psi(r) = r'$

$$\Rightarrow \phi(r+I) = r'$$

thus $\exists$ an element $r+I \in R/I$ such that $\phi(r+I) = r'$
$\therefore$ ϕ is onto.

To show that ϕ is one-one.
Let

$$\phi(a+I) = \phi(b+I)$$
$$\Rightarrow \psi(a) = \psi(b)$$
$$\Rightarrow \psi(a) - \psi(b) = 0'$$
$$\Rightarrow \psi(a-b) = 0'$$
$$\Rightarrow a-b \in \operatorname{Ker}\psi$$

but $\operatorname{Ker}\psi = I$

thus $a-b \in I$

$$\Rightarrow a+I = b+I \;\bigstar$$

$\bigstar$ $a-b \in I$
$\Rightarrow a \in b+I$ —(i)
but $a \in a+I$ —(ii)
from (i) & (ii)
$a+I = b+I$

This shows that ϕ is one-one.

$\therefore$ ϕ is an isomorphism from $R/I \to R'$

Hence $R/I \cong R'$

Maximal Ideal:-

An ideal M in a ring R is called maximal if $M \neq R$ and there are no ideals strictly between M and R, that is the only ideals containing M are M and R.

Recall that a ring is called simple if it has no ideals other than $\{0\}$ and R. So nonzero ring is simple precisely when $\{0\}$ is the maximal ideal.

OR

Let I be an ideal of a ring R, then I is said to be maximal ideal of R if $I \neq R$ and if J is an ideal of R such that $I \subseteq J \subseteq R$ always implies that either $J = R$ or $I = J$.

e.g

Ring of integers is

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ----\}.$$

$\langle 2 \rangle = \{0, \pm 2, \pm 4, \pm 6, ----\}$ is a maximal ideal of $\mathbb{Z}$.

also

$\langle 3 \rangle = \{0, \pm 3, \pm 6, \pm 9, ----\}$ is a maximal ideal of $\mathbb{Z}$.

but $\langle 4 \rangle = \{0, \pm 4, \pm 8, \pm 12, ---\}$ is not maximal, since $\langle 4 \rangle \subset \langle 2 \rangle \subset \mathbb{Z}$

Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

Theorem:-

In a ring of integers $\mathbb{Z}$; the ideal $\langle n\rangle$ where $n>1$ is maximal iff n is prime.

Proof:-

Suppose that $\langle n\rangle$ is maximal, we have to show that n is prime.

Let n is not a prime, then it is a Composite number, So let $n = n_1 n_2$, where n_1 and n_2 are prime and $1 < n_1 \leq n_2 < n$

$\therefore \quad \langle n\rangle \subset \langle n_1\rangle \subset \mathbb{Z}$

and $\langle n\rangle \subset \langle n_2\rangle \subset \mathbb{Z}$

this shows that n is not a maximal ideal, which is a Contradiction;

thus n is a prime.

Conversely, Suppose that n is a prime. we have to show that $\langle n\rangle$ is a maximal ideal.

If $\langle n\rangle$ is not a maximal then either $\langle n\rangle = \mathbb{Z}$ or $\langle n\rangle \subset \langle m\rangle$ for some ideal $\langle m\rangle$ of $\mathbb{Z}$

Since $1 \in \mathbb{Z}$ and 1 is not a multiple of n (because $n>1$) thus $1 \notin \langle n\rangle$ thus $\langle n\rangle \neq \mathbb{Z}$

For the second possibility i.e $\langle n\rangle \subset \langle m\rangle$

$\Rightarrow$ $m|n$ which is not possible since n is prime. therefore $\langle n\rangle \not\subset \langle m\rangle$

Hence $\langle n\rangle$ is a maximal ideal of $\mathbb{Z}$.

Note:-

Let I and J be the ideals of a ring R; then $I+J$, IJ, $I\cap J$ are also ideals of R containing both I and J, these ideals are also called the ideals generated by I and J.

Let us take $a\in R$, then $\langle a\rangle = aR = \{ar : r\in R\}$ is also an ideal of R, called the ideal of R generated by a.

Now if I is an ideal of R and take $a\in R$ such that $a\notin I$, then $\langle a\rangle$ is also an ideal of R. Hence $I+\langle a\rangle$ (Sum of two ideals) is also an ideal of R, where

$$I+\langle a\rangle = \{i+ar : i\in I \wedge ar\in\langle a\rangle\}$$

this ideal is called the ideal generated by $I\cup\langle a\rangle$ and is denoted by (I,a).

Theorem:-

Let I be an ideal of a ring R, then I is maximal iff $(I,a)=R$.

Proof:-

Suppose that I is maximal ideal of R. Since $a\notin I$ and $a\in R$ thus

$I\subset (I,a)\subset R$

because I is maximal; then either $I=(I,a)$ or $(I,a)=R$. The first case is impossible, since $a\notin I$

$\therefore$ $I\neq (I,a)$.

thus $(I,a)=R$.

Conversely, Suppose that $(I,a)=R$; we have to Show that I is maximal.

If I is not maximal ideal of R, then there is some ideal J of R such that

$$I \subset J \subset R \quad ; \text{ wher } I \neq J.$$

Since $I \subset J$ thus there is at least one element $a \in J$ such that $a \notin I$

$$\Rightarrow \quad I \subset (I,a) \subset J \subset R$$

$$\Rightarrow \quad (I,a) \subset J \subset R$$

$$\Rightarrow \quad R \subset J \subset R \qquad \because (I,a)=R$$

$$\Rightarrow \quad J = R$$

Hence I is the maximal ideal of R.

Theorem:-

Let M be a proper ideal of a Commutative Ring with unity, then M is maximal iff R/M is field.

Proof:-

Since M is proper ideal of R thus $M \subset R$ but $M \neq R$, also R is Commutative ring with unity thus R/M is also a Commutative ring with unity.

Take a non-zero element $a+M \in R/M$; then $a \in R$ but $a \notin M$ because if $a \in M$ then $a+M=M$ which is zero of R/M.

Now we Show that $a+M$ has its multiplicative inverse in R/M.

Since M is maximal ideal of R, so $(M,a)=R$ where $(M,a)=\{m+ar : r \in R, m \in M\}$.

Since $1 \in R \Rightarrow 1 \in (M, a)$ $\because (M,a) = R$

$\Rightarrow 1 = m + ar$ for some $m \in M$ and $r \in R$.
$\Rightarrow 1 - ar = m \in M$
$\Rightarrow (1-ar) + M = M$
$\Rightarrow 1 + M = ar + M$
$1 + M = (a+M)(r+M)$

Since $1+M$ is the multiplicative identity of R/M, thus $(r+M)$ is the multiplicative inverse of $(a+M)$.
Since each non-zero element $a+M \in R/M$ has its multiplicative inverse in R/M.
Thus R/M is a field.

Conversely, Suppose that R/M is a field. we have to show that M is maximal ideal of R.
If M is not a maximal ideal of R then there is an ideal I of R such that $M \subset I \subset R$ & $M \neq I$.
Since M is properly contained in I, so there is at least one element $a \in I$ such that $a \notin M$.
thus $a + M \neq M$ i.e $a+M$ is non-zero element of R/M.
Since R/M is a field, so each non-zero element of R/M has its multiplicative inverse in R/M.
Let $b + M \in R/M$ is the multiplicative inverse of $a+M$, where $b \notin M$, $b \in R$
$\therefore (a+M)(b+M) = 1 + M$
$\Rightarrow ab + M = 1 + M$
$\Rightarrow (-ab+1) + M = M$
$\Rightarrow -ab + 1 \in M$
$\Rightarrow -ab + 1 \in I$ $\because M \subset I$

$\because$ $a \in I$ and $b \in R \Rightarrow ab \in I \Rightarrow -ab \in I$. ($\because I$ is ideal)
also $-ab+1 \in I$
$\Rightarrow 1 \in I$
as we know that If I is an ideal of a ring R and $1 \in I$ then $I = R$
thus $I = R$
Hence for $M \subset I \subset R$
$\Rightarrow M \neq I$ but $I = R$
thus M is maximal ideal of R.

Prime Ideal:-

An ideal I of a ring R is said to be prime ideal of R if $\forall a, b \in R$ and $ab \in I \Rightarrow$ either $a \in I$ or $b \in I$

eg

A Commutative ring with unity is an integral domain if $\{0\}$ is a prime ideal.

In the ring of integers $\mathbb{Z}$ the ideals generated by p; where p is prime are prime ideals.

Theorem:-

Let R be a Commutative ring and P be an ideal of R, then P is prime ideal iff R/P is an integral domain.

Proof:-

Suppose that P is prime ideal of R, then $\forall a, b \in R$ and $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

Since R is Commutative, thus R/P is also a Commutative ring with additive identity P.
we have to show that R/P is an integral domain, i.e it has no zero divisor. for this let $a+P, b+P \in R/P$ and

$$(a+P)(b+P) = P$$
$$\Rightarrow \quad ab+P = P$$
$$\Rightarrow \quad ab \in P$$

Since P is prime ideal, so either $a \in P$ or $b \in P$.

If $a \in P$ then $a+P = P$ (P the zero of R/P)
If $b \in P$ then $b+P = P$ (" " " " ").

Hence R/P has no zero divisor.
thus R/P is an integral domain.

Conversely, Suppose that R/P is an integral domain. we have to show that P is prime ideal.
Let $ab \in P$, then

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

Here $a+P, b+P \in R/P$
as R/P is an integral domain and therefore has no zero divisor. thus
either $a+P = P$ or $b+P = P$.
If $a+P = P$ then $a \in P$
If $b+P = P$ then $b \in P$.
Hence for $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$
this shows that P is a prime ideal.

Theorem:-
In a Commutative ring with Unity every maximal ideal is a prime ideal.

Proof:- Let I be a maximal ideal of a Commutative ring R with unity.
We have to show that I is a prime ideal.
i.e $\forall\, a,b \in R$ and $ab \in I \Rightarrow$ either $a \in I$ or $b \in I$.
We suppose that $a \notin I$; thus we will show that $b \in I$.
Since I is maximal ideal and $a \notin I$; so
$(I,a) = R$
Since $1 \in R \Rightarrow 1 \in (I,a)$
thus $1 = i + ar$ for some $i \in I$ and $r \in R$.
also
$$b = 1\cdot b = (i+ar)b$$
$$= ib + (ar)b = ib + (ra)b \quad \because R \text{ is Commutative}$$
$$b = ib + r(ab)$$
Since $i \in I$ and $ab \in I$ and I is ideal, so
$$ib + r(ab) \in I$$
$$\Rightarrow \quad ib + r(ab) \in I$$
$$\Rightarrow \quad b \in I$$
Hence I is prime ideal.

Alternatively:-
Let I be the maximal ideal of a Commutative ring R with unity, thus R/I is a field. Since every field is an integral domain so R/I is an integral domain. By Previous theorem I is prime ideal.

Note:-

If R is a Commutative ring with unity then its every maximal ideal is a prime ideal but every prime ideal need not to be maximal.

If R is a finite Commutative ring and P is its prime ideal then R/P is a finite integral domain. Since every finite integral domain is a field so R/P is a field. and therefore P is maximal ideal of R.

The Field Of Quotients Of An Integral Domain

Every integral domain is not a field, but it Can be imbedded in a field Called the field of Quotients. e.g, set of integers $\mathbb{Z}$ is an integral domain but it Can be enlarged to the set of rational numbers $\mathbb{Q}$, which is a field.

Let D be our integral domain, rougly speaking the field we seek should be all Quotients $\frac{a}{b}$ where $a, b \in D$ with $b \neq 0$.

If D is not a set of integers then $\frac{a}{b}$ may very well be meaningless. Clearly we must have answers of the following three questions.

(i) when $\frac{a}{b} = \frac{c}{d}$

(ii) what is $\frac{a}{b} + \frac{c}{d}$

(iii) what is $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)$

Let for $\frac{a}{b}$ we use (a,b)

as when $\frac{2}{3} = \frac{8}{12} \Rightarrow 2\times 12 = 8\times 3$

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc$$

in terms of ordered pairs we write

$(a,b) \sim (c,d)$ when $ad = bc$

and

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\Rightarrow (a,b) + (c,d) = (ad+bc, bd)$$

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$$

$$\Rightarrow (a,b)(c,d) = (ac, bd)$$

Definition:-

Two elements $(a,b), (c,d)$ are equivalent and written as $(a,b) \sim (c,d)$ if and only if $ad = bc$

Lemma:-

Let M be the set of all ordered pairs (a,b); where $a, b \in D$ and $b \neq 0$. In M we define a relation as $(a,b) \sim (c,d)$ iff $ad = bc$. Show that this relation is an equivalence relation on M.

Proof:-

Here $M = \{(a,b) : a, b \in D \wedge b \neq 0\}$ where D is an integral domain.

as $a, b \in D$ where D is an integral domain, So is a Commutative ring, thus

$$ab = ba$$

$$\Rightarrow \frac{a}{b} = \frac{a}{b}$$

$$\Rightarrow (a,b) \sim (a,b)$$

So the relation is reflexive.

Let $(a,b) \sim (c,d)$

$$\Rightarrow ad = bc$$

Since D is Commutative ring, So

$$da = cb$$

or $\frac{c}{d} = \frac{a}{b}$

$$\Rightarrow (c,d) \sim (a,b)$$

thus the relation is symmetric.

Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

$$\frac{a}{b} = \frac{c}{d} \quad \text{and} \quad \frac{c}{d} = \frac{e}{f}$$

Here $b \neq 0$, $d \neq 0$; $f \neq 0$

$\Rightarrow ad = bc$ — ① and $cf = de$ — ②

from ② $\quad cf = de$

$\Rightarrow b(cf) = b(de) \qquad \because b \neq 0$

$\Rightarrow (bc)f = (bd)e$

$\Rightarrow (ad)f = (bd)e \qquad$ using ①

$\Rightarrow (da)f = (db)e \qquad \because D$ is Commutative

$\Rightarrow d(af) = d(be)$

$\Rightarrow d(af) - d(be) = 0$

Prof. M. Dabeer Mughal
Federal Directorate of Education
Islamabad, PAKISTAN

$d(af - be) = 0$ left distributive law.

Since D is an integral domain; and will have no zero divisor, so
either $d = 0$ or $af - be = 0$
$\because d \neq 0$ thus $af - be = 0$
$\Rightarrow af = be$
$\Rightarrow \frac{a}{b} = \frac{e}{f}$

$\Rightarrow (a,b) \sim (e,f)$

thus the relation is transitive.

Hence the relation is an equivalence relation.

Note:-

We will denote the equivalence class of (a,b) in M by $[a,b]$; where $a,b \in D$ with $b \neq 0$ and D is an integral domain.

Theorem:-

Let F be the set of all such equivalences $[a,b]$; $a,b \in D$; i.e

$F = \{[a,b] : a,b \in D \wedge b \neq 0\}$ then F is field.

Proof:-

First we will show that F is an abelian group under addition. Here we define the addition in F by $[a,b] + [c,d] = [ad+bc, bd]$
$\because b \neq 0$ and $d \neq 0 \Rightarrow bd \neq 0$
$\therefore [ad+bc, bd] \in F$ i.e F is closed under this

operation of addition.

Now we show that this addition is well defined. For this, let $[a,b]=[a',b']$ and $[c,d]=[c',d']$. Now we have to show that

$$[a,b]+[c,d]=[a',b']+[c',d']$$

or $$[ad+bc,bd]=[a'd'+b'c',b'd']$$

or in equivalent term as

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

$\because (a,b)\sim(c,d)$ iff $ad=bc$

Now

$$\begin{aligned}(ad+bc)b'd' &= (ad)(b'd')+(bc)(b'd')\\ &= ab'dd'+bb'cd' \quad \because D \text{ is Commutative}\end{aligned}$$

Since $[a,b]=[a',b'] \Rightarrow ab'=ba'$

and $[c,d]=[c',d'] \Rightarrow cd'=dc'$

using this in above we have

$$\begin{aligned}(ad+bc)b'd' &= ba'dd'+bb'dc'\\ &= (bd)(a'd')+(bd)(b'c') \quad \because D \text{ is Commutative}\\ &= (bd)(a'd'+b'c')\end{aligned}$$

as required;

thus the addition is well defined in F.

For associative law, Let $[a,b],[c,d],[e,f]\in F$

$$\begin{aligned}[a,b]+\{(c,d)+(e,f)\} &= [a,b]+[cf+de,df]\\ &= [a(df)+b(cf+de),b(df)]\\ &= [(ad)f+b(cf)+b(de),(bd)f]\\ &= [(ad)f+(bc)f+(bd)e,(bd)f]\end{aligned}$$

$$[a,b]+\{[c,d]+[e,f]\} = [(ad+bc)f+(bd)e,\ (bd)f]$$
$$= [ad+bc,\ bd]+[e,f]$$
$$= \{[a,b]+[c,d]\}+[e,f]$$

thus associative law holds in F under addition.

The element $[0,b] \sim [0,1]$; since $0 \cdot 1 = b \cdot 0 \Rightarrow 0 = 0$
$[0,b]$ is the zero element (additive identity) of F
because $\forall\ [a,c] \in F$

$$[a,c]+[0,b] = [a,c]+[0,1] \qquad \because [0,b] \sim [0,1]$$
$$= [a,c]$$

Now
$\forall\ [a,b] \in F$ there is $[-a,b] \in F$ such that

$$[a,b]+[-a,b] = [0,b^2]$$
$$= [0,1] \qquad \because [0,b^2] \sim [0,1]$$

thus each element of F has additive inverse in F.

Let $[a,b],[c,d] \in F$; thus $b \neq 0$; $d \neq 0$.
and

$$[a,b]+[c,d] = [ad+bc,\ bd]$$
$$= [da+cb,\ db] \qquad \because D \text{ is Commutative.}$$
$$= [cb+da,\ db]$$
$$= [c,d]+[a,b]$$

thus Commutative law holds in F under addition.

Hence F is an abelian group under addition.

Now we show that the non-zero elements of F forms an abelian group under multiplication.

We define the multiplication in F as

$$[a,b][c,d] = [ac, bd] \quad \forall [a,b],[c,d] \in F.$$

$\because [a,b],[c,d] \in F \quad \therefore b \neq 0 ; d \neq 0$

$\Rightarrow bd \neq 0$

thus $[ac, bd] \in F$

i.e F is closed under this operation of multiplication.

Now we show that this operation of multiplication is well defined.

Let $[a,b] = [a',b']$ and $[c,d] = [c',d']$

i.e $ab' = ba'$ —(i) and $cd' = dc'$ —(ii)

We have to show that $[a,b][c,d] = [a',b'][c',d']$

or $[ac, bd] = [a'c', b'd']$

or $[ac, bd] \sim [a'c', b'd']$

i.e $(ac)(b'd') = (bd)(a'c')$

Now

$(ac)(b'd') = a(cb')d' = a(b'c)d'$ $\because$ D is Commutative

$= (ab')(cd')$

$= (ba')(dc')$ from (i) and (ii)

$= b(a'd)c'$

$= b(da')c'$ $\because$ D is Commutative.

$= (bd)(a'c')$

as required.

thus multiplication is well defined.

For associative law; let $[a,b],[c,d],[e,f] \in F$

and

$[a,b]([c,d][e,f]) = [a,b][ce, df]$

$$[a,b]([c,d],[e,f]) = [a(ce), b(df)]$$
$$= [(ac)e, (bd)f]$$
$$= [ac, bd][e,f]$$
$$= ([a,b][c,d])[e,f]$$

this shows that associative law holds in F under multiplication.

$\because [d,d] \sim [1,1]$; since $d \cdot 1 = 1 \cdot d \Rightarrow d = d$
the element $[d,d]$ is the multiplicative identity of F, because $\forall\ [a,b] \in F$

$$[a,b][d,d] = [a,b][1,1] = [a,b]$$

Now take a non-zero $[a,b] \in F$, thus $a \neq 0, b \neq 0$ then $[b,a] \in F$ is also non-zero element of F and

$$[a,b][b,a] = [ab, ba]$$
$$= [1,1]$$

$[ab, ba] \sim [1,1]$
$\because (ab)1 = (ba)1$
$ab = ba$
$ab = ab$ $\quad \because$ D is Commutative.

this shows that $[b,a]$ is the multiplicative inverse of $[a,b]$. i.e each non-zero element of F has its multiplicative inverse in F.

Hence the non-zero elements of F forms a group under multiplication.

Now for $[a,b], [c,d] \in F$

$$[a,b][c,d] = [ac, bd]$$
$$= [ca, db] \quad \because \text{D is Commutative.}$$
$$= [c,d][a,b]$$

i.e Commutative law holds in F under multiplication.

Hence the non-zero elements of F forms an abelian group under multiplication.

Now we show that F hold distributive laws.
that is

$$[a,b]\left([c,d]+[e,f]\right) = [a,b][c,d]+[a,b][e,f]$$

or $\quad [a,b][cf+de,df] = [ac,bd]+[ae,bf]$

or $\quad [a(cf+de),b(df)] = [(ac)(bf)+(bd)(ae),(bd)(bf)]$

or equivalently

$$[a(cf+de),b(df)] \sim [(ac)(bf)+(bd)(ae),(bd)(bf)]$$

i.e

$$a(cf+de)(bd)(bf) = b(df)\left((ac)(bf)+(bd)(ae)\right)$$

Now

$$\begin{aligned} a(cf+de)(bd)(bf) &= (acf+ade)b(dbf) \\ &= (acfb+adeb)(dbf) \\ &= (dbf)(acfb+adeb) \quad \because D \text{ is Commutative} \\ &= b(df)\left((ac)(bf)+(bd)(ae)\right) \quad \text{"} \quad \text{"} \end{aligned}$$

as required.

Similarly we can show that right distributive law holds in F. (Which is not necessary, since D is Commutative, so left and right dist. laws are same).

Hence F is a field.

Theorem:-

Every integral domain can be imbedded in a field.

Proof

Let D be an integral domain and

$F = \{[a,b] : a,b \in D \wedge b \neq 0\}$ is the field.

To show that D can be imbedded in F, we have to show that there is an isomorphism from D to F.

Before doing so, we notice that for $x \neq 0, y \neq 0$ of D

$[ax,x] = [ay,y]$; Since $(ax)y = x(ay)$

$(ax)y = (xa)y = x(ay)$

Let us denote $[ax,x]$ by $[a,1]$

i.e $[ax,x] = [a,1]$; Since $(ax)1 = xa = ax$ $\because$ D is Commutative

Define $\phi : D \to F$ by

$$\phi(a) = [a,1] \quad \forall\, a \in D$$

First we show that ϕ is well defined; for this

let $a = b$

$\Rightarrow [a,1] = [b,1]$

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

$\because a = \frac{a}{1} = [a,1]$
$b = \frac{b}{1} = [b,1]$

thus ϕ is well defined.

Now we show that ϕ is a Homomorphism, for this

let $a,b \in D$

and $\phi(a+b) = [a+b,1]$

$= [a,1] + [b,1]$

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

$[a+b,1] = \frac{a+b}{1}$
$= \frac{a}{1} + \frac{b}{1}$
$= [a,1] + [b,1]$

and $\phi(ab) = [ab, 1]$
$= [a, 1][b, 1]$
$= \phi(a)\,\phi(b)$

$$[ab, 1] = \frac{ab}{1} = \frac{a}{1}\cdot\frac{b}{1} = [a, 1][b, 1]$$

thus ϕ is a Homomorphism.

ϕ is onto; since for each $[a, 1] \in F$ there is an element $a \in D$ such that $\phi(a) = [a, 1]$.

To show that ϕ is one-one.
Let

$$\phi(a) = \phi(b)$$
$$\Rightarrow [a, 1] = [b, 1]$$
$$\Rightarrow a(1) = 1(b)$$
$$\Rightarrow a = b$$

thus ϕ is one-one.

Hence ϕ is an isomorphism, so we have imbedded the integral domain D in the field F.

The field F is Called field of Quotients.

Q:-

The ring Q of quaternions is a division ring.

Sol:-

The elements of Q are of the form,

$$\underline{a} = a_0 I + a_1 i + a_2 j + a_3 K \quad \text{where } a_i \in \mathbb{R} \quad 0 \le i \le 3$$

and $\underline{a} = 0$ iff $a_i = 0 \quad 0 \le i \le 3$.

To show that Q is a division ring; we have to show that each non-zero element of Q has its inverse in Q.

Let a' denote the Conjugate of $\underline{a}$ in Q; where

$$a' = a_0 I - a_1 i - a_2 j - a_3 K$$

and $N(\underline{a}) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0 \quad \because \underline{a} \neq 0$

let $a^* = \dfrac{a_0}{N(\underline{a})} I - \dfrac{a_1}{N(\underline{a})} i - \dfrac{a_2}{N(\underline{a})} j - \dfrac{a_3}{N(\underline{a})} K$

Now

$$\underline{a} \cdot a^* = (a_0 I + a_1 i + a_2 j + a_3 K) \cdot \left(\frac{a_0}{N(\underline{a})} I - \frac{a_1}{N(\underline{a})} i - \frac{a_2}{N(\underline{a})} j - \frac{a_3}{N(\underline{a})} K \right)$$

$$= \frac{a_0^2}{N(\underline{a})} + \frac{a_1^2}{N(\underline{a})} + \frac{a_2^2}{N(\underline{a})} + \frac{a_3^2}{N(\underline{a})} = \frac{a_0^2 + a_1^2 + a_2^2 + a_3^2}{N(\underline{a})} = \frac{N(\underline{a})}{N(\underline{a})} = I$$

$$= 1 \cdot I + 0 i + 0 j + 0 K$$

thus a^* is inverse of $\underline{a}$

Hence Q is a division ring.

Prime Field:-

A field is said to be a prime field if it has no proper subfield.

e.g; for each prime p $\mathbb{Z}_p$ is a prime field.

the set of rational numbers is a prime field.

A subfield P of a field F is called prime subfield if P has no proper subfield. e.g the set Q of rational nos. is a prime subfield of field $\mathbb{R}$.