Def

## Ring:

(1) A ring R is a set together with two binary operations + and × (called addition and multiplication) satisfying the following axioms:-

1) $(R, +)$ is abelian group

(2) $\times$ is associative : $(a \times b) \times c = a \times (b \times c)$

for all $a, b, c \in R$

(3) the distributive law hold in R for all $a, b, c \in R$

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

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

(2) The ring R is commutative if multiplicaton is commutative

(3) The ring R is said to have an identity (or contain a 1) if there is an element $1 \in R$ with $1 \times a = a \times 1 = a$ for all $a \in R$

**Commutative Ring**:- A commutative ring is a ring R that satisfy the additional axiom that

$ab = ba$ for all $a, b \in R$

**Example**: $\mathbb{Z}$, $\mathbb{R}$, $2\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{C}$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

⇓

every non-zero element has an inverse.

**Division Ring**:- A ring R with identity 1, where $1 \neq 0$, is called division ring (skew field)

⇒ If every non-zero element $a \in R$ has a multiplicative inverse i.e there exist $b \in R$ such that $ab = ba = 1$.

**Example**:- Quaternions are division ring.

**Note**:- The quaternions are a division ring (that is, a ring in which each element has a multiplicative inverse, alternatively. Quaternion are non-commutative.

# Quartenions are the set

$\{a + bi + cj + dk\}$, where $a, b, c, d$ are any real number and the properties / behaviours of $i, j, k$ are given as follows

(i) $i^2 = j^2 = k^2 = ijk = -1$.

(ii) $ij = k = -ji$, $jk = i = -kj$

and $ki = j = -ik$.

# A Commutative division ring is called field.

Example :- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

⇒ In the ring $M_2(\mathbb{C})$. let

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

$$i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

The set $H$ of real quaternions consists of all matrices of the form.

$$a1 + bi + cj + dk = \begin{pmatrix} a+ib & c+di \\ -c+di & a-bi \end{pmatrix}.$$

where $a, b, c, d \in \mathbb{R}$.

## ± Subring :-

A non-empty subset $S$ of $R$ is a subring

if $a, b \in S \Rightarrow$ for all $a, b \in S$.

① $a - b \in S$

② $ab \in S$

i.e $S$ is closed under subtraction and multiplication

## Example of ~~Subdi~~ Subring.

① The even integer $2\mathbb{Z}$ from a subring of $\mathbb{Z}$.

But $3\mathbb{Z}$ will not form a subring of $\mathbb{Z}$

Since odd + odd = even.

$3 + 5$ = even $\notin$ odd.

so $3\mathbb{Z}$ will not form a subring of $\mathbb{Z}$.

Q. Is $2\mathbb{Z} \cup 3\mathbb{Z}$ form a subring of $\mathbb{Z}$?

Sol: No, since $2+3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

Q. Is $\mathbb{Z}_n$ is not a subring of $\mathbb{Z}$?

Sol: $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$.

take $a = 1, b = 2$.

$a.b = 2 \in \mathbb{Z}_n$.

$2.1 =$

$a - b = 1 - 2 = -1 \notin \mathbb{Z}_n$

so $\mathbb{Z}_n$ is not a subring of $\mathbb{Z}$.

Q. Sum of two subring need not be subring.

Sol: $A = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\} \Rightarrow a \in A$

$B = \left\{ \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} : c \in \mathbb{Z} \right\} \Rightarrow b \in B$

Take $a = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ & $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$$R = A + B$$

$$= \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} + \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \right\}.$$

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

Take $M_1 = (a+b)$

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

$$M_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$$

$$a' = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}, \quad b' = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$$

$$M_3 \cdot M_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 2+2 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}$$

$= \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \notin \quad R = \begin{pmatrix} a & c \\ b & 0 \end{pmatrix}$

Therefore sum of two subring need not be subring.

Q Let R be a ring with Identity and let S be a subring of R containing the identity. prove that if u is a unit in S, then u is a unit in R.

Show by Example converse is False.

Proof:-

Since U is a unit in S which implies that there exist a unique element $u^{-1} \in S \subseteq R$ such that-

$$U \cdot U^{-1} = 1 \quad , \quad U^{-1} \in S \subseteq R.$$

Since $U \in S \subseteq R$ and $u^{-1} \in S \subseteq R$.

so $u \in R$ and $U^{-1} \in R$ such that $uu^{-1} = 1$.

so $u^{-1}$ is multiplicative inverse of U in R.

Hence U is a unit in R.

But converse is False,

Since take ~~R~~ $R = \mathbb{Q}$ and $S = \mathbb{Z}$.

Then 2 is a unit in $\mathbb{Q}$

but not a unit in $\mathbb{Z}$ since $\frac{1}{2} \notin \mathbb{Z}$

For unit $2 \cdot \frac{1}{2} = 1$

## Subring :

A non-empty subsets $S$ of a ring $R$ is a subring of $R$ if and only if

(i) $a-b \in S$

(ii) $ab \in S$ for all $a, b \in S$.

**Theorem :** Prove that the intersection of two subring of a ring $R$ is a subring of $R$.

**proof :** let $A$ and $B$ be two subring of a ring $R$

Clearly $A \cap B$ will non-empty since $0 \in A \cap B$.

let $a, b \in A \cap B$. Then $a, b \in A$ and $a, b \in B$.

Since $A$ is a subring of $R$

$$a-b \in A$$

$$ab \in A$$

Similarly, $a-b \in B$

$$ab \in B$$

so $a-b \in A \cap B$ and $ab \in A \cap B$.

Hence $A \cap B$ is a subring of $R$.

**Q.** Prove that the intersection of any non-empty collection of subrings of a ring is also a subring.

**Soln:** let $\{S_\alpha\}_{\alpha \in I}$ is a collection (an arbitrary ~~collection~~ collection of subrings of a ring $(R, +, \cdot)$.

let $S = \bigcap_{\alpha \in I} S_\alpha$

**Note:** $I$ is an indexing set.

Index set mean a set whose element are used to indicate the order of the elements of a sequence, series etc.

To prove: $S = \bigcap_{\alpha \in I} S_\alpha$ is a subring of $R$.

then we have to show that-

If $a, b \in S \Rightarrow a-b,\ ab \in S$

Let $a, b \in S \Rightarrow a, b \in S_\alpha$ for every $\alpha$.

Since each $S_\alpha$ is a subring of $\mathbb{R}$,

we have $a - b \in S_\alpha$

$ab \in S_\alpha$ for every $\alpha \in I$

Therefore $a - b \in \bigcap S_\alpha$

$a \cdot b \in \bigcap S_\alpha$

i.e $a - b \in S$

$ab \in S$

So, $S = \bigcap_{\alpha \in I} S_\alpha$ is a subring of $\mathbb{R}$.

(e) The set of all rational number with odd - numerators (when written in lowest terms).

Sol^n. It is not subset of $\mathbb{Q}$

$\frac{1}{3}$ is in the set but $\frac{1}{3}+\frac{1}{3}=\frac{2}{3}$ is not in the set because $\frac{2}{3}$ is not set of rational with odd numerators.

(f) The set of all rational numerators with even numerators (when written in lowest terms).

Sol^n. The set is a subgroup.

Let $\frac{2a}{b}$ and $\frac{2c}{d}$ be elements of the group.

Here b and d are odd, ~~otherwise~~ otherwise the fraction can't be written in lowest term.

$$\frac{2a}{b}-\frac{2c}{d}=\frac{2(ad-bc)}{bd}$$ is an element of the set.

again $\frac{2a}{b}\cdot\frac{2c}{d}=\frac{(2\cdot 2)ac}{bd}$ is an element of the set.

Q. The set of all functions which have an infinite number of zeros is subring of the ring of all function from the closed interval $[0,1]$ to $\mathbb{R}$.

(True / False)

Ans: False, it is not closed under addition, define $f : [0,1] \longrightarrow \mathbb{R}$ and

Take $f(x) = \begin{cases} 1 & \text{if } x \text{ is rational} \\ 0 & \text{if } x \text{ is irrational.} \end{cases}$

$g : [0,1] \longrightarrow \mathbb{R}$ by

$g(x) = \begin{cases} 0 & \text{if } x \text{ is irrational} \\ +1 & \text{if } x \text{ is rational.} \end{cases}$

Both $f$ and $g$ having infinite number of zeroes

but their sum

$f + g = 1$ have ~~finite zero~~ no zero.

~~$f(x) + g(x) =$~~

$(f+g)(x) = h(x) = 1$

$\neq h(x) = 1$

$h(x)$

$h(x) = 1$ have no ~~roots~~ roots

because roots of a polynomial function are those value of the variable that cause the polynomial to evaluate to 0.

$h(x) \neq 0$ so no root.

Q The Set of all subring which have only a finite number of zero, together with the zero function. Is the subring of the ring of all function from the closed interval ~~[0,1]~~ $[0,1]$ to $\mathbb{R}$. (T/F

soln: F $\Rightarrow$ (False)

Take $f : [0,1] \longrightarrow \mathbb{R}$ by defined by

$f(x) = x$ which have exactly one zero.

$g : [0,1] \longrightarrow \mathbb{R}$ defined by

$g(x) = -x$ which have exactly one zero.

But $(f+g)(x) = 0 \quad \forall\, x \in [0,1]$

Take $h = f+g$

i.e $h(x)$ have infinite Root

$h(x) \notin$ set of all subring having finite zeros

## Boolean ring :

A ring R is boolean if all its elements are idempotent i.e $x^2 = x$ for all $x \in R$.

Every boolean ring have characteristic 2

$\Rightarrow$ $(a+1)^2 = a^2 + 2a + 1$.

$(a+1)^2 = a^2 + 1$.

since $a^2 = a$

$(a+1)^2 = (a+1)$

$\Rightarrow$ Q. Prove that every Boolean ring is commutative

Sol: $(x+x) = (x+x)^2$

$= x^2 + xx + xx + x^2$

$= (x+x) + (x+x)$ { since $x^2 = x$ }

Hence $(x+x) = 0$

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

$\Rightarrow (x+x) = 0$ for all $x \in R$.

$\Rightarrow (x+x) = 0$ for all $x \in \mathbb{R}$

Now, $(x+y)^2 = (x+y)$

$= x^2 + xy + yx + y^2$

$= x + xy + yx + y$

since $x \in R$ (boot can say)

so $x^2 = x$

$y^2 = y$ , $y \in R$

$(x+y)^2 = x + xy + yx + y = x+y$

this implies $xy + yx = 0$ — (1)

since from $x + x = 0$ for $x \in \mathbb{R}$.

we ~~B~~ also have ~~xy + 0~~ $yx + yx = 0$

put $yx = v$

$v + v = 0$ for $v \in R$.

$\Rightarrow v = -v$

$\Rightarrow yx = -yx$.

From (1), $xy + yx = 0$

$$xy + (-yx) = 0$$

$$\boxed{xy = yx}. \quad \text{for all } x, y \in R.$$

Q. Prove that the only Boolean ring that is also an integral domain is $\mathbb{Z}_2$.

Soln Suppose a Boolean ring $R$ is also an integral domain. Then $R$ contain unity 1.

Now take $r \in R - \{0\}$. Then

$$r^2 = r \quad \text{for all } r \in R.$$

$$\Rightarrow r^2 - r = 0$$

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

$$\Rightarrow r = 0 \text{ or } r = 1.$$

But $r \in R - \{0\}$ i.e $r \neq 0$

so $r - 1 = 0 \Rightarrow r = 1$,

We conclude that all non-zero elements are

The Multiplicative Identity ie 1

and if $r^2 = r$ for all $r \in R$

then $r^2 - r = 0$

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

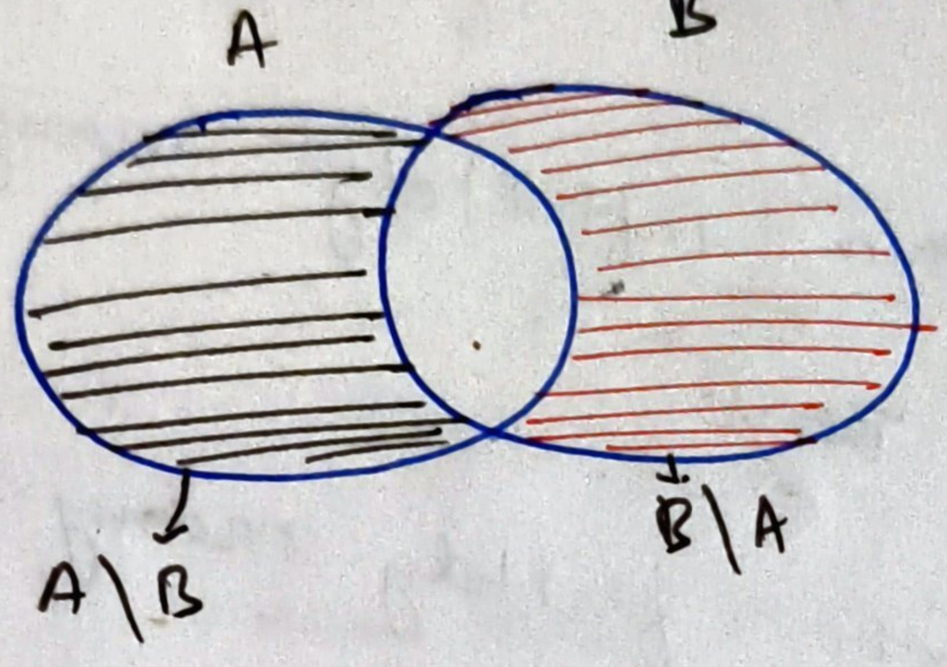
$\Rightarrow r = 0, r = 1.$

ie r is either 0 or 1.

So $R \cong \mathbb{Z}_2$

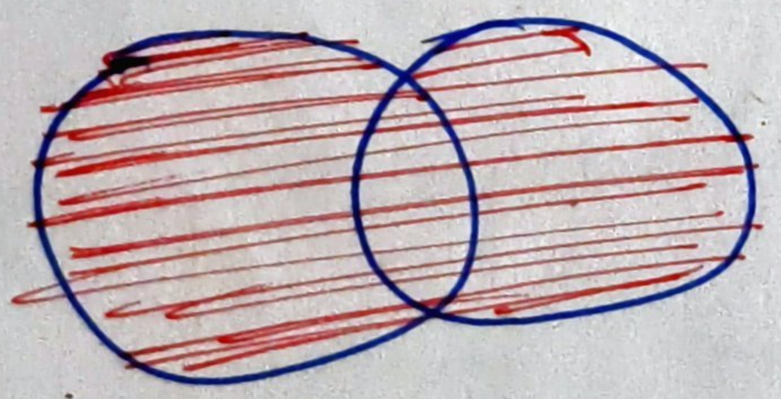
# Symmetric difference properties

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

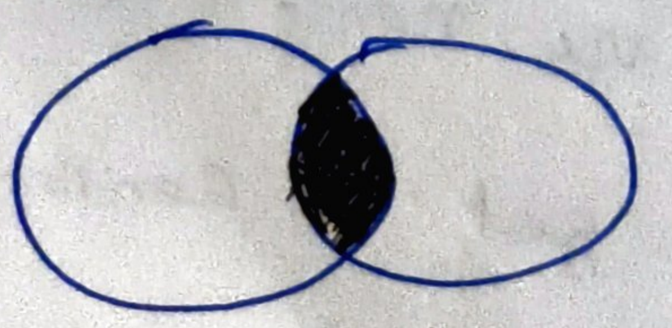


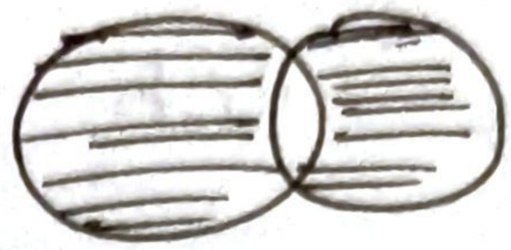

$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

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




$A \cup B - (A \cap B)$



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

$= A \triangle B.$

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

**Q.** Let $X$ be any non-empty set and let $P(X)$ be the set of all subsets of $X$ (the power set of $X$). Define addition and multiplication on $P(X)$ by

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

$$A \times B = A \cap B$$

i.e addition is symmetric difference and multiplication is intersection

(a) prove that $P(X)$ is a ring under these operation $(P(X))$ and its subring are often referred to as ring of sets.

Sol:

1. Commutativity of addition:

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

$$= B \triangle A$$

where $A \Delta B = B \Delta A$.

~~Addition~~

Additive identity :-

$\Rightarrow A \Delta \phi = (A - \phi) \cup (\phi - A)$

$= A \cup \phi$

$= A$

Additive inverse :-

$\Rightarrow A \Delta A = (A - A) \cup (A - A)$

$= \phi \cup \phi = \phi$

So additive inverse of A is A itself.

Associativity :-

$(A \Delta B) \Delta C = A \Delta (B \Delta C)$

Multiplication is distributive with respect to addition

$$(A \triangle B) \triangle C = (A - B) \cup (B - A) \cap C$$

$$= (A \cap C - B \cap C) \cup (B \cap C - A \cap C)$$

$$= (A \cap C) \triangle (B \cap C)$$

$\Rightarrow$ Symmetric difference and intersection of $P(X)$ satisfy every ring axiom

So $P(X)$ is a ring under Symmetric difference and intersection.

(b) Prove that $P(X)$ is a commutative ring with identity and is a Boolean ring.

Soln: $P(X)$ is a commutative ring

Since $A \cdot B = A \cap B = B \cap A = B \cdot A$

$A \cdot E = A \cap I = A$

$A \cdot X = A \cap X = A$ and $X \cdot A = X \cap A = A$

Since $A \cdot B = A \cap B = B \cap A = B \cdot A$

$\Rightarrow$ This implies $P(X)$ is Commutative ring.

$\Rightarrow$ since $A \cdot X = A \cap X = A$

$X \cdot A = X \cap A = A$

This implies $P(X)$ is contain identity

Therefore $P(X)$ is a commutative ring with identity.

$\Rightarrow$ Proof

Now let $S \subseteq X$, then

$(P(S), *, \cap)$ is a commutative ring with unity, in which the unity is $S$.

To show P(X) is a boolean ring.

**Proof:** P(X) denote the set of all subsets of X

i.e the power set of X

P(X) with given operation

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

$$A \times B = A \cap B$$

is isomorphics to the set F of functions

$$X \longrightarrow Z_2$$

where F is endowed with pointwise sum and product for $X_A, X_B \in F$

The characteristic function of a subset A of set X is a function

$$X_A : X \longrightarrow \{0, 1\} \quad \text{defined by}$$

$$X_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Let $B \subset X$

Then (i) $\chi_{A \cap B} = \chi_A \cdot \chi_B$

Proof:- (i) If $x \in A \cap B$, then

$$\chi_A(x) = \chi_B(x) = 1$$

$$\Rightarrow \chi_{A \cap B} = 1$$

$$\Rightarrow x \in A, \; x \in B \Rightarrow \chi_A \cdot \chi_B = 1 \cdot 1 = 1.$$

(ii) if $x \notin A \cap B$, then $\chi_A(x) = 0$,

$$\chi_B(x) = 0$$

$$\Rightarrow \chi_{A \cap B}(x) = 0$$

$$\Rightarrow x \notin A, \; x \notin B \Rightarrow \chi_A \cdot \chi_B = 0 \cdot 0 = 0$$

So $\boxed{\chi_{A \cap B} = \chi_A \cdot \chi_B.}$

(2) $\chi_{A\cup B} = \chi_A + \chi_B - \chi_{A\cap B}$

if $x \in A\cup B$, then $\chi_{A\cup B} = 1$.

$x \in A$, then $\chi_A = 1$.

$x \in B$. then $\chi_B = 1$.

$x \in A\cap B$, then $\chi_{A\cap B} = 1$.

$\chi_{A\cup B} = 1 + 1 - 1 = 1$.

So $\chi_{A\cup B}(x) = x_A + x_B$

$x_{A\cap B}(x) = x_A \cdot x_B$.

Now the isomorphism is given by

$P(X) \cong F$ where $F : X \longrightarrow \mathbb{Z}_2$

This implies $A \cong \chi_A$ where $A \subseteq P(X)$

and $\chi_A \in F$

Hence proved. $\mathbb{Z}_2$ is boolean ring.

By using the theorem, any boolean ring which is also an integral domain is isomorphics to $\mathbb{Z}_2$

Another Easy approach :-

For any $A \in P(X)$, we have

$$A \cdot A = A \cap A = A \times A$$

$$A^2 = A = A \cap A.$$

$\Rightarrow$ Therefore $P(X)$ is boolean ring.

Symmetric difference ring :-

A symmetric difference is a ring formed by the power set of a set where the addition operation is symmetric difference and the multiplication operation is the intersection of sets.

Q. Give an example of infinite Boolean ring.

Soln:

$$R = \prod_{i=1}^{\infty} \mathbb{Z}_2$$

$$R = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2 \dots$$

and $P(X)$ under $A+B = (A-U) \cup (B-A)$

and $A \times B = A \cap B$ operation.

---

The power set (the set of all subsets) of any set $X$, when equipped with symmetric difference as addition and intersection as multiplication forms a ring.

⇒ The empty set ($\phi$) act as the identity element for the symmetric difference

$A \Delta \phi = A$.

**Q.** Prove that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{Q}(\sqrt{D})$

**Soln:**

Here $$\omega = \begin{cases} \sqrt{D} & \text{if } D \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

$$\mathbb{Z}[\omega] = \{a+b\omega : a,b \in \mathbb{Z}\}$$

$$\mathbb{Q}(\sqrt{D}) = \{a+b\sqrt{d} : a,b \in \mathbb{Q}\}$$

**Our motive:** $\mathbb{Z}[\omega]$ is a subring of $\mathbb{Q}(\sqrt{D})$

**Proof:** (i) Clearly $0 \in \mathbb{Z}[\omega]$

(ii) Let $x, y \in \mathbb{Z}[\omega]$, then $x = a+b\omega$

$y = c+d\omega$

where $a,b,c,d \in \mathbb{Z}$

$\Rightarrow x-y = a+b\omega - c-d\omega$

$= (a-c) + (b-d)\omega \in \mathbb{Z}[\omega]$

(iii) Let $x, y \in \mathbb{Z}[\omega]$. then $x = a+b\omega$

$y = c+d\omega$

$\Rightarrow xy = (a+b\omega)(c+d\omega)$

$$xy = (a+b\omega)(c+d\omega)$$

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

$$= ac + ad\omega + bc\omega + bd\omega^2$$

we know $\omega = \frac{1+\sqrt{D}}{2}$.

$$\omega^2 = \frac{1+2\sqrt{D}+D}{4}$$

$$= \frac{2+2\sqrt{D}+D-1}{4}$$

$$\omega^2 = \omega + \frac{D-1}{4}$$

~~Q.E.D~~ $D \equiv 1 \pmod{4}$

Since it is given that

$D = 2, 3 \pmod 4$

$D = 1 \pmod 4$

$$w = \begin{cases} \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \\ \end{cases}$$

$$w^2 = 1 + \frac{D-1}{4}$$

$$= 1 + 1$$

$$w^2 = 2.$$

$\Rightarrow$ $w^2$ is always an integer.

Therefore $xy \in \mathbb{Z}[w]$

Hence $\mathbb{Z}[w]$ is a subring of $\mathbb{Q}(\sqrt{D})$

## RING Homomorphism :-

Let R and S be ring.

A ring ~~homomorphism~~ homomorphism is a function $f: R \longrightarrow S$ such that

(a) for all $x, y \in R$, $f(x+y) = f(x) + f(y)$

(b) for all $x, y \in R$, $f(xy) = f(x) f(y)$

**Note:-** If R and S are ring with 1, then

$$f(1_R) = 1_S.$$

**Example:-** $f: \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$ define by

$$f(x) = x^2.$$

$$f(x+y) = (x+y)^2 = x^2 + 2xy + y^2$$

$$= x^2 + y^2 \quad \{ \text{since } 2 \equiv 0 \pmod 2 \}$$

$$= f(x) + f(y)$$

$$f(xy) = (xy)^2 = x^2y^2 = f(x) f(y)$$

$$\Rightarrow f(1) = 1^2 = 1.$$

f is a ring homomorphism.

Example $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ define by

$$f(x) = 2x$$

$$f(x+y) = 2(x+y)$$

$$= 2x + 2y$$

$$= f(x) + f(y)$$

$$\Rightarrow f(1.3) = f(3) = 2.3 = 6$$

$$\text{where } f(1)\, f(3) = (2.1)(2.3)$$

$$= 12$$

$$\Rightarrow f(1.3) \neq f(1)\, f(3)$$

So f is not a ring homomorphism.

# If $f: Z_n \longrightarrow Z_m$ is a ring homomorphism

then $f(0) = 0$, $n f(1) = 0$, $f(1)^2 = f(1)$.

then $m$ implies $m \mid n$

proof: let us define $f: Z_n \longrightarrow Z_m$

such that $f(x) = ax$

let ~~Take~~ $f(1) = a$.

$f: Z_n \longrightarrow Z_m$

$: x \pmod n \longrightarrow ax \pmod m$.

Assume that there exist a ring homomorphism from $Z_n$ to $Z_m$.

$f(0 \pmod n) = f(n \pmod n)$

$= n f(1 \pmod n)$

$= n f(1)$

$f(0) = n f(1) = na \mod(m)$

Now if $m \mid n$, then $f(0) = 0 \cdot a \pmod m$

$f(0) = 0$

$$f(0) = 0 = n f(0)$$

$f(0) = 0$

and $n f(0) = 0$

$$a = f(1) = f(1^2) = f(1 \cdot 1)$$

$$= f(1) \cdot f(1)$$

$$= a^2 \pmod m$$

Since $f$ is ring homomorphism.

$$f(a.b) = f(a) . f(b)$$

$\Rightarrow$

$\Rightarrow \quad a = a^2 \pmod m$

$\Rightarrow \quad f(1) = (f(1))^2 \pmod m$

## Ideal :-

A subring $I$ of $R$ is a left ideal

if $a \in I$, $r \in R$

$ra \in I$ , $a-b \in I$

So $I$ is closed under subtraction and multiplication on the left by element $r \in R$ i.e element of big ring ($R$)

Similarly we can show right ideal by

if $a \in I$, $r \in R$

$ar \in I$

right.

## Two sided ideal :-

Two side ideal is both a left and ~~right ideal~~

i.e for $a, b \in I$, $r \in R$

$a-b \in I$, ~~$ab \in R$~~ $ar \in I$

$ra \in I$

## Proposition:

(1) Let $R$ be a ring and let $I$ be an ideal of $R$. Then the (additive) quotient group $R/I$ is a ring under the binary operations

$$(r+I) + (s+I) = (r+s) + I$$

and

$$(r+I) \times (s+I) = (rs) + I$$

for all $r, s \in R$.

(1) When $A \subseteq R$, then

$$\frac{A}{I} = \{a + I \mid a \in A\}$$

I be an ideal of R.

group R/I is

ations

+I

+I

}

Note :- Group has one - binary operation

whereas Ring has two binary operation

Every Ring need not be group.

$(\mathbb{Z}, +, \times) = (\mathbb{Z}, +, \cdot)$

Note : $\boxed{\cdot = \times}$ → symbolic meaning.

But $(\mathbb{Z}, \cdot)$ is not group.

since inverse doesn't exist.

$(\mathbb{R}^*, +, \times) = (\mathbb{R}^*, +, \cdot)$ is group)

but $(\mathbb{R}^*, +)$ is not group.

since $x + (-x) = 0 \notin \mathbb{R}^*$

$\Rightarrow (\mathbb{R}, \cdot), (\mathbb{Q}, \cdot)$ are not group.

We concluded that in multiplication operation. Ring don't form group.

In most of the cases, ring doesn't form group under $(\cdot, \times)$ operation

Example, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$ not form groups

But $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ form groups.

## Cosets:

The concept of coset in ring is basically as same in the group theory.

The whole idea of coset in Ring theory is about abelian group under addition.

Because when the ring consist of 0 or ring (R) contain 0, then they don't form a group under multiplication.

Example: $(R, +, \cdot)$ ~~$(\mathbb{Z}, +, \times)$~~, $(\mathbb{Z}, +, \cdot)$

$(Q, +, \times)$

Note: $\boxed{\cdot = \times}$ meaning.

- ~~denote multiplication~~
- denote multiplication.

So Coset is under multiplication operation are not applicable.

$R = (\{0\}, +, \cdot) = (\{0\}, +, \times)$

is Subring of all Ring. ($R'$)

since $0 - 0 = 0 \in R$

$0 \cdot 0 = 0 \in R$.

i/e $R$ is closed under subtraction and multiplication.

## Coset of Ring theory :-

If $I$ is an ideal of a ring $R$ and $a \in R$ then a coset of $I$ is a set of the form $a + I = \{a + s \mid s \in I\}$.

The set of all coset is denoted by

$$\frac{R}{I} = \{a + s \mid s \in I\}.$$

# Given a ring $R$ and a two sided ideal $I$ in $R$ then we can also write

$$\frac{R}{I} = [a] = \{a + s \mid s \in I\}$$

where $[a]$ denote the equivalence class and $a \in R$

i.e $a \in R,\ b \in R$

$\Rightarrow a \sim b$ if and only if $a - b$ is in $I$

~~or cde~~

or we can say

$$[a] = a \bmod I = \{a + s \mid s \in I\}$$

$$= a + I$$

Example:- $\frac{R}{I}$ = Set of equivalence class

where the relation Rs defined

as $a \sim b \Rightarrow (a-b) \in I$

Take $I = R$

Since $r + IR = R$ for any $r \in R$

so $0 + IR = R = r + IR$

$\Rightarrow 0 + IR = r + IR = R.$

Take $a = 0$, then

$= \{0 + r \mid r \in I\}$

$= 0 + I$

$= 0 + IR$ { Since $I = R$ }

$$\frac{\mathbb{R}}{\mathbb{R}} = \{[0]\}$$

Let $[a] = a + R$

$$= a + R = \{a + r \mid r \in R\}.$$

$$= 0 + (a + R)$$

since $a \in R$

so $a + R = R$

$$= [0]$$

$$[a] = [0]$$

$$\Rightarrow \frac{R}{R} \subseteq \{[0]\}$$

$$\Rightarrow \frac{R}{R} \supseteq \{[0]\} \quad \text{(trivial)}$$

Therefore $\frac{R}{R} = \{[0]\}$

# Let (m) and (n) be ideals of the integer Z

Let (d) = (m) + (n)

Then d = gcd (m, n)

Since Z is integer ⇒ m, n and d are integer

i.e Z is Ring of integer

Z is ~~pond~~ principal ideal domain

(m) = mZ , (n) = nZ

(d) = (m) + (n)

= {x ∈ Z : ∃ a, b ∈ Z
x = am + bn }.

(d) is the set of all integer combination of m and n

d = gcd {m, n}

Let R be a ring with identity $1 \neq 0$

② Prove that the ring $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphics

Proof:- Suppose $2\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphics

~~Then we have a ring homomorphism~~

$$f : 2\mathbb{Z} \longrightarrow 3\mathbb{Z}$$

Let $f(2) = 3x$ for some integer $x \in \mathbb{Z}$

this implies generator of $3\mathbb{Z}$ are $-3x$ and $+3x$

Therefore for $f$ to be an isomorphism we must have either

$$f(2) = 3x \text{ or } -3x$$

$$f(4) = f(2+2) = f(2) + f(2)$$

$$= 3x + 3x = 6x$$

$$f(4) = f(2^2) = f(2) \cdot f(2)$$

$$= 3x \cdot 3x = 9x^2$$

$f(4) = f(4)$

$\Rightarrow 6x = 3x^2$

so the integer solution is $x = 0$

$\Rightarrow f(x) = 3x$

$f(2) = 0$

$\Rightarrow f(0) = f(2) = 0$

$f(0) = 0.$

this contradicts $f$ is an isomorphism

$\Rightarrow$ contradict $f$ is an injective

# Assume there exists a ring isomorphism

$\phi : 2\mathbb{Z} \longrightarrow 3\mathbb{Z}$

A ring isomorphism must preserve both addition and multiplication.

$\phi(x+2)$ $x = 2$ in $2\mathbb{Z}$

using addition $\phi(4) = \phi(4+4) = 2\phi(4)$

using multiplication: $\phi(4) = \phi(2 \cdot 2) = (\phi(2))^2$

since $\phi$ is an isomorphism, these two results must be equal

$(\phi(2))^2 = 2\phi(2)$

$\phi\phi$
$(\phi(4-0)$

$f(0) = f(4) = 0$

Q. Prove that the ring $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

Sol^n. Suppose $f : \mathbb{Q}[x] \longrightarrow \mathbb{Z}[x]$ be an isomorphism

Since $f$ is a ring homomorphism, we have

$f(1) = 1$

Now $1 = f(1) = f(2 \cdot \frac{1}{2}) = 2 \cdot f(\frac{1}{2})$

since $f$ is a homomorphism and ~~$f(\frac{1}{2}) \in \mathbb{Z}[x]$~~

$f(\frac{1}{2}) \in \mathbb{Z}[x]$,

$f(\frac{1}{2}) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

$2 f(\frac{1}{2}) = 1 \Rightarrow 2 a_0 = 1 \Rightarrow a_0 = 1/2$.

$\Rightarrow a_n = a_{n-1} = \cdots = a_1 = 0$ ~~and $a_0 = 1$~~

$\Rightarrow a_0 = \frac{1}{2} \notin \mathbb{Z}$, a ~~Contra~~ Contradiction

So $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

**Q** Find all homomorphic images of $\mathbb{Z}$?

**Soln** Since $f: \mathbb{Z} \longrightarrow \mathbb{R}$ is a homomorphism,

then $\frac{\mathbb{Z}}{\ker f} \cong f(\mathbb{Z})$

$\ker f$ is an ideal of $\mathbb{Z}$

any ideal of $\mathbb{Z}$ is of the $n\mathbb{Z} = \langle n \rangle$

so $f(\mathbb{Z}) \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$

Q 8 find all the ring homomorphisms from $\mathbb{Z}$ to $\frac{\mathbb{Z}}{30\mathbb{Z}}$. In each case describe the kernel and the image.

Soln:

In order to be ring homomorphism, we must have $f(1) = (f(1))^2 \mod(30)$

ie $f: \mathbb{Z} \longrightarrow \mathbb{Z}_{30}$ is a ring homomorphism

then $f(1) = (f(1))^2$

The only number that satisfy the properties $x = x^2$ in $\mathbb{Z}_{30}$ are

0, 1, 6, 10, 15, 16, 21, 25

If $f(1) = 0$, then $\ker f = \mathbb{Z}$

If $f(1) = 1$, then $f(n) = f(1 + \cdots + 1)$ (n times)

$= f(1) + f(1) + \cdots + f(1)$

$= n \mod 30$

$$f(n) = n \bmod 30$$

Therefore $\ker f = 30\mathbb{Z}$

similarly if $f(1) = x$ where

$x \in \{6, 10, 15, 16, 21, 25\}$

then $f(n) = f(1 + \ldots + 1)$

$= f(1) + \ldots + f(1) \bmod 30$

$= xn \bmod 30$

$\ker(f) = 5\mathbb{Z}$ if $x = 6$

$\ker f = 3\mathbb{Z}$ if $x = 10$

$\ker f = 2\mathbb{Z}$ if $x = 15$

$\ker f = 15\mathbb{Z}$ if $x = 16$

$\ker f = 10\mathbb{Z}$ if $x = 21$

$\ker f = 6\mathbb{Z}$ if $x = 25$