Ring Theory

(Handwritten Classroom Study Material)

Submitted by
Rahul Anand
(MSc Math Student)
NIT Jalandhar, Punjab

No of Pages: 28

(Provide your Feedbacks/Comments/Suggestions at maths.whisperer@gmail.com)

Ring Theory

☆ Ring :-

A non-empty set R together with two binary operations '+' and '·' is said to be a ring if it satisfies the following conditions :-

(i) $(R,+)$ is an abelian group.
(ii) $(R,\cdot)$ is a semi group.
and (iii) $\forall a,b \in R$, $a(b+c) = ab + ac$

Basic terms :-

'+' → addition
'·' → multiplication
'0' → Additive identity. (zero element)
$-a$ → Additive inverse (negative of a)
1 → multiplicative identity (Unity)
$\frac{1}{a}$ → multiplicative inverse (reciprocal of **a**)

e.g. $(P(N), \Delta, \cap)$
Δ ← + Denoted ($\because (P(N), \Delta) \to$ abelian of operation Δ)
$\cap$ ← · Denoted

$0 \to \phi$
$1 \to N$

☆ Unit :-

An element $a \in R$ is said to be a unit of R.
If $\exists\, b \in R$ s.t. $a \cdot b = 1 = b \cdot a$

i.e. 'a' is a unit of R iff 'a' has a multiplicative inverse in R.

E.g.: ① $(\mathbb{Z}, +, \cdot)$ is a ring.

as (i) $(\mathbb{Z}, +)$ is an abelian group.

(ii) $(\mathbb{Z}, \cdot)$ is a semigroup.

(iii) $\forall a, b, c \in \mathbb{Z}$, $a(b+c) = ab + ac$

Units in $\mathbb{Z}$ are 1 and -1 only. [or $U(\mathbb{Z}) = C_2 \leftarrow (C_2, \cdot)$]

② $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings.

$U(\mathbb{Q}) = \mathbb{Q}_0$, $U(\mathbb{R}) = \mathbb{R}_0$, $U(\mathbb{C}) = \mathbb{C}_0$

③ $(M_n(\mathbb{R}), +, \cdot)$ is a ring.

unit $\leftarrow U(M_n(\mathbb{R})) = GL_n(\mathbb{R})$

④ $(\mathbb{Z}_n, +_n, \times_n)$ is a ring.

Unit of $\mathbb{Z}_n \leftarrow U(\mathbb{Z}_n) = U(n)$

$\rightarrow$ group of $U(n) \rightarrow \times_n$

⑤ $(F(D), +, \cdot)$ is a ring. where

$F(D) := \{ f \mid f : D \to \mathbb{R} \text{ is a function} \}$

$\therefore$ zero element $\div$ zero function

Unity $\div$ $f(x) = 1$, $\forall x \in D$

Unit $\div$ $\{ f \mid f \in F(D)$ & $0 \notin R_f \}$

$f \in F(D)$

$0 \in R_f \Rightarrow \exists x \in D$ s.t. $f(x) = 0$

$\therefore \frac{1}{f}(x) = \frac{1}{f(x)} = $ D.N.E. in $\mathbb{R}$.

In general, $(F(D), +, \cdot)$ is a ring iff the Codomain of functions of $F(D)$ is a ring.

(6) $(C(\mathbb{R}), +, \cdot)$, $(C'(\mathbb{R}), +, \cdot)$, $(C''(\mathbb{R}), +, \cdot)$, ...

$(C^n(\mathbb{R}), +, \cdot)$ are rings:

where

$C^n(\mathbb{R}) := \{ f \mid f: \mathbb{R} \to \mathbb{R}$ is a function where $f^{(n)}$ is continuous $\}$

Unit :- $\{ f \mid f \in C(\mathbb{R})$ & $0 \notin R_f \}$

(7.) If R is a ring then

$R[x] :=$ The set of all polynomials in x whose coefficients are elements of R.

is a ring of polynomials.

Zero element :- zero polynomial.

Unity :- $P(x)$

E.g. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_n[x]$, $\mathbb{R}[x]$, $M_n(\mathbb{R})[x]$ are examples of polynomial ring.

(8.) If R is a ring then

$R[x, y]$ is a polynomial ring in two variables x and y.

where

$P(x, y) \in R[x, y]$ is defined as

$$P(x, y) = P_0(x) + P_1(x)y + P_2(x)y^2 + \cdots + P_n(x)y^n$$

$$= q_0(y) + q_1(y)x + q_2(y)x^2 + \cdots + q_n(y)x^n$$

$\therefore R[x, y] = R[x][y] = R[y][x]$

Unit of polynomial is same as ring of ~~poly~~ Unit.

E.g. $p(x,y) = xy^2 + 2xy + x^3y$

$= (y^2+2y)x + x^3y$

$= p(y)x + p(x)y$

(9.) If $a \notin R$ then $R[a]$ is a ring.

where $R[a] := \{a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n \mid a_i \in R\}$

E.g. $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Q}[i]$, $\mathbb{Z}_n[i]$ are rings.

$\because \sqrt{2}$ is place value

$a+b\sqrt{2}$, $a+_n b\sqrt{2}$ $\to (a,b)$

Where

$\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$

$\mathbb{Q}[i] = \{a+bi \mid a,b \in \mathbb{Q}\}$

$\mathbb{Z}_n[i] = \{a +_n bi \mid a,b \in \mathbb{Z}_n\}$

(10.) **Quaternian Ring:**

$Q_R = \{a+bi+cj+dk \mid a,b,c \in R,\ i,j,k \in Q_8\}$

wher R is a ring.

Addition: $(a_1+b_1 i+c_1 j+d_1 k) + (a_2+b_2 i+c_2 j+d_2 k)$

$= (a_1+a_2) + (b_1+b_2)i + (c_1+c_2)j + (d_1+d_2)k$

Identity $= 0 = 0+0i+0j+0k$

Inverse $= -(a+bi+cj+dk)$

$= -a-bi-cj-dk$

Multiplication :-

$$(a_1+b_1i+c_1j+d_1k)(a_2+b_2i+c_2j+d_2k)$$

$$= a_1a_2 + b_1a_2 i + c_1a_2 j + d_1a_2 k$$
$$- b_1b_2 + a_1b_2 i + d_1b_2 j - c_1b_2 k$$
$$- c_1c_2 - d_1c_2 i + a_1c_2 j + b_1c_2 k$$
$$- d_1d_2 + c_1d_2 i - b_1d_2 j + a_1d_2 k$$

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (b_1a_2 + a_1b_2 - d_1c_2 + c_1d_2) i$$
$$+ (c_1a_2 + d_1b_2 + a_1c_2 - b_1d_2) j + (d_1a_2 - c_1b_2 + b_1c_2 + a_1d_2) k \quad \text{---} (*)$$

Unity $= 1 = 1 + 0i + 0j + 0k$

Unit:- $= \dfrac{1}{a+bi+cj+dk}$

$$= \frac{a-bi-cj-dk}{(a+bi+cj+dk)(a-bi-cj-dk)}$$

$\Rightarrow$ put $a_2 = a_1$, $b_2 = -b_1$, $c_2 = -c_1$, $d_2 = -d_1$ in eqn $(*)$

$$= \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

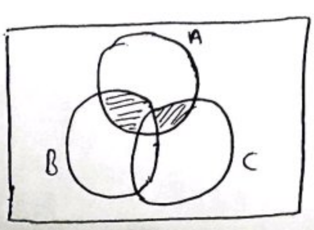
So, If $a^2+b^2+c^2+d^2 \neq 0$ then $a+bi+cj+dk$ is a unit.

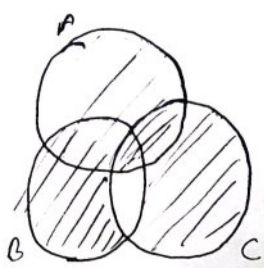
(11) If S is a non-empty set then $(P(S), \Delta, \cap)$ is a ring.

But $(P(S), \Delta, \cup)$ is not a ring.

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

But $A \cup (B \Delta C) \neq (A \cup B) \Delta (A \cup C) \rightarrow$





(12) $(\mathbb{R}^+, \cdot, *)$ where $a*b = a^{\log b}$

(i) $(\mathbb{R}^+, \cdot)$ is an abelian group.

(ii) $a*b = a^{\log b} = e^{(\log a)(\log b)} \in \mathbb{R}^+$

$\therefore a*b \in \mathbb{R}^+$

(iii) $a*(b*c) = a*b^{\ln c}$ $\quad [\because a^x = e^{x \ln a}]$

$= a*e^{(\log b)(\log c)}$

$= a^{(\log b)(\log c)}$

$= e^{(\log a)(\log b)(\log c)}$

Now, $(a*b)*c = a^{\log b} * c$

$= e^{(\log a)(\log b)} * c$

$= \left(e^{(\log a)(\log b)}\right)^{\log c}$

$= e^{(\log a)(\log b)(\log c)}$

$\therefore a*(b*c) = (a*b)*c$

(iv) $a*(b\cdot c) = a^{\log(bc)} = a^{\log b + \log c}$

$= a^{\log b} \cdot a^{\log c}$

$= (a*b)\cdot(a*c)$

☆ Types of Rings :-

(5)
① Commutative Ring :- A ring $(R,+,\cdot)$ is said to be Commutative.

If $\forall a,b \in R$, $ab = ba$ (only chake $\cdot$ ← operation)

E.g. ⇒ $(\mathbb{Z},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ are Commutative ring.

⇒ $(M_n(\mathbb{R}),+,\cdot)$ is not a Commutative ring.

⇒ $(P(S),\Delta,\cap)$ is a Commutative ring.

⇒ Quaternian ring is a not a Commutative ring.

~~⇒ R[x]~~
⇒ $R[x]$ is a Commutative ring iff R is a ~~Commutati~~ Commutative ring.

⇒ $(F(R),+,\cdot)$ is Commutative iff R (Co-domain) is Commutative.

(3)
② Ring with unity :- A ring $(R,+,\cdot)$ is said to be a ring with unity.

If $\exists\, 1_R \in R$ s.t. $\forall a \in R$, $a\cdot 1_R = a = 1_R\cdot a$

where 1_R is Called the unity of ring R.

⇒ If a ring $(R,+,\cdot)$ does not have unity then it is Called a ring without unity.

E.g. $\Rightarrow$ $(\mathbb{Z},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(M_n(\mathbb{R}),+,\cdot)$, Quaternian ring are rings with unity.

$\Rightarrow$ $(2\mathbb{Z},+,\cdot)$, $(3\mathbb{Z},+,\cdot)$, $(n\mathbb{Z},+,\cdot)$ are rings without unity.

$\Rightarrow$ $\left(\left\{\begin{bmatrix} a & a \\ a & a\end{bmatrix} \middle| a\in\mathbb{R}\right\},+,\cdot\right)$ is a ring with unity. $\left(\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2}\end{bmatrix}\right)$

$\Rightarrow$ $\left(\{0,2,4,6,8\},+_{10},\times_{10}\right)$ is a ring with unity 6.

$2\mathbb{Z}=\{0,\pm 2,\pm 4,\pm 6,\ldots\}$

$(2n)\cdot(2m)=2n$

$\Rightarrow m=\frac{1}{2}\notin\mathbb{Z}$

$\therefore 2m\notin 2\mathbb{Z}$

$\Rightarrow$ $R[x]$ is a ring with unity iff R is a ring with unity.

and unity of $R[x]$ = unity of R.

$\Rightarrow$ $M_n(2\mathbb{Z})$ is a ring without unity.

3+5

(3) Commutative ring with unity (CRU): A ring $(R,+,\cdot)$ is said to be Commutative (~~i.e. $\forall a,b\in R$, $ab=ba$~~) ring with unity.

If R is Commutative (i.e. $\forall a,b\in R$, $ab=ba$)
and R has Unity (i.e. $\exists\, 1_R\in R$ s.t. $a\cdot 1_R=a=1_R\cdot a,\ \forall a\in R$)

Eg. $\Rightarrow$ $(\mathbb{Z},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $\cancel{(M_n(\mathbb{Z}),+,\cdot)}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$ etc. are CRU.

$\Rightarrow$ $(2\mathbb{Z},+,\cdot)$, $(n\mathbb{Z},+,\cdot)$ are Commutative ring without unity.

$\Rightarrow$ Quaternian ring is a non-commutative ring with Unity.

$\Rightarrow$ $R[x]$ is a CRU iff R is a CRU

$\Rightarrow$ $(\mathbb{Z}_n, +_n, \times_n)$ is a CRU.

$\Rightarrow$ $\mathbb{Z}[i]$, $\mathbb{Q}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}]$ etc. are CRU.

$\Rightarrow$ $(M_n(\mathbb{R}),+,\cdot)$ is a non-commutative ring with unity.

(4.) **Division Ring or Skew Field :**

A ring $(R,+,\cdot)$ is said to be a division ring

iff (i) R has unity 1_R

and (ii) Every non-zero element of R is a unit.

i.e. $\forall a \in R$, $a \neq 0$, $\exists\, b \in R$ s.t. $a\cdot b = 1_R = b\cdot a$

(Multiplicative inverse exists है)

Eg. $\Rightarrow$ $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C}, \cancel{\mathbb{R}}+,\cdot)$ are division ring.

$\Rightarrow$ $(M_n(\mathbb{R}),+,\cdot)$ is not a division ring.

$\Rightarrow$ $\left(\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} \,\middle|\, a \in \mathbb{R}\right\},+,\cdot\right)$ is a division ring.

$\Rightarrow$ $(\mathbb{Z}_p, +_p, \times_p)$ is a division ring. where $p \Rightarrow$ prime.

$\Rightarrow$ $R[x]$ is never a division ring. $\rightarrow$ $\boxed{(ax+b)q(x)=1 \quad q(x)=\frac{1}{ax+b} \leftarrow \text{Not a poly.}}$

$\Rightarrow$ $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$ are not division ring.

$\Rightarrow$ $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$. are not division ring. $\rightarrow$ $\boxed{3+4i = \frac{3-4i}{25} \Rightarrow \frac{3}{25}-\frac{4}{25}i \notin \mathbb{Z}[i]}$

$\Rightarrow$ $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ are division ring.

$\Rightarrow$ $(\{0,2,4,6,8\}, +_{10}, \times_{10})$ is a division ring.

$\Rightarrow$ Quaternian ring is a division ring.

$$(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

☆ **Field** :-

A Commutative division ring is Called a field.

or A CRU $(F,+,\cdot)$ is said to be a fied if every non-zero element of F is a unit.

or An algebraic Structure $(F,+,\cdot)$ is said to be a field if (i) $(F,+)$ is an abelian group.

(ii) $(F^*,\cdot)$ is an abelian group. $(F^* = F\setminus\{0\})$

(iii) $\forall a,b,c \in F$, $a(b+c) = ab+ac$.

Eg. $(\mathbb{R}^+, \cdot, *)$ where $a*b = a^{\log b}$

$\rightarrow$ (i) $(\mathbb{R}^+,\cdot) \rightarrow$ abelian group.

zero element = 1

Multiplication $(*)$:-

① closure :- $\forall a,b \in \mathbb{R}^+$, $a*b = a^{\log b} \in \mathbb{R}^+$

② <u>Associative</u> :- $\forall a,b,c \in \mathbb{R}^+$

$$a*(b*c) = e^{\ln a(\ln b \ln c)}$$
$$(a*b)*c = e^{(\ln a \ln b)\ln c}$$

③ <u>Unity</u> :- $a*b = a$

$\Rightarrow a^{\log b} = a$

$\Rightarrow \log b = 1$

$\Rightarrow b = e \approx 2.71$

$\Rightarrow b*a = a$

$\Rightarrow b^{\log a} = a$

$\Rightarrow a^{\log b} = a$

$\Rightarrow \log b = 1$

$\Rightarrow b = e \approx 2.71$

$\boxed{\because a^{\log b} = b^{\log a}}$

④ <u>Inverse</u> :- Let $a*b = e$

$$a^{\log b} = e$$
$$e^{\ln a \cdot \ln b} = e$$
$$(\ln a)(\ln b) = 1$$
$$\ln b = \frac{1}{\ln a}$$

<u>Eg.</u> $\Rightarrow$ $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are fields. [$\because U(F) = F^*$]

$\Rightarrow$ $(\mathbb{Z},+,\cdot)$ is not a field. [$\because U(\mathbb{Z}) = C_2\{\} \{1,-1\}$]

$\Rightarrow$ Zero ring $\{0\}$ is not a field.

$\Rightarrow$ $(\mathbb{Z}_n, +_n, \times_n)$ is a field iff n is a prime.

($\because U(\mathbb{Z}_n) = U(n)$
So, $\forall k \in \mathbb{Z}_n$, $k \neq 0$, $k \in U(n)$ iff n is a prime)

$\Rightarrow$ $F[x]$ is never a field where F is a field.

$\Rightarrow$ $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ etc. are not field.

$\Rightarrow$ $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ are field.

$\Rightarrow$ $(M_n(\mathbb{R}), +, \cdot)$ is not a field.

But $\left(\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| a \in \mathbb{R}\right\}, +, \cdot\right)$ is a field.

$\Rightarrow$ $\mathbb{Z}_{10}$ is not a field.

But $(\{0, 2, 4, 6, 8\}, +_{10}, \times_{10})$ is a field.

$\Rightarrow$ Quaternian ring is not a field.

$\Rightarrow$ $\mathbb{Z}_p[i]$ is a field iff $p \equiv 3 \pmod 4$ (i.e. $4 \mid (P-3)$) where $p \to$ prime

$$\mathbb{Z}_p[i] := \{a + ib \mid a, b \in \mathbb{Z}_p\}$$

$$(a+ib)(c+id) = 1$$

$$c + id = \frac{a-ib}{a^2+b^2}$$

$$= \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$$

$\frac{1}{a^2+b^2}$

$\forall\ a, b \in \mathbb{Z}$

(i) Both are even.

$a = 2m$, $b = 2n$.

$a^2+b^2 = (2m)^2 + (2n)^2$

$= 4(m^2+n^2)$

(ii) a is even & b is odd.

$a = 2m$, $b = 2n+1$

$a^2+b^2 = (2m)^2 + (2n+1)^2$

$= 4m^2 + 4n^2 + 4n + 1$

$= 4(m^2+n^2+n) + 1$

(iii) Both are odd.

$a = 2m+1$, $b = 2n+1$

$a^2+b^2 = (2m+1)^2 + (2n+1)^2$

$= 4m^2 + 4m + 1 + 4n^2 + 4n + 1$

$= 4(m^2+n^2+m+n) + 2$

$\Rightarrow \forall\ a, b \in \mathbb{Z}$, $a^2+b^2 \neq 4K+3$ for any $K \in \mathbb{Z}$

So, If p is a prime s.t. $p = 4K+3$

then $p \neq a^2+b^2$

So $a^2+b^2 \neq 0$ in $\mathbb{Z}_p$, except $(a = 0 = b)$

So, $\frac{1}{a^2+b^2}$ exists in $\mathbb{Z}_p$.

So, $\mathbb{Z}_3[i]$, $\mathbb{Z}_7[i]$, $\mathbb{Z}_{11}[i]$ are fields.

But $\mathbb{Z}_5[i]$, $\mathbb{Z}_{13}[i]$, $\mathbb{Z}_{17}[i]$ are not fields.

$4+3i$, $1+2i$, $5+12i$

★ Units of a ring : An element 'a' of a ring R is said to be a unit. if it has multiplicative inverse in R.

$U(R) :=$ The set of all the units of a ring R.

(i) 0 is never a unit.

(ii) Unity is always a unit.

(iii) If a is a unit of R then a^{-1} is also a unit of R

$\because a \in U(R) \Rightarrow \exists b \in R$ s.t. $ab = 1_R = ba \Rightarrow b \in U(R)$

(iv) If a is unit of R then $-a$ is a unit of R.

$\because a \in U(R) \Rightarrow \exists b \in R$ s.t. $ab = 1_R = ba$

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

(v) If a and b are units of R then $ab \in U(R)$.

$\because a \in U(R) \Rightarrow \exists x \in R$ s.t. $ax = 1 = xa$

$b \in U(R) \Rightarrow \exists y \in R$ s.t. $by = 1 = yb$

$\therefore (ab)(yx) = a(by)x = a \cdot 1 \cdot x = ax = 1$

$(yx)(ab) = y(xa)b = y \cdot 1 \cdot b = yb = 1$

$\therefore ab$ is a unit.

(vi) If a and b are units then $a+b$ need not be a unit.

Eg. If $a \in U(R)$, $-a \in U(R)$

But $a+(-a) = 0 \notin U(R)$

(vii) The set of all units of a ring R is a group under multiplication operation.

Examples:-

$U(\mathbb{Z}) = C_2 = \{1,-1\}$

$U(\mathbb{Z}_n) = U(n)$

$U(\mathbb{Z}_p) = U(p)$

$U(\mathbb{Q}) = \mathbb{Q}_0$

$U(\mathbb{R}) = \mathbb{R}_0$

$U(\mathbb{Z}[i]) = \{1,-1,i,-i\} = C_4$

$U(\mathbb{Q}[i]) = \cancel{\mathbb{Q}_0[i]}\ \mathbb{Q}[i] \setminus \{0\}$

$U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1,-1\}$

$U(\mathbb{R}[x]) = U(\mathbb{R}) = \mathbb{R}_0$

$U(M_n(\mathbb{R})) = GL_n(\mathbb{R})$

$U(P(\mathbb{N}), \Delta, \cap) = \{\mathbb{N}\} \approx \mathbb{Z}_1 \quad [\because A \cap B = \mathbb{N}]$

Q. If R is a commutative ring with unity 'a' is a unit of R and $b \in R$ s.t. $b^2 = 0$ then show that $a+b$ is unit.?

Solⁿ:- 'a' is a unit $\Rightarrow \exists\, c \in R$ s.t. $ac = 1 = ca$

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

$= 1 - 0 = 1 \quad (\because b^2 = 0)$

$\therefore (a+b)^{-1} = (a^{-1} - ba^{-2})$ So, $a+b$ is a unit.

★ Direct product of rings :-

If $R_1, R_2, R_3, \ldots, R_n$ are ~~ring~~ rings then $\cancel{R_1 \times R_2 \times \cdots \times R_n}$:-

$R_1 \times R_2 \times \cdots \times R_n := \{(r_1, r_2, \ldots, r_n) \mid r_i \in R_i\}$ is a ring.

⇒ $R_1 \times R_2 \times \cdots \times R_n$ is a ring with unity, iff each R_i is a ring with unity. ⇔ provided R_i is not a zero ring.

⇒ $R_1 \times R_2 \times \cdots \times R_n$ is a commutative ring iff each R_i is a commutative ring.

⇒ $R_1 \times R_2 \times \cdots \times R_n$ is a CRU iff each R_i is a CRU.

⇒ If R_1 and R_2 are division rings then $R_1 \times R_2$ is never a division ring.

⇒ If R_1 and R_2 are fields then $R_1 \times R_2$ is never a field.

Special Case :- Zero ring :- $(\{0\}, +, \cdot)$ does not have unity.

⇒ So, zero ring is commutative ring without unity.

~~→ If~~

⇒ If R is a ring with unity then $R \times \{0\}$ is a ring with unity $(1_R, 0)$.

$\because \forall (a,0) \in R \times \{0\}, \quad (a,0)\cdot(1_R, 0) = (a,0)$

⇒ If $R_1, R_2, \ldots, R_n$ are rings then

$$U(R_1 \times R_2 \times \cdots \times R_n) = U(R_1) \times U(R_2) \times \cdots \times U(R_n)$$

Eg: $|U(\mathbb{Z} \times \mathbb{Z}[i] \times \mathbb{Z}_3[i])| = |U(\mathbb{Z}) \times U(\mathbb{Z}[i]) \times U(\mathbb{Z}_3[i])|$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$

~~$\{1,-1\} \times \{1,-1,i,-i\} \times \{1,\omega,\omega^2\}$~~

$|U(\mathbb{Z})| \times |U(\mathbb{Z}[i])| \times |U(\mathbb{Z}_3[i])|$

$= |C_2| \times |C_4| \times |\ |$

$= 2 \times 4 \times 8$

$= 64$

$\because \mathbb{Z}_3[i] = \{a+ib \mid a,b \in \mathbb{Z}_3\}$

$\therefore |\mathbb{Z}_3[i]| = 9$

Non-zero → 8

$\boxed{\begin{array}{l} \star\ |\mathbb{Z}_n[i]| = n^2 \\ |\mathbb{Z}_p[i]| = p^2 \end{array}}$

★ **Zero divisor :-** A non-zero element 'a' of a ring R is said to be a zero divisor of R.

if $\exists\, b \in R,\ b \neq 0$ and $a \cdot b = 0$ or $b \cdot a = 0$

Eg. → 2 and 3 are zero divisors of $\mathbb{Z}_6$.

→ 4 is a zero division of $\mathbb{Z}_6$.

→ $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ are zero divisors of $M_2(\mathbb{Z})$.

→ $R = F([0,1], \mathbb{R})$

$f(x) = \begin{cases} 1 & , 0 \le x \le \frac{1}{2} \\ 0 & , \frac{1}{2} < x \le 1 \end{cases}$ ← any function , $g(x) = \begin{cases} 0 & , 0 \le x \le \frac{1}{2} \\ 1 & , \frac{1}{2} < x \le 1 \end{cases}$

any function ($\sin x$, $\ln x$) etc.

then $f \neq 0$, $g \neq 0$ But

$f \cdot g = 0$

→ $R = C[0,1]$, $C : [0,1] \to [0,1]$

$f(x) = \begin{cases} x - \frac{1}{2} & , 0 \le x < \frac{1}{2} \\ 0 & , \frac{1}{2} \le x \le 1 \end{cases}$, $g(x) = \begin{cases} 0 & , 0 \le x < \frac{1}{2} \\ x - \frac{1}{2} & , \frac{1}{2} \le x \le 1 \end{cases}$

then $f \neq 0$, $g \neq 0$ But $f \cdot g = 0$

→ $R = C^n[0,1]$

$f(x) = \begin{cases} (x-\frac{1}{2})^{n+1} & , 0 \le x < \frac{1}{2} \\ 0 & , \frac{1}{2} \le x \le 1 \end{cases}$, $g(x) = \begin{cases} 0 & , 0 \le x < \frac{1}{2} \\ (x-\frac{1}{2})^{n+1} & , \frac{1}{2} \le x \le 1 \end{cases}$

then $f \neq 0$, $g \neq 0$ But $f \cdot g = 0$.

★⇒ If R_1 and R_2 are two rings each having non-zero elements then $R_1 \times R_2$ has zero divisors.

∵ as, Let $a \in R_1, a \neq 0$ \& $b \in R_2, b \neq 0$

then $(a,0) \in R_1 \times R_2$
$(0,b) \in R_1 \times R_2$

and $(a,0) \cdot (0,b) = (0,0)$

→ $\mathbb{Z} \times \{0\}$ does not have any zero divisor.

★⇒ If 'a' is a zero divisor of a ring R then 'a' can never be a unit.

proof:— Let a be a zero divisor.

⇒ $\exists\ b \in R$, $b \neq 0$ s.t. $ab = 0$

If 'a' is a unit then $\exists\ c \in R$, $b \neq 0$

and $a \cdot c = 1 = c \cdot a$

$\Rightarrow (c \cdot a) b = 1 \cdot b$

$\Rightarrow c(ab) = b$

$\Rightarrow c \cdot 0 = b$

$\Rightarrow b = 0$

But $b \neq 0$, So, 'a' can never be a unit.

★ $\Rightarrow$ If 'a' is a unit of R then 'a' can never be a zero divisor.

Proof:- $\because$ 'a' is a unit of R

So, $\exists\ c \neq 0$, $c \in R$ s.t.

$a \cdot c = 1 = c \cdot a$

Now, If 'a' is a zero divisor

then $\exists\ b \in R$, $b \neq 0$ and $ab = 0$

If $ab = 0$

$\Rightarrow c(ab) = c \cdot 0$

$\Rightarrow (ca)b = 0$

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow b = 0$

then, a can never be a zero divisor.

★ $\Rightarrow$ There may be elements in a ring which are neither units nor zero divisors.

E.g. $\rightarrow$ 0 is ~~never~~ neither a unit nor a zero divisor.

$\rightarrow$ Every element of $\mathbb{Z}$ ~~exist~~ except 1 and -1 is neither a unit nor a zero divisor.

☆⇒ Every non-zero element of a finite ring is either a zero divisor or a unit.

Q. Find the zero divisors in $(P(S), \Delta, \cap)$?

Sol^n:- Unity $= S$

Zero element $= \phi$

Unit $= S$ ← If $A \neq S$, $A \in P(S)$

$A \cap B \neq S$, $\forall B \in P(S)$

Zero divisor $= P(S) \setminus \{\phi, S\}$

If $A \in P(S)$, $A \neq \phi$, $A \neq S$

then $A \cap A^c = \phi$ But $A \neq \phi$ and $A^c \neq \phi$ $(\because A \neq S)$

Q. The units of $M_n(\mathbb{Z})$?

Sol^n:- Units of $M_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}$

$\Rightarrow \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}$ is not a unit in $M_2(\mathbb{Z})$.

↳ is not a zero divisor.

$\boxed{AB = 0}$

$\Rightarrow A^{-1}(AB) = 0$

$\Rightarrow B = 0$

⇒ The zero divisor of $M_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = 0, A \neq 0\}$

∴ elements of $M_n(\mathbb{Z})$ having determinant other than $0, 1, -1$ are neither units nor zerodivisor.

☆ Every non-zero matrix of $M_n(\mathbb{F})$ is either a unit or a zero divisor. where $\mathbb{F}$ is a field.

☆ Let $(R,+,\cdot)$ be a ring and S be a nonempty set then

$$\text{Let } R_S := \{ f \mid f : S \to R \text{ is a function} \}$$

If R is a CRU then R_S is a CRU.

→ $U(R_S) := \{ f \in R_S \mid f(S) \subseteq U(R) \}$ where $U(R)$ is the set of units of R.

Unit

$0 \notin f(S)$

$$\left(\because \frac{1}{f}(x) = \frac{1}{f(x)}, \forall x \in S \right)$$

→ Zerodivisors of $R_S = \{ f \in R_S \mid f \not\equiv 0$ and $f(x)$ Contains 0 or a zerodivisor of $R \}$

e.g. $f : [0,1] \to \mathbb{Z}_{10} \to \{1,3,7,9\}$

$$f(x) = \begin{cases} 1, & 0 \le x \le \frac{1}{3} \\ 7, & \frac{1}{3} < x \le \frac{1}{2} \\ 9, & \frac{1}{2} < x \le 1 \end{cases} \qquad g(x) = \frac{1}{f}(x) = \begin{cases} 1, & 0 \le x \le \frac{1}{3} \\ 3, & \frac{1}{3} < x \le \frac{1}{2} \\ 9, & \frac{1}{2} < x \le 1 \end{cases}$$

units

$$\therefore fg(x) \equiv 1 \quad \forall x \in [0,1]$$

zero divisors → $f(x) = \begin{cases} 0, & 0 \le x \le \frac{1}{3} \\ 4, & \frac{1}{3} < x \le \frac{1}{2} \\ 6, & \frac{1}{2} < x \le \frac{3}{4} \\ 8, & \frac{3}{4} < x \le 1 \end{cases}$, $g(x) = \begin{cases} 7, & 0 \le x \le \frac{1}{3} \\ 5, & \frac{1}{3} < x \le \frac{3}{4} \\ 0, & \frac{3}{4} < x \le 1 \end{cases}$

☆ If $R_S = \{f \mid f: S \to R$ is a function$\}$

If every non-zero element of R is either a unit or a zerodivisor then every nonzero element of R_S is either a unit or a zerodivisor

☆ If R has an element which is neither unit nor zerodivisor then R_S has an element which is neither unit nor a zerodivisors.

E.g. $\mathbb{Z}_{[0,1]} := \{f: [0,1] \to \mathbb{Z} \mid f$ is a function$\}$

then $f(x) = \begin{cases} 2, & 0 \le x \le \frac{1}{2} \\ 3, & \frac{1}{2} < x \le 1 \end{cases}$ is neither a zerodivisor nor a unit of R_S.

☆ If R is a field then

→ $U(R_S) = \{f \in R_S \mid f(x) \in R^*, \forall x \in S\}$

→ Zerodivisors of $R_S = \{f \in R_S \mid f \neq 0$ and $0 \in f(S)\}$

☆ $C^0(\mathbb{R}) := \{f \mid f: \mathcal{D} \to \mathbb{R}$ is a Continuous function$\}$.

→ $U(C^0(\mathbb{R})) = \{f \mid f: \mathcal{D} \to \mathbb{R}_0$ is continuous$\}$.

→ f is a zerodivisor of $C^0(\mathbb{R})$ if

$f(x) = \begin{cases} f_1(x), & x \in \mathcal{D}_1 \\ 0, & x \in \mathcal{D}_2 \end{cases}$, $g(x) = \begin{cases} 0, & x \in \mathcal{D}_1 \\ f_2(x), & x \in \mathcal{D}_2 \end{cases}$

provided both $f(x)$ and $g(x)$ are continuous.

Q: If $f \in C^0(\mathbb{R})$ such that f has finitely many zeroes in $\mathbb{R}$.

$f : \mathbb{R} \to \mathbb{R}$

$f(x) = x(x-1)(x-2)$ — $0, 1, 2$

$$g(x) = \begin{cases} 0 & , x \neq 0,1,2 \\ 1 & , x = 0 \\ 2 & , x = 1 \\ 3 & , x = 2 \end{cases}$$

But then $g(x)$ is not Continuous.

So, $g(x) \notin C^0(\mathbb{R})$

∴ If $f \in C^0(\mathbb{R})$ such that $f(x) = 0$ at atleast one and atmost Countable points.
then f is neither a zerodivisor nor a unit of $C^0(\mathbb{R})$.

Hence, if $f \in C^0(\mathbb{R})$ is a zerodivisor then f must be zero at uncountable number of points.

Eg: $f(x) = \sin x$ is neither a zero divisor nor a unit.

$= x^2+1$, unit.

$= x^2+x+1$, unit

$= x^2-x+1$, unit

$= e^x$, unit

$= \tan^{-1}(x)$, neither unit nor zero divisor (only $=0$)

$= x^2-1$, ,,

★ Properties of zero divisors :-

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

① If 'a' is a zerodivisor of R then

(i) $-a$ is a zerodivisor of R.

(ii) na is " "

(iii) a^n is " " ", $n \in \mathbb{N}$.

proof:- If 'a' is a zerodivisor of R

then $\exists\, b \in R$, $b \neq 0$ s.t. $ab = 0$

$\therefore (-a)b = -(ab) = -0 = 0$

and $(na)(b) = (a+a+ \cdots +a)b$
$= ab + ab + \cdots + ab$
$= 0 + 0 + \cdots + 0 = 0$

and $a^n b = (a \cdot a \cdots a)b$
$= (a \cdot a \cdots a)(a \cdot b)$
$= (a \cdot a \cdots a) \cdot 0 = 0$

② If a and b are two zero divisors of R then

(i) $a+b$ need not be zerodivisor of R. (Eg. $2, 3 \in \mathbb{Z}_6 \rightarrow 2+3 = 5$)

(ii) ab or ba is a zerodivisor of R.

$db = 0$, $bd \neq 0$
$ac = 0$, $ca \neq 0$

(R → commutative) ab ba

No. of zerodivisors of $\mathbb{Z}_m \times \mathbb{Z}_n = mn - \phi(m)\phi(n) - 1$

$\because |U(\mathbb{Z}_m \times \mathbb{Z}_n)| = |U(\mathbb{Z}_m)|\,|U(\mathbb{Z}_n)|$
$= \phi(m)\,\phi(n)$

$\because \mathbb{Z}_m \times \mathbb{Z}_n$ is a finite ring with unity.

E.g. $R = \mathbb{Z}_5 \times \mathbb{Z}_7 \rightarrow 35 - 4\times 6 - 1 = 10$

Zerodivisors:-
$(0,1), (0,2), (0,3), (0,4), (0,5), (0,6)$
$(1,0), (2,0), (3,0), (4,0)$

$R = \underset{\{2\}}{\mathbb{Z}_4} \times \underset{\{2,3,4\}}{\mathbb{Z}_6} \rightarrow 24 - 2\times 2 - 1 = 19$

Zerodivisors:-
$(0,1), (0,2), (0,3), (0,4), (0,5),$
$(2,1), (2,2), (2,3), (2,4), (2,5),$
$(1,0), (2,0), (3,0)$
$(1,2), (3,2), (1,3), (3,3),$
$(1,4), (3,4).$

Zerodivisors of $\mathbb{Z} \times \mathbb{Z} = \{(0,a) \mid a \in \mathbb{Z}\setminus\{0\}\} \cup \{(b,0) \mid b \in \mathbb{Z}\setminus\{0\}\}$

If R and S are rings without zerodivisors then $R \times S$ has zerodivisors of the form
$\{(a,0) \mid a \in R\setminus\{0\}\} \cup \{(0,b) \mid b \in S\setminus\{0\}\}$

Homomorphism & Isomorphism :

Ex: ① Let G & G' be two groups then a function $f: G \to G'$ s.t. $f(x) = e'$, $\forall x \in G$, where e' is the identity of G' satisfies operation preserving.

Sol^n: $\forall x, y \in G$ $\quad f(xy) = e'$ $\quad$ → Not one-one → not onto

$= e' \cdot e'$

$= f(x) f(y)$ $\quad$ (yes)

② $f: \mathbb{C} \to \mathbb{C}$ s.t. $f(z) = \bar{z}$. $\quad$ → one-one → onto

$\forall z_1, z_2 \in \mathbb{C}$

$K_f = \{0\}$, $R_f = \mathbb{C}$

$f(z_1 + z_2) = \overline{z_1 + z_2}$

$= \bar{z}_1 + \bar{z}_2$

$= f(z_1) + f(z_2)$

⇒ identity of $\mathbb{C} = 0$, $e' = 0$, $f(z) = 0$, $\bar{z} = 0$ ⇒ $z = 0$

③ $f: \mathbb{R} \to \mathbb{R}^+$ s.t. $f(x) = 2^x$ $\quad$ → one-one → not onto

$\forall x, y \in \mathbb{R}$ $\quad$ → $K_f = \{0\}$ → $R_f \neq \mathbb{R}^+$

$f(x+y) = 2^{x+y}$

$= 2^x \cdot 2^y$

$= f(x) \cdot f(y)$

$e' = 1$, $\therefore f(x) = 1 \Rightarrow 2^x = 1$, $x = 0$, $\therefore K_f = \{0\}$

④ $f: \mathbb{C} \to \mathbb{C}$ s.t. $f(z) = |z|$ $\quad$ → not one-one → not onto

$\forall z_1, z_2 \in \mathbb{C}$

$f(z_1 + z_2) = |z_1 + z_2|$

$\neq |z_1| + |z_2|$

$\neq f(z_1) + f(z_2)$

So, f does not satisfy operation preserving property.

⑤ $f: \mathbb{C}_0 \to \mathbb{R}_0$ s.t. $f(z) = |z|$ $\quad$ → not one-one → not onto

then $\forall z_1, z_2 \in \mathbb{C}_0$

$R_f = \mathbb{R}_0^+$

$f(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = f(z_1) \cdot f(z_2)$

$e' = 1 \Rightarrow f(z) = 1 \Rightarrow |z| = 1$

$\therefore K_f = \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$

⑥ $f: M_n(\mathbb{R}) \to \mathbb{R}$ s.t. $f(M) = tr(M)$ $\quad$ → not one-one → onto → Epimorphism

$\forall A, B \in M_n(\mathbb{R})$

$f(A+B) = tr(A+B)$

$= tr(A) + tr(B)$

$= f(A) + f(B)$

$e' = 0$, $\therefore f(M) = 0 \Rightarrow tr(M) = 0$

$K_f = \{M \in M_n(\mathbb{R}) \mid tr(M) = 0\}$

$R_f = \mathbb{R}$

⑦ $f: GL_n(\mathbb{R}) \to \mathbb{R}_0$ s.t. $f(M) = tr(M)$ $\quad$ → not one-one → onto → Epimorphism

$\forall A, B \in GL_n(\mathbb{R})$

$f(AB) = tr(AB)$

$\neq tr(A)\, tr(B)$

$f(A) f(B)$

⑧ $f: GL_n(\mathbb{R}) \to \mathbb{R}_0$ s.t. $f(M) = \det(M)$ $\quad$ → not one-one → onto.

Now $\forall A, B \in GL_n(\mathbb{R})$

$f(AB) = \det(AB)$

$= \det(A) \cdot \det(B)$

$= f(A) f(B)$

$e' = 1$, $f(M) = 1$, $\det(M) = 1$

$K_f = \{M \in GL_n(\mathbb{R}) \mid \det(M) = 1\}$

$K_f = SL_n(\mathbb{R})$

$R_f = \mathbb{R}_0$

properties:-

1. → OP
2. → one-one
3. → onto
4. → $G = G'$

properties	Function
(1)	→ Homomorphism
(1)+(2)	→ Monomorphism (one-one-Homomorphism)
(1)+(3)	→ Epimorphism (onto-Homomorphism)
(1)+(4)	→ Endomorphism
(1)+(2)+(3)	→ Isomorphism.
(1)+(2)+(3)+(4)	→ Automorphism.

Examples:- (1) For every two groups G & G' there exists a homomorphism $f: G \to G'$ s.t. $f(x) = e'$ $\forall x \in G$ which is Called trivial homomorphism.

(2) For every group G, there exists an endomorphism $f: G \to G$ s.t. $f(x) = e$, $\forall x \in G$ which is Called trivial endomorphism.

(3) For every group G, there exists an automorphism $f: G \to G$ s.t. $f(x) = x$ $\forall x \in G$ which is Called trivial automorphism. ($\because \forall x, y \in G$, $f(xy) = xy = f(x) f(y)$) → (inner automorphism or identity automorphism)

(4) For every group G and $\forall a \in G$, there exists a function $f_a: G \to G$ s.t. $f_a(x) = axa^{-1}$ $\forall x \in G$ which is an automorphism.
This is Called inner automorphism of G, induced by $a \in G$.

(5) Let G be a group and $f: G \to G$ is a function s.t. $f(x) = x^{-1}$ $\forall x \in G$ Then $f: G \to G$ is an automorphism iff G is abelian.

proof:- Since every element of G has a unique inverse in G.
So, $f: G \to G$ s.t. $f(x) = x^{-1}$ is bijective. [always for any G]
Now, If G is abelian then $\forall x, y \in G$, $xy = yx$
$\Rightarrow f(xy) = f(yx) = (yx)^{-1} = x^{-1}y^{-1} = f(x) f(y)$
So, f is an automorphism.

Conversely:- Let $f: G \to G$ s.t. $f(x) = x^{-1}$ is an automorphism then
$\forall x, y \in G \Rightarrow f(xy) = f(x) f(y)$
$\Rightarrow (xy)^{-1} = x^{-1} y^{-1}$
$\Rightarrow (xy)^{-1} = (yx)^{-1} \Rightarrow xy = yx$ $\quad \therefore G$ is abelian.

Some Useful Links:

1. **Free Maths Study Materials (**https://pkalika.in/2020/04/06/free-maths-study-materials/**)**

2. **BSc/MSc Free Study Materials (**https://pkalika.in/2019/10/14/study-material/**)**

3. **PhD/MSc Entrance Exam Que. Paper: (**https://pkalika.in/que-papers-collection/**)**
[CSIR-NET, GATE(MA), BHU, CUCET,IIT, JAM(MA), NBHM, ...etc]

4. **CSIR-NET Maths Que. Paper: (**https://pkalika.in/2020/03/30/csir-net-previous-yr-papers/**)**
[Upto Lastest CSIR NET Exams]

5. **PhD/JRF Position Interview Asked Questions:**
(https://pkalika.in/phd-interview-asked-questions/)

6. **List of Maths Suggested Books** (https://pkalika.in/suggested-books-for-mathematics/)

7. **CSIR-NET Mathematics Details Syllabus (**https://wp.me/p6gYUB-Fc)

8. **CSIR-NET, GATE, PhD Exams, ...etc Study Materials & Solutions**
https://pkalika.in/kalika-notes-centre/

9. **CSIR-NET, GATE, ... Solutions** (https://wp.me/P6gYUB-1eP)

10. **Topic-wise Video Lectures (Free Crash Course)**
https://www.youtube.com/pkalika/playlists