Ring :→ **Definition** :→ Suppose R is a non-empty set equipped with two binary operations called addition and multiplication denoted by '+' & '.' respectively i.e., for all $a, b \in R$ we have $a+b \in R$ & $a \cdot b \in R$.
Then the algebric structure $(R, +, \cdot)$ is called ring, if the following postulates are satisfied.

1. $(R, +)$ is form an abelian group i.e.
   (i) Addition is associative i.e.
   $$(a+b)+c = a+(b+c) \quad \forall\, a,b,c \in R$$
   (ii) There exist an identity s.t. $\exists\, 0 \in R$
   $$0+a = a \quad \forall\, a \in R$$
   (iii) To each elements a in R $\exists$ an elements $-a$ in R s.t.
   $$(-a)+a = 0$$
   (iv) Addition is commutative
   $$a+b = b+a \quad \forall\, a,b \in R$$

2. Multiplication is associative, i.e.
$$a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \forall\, a,b,c \in R$$

3. Multiplication is distributive w.r.t. addition i.e.
   (i) $a\cdot(b+c) = a\cdot b + a\cdot c$ → left distribution
   (ii) $(a+b)\cdot c = a\cdot c + b\cdot c$ → Right "
   $\forall\, a,b,c \in R$

Ring with Unity :→ If in a ring R $\exists$ an element denoted by 1 such that $1\cdot a = a\cdot 1 = a \;\forall\, a \in R$, then R is called ring with unit element. The elements $1 \in R$, is called the unit element of ring.
Thus if a ring possesses multiplicative identity, it is a ring with unity.

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

Ex. of Ring :→ (i) $\langle R, +, \cdot \rangle$ where R is a set of real no.
(ii) $\langle I, +, \cdot \rangle$ " I " " of all integers
(iii) $\langle Q, +, \cdot \rangle$ set of rational no. is commutative ring with unity.

Ring with zero divisors: In a ring R there exist non-zero elements a & b such that $ab = 0$, then R is said to be a ring with zero divisors.

Exp: Matrix multiplication $[M, +, \times]$, $(\{0,1,2,3,4,5\}, +_6, \times_6)$

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

exp: Any number system like set of Real no.

(i) $\langle R, +, \cdot \rangle$ (ii) $\langle I, +, \cdot \rangle$

Integral Domain: A ring is called an integral domain if it (i) is commutative (ii) has unit element (iii) is without zero divisors.

Exp: $\langle R, +, \cdot \rangle$, $\langle Q, +, \cdot \rangle$, $\langle C, +, \cdot \rangle$

Field: A ring R with at least two elements is called a field if it,

(i) is commutative (ii) has unity (iii) is such that each non-zero element possesses multiplicative inverse.

Exp: $\langle R, +, \cdot \rangle$, $\langle Q, +, \cdot \rangle$

Division ring or skew field: A ring R with at least two elements is called a division ring or a skew field if it (i) has unity (ii) is such that each non-zero element possesses multiplicative inverse.

Thus a commutative division ring is a field.

Every field is also a division ring but a division ring is a field if it is also commutative.

✱ **Theorem:** Every field is an integral domain.

Proof: Since a field F is a commutative ring with unity, therefore in order to show that every field is an integral domain we should show that a field has no zero divisors.

Let a, b be elements of F with $a \neq 0$ such that $ab = 0$

Since $a \neq 0$, a^{-1} exists we have

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

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

$$\boxed{b = 0}$$

Similarly $b \neq 0$, b^{-1} exists we have

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

$$\boxed{a = 0}$$

Thus $ab = 0 \Rightarrow a = 0$ or $b = 0$, but converse is not true.

Ideals :→

(a) <u>Left Ideal</u> :→ A non empty subset S of a ring R is said to be a left ideal of R if:

(i) S is a subgroup of R w.r.t addition

(ii) $rs \in S \ \forall \ r \in R \ \& \ \forall \ s \in S$.

(b) <u>Right Ideal</u> :→ A non-empty subset S of a ring R is said to be a right ideal of R if

(i) S is a subgroup of R under addition.

(ii) $sr \in S \ \forall \ r \in R \ \& \ \forall \ s \in S$.

(c) <u>Ideal</u> :→ A non-empty subset S of a ring R is said to be an ideal (also a two sided ideal) if and only if it is both a left and a right ideal. Thus a non-empty subset S of a ring R is said to be an ideal of R if:

(i) S is a subgroup of R under addition i.e., S is a subgroup of the additive group of R.

(ii) $rs \in S \ \& \ sr \in S$ for every $r \in R$ and for every $s \in S$.

<u>Principal Ideal Ring</u> :→ A commutative ring R without zero divisors and with unity element is a principal ideal ring if every ideal S in R is a principal ideal i.e., if every ideal S in R is of the form $S = (a)$ for some $a \in S$.

<u>Theorem</u> :→ Every field is a principal ideal ring.

<u>Proof</u> :→ A field has no proper ideals. The only ideals of a field are

(i) the null ideal with is a principal ideal generated by 0 &

(ii) the field itself which is also a principal ideal generated by 1.

Thus a field is always a principal ideal ring.

<u>Divisibility in an Integral Domain</u> :→ Suppose $0 \neq a \in R$ is an element of a commutative ring R. Then a is said to be divide $b \in R$, if there exists an element $c \in R$ s.t. $\boxed{b = ac}$

<u>Theorem</u> :→ If R is a commutative ring, then

(i) $a|b \ \& \ b|c \Rightarrow a|c$ i.e. the relation of divisibility in R is a transitive relation.

(ii) $a|b \ \& \ a|c \Rightarrow a|(b+c)$

(iii) $a|b \Rightarrow a|bx \ \forall \ x \in R$

<u>Proof</u> :→ (i) $a|b \Rightarrow b = ap$ for some $p \in R$

$b|c \Rightarrow c = bq$ for some $q \in R$

Now $c = bq = (ap)q = a(pq)$

$\Rightarrow a|c$ since $pq \in R$

(ii) $a|b \Rightarrow b = ap$ for some $p \in R$

$a|c \Rightarrow c = aq$ for " $q \in R$

Now

$b = ap$ & $c = aq \Rightarrow b+c = ap + aq$
$= a(p+q)$

$\Rightarrow a \mid (b+c)$ Since $p+q \in R$

(iii) $a|b \Rightarrow b = ap$ for some $p \in R$

$b = ap \Rightarrow bx = (ap)x \;\forall\; x \in R$

$bx = a(px) \Rightarrow a|bx$ since $px \in R$

Units :→ let R be a commutative ring with unity element 1. An element $a \in R$ is a unit in R if ∃ an element $b \in R$ such that $ab = 1$. In other words Units of R are those elements of R which possess multiplicative inverse.

5(b) 2015 **Example** :→ Find all the units of the integral domain of Gaussian integers.

Solution :→ let $D = \{a+ib ;\ a, b \in I$ the set of integers$\}$ be the ring of Gaussian integers. The element $1+0i$ is the unit element of the ring. let $x+iy$ be a unit and $x'+iy'$ be its inverse then

$$(x+iy)(x'+iy') = 1+0i$$

$$(xx' - yy') + i(xy' + yx') = 1+0i$$

Equating real & imaginary part

$$xx' - yy' = 1 \longrightarrow ①$$

$$xy' + yx' = 0 \longrightarrow ②$$

squaring & adding ① & ②

$$x^2x'^2 + y^2y'^2 + x^2y'^2 + x'^2y^2 = 1$$

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

Now the product of two positive integer is equal to 1 if & only if each of them is 1.

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

If $x^2=0$; $y^2=1$

$x^2 = 1$; $y^2 = 0$

$x = 0$, $y = \pm 1$

$x = \pm 1$; $y = 0$

The only units of the integral domain of Gaussian integers are $0 \pm i$, $\pm 1 + 0i$ i.e. $1, -1, i, -i$.

Proper & Improper Divisors: Let D be an integral domain with unity element 1. Let a be any non-zero element of D. Then the units of D and associates of a are always divisor of a. These are called improper or trivial divisors of a. Any other divisors of a are called proper or non-trivial divisors of a.

Exp: $\pm 1, \pm 6$ are trivial or improper divisors of 6. But $\pm 2, \pm 3$ are proper or non-trivial divisors of 6.

Prime Elements: Let D be an integral domain with unity element 1. A non-zero non-unit element $a \in D$, having only trivial divisors, is called a prime or irreducible element of D. An element $0 \neq b \in D$ having proper divisors is called a reducible or composite element of D.

Greatest Common Divisor (GCD): Let R be a commutative ring. If $a, b \in R$ then $0 \neq d \in R$ is said to be a gcd of a & b if

(i) $d|a$ & $d|b$

(ii) whenever $c|a$ & $c|b$ then $c|d$.

Relatively Prime Elements: Let D be an integral domain with unity element 1. Two element $a, b \in D$ is said to be relatively prime if their gcd is a unity of D.

2015 4(a) **Euclidean Ring or Euclidean Domains:** Let R be an integral domain i.e., let R be a commutative ring without zero divisors. Then R is said to be a Euclidean ring if to every non-zero element $a \in R$ we can assign a non non-negative integer $d(a)$ such that: $d: R^* \longrightarrow R$ where $R^* = R - \{0\}$

(i) $\forall\, a, b \in R^* \Rightarrow d(ab) \geq d(a)$

or

$a|b \Rightarrow d(b) \geq d(a)$

(ii) For any $a, b \in R^*$ $\exists\, q, r \in R^*$ such that
$a = bq + r$ where $r = 0$ or $d(r) < d(b)$.

The second part is also know as division Algorithm.

2015
4(a)

Example 1: → The ring of integers is an Euclidean ring.

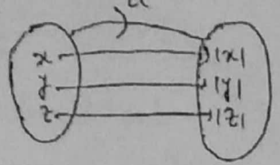
Soln: → Let $\langle I, +, \cdot \rangle$ be the ring of integers where

$$I = \{0, \pm 1, \pm 2, \pm 3 \cdots \infty\}$$

Let $d : I^* \longrightarrow I$

$$d(x) = |x|$$

$$\forall\, x \in I^*$$



Further if $a, b \in I^*$

then $|ab| = |a||b|$

$$|ab| \geq |a|$$

$$\boxed{d(ab) \geq d(a)}$$

Finally we know that if $a, b \in I^*$ & q & r are two integers

$a = qb + r$ where $0 \leq r < |b|$

where either $r = 0$ or $1 \leq r < |b|$

" " $\boxed{r = 0 \text{ or } d(r) < d(b)}$

Therefore the ring of integers is an Euclidean ring.

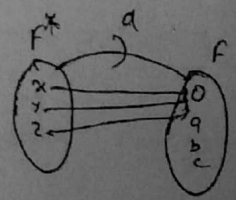
Example 2: → Every field is an Euclidean ring.

Soln: → Let F be any field.

$$d : F^* \longrightarrow F$$

Let the function d is defined as

$$d(x) = 0 \;\forall\; x \in F^*$$



If $a, b \in F^*$

$$d(ab) = 0 = d(a)$$

then $d(ab) \geq d(a)$

We can write

$$a = a + 0$$

$$a = a \cdot b^{-1} b + 0 \quad (\because b \in F^* \text{ \& } F \text{ is field})$$

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

i.e. $a = qb + r$ where $q = ab^{-1}$ & $r = 0$

Hence every field is an Euclidean ring.

Example 3: → The ring of Gaussian integers is an Euclidean ring.

Solution : → Let $(G, +, \cdot)$ be the ring of Gaussian integers

where $G = \{x+iy \,;\, \forall x, y \in I\}$

$d : G^* \longrightarrow G$

Let function d is defined as

$$d(x+iy) = |x+iy|^2 = x^2+y^2$$

If $x+iy$, $m+in \in G^*$

$$d\left[(x+iy)(m+in)\right] = d\left[(xm-ny)+i(my+xn)\right]$$
$$= (xm-ny)^2 + (my+xn)^2$$
$$= x^2m^2 + n^2y^2 - 2m\cancel{nxy} + m^2y^2 + x^2n^2 + 2m\cancel{nxy}$$
$$= m^2(x^2+y^2) + n^2(x^2+y^2)$$
$$= (x^2+y^2)(m^2+n^2)$$
$$\geq (x^2+y^2)$$

$$\boxed{d\left[(x+iy)(m+in)\right] \geq d(x+iy)}$$

Let $\alpha \in G$ and let β be ~~an~~ non-zero elements of G. Let $\alpha = x+iy$ & $\beta = m+in$. Define a complex number λ by $\lambda = \frac{\alpha}{\beta} = \frac{x+iy}{m+in} = \frac{(x+iy)(m-in)}{m^2+n^2} = p+iq$

where p & q are rational no.

Here λ is non necessarily a gaussian integer.

Also division of β is possible since $\beta \neq 0$.

Let p' & q' be the nearest point of p & q respectively.

then $|p-p'| \leq \frac{1}{2}$, $|q-q'| \leq \frac{1}{2}$.

Let $\lambda' = p'+iq'$. Then λ' is a Gaussian integer.

Now

$$\lambda = \frac{\alpha}{\beta} \Rightarrow \alpha = \lambda\beta$$
$$\Rightarrow \alpha = \lambda'\beta + \lambda\beta - \lambda'\beta$$

Thus
$$\alpha = \lambda'\beta + (\lambda-\lambda')\beta \longrightarrow (1)$$

Since α, β, λ' are Gaussian integers, therefore from (1) it implies that $(\lambda-\lambda')\beta$ is also a Gaussian integer.

Now if p & q are integers then $p = p'$, $q = q'$

So $\lambda - \lambda' = (p-p') + i(q-q') = 0 + i0$ thus $(\lambda-\lambda')\beta = 0+i0$

If p & q are not both integers, then $(\lambda-\lambda')\beta$ is a non-zero Gaussian integer and we have

$$d[(\lambda-\lambda')\beta] = d[\{(p-p') + i(q-q')\}(m+in)]$$
$$= [(p-p')^2 + (q-q')^2](m^2+n^2)$$
$$= [(p-p')^2 + (q-q')^2]\, d(\beta)$$
$$\leq \left[\frac{1}{4} + \frac{1}{4}\right] d(\beta) = \frac{1}{2} d(\beta) < d(\beta)$$

Thus $\alpha = \lambda'\beta + (\lambda-\lambda')\beta$ where λ' & $(\lambda-\lambda')\beta$ are Gaussian integers & either $(\lambda-\lambda')\beta = 0$

or $d[(\lambda-\lambda')\beta] < d(\beta)$.

Hence the ring of Gaussian integers is an Euclidean ring.

5(a) 2015

Theorem:→ Let R be a Euclidean ring and a & b be any two elements in R, not both of which are zero. Then a & b have a greatest common divisor d which can be expressed in the form

$d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Proof:→ Consider the set

$$S = \{sa + tb : s, t \in R\}$$

We claim that S is an ideal of R.

The proof is as follows:

Let $x = s_1 a + t_1 b$ & $y = s_2 a + t_2 b$ be any two elements of S.

Then $s_1, t_1, s_2, t_2 \in R$. We have

$$x - y = (s_1 a + t_1 b) - (s_2 a + t_2 b) = (s_1 - s_2)a + (t_1 - t_2)b \in S$$

Since $s_1 - s_2$ & $t_1 - t_2$ are both elements of R.

Thus S is subgroup of R w.r.t addition.

Also if u be any element of R, then

$$xu = ux = u(s_1 a + t_1 b) = (us_1)a + (ut_1)b \in S$$

Since $us_1, ut_1 \in R$.

Therefore S is an ideal of R. Now every ideal in R is a principal ideal. Therefore there exists an element d in S such that every elements in S is a multiple of d.

Since $d \in S$, therefore from 1, we see that $\exists$ $\lambda, \mu \in R$ s.t. $d = \lambda a + \mu b$.

Now R is a ring with unity element 1.

$\therefore$ Putting $s = 1$, $t = 0$ in 1, we see that $a \in S$.

Also putting $s = 0$, $t = 1$ in 1, we see that $b \in S$

Now a, b are elements of S. Therefore they are both multiples of d. Hence $d|a$ & $d|b$.

Now suppose $c|a$ & $c|b$.

Then $c|\lambda a$ & $c|\mu b$. Therefore c is also a divisor of $\lambda a + \mu b$ i.e. c is a divisor of d.

Thus d is a greatest common divisor of a & b.

Unique Factorization Domain :→

Statement :→ Let R be an Euclidean domain/ring.

If $n > 1$

$$n = p_1 \cdot p_2 \cdot p_3 \cdots\cdots p_m = q_1 \cdot q_2 \cdot q_3 \cdots q_n$$

then $\boxed{m = n}$ & $\boxed{p_i = q_j}$ for some i & j.

$\forall$ p_i's, q_j's $\in R^*$

& all p_i's & q_j's are prime elements.

Proof :→ $n > 1$

$$\left.\begin{aligned} n &= p_1 \cdot p_2 \cdot p_3 \cdots p_m \\ &= q_1 \cdot q_2 \cdot q_3 \cdots q_n \end{aligned}\right\} \forall\ p_i\text{'s},\ q_j\text{'s} \in R^* \longrightarrow (1)$$

Case 1 If $m = n$:→

$$p_1 \cdot p_2 \cdot p_3 \cdots p_m = q_1 \cdot q_2 \cdot q_3 \cdots q_n \quad \text{from } (1)$$

Let $c = p_2 \cdot p_3 \cdot p_4 \cdots p_m$

$$p_1 \cdot (c) = q_1 \cdot q_2 \cdot q_3 \cdots q_n \longrightarrow (2)$$

from equ (2)

$$p_1 \mid q_1 \cdot q_2 \cdot q_3 \cdots q_n$$

$\because$ p_1 & q_j's are all prime elements

then any one of q_j's is equal to p_1

$\Rightarrow$ $p_1 = q_j$ for any j. $\longrightarrow (3)$

Kajol

Similarly let $c_1 = p_1 \cdot p_3 \cdot p_4 \cdots p_m$

$p_2 \cdot c_1 = q_1 \cdot q_2 \cdot q_3 \cdots q_n$

then $p_2 \mid q_1 \cdot q_2 \cdot q_3 \cdots q_n$

by the same way

$p_2 = q_j$ for some j. $\longrightarrow$ (4)

<u>Conversely</u>

$q_1 \cdot q_2 \cdot q_3 \cdots q_n = p_1 \cdot p_2 \cdot p_3 \cdots p_m$ from (1)

let $d = q_2 \cdot q_3 \cdots q_n$

$q_1 \cdot d = p_1 \cdot p_2 \cdot p_3 \cdots p_m$

$q_1 \mid p_1 \cdot p_2 \cdot p_3 \cdots p_m$ $\forall$ q_1 & p_i's are prime

$\Rightarrow$ $q_1 = p_i$'s for some i. $\longrightarrow$ (5)

Similarly $q_2 = p_i$'s for some i $\longrightarrow$ (6)

from (3), (4), (5) & (6)

$\boxed{p_i = q_j}$ for some i & j

when $\boxed{m = n}$

<u>Case 2:</u> $\rightarrow$ if <u>$m > n$</u>

$p_1 \cdot p_2 \cdot p_3 \cdots p_m = q_1 \cdot q_2 \cdot q_3 \cdots q_n$ from (1)

If <u>$m > n$</u>

then some p_i's are equal to 1.

$\because$ All p_i's are prime elements and prime elements are greater than 1.

Hence It is a contradiction.

Hence $m > n$ is not possible.

<u>Case 3:</u> $\rightarrow$ If <u>$m < n$</u>

Same as case (2)

some q_j's are equal to 1.

& It is a contradiction

Hence $m < n$ is not possible.