⇒ Modern Algebra

⇒ Basics :

1) $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ — sets of non-zero nos in $\mathbb{I}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

2) Cartesian Product of sets A & B = $A \times B = \{(a,b) \mid a \in A, b \in B\}$

   a) If A & B are non-empty, any subset of $A \times B$ is called a relation from A to B.

   b) If $A \neq \phi$, then subset of $A \times A$ is called Binary Relation on A.

3) Function: f is a relation from A to B. It is called a function for each $a \in A$ $\exists$ a unique $b \in B$ st $(a,b) \in f$

4) Binary Operation: $\forall$ $a, b \in S$, if $a * b \in S$, then * is a b-op^n on S.
   (it is $f: A \times A \longrightarrow A$)

   * S = set of all matrices with real entries
   $+^n, -^n, \times^n$ are not b-o's on S.

5) Algebraic structure : Non-empty set equipped with one or more b-op^{n}s.

Groupoid | Quasi-group	closure in $(G, *)$
Semi-group | Demi-group	closure + associativity
Monoid	semi group + identity elt
Group	Monoid + inverse elt
Abelian group	Group + commutative

6) Group :

i) $(G, *)$ is a group if it satisfies :

a) closure $\forall\ a, b \in G \Rightarrow a * b \in G$

b) associativity $\forall\ a, b, c \in G \Rightarrow (a*b)*c = a*(b*c)$

c) Existence of Identity : $\exists\ e \in G$ st $\forall\ a \in G \Rightarrow a*e = e*a = a$

d) Existence of inverse : for each $a \in G$, $\exists\ b \in G$ st

$$a * b = b * a = e$$

ii) Order of group = $o(G) = |G| =$ no. of elts in finite group G.

iii) Properties :

a) LCL & RCL hold in G

$\forall\ a, b, c \in G$ $\quad ab = ac \Rightarrow b = c$

$\quad\quad\quad\quad\quad\quad\quad\quad ba = ca \Rightarrow b = c$

But not in semi-group necessarily

eg Matrix Multiplication $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

REMEMBER: But a finite semigroup with cancellation laws holding is a group. [$\because$ using Pigeonhole principle]

b) Identity element is unique in a G. [$\because e_1 = e_1 e_2 = e_2$]

c) Inverse of each element is unique [$aa' = e = aa'' \Rightarrow a' = a''$]

iv) Sufficient conditions to prove a group

a) closure

b) Associativity

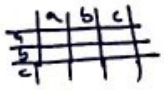
c) Existence of left Identity, ie, $\exists\ e \in G$ st $\forall\ a \in G$ $e * a = a$

d) Existence of left Inverse, ie, for each $a \in G$, $\exists\ b \in G$ st

$$b * a = e$$

7) Composition Table for finite sets :

a) Make the table of size $n \times n$ with ij^{th} element being $a_i * a_j$ for $G = \{a_1, a_2, \ldots, a_n\}$ which is a finite set of distinct elements



b) check for :

i) closure : $A_{ij} \in G \quad \forall \; i, j$

ii) identity : Any row coincides with the top row

iii) inverse : every row & every column contains the identity element

iv) commutative : transpose gives the same table.

v) Associativity : need to show separately.

REMEMBER : i) $\{1, -1, i, -i\}$ is an abelian group

* ii) Every group of order 4 is and less is abelian

** iii) Quaternion group : $\{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2 = j^2 = k^2 = -1$

$ij = -ji = k$

$jk = -kj = i$

$ki = -ik = j$

Very important example to negate or contradict.

8) Addition modulo m : $a +_m b = r$ [r is remainder when $a+b$ is divided by r]

9) Congruence : $a \equiv b \pmod m$ if $(a-b)$ is divisible by m

$a \equiv b \pmod m \iff m \mid a-b$

$\Rightarrow$ a & b give same remainder when divided by m

$\Rightarrow$ ~~or~~ $a \equiv b \pmod m \Rightarrow a +_m c = b +_m c$

10) Equivalence class for $a \in A$ for relation R (equivalence relation in A)

$A_a = [a] = \bar{a} = \{ x \mid x \in A \text{ and } (x, a) \in R \text{ i.e. } x R a \}$

11) Operation congruence modulo 'm' is an equivalence relation in $\mathbb{Z}$ & partitions it into disjoint equivalence classes called Residue classes

$m \in N$ & $r \in \mathbb{Z}$ Let $\bar{r} = \{x \mid x \in \mathbb{Z},\ x \equiv r \pmod m\}$

Then $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(m-1)}\}$ is called the complete set of least +ve residue classes modulo m.

$\{0, 1, 2, \ldots, m-1\}$ is the set of residues modulo m

$(\mathbb{Z}_m, +)$ is an abelian group where + is defined as $\bar{a} + \bar{b} = \overline{a+b}$
of order (m)

12) Multiplication modulo p : $a \times_p b = r$ [r is remainder when ab is divided by p]

$a \times_p b = ab \pmod p$

13) Prime Integer : $p \in \mathbb{Z}$ is prime if $p \neq 0, p \neq \pm 1$ and only divisors of p are $\pm 1, \pm p$

If p is prime & $a, b \in I$, then

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$

14) $G = \{1, 2, \ldots, p-1\}$ where p is prime forms a finite abelian group of order $(p-1)$ wrt multiplication mod p.

If $0 \in G$, G is not a group (∵ no inverse)

If p is composite, G is not closed

15) Integral exponents

$a \in G$ & $n \in I$, then:

i) $a^0 = e$ ii) $a^1 = a$ iii) $a^{n+1} = a^n \cdot a$ for $n \geq 1$

iv) $a^{-n} = (a^{-1})^n$ for $n > 0$

While proving don't just treat as ex integers & arrive at result Need to use induction to prove cases.

eg prove a^n & a^{-n} are inverses of each other

for $n=1$, $a \cdot a^{-1} = e = a^{-1} \cdot a$ $S(1)$ is true

for say $S(k)$ is true ie $a^k \cdot a^{-k} = e = a^{-k} \cdot a^k$.

Now $S(k+1) \Rightarrow a^{k+1} \cdot a^{-(k+1)} = a^k \cdot a \cdot (a^{-1})^k \cdot (a^{-1})$

$= a \cdot a^k \cdot a^{-k} \cdot a^{-1}$ [use $a \cdot a^n = a^n \cdot a$]

$= a \cdot (a^k a^{-k}) \cdot a^{-1}$ ↳ prove if not stated.

$= a(e)a^{-1} = e$

similarly $a^{-(k+1)} \cdot a^{k+1} = e$

16) If G is abelian : $(ab)^n = a^n b^n$ $a, b \in G$. $n \in I$.

eg.* In G, $(ab)^m = a^m b^m$ for 3 successive integers m $\forall a, b \in G$ ST. G is abelian

given $(ab)^m = a^m b^m$ $(ab)^{m+1} = a^{m+1} b^{m+1}$ $(ab)^{m+2} = a^{m+2} b^{m+2}$

Now $(ab)^{m+2} = (ab)^{m+1}(ab)$

$a^{m+2} b^{m+2} = a^{m+1} b^{m+1} ab$

$a \cdot a^{m+1} b^{m+1} b = a \cdot a^m b^m \cdot bab$

$a^{m+1} b^{m+1} = a^m b^m ba$

$(ab)^{m+1} = (ab)^m ba$

$(ab)^m (ab) = (ab)^m (ba)$

$ab = ba$

17) Order of an element : least +ve integer n st $a^n = e$

$o(a) = n$

If there is no such integer $o(a) =$ infinite order.

$o(e) = 1$

If $a^m = e \Rightarrow o(a) \leq m$

18) In a finite group (G), $o(a)$ = finite $\forall$ $a \in G$
& $o(a) \leq o(G)$

If $o(a) = n > o(G)$
then $a^1, a^2, \ldots, a^n \in G$ by closure
Since G is finite $a^r = a^s$ for some $r, s < n$

$\Rightarrow a^{r-s} = e$

$\Rightarrow o(a) \leq r-s < n$ #

$\therefore$ $a^1, a^2, \ldots, a^n$ are distinct
But G can't have more than $o(G)$ elts.

$\therefore$ $o(a) \leq o(G)$.

19) a) $o(a) = o(a^{-1})$ [use $o(a) \leq o(a^{-1})$ & $o(a^{-1}) \leq o(a)$ method]

b) $o(a^r) \leq o(a)$ $\forall$ $a \in G$ & $r \in N$

$o(a) = n \Rightarrow a^n = e$

$(a^n)^r = e \Rightarrow (a^r)^n = e \Rightarrow o(a^r) \leq n$

c) $o(a) = o(b^{-1}ab)$

d) $o(ab) = o(ba)$ [using $o(a) = o(b^{-1}ab)$, put $a = ba$]

e) $o(a) = n$ & p is prime to n. $\Rightarrow o(a^p) = n$

REMEMBER: If a & b are relatively prime
$\exists$ $x, y \in I$ st $ax + by = 1$

Let $o(a) = n$
$o(a^p) = m$
$m \leq n$

$a = a^{px+ny} = a^{px} \cdot a^{ny} = a^{px} \cdot e^y = a^{px} \cdot e$

$a = (a^p)^x \Rightarrow a^m = ((a^p)^x)^m = [(a^p)^m]^x = e^x = e$

$\therefore o(a) \leq m \Rightarrow n \leq m$
$\therefore m = n$.

f) $a^m = e \Leftrightarrow o(a) \mid m$

g) If G is abelian & $o(a) = m$ $o(b) = n$ & $(m,n) = 1$
then $o(ab) = mn$

Use Proof: Let $o(ab) = p$.

$(ab)^{np} = a^{nb} b^{np} = a^{np} = e \Rightarrow m \mid np \Rightarrow m \mid p$ [$\because (m,n) = 1$]

Similarly $n \mid p$
$\Rightarrow mn \mid p$ [$\because (m,n) = 1$] Easy to prove $p \mid mn$

20) To prove results for any integer 'n', do not forget the case where $n < 0$.

eg $(bab^{-1})^n = ba^nb^{-1}$

for $n < 0$ Let $n = -m$

$(bab^{-1})^{-m} = [(bab^{-1})^m]^{-1} = [ba^mb^{-1}]^{-1}$ [∵ using result from $n \geq 0$ case]

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

$= b\,a^{-m}b^{-1}$

$= ba^nb^{-1}$

21) Klein-4 group : $O(G) = 4$ and $a = a^{-1}\ \forall\ a \in G$

22) eg. $x^2ax = a^{-1}$ is solvable iff $a = b^3$ for some $b \in G$.

if $x^2ax = a^{-1}$ is solvable

$\exists\ c$ st $c^2ac = a^{-1}$

$\Rightarrow c(ca)(ca) = e$

$\Rightarrow (ca)(ca) = c^{-1}$

$\Rightarrow (ca)(ca)(ca) = a$

$\therefore a = (ca)^3$

if $a = b^3$, then $x = b^{-2}$ is a solution

$(b^{-2})^2 b^3 \cdot b^{-2} = b^{-3} = (b^3)^{-1} = a^{-1}$

23) $O(a) = n$, then $O(a^k) = \dfrac{n}{HCF(n,k)}$ $\quad k \in I$

Let $(n,k) = m$

$n = pm \quad k = qm$ st $(p,q) = 1$

Let $O(a^k) = L \Rightarrow (a^k)^L = e \Rightarrow a^{kL} = e$

$\Rightarrow O(a) \mid kL \Rightarrow n \mid kL$

$\Rightarrow pm \mid qmL \Rightarrow p \mid qL$

$\Rightarrow p \mid L \quad [\because (p,q) = 1]$

Now $(a^k)^p = (a^{qm})^p = (a^{pm})^q = e^q = e$

$\Rightarrow O(a^k) \mid p$

$\Rightarrow L \mid p$

$\Rightarrow L = p$

$\therefore O(a^k) = \dfrac{n}{m} = \dfrac{n}{(n,k)}$

⇒ Permutation Groups :

1) A permutation of a set A is a function $\phi: A \to A$ that is both one-one and onto.

$$\phi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \begin{matrix} \to \text{elements} \\ \to \text{images} \end{matrix}$$

2) There are $n!$ different permutations of degree 'n'

Degree → no of elements in the finite set A.

$P_n = S_n$ = symmetric set of perms of deg $= n = \{f : f$ is a permutation of degree $n\}$
$n \le 2 \to S_n$ is abelian ; $n \ge 3$ – non-abelian

3) Multiplication of permutations is not commutative.
" " associative.

4) $S = \{a_1, \cdots, a_n\}$ and f is a permutation on S.
If for $a \in S$, $\exists$ a smallest +ve integer 'l' (depending on 'a')
st $f^l(a) = a$, then
$\{a, f^1(a), f^2(a), \cdots, f^{l-1}(a)\}$ is called orbit of 'a' under f.
This ordered set is called cycle of f.

eg. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} = (1\ 2)(3)(4\ 5\ 6)$

5) Cyclic Permutation :

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix} = (1\ 3\ 5\ 7)$ → cycle of length 4

a) Cycle of length 1 : identity permutation
b) cycle of length 2 : transposition
c) Disjoint cycles : $S = \{a_1, \cdots a_n\}$ & f, g are 2 cycles on S such that they do not have any common element.
d) Product of disjoint cycles is commutative.

e) Inverse of cyclic permutation:

$f = (1\ 2\ 3\ 4)$ $\quad f^{-1} = (4\ 3\ 2\ 1)$

inverse of transposition is the transposition itself.

f) Order of a cyclic permutation:

smallest $n \in \mathbb{Z}^+$ st $f^n = I$ is order of cyclic perm f.

6) Every permutation can be expressed as product of disjoint cycles.

* Every cycle can be expressed as a product of transpositions in many ways.

$$f = (a_1\ a_2 \cdots a_n) = (a_1\ a_n)(a_1\ a_{n-1}) \cdots (a_1 a_3)(a_1 a_2)$$

eg $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$

* cycle of length 'n' may be expressed as a product of (n-1) transpositions.

In any case their no is always odd or always even

[∵ as $f = (a_1 a_2 a_3) = (a_1 a_3)(a_1 a_2) = (a_1 a_3)(a_1 a_2)\ \underbrace{T\ T}$

$T = T^{-1}$
$\therefore TT = I$
T is any transposition]

* Odd no of transpositions ⇒ odd permutation
Even ——"—— ⇒ even permutation

* 7) n is odd ⇒ f is even
n is even ⇒ f is odd

Every transposition is odd

Every identity permutation is even.

8) odd permutation × odd permutation = even permutation
even × even = even permutation
odd × even = odd permutation [⇒ inverse of odd is odd]

9) S_n is permutation group on 'n' symbols.
Then $\frac{1}{2}n!$ are even permutations & $\frac{1}{2}n!$ are odd.

Proof: Let there be p even & q odd permutations
st $S_n = \{e_1 e_2 \cdots e_p, o_1, o_2, \cdots o_q\}$. $p+q = n!$.
Let $t \in S_n$ be a transposition.
Now $te_i \in S_n$ & $to_j \in S_n$ [$\because S_n$ is closed]
te_is are all odd & to_js are all even [$\because t$ is odd]
None of the te_is are equal & neither any of the to_js.
say $te_i = te_j \Rightarrow e_i = e_j$ [LCL]
Hence all te_is are distinct odd perms $\Rightarrow p \leq q$
Similarly $\Rightarrow q \leq p$
$\Rightarrow p = q = \frac{n!}{2}$

10) A_n = Alternating set of permutations of degree n =
= set of all even permutations of S_n.
$O(A_n) = \frac{n!}{2}$ & A_n forms a group wrt X^n.

11) Order of an n-cycle:
$f = (1\ 2\ 3 \cdots n)$
$f^2 = (1\ 3\ 5\ 7 \cdots)(2\ 4\ 6 \cdots)$
$f^2 = (1\ 3\ 5\ 2\ 4)$
f^2 moves every symbol 2 places
f^3 moves every symbol 3 places
f^n moves every symbol n places
ie, $f^n = (1)(2) \cdots (n) = I$
$\therefore$ order of f is n

12) Order of product of disjoint cycles of lengths $m_1, m_2, \cdots, m_k$:
order = LCM of $m_1, m_2, \cdots, m_k$

⇒ Subgroups :

1) **Complex**: non-empty subset of a group is called complex.

Product of complexes $MN = \{ mn \in G \mid m \in M, n \in N \}$

$M(NP) = (MN)P$

$M^{-1} = \{ m^{-1} \in G \mid m \in M \}$.

$(MN)^{-1} = N^{-1}M^{-1}$

2) **Subgroup**:

G is a group & H is non-empty subset of G.

H is a subgroup of G if H is a group wrt b-op^n in G

3) **Properties & Theorems on subgroup**:

a) If H is a subgroup $\Rightarrow$ $H^{-1} = H$

converse fails: eg $H = \{-1\}$ $G = \{1, -1\}$

b) if H is a subgroup $\Rightarrow$ $HH = H$

c) G is a group & $H \subseteq G$, then

H is a subgroup $\Leftrightarrow$ i) $a, b \in H \Rightarrow ab \in H$ [wrt x^n]
ii) $a \in H \Rightarrow a^{-1} \in H$

$\Leftrightarrow$ i) $a, b \in H \Rightarrow a+b \in H$ [wrt +^{n}]
ii) $a \in H \Rightarrow -a \in H$

$\Leftrightarrow$ $a, b \in H \Rightarrow \underline{ab^{-1} \in H}$

$\Leftrightarrow$ $HH^{-1} \subseteq H$

$\Leftrightarrow$ $HH^{-1} = H$

(if H is finite) $\Leftrightarrow$ $a, b \in H \Rightarrow a.b \in H$

d) $H \leq G$, $K \leq G$, $HK \leq G$ iff $\underline{HK = KH}$

[∵ use $(HK)(HK)^{-1} = (HK)$ for 1 dirn^n & $(HK) = (HK)^{-1}$ for other]

e) $H_1 \leq G$, $H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G$

f) $H_1 \cup H_2$ need not be a subgroup

eg $H_1 = \{2n \mid n \in I\}$ $H_2 = \{3n \mid n \in I\}$

$H_1 \cup H_2$ is not closed

g) $H_1 \cup H_2 \leq G \iff H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

4) G is a group & $a \in G$, then $H = \{a^n \mid n \in I\}$ [or $\{na \mid n \in I\}$] is called the subgroup generated by 'a'

5) **Normalizer** of an element of a group:

$N(a) = \{x \in G \mid xa = ax\}$

$N(a) \leq G$

6) Self-conjugate | Invariant element: $a \in G$ st $a = x^{-1}ax$ $\forall x \in G$

7) **Centre** of a group: $Z = \{z \in G \mid zx = xz \ \forall x \in G\}$

$Z = G$ if G is abelian

$Z \leq G$

8) Finite Group can never be expressed as union of 2 of its proper subgroups eg Quaternion group [$\because$ use lagrange theorem]

9) Abelian group $\Rightarrow$ Abelian subgroup always

Non-Abelian group $\Rightarrow$ Subgroup may be

i) Abelian - eg P_3 & A_3

ii) Non-abelian - eg P_4 & A_4

⇒ Cosets :

1) $(H, \cdot)$ is subgroup of $(G, \cdot)$

Left coset of H = $aH = \{ah \mid h \in H\}$

Right coset of H = $Ha = \{ha \mid h \in H\}$

generated by $a \in G$.

2) Left & Right cosets are non-empty [$\because a \in aH, a \in Ha$ as $e \in H$]

3) Left & Right cosets need not be a subgroup of G.

eg $G = \{\pm 1, \pm i\}$ $H = \{\pm 1\}$

$H(-1) = \{-1, 1\}$ $H(1) = \{-1, 1\}$

$H(i) = \{+i, -i\}$ $H(-i) = \{+i, -i\}$

4) Properties of cosets :

a) $H \leq G$ & $a \in H \Rightarrow aH = Ha = H$

*b) $H \leq G$ & $a, b \in G$ $aH = bH \iff a^{-1}b \in H$

$Ha = Hb \iff ab^{-1} \in H$

c) $a, b \in G$ & $H \leq G$, then $a \in bH \iff aH = bH$

$a \in Hb \iff Ha = Hb$

d) Any 2 left (right) cosets of a subgroup are either disjoint or identical

Proof. Let $aH \cap bH \neq \phi$, i.e., $c \in aH \cap bH$

$\Rightarrow c \in aH$ & $c \in bH$.

$\Rightarrow c = ah_1$ for $h_1 \in H$ & $c = bh_2$ for $h_2 \in H$

$\Rightarrow ah_1 = bh_2$

$b^{-1}ah_1 = h_2$

$b^{-1}ah_1H = h_2H$ [$\because h_1 \in H \Rightarrow h_1H = H$]

$b^{-1}aH = H$

$aH = bH$

e) If $H \leq G$, G = union of all left (right) cosets of H in G.

5) Set of all right cosets of H in G gives a partition of G.

6) If $H \leq G$, there is a <u>one-one correspondence</u> b/w any two left (right) cosets of H in G.

$f: aH \longrightarrow bH$
st $f(ah) = bh$ for $h \in H$

Easy to show that f is 1-1 & onto.

7) If $H \leq G$, there is 1-1 correspondence b/w the set of all distinct left cosets of H in G & the set of all distinct right cosets of H in G.

$f: G_1 \longrightarrow G_2$
st $f(aH) = Ha^{-1} \quad \forall \ a \in G$.

8) If $H \leq G$ where G is finite, then

a) no of distinct left cosets of H in G = no of distinct right cosets of H in G

b) no of elements in a left coset of H = no of elements in a right coset of H.

9) **Congruence modulo H** :

for $a, b \in G$ if $b^{-1}a \in H$, we say $a \equiv b \pmod H$

$a \equiv b \pmod H$ relation is an <u>equivalence relation</u>

10) Let $H \leq G$. For $a \in G$, eq. class $\bar{a} = \{x \in G \mid x \equiv a \pmod H\}$

$\Rightarrow \quad \underline{\bar{a} = aH}$

i.e., Cosets form the residue / equivalence classes

11) $H \leq G$ & G is finite

$[G:H] = i_G(H)$ = index of H in G = no of distinct Left (or right) cosets of H in G.

12) Lagrange Theorem:

If G is a finite group & $H \leq G \Rightarrow O(H) \mid O(G)$

Proof: Let $H, Ha, Hb, \ldots$ be the right cosets of H in G

$O(Ha) = O(Hb) = \ldots = O(H) = m$

Let no of distinct right cosets be 'k'

The distinct right cosets form a partition of G

$\therefore O(G) = O(Ha) + O(Hb) + \ldots + O(H)$

$n = km$

$\therefore k = n/m \Rightarrow O(H) \mid O(G)$

13) $[G:H] = i_G(H) = \dfrac{O(G)}{O(H)}$

14) Converse of Lagrange is not true:

If $m \mid n \not\Rightarrow$ G must have subgroup of order m.

15) If G is finite and $a \in G \Rightarrow O(a) \mid O(G)$

$\Rightarrow a^{O(G)} = e$

16) If $O(G)$ is prime, G doesn't have a proper subgroup

17) Poincare's Theorem:

G is a group & H, K are 2 finite index subgroups of G.

then $H \cap K$ is of finite index

18) If H & K are finite subgroups of $G \Rightarrow$ $\boxed{O(HK) = \dfrac{O(H)\,O(K)}{O(H \cap K)}}$

[$\because$ use $T = H \cap K$, $K = TK_1 \cup TK_2 \cup \ldots \cup TK_m \Rightarrow HK = HK_1 \cup HK_2 \ldots \cup HK_m$ $m = \frac{O(K)}{O(T)}$ & proceed.]

19) If $O(H) > \sqrt{O(G)}$ & $O(K) > \sqrt{O(G)}$

then $O(H \cap K) > 1$, i.e., $H \cap K \neq \phi$

20) eg $O(G) = 35$, st it can't have 2 subgroups of order 7.

Ans: Suppose H & K are 2 subgroups st $O(H) = O(K) = 7$ & $H \neq K$

since $H \cap K \leq H$

$\Rightarrow O(H \cap K) \mid O(H) = 7 \Rightarrow O(H \cap K) = 1$ or 7

if $O(H \cap K) = 1 \Rightarrow O(HK) = \frac{7 \times 7}{1} = 49 > O(G)$ #

if $O(H \cap K) = 7 \Rightarrow H \cap K = H \Rightarrow K = H \Rightarrow$ #

21) eg $O(G) = 2p$ [p is prime & $p > 2$]

st G has exactly one subgroup of order p.

Ans: suppose it has 2. $O(H) = O(K) = p$

$p > 2 \Rightarrow p^2 > 2p \Rightarrow p > \sqrt{2p} > p > \sqrt{O(G)}$

$\Rightarrow O(H \cap K) > 1$

$O(H \cap K) \mid O(H) \Rightarrow O(H \cap K) = p \Rightarrow H \cap K = H$

$\Rightarrow K = H$.

22) $H = \{I, (12)\}$ $K = \{I, (13)\}$. St HK is not subgroup of S_3

$O(S_3) = 6$ $O(HK) = 4$ $O(HK) \nmid O(S_3) \Rightarrow HK \not\leq S_3$.

23) Finite group cannot be expressed as union of 2 of its proper subgroups.

$\Rightarrow$ Let $G = HUK$ Now $e \in H$ & $e \in K \Rightarrow H \cap K \neq \phi$

$\therefore$ Either 1 of H & K has to have $> \frac{O(G)}{2}$ elts

$\Rightarrow \frac{O(G)}{2} < O(H) < O(G)$ But $O(H) \mid O(G) \Rightarrow$ #

24) No. of elts of order 'd' in a FINITE GROUP is multiple of $\phi(d)$

⇒ Cyclic Groups.

1) G is a group & there is $a \in G$ st $G = \{a^n / n \in \mathbb{Z}\}$ then G is cyclic group denoted by $\langle a \rangle$ or (a) or $\{a\}$

2) Cyclic group we can be both finite & infinite.

3) There may be more than one generators of a cyclic group.

4) Let G be any group & $a \in G$, then $H = \{a^n \mid n \in \mathbb{Z}\}$ is cyclic subgroup of G generated by a.

5) Set of residue classes modulo m forms cyclic group w.r.t $+_m$
If m is prime $1, 2, 3, \ldots, m-1$ all are generators of $\mathbb{Z}_m$

6) Every cyclic group is Abelian., but converse is not true [eg Abelian Klein-4 group]

7) If $G = \langle a \rangle$, then $G = \langle a^{-1} \rangle$

8) No of generators of an infinite cyclic group is two.

9) Every subgroup of a cyclic group is cyclic.
If $G = \langle a \rangle$ then $H = \langle a^m \rangle$ where m is the least +ve integer st $a^m \in H$
Converse is not true. eg $(\mathbb{Z}, +)$ & $(\mathbb{R}, +)$

10) A group of prime order is cyclic. [using Lagrange thm]

a) For a group with prime order, every element other than identity is a generator.

b) Every group of order less than 6 is abelian

c) Cyclic group need not have prime order. eg $\{\pm 1, \pm i\}$

11) If G is finite & $O(G) = n$, if $\exists\ a \in G$ st $O(a) = n$ then G is cyclic.
This is useful to check in a group is cyclic. check order of all the elts in G.

12) Every finite group of composite order possesses proper sub-group. [Proof: 2 cases : G is cyclic & G is non-cyclic]

13) ☆ If $G = \langle a \rangle$ & $o(a) = n$
then $G = \langle a^m \rangle$ iff $(m, n) = 1$

14) If G is finite cyclic group & $o(G) = n$ & $G = \langle a \rangle$
☆ then subgroups of G are subgroups generated by a^m where $m|n$.

15) Euler ϕ- function:
$\phi(n)$ = no of +ve integers less than n which are coprime to n.
∟ $\phi(1) = 1$ $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$ $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

a) No of generators of a finite group of order $n = \phi(n)$

Notation : U_n = group of integers relatively prime to n under multiplication mod n

16) eg $o(a) = 12$, $o(b) = 22$ & $\langle a \rangle \cap \langle b \rangle \neq \{e\}$. PT $a^6 = b^{11}$
$\langle a \rangle \cap \langle b \rangle \leq \langle a \rangle$ & $\langle a \rangle \cap \langle b \rangle \leq \langle b \rangle$
$\therefore o(\langle a \rangle \cap \langle b \rangle) = 2, 3, 4, 6, 12$
$o(\langle a \rangle \cap \langle b \rangle) = 2, 11, 22$
$\therefore o(\langle a \rangle \cap \langle b \rangle) = 2 \Rightarrow a^6 = b^{11}$

17) If G is cyclic, then there exists a subgroup H of G such that $|H| \mid |G|$ and for each positive integer $m \mid o(G)$, there exists a UNIQUE SUBGROUP of order m. $\Rightarrow \langle a^{n/m} \rangle$
$\Rightarrow$ $o(G) = 48 \Rightarrow$ G cannot be a 'simple' group.

⇒ Normal Subgroups :

1) Subgroup H of G is said to be a normal subgroup if $\forall\, x \in G$ & $\forall\, h \in H$ $\quad xhx^{-1} \in H$

   a) $H \trianglelefteq G$ iff $xHx^{-1} \subseteq H \quad \forall\, x \in G$

   b) $H \trianglelefteq G$ iff $x^{-1}Hx \subseteq H \quad \forall\, x \in G$

   c) $H = \{e\}$ & $H = G$ (improper subgroups) are normal subgroups

2) **Hamilton group** : Non-abelian group whose every subgroup is normal

3) **Simple group** : A group having no proper normal subgroup.
   eg every group of prime order.

4) $H \trianglelefteq G$ iff $xHx^{-1} = H$

5) $H \trianglelefteq G$ iff each left coset of H in G is a right coset of H in G

6) $H \trianglelefteq G$ iff product of 2 right (left) cosets of H in G is again a right (left) coset of H in G.
   $(Ha)(Hb) = Hab$ [$h \in H,\ x \in G \quad xhx^{-1} = (ex)(hx^{-1}) \in (Hx)(Hx^{-1}) \in H(xx^{-1}) \in H$].

7) If $H \trianglelefteq G$, then following statements are equivalent :

   a) $x^{-1}hx \in H$ for $x \in G$ & $h \in H$

   b) $xHx^{-1} = H$ for $x \in G$

   c) $xH = Hx$ for $x \in G$

   d) Set of right (left) cosets is closed wrt x^n.

8) Every subgroup of an abelian group is normal.

9) G is a group & $[G:H] = 2 \Rightarrow H \trianglelefteq G$

Proof: No of distinct cosets are 2.

Let $x \in G$, then H, Hx & H, xH are cosets.

if $x \in H$ $\quad xH = Hx \Rightarrow H \trianglelefteq G$

if $x \notin H$ $\quad H \neq Hx$, $H \neq xH$ & $G = H \cup Hx = H \cup xH$

Converse is false: eg. Quaternion Group. & $N = \{-1, +1\} \Rightarrow Hx = xH$ $[\because H \cap Hx \neq \phi]$

10) Intersection of normal subgroups is normal.

11) $N \trianglelefteq G$ & H is a complex of $G \Rightarrow NH = HN$

Cor. NH is a subgroup of G.

12) $H \leq G$, $N \trianglelefteq G \Rightarrow$ $H \cap N \trianglelefteq H$

$N \trianglelefteq HN$

13) $N \trianglelefteq G$, $M \trianglelefteq G \Rightarrow NM \trianglelefteq G$.

14) $M \trianglelefteq G$, $N \trianglelefteq G$ & $M \cap N = \{e\}$ st $mn = nm$ $\forall$ $m \in M$, $n \in N$

$n \in N$, $n^{-1} \in N \Rightarrow m^{-1}n^{-1}m^{-1} \in N \Rightarrow nmn^{-1}m^{-1} \in N$

$m \in M$, $m^{-1} \in M \Rightarrow nmn^{-1} \in N \Rightarrow nmn^{-1}m^{-1} \in M$

$\therefore nmn^{-1}m^{-1} \in M \cap N$

$\therefore nmn^{-1}m^{-1} = e$

$nm = mn$.

15) H is the only subgroup of finite order 'm' in G.

Then $H \trianglelefteq G$.

16) Every subgroup of a cyclic group is normal.

$[\because$ every cyclic group is abelian$]$

Proof: Let $H \leq G$, Define $K = \{ghg^{-1} \mid gh \in H\}$ for a given g

i.e., $K = gHg^{-1}$. It can be proved that $O(K) = O(H)$

using $f: H \to K$ st. $f(h) = ghg^{-1} \in K$

If $O(H) = m = O(k) \Rightarrow H = K \Rightarrow H = gHg^{-1} \Rightarrow Hg = gH$

$\Rightarrow H$ is normal.

⇒ Quotient group : [only for normal subgroups]

1) $H \trianglelefteq G$, set $\frac{G}{H}$ of all cosets of H in G wrt coset multiplication is a group.
(distinct / forget)

$$\frac{G}{H} = \{ Ha \mid a \in G \}$$

2) $o\left(\frac{G}{H}\right) = \frac{o(G)}{o(H)}$

3) Quotient group of an abelian group is abelian.

4) $A_n \trianglelefteq P_n$

5) QG of a cyclic group is cyclic $\left[\because \frac{G}{N} = \langle Na \rangle \right.$, $\left. G = \langle a \rangle \right]$

6) eg. P_3 is symmetric group on (a, b, c). write composition table for $\frac{P_3}{A_3}$.

$P = \{a, b, c\}$ $\quad P_3 = \{ I, (ab), (bc), (ac), (abc), (acb) \}$

$A_3 = \{ I, (abc), (acb) \}$

$o\left(\frac{P_3}{A_3}\right) = \frac{6}{3} = 2$ there are only 2 distinct cosets of A_3 in P_3. They are A_3 & $A_3(ab)$

$\therefore$ composition table :

	A_3	$A_3(ab)$
A_3	A_3	$A_3(ab)$
$A_3(ab)$	$A_3(ab)$	A_3

7) eg. $H \leq G$ st $x^2 \in H \ \forall \ x \in G$. PT $\frac{G}{H}$ is abelian.

H can be shown to be normal group. [$g^{-2} \in H$, $(gh)^2 \in H$, $h^{-1} \in H$
$\therefore g^{-2} ghgh^{-1} \in H$
, $g^{-1}hg \in H$ for $g \in G$, $h \in H$]

Now G/H is abelian if $Hxy = Hyx$

to show ⇒ $xy(x^{-1}y^{-1}) \in H$

like ⇒ $xx x^{-1}y x^{-1} yyy^{-1} \in H$

i.e., $x^2 (x^{-1}y)^2 y^{-2} \in H$

which is true as $x^2, (x^{-1}y)^2, y^2 \in H$ [proceed in reverse direction]

8) Conjugate Elements:

$a, b \in G$, then $a \sim b$ if $\exists\, x \in G$ st $a = x^{-1}bx$

ie, $a \sim b \iff a = xbx^{-1}$ for some $x \in G$.

a) $\sim$ is an equivalence relation

b) Equivalence class of 'a': $C(a) = \{x \in G \mid x \sim a\}$

$= \{x \in G \mid x = y^{-1}ay \;\; y \in G\}$

$\therefore$ $\boxed{C(a) = \{y^{-1}ay \mid y \in G\}}$.

c) Conjugacy partitions G into disjoint equivalence classes

$$G = \bigcup_{a \in G} [a]$$

9) Lemma: conjugacy in Permutation groups.

:→ If $f \in S_n$ be st $f: i \longrightarrow j$ then

$\theta f \theta^{-1} : \theta(i) \longrightarrow \theta(j)$ for all $\theta \in S_n$

Step: To compute $\theta f \theta^{-1}$: replace every symbol in f by its θ image.

eg $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$ $\theta(123)\theta^{-1} = (541)$

* To get conjugate classes of S_3 just put cycles of same length in the same class. Length of the cycle doesn't change on $\theta f \theta^{-1}$ operation.

eg. for S_3 classes are $\{I\}, \{(12),(13),(23)\}, \{(123), (132)\}$

10) In an abelian group, $o(C(a)) = 1$ • $[\because C(a) = \{a\}]$

10) Normalizer of element of a group:

$$N(a) = \{ x \in G \mid ax = xa \}$$

$N(e) = G$

if G is abelian $N(a) = G$.

$$O(Cl(a)) = \frac{O(G)}{O(N(a))} = [G : N(a)] = i_G(N(a))$$

Proof: Σ: set of distinct right cosets of $N(a)$ in G.

Define $f: C(a) \longrightarrow \Sigma$

as $f(x^{-1}ax) = N(a).x \quad , x \in G.$

Easy to prove f is well-defined, one-one & onto.

11) Class equation of a group:

$$O(G) = \sum_{a \in G} i_G(N(a)) = \sum_{a \in G} \frac{O(G)}{O[N(a)]}$$

Sum is over 1 element in each conjugate class.

12) Self-Conjugate Element of a group:

$a = x^{-1}ax \quad \forall x \in G$. They are aka invariant elts.

a) Centre of group: $Z = \{ z \in G \mid zx = xz \ \forall x \in G \}$

= set of all self-conjugate element

b) $Z \leq G$ & $Z \trianglelefteq G$

c) $a \in Z$ iff $N(a) = G$

$a \in Z$ iff $O(N(a)) = O(G)$ if G is finite.

13) Second form of class equation:

If G is finite, $O(G) = O(Z) + \sum_{a \notin Z} \frac{O(G)}{O(N(a))}$

↓ Sum over 1 elt from each conjugate class with more than 1 element.

14) Important application of 2nd form :

a) $O(G) = p^n$, p is prime then $O(Z) > 1$ [∵ use lagrange theorem on $N(a) \leq G$.]

b) $O(G) = p^2$, p is prime then G is abelian

$O(Z) \mid O(G) \Rightarrow O(Z) = p$ or p^2

If $O(Z) = p^2 \Rightarrow Z = G \Rightarrow G$ is abelian

If $O(Z) = p \Rightarrow O\left(\frac{G}{Z}\right) = p$ ⊛ $\frac{G}{Z}$ is cyclic $\Rightarrow G$ is abelian

Important Results to remember: [Group - G, $H \leq G$, $N \trianglelefteq G$]

i) If $\frac{G}{N}$ is abelian, G need not be abelian

But G is abelian $\Rightarrow \frac{G}{H}$ is abelian [$H \trianglelefteq G$ as subgroup of abelian group is normal]

ii) If $\frac{G}{N}$ is cyclic, G need not be cyclic

But G is cyclic $\Rightarrow \frac{G}{H}$ is cyclic. [Here $H \trianglelefteq G$ as subgroup of cyclic group is normal]

iii) If $\frac{G}{Z}$ is cyclic $\Rightarrow G$ is abelian

$\frac{G}{Z} = \langle Za \rangle \Rightarrow Zx = Za^n \Rightarrow xa^{-n} \in Z$; $Zy = Zb^m \Rightarrow ya^{-m} \in Z$ ⇒ Apply commutativity in Z to xa^{-n} & ya^{-m}

$Zx \cdot Zy = Zxy = Za^{m+n}$

$= Za^m \cdot Za^n$

$= Zy\,Zx$

⇒ Homomorphism, Isomorphism of groups:

Homo
Homo + onto
Homo + 1-1 : Iso
Homo + 1-1 + Into : mono
Homo + onto + 1-1 : ≅ isomorphism
Self Homo + into : endo
Self Homo + into + 1-1 : auto

1) $(G, \cdot)$, $(G', *)$ are 2 groups.

$f: G \longrightarrow G'$ is a homomorphism if

$$f(a \cdot b) = f(a) * f(b) \quad \forall\ a, b \in G$$

2) If f is onto, G' is called homomorphic image of G. $(G \simeq G')$. onto-homomorphism ≡ epimorphism

3) Isomorphism: f is one-one homomorphism

$G \cong G'$: f is one-one, onto homomorphism.

G' is called isomorphic image of G.

[Monomorphism = Isomorphism + Into]

4) Endomorphism: Homomorphism into itself, ie. $G \longrightarrow G$

Automorphism: Isomorphism into itself, ie. 1-1 endomorphism

5) Properties of Homomorphism:

a) $f(e) = e'$ e is identity in G & e' in G'

b) $f(a^{-1}) = [f(a)]^{-1}$

c) $f: G \longrightarrow G'$ homomorphism, then $(f(G), \cdot) \leq (G', *)$

, ie, $f(G)$ is subgroup of G'

$$f(G) = \{ f(a) \mid a \in G \}$$

d) Homomorphic image of abelian group is abelian

But converse is not true. eg P_2, A_2 & $\frac{P_3}{A_3}$ is homoimage of P_3 of order 2

Converse holds for isomorphism

e) G is a group & G' is a non-empty set & There is a mapping 'f' from G onto G' st $f(ab) = f(a) \cdot f(b)\ \forall a, b \in G$ then G' is a group.

Kernel of Homomorphism :

$$\text{Kernel } f = \{ x \in G \mid f(x) = e' \} = K$$

a) $\text{Ker } f \neq \phi$ as $e \in \text{Ker } f$.

b) $f: G \to G'$ (into) homomorphism, then $\boxed{\text{Ker } f \trianglelefteq G}$

[Do not forget to prove that Ker f is a subgroup before going for $xhx^{-1} \in H$ definition]

c) $\text{Ker } f = \{e\} \iff f$ is isomorphism of G onto G'

[Here f is already an onto- homomorphism]

d) $f: G \to G'$ · homomorphism onto G'.

Let $\text{Ker } f = K$ & $a \in G$ st $f(a) = a'$

set of all elements of G which have image a' is the coset Ka of K in G.

ie, $Ka = \{ x \mid f(x) = f(a) = a' \}$

Natural | Canonical Homomorphism :

$f: G \to \frac{G}{N}$ where $N \trianglelefteq G$ & $f(x) = Nx$ for $x \in G$

f is homomorphism G onto $\frac{G}{N}$

∴ Every quotient group of a group is a homomorphic image of the group.

Also $\text{Ker } f = N$

Fundamental Theorem on Homomorphism of groups :

Every homomorphic image of a group G is isomorphic to some quotient group of G.

⇒ If $f: G \to G'$ is an onto- homomorphism with kernel K then $\frac{G}{K} \cong G'$

Proof: $K \trianglelefteq G$ & $f(a) \in G'$ $\forall$ $a \in G$. $\left\{\frac{G}{K} \cong f(G)\right\}$

Define $\phi : \frac{G}{K} \to G'$ st $\phi(Ka) = f(a)$

Show that ϕ is well-defined, one-one & onto.

9) $f: G \to G'$ is an homomorphism
$a \in G$ st $O(a)$ is finite, then $O(f(a)) \mid O(a)$
Also if f is isomorphism $\Rightarrow O(f(a)) = O(a)$

$\therefore$ for isomorphism $f: G \to G'$

i) $f(e) = e'$
ii) $f(a^{-1}) = [f(a)]^{-1}$
iii) $O(a) = O(f(a))$.

} useful in constructing isomorphic mapping, i.e, it should preserve identity, inverses & order.

eg. find $f: G \to G'$ - isomorphic mapping where
$G = (\{0,1,2,3\}, +_4)$ $G' = \{+1, -1, +i, -i\}$
[$\because$ identities]

$f(0) = 1$

$f(1) = i$ or $-i$
$f(2) = -1$
$f(3) = -i$ or i

$f(i) = i$ or $-i$
$f(-1) = -1$
$f(-i) = -i$ or i

$\therefore$ $f(2)$ has to be -1
$f(1)$ can be i or $-i$
$f(3)$ can be i or $-i$

10) If H & N are subgroups of G & $N \trianglelefteq G$, then

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

show $\phi: H \to \frac{HN}{N}$ is onto homomorphism where $\phi(x) = Nx$

then using 1st theorem $\frac{H}{\text{Ker}\,\phi} \cong \frac{HN}{N}$, now prove $H \cap N = \text{Ker}\,\phi$

11) Homomorphic image of infinite group can be finite
Isomorphic image of infinite group can never be finite

12) Any infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ of all integers. So $(\mathbb{Z}, +)$ is the one & only infinite cyclic group upto isomorphism ($f: \mathbb{Z} \to G$, $f(n) = a^n$ where $G = \langle a \rangle$ isomorphism)

13) Total no of homomorphisms from Z_m to Z_n are $\gcd(m,n)$

Proof: for any $[a] \in Z_m$ $f([a]) = a\, f([1])$

so $f([1])$ determines the homomorphism.

Now $O(f([1])) \mid O([1])$ & $O(f([1])) \mid O(Z_n)$

[∵ order of image divides order of elt] [∵ $o(a) \mid o(G)$]

$\therefore O(f[1]) = \gcd(m,n)$. [work on these lines]

14) If G is a finite cyclic group of order n $G \simeq \frac{Z}{nZ} \simeq Z_n$.

define: $f: Z \longrightarrow G$.

$f(m) = a^m$ where $G = \langle a \rangle$

f is epimorphism & $\ker f = nZ \Rightarrow \frac{Z}{nZ} \simeq G$

define: $\phi: Z \to Z_n$

$\phi(t) = [t]$

ϕ is epimorphism & $\ker\phi = nZ \Rightarrow \frac{Z}{nZ} \simeq Z_n$.

Cor. (1) Any 2 finite cyclic group of same order are isomorphic

(11) For each prime p, ∃ one & only one group of order p, Z_p upto isomorphism.

15) eg. Show that Z_4 is not homomorphic image of Z_{16}

Ans suppose ∃ $f: Z_{16} \to Z_4$ epimorphism

$\Rightarrow \frac{Z_{16}}{\ker f} \simeq Z_4 \Rightarrow O\left(\frac{Z_{16}}{\ker f}\right) = O(Z_4)$

$\frac{16}{|\ker f|} = 4 \Rightarrow \#$

16) Upto isomorphism, there are only 2 groups of order 4 = Z_4 & Klein-4

amazing proof in notes ← ☆ there are only 2 groups of order 6 = Z_6 & S_3

lots of concepts in single proof

⇒ RINGS & FIELDS

(1) Conditions

(i) $(R, +)$ is an abelian group (5 conditions)

(ii) $(R, *)$ is a semigroup (2 conditions)

(iii) $+, *$ are distributive (2 conditions)

$a \cdot (b+c) = a \cdot b + a \cdot c$ (LDL)

& $(b+c) \cdot a = b \cdot a + c \cdot a$ (RDL)

Ring with unity : if $\exists\ 1 \in R$ st $a \cdot 1 = 1 \cdot a = a$ $\forall a \in R$

commutative Ring : commutativity holds for $(*)$ (multiplication)

Division Ring : Non-zero elts. form a group wrt x^n
(atleast 2 elts, unity, inverse for $a \neq 0$).

Zero Divisor of a Ring : $\exists\ a, b \in R$ st $a = 0$, $b \neq 0$ but $ab = 0$

eg $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Integral Domain : commutative Ring without zero divisors.
(no unity needed)

(2) Field : commutative Division Ring.

⇓

(11 conditions) = [5 for $(R, +)$ abelian] + [5 for $(R, *)$ abelian] + distributivity.

) Properties : If R is a ring & $0, a, b \in R$

(a) $a0 = 0a = 0$

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

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

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

(4) Null Ring | Zero Ring : $(\{0\}, +, \cdot)$

Note : I is not a field (only an ID)
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
$\mathbb{Q}(\sqrt{2}) = \{ a+b\sqrt{2} \mid a,b \in \mathbb{Q} \}$ is a field.
$\mathbb{Z}(\sqrt{2}) = \{ a+b\sqrt{2} \mid a,b \in \mathbb{Z} \}$ is not a field.

(5) Cancellation Laws in a Ring :

$a,b,c \in R$, if $a \neq 0$, $ab = ac \Rightarrow b = c$
$ba = ca \Rightarrow b = c$

then we say cancellation laws apply

6) THM: Ring R is without ZD $\Leftrightarrow$ Cancellation laws hold in R

Ques R is a unity Ring , $x \neq 0 \in R$ & $\exists$ a unique y such that $xyx = x$. Show That $xy = yx = 1$

Let $xa = 0$
Now $x(y+a)x = xyx + xax$
$= xyx + 0x = xyx + 0 = xyx = x$

$\Rightarrow y + a = y$ [$\because$ y is unique]
$\Rightarrow a = 0$ $\therefore$ $xa = 0 \Rightarrow a = 0$

Now $xyx = x \Rightarrow xyx - x1 = 0 \Rightarrow (xy-1)x = 0$
$\Rightarrow xy - 1 = 0 \Rightarrow xy = 1$

Similarly $yx = 1$.

7) Every field is an Integral Domain

8) & Finite Integral Domain is a field

Use pigeonhole principle : $F = \{a_1, a_2, \dots, a_n\}$ is an ID
Take $a \in R F$ & $a \neq 0 \Rightarrow aa_1, aa_2, \dots, aa_n \in F$ & all are distinct
Now one of $aa_i = 1$ ($\because$ ID) $\Rightarrow a^{-1} = a_i \Rightarrow$ Inverse of every non-zero elt exists

9) Example: Composition Tables.

$F = (\{0,1,2,3\}, +_4, \times_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\Rightarrow$ Not a field. Zero divisors present

10) THM: Let p be a prime no. $I_p = \{0, 1, 2, 3, \dots, p-1\}$ is a field wrt $+_n$ & x_n modulo p.

Remember in proofs: $(a +_p b) \times_p c = (a \times_p c) +_p (a \times_p b)$

11) If $(I_p, +_p, \times_p)$ is a field then p is prime

(residue class)

Suppose p is not prime, then $p = mn$ $1 < m < p$, $1 < n < p$

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

$= \bar{m} \cdot \bar{n} = 0$

Also $\bar{m} \neq 0$ & $\bar{n} \neq 0$ due to

$\therefore$ I_p has zero divisors

but I_p is a field. Hence #.

12) Boolean Ring: every elt is idempotent, ie, $\forall\, a \in R, a^2 = a$

Every Boolean Ring is abelian [Steps: show $(a+a) = 0$; show $(a+b) = 0$; show $ab = ba$]

13) Fields & IDs contain only 2 idempotent elts 0 & 1.

14) ID has no nilpotent other than 0.

Nilpotent: $\exists\, n$ st $a^n = 0$, then a is nilpotent.

$\Rightarrow$ a, b are nilpotent in a non-commutative ring (read Matrix for easy understanding) then $a+b$, $a \cdot b$ are not nilpotent.

eg $A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ $A+B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $AB = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Remember: $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ & $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ are idempotent

$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ & $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are nilpotent.

15) R is a ring, $a, b \in R$: if ab is nilpotent, ba is nilpotent.

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

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

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

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

$\Rightarrow$ $xy = yx$.

16) Opposite Ring: $(R, +, \cdot)$ is a Ring, then $(R, +, \circ)$ is also a Ring where $x \circ y = y \cdot x \ \forall y, x \in R$.

⇒ SUBRINGS

1) Defn: Let R be a ring. S be a non-empty subset of R.
If S is a Ring wrt $(+, \cdot)$, then S is subring.

2) Let F be a field & $S \subseteq F$
If S is a field wrt b-op's, then S is subfield of F.

If S is subfield of F, then
$(S, +)$ is subgroup of $(F, +)$
$(S - \{0\}, \cdot)$ is subgroup of $(F - \{0\}, \cdot)$.

3) S is a subring of R iff $\forall\ a, b \in S \Rightarrow$
$a - b \in S$
$ab \in S$.

F is a field. K is subfield iff $\forall\ a, b \in K \Rightarrow$
$a - b \in K$
$ab^{-1} \in K$.

(very intuitive)

4) Centre of a Ring is a subring
Centre of a Division Ring is a field.

Ex. Subring of a Ring with unity may fail to be a subring with unity.
eg $R: \{I, +, \cdot\}$ $1 \in R$. $S: \{2I, +, \cdot\}$ $1 \notin S$.

Subring of non-commutative Ring may or may not be commutative
(Read M_2 matrix ring)

Ring has no unity but subring has unity.

$$R = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \qquad S = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$$

Subring with different unity than parent Ring.

$R = \mathbb{Z}_{10}$ $\quad S = \{0, 2, 4, 6, 8\}$ $\quad (X_{10})$.

unity = 1 $\quad$ unity = 6.

* Sum of 2 subrings maynot be a subring eg $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix}$

$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \; a,b,c,d \in \mathbb{R} \right\}$ $\quad S = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle| \; x \in \mathbb{R} \right\}$

unity $= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $\quad$ unity $= \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$

5) Characteristic of a Ring:

R is said to be of finite characteristic, if there exists a +ve integer 'n' st $na = 0 \;\forall\; a \in R$.

Smallest +ve $n = p$ is called the char of R

$\text{char } R = p$.

Characteristic = 0 or infinite if $\nexists\, n$ st $na = 0 \;\forall\; a \in R$.

Examples: $\text{Char } \mathbb{Z} = 0$ $\quad \text{Char } \mathbb{Q} = 0$ $\quad \text{char } \mathbb{R} = 0$

$\text{Char } \mathbb{Z}_n = n$ $\quad \mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$.

6) R is a ring with unity,

$\text{char } R = p\,(>0)$ iff p is the least +ve integer st $p \cdot 1 = 0$

⇒ Characteristics of a Ring with unity is the order of the unit element regarded as the member of the additive group $(R, +)$

7) Characteristic of an ID is either a prime or zero.

Let char $R = p\ (\neq 0)$.

Suppose p is not prime, $\Rightarrow p = mn$

then $\forall\ a \in R$, $pa = 0$

$(mn)a = 0$

$(mn)ab = ob = 0$

$(ma)(nb) = 0 \quad 1 < m, n < p$

Now either one of ma & $nb = 0$ [$\because$ R is ID]

$\therefore$ $ma = 0$ but $m < p$ } contradiction.
or $nb = 0$ but $n < p$

8) Same holds for a field $\because$ and also for a Division Ring

9) Char of a boolean Ring is 2. [use $(a+a)^2 = (a+a)(a+a)$
$(a+a) = a+a+a+a$
$\vdots$]

10) Order of a finite field F is p^n for some prime 'p' & some +ve integer 'n'

First prove char $F \neq 0$ [$\because$ F is finite, so for some $i \neq j$, $ia = ja$
$\Rightarrow (i-j)a = 0$]

$\therefore\ \forall\ a \in F$, $pa = 0$ (p has to be prime)

Now $O(a) = p$ in group $(F, +)$ see #7.

Lagrange's $\Rightarrow$ $O(a) \mid O(F,+) \Rightarrow O(F) = p^n$ for some n.

11) If R is finite (non 0) ID, then $O(R) = p^n$ where p is prime & n is a +ve integer.

12) * If $a \in F$, then $a^{p^n} = a$.

Simple take $(F - \{0\}, *)$ as the * group with order $p^n - 1$. $\Rightarrow a^{p^n - 1} = e \Rightarrow a^{p^n} = a$.

⇒ IDEALS

1) Let $(R, +, \cdot)$ be a Ring. A non-empty subset S of a ring R is called an ideal (2 sided) of R if

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

(b) $s \in S$ and $r \in R \Rightarrow sr \in S$ & $rs \in S$.

Left ideal : only $rs \in S$

Right ideal : only $sr \in S$

2) Unit Ideal : R itself is an ideal of R

Null Ideal : $S = \{0\}$ is a null ideal of R.

3) Commutative Ring : every ideal is doubled sided.

4) I is ring of integers and $n \in I$. then

$\boxed{S = (n) = \{ nx \mid x \in I \}}$ is an ideal of I.

* I is subring of $\mathbb{Q}$ but not an ideal

Similar for $[\mathbb{Q}$ & $\mathbb{R}]$ & $[\mathbb{R}$ & $\mathbb{C}]$

Remember : ideal ⇒ subring

but subring ⇏ ideal (eg. I, $\mathbb{Q}$)

5) * VVI If S is an ideal of a ring R with unity, then $S = R$. & $1 \in S$

6) Field has no proper ideals.

7) Intersection of arbitrary family of ideals is an ideal.

Repeat the subring result for union here also ÷

8) If R is a commutative ring & $a \in R$, then

$\boxed{Ra = \{ra \mid r \in R\}}$ is an ideal of R.

Corr: A commutative ring R with unit element is a field if R has no proper ideals.

* If R is a ring with unit element & R has no proper ideals, then R is a division ring.

9) If S_1 & S_2 are ideals of R, then $S_1 + S_2$ is an ideal of R.

$S_1 + S_2 = \{a+b \mid a \in S_1, b \in S_1\}$.

10) Product of ideals:

$S_1 S_2 = \{ a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_i \in S_1,\ b_i \in S_2 \text{ & } 1 \le i \le n \text{ & } n > 0 \}$

is an ideal of R.

11) If A & B are 2 ideals of ring R, then $AB \subseteq A \cap B$

$\because$ AB, $A \cap B$ are ideals of R

Let $x \in AB$ then $x = a_1b_1 + a_2b_2 + \cdots + a_nb_n$

Now $a_i \in A$, $b_i \in R \Rightarrow a_ib_i \in A$ ($\because A$ is ideal)

$\Rightarrow a_1b_1 + \cdots + a_nb_n \in A$

$\Rightarrow x \in A$

Similarly $x \in B \Rightarrow x \in A \cap B$

$\therefore x \in AB \Rightarrow x \in A \cap B$

$\Rightarrow$ $AB \subseteq A \cap B$.

Similar for $AB \subseteq A+B$. [$\because a_1b_1 \in A$ & $a_2b_2 + \cdots + a_nb_n \in B$]

12) $Z(R)$, the centre of a ring R, is only a subring & need not be an ideal of R.

eg. $R = M_2(\mathbb{Z})$ then $Z(R) = \left\{ \begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix} \mid p \in I \right\}$.

$S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in R \qquad A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in Z(R)$

$SA = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \notin Z$

13) Co-Maximal Ideals: 2 ideals A & B satisfying $A+B = R$

Que Let A, B be comaximal ideals of a commutative ring with unity. ST $AB = A \cap B$

$AB \subseteq A \cap B$ (point #11)

Now we show $A \cap B \subseteq AB$.

Let $x \in A \cap B$. Also $1 \in R \Rightarrow 1 \in A+B$.

$\Rightarrow 1 = a+b$ for some $a \in A$ & $b \in B$.

Now $x = x \cdot (1) = x(a+b) = xa + xb$.

Now $x \in A$ & $b \in B \Rightarrow xb \in AB$

Also $x \in B$ & $a \in A \Rightarrow ax = xa \in AB$ [commutative]

$\Rightarrow xa + xb \in AB$ [$\because AB$ is an ideal]

$\Rightarrow x(a+b) \in AB$

$\Rightarrow x \in AB$

$\therefore x \in A \cap B \Rightarrow x \in AB \Rightarrow A \cap B \subseteq AB$.

14) If A, B, C are ideals of R, then $\boxed{A(B+C) = AB + AC}$

TRICK: for harder side $b = b \in B \Rightarrow b + 0 \in B + C$

$\Rightarrow B \subseteq B+C \Rightarrow AB \subseteq A(B+C)$

Also: $C \subseteq B+C \Rightarrow AC \subseteq A(B+C)$

$\Rightarrow AB + AC \subseteq A(B+C)$

Ques A, B, C are ideals of R & $B \subseteq A$,

PT: $A \cap (B+C) = B+(A \cap C) = (A \cap B)+(A \cap C)$

Let $x \in A \cap (B+C)$. AB, A+B, A∩B are all ideals

Then $x \in A$ and $x \in B+C$

We have $x \in B+C \Rightarrow x = b+c$. for some $b \in B$ & $c \in C$

Thus $b+c \in A$ $(\because x \in A)$

& $b \in A$ $(B \subseteq A)$

$\Rightarrow b+c-b \in A$ $(\because A$ is ideal$)$

$\Rightarrow c \in A$

$\therefore c \in C$ & $c \in A \Rightarrow c \in A \cap C$

$\therefore x = b+c \Rightarrow x \in B+(A \cap C)$

$\Rightarrow A \cap (B+C) \subseteq B+(A \cap C)$ ——— (I)

Let $x \in B+(A \cap C)$

Then $x = b+t$ for $b \in B$ & $t \in A \cap C$

$\Rightarrow t \in A$ & $t \in C$

$\Rightarrow x \in B+C$ $[\because b \in B$ & $t \in C]$

Also $b \in B \Rightarrow b \in A$

Thus $b+t \in A$ $[\because t \in A]$

$\therefore x \in A$

$\Rightarrow x \in A \cap (B+C)$ ——— (II)

So $A \cap (B+C) = B+(A \cap C)$

Since $B \subseteq A$, $A \cap B = B$

$\therefore A \cap (B+C) = (A \cap B)+(A \cap C)$.

15) Radical of A : R is a commutative Ring & A is an ideal of R

then Radical of $A = \sqrt{A} = \{ x \in R \mid x^n \in A$ for some +ve $n \in I \}$

$\sqrt{A}$ is an ideal of R

(i) $A \subseteq \sqrt{A}$

(ii) $\sqrt{\sqrt{A}} = \sqrt{A}$

(iii) If R has unity & $\sqrt{A} = R$, then $A = R$.

Ques

16) R is a ring with unity. If R has no right ideals except R & {0}, pt R is a division ring.

Use the ideal $aR = \{ar \mid r \in R\}$ for $a \neq 0$

easy to prove $aR = R \Rightarrow \exists\ b \in R$ st $ab = 1$ → [$\because 1 \in R$]

Also to prove $ba = 1$

use → $ba = ba \cdot 1 = (ba)\cdot(bc)$ [If $b \neq 0$, $\exists\ c$ st $bc = 1$ using]

$= b(ab)c$

$= (b)(1)(c) = bc = 1$

$\Rightarrow ab = ba = 1$

$\therefore$ R is ring with unity & non-zero elts have inverse.

Improvisation

17) R is a ring with more than 1 elt st $aR = R\ \forall\ a \neq 0 \in R$

then R is a division ring.

If $x \neq 0 \in R$ & $y \neq 0 \in R$, then $xR = R$ & $yR = R$

Now $0 = xy \Rightarrow 0 \cdot R = (xy)R = R$ $x(yR) = xR = R$

$\therefore 0 \cdot R = R$

(i) Have to prove absence of zero divisors

$\Rightarrow R = \{0\}$ which is a contradiction

(ii) Have to prove common

$\therefore x \neq 0, y \neq 0 \Rightarrow xy \neq 0$. —(1)

Since $R \neq \{0\}$ $\exists\ a \in R$ st $aR = R$ ($a \neq 0$)

e for $\neq x \in R$

(iii) Have to prove each x has inverse

$a \in R \Rightarrow a \in aR \Rightarrow a = ae$ for some $e \in R$

Now $e \neq 0$, o/w $a = a0 = 0 \Rightarrow \#$

$\therefore ae = a$

$ae^2 = ae \Rightarrow a(e^2 - e) = 0$

$\Rightarrow e^2 - e = 0$ [using (1)]

Let $x \in R$, then $(xe - x)e = xe^2 - xe = xe - xe = 0$

$\therefore xe - x = 0 \Rightarrow xe = x$ $\therefore$ e is right identity in R

Now Let $x \neq 0 \in R$, then $xR = R$, since $e \in R \Rightarrow e \in xR$

$\therefore \exists\ y$ st $e = xy \Rightarrow y$ is right inverse $\Rightarrow$ R is Division ring.

15) Ideal generated by a subset of Ring :

Let S be a subset of ring R.

Ideal U is said to be generated by S if it is the smallest ideal containing S

i.e, (i) $S \subseteq U$

(ii) for any ideal V of R, if V contains S, then $U \subseteq V$.

or $S \subseteq V \Rightarrow U \subseteq V$

Ideal U generated by S is (S) or $\langle S \rangle$ or $\{S\}$

Ques. If A & B are two ideals of a ring R, show that A+B is an ideal generated by $A \cup B$, i.e,

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

easy to show $A \subseteq A+B$ & $B \subseteq A+B \Rightarrow A \cup B \subseteq A+B$ — (1)

Let I be an ideal st $A \cup B \subseteq I$ — (2)

we have to prove $A+B \subseteq I$

Let $x \in A+B \Rightarrow x = a+b$ for some $a \in A$ & $b \in B$

Since $A \subseteq A \cup B$ & $B \subseteq A \cup B$

$a, b \in A \cup B$

$\Rightarrow a, b \in I$ (from (2))

$\therefore a+b \in I$ ($\because$ I is ideal)

$\therefore x \in I \Rightarrow A+B \subseteq I$.

$\therefore$

⇒ PRINCIPAL IDEAL

(1) * Ideal U of a ring R generated by a single elt $S=\{a\}$

$U = (a)$ or $\langle a \rangle$

* U is PI if $\exists\ a \in U$ st for any ideal V of R
$a \in V \Rightarrow U \subseteq V$

* U is the smallest ideal containing 'a'

(2) Null ideal is generated by 0 ; Unit ideal by unit elt.

(3) Every ideal of a field is a PI [∵ there are no proper ideals in F]

4) THM: R is commutative Ring with unity & $a \in R$.

then $U = \{ra \mid r \in R\}$ is a PI of R generated by 'a'

Steps: Prove U is an ideal (easy).

Let V be an ideal st $a \in V$

Now let $x = ra \in U$

$r \in R$ & $a \in V \Rightarrow ra \in V$

$\Rightarrow x \in V$

$\therefore U \subset V$

5) If R is commutative without unity, then

$(a) = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$

↳ to ensure $a \in (a)$ as $1 \notin R$.

9 If R is not commutative, then

Left ideal generated by $a = \langle a \rangle_L = \{ra \mid r \in R\}$

Right ideal generated by $a = \langle a \rangle_R = \{ar \mid r \in R\}$

Ideal generated by $a = \langle a \rangle = \{sar + na \mid s, r \in R, n \in \mathbb{N}\}$

PRINCIPLE IDEAL RING:

Ring R is PIR if every ideal in R is a PI.

PRINCIPLE IDEAL DOMAIN:

A commutative Ring without zero divisors & with unity element is a principle ideal domain if every ideal S in R is a PI.

→ { * PID = ID + unity + every ideal is PI
  * Need unity to generate R }

Every field is a PID

* $(I, +, \cdot)$ is a PID
  Ring of Integers.

Proof: I is a commutative ring with unity w/o ZD.

Let S be an ideal of I

If $S = \{0\}$ ⇒ generated by 0.

If $S \neq \{0\}$, then Let $a \neq 0 \in S \Rightarrow -a \in S$

∴ S has both +ve & -ve elts.

Let s be the smallest elt in S. & $p \in S$.

then by division theorem : $p = qs + r$ $(q \in I, 0 \le r < s)$

Now $q \in I$, $s \in S \Rightarrow qs \in S \Rightarrow -qs \in S$

$\Rightarrow p - qs \in S \Rightarrow r \in S$, but $r < s$ &

∴ $r = 0 \Rightarrow p = qs$.

∴ $p \in S \Rightarrow p = sq$ for some $q \in I$.

Hence S is a PI of I generated by S.

Always remember the Division Theorem usage.

Most Handy.

Quotient Rings (or) Rings of Residue Classes

1) S is an ideal of ring R

Then S is a subgroup over $+^n$,

Therefore $S+a = \{ s+a \mid s \in S \}$ is called Right coset

$\because$ R is abelian group wrt $+^n$

$S+a = a+S$

Residue classes of S in R = cosets of S in R.

Note: if $a, b \in R$ then $S+a = S+b \Leftrightarrow a-b \in S$

$a \in S \Leftrightarrow S+a = S$

2) $\frac{R}{S} = \{ S+a \mid a \in R,\ S$ is an ideal of $R \}$ is the set of all residue classes of S in R

3) THM: $\frac{R}{S} = \{ S+a \mid a \in R,\ S$ is an ideal of $R \}$ forms a rings for the two compositions in $\frac{R}{S}$ defd as:

$(S+a) + (S+b) = S + (a+b)$ (addition of Residue classes)

$(S+a)(S+b) = S + ab$ ($\times^n$ of Residue classes)

NOTE: In proof imp^t to show that these are well defd.

if $S+a = S+a'$ & $S+b = S+b'$

then $(S+a) + (S+b) = (S+a') + (S+b')$

& $(S+a)(S+b) = (S+a')(S+b')$

TIP: $S+a = S+a' \Rightarrow a' = 0+a' \in S+a' \Rightarrow a' \in S+a \Rightarrow a' = \alpha+a$, $\alpha \in S$.

Sly $b' = \beta + b$ $\beta \in S$.

$\therefore$ $a'+b' = \alpha+\beta+a+b \Rightarrow (a'+b') - (a+b) = \alpha+\beta \in S \Rightarrow S+(a+b) = S+(a'+b')$

Similar for $S+ab = S+a'b'$

4) Quotient Ring / Residue Class Ring :

$\left(\frac{R}{S}, +, \cdot\right)$ where $+, \cdot$ are defined in previous result

Also denoted as $[a]$ or $\bar{a} = S+a$

then $+^n$: $[a]+[b] = [a+b]$

$\times^n$: $[a][b] = [ab]$

5) If $\frac{R}{S}$ is the quotient ring, then

(i) R is commutative $\Rightarrow$ $\frac{R}{S}$ is commutative

(ii) R has unity $\Rightarrow$ $\frac{R}{S}$ has unity

(iii) R is boolean ring $\Rightarrow$ $\frac{R}{S}$ is boolean ring

6) PRIME IDEAL : Ideal P is prime ideal of R, if

if for any $a \in R$, $b \in R$; $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$

eg. - ideal $P = \{0\}$ in $\mathbb{Z}$ (ring of integers)

- for any prime p, $(p) = \{px \mid x \in \mathbb{Z}\}$ is prime ideal of $\mathbb{Z}$

(4) is not prime ideal as $12 = 4 \times 3 \in (4)$

But $2, 6 \notin (4)$

** 6.a) Let R be a commutative Ring.

Ideal P of R is a prime ideal iff $\frac{R}{P}$ is an integral domain

7) MAXIMAL IDEAL : Ideal $M \neq R$ is maximal ideal of R if there doesn't exist any proper ideal b/w M & R

ie, if U is an ideal st $M \subset U \subset R$ then either $M = U$ (or) $U = R$

⇒ MI is not included in any other ideal except R.

eg Let R = I

$S_2 = \{2n \mid n \in I\} = \{\dots -6, -4, -2, 0, 2, 4, 6 \dots\}$

$S_3 = \{3n \mid n \in I\} = \{\dots -9, -6, -3, 0, 3, 6, 9 \dots\}$

$S_4 = \{4n \mid n \in I\} = \{\dots -12, -8, -4, 0, 4, 8, 12 \dots\}$

$S_5 = \{5n \mid n \in I\} = \{\dots -15, -10, -5, 0, 5, 10, 15 \dots\}$

$S_6 = \{6n \mid n \in I\} = \{\dots -18, -12, -6, 0, 6, 12, 18 \dots\}$

$S_6 \subset S_3 \subset I$, $S_6 \subset S_2 \subset I$

$S_5 \subset I$ $S_4 \subset S_2 \subset I$ ⇒ S_2, S_3, S_5 are MI

$S_3 \subset I$ $S_2 \subset I$ S_4, S_6 not MI.

⇒ nI is maximal iff n is prime.

⇒ $\{0, 2, 4, 6\}$ is maximal ideal of Z_8

* NOTE: Look for subgroups for ideal possibilities

** Write nI or (n) as the maximal ideal where n is prime

eg maximal ideals of Z_6 : (2), (3)

maximal ideals of Z_{12} : (2), (4), (6), (3) are proper ideals

& (2), (3) are maximal ideals.

8) $\{0\}$ is the only maximal ideal of a field F.

Ques ST (4) is the MI of ring E of even integers.

Steps : $2 \notin (4)$, $(4) \neq E$

Let U be an ideal st $(4) \subset U \subset E$, $(4) \neq U$

Then ∃ some $x \in U$ st $x \notin (4)$ [otherwise $U \subseteq (4) \Rightarrow U = (4)$]

⇒ x is even integer not divisible by 4 ⇒ $x = 4n+2$

⇒ $2 = 4x - 4n$ Now $[x \in U \& 4n \in U \Rightarrow x - 4n \in U] \Rightarrow (2) \in U$

⇒ $(2) \subseteq U \Rightarrow E = U$.

PID & UFD

Eg) **Thm**: $M = (n_0)$ is an maximal ideal of $\mathbb{Z}$ iff n_0 is a prime number.

Proof: Easy to show that M is an ideal.

$\Rightarrow$ Let n_0 be a prime no, we prove $M(n_0)$ is MI

Let $U=(n)$; $n_0 \in M$, $n_0 \in U \Rightarrow n_0 = nx$ for some $x \in \mathbb{Z}$

$\Rightarrow n = 1$ or $n = n_0$ [$\because n_0$ is prime]

If $n = 1$, then $U = (1) = \mathbb{Z}$

If $n = n_0$, then $U = M$

$\Rightarrow$ Let $M = (n_0)$ be a maximal ideal of $\mathbb{Z}$

Suppose n_0 is a composite no.

where $n_0 = ab$ $\quad a \neq \pm 1$, $b \neq \pm 1$

Let $U = (a)$

Suppose $x \in M \Rightarrow x = n_0 r$ for some $r \in \mathbb{Z}$

$\Rightarrow x = (ab)r = a(br) \in U$

$\Rightarrow M \subset U \subset \mathbb{Z}$

$\Rightarrow$ # as M is maximal

$\therefore$ either $M = U$ or $U = \mathbb{Z}$

If $U = \mathbb{Z}$, then $a = 1$, again #

If $M = U$, then $a = n_0 l$ for some l

$n_0 = ab$

$= n_0 lb$

As $n_0 \neq 0$ $\quad \therefore lb = 1$

$\Rightarrow b = 1 \quad \Rightarrow$ #

$\therefore$ n_0 is not composite.

TIP To show an ideal as MI, assume $\exists$ U st $M \subset U \subseteq R$

Then try to show U must contain unity elt $\Rightarrow U = R$.

(107) If R is a commutative Ring with unity, then an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

$\Rightarrow$ M is ideal, R is comm with unity

$\therefore$ $\frac{R}{M} = \{a+M \mid a \in R\}$ is a commutative ring with unity

zero elt of $\frac{R}{M} = 0+M = M$ where $0 \in R$ is 0 elt of R

unity of $\frac{R}{M} = 1+M$ where 1 is unity of R

(i) suppose M is a maximal ideal.

We have to show every non-zero elt of $\frac{R}{M}$ has inverse

Let $a+M \in \frac{R}{M}$ & $a+M$ be non-zero

$\Rightarrow a+M \neq M$

$\Rightarrow a \notin M$

If $\langle a \rangle = \{ar \mid r \in R\}$ is a PI of R, then $\langle a \rangle + M$ is also an ideal of R ($\because$ sum of 2 ideals is an ideal)

Again $a = a\cdot 1 + 0 \in \langle a \rangle + M$ & $a \notin M$

$\therefore M \subset \langle a \rangle + M \subseteq R$

Now since M is MI of $R \Rightarrow \langle a \rangle + M = R$

since $1 \in R \Rightarrow 1 \in \langle a \rangle + M$

$\Rightarrow 1 = ar+m$ for some $r \in R, m \in M$

Now $1+M = (ar+m)+M = (ar+M)+(m+M)$

$1 = (ar+M)+M = ar+M$

$1 = (a+M)(r+M)$

$\therefore (a+M)(r+M) = (r+M)(a+M) = 1 \Rightarrow (a+M)^{-1} = r+M \in \frac{R}{M}$

$\therefore \frac{R}{M}$ is a field.

(ii) Suppose $\frac{R}{M}$ is a field. , we prove M is MI of R

Let $\exists\ U$ st $M \subset U \subseteq R$ & $M \neq U$.

Since $M \subset U$ & $M \neq U$, $\exists\ p \in U$ & $p \notin M$

ie $p + M \neq M$

ie $p+M$ is non zero in R/M

$\Rightarrow$ $p+M$ has an inverse say $q+M$

$\Rightarrow$ $(p+M)(q+M) = 1+M$

$\Rightarrow$ $pq + M = 1+M \Rightarrow 1-pq \in M$

$p \in U$ & $q \in R \Rightarrow pq \in U$

$1-pq \in M \Rightarrow 1-pq \in U$

$\Rightarrow$ $1-pq+pq \in U \Rightarrow 1 \in U \Rightarrow U = R$.

(11) ☆ commutative Ring with unity, then MI is a prime ideal.

Easy: $\frac{R}{U}$ is a field $\Rightarrow$ $\frac{R}{U}$ is an ID $\Rightarrow$ U is prime (Result 6.a)

Converse not true: Prime ideal need not be Maximal.

eg $(0) \subset (2) \subset \mathbb{Z}$

(0) ⇓ prime ideal.

* comm. Ring w/o unity, maximal need not be prime

eg $R = 2I$, ideal $= 4I$.

☆ UNITY UNITES MAXIMAL & PRIME IDEALS

12) Comm Ring with unity, if M is maximal ideal & $x \in R$, then pt $\exists\ \alpha \in R$ st $x \notin M \Rightarrow 1 - x\alpha \in M$

Easy: $\langle x \rangle$ is an ideal, then $\langle x \rangle + M$ is ideal of R

$x \in \langle x \rangle + M$ but $x \notin M \Rightarrow M \subset \langle x \rangle + M \subseteq R \Rightarrow \langle x \rangle + M = R$ ∵ M is MI

$\Rightarrow$ $1 \in R \Rightarrow 1 \in \langle x \rangle + M \Rightarrow 1 = m + \alpha x \Rightarrow 1 - \alpha x = m \in M$

Examples

i) R is ring of all real valued functions on $[0,1]$.

ST. $M = \{f \in R \mid f(\frac{1}{3}) = 0\}$ is MI of R.

Easy to prove M is an ideal.

Now suppose U is an ideal st $M \subset U \subseteq R$

Define $\theta : [0,1] \to \mathbb{R}$

st $\theta(x) = 1 \quad \forall \ x \in [0,1]$

$\therefore \quad \theta \notin M \quad [\because \theta(1/3) \neq 0] \quad \& \quad \theta \in R$

$\therefore \quad M \neq R$

$\because M \neq U \ \& \ M \subseteq U, \ \exists \ \lambda \notin M$ ie $\lambda(1/3) \neq 0$

Let $\lambda(1/3) = c \neq 0$

Define $\beta : [0,1] \to \mathbb{R}$ st $\beta(x) = c \quad \forall \ x \in [0,1]$

then $\beta \in R$

Let $\psi = \lambda - \beta$ then $\psi(1/3) = \lambda(1/3) - \beta(1/3) = 0$

$\therefore \quad \psi \in M \Rightarrow \psi \in U$

$\therefore \quad \beta = \lambda - \psi \in U \quad [\because \lambda, \psi \in U]$

Similarly $\gamma(x) = \frac{1}{c}$ is another function $\in R$

$\therefore \quad (\gamma\beta)(x) = \gamma(x)\beta(x) = 1 = \theta(x) \quad \forall \ x$

$\Rightarrow \quad \gamma\beta = \theta$

$\gamma \in R, \ \beta \in U \Rightarrow \gamma\beta \in U \Rightarrow \theta \in U$

But θ is unity $\Rightarrow U = R \Rightarrow M$ is maximal.

(ii) R is comm Ring with unity. If every ideal of R is prime, then R is a field.

R can be shown as Integral domain ($\because ab = 0 \Rightarrow ab \in \{0\}$ = prime ideal $\Rightarrow a \in \{0\}$ or $b \in \{0\}$)

Let $a \neq 0 \in R$, then a^2R is an ideal (or prime ideal)

Now $a \cdot a = a^2 = a^2 \cdot 1 \in a^2R \Rightarrow a \in a^2R \Rightarrow a = a^2b$

$\Rightarrow a(1-ab) = 0 \Rightarrow 1 - ab = 0 \Rightarrow ab = 1 \quad \therefore b$ is inverse of a.

(iii) R is comm Ring with unity & M is maximal ideal of R such that $M^2 \supseteq \{0\}$. ST if N is any maximal ideal of R then N = M

Remember: By Defntion maximal ideal $\neq R$.

Try: Let $m \in M \Rightarrow m^2 \in M = \{0\}$

$\Rightarrow m^2 = 0 \in N$ [$\because$ N is ideal]

$\therefore m^2 \in N \Rightarrow m \in N$ [$\because$ N is prime as N is maximal]

$\Rightarrow M \subseteq N \subseteq R$

But $\because$ M is maximal $\Rightarrow$ M = N or N = R

But N is maximal $\Rightarrow N \neq R$

$\therefore M = N$.

(iv) In a Boolean Ring R, every prime ideal P $\neq R$ is MI

Let $P \subseteq I \subseteq R$ & $x \in I$, $x \notin P$

as $x \in R$, $x^2 = x$

Let $y \in R$, then $x^2y = xy$

$x^2y - xy = x(xy - y) = 0 \in P$ [$\because$ P is ideal]

Always use the trick $a - b = 0 \in$ prime ideal & then manipulate 0 is present in all prime ideals

$\therefore x \in P$ or $xy - y \in P \Rightarrow xy - y + p \in P$ for some $p \in P$

$\Rightarrow y = xy - p \in I$ [$\because xy \in I$ & $p \in I$]

$\Rightarrow R \subseteq I$

$\Rightarrow R = I \Rightarrow P$ is MI.

13) SEMI-PRIME IDEAL:

Ideal I of a commutative Ring R is called semi-prime ideal if $a^2 \in I \Rightarrow a \in I \ \forall\ a \in R$.

Every prime ideal is semi-prime.

eg $I = \{6n \mid n \in Z\}$ $a^2 \in I \Rightarrow 6 \mid a^2 \Rightarrow 2 \mid a^2 \Rightarrow 2 \mid a$

& $3 \mid a^2 \Rightarrow 3 \mid a$

$\Rightarrow 6 \mid a \Rightarrow a \in I$.

But I is not prime as $2 \cdot 3 = 6 \in I$ but $2, 3 \notin I$.

⇒ HOMOMORPHISM & EMBEDDING OF RINGS

1) Mapping $f: R \to R'$ is **homomorphism** if
   (i) $f(a+b) = f(a) \oplus f(b)$
   (ii) $f(a \cdot b) = f(a) \otimes f(b)$ $\forall\ a, b \in R$

2) R' is **homomorphic image** of R if homomorphism f is R onto R' $\Rightarrow$ **$R' \simeq R'$**

3) f is **isomorphism** if (i) f is homomorphism
   (ii) f is one-one

4) f is **isomorphic image** if (i) f is homomorphism
   (ii) f is 1-1
   (iii) f is onto
   $R \cong R'$

5) Natural Homomorphism / Canonical Homomorphism: $f: R \to \frac{R}{U}$ $f(x) = x + U$ $\forall\ x \in R$
   U is an ideal of R

6) Properties: THM 1
   $f(0) = 0'$
   $f(-a) = -f(a)$ $\forall\ a \in R$
   $f(a-b) = f(a) - f(b)$ $\forall\ a, b \in R$

7) THM 2: $f(R)$ is a subring of R' $[f(R) = \{f(a) \mid a \in R\} \leq R']$

8) R is commutative $\Rightarrow$ $f(R)$ is commutative
   $f(R)$ is commutative $\not\Rightarrow$ R is commutative

   eg. $f: \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle|\ a, b \in \mathbb{R}\right\} \to \mathbb{R}$
   where $f\left(\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\right) = a$

Impt negation example: $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| \; a, b \in \mathbb{Z} \right\}$

9) R is ring with unity, f(R) is also ring with unity
▷ f(1) is the unit elt.
Converse is not true.

10) Kernel of homomorphism: $\ker(f) = \{ a \in R \mid f(a) = 0', \; 0' \text{ is } +^n \text{ identity in } R' \}$

11) Kerf is an ideal of R.

12) f is onto - ~~homomorphism~~ isomorphism $\Leftrightarrow$ Kerf $= \{0\}$

13) Quotient Ring is a homomorphic image of R
i.e., $f: R \to \frac{R}{U}$ is onto - homomorphism.

14) Fundamental Theorem of homomorphism:
$$R \simeq R' \Rightarrow \frac{R}{\text{Ker}f} \cong R'$$

15) Ring of Endomorphisms of an Abelian group:
* Endomorphism = homomorphism onto itself.
⇒ (G, +) is an abelian group, then Hom(G, G) is a ring under $+^n$ & $\times^n$ of mappings
* Hom(G, G) = set of all endomorphisms of G.
$(f+g)(x) = f(x) + g(x)$
▷ $(fg)(x) = f(g(x))$ ∀ $x \in G$.

NOTE: In proofs while considering $0: G \to G$ & $-f: G \to G$ & fg it is necessary to show both of these are homomorphisms before proceeding.

16) Embedding of Rings :

* R is said to be embedded into R', if there exists an isomorphism of R into R'

  ie, $\exists\ f: R \longrightarrow R'$
  such that (i) f is homomorphism
  (ii) f is 1-1.

* R' is said to be an extension ring of R

* R & f(R) are isomorphic rings [$\because f(R)$ is subring of R']

* $f: R \longrightarrow f(R)$ is an onto-isomorphism $\Rightarrow R \cong f(R)$

** VVI *

#) Every Ring R can be embedded in a ring with unity.

$$R' = R \times Z = \{(a, m) \mid a \in R, m \in Z\}$$

$+^n$: $(r, m) + (s, n) = (r+s, m+n)$

$\times^n$: $(r, m) \cdot (s, n) = (rs + ms + nr, mn)$

$r, s \in R$
$m, n \in Z$

It can be easily shown that $R \times Z$ is a ring with unity $\Downarrow$ $(0,1)$

$f: R \to R' \Rightarrow f(r) = (r, 0)\ \forall\ r \in R$

17) QUOTIENT FIELD :

MOTIVATION : I is a Ring of integers & Q is a field of rational nos which are essentially quotients of 2 integers.

$(Q, +, \cdot)$ is the smallest field containing I

Also : (i) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ (ii) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ (iii) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Thm Every integral domain D can be embedded in a field F such that every elt of F can be regarded as quotient of 2 elts of D.

Construction Let D be an ID with atleast 2 elts.

Consider $S = \{(a,b) \mid a,b \in D, b \neq 0\}$

then $S \neq \phi$ & $S \subset D \times D$

Define Relation '$\sim$' on 'S' as $(a,b) \sim (c,d) \Leftrightarrow ad = bc$

Then $\sim$ is an equivalence relation & partitions S into equivalence classes which are identical or disjoint

Let $\frac{a}{b}$ be equivalence class of (a,b)

then $\frac{a}{b} = \{(x,y) \in S \mid (x,y) \sim (a,b) \Leftrightarrow xb = ya\}$

If $\frac{a}{b}$ & $\frac{c}{d}$ are 2 classes, then either $\frac{a}{b} = \frac{c}{d}$ or $\frac{a}{b} \cap \frac{c}{d} = \phi$

Construct F = set of all equivalence classes $= \left\{\frac{a}{b} \mid (a,b) \in S\right\}$

Define : $+^n$: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ * Here $bd \neq 0$ as D is w/o ZDs & $b \neq 0, d \neq 0$

$\times^n$: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

F can be proved as a Field.

Isomorphism Define $\phi : D \to I$ by

$\phi(a) = \frac{ax}{x}$ $\forall$ $a \in D$ & $x (\neq 0) \in D$

$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$ $\quad [(a,b)] = [(c,d)] \Leftrightarrow ad = bc.$

$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$

0 elt : $[(0,1)]$

1 elt : $[(1,1)]$

Important Examples

1) UNITS OF A RING : All the elts which have multiplicative inverse eg $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ in $\mathbb{Z}_8$.

$[x]$ is a unit in $\mathbb{Z}_n$ iff $\gcd(x,n) = 1$

2) $R = \{a, b, c, d\}$ is a ring, complete the table

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

x	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

$\forall x : 2x = 0 \Rightarrow x = -x$

$(b+c)b = b^2 + cb$

$db = b + cb$

$b = b + cb \Rightarrow cb = \cancel{(-b)+c}$ (a) $\cancel{-b+c}\ 0$

$= (d)$

$(b+d)c = bc + dc$

$c^2 = bc + c$

$\cancel{(bc+d)d =}$ $c(c+d) = c^2 + cd$

$cb = c^2 + cd$

$a = c^2 + c \Rightarrow c^2 = a + (-c)$

$= a + c = c$

$c^2 = bc + c$

$c = bc + c$

$\Rightarrow bc = a$

$b(c+d) = bc + bd$

$b^2 = bc + bd$

$d(b+d) = db + d^2$

$dc = db + d^2$

$c = db + d^2 \Rightarrow d^2 = b + c = d$

d is identity, x^n is commutative, $a^2 = x \ \forall\ x \in R$

3) In a Ring R, eqn $ax = b \ \forall\ a, b\ (a \neq 0)$ has a soln. ST R is division Ring

$ax = a$ has solution $\Rightarrow x = e_1$ $\quad bx = e_1$ has solution $= e_2$

Let $a \neq 0$, $ab = 0 \Rightarrow abe_2 = 0e_2 = 0 \Rightarrow a(be_2) = 0 \Rightarrow ae_1 = 0 \Rightarrow a = 0 \Rightarrow \#$

$\therefore$ R has no ZD.

Let $x = e$ be soln to $ax = a \Rightarrow ae = a \Rightarrow aex = ax \Rightarrow a(ex - x) = 0$

$\Rightarrow ex - x = 0 \ \forall\ x \in R \Rightarrow$ e is left ID, Sly e is right ID.

$\therefore ax = e$ has a soln $\forall\ a \neq 0 \Rightarrow \exists\ b$ st $ab = e \Rightarrow$ inverse exists

4) R is a ring w/o any non-zero nilpotent elts, then st for idempotent e, $ex = xe \ \forall \ x \in R$, i.e., $e \in Z(R)$

$e^2 = e$

$(exe - ex)^2 = (exe - ex)(exe - ex)$

$= exexe - exexe - exexe + exex$

$= exexe - exexe - exex + exex$

$= 0$

$\Rightarrow$ $exe - ex$ is nilpotent

$\Rightarrow$ $exe - ex = 0 \Rightarrow exe = ex$ ~~$\Rightarrow e^2xe = e^2x$~~

~~$\Rightarrow xe = ex$~~

Sly $exe = xe \Rightarrow ex = xe$.

IMPORTANT (CRAM)

i) R is comm Ring with unity & $a \in R$ then $U = \{ra \mid r \in R\}$ is a principal ideal

ii) R is comm. Ring, P is prime ideal iff $\frac{R}{P}$ is ID.

iii) R is comm Ring with unity, M is maximal iff $\frac{R}{M}$ is a field

iv) [ii + iii] $\Rightarrow$ R is comm Ring with unity, maximal ideal $\Rightarrow$ prime ideal.

v) R is comm Ring with unity, prime $\not\Rightarrow$ maximal (eg Null ideal) only exception In a PID, non-zero ideals are maximal

vi) R is comm Ring w/o unity, maximal $\not\Rightarrow$ prime [eg ideal = 4I Ring = 2I]

vii) **UNITY UNITES PRIME & MAXIMAL IDEALS**

viii) R is comm Ring with unity, ALL ideals of R are prime $\Rightarrow$ R is a field.

IDEALS

ix) Comm Ring with unity & without proper ideals is a Field

~~x) Comm Ring without proper ideals~~

x) Ring with unity without proper ideals is a Division Ring

xi) Ring with more than 1 element such that $aR = R \ \forall a \neq 0 \in R$ then R is division Ring.

xii) Abelian group of order 6 is cyclic.

xiii) PID $\not\Rightarrow$ UID example: $R = \left\{ a + b\left(\frac{1+\sqrt{19}\,i}{2}\right) \mid a, b \in Z \right\}$.

⇒ Euclidean Domain

Motivation : Division algorithm in ring of integers

⇒ **Defⁿ:** Integral domain R is Euclidean Domain if

$\exists$ a mapping $d: R-\{0\} \longrightarrow \mathbb{Z}$ such that

(i) $d(a) \geq 0 \quad \forall\ a \in R-\{0\}$ — $d(0)$ is not defd but sometimes taken as 0.

(ii) $d(a) \leq d(ab) \quad \forall\ a, b \in R-\{0\}$

(iii) for any $a \in R$, $b \in R-\{0\}$

↓ division algorithm $\exists\ q, r \in R$ so that $a = bq + r$ where $d(r) < d(b)$ or $d(r) = 0$

eg for ring $\mathbb{Z}$ of integers define $d(a) = |a| \quad \forall\ a \in \mathbb{Z}-\{0\}$

Ques Show that Ring of Gaussian integers is an euclidean ring.

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

Define $d(a+ib) = a^2+b^2 \quad \forall\ a+ib \in \mathbb{Z}[i]-\{0\}$

(i) & (ii) are easy

for (iii) consider, $\frac{z_1}{z_2} = \frac{a+ib}{c+id} = \frac{a+ib}{c+id} \cdot \frac{c-id}{c-id}$

$$= \frac{(ac+bd)}{c^2+d^2} + i\,\frac{(bc-ad)}{c^2+d^2}$$

$p = \frac{ac+bd}{c^2+d^2}$, $q = \frac{bc-ad}{c^2+d^2}$ are rationals.

If we can find suitable integers p' & q' st $|p'-p| \leq \frac{1}{2}$ & $|q'-q| \leq \frac{1}{2}$

Let $t = p'+iq'$ then $t \in \mathbb{Z}[i]$ $\qquad \lambda = p+iq$

$z_1 = tz_2 + r$ where $r = (\lambda - t)\, z_2$

$z_1, z_2, t \in \mathbb{Z}[i] \Rightarrow r \in \mathbb{Z}[i]$

$d(r) = d[(\lambda-t)z_2] = d((p'-p)+(q'-q)i)\, d(z_2) = [(p'-p)^2+(q'-q)^2]\, d(z_2)$

$\leq \frac{d(z_2)}{2}$

3) d is called the euclidean evaluation
(iii) is called the euclidean algorithm

4) Thm: Every field is a Euclidean Ring.

Define $d(a)=0 \quad \forall \quad a \in F-\{0\}$
or $d(a)=1 \quad \forall \quad a \in F-\{0\}$

Ques Show that $\mathbb{Z}[\sqrt{2}] = \{m+n\sqrt{2} ; m,n \in \mathbb{Z}\}$ is ED.

Just like $\mathbb{Z}[i]$ go for $d(z) = z\bar{z} = |m^2-2n^2|$

$z_1 = a+b\sqrt{2}$
$z_2 = c+d\sqrt{2}$

$z_1 z_2 = (ac+2bd)+(ad+bc)\sqrt{2}$

$d(z_1z_2) = [(ac+2bd)^2 - 2(ad+bc)^2]$
$= |a^2c^2+4b^2d^2-2a^2d^2-2b^2c^2|$
$= |(a^2-2b^2)(c^2-2d^2)|$

$a,b \neq 0$, then $|a^2-2b^2| \geq 1$

Just like $\mathbb{Z}[i]$ take $\frac{z_1}{z_2} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = p+q\sqrt{2}$ take $p', q' \in I$ st $|p'-p| < \frac{1}{2}$ & $|q'-q| < \frac{1}{2}$

$z_1 = tz_2 + r \quad r = (\lambda - t) z_2$
$\lambda = p+q\sqrt{2}$

5) Thm: Every Euclidean ring is a principal ideal ring.
(i.e. Every ideal is generated by the elt with smallest d)

Converse is not true.
eg $R = \{a+b\left(\frac{1+\sqrt{19}i}{2}\right) \mid a,b \in \mathbb{Z}\}$

TRICK: Remember in our study flow Euclidean is an advancement over principal ideal ring, so ER has to be PIR first ∴

6) Every Euclidean Ring possesses unity element.

Let $R = \langle a \rangle \Rightarrow \exists e$ st $ae = a$
Let $x \in R$, then $x = ad$ for some $d \in R$
$xe = ade = d(ae) = da = ad = x$ [∵ 2)]

∴ e is the unity elt.

COROLARY : $\mathbb{Z}[i]$ & $\mathbb{Z}[\sqrt{2}]$ are principal ideal domains.

Remember : Euclidean Domain ⇒ PID ⇒ Euclidean Domain as unity & $\langle 1 \rangle = R$

7) Divisibility: Let R be a commutative ring & $a, b \in R$

if $\exists\, q \in R$ st $b = aq$, then we say a divides b $\to a|b$

* $\forall\, a \in R$ $a|0$ $[\because 0 = a0]$

* $a, b \in R$ and $a|b \iff b = aq$ for some $q \in R$

* In $\mathbb{Z}$ $3 \nmid 7$ & $3 \nmid 15$
But in $\mathbb{Q}$ $3|7$ as $7 = 3\left(\frac{7}{3}\right)$

8) R is a commutative ring with unity & $a, b, c \in R$
then a(i) $a|a$ (ii) $a|b, b|c \Rightarrow a|c$ (iii) $a|b \Rightarrow a|bx$ $\forall\, x \in R$

(iv) $a|b, a|c \Rightarrow a|bx+cy$ $\forall\, x, y \in R$

9) UNITS: R is a commutative ring with unity.

$a \in R$ is a unit in R if $\exists\, b \in R$ st $ab = 1$

Units are elements of R which possess multiplicative inverses

* Units + Unity ~~elements~~ (unity is unique)

* a is unit st $ab = 1$, then $b \in R$ is also a unit
a, b are units then (ab) is also a unit.

* Every non-zero elt in a Field is a unit.

10) Let $a \neq 0, b \neq 0 \in R$ & R is Euclidean Ring, then
(i) if b is a unit in R, $d(ab) = d(a)$ and
(ii) if b is not a unit in R, $d(ab) > d(a)$.

$\Rightarrow$ (i) is easy $d(ab) \geq d(a)$ & $d(abc) \geq d(ab)$ where $bc = 1$

(ii) $a \neq 0, b \neq 0 \Rightarrow ab \neq 0 \Rightarrow \exists\, q, r$ st $a = (b)q + r$ $r = 0$ or $d(r) < d(ab)$

* if $r = 0 \Rightarrow a = abq \Rightarrow a(1-bq) = 0 \Rightarrow 1 - bq = 0$ $[\because R$ is ID$] \Rightarrow b$ is unit

* if $r \neq 0$ $d(r) < d(ab) = d(a(1-qb)) < d(ab) \Rightarrow d(a) \leq d(a(1-qb)) < d(ab)$
$\Rightarrow d(a) < d(ab)$.

11) THM: Non zero elt in ER 'R' is **unit $\Leftrightarrow$ $d(a)=d(1)$**

12) ASSOCIATES: R is a commutative ring with unity

An elt $a \in R$ is said to be an associate of $b \in R$ if $a = bu$ where u is a unit in R

* 'Being Associates' is an equivalence relation
* $d(a) = d(bu) = d(b)$
* Unity element '1' is an associate of unit 'a' $\in R$ $\because a = 1 \cdot a$

eg: In $\mathbb{Z}$, $(1, -1)$ are the only units

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

$\therefore a \in \mathbb{Z}$ has 2 associates $a, -a$

In $Z_6 = \{0,1,2,3,4,5\}$ $(1,5)$ are the only units

2 has 2 associates 2 & 4.

In $Z[i]$, $(2+3i)$ & $(2i-3)$ are associates

13) R is an integral domain with unity & $a, b \in R - \{0\}$ then a & b are associates in R iff $a|b$ & $b|a$

14) GREATEST COMMON DIVISOR: Let R be commutative Ring with unity & $a \neq 0, b \neq 0 \in R$. Then $d \neq 0 \in R$ is $\gcd(a,b)$ if (i) $d|a$ & $d|b$

(ii) whenever $c \neq 0 \in R$ & $c|a$ & $c|b \Rightarrow c|d$

LEAST COMMON MULTIPLE: c is lcm of (a,b) if

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

(ii) whenever $x \neq 0 \in R$ st $a|x$ & $b|x \Rightarrow c|x$

$d = \gcd(a,b) = (a,b)$ & $c = \text{lcm}(a,b) = [a,b]$

NOTE: a & b may or may not have lcm/gcd
They may even have more than one lcm/gcd.

Examples In $\mathbb{Z}$. 2 & -2 are gcd of 4, 6
12 & -12 are lcm of 4, 6

In $2I$, 4 & 6 do not have a gcd
12 is not lcm as $4 \nmid 12$ as $4 \cdot 3 = 12$ & $3 \notin 2I$.

Ques Find lcm & gcd of $\bar{6}$ & $\bar{8}$ in $\mathbb{Z}_{12}$.

$\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \bar{10}, \bar{11}\}$

* $\bar{6} = \bar{3} \cdot \bar{2}$ & $\bar{8} = \bar{4} \cdot \bar{2} \Rightarrow \bar{2}$ is a common divisor
If $\bar{x} \in \mathbb{Z}_{12}$ st $\bar{x} | \bar{6}$ & $\bar{x} | \bar{8} \Rightarrow \bar{x} | \bar{8} - \bar{6} \Rightarrow \bar{x} | \bar{2}$
$\Rightarrow \bar{2}$ is gcd$(\bar{6}, \bar{8})$

* $\bar{6} = \bar{10} \cdot \bar{3}$ & $\bar{8} = \bar{10} \cdot \bar{2} \Rightarrow \bar{10} | \bar{6}$ & $\bar{10} | \bar{2}$
Also $\bar{x} | \bar{6}$ & $\bar{x} | \bar{8} \Rightarrow \bar{x} | 2 \cdot \bar{8} - \bar{6} \Rightarrow \bar{x} | \bar{10} \Rightarrow \bar{10}$ is gcd$(\bar{6}, \bar{8})$

* Let $\bar{x}$ be lcm$(\bar{6}, \bar{8}) \Rightarrow \bar{6} | \bar{x}$ & $\bar{8} | \bar{x}$
$\Rightarrow \bar{x} = \bar{6} \cdot \bar{y}$ for $\bar{y} \in \mathbb{Z}_{12}$
$\Rightarrow \bar{x} = \bar{0}$ or $\bar{6}$ but lcm $\neq 0$
$\Rightarrow \bar{x} = \bar{6}$ but $\bar{8} \nmid \bar{6}$

NOTE: If d_1, d_2 are 2 gcds of a, b then by the definition
$d_1 | d_2$ and $d_2 | d_1 \Rightarrow$ d_1 & d_2 are associates *
in $\mathbb{Z}_{12}$, $\bar{2}$ & $\bar{10}$ are associates

15) In the Euclidean Ring R, 2 elts 'a' & 'b' are said to be relatively prime iff gcd(a, b) = a unit of R.
a, b are relatively prime $\Leftrightarrow$ gcd(a, b) = unit elt of R
$\Leftrightarrow$ (a, b) = 1
$\Leftrightarrow$ $ax + by = 1$ for some $x, y \in R$

16) b is a proper divisor of a if $a = bd$ where d is not a unit elt

Improper divisors: for $a \neq 0 \in R$, units & associates of 'a' are improper divisors.

17) **IRREDUCIBLE ELEMENT**: Commutative Ring with unity

$p \neq 0$ & not unit is irreducible if $p = ab \Rightarrow$ either a or b is unit

If p is reducible $\rightarrow p = ab$ & a, b are not unit elt.

18) **PRIME ELEMENT**: $p \neq 0 \in R$ is prime if $p \mid ab \Rightarrow$ either $p \mid a$ or $p \mid b$
& p is non-unit.

Non-zero & Non-unit needed for both irreducible & prime elts.

eg $1+i$ is a prime elt in $\mathbb{Z}[i]$

In $\mathbb{Z}$, prime nos are both prime elt & irreducible elt.

Any Field has neither any prime, nor irreducible elt as all the elts in a field are units

Ques. St $\bar{2}$ is prime but not irreducible in $\mathbb{Z}_6$:

$\bar{1}$ & $\bar{5}$ are units in $\mathbb{Z}_6$

Let $\bar{2} \mid \bar{a}\bar{b} \Rightarrow 6 \mid ab-2 \Rightarrow ab-2 = 6x$ for some $x \in \mathbb{Z}_6$

$\Rightarrow ab = 2(1+3x)$

$\Rightarrow 2 \mid ab \Rightarrow 2 \mid a$ or $2 \mid b$ are $2 \in$ prime

$\Rightarrow \bar{2} \mid \bar{a}$ or $\bar{2} \mid \bar{b} \Rightarrow \bar{2}$ is prime elt

Also $\bar{2} \times_6 \bar{4} = \bar{2} \Rightarrow$ not irreducible

Ring: $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$

19) Important examples:

(a) $1, -1$ are the only unit elements.

$a+ib\sqrt{5}$ is unit iff $a^2 + 5b^2 = 1$

(b) Irreducible elements: $2, 3, 1+i\sqrt{5}, 1-i\sqrt{5}$

If 3 is reducible $= (a+ib\sqrt{5})(c+id\sqrt{5}) \Rightarrow \bar{3} = (a-ib\sqrt{5})(c-id\sqrt{5})$

$\Rightarrow 9 = (a^2+5b^2)(c^2+5d^2) =$ (1)×9 or 9×(1) or (3×3) becomes unit elt.

$a+ib$

(c) $2, 3, 1 \pm i\sqrt{5}$ are not prime elements

consider: $2+i\sqrt{5}$ & $2-i\sqrt{5}$: $3 \mid (2+i\sqrt{5})(2-i\sqrt{5}) = 9$ but $3 \nmid 2 \pm i\sqrt{5}$

as $\nexists\ a \in \mathbb{Z}(\sqrt{5})$ s.t. $3a = 2$

(d) $i\sqrt{5}$ is prime element in $\mathbb{Z}[i\sqrt{5}]$

Remember to prove $i\sqrt{5}$ is non unit using $1=(i\sqrt{5})(a+ib\sqrt{5})$

Suppose $i\sqrt{5} \mid (a+ib\sqrt{5})(c+id\sqrt{5}) \Rightarrow (ac-5bd)+i(ad+bc)\sqrt{5}$
$= i\sqrt{5}(x+iy\sqrt{5})$

$\Rightarrow ac-5bd = -5y$

$\Rightarrow 5(y-bd) = ac$

$\Rightarrow 5 \mid ac \Rightarrow 5 \mid a$ or $5 \mid c$

if $5 \mid a$, then $-5 \mid a \Rightarrow (\sqrt{-5})(-\sqrt{-5}) \mid a \Rightarrow \sqrt{-5} \mid a$

Also $\sqrt{-5} \mid ib\sqrt{5} \Rightarrow i\sqrt{5} \mid a+ib\sqrt{5}$

eg: Irreducible but no prime : 3, $2+i\sqrt{5}$

$\Downarrow$

$2+i\sqrt{5} \mid 9 = 3\times 3$

but $2+i\sqrt{5} \nmid 3$

2) THM: R is integral domain with unity,

every prime element of R is irreducible

& converse is not true. (eg 3 in $\mathbb{Z}[i\sqrt{5}]$)

Application: Use prime to show ett is Irreducible

eg $i\sqrt{5}$ in $\mathbb{Z}[i\sqrt{5}]$

$\Downarrow$

(Proof later) In principal ideal domain, prime $\Leftrightarrow$ irreducible

Easy Results * ID with unity, then (i) $a \mid b$ & $b \mid a \Leftrightarrow (a)=(b)$

(ii) $(a)=(b) \Leftrightarrow a$ & b are associates

* In a PID, any associate of a gcd is a gcd.

2) PID If $(a,b)=d$, then $d=\lambda a+\mu b$ for some $\lambda, \mu \in R$

Consider $A=\{ax+by \mid x,y \in R\}$ & show that A is an ideal

A is ideal, then $A=(d)$ [$\because$ A is PID] $\therefore d=\lambda a+\mu b$ for some λ, μ

$a=1\cdot a+0\cdot b \in (d)$ & $b=0\cdot a+1\cdot b \in (b) \Rightarrow d \mid a$ & $d \mid b$.

Assume $c \mid a$ & $c \mid b \Rightarrow c \mid \lambda a+\mu b \Rightarrow c \mid d \Rightarrow d$ is gcd.

22) In a PID, prove that any 2 non-zero elts have a lcm

take $A=(a)$ & $B=(b)$ then $A\cap B$ is an ideal $=(l)$

We show l is lcm(a,b)

$l\in A\cap B \Rightarrow l\in A=(a)$ & $l\in B=(b)$

$\Rightarrow l = ax$ for some x & $l=by$ for some y

$\Rightarrow a|l$ & $b|l$.

Suppose $\exists\, x$ st $a|x$ & $b|x$

$\Rightarrow x = ar$ & $x = bs$ $r,s\in R$

$\Rightarrow x\in(A)$ & $x\in(B) \Rightarrow x\in A\cap B=(l)$

$\Rightarrow x = ly$ $y\in R$

$\Rightarrow l|x$

PROOF

23) In a PID, prime element $\iff$ irreducible element

prime $\longrightarrow$ irreducible is easy

We show irreducible $\longrightarrow$ prime consider $p=ab$ as irreducible

Let $p|ab$ & $p\nmid a$, we show $p|b$

consider ideals $\langle p\rangle$ & $\langle b\rangle$ $\Rightarrow \langle p\rangle+\langle b\rangle$ is also ideal $=\langle d\rangle$

$\Rightarrow \langle p\rangle+\langle b\rangle=\langle d\rangle \Rightarrow \langle p\rangle\subseteq\langle d\rangle \Rightarrow p\in\langle d\rangle$

$\Rightarrow p=dx$ $x\in R$ — (1)

p is irreducible $\Rightarrow$ either d is unit or x is unit

(i) d is unit $\Rightarrow d^{-1}\in R \Rightarrow dd^{-1}=1\in\langle d\rangle=\langle p\rangle+\langle b\rangle$

$\therefore 1 = apr+bs \Rightarrow a = apr+abs$

$p|apr$ & $p|ab \Rightarrow p\,|\,apr+abs \Rightarrow p|a$ #

(ii) x is unit $\Rightarrow x^{-1}\in R$ ~~$\Rightarrow x^{-1}d\in\langle d\rangle \Rightarrow x^{-1}d=dy$ for some $y\in R$~~

$\therefore$ from (1): $d=px^{-1}$

Let $\alpha\in(d) \Rightarrow \alpha = dy = px^{-1}y \Rightarrow \alpha\in\langle p\rangle \Rightarrow \langle d\rangle\subseteq\langle p\rangle$

$\therefore \langle p\rangle=\langle 1\rangle=\langle p\rangle+\langle b\rangle$

$\Rightarrow \langle b\rangle\subseteq\langle p\rangle$

$\Rightarrow b\in\langle p\rangle$

$\Rightarrow b = pt$ $t\in R$

$\Rightarrow p|b$.

Use this to show an ID is not PID

eg $\mathbb{Z}[i\sqrt{5}]$

3 is irreducible but not prime

$\Rightarrow \mathbb{Z}[i\sqrt{5}]$ is not PID.

24) R is a PID which is not a field
$A = \langle a \rangle$ is maximal ideal $\Leftrightarrow$ a is irreducible element of R

25) R is a PID, non-zero ideal $P \neq R$ is prime $\Leftrightarrow$ P is maximal

26) Ideal $A = (a)$ of a Euclidean domain R is maximal $\Leftrightarrow$ a is irreducible (prime) element of R

27) $\gcd(a,b) \times \text{lcm}(a,b) = ab$
Use it to find lcm of $(a+ib), (c+id) \in \mathbb{Z}[i]$
gcd can be found using the iterative method

$$\beta = q\gamma + s$$
$$\gamma = st + u$$
$$s = uv \quad \text{then } \gcd(\beta, \gamma) = v$$

Remember to have $d(s) < d(\gamma)$ in the manipulations.

⇒ POLYNOMIAL RINGS

1) Let R be a ring. The expression

$$f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n \quad \forall\, x\, a_i \in R \;\&\; n \geq 0$$

is called polynomial in x over R.

If $a_n \neq 0$ & n is largest, then a_n is called leading coefficient.

2) $f(x) = g(x) \iff a_i = b_i \quad \forall\, i \geq 0$

3) Monic Polynomial: leading ~~coeff~~ coeff is unity element.

4) Ring of Polynomials over ring R is

$$R[x] = \{ f(x) = a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R,\ n \geq 0 \underset{\in Z}{} \}$$

Additive identity = 0
unity = 1 (if R has unity)
inverse = $-f(x)$ $\forall\, f(x) \in R[x]$

5) R is commutative $\Rightarrow$ $R[x]$ is commutative
R has unity $\Rightarrow$ $R[x]$ has unity
F is a field $\Rightarrow$ $F[x]$ is commutative ring with unity.
But $F[x]$ is not a field.

R is an ID $\Rightarrow$ $R[x]$ is an ID

6) Degree of polynomial ≥ 0
Degree of constant = 0
Degree of $0(x)$ is not defined.

7) $\deg(f(x) + g(x)) = \text{Max}(m,n) \quad m \neq n$
$\leq m \quad$ when $m = n$

$\deg(f(x)) = m$
$\deg(g(x)) = n$

8) If $f(x) \cdot g(x) \neq 0 \Rightarrow \deg(f(x) * g(x)) \leq \deg(f(x)) + \deg(g(x))$

9) R is an ID then $\deg(fg) = \deg f + \deg g$

R is an ID then $\deg f \leq \deg(fg)$

10) If R is an ID with unity, then the units of R & R[x] are same

proving converse : Let $f(x)$ be unit in $R[x]$

$\Rightarrow \exists\ g(x)$ st $f(x)g(x) = 1$

$\therefore \deg(fg) = \deg f + \deg g = 0$

$\Rightarrow \deg f = \deg g = 0$

$\therefore f(x) = a_0 \quad g(x) = b_0$

$f(x)g(x) = a_0 b_0 = 1 \Rightarrow a_0, b_0$ are units in R

11) If R is an ID with unity, then any irreducible element of R is an irreducible element of R[x].

12) Every Ring can be embedded into a polynomial ring R[x].

Define $\theta : R \to R[x]$ as $\theta(a) = a + 0x + 0x^2 + \cdots + 0x^n + \cdots \quad a \in R$

θ is homomorphism : $\theta(a+b) = \theta(a) + \theta(b)$ & $\theta(ab) = \theta(a)\theta(b)$

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

13) Ring is an ID $\Leftrightarrow$ R[x] is an ID.

Proof : use that any subring of an ID is an ID.

14) Ring R has no proper ZD $\Leftrightarrow$ R[x] has no proper ZD.

need for deg(fg) ≥ deg f ← GdE

15) **DIVISION ALGORITHM**:

Let $f(x)$ & $g(x)$ be 2 non-zero polynomials in $F[x]$ then $\exists$ a unique polynomials $t(x)$ & $r(x)$ in $F[x]$ such that $f(x) = t(x)\,g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

Proof consider set $S = \{ f(x) - h(x)\,g(x) \mid h(x) \in F(x) \}$

case (i) $0 \in S \Rightarrow \exists\ t(x)$ st $f(x) - t(x)\,g(x) = 0$ (x) HP

case (ii) $0 \notin S \Rightarrow$ every polynomial is non zero & hence non-zero degree

Let $r(x) \in S$ be polynomial with least degree

$\therefore \exists\ q(x) \in F(x)$ st $f(x) - q(x)\,g(x) = r(x)$ ... HP

show deg(r(x)) is least & r & q are unique

16) **If F is a field, then F[x] is Euclidean Domain.**

Define d as $d(f(x)) = \deg(f(x))$ $\forall\ f(x) \neq 0 \in F[x]$

$\deg(fg) = \deg f + \deg g \geq \deg f$

CORR: F is field $\Rightarrow$ F[x] is ED $\Rightarrow$ F[x] is PID

Proof: Let U be an ideal of F[x]

If $U = \{0\} \Rightarrow U = \langle 0 \rangle$, principal ideal generated by 0

If $U \neq \{0\}$, then U contains polynomials of degree ≥ 0.

By **well-ordering principle**, $\exists\ f(x) \in U$ st $f(x) \neq 0$ & $\deg f \leq \deg g$ where $g \in U$ & $g(x) \neq f(x)$

Let $h(x)$ be any polynomial in U

By division algorithm, $\exists\ q(x), r(x) \in F[x]$ st $h(x) = f(x)q(x) + r(x)$

$f(x) \in U$ & $q(x) \in F[x] \Rightarrow f(x)q(x) \in U \Rightarrow r(x) \in U$

if $r(x) = 0$ then $h(x) = f(x)q(x)$

$r(x) \neq 0 \Rightarrow \deg r(x) < \deg(f(x)) \Rightarrow r(x) = 0$

$\therefore U = \{ f(x)\,q(x) \mid q(x) \in F[x] \} = \langle f(x) \rangle$

NOTE: $Z[x]$ over Ring of integers is not an Principal Ideal Ring.

17) Ideal $A = \langle p(x) \rangle$ in $F[x]$ is a maximal ideal iff $p(x)$ is an irreducible element of $F[x]$

18) $\frac{F[x]}{\langle f(x) \rangle}$ is a field iff $f(x)$ is an irreducible element of $F[x]$

Ques Show that $\frac{\mathbb{Q}[x]}{\langle x+2 \rangle}$ is a field.

$\mathbb{Q}[x]$ is a PID

It suffices to show $(x+2)$ is irreducible element of $\mathbb{Q}[x]$

Let $x+2 = f(x)\,g(x) \Rightarrow \deg(fg) = \deg(x+2)$

$\Rightarrow \deg f + \deg g = 1 \Rightarrow \deg f = 1 \text{ & } \deg g = 0$ or $\deg f = 0 \text{ & } \deg g = 1$

if $\deg f = 1$ & $\deg g = 0$

$\Rightarrow a(b_0 + b_1 x) = x+2 \Rightarrow a b_0 = 1 \Rightarrow a$ is unit $\Rightarrow f$ is unit

$a b_1 = 2$

$\Downarrow$

$x+2$ is irreducible

19) If R is a ring, $\frac{R[x]}{\langle x \rangle} \cong R$. [use $\theta : R[x] \to R$ as $\theta(a_0 + a_1 x + \dots) = a_0$ & use $\frac{R[x]}{\ker \theta} \cong R$]

20) Integral Domain R with unity is a field iff $R[x]$ is a principal ideal domain.

$\frac{R[x]}{\langle x \rangle} \cong R$, $\langle x \rangle$ is irreducible element in $R[x]$

$\Rightarrow \frac{R[x]}{\langle x \rangle}$ is field. (Better to show $\langle x \rangle$ is maximal ideal)

Corr: $\mathbb{Z}[x]$ is not a PID

Ques Prove that $\langle x \rangle$ is a prime ideal of $\mathbb{Z}[x]$ but not maximal

$\langle x \rangle = \{x\,p(x) \mid p(x) \in \mathbb{Z}[x]\}$ Let $f(x)g(x) = x\,p(x)$

$\Rightarrow a_0 b_0 = 0 \Rightarrow a_0 = 0$ or $b_0 = 0$

Consider $A = \{x f(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}\}$ $\quad$ $f(x) \in \langle x \rangle$ $\quad$ $g(x) \in \langle x \rangle$

A is a proper ideal

$\hookrightarrow \langle x \rangle \subset A \subset \mathbb{Z}[x] \Rightarrow \langle x \rangle$ is not maximal.

Ques $\mathbb{Z}[x]$ is not a principal ideal ring. Prove.

Consider $S = \{x, 2\} \subset \mathbb{Z}[x]$. We show that ideal generated by $S = \{x, 2\}$ is not a principal ideal.

Assume it is principal ideal $\Rightarrow \exists\ a(x)$ st $\{x, 2\} = [a(x)]$

$\Rightarrow x \in [a(x)] \Rightarrow \exists\ b(x)$ st $a(x)b(x) = x$ — (1)

$\Rightarrow 2 \in [a(x)] \Rightarrow \exists\ c(x)$ st $a(x)c(x) = 2$ — (2)

from (2) : $\deg a + \deg c = 0 \Rightarrow \deg a = 0$ & $\deg c = 0$

$\Rightarrow a(x)c(x) = 2$ & $a(x)$, $c(x)$ are non-zero integers.

$\Rightarrow a(x) = \pm 1$, $c(x) = \pm 2$ or $a(x) = \pm 2$, $c(x) = \pm 1$

If $(a(x)) = 1$, then $[a(x)] = \mathbb{Z}[x]$

$\Rightarrow \{x, 2\} = \mathbb{Z}[x]$

If $a(x) = \pm 2 \Rightarrow x = \pm 2\, b(x) \Rightarrow x = \pm 2[b_0 + b_1 x + \cdots]$

$\Rightarrow 1 = \pm 2 b_1$, $b_1 \in \mathbb{Z}$ ⇒ contradiction

$\therefore S = \{x, 2\}$ is not a Principle ideal.

Ques Show that $A = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ is a maximal ideal of $\mathbb{Z}[x]$.

Let $A \subseteq M \subseteq R$

$\mathbb{Z}[x]$ is not PID, so dont take $M = \langle p(x) \rangle$

consider ideal M, we show $1 \in M \Rightarrow M = R$

Let $p(x) \in M$ & $p(x) \notin A$

If $p(x)$ has even constant term $\Rightarrow a_0 = 2k$ $k \in \mathbb{Z}$

then $p(x) = 2k + x a_1 + x^2 a_2 + \cdots$

$= x(\ ) + 2(\ ) \in A$ so contradiction

If $a_0 = 2k+1$, then $p(x) = x(\ ) + 2(\ ) + 1$

$= g(x) + 1$.

Now $p(x) \in M$ & $g(x) = x(\ ) + 2(\ ) \in A \Rightarrow g(x) \in M$

$\Rightarrow p(x) - g(x) \in M \Rightarrow 1 \in M \Rightarrow M = R$.

⇒ UNIQUE FACTORIZATION DOMAIN (GAUSSIAN DOMAIN):

1) Integral Domain with unity is UFD if
   (i) Every non-zero, non-unit element a of R can be expressed as a product of finite no of irreducible elts.
   (ii) The factorisation is unique upto associates of the irreducible elements.

2) Every field F is a UFD as there are no non-zero non-unit elts.

3) $\mathbb{Z}$ is a UFD

4) In a UFD, prime element $\iff$ irreducible element

5) 2nd defn: ID R with unity is UFD if
   (i) non-zero & non-units are factorizable into irreducible elts
   (ii) Every irreducible element is prime.

6) Every Euclidean Domain is a UFD [ED = UFD, ED = PID]
   Also, every PID is UFD
   But UFD $\not\Rightarrow$ PID eg $\mathbb{Z}[x]$. (Ideal generated by (x, 2) is not principal)

7) F is a field $\Rightarrow$ F[x] is ED $\Rightarrow$ F[x] is PID $\Rightarrow$ F[x] is UFD

TIP: To show not PID, show not UFD
To show not ED, show not UFD/PID.

Example: Show $\mathbb{Z}[i\sqrt{5}]$ is not UFD.

$\mathbb{Z}[i\sqrt{5}]$ has $3, 2 \pm i\sqrt{5}$ as irreducible elements.

Now $9 = 3.3 = (2+i\sqrt{5})(2-i\sqrt{5})$

And 3 is not associate of $2 \pm i\sqrt{5}$

8) R is a UFD $\Rightarrow$ R[x] is UFD

eg $\mathbb{Z}$ & $\mathbb{Z}[x]$

9) gcd & lcm are assured in a UFD

10) Proof for PID $\Rightarrow$ UFD

Use the fact that every irreducible elt in PID is prime

We have to use induction for $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$

11) Irreducible Polynomial :

R is ID with unity, $f(x) \in R[x]$ is irreducible

if $f(x) = g(x)h(x) \Rightarrow$ either deg $g(x) = 0$ or deg $h(x) = 0$.

Remember: units of R & R[x] are same

irreducible elt of R $\Rightarrow$ irreducible elt of R[x]

12) R is ID with unity, irreducible elt in R[x] $\Rightarrow$ irreducible polynomial R[x]

converse not true: eg $f(x) = 3x^2+3 = 3(x^2+1)$ deg(3)>0

But neither 3 is unit, nor x^2+1

13) F is a field & $f(x) \neq 0 (x) \in F[x]$, irreducible elt $\Leftrightarrow$ irreducible polynomial

if $f(x) = g(x)h(x)$ is irreducible polynomial

$\Rightarrow$ deg g or deg h = 0 $\Rightarrow$ either $g(x) = \alpha$ or $h(x) = \beta$

Now α, β are units in F $\Rightarrow \alpha = g(x)$ is unit in F[x]

14) F is a field, $A = \langle p(x) \rangle$ is maximal $\Leftrightarrow$ $p(x)$ is irreducible polynomial

Also $\frac{F}{\langle p(x) \rangle}$ is a field

15> Eisenstein Criteria for Irreducibility over $\mathbb{Q}$:

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial with integer coefficients. Let p be a prime no st

$p \mid a_0, p \mid a_1, p \mid a_2 \cdots \to p \mid a_{n-1}$ But $p \nmid a_n$ & $p^2 \nmid a_0$

Then $f(x)$ is irreducible over $\mathbb{Q}$.

eg $f(x) = x^n - p$ is irreducible over $\mathbb{Q}$.

$f(x) = -p + 0\cdot x + 0\cdot x^2 + \cdots + 0\cdot x^{n-1} + 1\cdot x^n$

$p \mid a_0, a_1, \cdots a_{n-1}$, $p \nmid 1$ & $p^2 \nmid p$ $\therefore$ irreducible

eg $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ p is prime

$f(x) = \dfrac{x^p - 1}{x-1}$ Put $x = x+1$

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \frac{1}{x}\left[1 + px + \frac{p(p-1)}{2}x^2 + \cdots + px^{p-1} + x^p - 1\right]$$

$$= p + \frac{p(p-1)}{2}x + \cdots + px^{p-2} + x^{p-1}$$

Now $f(x+1)$ is irreducible.

eg $f(x) = x^4 + 1$ $f(x-1) = (x-1)^4 + 1 = x^4 + 4x^2 + 1 - 4x^3 - 4x + 2x^2 + 1$

$= x^4 - 4x^3 + 6x^2 - 4x + 2$

TIP: Always look for $\begin{matrix} x \to x+1 \\ x \to x-1 \\ x \to x+2 \end{matrix}$ replacements, till we get the Eisenstein conditions

eg factorise $x^2 + 3x + 1$ in $F[x]$ where F is the field $\mathbb{Z}_{11}$

$x^2 + 3x + 1 = (x+a)(x+b) \Rightarrow a + b = 3$, $ab = 1$

$ab = 1 \Rightarrow [(1,1), (3,4), (5,9), (7,8), (8,7), (9,5), (10,10)]$ (2,6) (4,2)

only $(5,9)$ satisfy $5 + 9 = 3$ $\Rightarrow (x+5)(x+9)$

eg. Prove that $x^3 - 9$ is reducible over Z_{11}.

$x^3 - 9 = x^3 + 2 \quad [\because -9 = 2 \bmod 11]$

$\to (x+a)(x^2+bx+c)$

$x^3 + (a+b)x^2 + (ab+c)x + ac = x^3 + 2$

$\Rightarrow \quad a+b = 0$
$ab+c = 0$
$2 = ac$

$(1,10,2), (2,9,1), (3,8,8)$
$(4,7,6), (5,6,7), (6,5,4),$
$(7,4,5), (8,3,3), (9,2,10)$

only $(7,4,5)$ satisfy (ii)
$(10,1,9)$

$\Rightarrow \quad x^3 - 9 = (x+7)(x^2+4x+5)$

* eg Show that x^2+2x+3 is irreducible over Z_5. Hence create a field containing 25 elts.

Use same trick to construct a field of order p^n where p is prime. Make a poly $f(x)$ irreducible where $\deg(f(x)) = n$

$f(x) = x^2+2x+3 = (x+a)(x+b) \to a+b = 2, \; ab = 3 \not\Rightarrow a, b$

$\therefore$ irreducible

Z_5 is field $\Rightarrow f(x)$ is irreducible $\Rightarrow f(x)$ is irreducible elt & $\langle f(x) \rangle$ is maximal

$\Rightarrow \quad \dfrac{F[x]}{\langle f(x) \rangle}$ is a field.

In $F[x]$, $p(x) \in F[x]$, $f(x) \in f(x)$, $\Rightarrow \exists \; q(x), r(x)$ st

$p(x) = q(x) f(x) + r(x)$

$\deg(r(x)) < \deg(f(x)) = 2 \Rightarrow (r(x)) = \alpha x + \beta$

$\therefore$ Any elt in $\dfrac{F[x]}{\langle f(x) \rangle}$ is $\langle f(x) \rangle + p(x) \quad p(x) \in F[x]$

$= \langle f(x) \rangle + q(x) f(x) + \alpha x + \beta$

$= \langle f(x) \rangle + \alpha x + \beta \quad \because q(x) f(x) \in \langle f(x) \rangle$

$\alpha, \beta \in Z_5 \Rightarrow O\left(\dfrac{F[x]}{\langle f(x) \rangle}\right) = 25$