MAA OMWATI DEGREE COLLEGE
HASSANPUR (PALWAL)

NOTES

NAME :

SUBJECT : Groups & Rings

CLASS : B.SC 5th Sem

SESSION : 2021-2022

1 Groups & Subgrps.

Defn Binary operation:- An operation which combines two elts. of a set to give another element of the same set is called a binary operation.

A fn denoted by '*' from $G \times G \to G$ is called binary operation on G if $a * b \in G \ \forall \ a, b \in G$.

Examples:- '+' is a binary operation on Z.
'x' is a binary operation on Z.

Def:- Algebraic structure:- A non empty set G equipped with one or more binary operation defined on it is called an algebraic structure. e.g. $(N, +)$, $(R, +, \times)$ are algebraic structu

Def:- Group:- A non empty set G along with binary operation '*' is said to be a group if it satisfies the following four properties:-

a) **Closure property:-**
If $a, b \in G$
then $a * b \in G$.

(b) **Associative law:-** If $a, b, c \in G$
then $a * (b * c) = (a * b) * c$

c) Existence of identity elt:- For all $a \in G$, there exists an element $e \in G$ s.t
$a * e = e * a = a$.
The elt. e is called identity elt.

(d) Existence of inverse:- For each $a \in G$, there exist a unique elt $b \in G$ s.t
$a * b = b * a = e$.
The elt. b is called inverse of a.

Def:- Abelian group:- A group $(G, *)$ is said to be abelian if in addition to the above four postulates, the following postulate is also satisfied

(e) Commutative property:-
$a * b = b * a$ for all $a, b \in G$.

Def:- Semi group:- An algebraic structure $(G, *)$ is called a semi group, if only the first two properties i.e closure & associative law are satisfied.

Def:- Finite and infinite groups:- If the no. of elts in the group are finite, then the gp. is called a finite gp., otherwise it is an infinite

group.

Def:- Order of a group:- The no. of elements in a finite group is called the order of the group. It is denoted by $O(G)$.

Def:- Addition modulo 'm':- It is written as $a +_m b$ where a & b are integers and m is a fixed +ve integers and is defined as $a +_m b = r$, $0 \le r \le m-1$, where r is a least non-ve remainder

Ex:- $15 +_5 9 = 4$.

Def:- Multiplication modulo 'm':- It is written as $a \times_m b$ where a & b are integers and m is a fixed +ve integer & is defined as $a \times_m b = r$, $0 \le r \le m-1$.

Ex $8 \times_3 4 = 2$.

Example:- Let $S = \{0, 1, 2, 3, 4\}$ and $+_5$ is the binary operation. Prove than S is an abelian gp. w.r.t $+_5$.

Sol:- Composition Table:-

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(i) Closure property:- $\forall\ a, b \in S$, we have
$a +_5 b \in S$.

(ii) Associativity:- If a, b, c are any elts of S, then
$a +_5 (b +_5 c) = a +_5 (b+c)$
= least non-ve remainder when divided by 5
$= (a+b) +_5 c = (a +_5 b) +_5 c$

(iii) Existence of Identity elt:- We have $0 \in S$
$0 +_5 a = a +_5 0 = a \quad \forall\ a \in S$.
Hence 0 is the identity elt. of S.

(iv) Existence of inverse:- from the table, the inverses of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 resp.

(v) Commutative law:- For all $a, b \in S$.
$a +_5 b = b +_5 a$

Hence $(S, +_5)$ is a finite abelian group of order 5.

Thm:- If every elt. of a group is its own inverse, then show that the group is abelian.

Sol. Let $(G, \cdot)$ be a group s.t

$x = x^{-1}$ and $y = y^{-1}\ \forall\ x, y \in G$.
As $x \cdot y \in G$ therefore $(xy)^{-1} = xy$
$y^{-1} x^{-1} = xy$
$yx = xy$
Hence G is an abelian group.

Ques If a group has four elements, show that it must be abelian.

Sol:- Let $G = \{e, a, b, c\}$ be a group of order four, s.t e is the identity element of G. Since $e^{-1} = e$, Therefore there is atleast one more element in G which is the inverse of itself.
Suppose that a is also an element of G s.t $a^{-1} = a$.

Case I:- When $b^{-1} = b$ and $c^{-1} = c$.
This case lead to the result that every element of G has its own inverse and so G is an abelian gp.

Case II:- When $b^{-1} = c$ and $c^{-1} = b$.
Here $bc = e = cb$.
The assumption $a^{-1} = a \Rightarrow a^2 = e$
Since $ab \in G$ so ab is either equal to e or b or c.
If $ab = e$, then $a^{-1} = b$ which is not true.
If $ab = a$, then $b = e$ which is not true
If $ab = b$, then $a = e$ which is also not true.

$\therefore$ $ab = c$

IIly, we can prove that $ba = c$ & $ac = b = ca$.

Composition table:

•	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	b^2	e
c	c	b	e	c^2

Since the elts in each row of the composition table are distinct,

$\therefore$ $b^2 = a$ and $c^2 = a$

We observe that the elts in the corresponding rows and columns are same.

$\therefore$ The composition in G is commutative

Hence, G is an abelian group.

Def:- Order of an element of a group

Let $(G, \circ)$ be a group with identity element e.

For $a \in G$, if there exist a least positive integer m s.t $a^m = e$ then m is called the order of element a and we write $o(a) = m$.

If there exist no +ve integer m s.t $a^m = e$, then we say that order of a is either infinite or zero.

Theorem:- The order of every element of a finite group is finite and is less than or equal to the order of the group.

Proof:- Let $(G, \cdot)$ be a finite group & a be any element of G.

$\therefore$ $a, a^2, a^3, a^4, \ldots$ are all elts of G.

Since the no. of elements in G are finite therefore $a, a^2, a^3, \ldots$ are not all distinct.

let $a^{m_1} = a^{m_2}$ $(m_1 > m_2)$

$\therefore$ $a^{m_1 - m_2} = a^0 = e \Rightarrow a^m = e$

where $m = m_1 - m_2$

Thus, there exist a positive integer m s.t $a^m = e \Rightarrow o(a) \leq m$.

$\Rightarrow$ order of a is finite.

Let n be the order of a.

$\therefore$ $a, a^2, a^3, \ldots, a^n$ are all n distinct elements of G.

Suppose that $o(a) > o(G)$

$n > o(G)$

$\Rightarrow$ Number of elements in $G < n$.

which is a contradiction to the result that $a, a^2, \ldots, a^n$ are n distinct elements of G.

Hence our supposition is wrong.

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

Hence the proof.

Ques:- If $(G, \cdot)$ is a group and a, b are any elements of G, then orders of ab and ba are same.

Sol:- As a, b are two elements of G.
$\therefore ab \in G$.
Also ab and $x^{-1}abx$ are of same order for some $x \in G$
i.e $O(ab) = O(x^{-1}abx)$
Taking $x = a$, $O(ab) = O(a^{-1}aba)$
$\Rightarrow O(ab) = O(ba)$
Hence the result.

Theorem:- A necessary and sufficient condition for a non empty finite subset H of group $(G, \cdot)$ to be a subgroup is that H must be closed with respect to multiplication.

Proof:-

Condition is necessary:-
Suppose H is a subgroup of $(G, \cdot)$
$a, b \in H \Rightarrow a \cdot b \in H$.
Thus H is closed w.r.t multiplication.

Condition is sufficient:-

It is given that for all $a, b \in H$
$\Rightarrow ab \in H$
For $a, a \in H \Rightarrow a^2 \in H$.

For $a, a^2 \in H \Rightarrow a^3 \in H$
For $a, a^3 \in H \Rightarrow a^4 \in H$
Hence $a, a^2, a^3, \ldots, a^n$, all belong to H
But H is a finite set
$\therefore$ Elements of this collection must be repeated
let $a^r = a^s$ where $r > s$
$\Rightarrow a^r \cdot a^{-s} = a^s \cdot a^{-s}$
$\Rightarrow a^{r-s} = a^0 = e$
where e is identity of G
But $r-s$ is a positive integer.
$\therefore a^{r-s} \in H \Rightarrow e \in H$
Hence identity exist.
As $r - s \geq 1$
$r - s - 1 \geq 0 \Rightarrow a^{r-s-1} \in H$
Now for each $a \in H$, $a\, a^{r-s-1} = a^{r-s}$
$= e$.
$\Rightarrow a^{r-s-1}$ is inverse of a.
Thus the inverse exists.
Also, the elements of H are also elements of group G. Therefore the composition in H is associative.
Hence H is a subgroup of G.
Hence the proof.

Theorem:- If H and K are two subgroups of a group G, then HK is a subgroup of G iff $HK = KH$.

Proof:- Let H, K be two subgroups of groups such that $HK = KH$

$HH^{-1} = H^{-1}H = H$ — (1)

& $KK^{-1} = K^{-1}K = K$ — (2)

Now $(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1})$

$= H(KK^{-1})H^{-1}$

$= HKH^{-1}$

$= KHH^{-1} = KH = HK$

Thus HK is a subgp. of G.

Conversely, Suppose that H, K and HK are subgroups of G. Now, we have to that $HK = KH$

Let hk be any elt. of HK where $h \in H$ and $k \in K$

As H, K are subgroups of G

$h^{-1} \in H$ and $k^{-1} \in H$

$\Rightarrow k^{-1}h^{-1} \in KH$

$(hk)^{-1} \in KH$

But KH is a subgroup of G

$hk \in KH$

Thus we have proved that $hk \in HK$

$\Rightarrow hk \in KH$

$\therefore HK \subseteq KH$ — (3)

Again, let kh be any elt. of KH where $k \in K$ and $h \in H$

As H, K are subgroups of G

$h^{-1} \in H$ and $k^{-1} \in K$

$\Rightarrow h^{-1}k^{-1} \in HK$.

$(kh)^{-1} \in HK \Rightarrow kh \in HK$

Thus, we have proved that $kh \in KH$

$\Rightarrow kh \in HK$

$\therefore KH \subseteq HK$ — (4)

From (3) & (4), we have $HK = KH$.

Theorem:- If H_1 and H_2 are two subgroups of G, then $H_1 \cap H_2$ is also a subgp of G.

Proof:- Identity element e is a common element of H_1 and H_2

$\therefore e \in H_1 \cap H_2$ i.e $H_1 \cap H_2 \neq \phi$

In order to prove that $H_1 \cap H_2$ is a subgp. of G, it is sufficient to prove that $a, b \in H_1 \cap H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

Let $a, b \in H_1 \cap H_2$

$\therefore a, b \in H_1$ and $a, b \in H_2$

But H_1 and H_2 are subgp. of G.

$\therefore ab^{-1} \in H_1$ and $ab^{-1} \in H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

$\therefore a, b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Hence $H_1 \cap H_2$ is a subgp. of G.

Example:- Show that the union of two subgp is a subgp if and only if one is contained in other.

Sol:- Suppose that H_1, H_2 are two subgps of a gp. of G s.t either

$H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

If $H_1 \subseteq H_2$, then $H_1 \cup H_2 = H_2$ which is a subgroup of G.

If $H_2 \subseteq H_1$, then $H_1 \cup H_2 = H_1$ which is a subgroup of G.

Hence, $H_1 \cup H_2$ is a subgroup of G.

Conversely, let H_1, H_2 be two subgroups of G s.t $H_1 \cup H_2$ is also a subgroup of G.

We have to prove that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Suppose that neither H_1 is a subset of H_2 nor H_2 is a subset of H_1

As H_1 is not a subset of H_2, therefore there exists $a \in H_1$ and $a \notin H_2$ but $a \in H_1 \cup H_2$ — (1)

Again as H_2 is not a subset of H_1, therefore there exist $b \in H_2$ and $b \notin H_1$ but $b \in H_1 \cup H_2$ — (2)

As $H_1 \cup H_2$ is a subgp. of G

$\therefore a, b \in H_1 \cup H_2 \Rightarrow ab \in H_1 \cup H_2$

$\therefore$ Either $ab \in H_1$ or $ab \in H_2$

Case I:- When $ab \in H_1$:

$ab \in H_1$

Also $a^{-1} \in H_1 \Rightarrow a^{-1} \cdot ab \in H_1$

$\Rightarrow b \in H_1$, which is a contradiction to (2),

Case II:- When $ab \in H_2$

we have $ab \in H_2$

Also $b^{-1} \in H_2$

$ab \cdot b^{-1} \in H_2$

$\Rightarrow a \in H_2$ which is a cont. to (1)

Hence either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Def:- Cyclic groups:- let G be a group. If for some $a \in G$, every element x of G is of the type a^n, where n is an integer, then G is called cyclic gp and is denoted by $\langle a \rangle$.

i.e $G = \{ \ldots a^{-3}, a^{-2}, a^{-1}, e, a, \ldots \} = \langle a \rangle$

Here a is called the generator of G.

1st Theorem:- Order of a cyclic group is the order of its generator.

Proof:- Let G be a cyclic group and 'a' be its one generator.

Case I:- When order of a is finite:-

Let $o(a) = n$

$\therefore$ G contains atleast n distinct elements $a, a^2, a^3, - - -, a^n = e$

We claim that G contains no more elements.

For each $x \in G$, we have $x = a^m$ where m is any integer.

For division algorithm, $m = nq + r$

$x = a^m = a^{nq+r} = a^{nq} \cdot a^r$

$= (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$, $0 \le r < n$

$\therefore$ Each element of G is of form a^r.
Hence G contains exactly n elements.
Thus, we have $o(a) = o(G) = n$.

Case II:- When order of a is infinite:
Suppose that $o(G)$ = finite
$\therefore$ There exists integers r and s s.t $r > s$ and $a^r = a^s$
$\Rightarrow a^{r-s} = a^0 = e$.
$\Rightarrow$ Order of a is finite which is a contradiction.
Hence our supposition that $o(a)$ is finite is wrong.
Thus $o(G)$ = infinite.
Hence we have $o(G) = o(a)$.
Hence the proof.

Theorem:- Every subgroup of a cyclic group is cyclic

Proof:- Let G be a cyclic group generated by a i.e $G = \langle a \rangle$.
Let H be a subgroup of G.
If $H = G$ or $H = \{e\}$, then H is cyclic
Now let H be a proper subgroup of G
$\therefore$ $x \in H \Rightarrow x \in G \Rightarrow x = a^t$ for some $t \in Z$

Since H is a group, therefore x^{-1} exists
$\Rightarrow a^{-t} \in H$
Thus H contains elements which are positive as well as negative powers of a.
If m is the least positive integer s.t $a^m \in H$, then we shall prove that H is cyclic and $H = \langle a^m \rangle$.
Let a^t be an arbitrary elt of H. We claim that t is a multiple of m, otherwise $t = mq + r$ where $r \neq 0$
Since $a^m \in H \Rightarrow a^{mq} \in H \Rightarrow a^{-mq} \in H$
Now $a^{-mq}, a^t \in H$
$\Rightarrow a^t \cdot a^{-mq} = a^{t-mq} = a^r \in H$
But m is the least positive integer s.t $a^m \in H$ which is a contradiction
Hence r must be zero
$\Rightarrow t = mq$
$a^t = a^{mq} = (a^m)^q$
Hence, every element of H is of form $a^t = (a^m)^q$
Therefore H is cyclic and a^m is its generator.

Chapter - 2
Cosets

Def:-
Cosets:- Let G be a group and H be any subgp of G. For any $a \in G$, the set
$Ha = \{ha : h \in H\}$ is called right coset of H in G generated by a.
Illy $aH = \{ah : h \in H\}$ is called left coset of H in G generated by a.

Theorem:- Any two right (left) cosets of a subgroup are either disjoint or identical.

Proof:- Suppose H is a subgroup of group G and let Ha and Hb be two right cosets of H in G.

Case I:- Ha and Hb are not disjoint sets.
Let d be a common element of Ha and Hb.
Now $d \in Ha$
$\Rightarrow d = h_1 a$ where $h_1 \in H$.
and $d \in Hb \Rightarrow d = h_2 b$ where $h_2 \in H$
$\Rightarrow \therefore h_1 a = h_2 b$
$\Rightarrow h_1^{-1} h_1 a = h_1^{-1} h_2 b$
$ea = h_1^{-1} h_2 b$
$a = h_1^{-1} h_2 b$
$\therefore Ha = H h_1^{-1} h_2 b = Hb$.

Thus if Ha and Hb are not disjoint sets, then they are identical.

Case II:- Ha and Hb are disjoint sets.
In this case, the required result is true
From the above two cases, we have either $Ha \cap Hb = \phi$ or $Ha = Hb$
Illy, we can prove that either $bH \cap aH = \phi$ or $bH = aH$.

Def:- Index of a subgroup in a group:-
If H is a subgroup of a group G, then the no. of distinct right (left) cosets of H in G called index of H in G and is denoted by $[G:H]$.

Ex:- If G is the additive group of integers and H is the subgroup of G obtained on multiplying the elements of G by 4, find the index of H in G.

Sol:- Here $G = \{\ldots, -4, -3, -2, -1, 0, 1, 2, \ldots\}$
and $H = \{\ldots, -16, -12, -8, -4, 0, 4, 8, \ldots\}$
Here G is an abelian group w.r.t addition of integers, so every right coset is equal to the corresponding left coset in G.
Now, right cosets of H in G are as under:-
For $0 \in G$, $H+0 = \{\ldots -16, -12, -8, -4, 0 \ldots\}$

For $1 \in G$, $H+1 = \{\ldots, -15, -11, -7, -3, 1, 5, \ldots\}$
For $2 \in G$, $H+2 = \{\ldots -14, -10, -6, -2, 2, 6, \ldots\}$
For $3 \in G$, $H+3 = \{\ldots, -13, -9, -5, -1, 3, 7, \ldots\}$
For $4 \in G$, $H+4 = \{\ldots -12, -8, -4, 0, 4, 8, \ldots\}$
$= H+0$.

For $5 \in G$, $H+5 = H+1$.
The distinct and disjoint right cosets are
$H+0$, $H+1$, $H+2$, $H+3$
$G = (H+0) \cup (H+1) \cup (H+2) \cup (H+3)$
Hence the index of H in G is 4.

Theorem:- Lagrange's theorem:-

Statement:- The order of each subgroup of a finite group is a divisor of the order of the group.

Proof:- Let G be a finite group of order n and H be its subgroup of order m

$\therefore$ $O(G) = n$, $O(H) = m$

Let $H = \{h_1, h_2, h_3, \ldots, h_m\}$
For $a_1 \in G$, $Ha_1 = \{h_1a_1, h_2a_2, \ldots, h_ma_1\}$
For $a_2 \in G$, $Ha_2 = \{h_1a_2, h_2a_2, \ldots, h_ma_2\}$
For $a_3 \in G$, $Ha_3 = \{h_1a_3, h_2a_3, \ldots, h_ma_3\}$
. . . . . .
For $a_k \in G$, $Ha_k = \{h_1a_k, h_2a_k, \ldots, h_ma_k\}$
Every right coset of H has m distinct elements and there is no

common element between the right cosets of H in G.

$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$

Thus no. of elements in G
= no. of elts in Ha_1 + no. of elts in Ha_2 + . . . + no. of elts in Ha_k

$O(G) = k \cdot m$
$n = k \cdot m$
$k = \frac{n}{m} = \frac{O(G)}{O(H)}$

Hence, order of H is a divisor of order of G.

Hence the proof.

Theorem:- The order of every elt. of a finite group is a divisor of the order of the group.

Proof:- Let G be a finite group of order n and a be any element of G of order m.

Let H be a subgroup of G consisting of all integral powers of a

$\therefore$ $H = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, \ldots\}$

We shall prove that H contains only m distinct elements

i.e $H = \{a, a^2, a^3, \ldots, a^m = e\}$

Suppose that $a^r = a^s$ where $1 \le r \le m$, $1 \le s \le m$ and $r > s$

$\therefore$ $a^r \cdot a^{-s} = a^s \cdot a^{-s}$

$a^{r-s} = a^0 = e$ where $r-s < m$

which is a contradiction as m is the least positive integer s.t $a^m = e$

$\therefore$ $a, a^2, a^3, \ldots a^m$ are all distinct elts of H.

If $l > m$ is any integer, Then

$l = mp+q$, where p, q are integers and $0 \le q \le m$

Now $a^l = a^{mp+q}$

$= a^{mp} \cdot a^q$

$= (a^m)^p \cdot a^q = e \cdot a^q = a^q$

As $0 \le q < m$, Therefor a^l is one of the m elements $a, a^2, a^3, \ldots, a^m = e$

Hence H has only m distinct elts and order of H is m.

$\therefore$ By Lagrange's theorem, m is a divisor of n.

Thus order of every elt. of a finite group is a divisor of the order of the group.

Hence the proof.

Def: Normal subgroup: A subgroup H of G is called a normal subgroup of G if $xhx^{-1} \in H$ for $x \in G$ & $h \in H$.

Simple groups:- If a group G has no proper normal subgroups, i.e if the only normal subgroups of G are $\{e\}$ and G itself, then G is called a simple group.

Theorem:- A subgroup H of a group G is normal iff each left coset of H in G is a right coset of H in G.

Proof:- Let H be a normal subgroup of G

$\Rightarrow$ $xHx^{-1} = H$ for all $x \in G$

$\Rightarrow$ $(xHx^{-1})x = Hx$

$xH = Hx \quad \forall\ x \in G$

Conversely, Suppose that each left coset of H in G is a right coset of H in G

Let $x \in G$, then $xH = Hy$ for some $y \in G$

Since $e \in H \Rightarrow xe \in xH$

$\Rightarrow x \in xH$

$x \in Hy \quad [\because xH = Hy]$

Also for $x \in G$, Hx is a right coset of H in G

$\therefore$ $ex \in Hx$

$x \in Hx$

$\therefore$ Hy, Hx are two right cosets of H in G, each containing x.

$\therefore$ $Hy \cap Hx \neq \phi$

Since two right cosets of H in G are disjoint or identical

$\therefore$ $Hy = Hx$

Thus $xH = Hy = Hx$

$xH = Hx$

$xHx^{-1} = Hxx^{-1}$

$xHx^{-1} = He = H$

$xHx^{-1} \subseteq H$

$\Rightarrow$ $xhx^{-1} \in H \ \forall \ h \in H, x \in G$

$\therefore$ H is a normal subgroup of G.

Hence the proof.

Theorem: A subgroup H of G is normal iff the product of two right cosets of H in G is again a right coset of H in G.

Proof: Let Ha and Hb be two right cosets of H in G and H be a normal subgroup of G.

Now $(Ha)(Hb) = H(aH)b$

$= H(Ha)b$

$= Hab$ where $ab \in G$

So product of two right cosets is also a right coset.

Conversely, if Hx and Hx^{-1} are two right cosets of H in G, then $HxHx^{-1}$ is also a right coset of H in G

Since $e \in H \Rightarrow e = exex^{-1} \in HxHx^{-1}$

Also, H is itself a right coset in G

$\Rightarrow e \in H$ and $e \in HxHx^{-1}$

So both right cosets of H in G are either equal or disjoint.

i.e $HxHx^{-1} = H \ \forall \ x \in G$

$\Rightarrow h_1 xhx^{-1} \in H \ \forall \ x \in G$ & $\forall \ h_1, h_2 \in H$

$\Rightarrow$ $xhx^{-1} \in h_1^{-1}H = H$

$\Rightarrow$ H is a normal subgroup of G.

Def: **Quotient group (or Factor group):-**

Let G/H be the collection of all cosets of H in G

i.e $G/H = \{Ha : a \in G\}$

If $a, b \in G$, then $(Ha)(Hb) = H(aH)b$

$= Hab$

Hence, the set G/H of all cosets of H in G is a group w.r.t '$\circ$' and is called quotient group of G by H.

The identity element of quotient group G/H is H.

Theorem: If H is a normal subgroup of G & $a \in G$ is of order n, prove that $O(Ha) = m$, then m divides n.

Proof: We know that the identity elt. of G/H is H. If e is the identity of G and $O(a) = n$ then $a^n = e$.

$\therefore$ $Ha^n = He = H$

But $Ha^n = H(aa...a) = (Ha)(Ha)...(Ha)$

$= (Ha)^n$

$\Rightarrow (Ha)^n = Ha^n = H$ which is an identity of G/H.

As order of Ha in G/H is m and $(Ha)^n$ = identity of G/H.

$\therefore$ m divides n.

Hence the proof.

Chapter-3
Homomorphism and Automorphism

Defi:- Homomorphisms of groups:-

Let G_1 and G_2 be two groups and '$\circ$' and '$*$' denote their respectively binary compositions. Then a mapping $f: G_1 \to G_2$ defined by $f(a \circ b) = f(a) * f(b)$ $\forall$ $a, b \in G_1$, is called homomorphism.

Here, $f(G_1) = \{f(x) : x \in G_1\}$ is called the homomorphic image of G_1.

- Let G_1 and G_2 be two additive groups. Then $f: G_1 \to G_2$ defined by $f(a+b) = f(a) + f(b)$ $\forall$ $a, b \in G_1$.
- Let G_1 and G_2 be two multiplicative groups. Then $f: G_1 \to G_2$ defined by $f(ab) = f(a)f(b)$ $\forall$ $a, b \in G_1$.
- If the homomorphism $f: G_1 \to G_2$ is also one-one, then f is called monomorphism.
- A homomorphism which is also onto, is called epimorphism
- A homomorphism $f: G_1 \to G_2$ is called trivial homomorphism if $f(x)$ = identity of G_2 for all $x \in G_1$.
- A homomorphism $f: G_1 \to G_1$ is called identity homomorphism if $f(x) = x$ $\forall$ $x \in G_1$

Def:- **Isomorphisms:-** A homomorphism which is one-one and onto is called isomorphism.

Def:- **Isomorphic groups:-** Two groups G and G' are called isomorphic groups if there exists an isomorphism from G to G'. i.e $G \cong G'$.

Ex:- Show that the mapping $x \to x^{-1}$ of a group G onto itself is an isomorphism iff G is abelian, x being any arbitrary elt. of G.

Sol:- Let $f: G \to G$ defined by $f(x) = x^{-1} \forall x \in G$.
Since inverse of an elt. of a group is unique.
$\therefore$ f is well defined.
Let G be an abelian group. We have to show that f is an isomorphism.
f is homomorphism:-
For $x, y \in G$, $f(xy) = (xy)^{-1} = y^{-1}x^{-1}$
$= x^{-1}y^{-1} = f(x)f(y)$
$\therefore$ f is a homomorphism.
f is one-one:- For $x, y \in G$, $f(x) = f(y)$
$\Rightarrow x^{-1} = y^{-1}$
$(x^{-1})^{-1} = (y^{-1})^{-1}$
$x = y$
f is one-one.

f is onto:- For $z \in G$, $z^{-1} \in G$ and $f(z^{-1}) = (z^{-1})^{-1} = z$
$\therefore$ f is onto.
Hence, $f: G \to G$ is an isomorphism.
Conversely, let $f: G \to G$ be an isomorphism. We have to show that G is abelian.
For $x, y \in G$, we have
$f(xy) = f(x)f(y)$
$(xy)^{-1} = x^{-1}y^{-1}$
$(xy^{-1})^{-1} = (x^{-1}y^{-1})^{-1}$
$xy = yx$
Hence G is an abelian group.
Hence the proof.

Def:- **Kernel of homomorphism:-** Let $f: G \to G'$ be a homomorphism. Then kernel of f is the set of all those members of G which are mapped by f into identity element of G'.
i.e kernel of f = $\{x : x \in G, f(x) = e'$ where e' is the identity of $G'\}$.

Theorem:- If $f: G \to G'$ is a homomorphism, then prove that kernel of f is a normal subgroup of G.

Proof:- Let e and e' be identities of G and G' respectively.

Since f is homomorphism, therefore
$f(e) = e'$
$\Rightarrow$ $e \in$ Kerhel $f = K \Rightarrow K \neq \phi$
Let $a, b \in K \Rightarrow f(a) = f(b) = e'$
Now, $f(ab^{-1}) = f(a) f(b^{-1})$
$= f(a)[f(b)]^{-1} = e'(e')^{-1} = e'$
$ab^{-1} \in K \Rightarrow K$ is subgp. of G.
Let $g \in G$ and $k \in K$ i.e $f(k) = e'$
$f(gkg^{-1}) = f(g) f(k) f(g^{-1})$
$= f(g) e' f(g^{-1}) = f(g)[f(g)]^{-1}$
$= e'$

$gkg^{-1} \in K$.
Hence K is a normal subgp. of G.
Hence the proof.

Theorem:- The necessary and sufficient condition for a homomorphism f to be one-one is that kernel $f = \{e\}$, where e is identity of domain.

Proof:- Let $f: G \to G'$ be a homomorphism s.t f is one-one.
Let e be identity of G and e' be identity of G'. Let K be kernel of f and a be any element of K.
Then $f(a) = e'$
But $f(e) = e' \Rightarrow f(a) = f(e)$
$\Rightarrow a = e$
$K = \{e\}$

Conversely, Suppose that f is homomorphism and K is kernel of f s.t $K = \{e\}$.
Let $a, b \in G$.
Consider $f(a) = f(b)$
$f(a) f(b)^{-1} = f(b)[f(b)]^{-1}$
$\Rightarrow f(a) f(b^{-1}) = e'$
$\Rightarrow f(ab^{-1}) = e' \Rightarrow ab^{-1} \in K$
But $K = \{e\}$
$\therefore ab^{-1} = e \Rightarrow ab^{-1}b = eb$
$\Rightarrow a = b$
Thus we have $f(a) = f(b) \Rightarrow a = b$.
Thus the function f is one-one.
Hence the proof.

Fundamental theorem on homomorphism of groups.

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

Proof:- Let $f: G \to G'$ be an onto homomorphism i.e G' is the homomorphic image of G.
Let K be the kernel of f. Then K is a normal subgroup of G.
We shall prove that $G' \cong G/K$.
Let $a \in G$, then $Ka \in G/K$ and $f(a) \in G'$
Consider the mapping $\phi: G/K \to G'$ s.t
$\phi(Ka) = f(a)$ $\forall$ $a \in G$
ϕ is well defined:

If $a, b \in G$ and $Ka = Kb$ then $ab^{-1} \in K$

$\Rightarrow f(ab^{-1}) = e'$ where e' is identity of G'.

$\Rightarrow f(a) f(b^{-1}) = e'$

$\Rightarrow f(a) [f(b)]^{-1} = e'$

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

$\Rightarrow \phi(Ka) = \phi(Kb)$

Therefore ϕ is well defined.

ϕ is one to one:-

Let $\phi(Ka) = \phi(Kb) \Rightarrow f(a) = f(b)$

$\Rightarrow f(a)[f(b)]^{-1} = e'$

$\Rightarrow f(ab^{-1}) = e'$

$\Rightarrow ab^{-1} \in K$.

$\Rightarrow Ka = Kb$

Thus $\phi(Ka) = \phi(Kb) \Rightarrow Ka = Kb$

$\therefore \phi$ is one to one.

ϕ is onto:-

Let $y \in G'$. Then $y = f(a)$ where $a \in G$

$\therefore$ There exists $Ka \in G/K$ s.t $\phi(Ka) = f(a) = y$

Thus ϕ is onto.

Hence ϕ is one-one and onto.

Also $\phi[(Ka)(Kb)] = \phi[K(ab)] = f(ab)$

$= f(a) f(b)$

$= \phi(Ka)\phi(Kb)$

Therefore ϕ is homomorphism.

Hence, G/K is isomorphic to G'.

Hence the proof.

Def:- Automorphism of a group:-

An isomorphism from a group G to itself is called an automorphism of G. Thus a one one onto map $f: \langle G, * \rangle \to \langle G, * \rangle$ is called an automorphism of G if

$f(x * y) = f(x) * f(y) \quad \forall \; x, y \in G$.

Let $(G, *)$ be a group. A mapping $f: (G, *) \to (G, *)$ is called an automorphism of a group G if

(i) f is a homomorphism

(ii) f is one-one

(iii) f is onto.

Ex:- Let G be an abelian group and $f: G \to G$ be s.t $f(x) = x^{-1}$, show that f is an automorphism.

Sol:- Let x, y be any two elts of G.

(i) **f is homomorphism:-**

$f(xy) = (xy)^{-1}$

$= y^{-1}x^{-1} = x^{-1}y^{-1}$

$= f(x) f(y)$

$\therefore f$ is a homomorphism.

(ii) **f is one-one:-** $f(x) = f(y)$

$\Rightarrow x^{-1} = y^{-1}$

$(x^{-1})^{-1} = (y^{-1})^{-1}$

$\Rightarrow x = y$

$\Rightarrow f$ is one-one.

(iii) f is onto:- For any $x \in G$, $x^{-1} \in G$
$f(x^{-1}) = (x^{-1})^{-1} = x$
$\therefore$ f is onto.
Thus f is a homomorphism and $f: G \to G$ is one-one and onto.
Hence f is an automorphism of G.

Theorem:- Let G be a group and let $Aut(G)$ denote the set of all automorphisms of a group G. Then $Aut(G)$ forms a group under the composition of mappings as binary operation.

Proof:- Let $Aut(G) = \{f : f \text{ is an aut. of } G\}$
We shall show that $Aut(G)$ forms a group w.r.t composition of mappings.
Closure property:- If $f, g \in Aut(G)$, then $gf : G \to G$ being the composition of f and g is also one one onto mapping
If $x, y \in G$, then
$$\begin{aligned}(gf)(xy) &= g[f(xy)] \\ &= g[f(x)\, f(y)] \\ &= g[f(x)]\; g[f(y)] \\ &= (gf)(x)\,(gf)(y)\end{aligned}$$
Thus gf is also an auto. of G and so $gf \in Aut(G)$. This shows that comp. of auto. is a binary operation.

Associativity:- Let $f, g, h \in Aut(G)$
$$\begin{aligned}(f(gh))(x) &= f(gh)(x) \\ &= f(g(h(x))) \\ ((fg)h)(x) &= (fg)(h(x)) \\ &= f(g(h(x)))\end{aligned}$$
$\therefore$ $f(gh) = (fg)h$. $\forall$ $f, g, h \in Aut(G)$

Existence of identity:-
Let $I : G \to G$ be the identity fn of G,
s.t $I(x) = x$ $\forall$ $x \in G$
Obviously I is one one onto
Let $x, y \in G$, then $xy \in G$
$$I(xy) = xy = I(x)\, I(y)$$
$\Rightarrow$ I is a homomorphism.
Thus $I : G \to G$ is an isomorphism.

Existence of inverse:- Let $f \in Aut(G)$
$\Rightarrow$ f is a one-one onto map. from G to G.
$\Rightarrow$ f^{-1} is also one-one onto map. from $G \to G$.
Let $x, y \in G$. Then there exist $x_1, y_1 \in G$, s.t
$f^{-1}(x) = x_1 \Leftrightarrow f(x_1) = x$.
$f^{-1}(y) = y_1 \Leftrightarrow f(y_1) = y$
Then $f^{-1}(xy) = f^{-1}[f(x_1) f(y_1)]$
$$\begin{aligned}&= f^{-1}[f(x_1 y_1)] \\ &= x_1 y_1 \\ &= f^{-1}(x)\, f^{-1}(y)\end{aligned}$$
Also f^{-1} is one one onto
$\Rightarrow$ f^{-1} is an auto and so $f^{-1} \in Aut(G)$
Thus $Aut(G)$ forms a group w.r.t comp. of mappings as binary operation.
Hence the proof.

Ex If $o(Aut(G)) > 1$, then show that $o(G) > 2$

Sol:- If $o(G) = 1$, then G has only one automorphism called identity map I which is a contradiction to the given statement that $o(Aut\,G) > 1$.

If $o(G) = 2$, then $G = \{e, a : a \neq e, a^2 = e\}$

Also $o(Aut\,G) > 1$.

$\Rightarrow$ There exist $T \in Aut\,G$ s.t $T \neq I$

Thus there exist $x \in G$ s.t $T(x) \neq x$

But $T(e) = e$

Therefore $T(a)$ must be equal to a, which is a contradiction to the hypothesis, that there exist x st $T(x) \neq x$.

$\therefore o(G) \neq 2$

Hence $o(G) > 2$.

Def:- **Inner automorphism:-** Let G be a group and $a \in G$. Then the mapping $T_a : G \to G$ defined by $T_a(x) = a^{-1}xa$ is an auto. of G and it is called an inner auto. of G.

Ex Prove that the identity mapping is the only inner automorphism for an abelian group.

Sol. For an abelian group G, we have

$T_a(x) = a^{-1}xa \;\forall\; x \in G$

$T_a(x) = a^{-1}(ax) = (a^{-1}a)x = x$.

i.e $T_a(x) = x \quad \forall\; x \in G$

which show that T_a is the identity map.

Ex If f is an inner automorphism of G, Show that $o(f(a)) = o(a)$ for $a \in G$. Also Show that $o(b^{-1}ab) = o(a)$ $\forall$ $a, b \in G$.

Sol:- **Case I:-** When order of a is finite

Let $o(a) = m$, then m is the least positive integer s.t $a^m = e$

Since f is an auto. of G.

$(f(a))^m = f(a)f(a)\ldots$ m times

$= f(a.a, \ldots m \text{ times})$

$= f(a^m) = f(e) = e$.

$\therefore o(f(a)) \leq m$.

If $o(f(a)) < m$, then let us take $o(f(a)) = m_0$ where m_0 is a +ve integer less than m.

Now $o(f(a)) = m_0$

$\Rightarrow f(a)(f(a)) \ldots m_0$ times $= e$

$f(a.a \ldots m_0 \text{ times}) = e$

$f(a^{m_0}) = e = f(e)$

$\Rightarrow a^{m_0} = e$ [$\because$ f is one one]

which is a contradiction as $o(a) = m$

$\therefore o(f(a)) \neq m$, then $o(f(a)) = m = o(a)$

Case II:- When order of a is infinite :-

Suppose that $o(f(a)) =$ finite $= n$ (say)

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

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

$\Rightarrow$ $a^n = e$

$\Rightarrow$ $o(a)$ is finite, which is a contradiction

Hence $o(f(a)$ is infinite.

Part b:- $f_b(a) = b^{-1}ab$

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

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

Hence the solution.

Theorem: Let f be an automorphism of G. Let N be a normal subgroup of G. Prove that $f(N)$ is a normal subgp. of G.

Sol:- Let $f(N) = \{f(n) : n \in N\}$

If a, b be any two elts of $f(N)$, then $a = f(n_1)$ and $b = f(n_2)$ $\forall$ $n_1, n_2 \in N$

Now $n_1, n_2 \in N \Rightarrow n_1 n_2^{-1} \in N$

$\Rightarrow f(n_1 n_2^{-1}) \in f(N)$

$\Rightarrow f(n_1) f(n_2^{-1}) \in f(N)$

$\Rightarrow f(n_1) f(n_2)^{-1} \in f(N)$

$\Rightarrow ab^{-1} \in f(N)$

Thus $f(N)$ is a subgp. of G.

Since f is a function of G onto G.

For $x \in G$, $x = f(y)$ where $y \in G$.

If $k \in f(N)$, then $k = f(n)$ for $n \in N$

$xkx^{-1} = f(y) f(n) [f(y)]^{-1}$

$= f(y) f(n) f(y^{-1})$

$= f(yny^{-1})$

As N is a normal subgp of G. Therefore $yny^{-1} \in N$ $\forall$ so $f(yny^{-1}) \in f(N)$

$\therefore$ $xkx^{-1} \in f(N)$

Hence $f(N)$ is a normal subgp. of G.

Hence the proof.

Ex:- Let G be an infinite cyclic group. Show that order of $Aut(G)$ is 2.

Sol.- Let $G = \langle a \rangle$

If $T \in Aut(G)$ then $T : G \to G$ is an automorphism.

Here T is an onto map.

For each $x \in G$, there exist some $y \in G$ s.t

$x = T(y)$

Also $y \in G \Rightarrow y = a^m$, where m is an integer

$\therefore$ $x = T(y) = T(a^m) = (T(a))^m$

which shows that $T(a)$ is a generator of G.

But the only generators of infinite cyclic group $G = \langle a \rangle$ are a and a^{-1}.

$\therefore$ either $T(a) = a$ or $T(a) = a^{-1}$

which shows that T has only two choices.

$\therefore$ $o(Aut\ G) \leq 2$.

Define a map $T : G \to G$ s.t $T(x) = x^{-1}$

obviously, $T \in Aut(G)$

Let $x \in G$ be arbitrary.

If $T = I$ then $T(x) = x$

$\Rightarrow$ $x^{-1} = x$

$\Rightarrow a^{-1} = a$

$\Rightarrow a^2 = e$

$\Rightarrow o(a)$ is finite, which is a contradiction

i.e $T \neq I$ and so G has at least two automorphism.

Thus $o(Aut(G)) \geq 2$

From (1) & (2), it follows that

$o(Aut\, G) = 2$.

Def:- Centre of a group:- Let G be a group. The set of all those elements of G which commute with every element of the group is called centre of G and is denoted by $Z(G)$.

$Z(G) = \{z \in G : zx = xz \ \forall\ x \in G\}$.

Theorem: Prove that centre of a group is a normal subgroup of G.

Proof:- Let $Z(G)$ be the centre of the group G.

Since $e \in Z(G)$ therefore $Z(G) \neq \phi$

Again $a, b \in Z(G)$

$\Rightarrow ax = xa,\ bx = xb \ \forall\ x \in G$

Now $bx = xb$

$b^{-1}(bx)b^{-1} = b^{-1}(xb)b^{-1}$

$xb^{-1} = b^{-1}x \ \forall\ x \in G$

$\Rightarrow b^{-1} \in Z(G)$

Also $(ab^{-1})x = a(b^{-1}x)$

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

$= (ax)b^{-1} = (xa)b^{-1}$

$= x(ab^{-1})$

$\Rightarrow ab^{-1} \in Z(G)$

Thus $Z(G)$ is a subgp. of G.

Let $a \in Z(G)$ then

$xax^{-1} = (xa)x^{-1} = (ax)x^{-1} = a(xx^{-1})$

$= a \in Z(G)$

$\Rightarrow xax^{-1} \in Z(G) \ \forall\ x \in G$

Hence $Z(G)$ is a normal subgp. of G.

Hence the proof.

Theorem:- The set $Inn(G)$ of all inner auto. of a group G is isomorphic to the quotient group $G/Z(G)$ i.e $Inn(G) \cong G/Z(G)$

Proof:- Define a mapping $f: G \to Inn(G)$ s.t

$f(a) = T_{a^{-1}} \ \forall\ a \in G$

f is well defined

Let a, b be two elts of G s.t $a = b$

$\Rightarrow a^{-1} = b^{-1}$

$\Rightarrow T_{a^{-1}} = T_{b^{-1}}$

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

$\therefore f$ is well defined.

f is onto :- For each $T_a \in Inn(G)$ s.t $a \in G$.

$\Rightarrow a^{-1} \in G$

$\Rightarrow f(a^{-1}) \in T_{(a^{-1})^{-1}} = T_a$.

Thus every $T_a \in Inn(G)$ is a f-image of some $a^{-1} \in G$ & so f is onto.

f is homomorphism :-

For $a, b \in G$, we have

$f(ab) = T_{ab} = T_{b^{-1}a^{-1}} = T_{a^{-1}} T_{b^{-1}}$

$= f(a) f(b)$

$\therefore$ f is homomorphism.

Finally, we shall show that $\ker f = Z(G)$.

$\ker f = \{ x \in G : T_{x^{-1}} = I \}$

$= \{ x \in G : T_{x^{-1}}(y) = I(y) \ \forall \ y \in G \}$

$= \{ x \in G : xyx^{-1} = y \ \forall \ y \in G \}$

$= \{ x \in G : xy = yx \ \forall \ y \in G \}$

$= Z(G)$.

Thus we have shown that $f : G \to \text{Inn}G$ is a onto homomorphism with $\ker f = Z(G)$

Hence by fundamental theorem,

$\text{Inn}(G) \cong G/\ker f$.

$\text{Inn}(G) \cong G/Z(G)$.

Hence the proof.

Ex Let $Z(G)$ be the centre of a group G. If G/Z is cyclic, then prove that G is abelian.

Sol:- Since G/Z is cyclic, so G/Z has a generator, say Zg where $g \in G$

Let $a, b \in G$ be arbitrary, Obviously

$Za \in G/Z$

$\Rightarrow$ $Za = (Zg)^n = Zg^n$ for some int n.

Now $a \in Za$ & $Za = Zg^n$

$\Rightarrow a \in Zg^n$

$\Rightarrow a = z_1 g^n$ for some $z_1 \in Z$

Ily $b = z_2 g^m$ for some $z_2 \in Z$ & some int m

Now $ab = (z_1 g^n)(z_2 g^m)$

$= z_1 g^n z_2 g^m = z_1 z_2 g^n g^m$

$= z_1 z_2 g^{n+m}$

Also $ba = (z_2 g^m)(z_1 g^n) = z_2 z_1 g^m g^n$

$= z_2 z_1 g^{m+n}$

$\therefore$ $ab = ba \ \forall \ a, b \in G$

Hence G is abelian.

Ex Let G be a non abelian group s.t $O(G) = p^3$ where p is a prime. Show that $O(Z(G)) = p$.

Sol: Since $O(G) = p^3$, where p is a prime no.

$\therefore$ $Z(G) \neq \{e\} \Rightarrow O(Z) > 1$

But $Z(G)$ is a subgp of G

$\therefore$ $O(Z(G)$ must be div of $O(G)$.

$\Rightarrow$ $O(Z(G))$ must be a div of p^3.

But p is a prime no.

$\therefore$ either $O(Z(G)) = p$ or p^2 or p^3

(i) If $O(Z(G)) = p^3$, then $O(Z(G)) = O(G)$

$\Rightarrow Z(G) = G$

$\Rightarrow G$ is abelian which is a contr.

$\therefore$ $O(Z(G)) \neq p^3$.

(ii) If $O(Z(G)) = p^2$, then
$O(G/Z(G)) = \frac{O(G)}{O(Z(G))} = \frac{p^3}{p^2} = p$

$\Rightarrow$ $O(G/Z(G)) = p$ (prime)

$\Rightarrow$ $G/Z(G)$ is cyclic $\Rightarrow$ G is abelian.
which is again a contradiction
$\therefore$ $O(Z(G)) \neq p^2$

From (i) & (ii), the only possibility is that $O(Z(G)) = p$.
Thus the centre $Z(G)$ of G has exactly p elements.

Def:- **Characteristic subgroups:-**
Let G be a group. A subgroup H of G is said to be a characteristic subgp of G if $T(H) \subseteq H$ $\forall$ $T \in Aut(G)$

Ex:- Show that a characteristic subgroup of a group G is a normal subgp of G. Is the converse true?

Sol:- Let H be a characteristic subgp of G.
By def, $T(H) \subseteq H$ $\forall$ $T \in Aut(G)$
Let $a \in G$, $x \in H$
Let $T_{a^{-1}}(H) \subseteq H$
$axa^{-1} = T_{a^{-1}}(x) \in T_{a^{-1}}(H) \subseteq H$
Thus H is a normal subgp of G
However, the converse is not true.
Let $G = \{e, a, b, ab : a^2 = b^2 = (ab)^2 = e$
$ab = ba\}$

be an abelian gp of order four.
Obviously, $H = \{e, a\}$ is a subgp of G.
Also index of H in $G = \frac{O(G)}{O(H)} = \frac{4}{2} = 2$
$\therefore$ H is a normal subgp of G.
Define $T: G \to G$ s.t $T(a) = b$, $T(b) = a$
$T(ab) = ab$, $T(e) = e$.
$\therefore$ T defined above $\in Aut(G)$
But $T(a) = b \notin H$
Hence H is not a characteristic subgp of G.

Def:- **Normalizer of an element:-** Let G be a group. If $a \in G$ be any element, then the set of all those element of G which commute with a is called normalizer of element a in G.
$N(a) = \{x \in G : ax = xa\}$

Theorem:- Let $Z(G)$ be the centre of a group G. Then $a \in Z(G)$ iff $N(a) = G$. If G is a finite group, then $a \in Z(G)$ iff $O(N(a)) = O(G)$

Proof:- For $a \in G$, we know that
$N(a) = \{x \in G : xa = ax\}$ is a subgp of G
& $Z(G) = \{z \in G : zx = xz\}$ $\forall$ $x \in G\}$
Now $a \in Z(G) \Rightarrow ax = xa$ $\forall$ $x \in G$.
$\Rightarrow$ $x \in N(a)$
$G \subseteq N(a)$
Also $N(a) \subseteq G$

Thus $N(a) = G$.

Conversely, if $N(a) = G$ then $G \subseteq N(a)$

Thus for $x \in G$, $x \in N(a)$

$xa = ax \quad \forall x \in G$.

$a \in Z(G)$

Thus $N(a) = G \Rightarrow a \in Z(G)$

If G is finite, $N(a) = G$.

iff $o(N(a)) = o(G)$

Hence the proof.

Def:- Commutator:- Let G be a group. For $a, b \in G$, the element $a^{-1}b^{-1}ab$ is called a commutator of a and b.

Symbolically, $[a,b] = a^{-1}b^{-1}ab$.

Theorem:- If G' is a commutator subgp (derived group) of G, then

(i) G' is a normal subgp. of G.

(ii) G/G' is abelian

(iii) G' is the smallest subgp of G s.t G/G' is abelian.

Proof:- (i) Let $T = \{a^{-1}b^{-1}ab : a, b \in G\}$

G' is generated by T & $T \subset G' \subset G$

Let $x \in G$ & $g \in G'$ be arbitrary

$xg \in G \Rightarrow g, x^{-1} \in G$

$g^{-1}(x^{-1})^{-1} gx^{-1} \in G'$

$(g^{-1}x)(gx^{-1}) \in G'$

$g^{-1}(xgx^{-1}) \in G'$

$g(g^{-1}(xgx^{-1})) \in G'$

$\Rightarrow xgx^{-1} \in G'$

Thus G' is a normal subgp of G.

(ii) Let $a, b \in G$ be arbitrary

$G'a$ and $G'b$ are arbitrary elt. of G/G'.

Since G' is normal in G,

$G'a = aG'$

$G'ab = (G'a)(G'b)$

By def, $a, b \in G \Rightarrow a^{-1}b^{-1}ab \in G'$

$(ba)^{-1}ab \in G'$

$G'(ba) = G'(ab)$

$(G'b)(G'a) = (G'a)(G'b)$

Thus G/G' is abelian

(iii) Let G/K be abelian

We shall show that $G' \subset K$

Let $Ka, Kb \in G/K$ be arbitrary

Since G/K is abelian,

$KaKb = KbKa \quad \forall a, b \in G$

$Kab = Kba$

$(ab)(ba^{-1}) \in K$

$aba^{-1}b^{-1} \in K$.

$(a^{-1})^{-1}(b^{-1})^{-1}a^{-1}b^{-1} \in K$

$T \subseteq K$.

$\therefore$ K is a subgroup of G containing T

But G' is the smallest subgp of G containing T

Hence $G' \subseteq K$.

Hence the proof.

Chapter - 4
Permutation groups.

Def: **Permutation :-** Let S be a non-empty set. Then a one one onto fn f from S onto itself is called a permutation on S.

If the set S is finite and contains n elements, then f is a permutation of degree n.

e.g Let $S = (1,2,3)$ & $f : S \to S$ defined as $f(1) = 2$, $f(2) = 1$, $f(3) = 3$

then $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Def: **Equality of permutations :-** Two permutation f and g of degree n are said to be equal permutation if $f(a) = g(a)$ $\forall$ $a \in S$.

e.g Let $S = \{1,2,3,4\}$

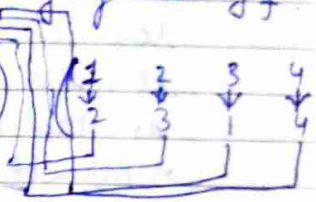
and $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ & $g = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

If S is a finite set having n distinct elements, then these n elements of S can be arranged in $n!$ ways.

Def: **Product (Composition) of two permutations**

Let f, g be two permutation defined on the same set S. Then their composition fog is obtained by first carrying out the operation defined by g then by f

$$fog = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$



$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Def: **Identity permutation :-** Let $I : S \to S$ be one to one mapping s.t $I(x) = x$ $\forall x \in S$ Then I is called identity permutation.

Thus $f \cdot I = I \cdot f = f$ $\forall$ $f \in P_n$.

Def: **Inverse of a permutation :-** A permutation g is said to be inverse of a permutation f if fog and gof are identity permutation.

Usually inverse of f denoted by f^{-1} and $ff^{-1} = f^{-1}f = I$ $\forall$ $f \in P_n$.

e.g $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

then $f^{-1} = \begin{pmatrix} 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Def: **Cyclic permutation:-** Let S be the set having n elements and f be a permutation which arranges 'm' elements of S in a row in such a way that f-image of each elt. in the row is the element which follows it; the f image of the last element is the first element and the remaining $(n-m)$ elt. of S remain unchanged. Then f is called cyclic permutation of length m.

e.g $f = \begin{pmatrix} 1 & 2 & 4 & 3 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

$\therefore$ $1 \to 2 \to 4 \to 3 \to 1$ & $5 \to 5, 6 \to 6$

So the cycle is $(1\,2\,4\,3)$ and $5, 6$ remains unchanged.

Def: **Inverse of cyclic permutation:-** If $(a_1, a_2, a_3 \ldots, a_n)$ is a cyclic permutation then its inverse is denoted by

$$(a_1, a_2, \ldots a_n)^{-1} = (a_n a_{n-1} \ldots a_2 a_1)$$

Def: **Inverse of the product of cyclic permutation:-** If f and g are two cyclic permutations, then

$$(fg)^{-1} = g^{-1} f^{-1}$$

Def:- **Transposition:-** A cyclic of length two is called a transposition

e.g $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ = transposition $(1,3)$

Ⓐ A cyclic of length one represents the identity permutation

Def:- **Disjoint cycles:-** Two cycles are disjoint if they have no common elements in their one rowed representation

e.g $(1\,3\,4)$ and $(2\,5\,7)$ are disjoint cycles

Theorem:- Every permutation can be expressed as the product of disjoint cycles.

Proof:- Let f be the permutation defined on S as

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & & b_n \end{pmatrix} \text{ where } b_i = a_j$$

First select all those a_i where $a_i = b_i$. These are the cycles of length 'one'. Now if $a_1 \neq b_1$ i.e a_1 has image b_1, then find image of b_1 which is b_2 (say) If $b_2 = a_1$, then the cycle is (a_1, b_1) If $b_2 \neq a_1$, then find image of b_2 which is b_3 (say). If $b_3 = a_1$, then cycle is (a_1, b_1, b_2). If $b_3 \neq a_1$), then proceeding in the same manner. Thus we obtain disjoint cycles and the product

Def:- Cyclic permutation:- Let S be the set having n elements and f be a permutation which arranges 'm' elements of S in a row in such a way that f-image of each elt. in the row is the element which follows it; the f image of the last element is the first element and the remaining $(n-m)$ elt. of S remain unchanged. Then f is called cyclic permutation of length m.

e.g $f = \begin{pmatrix} 1 & 2 & 4 & 3 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

$\therefore 1 \to 2 \to 4 \to 3 \to 1$ & $5 \to 5, 6 \to 6$

So the cycle is $(1\,2\,4\,3)$ and 5, 6 remains unchanged.

Def:- Inverse of cyclic permutation:- If $(a_1, a_2, a_3 \ldots, a_n)$ is a cyclic permutation then its inverse is denoted by

$(a_1, a_2, \ldots a_n)^{-1} = (a_n a_{n-1} \ldots a_2 a_1)$

Def:- Inverse of the product of cyclic permutation:- If f and g are two cyclic permutations, then

$(fg)^{-1} = g^{-1} f^{-1}$

Def:- Transposition:- A cyclic of length two is called a transposition

e.g $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ = transposition $(1,3)$

⊛ A cyclic of length one represents the identity permutation.

Def:- Disjoint cycles:- Two cycles are disjoint if they have no common elements in their one rowed representation

e.g $(1\,3\,4)$ and $(2\,5\,7)$ are disjoint cycles.

Theorem:- Every permutation can be expressed as the product of disjoint cycles.

Proof:- Let f be the permutation defined on S as

$f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & & b_n \end{pmatrix}$ where $b_i = a_j$

First select all those a_i where $a_i = b_i$. These are the cycles of length 'one'. Now if $a_1 \neq b_1$ i.e a_1 has image b_1, then find image of b_1 which is b_2 (say) If $b_2 = a_1$, then the cycle is (a_1, b_1) If $b_2 \neq a_1$, then find image of b_2 which is b_3 (say). If $b_3 = a_1$, then cycle is (a_1, b_1, b_2). If $b_3 \neq a_1$, then proceeding in the same manner. Thus we obtain disjoint cycles and the product

of all these disjoint cycles.

Def:- Even and odd permutation :- A permutation is said to be an even permutation if it can be expressed as a product of even no. of transposition.

If the no. of transposition is odd, then it is called odd permutation.

Properties of Even and odd permutation:-

(i) Any permutation is either even or odd i.e it cannot be expressed as even in one way and odd in another way.

(ii) A cycle of length n can be expressed as the product of n-1 transpositions. Therefore a cycle of length n will be an even permutation if n is odd and odd permutation if n is even.

(iii) Identity permutation is always an even permutation

(iv) Product of even permutation will always be even.

(v) Product of two odd permutations is always an even permutation.

(vi) Product of an even and odd permutation is always an odd permutation.

(vii) Inverse of even permutation is even and that of odd permutation is odd.

(viii) From the total n! permutation on n symbols, half are even and half are odd.

Cayley Theorem:-

Statement:- Every group is isomorphic to a permutation group.

Proof:- Let $(G, \cdot)$ be the group s.t $a, x \in G$

$\Rightarrow ax \in G$.

Consider the function $f_a : G \to G$ defined by $f_a(x) = ax \ \forall \ x \in G$

f_a is one one:-

let $f_a(x) = f_a(y) \Rightarrow ax = ay$

$\Rightarrow x = y$

Thus function f_a is one-one.

f_a is onto:- For every $x \in G$, there exists $a^{-1}x \in G$ s.t

$f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x$

Hence f_a is onto.

$\Rightarrow$ f_a is a permutation on G.

Consider $G' = \{f_a : a \in G$ and f_a is a permutation on $a\}$.

To prove G' is a group

Closure law:- Let $f_a, f_b \in G'$

$\therefore f_a(x) = ax \ \forall \ x \in G$

$f_b(x) = bx \ \forall\ x \in G$

$\therefore (f_a f_b)x = f_a[f_b(x)] = f_a(bx)$
$= abx = f_{ab}(x)$

$\Rightarrow f_a \cdot f_b = f_{ab}$

As $ab \in G \Rightarrow f_{ab} \in G' \Rightarrow f_a f_b \in G'$

Hence G' is closed w.r.t '.'.

Associative law:- Let $f_a, f_b, f_c \in G'$ where $a, b, c \in G$,

$f_a(f_b \cdot f_c)x = f_a(f_{bc})x = f_{abc}(x)$
$= abcx$
$= f_{ab}(cx) = f_{ab}(f_c x) = (f_a \cdot f_b) f_c x.$

$\therefore$ Associative law is satisfied.

Existence of identity:- If e is identity of G, then $ea = ae = a \ \forall\ a \in G$.

for $f_e \in G'$ $f_e f_a = f_{ea} = f_a \ \forall\ f_a \in G'$

$\Rightarrow f_e f_a = f_a = f_a f_e$.

$\therefore f_e$ is the identity of G'.

Existence of inverse:- Let a^{-1} be the inverse of a in G.

$\therefore f_{a^{-1}} \in G$.

$a^{-1}a = e = aa^{-1}$

$f_{a^{-1}} f_a = f_{a^{-1}a} = f_e = f_{aa^{-1}} = f_a f_{a^{-1}}$

Hence $f_{a^{-1}}$ is the inverse of f_a.

Thus G' is a group.

Consider a mapping $\phi : G \to G'$ s.t $\phi(a) = f_a \ \forall\ a \in G$.

ϕ is one one:-

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

$\Rightarrow f_a = f_b \Rightarrow a = b$.

Hence ϕ is one to one

ϕ is onto:-

For each $f_a \in G'$, $\exists\ a \in G$ s.t $\phi(a) = f_a$

Hence ϕ is onto.

ϕ is homomorphism:-

$\phi(ab) = f_{ab} = f_a \cdot f_b = \phi(a)\phi(b)$

$\therefore$ ϕ is homomorphism.

Hence ϕ is an isomorphism between G & G'

This proves the result.

Chapter - 5
Rings and fields

Def:- Ring:→ A non empty set R equipped with two binary operations called addition and multiplication denoted by (+) and (·) is said to form a ring if the following properties are satisfied:

1) R is closed w.r.t +,
i.e $a, b \in R$ then $a+b \in R$.
2) R is associative w.r.t +.
$(a+b)+c = a+(b+c)$ $\forall$ $a, b, c \in R$
3) Addition is commutative
i.e $a+b = b+a$ $\forall$ $a, b, c \in R$.
4) Existence of additive identity
$0+a = a+0 = a$ $\forall$ $a \in R$.
5) Existence of inverse
$-a+a = 0 = a+(-a)$
6) R is closed w.r.t '·'.
i.e if $a, b \in R$ then $a \cdot b \in R$
7) Multiplication is associative
i.e $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\forall$ $a, b, c \in R$
8) Multiplication is distributive w.r.t '+'
$a \cdot (b+c) = a \cdot b + a \cdot c$
$(b+c) \cdot a = b \cdot a + c \cdot a$.

Types of rings:-

1) **Commutative ring:-** A ring in which $a \cdot b = b \cdot a$ $\forall$ $a, b \in R$ is called commutative ring.
2. **Ring with unity:-** If in a ring, there exists an element denoted by 1 s.t $1 \cdot a = a \cdot 1$ $\forall$ $a \in R$, then R is called a ring with unit element.
3. **Null ring or zero ring:-** The set R consisting of a single element 0 with two binary operation defined by $0+0=0$ and $0 \cdot 0 = 0$ is a ring.

Def:- Rings without or with zero divisors:-
A ring $(R, +, \cdot)$ is said to be without zero divisors if $\forall$ $a, b \in R$.
$a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$.
On the other hand, if in a ring R there exists non zero elements a and b s.t $a \cdot b = 0$, then R is said to be a ring with zero divisors.

Ex The ring $\{0, 1, 2, 3, 4, 5\}, +_6, \times_6\}$ is a ring with zero divisors.

Def:- Integral domain:- A commutative ring which has unit element and is without zero divisors is called an integral domain. e.g. $(Z, +, \cdot)$, $(Q, +, \cdot)$

Def:- Division ring or a skew field:- A ring is said to be a division ring or a skew field if its non zero elements forms a group under '×'.

Def:- Field:- A field is a commutative division ring

or

A field has eleven properties, five under addition, five under multiplication & distributive law.

Theorem:- Every field is an integral domain.

Proof:- Field F is a commutative ring with unity. Therefore to prove that every field is an integral domain, we have to show that every field ~~is an integral domain~~, has no zero divisors.

i.e $\forall\ a, b \in F,\ a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

Suppose $a \neq 0$ so that a^{-1} exists

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

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

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow b = 0$.

Similarly, if $b \neq 0$ and $ab = 0$ then $a = 0$

Therefore in a field $ab = 0 \Rightarrow a = 0$ or $b = 0$

Thus, a field has no zero divisors.

Hence, every field is an integral domain.

Theorem:- Every finite non zero integral domain is a field.

Proof:- Let F be a finite non zero integral domain having n elts $a_1, a_2, \ldots, a_n$

This implies that F is a commutative ring without zero divisors.

We shall prove that F is a field i.e F is a ring with unity and every non-zero element of F has a multiplicative inverse.

Consider any non zero elt $a \in F$. Then $aa_1, aa_2, \ldots, aa_n$ are all in F.

If possible, let us assume $aa_i = aa_j, i \neq j$

$\Rightarrow aa_i - aa_j = 0$

$\Rightarrow a(a_i - a_j) = 0$

$\Rightarrow$ either $a = 0$ or $a_i - a_j = 0$

$\Rightarrow a_i - a_j = 0$

$\Rightarrow a_i = a_j \Rightarrow i = j$ which is not true

$\Rightarrow aa_i \neq aa_j$ for $i \neq j$

Thus $aa_1, aa_2, \ldots, aa_n$ are distinct elts of F.

Since $a \in F$, $a = aa_i$ for some i

$\Rightarrow a = aa_i = a_i a$

Now, we shall show that a_i is the multiplicative identity of F.

Let $b \in F$ be any arbitrary element.

Now $ab = (aa_i)b$

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

$\Rightarrow$ $b - a_i b = 0$

$\Rightarrow$ $b = a_i b = b a_i$

$\Rightarrow$ a_i is the multiplicative identity of F.
Let $a_i = 1$. Then $1 \in F$ & so F is a ring with unity.
Thus $1 = a a_r = a_r a$ for some r.

$\Rightarrow$ a_r is multiplicative inverse of nonzero element $a \in F$.

$\therefore$ Every non zero element of F has multiplicative inverse.
Hence F is a field.
Hence the proof.

Def:- Subrings:- If R is a ring under two binary composition and S is a non empty subset of R s.t S itself is a ring under the same binary operations, then S is called subring of R.

e.g Z is a subring of the ring $(Q, +, \cdot)$

Theorem: The necessary and sufficient condition for a non empty subset of the ring R to be a subring of R are
(i) $S + (-S) = S$ & (ii) $SS \subseteq S$.

Proof:- Conditions are necessary:
Suppose $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$
Let $x \in S + (-S)$ be arbitrary

$x = a + (-b)$ for some $a, b \in S$
$= a - b \in S$
$S + (-S) \subseteq S$ — ①
Also if $y \in S$ is arbitrary, then
$y = y + 0 = y + (-0)$
$= S + (-S)$
$S \subseteq S + (-S)$ — ②
From ① & ②, we get $S + (-S) = S$.
Again, let $x \in SS$ be arbitrary,
$x = ab$ for some $a, b \in S$
Since R being a ring is closed w.r.t 'x'
$ab \in S \Rightarrow x \in S$
$\therefore x \in SS \Rightarrow x \in S$
$SS \subseteq S$.

Conditions are sufficient :-
Suppose S is a non empty subset of R s.t (i) $S + (-S) = S$ & $SS \subseteq S$
We have to prove that S is a subring of R.
Let $a, b \in S$
$a + (-b) \in S + (-S)$
$a + (-b) \in S$.
$SS \subseteq S \Rightarrow ab \in S \ \forall \ a, b \in S$
Therefore, S satisfies both the condition to be a subring of R.
Hence the proof.

Theorem:- Prove that the intersection of Two Subrings is a subring.

Proof:- Let S_1 and S_2 be two subrings of R. As additive identity 0 is common elt. of S_1 and S_2

$\therefore S_1 \cap S_2 \neq \phi$.

To show that $S_1 \cap S_2$ is a subring, it is sufficient to prove that

(i) $a, b \in S_1 \cap S_2 \Rightarrow a-b \in S_1 \cap S_2$

(ii) $a, b \in S_1 \cap S_2 \Rightarrow a \cdot b \in S_1 \cap S_2$

Let a, b be any two elts of $S_1 \cap S_2$

$\therefore a, b \in S_1$ and $a, b \in S_2$

Since S_1 and S_2 are subrings

$\therefore a-b \in S_1$ and $a-b \in S_2$

$a \cdot b \in S_1$ and $a \cdot b \in S_2$

$\Rightarrow a-b \in S_1 \cap S_2$ & $a \cdot b \in S_1 \cap S_2$

Hence $S_1 \cap S_2$ is a subring of R.

Def:- **Centre of a ring:-** Let R be a ring. The set of all those elts of R which commute with every elt. of the ring is called centre of a ring R and is denoted by Z(R). Thus,

$Z(R) = \{r \in R : rx = xr \ \forall \ x \in R\}$.

Def:- **Characteristic of a ring:-** Let R be a ring with additive identity 0 and let there exist a positive integer n s.t $an = 0$ or $na = 0 \ \forall \ a \in R$. The smallest of all such n is called characteristic of the ring R.

If there exist no such positive integer, then the characteristic of R is either zero or infinite.

Theorem:- The order of each non zero element of an integral domain is same.

Proof:- Let R be the integral domain & a be any non zero elt of R. Let n be the order of a as an element of the group (R, +). Let b be any other non-zero elt. of R.

Case I:- When $n = 0$.

$\therefore$ There does not exist any +ve integer K s.t $ka = 0$.

If possible let $o(b) = m$ & $m > 0$.

$\therefore mb = 0$

$\Rightarrow a(mb) = 0$

$\Rightarrow a(b+b+\ldots \text{ m times}) = 0$

$\Rightarrow ab+ab+\ldots+ \text{m times} = 0$

$\Rightarrow (a+a+a\ldots+\underset{\text{m times}}{a})b = 0$

$\Rightarrow (ma)b = 0$

$\Rightarrow ma = 0$

$\Rightarrow$ Order of a is not-zero.

which is a contradiction and hence our supposition is wrong. Therefore $o(b) = o(a) = 0$

Case II:- When $n > 0$

$na = 0$

$\Rightarrow (na)b = 0$

$\Rightarrow (a+a+\text{---}\ n \text{ times})b = 0$

$\Rightarrow ab+ab+\text{---}\ n \text{ times} = 0$

$\Rightarrow a(b+b+\text{---}\ n \text{ times}) = 0$

$\Rightarrow a(nb) = 0$

$nb = 0$

$O(b) \leq n$.

Suppose that $O(b) = m < n$.

$mb = 0$

$\Rightarrow a(mb) = 0$

$\Rightarrow a(b+b+\text{---}\ m \text{ times}) = 0$

$\Rightarrow ab+ab+\text{---}\ m \text{ times} = 0$

$\Rightarrow (a+a+\text{---}\ m \text{ times})b = 0$

$\Rightarrow (ma)b = 0$

$\Rightarrow ma = 0$

$\Rightarrow O(a) \leq m$.

$\Rightarrow n \leq m$ which is impossible

$\therefore O(b) = n = O(a)$

Hence the proof.

Theorem- Prove that characteristic of an integral domain is either zero or a prime number.

Proof:- Let R be integral domain & a be any non zero elt of R.

If order of $a = 0$, then characteristic of R is 0 and the result is proved.

Now let $O(a) = p$, $p \neq 0$

∴ characteristic of R is p

We shall prove that p is prime.

If possible, let p be a composite number

$\Rightarrow p = p_1 p_2$, $0 \leq p_1, p_2 < p$

Since R is integral domain & $a \neq 0$

$a^2 = a.a \neq 0$

Now a^2 is non zero member of R.

$O(a^2) = p$

$\Rightarrow pa^2 = 0$

$\Rightarrow (p_1 p_2)a^2 = 0$

$\Rightarrow (p_1 a)(p_2 a) = 0$

$\Rightarrow$ either $p_1 a = 0$ or $p_2 a = 0$

But $O(a) = p \Rightarrow$ either $p_1 > p$ or $p_2 > p$ which is a contradiction.

Thus our assumption that p is composite is wrong

So p must be a prime no.

Hence the proof.

Chapter - 6
Ideals and quotient rings

Def:- Ideal:-
A non empty subset S of a ring R is said to be an ideal of R if
(i) $a, b \in S \Rightarrow a-b \in S$
& (ii) $ar \in S$ & $ra \in S$ $\forall$ $a \in S$ & $r \in R$

(*) In every ring R, the ideals $\{0\}$ and R are called improper ideals. Any ideal except these two is called a proper ideal.

(*) The ideal $\{0\}$ and R are called null ideal and unit ideal of R respectively.

Sum of two ideals:-

Theorem:- Let S_1 and S_2 be two ideals of a ring R. Let $S_1+S_2 = \{a_1+a_2 : a_1 \in S_1 \& a_2 \in S_2\}$. Then S_1+S_2 is called sum of ideals S_1 and S_2 and is an ideal of R.

Proof:- $S_1+S_2 \neq \phi$ as $0+0=0 \in S_1+S_2$
Also as S_1 and S_2 are ideals of ring R therefore
1) S_1 and S_2 are subgps of R w.r.t '+'
2) $r \in R$, $a_1 \in S_1 \Rightarrow ra_1$ and $a_1 r \in S_1$

and $r \in R$, $a_2 \in S_2 \Rightarrow ra_2$ and $a_2 r \in S_2$
3) S_1+S_2 is additive subgp of R
For $a_1+a_2 \in S_1+S_2$, $b_1+b_2 \in S_1+S_2$
$\Rightarrow$ $a_1 \in S_1$, $a_2 \in S_2$, $b_1 \in S_1$, $b_2 \in S_2$
$\Rightarrow$ $a_1, b_1 \in S_1$ and $a_2, b_2 \in S_2$
$\Rightarrow$ $a_1-b_1 \in S_1$ and $a_2-b_2 \in S_2$
$\Rightarrow$ $(a_1-b_1)+(a_2-b_2) \in S_1+S_2$
$\Rightarrow$ $(a_1+a_2)-(b_1+b_2) \in S_1+S_2$

Since $\langle R, + \rangle$ is an abelian group
$\therefore$ $a_1+a_2, b_1+b_2 \in S_1+S_2 \Rightarrow (a_1+a_2)-(b_1+b_2) \in S_1+S_2$

4) $r \in R$, $a_1+a_2 \in S_1+S_2$
$\Rightarrow$ $r(a_1+a_2)$ & $(a_1+a_2)r \in S_1+S_2$
For $r \in R$, $a_1+a_2 \in S_1+S_2$
$\Rightarrow$ $r \in R$, $a_1 \in S_1$, $a_2 \in S_2$
$\Rightarrow$ $r \in R$, $a_1 \in S_1$ & $r \in R$, $a_2 \in S_2$
$ra_1, a_1 r \in S_1$ and $ra_2, a_2 r \in S_2$
$\Rightarrow$ $ra_1+ra_2 \in S_1+S_2$ & $a_1 r+a_2 r \in S_1+S_2$
$\Rightarrow$ $r(a_1+a_2) \in S_1+S_2$ & $(a_1+a_2)r \in S_1+S_2$
Thus S_1+S_2 is an ideal of R.

Cor S_1 is an ideal of S_1+S_2
For $a_1, b_1 \in S_1 \Rightarrow a_1-b_1 \in S_1$
Also if $a \in S_1$ and $s \in S_1+S_2$
$s = a_1+a_2$
Now as $as = a(a_1+a_2) = aa_1+aa_2$
Since $a, a_1 \in S_1 \Rightarrow aa_1 \in S_1$ & $a \in S_1, a_2 \in S_2 \subseteq R$
$\Rightarrow aa_2 \in S_1$

$as \in S_1$

IIly $\&a \in S_1$

Thus S_1 is an ideal of $S_1 + S_2$

Hence the proof.

Def:- **Ideal generated by a set** :- Let R be a ring and S be any subset of R. An ideal A of R is said to be generated by S if

(I) $S \subseteq A$

(II) $S \subseteq I$ where I is any ideal of R. Then $A \subseteq I$

$A = \langle S \rangle$

Def:- **Product of two ideals** :- If S_1 and S_2 are two ideals of a ring R, then the product S_1S_2 of S_1 and S_2 as

$$S_1S_2 = \sum_{i=1}^{n} a_ib_i : a_i \in S_1, b_i \in S_2$$

Theorem:- If S_1, S_2 are two ideals of a ring R, then their product S_1S_2 is an ideal of R.

Proof:- $S_1S_2 \neq \phi$ as $0 = 0.0 \in S_1S_2$

Also as S_1, S_2 are ideals of a ring R, therefore

1) S_1 and S_2 are subgp of R w.r.t '+'
2) $r \in R, a_1 \in S_1 \Rightarrow ra_1$ and $a_1r \in S_1$ and $r \in R, b_1 \in S_2 \Rightarrow rb_1$ and $b_1r \in S_2$

let $S = S_1S_2$ and $x, y \in S$ be arbitrary

$x = a_1b_1 + a_2b_2 + \dots + a_mb_m$

$y = a_1'b_1' + a_2'b_2' + \dots + a_n'b_n'$

where $a_i, a_j' \in S_1$ and $b_i, b_j' \in S_2$

To prove that S is an additive subgp of R, we show that $x, y \in S \Rightarrow x - y \in S$

Now, $x - y = (a_1b_1 + \dots + a_mb_m) - (a_1'b_1' + \dots + a_n'b_n')$

$= a_1b_1 + \dots + a_mb_m + (-a_1')b_1' + \dots + (-a_n')b_n'$

By condition I,

$a_1', a_2', \dots a_n' \in S_1 \Rightarrow -a_1', -a_2', \dots, -a_n' \in S_1$

Also $b_1, b_2, \dots, b_m, b_1', b_2', \dots, b_n' \in S_2$

$x - y \in \alpha_1\beta_1 + \alpha_2\beta_2 + \dots + \alpha_k\beta_k$ (say)

where $\alpha_1, \alpha_2, \dots, \alpha_k \in S_1$; $\beta_1, \beta_2, \dots \beta_k \in S_2$

and $k = m+n$

Thus $x - y \in S_1S_2$

We shall now show that $r \in R, x \in S$

rx and $xr \in S$

$rx = r(a_1b_1 + a_2b_2 + \dots + a_mb_m)$

$= (ra_1)b_1 + (ra_2)b_2 + \dots + (ra_m)b_m$

By condition II, $r \in R$ and

$a_1, a_2, \dots, a_m \in S_1 \Rightarrow ra_1, ra_2, \dots, ra_m \in S_1$

Also, $b_1, b_2, \dots, b_m \in S_2$

$\Rightarrow rx \in S_1S_2$

IIly $xr = (a_1b_1 + a_2b_2 + \dots + a_mb_m)r$

$= a_1(b_1r) + a_2(b_2r) + \dots + a_m(b_mr)$

$r \in R$ & $b_1, b_2, \dots, b_m \in S_2$

$\Rightarrow b_1r, b_2r, \dots, b_mr \in S_2$

Also $a_1, a_2, \dots, a_m \in S_1$

$xr \in S_1S_2$

$\Rightarrow$ $S_1 S_2$ is an ideal of R

Hence the proof.

Def: Simple ring :- A division ring is a simple ring.

Theorem: A division ring is a simple ring.

Proof: Let R be a division ring i.e a ring whose non zero elements form a group w.r.t '$\cdot$'.

Let S be an arbitrary ideal of R.

If $S = \{0\}$, then the theorem is proved.

Let us take $S \neq \{0\}$.

Then there exist atleast one $a \in S$ s.t $a \neq 0$

Since $S \subset R$, so $a \in R$ and R being a division ring $\Rightarrow a^{-1} \in R$

Now $a \in S$, $a^{-1} \in R \Rightarrow a^{-1} a \in S$

$\Rightarrow 1 \in S$

Also $r \in R \Rightarrow r \in R, 1 \in S$

$\Rightarrow 1 \cdot r \in S$

$\Rightarrow r \in S$

$\Rightarrow R \subset S$.

But $S \subset R$

Thus, we have $S = R$

$\therefore$ R can have only ideals R and $\{0\}$ and hence R is a simple ring.

Hence the proof.

Some Imp. definitions.

Def: Annihilator of a set :- Let R be a ring and $S \subseteq R$. Then the annihilator of set S is defined as

$r(S)$ or $l(S) = \{r \in R : ra, ar = 0 \ \forall a \in S\}$

Def: Principal ideal :- Let R be a ring. An ideal S of R is called a principal ideal if there exist an elt $a \in S$ s.t S contains multiples of the element a i.e if S is generated by a single elt. of R.

i.e $S = \langle a \rangle$.

Def: Unity ideal :- If R is a ring with unity elt e, then principal ideal generated by e is the whole ring R. The ring R is called unity ideal.

Def: Zero ideal :- If R is a ring with unit element, then the principal ideal generated by 0 is ~~the~~ called Zero ideal.

Def: Principal ideal ring and principal ideal domain :- Let R be a ring without zero divisors and with unity element. Then R is said to be a principal ideal ring if every ideal S in R is a principal

ideal.

An integral domain R with unit element is called P.I.D if every ideal of R is a principal ideal.

Theorem: The ring of integers is a principal ideal ring.

Proof: Let $\langle Z, +, \cdot \rangle$ be the ring of integers. To prove that Z is a principal ideal ring, we shall show that if S is any ideal of Z, then S is a principal ideal of Z.

If $S = \{0\}$ i.e a null ideal, then obviously S is a principal ideal.

Let us take $S \neq \{0\}$.

∴ There exist atleast one non zero integer $a \in S$

Since $\langle S, + \rangle$ is a subgp of Z

∴ $a \in S \Rightarrow -a \in S$.

$\Rightarrow$ S contains atleast one +ve integer

W.K.T $S_+ = \{s \in S : s \text{ is a +ve integer}\}$.

Since every set of positive elements has a least member, let b be this element.

We claim $S = \langle b \rangle$. i.e S is a principal ideal generated by b.

Let $s \in S$ be arbitrary.

∴ By division algorithm, there exist integers q and r s.t $s = bq + r$, $0 \leq r < b$

Now, $b \in S$, $q \in Z \Rightarrow bq \in S$.

Also $s \in S$, $bq \in S \Rightarrow s \in S, -bq \in S$.

$\Rightarrow s - bq \in S$

$\Rightarrow r \in S$

But $0 \leq r < b$ and b is the least +ve belonging to S

∴ r must be 0 and so $s = bq$.

Thus we have shown that every element $s \in S$ can be expressed as $s = bq$ for some $q \in Z$

i.e $S = \{bq : q \in Z\} = \langle b \rangle$.

Since S is an ideal of Z generated by a single element b i.e S is a principal ideal. Hence ring of integers is a principal ideal ring.

Hence the proof.

Theorem: A field has no proper ideals.

Proof: Let F be a field and S be an arbitrary ideal of F.

If $S = \{0\}$, then there is nothing to prove.

Let us consider $S \neq \{0\}$

∴ There exist atleast one element $0 \neq a \in S$.

Since $S \subset F$, therefore $a \in F \Rightarrow a^{-1} \in F$

Now $a \in S$, $a^{-1} \in F \Rightarrow a^{-1}a \in S$

$\Rightarrow 1 \in S$.

Let $x \in F$ be arbitrary

Then $1 \in S, x \in F \Rightarrow 1.x \in S$

$\Rightarrow x \in S$

i.e. $x \in F \Rightarrow x \in S$

$F \subset S$

But $S \subseteq F$

$\therefore S = F$

Thus $\{0\}$ and F are the only ideals of F and so a field F has no proper ideals. Hence the proof.

Def:- **Maximal ideal:-** An ideal S of a ring R is called maximal if

(i) $S \neq R$ i.e S is properly contained in R.

(ii) For any ideal $S' \supseteq S$ either $S' = S$ or $S' = R$.

(*) A field F has only two ideals F and $\{0\}$ and $\{0\}$ is the only maximal ideal of F.

Def:- **Prime ideal:-** An ideal S of a ring R is called a prime ideal if S_1 and S_2 are ideals of R s.t $S_1 S_2 \subset S$ then $S_1 \subseteq S$ or $S_2 \subseteq S$.

Alternatively, an ideal S of a ring R is called a prime ideal of R if $ab \in S \Rightarrow a \in S$ or $b \in S$.

Def:- **Semiprime ideal:-** An ideal S of a commutative ring is called a semi-prime ideal if $a^2 \in S \Rightarrow a \in S \ \forall a \in R$.

Theorem: An ideal of a ring of integers is maximal iff it is generated by some prime integer.

Proof:- Let $\langle Z, +, \cdot \rangle$ be a ring of integers and S be an ideal of Z.

We know that Z is a principal ideal ring.

$\Rightarrow$ S is a principal ideal and so can be generated by a single integer, say p.

Since ideal generated by p and -p are same. Take $S = \langle p \rangle$ where p is a +ve integer.

Let p is a prime no and S' be an ideal of Z s.t $S \subset S' \subset Z$

Since Z is a principal ideal ring.

$\therefore S' = \langle q \rangle$ say where q is a +ve.

Now $S \subset S'$

$\Rightarrow \langle p \rangle \subset \langle q \rangle$

$\Rightarrow p \in \langle q \rangle$

$\Rightarrow p \in \{qm : m \in Z\}$

$\Rightarrow p = qn$ for some int. $n \in Z$.

Since p is prime, therefore either $n = 1$ or $n = p$.

$\Rightarrow$ either $q=p$ or $q=1$

$\Rightarrow$ $\langle q\rangle = \langle p\rangle$ or $\langle q\rangle = \langle 1\rangle$

$\Rightarrow$ $S' = S$ or $S' = Z$

Thus $S \subset S' \subset Z$

$\Rightarrow$ $S = S'$ or $S' = Z$

Hence S is maximal.

Conversely, let S be maximal, then we have to show that p is prime.

If possible, let p is not a prime.

i.e p is composite, let $p = ab$.

Now $p = ab \Rightarrow \langle p\rangle \subset \langle a\rangle \subset \langle 1\rangle = Z$

$\langle p\rangle \subset \langle b\rangle \subset \langle 1\rangle = Z$

$\Rightarrow S \subset \langle a\rangle \subset Z$.

Since S is maximal, therefore

$\langle a\rangle = S$ or $\langle a\rangle = Z$

If $\langle a\rangle = Z \Rightarrow \langle a\rangle = \langle 1\rangle$

$\Rightarrow a = 1$

which is a contradiction.

otherwise, if $\langle a\rangle = S \Rightarrow \langle a\rangle = \langle p\rangle$

$\Rightarrow \langle a\rangle = \{pm : m \in Z\}$

$\Rightarrow a = pn$ some n.

Also $p = ab \Rightarrow a = abn \Rightarrow bn = 1$

Since b and n are both integers

$\therefore b = 1$ and $n = 1$

i.e $b = 1$ which is a contradiction

Hence p can not be composite and is a prime.

Hence the proof.

Def:- Co-maximal ideals:- Two ideals S and T of any ring R are said to be co-maximal if $S + T = R$.

Def:- Nilpotent ideal:- Let S be an ideal of a ring R. Then S is said to be nilpotent if for some +ve integer $S^n = \langle 0\rangle$.

Def:- Nil ideal:- An ideal S of a ring R is said to be a nil ideal if each element of S is nilpotent i.e for each $a \in S$, there exist a +ve int n s.t $a^n = 0$.

Ex:- Find the principal ideal generated by 3, in the ring of integers.

Sol:- The ring of integers is a commutative ring with unity.

Thus principal ideal generated by

$3 = \langle 3\rangle = \{3m : m \in Z\}$

$= \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

Def:- Quotient Rings:- Let R/S denote the family of cosets of S in R.

i.e $R/S = \{S + a : a \in R\}$.

R/S forms a group under '+' defined by

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

R/s forms a group defined by $(s+a)(s+b) = s+ab$.

Theorem:- An ideal S of a commutative ring R with unity is maximal iff R/s is a field.

Proof:- Let the ideal S be maximal. Since R is a commutative ring with unity, R/s is also a commutative ring with unity.
Let $S+a \in R/s$ be any non zero element.
Then to show that R/s is a field, then to show that $(S+a)$ is invertible and $(s+a)^{-1} \in R/s$.
Now $S+a \in R/s$
$\Rightarrow S+a \neq S \Rightarrow a \notin S$
Let $aR = \{ar : r \in R\}$
Here $aR = \langle a \rangle$ is principal ideal of R generated by a
Since sum of two ideals is an ideal, $S+aR$ will be an ideal of R.
Also $a = 0+a\cdot 1 \in S+aR$ and $a \notin S$
$\therefore S \subset S+aR \subseteq R$
S is maximal $\Rightarrow S+aR = R$
$\because 1 \in R \Rightarrow 1 \in S+aR$
$\Rightarrow 1 = s+ar$ for $s \in S, r \in R$
$\Rightarrow S+1 = S+(s+ar)$
$= (S+s)+(S+ar) = S+ar$
$= (S+a)(S+r)$

$\Rightarrow S+r$ is a multiplicative inverse of $S+a$.
Thus R/s is a field.

Conversely, Let R/s be a field.
Let S' be any ideal of R s.t $S \subset S' \subseteq R$
$\therefore$ There exist $s \in S'$ s.t $s \notin S$
Now $s \notin S \Rightarrow S+s \neq S$
$\Rightarrow S+s$ is a non zero elt. of R/s
Since R/s is a field, so $S+s$ has a multiplicative inverse
Let $(S+t)$ be its inverse
$\therefore (S+s)(S+t) = S+1$
$\Rightarrow S+st = S+1$
$\Rightarrow st-1 \in S$
$\Rightarrow st-1 = s'$ for some $s' \in S$
$\Rightarrow 1 = st-s' \in S'$
Thus S' is an ideal of R with unity element.
Hence S is a maximal ideal of R.
Hence the proof.

Theorem:- Let R be a commutative ring and S is an ideal of R. Then R/s is an integral domain iff S is a prime ideal.

Proof:- Let S be a prime ideal of R
Let $(S+a)(S+b) = 0+S$
$\Rightarrow S+ab = S$
$\Rightarrow ab \in S$

$\Rightarrow a \in S$ or $b \in S$

$\Rightarrow S+a = S$ or $S+b = S$

Thus R/S is an integral domain.

Conversely, let R/S is an integral domain

let $ab \in S$ then $S+ab = S$

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

$\Rightarrow S+a = S$ or $S+b = S$

$\Rightarrow a \in S$ or $b \in S$.

$\Rightarrow S$ is a prime ideal.

Hence the proof.

Chapter - 7
Homomorphism of rings

A mapping $f : R \to R'$ is called a ring homomorphism if it satisfies the following properties:

(i) $f(a+b) = f(a) * f(b)$

(ii) $f(a \cdot b) = f(a) \circ f(b)$

Ex Show that the mapping $f : C \to C$ defined by $f(a+ib) = a-ib$ is a homomorphism.

Sol: let $a+ib, c+id \in C$ be arbitrary.

$$\therefore f[(a+ib)+(c+id)] = f[(a+c)+i(b+d)]$$
$$= (a+c) - i(b+d)$$
$$= (a-ib) + (c-id)$$
$$= f(a+ib) + f(c+id)$$

and $f[(a+ib)(c+id)] = f[(ac-bd)+i(ad+bc)]$
$$= (ac-bd) - i(ad+bc)$$
$$= (a-ib)c - id(a-ib)$$
$$= (a-ib)(c-id)$$
$$= f(a+ib)f(c+id)$$

Theorem:- Every homomorphic image of a commutative ring is commutative.

Proof:- Since R is a commutative ring

$a, b \in R \Rightarrow ab = ba$

$\Rightarrow f(ab) = f(ba)$

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

where $f(a), f(b) \in R'$
Thus R' is a commutative ring.

Def:- Kernel of a ring homomorphism:-
Let $f: R \to R'$ be a homomorphism. The kernel of f is defined as $\ker f = \{x \in R : f(x) = 0'\}$ where $0'$ is the zero elt. of R'.

Theorem:- $\ker f$ is an ideal of R.

Proof:- Let $f: R \to R'$ be a ring homomorphism and let S denote the kernel of f.
$S = \ker f = \{x \in R : f(x) = 0'\}$
Let 0 be the zero elt. of R s.t $f(0) = 0'$ where $0'$ is the zero elt of R'.
Let $a, b \in S$ be arbitrary
$f(a) = 0'$, $f(b) = 0'$
$f(a-b) = f(a + (-b))$
$= f(a) + f(-b)$
$= f(a) - f(b) = 0' - 0'$
$f(a-b) = 0'$
$a - b \in S$.
If $r \in R$ is arbitrary,
$f(ar) = f(a) f(r) = 0' f(r) = 0'$
$f(ra) = f(r) f(a) = f(r) 0' = 0'$
$\Rightarrow$ $f(ar) = 0' = f(ra)$ $\forall$ $ar, ra \in R$
$\Rightarrow$ $ar, ra \in S$.
Hence $S = \ker f$ is an ideal of R
Hence the proof.

Theorem:- Let $f: R \to R'$ be a ring homomorphism. Let S be an ideal of R. Then $f(S)$ is an ideal of $f(R)$.

Proof:- Let $f(S) = \{x \in R' : a \in S \text{ so that } x = f(a)\}$
Let 0 be the zero elt of R s.t $f(0) = 0'$.
$\therefore$ $0' \in f(S)$ and so $f(S)$ is non empty.
Let $x, y \in f(S)$ be arbitrary.
$\therefore$ There exist $a, b \in S$ s.t $x = f(a)$, $y = f(b)$
Now $x - y = f(a) - f(b) = f(a-b)$
Since $a, b \in S \Rightarrow a - b \in S$.
$f(a-b) = x - y \in f(S)$
Also if $r_1 \in f(R)$ is arbitrary, then there exist some $r \in R$ s.t $r_1 = f(r)$
Now $r_1 x = f(r) f(a) = f(ra)$
$x r_1 = f(a) f(r) = f(ar)$
Since $ra, ar \in S$
$\therefore$ $r_1 x \in f(S)$ and $x r_1 \in f(S)$
Hence $f(S)$ is an ideal of $f(R)$
Hence the proof.

Fundamental theorem of Homomorphism

Statement:- Let $f: R \to R'$ is an onto homomorphism, then R' is isomorphic to the quotient ring R/S of R where $S = \ker f$ i.e $R' \cong R/S$.

Proof:- Let $f: R \to R'$ be an onto homomorphism

Consider a mapping $\phi: R/s \to R'$ s.t
$\phi(S+a) = f(a)$ $\forall$ $a \in R$
where $S = \ker f$ is an ideal of R.
Now $S+a = S+b$
$\Rightarrow$ $a-b \in S$
$\Rightarrow$ $f(a-b) = 0'$
$\Rightarrow$ $f(a) + f(-b) = 0'$
$\Rightarrow$ $f(a) - f(b) = 0'$
$\Rightarrow$ $f(a) = f(b)$
$\Rightarrow$ $\phi(S+a) = \phi(S+b)$
$\therefore$ $S+a = S+b \Rightarrow \phi(S+a) = \phi(S+b)$
therefore ϕ is well defined.
Let $S+a, S+b \in R/s$
Then $\phi[(S+a)+(S+b)] = \phi[S+(a+b)]$
$= f(a+b)$
$= f(a)+f(b)$
$= \phi(S+a) + \phi(S+b)$
and $\phi[(S+a)(S+b)] = \phi[S+ab]$
$= f(ab)$
$= f(a)f(b)$
$= \phi(S+a)\,\phi(S+b)$
$\therefore$ ϕ is a homomorphism.
Also $\phi(S+a) = \phi(S+b)$ for $S+a, S+b \in R/s$
$\Rightarrow$ $f(a) = f(b)$
$\Rightarrow$ $f(a) - f(b) = 0'$
$\Rightarrow$ $f(a-b) = 0'$
$\Rightarrow$ $a-b \in S$
$\Rightarrow$ $S+a = S+b$

$\Rightarrow$ ϕ is one to one.
Let $a' \in R'$, then there exist some $a \in R$ s.t $f(a) = a'$
$\Rightarrow$ $\phi(S+a) = f(a) = a'$
$\Rightarrow$ ϕ is onto R'.
Thus $\phi: R/s \to R'$ is an onto homomorphism.
Hence $R/s \cong R'$ so that $R' \cong R/s$.
Hence the proof.

First theorem of Isomorphism

Statement:- Let $S \subseteq T$ be two ideals of a ring R, then $R/T \cong \frac{R/S}{T/S}$

Proof:- Consider a mapping $f: R/s \to R/T$ defined by
$f(S+a) = T+a$ $\forall$ $a \in R$.
f is well defined:- Let $S+a, S+b \in R/s$ be any two elts s.t
$S+a = S+b$
$S+(a-b) = S$
$a-b \in S \Rightarrow a-b \in T$.
$\Rightarrow$ $T+(a-b) = T$
$\Rightarrow$ $T+a = T+b$
$\Rightarrow$ $f(S+a) = f(S+b)$
Thus f is well defined.

f is a homomorphism: - let $a, b \in R$ be arbitrary

$$f[(S+a)(S+b)] = f(S+ab) = T+ab = (T+a)(T+b) = f(S+a)f(S+b)$$

Also $f[(S+a)+(S+b)] = f(S+a+b) = T+(a+b) = (T+a)+(T+b) = f(S+a)+f(S+b)$

f is onto:- for any $(T+a) \in R/T$, there exist $(S+a) \in R/S$ s.t $f(S+a) = T+a$

$\therefore$ f is onto.

From 1, 2 & 3, it follows that $f: R/S \to R/T$ is an onto homomorphism

$\therefore$ By fundamental theorem of homo

$$R/T \cong \frac{R/S}{\text{Ker} f}$$

$\text{Ker} f = \{S+r \in R/S : f(S+r) = T\}$, T is a zero elt of R/T

$= \{S+r \in R/S ; T+r = T\}$

$= \{S+r \in R/S ; r \in T\}$

$= T/S$

From (4), $R/T \cong \frac{R/S}{T/S}$.

Hence the proof

—

Second theorem of isomorphism:-

Statement:- Let S, T be two ideals of a ring R, then $(S+T)/S \cong T/(S \cap T)$

Proof:- Consider a mapping $f: T \to (S+T)/S$ defined by $f(t) = S+t \ \forall \ t \in T$

(i) f is well defined as any $t \in T$

$\Rightarrow$ $t = 0+t \in S+T$

$\Rightarrow$ $t \in S+T$

$\Rightarrow$ $S+t \in (S+T)/S$

$\Rightarrow$ $f(t) \in (S+T)/S$

(ii) f is onto, $S+x \in (S+T)/S$

$x \in S+T$

$\Rightarrow x = a+b$, $a \in S$, $b \in T$

$S+x = S+(a+b) = (S+a)+b = S+b$.

Thus $S+x = S+b = f(b)$, $b \in T$

$\therefore$ b is pre-image of $S+x$ under f

$\therefore$ f is onto.

(iii) Let $t_1, t_2 \in T$

$\therefore$ $f(t_1+t_2) = S+(t_1+t_2) = (S+t_1)+(S+t_2) = f(t_1)+f(t_2)$

and $f(t_1 t_2) = S+t_1 t_2 = (S+t_1)(S+t_2) = f(t_1) f(t_2)$

From ①, ② & ③, it follows that f is a homomorphism

$\therefore$ By fundamental theorem of homo,
$(S+T)/S \cong T/\text{Ker}f$

$\text{Ker}f = \{x \in T : f(x) = s\}$ where S is zero elt of $(S+T)/S$
$= \{x \in T : S+x = S\}$
$= \{x \in T : x \in S\}$
$= \{x : x \in T \text{ and } x \in S\}$
$= S \cap T$

Thus $\text{Ker}f = S \cap T$
Hence $(S+T)/S \cong T/(S \cap T)$
Hence the proof.

Ex Let f be a ring isomorphism of R onto R'. Show that if R is an integral domain, then so is R'.

Solution Since $f: R \to R'$ is an isomorphism
$\therefore$ For any $x, y \in R'$, there exist some $a, b \in R$ s.t
$f(a) = x$ and $f(b) = y$
Also $xy = f(a)f(b) = f(ab) = f(ba)$
$= f(b)f(a) = yx$
$\Rightarrow$ R' is also a commutative ring.
$xy = 0'$ for $x, y \in R'$
$\Rightarrow f(a)f(b) = 0'$

$\Rightarrow f(ab) = 0'$
$\Rightarrow ab = 0$
$\Rightarrow$ either $a = 0$ or $b = 0$
If $a = 0 \Rightarrow f(a) = f(0) = 0'$
and $b = 0 \Rightarrow f(b) = 0'$
$\Rightarrow x = 0'$ and $y = 0'$
Thus $xy = 0' \Rightarrow$ either $x = 0'$ or $y = 0'$
Thus we have shown that R' is a commutative ring s.t
$xy = 0' \Rightarrow$ either $x = 0'$ or $y = 0'$
Hence R' is an integral domain.
Hence the proof.

Def: Embedding of rings :- Let R and R' be two rings. If $f: R \to R'$ is a ring isomorphism, then f is called embedding mapping.

Embedded ring :- A ring R is said to be embedded in a ring R' if there exists a one-one homo. from R to R'.

Theorem: An integral domain can be embedded into a field.

Proof: Let R be an integral domain.
Let $S = R \times R' = \{(a, b) : a \in R, b \in R'\}$ where R' is the set of non zero

elements of R.
Define a relation $\sim$ on S by $(a,b) \sim (c,d)$ iff $ad = bc$.
Let $(a,b)(c,d)(g,h)$ be arbitrary elts of S.

Reflexive:- $(a,b) \sim (a,b)$

symmetric:- $(a,b) \sim (c,d)$
$(c,d) \sim (a,b)$

For $(a,b) \sim (c,d) \Rightarrow ad = bc$
$= cb = da$
$= (c,d) \sim (a,b)$

Transitive:- $(a,b) \sim (c,d), (c,d) \sim (g,h)$
$\Rightarrow (a,b) \sim (g,h)$
$\Rightarrow ad = bc, ch = dg$
$\Rightarrow adh = bch, bch = bdg$
$\Rightarrow adh = bdg$
$\Rightarrow d(ah - bg) = 0$
$\Rightarrow ah = bg$
$\Rightarrow (a,b) \sim (g,h)$

Thus $\sim$ is an equivalence relation and it partitions S into disjoint equivalence classes.

Let equivalence class of (a,b) be denoted by $\frac{a}{b}$. Let F be the set of all these equivalence classes ie

$$F = \left\{ \frac{a}{b} : (a,b) \in R \times R' \right\}$$

We claim that F forms a field

under addition and multiplication defined by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ and } \frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd}$$

where $b, d \in R' \Rightarrow b, d \neq 0$.
Since R has no zero divisors
$\Rightarrow bd \neq 0 \Rightarrow \frac{ad+bc}{bd}, \frac{ac}{bd} \in F$

$\Rightarrow \frac{a}{b} + \frac{c}{d} \in F$ & $\frac{a}{b}\cdot\frac{c}{d} \in F$.

F is closed w.r.t '+' & '.'.

(1) Addition is well defined
We shall show that if $\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}$ then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$

and $\frac{a}{b}\cdot\frac{c}{d} = \frac{a'}{b'}\cdot\frac{c'}{d'}$

To show that $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$, we have to prove

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

i.e $(ad+bc)b'd' = bd(a'd'+b'c')$
$(ad+bc)b'd' = adb'd' + bcb'd'$
$= ab'(dd') + (bb')(cd')$
$= (ba')(dd') + (bb')(cd')$
$= bd(a'd' + b'c')$

2) Multiplication is well defined
We shall show that $\frac{a}{b}\cdot\frac{c}{d} = \frac{a'}{b'}\cdot\frac{c'}{d'}$

which will hold if
$\frac{ac}{bd} = \frac{a'c'}{b'd'}$ i.e $ac \cdot b'd' = bd \cdot a'c'$

$ac \cdot b'd' = (ab')(cd') = (ba')(dc')$
$= bd\, a'c'$.

(3) Addition is associative in F i.e
$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{g}{h} = \frac{a}{b} + \left(\frac{c}{d} + \frac{g}{h}\right)$

$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{g}{h} = \frac{ad+bc}{bd} + \frac{g}{h} = \frac{h(ad+bc)+bdg}{bdh}$.

$= \frac{had + hbc + bdg}{bdh}$.

$= \frac{had + b(ch+dg)}{bdh} = \frac{a}{b} + \frac{ch+dg}{dh}$.

$= \frac{a}{b} + \left(\frac{c}{d} + \frac{g}{h}\right)$

4) Existence of additive identity:-
$\frac{a}{b} + \frac{0}{x} = \frac{ax+b0}{bx} = \frac{ax}{bx} = \frac{a}{b}$

$\therefore \frac{0}{x} \in F$ is additive identity of $F \forall x \in R'$

5) Existence of additive inverse:-
let $\frac{a}{b} \in F \Rightarrow a \in R, b \in R' \Rightarrow -a \in R, b \in R'$
$\Rightarrow -\frac{a}{b} \in F$

Now, $-\frac{a}{b} + \frac{a}{b} = \frac{-ab+ba}{b^2} = \frac{0}{b^2} = \frac{0}{x}$

i.e $-\frac{a}{b} + \frac{a}{b} = \frac{0}{x}$ = zero element of F.

$\Rightarrow -\frac{a}{b} \in F$ is the additive inverse of any $\frac{a}{b} \in F$.

6) Additive is commutative in F,
i.e $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$

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

$= \frac{c}{d} + \frac{a}{b}$.

7) Multiplication is associative in F i.e
$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{g}{h} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{g}{h}\right)$

$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{g}{h} = \frac{ac}{bd} \cdot \frac{g}{h} = \frac{(ac)g}{(bd)h} = \frac{a(cg)}{bdh}$

$= \frac{a}{b} \cdot \frac{cg}{dh} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{g}{h}\right)$

8) Existence of multiplicative identity:
$\frac{a}{b} \cdot \frac{x}{x} = \frac{ax}{bx} = \frac{a}{b}$ i.e $\frac{a}{b} \cdot \frac{x}{x} = \frac{a}{b}$

Also $x \neq 0 \Rightarrow x \in R' \Rightarrow \frac{x}{x} \in F$
$\Rightarrow \frac{x}{x} \in F$ is the multiplicative identity for each $x \neq 0$.

9) Existence of multiplicative inverse:-

let $\frac{a}{b} \in F$ s.t $\frac{a}{b} \neq \frac{0}{x} \Rightarrow a, b \neq 0 \Rightarrow \frac{b}{a} \in F$

$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{x}{x}$.

$\frac{a}{b}\cdot\frac{b}{a} = \frac{x}{x}$ = unity element of F

⇒ Every non zero elt. of F has a multiplicative inverse of F and $\frac{b}{a} \in F$ is the multiplicative inverse of $\frac{a}{b}$.

(c) Multiplication is commutative in F i.e.

$\frac{a}{b}\cdot\frac{c}{d} = \frac{c}{d}\cdot\frac{a}{b}$.

We have $\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\cdot\frac{a}{b}$.

(d) Distributivity :- $\frac{a}{b}\left(\frac{c}{d}+\frac{g}{h}\right) = \frac{a}{b}\cdot\frac{c}{d} + \frac{a}{b}\cdot\frac{g}{h}$

and $\left(\frac{c}{d}+\frac{g}{h}\right)\frac{a}{b} = \frac{c}{d}\cdot\frac{a}{b} + \frac{g}{h}\cdot\frac{a}{b}$

$\frac{a}{b}\left(\frac{c}{d}+\frac{g}{h}\right) = \frac{a}{b}\left(\frac{ch+dg}{dh}\right) = \frac{a(ch+dg)}{bdh}$

$= \frac{ach+adg}{bdh} = \frac{ac}{bd} + \frac{ag}{bh}$

$= \frac{a}{b}\cdot\frac{c}{d} + \frac{a}{b}\cdot\frac{g}{h}$.

Hence $\langle F, +, \cdot\rangle$ is a field and this field is called the field of quotients of the integral domain R.

We shall show that F contains a subset D s.t $D \cong R$.

Let $D = \{\frac{a}{1} : a \in R\}$

Obviously $D \subset F$

Define a mapping $\phi : D \to R$ s.t $\phi\left(\frac{a}{1}\right) = a$ $\forall$ $a \in R$.

ϕ is one to one as $\phi\left(\frac{a}{1}\right) = \phi\left(\frac{b}{1}\right)$ $\forall$ $a, b \in R$

$\Rightarrow a = b \Rightarrow \frac{a}{1} = \frac{b}{1}$

ϕ is onto as for any $a \in R$, there exist $\frac{a}{1} \in D$ s.t $\phi\left(\frac{a}{1}\right) = a$.

ϕ is a homomorphism.

Let $a, b \in R$ be arbitrary, then

$\phi\left(\frac{a}{1}+\frac{b}{1}\right) = \phi\left(\frac{1\cdot a+1\cdot b}{1\cdot 1}\right) = \phi\left(\frac{a+b}{1}\right) = a+b$

$= \phi\left(\frac{a}{1}\right) + \phi\left(\frac{b}{1}\right)$

$\phi\left(\frac{a}{1}\cdot\frac{b}{1}\right) = \phi\left(\frac{ab}{1\cdot 1}\right) = \phi\left(\frac{ab}{1}\right) = ab$

$= \phi\left(\frac{a}{1}\right)\phi\left(\frac{b}{1}\right)$

$\phi\left(\frac{a}{1}+\frac{b}{1}\right) = \phi\left(\frac{a}{1}\right) + \phi\left(\frac{b}{1}\right)$ & $\phi\left(\frac{a\cdot b}{1\cdot 1}\right) = \phi\left(\frac{a}{1}\right)\phi\left(\frac{b}{1}\right)$

So ϕ is one-one, onto homomorphism.

Thus $\phi : D \xrightarrow{\text{onto}} R$

Hence an integral domain can be embedded into a field.

Ch-8
Euclidean Rings

Def:- Divisibility in a commutative ring :-
Let R be a commutative ring and $a, b \in R$. We say that $0 \neq a$ divides b if there exist $c \in R$ s.t $b = ac$.

* **Unit element:-** Let R be a commutative ring with unity element 1. An element $a \in R$ is a unit of R if $a/1$. i.e if there exist an element $b \in R$ s.t $ab = 1$
Thus units of R are those elements of R which have multiplicative inverse.

Theorem:- The product of two units $a, b \in R$ is also a unit of R.

Proof:- Let a and b be two units in a commutative ring with unity elt. 1.
∴ By def, there exist $c, d \in R$ s.t
$ac = 1$, $bd = 1$
$\Rightarrow (ac)\cdot(bd) = 1 \cdot 1$
$\Rightarrow$ ~~a(cd)~~ $a(cb)d = 1$
$a(bc)d = 1$
$(ab)(cd) = 1$.
$\Rightarrow$ ab is also a unit of R.

Def:- **Associates:-** Let R be a commutative ring with unity element. Two elements a, b are associates in R if $a = ub$ for some unit 'u' in R.

* **Prime element:-** An element p of a commutative ring R with unity is called a prime element if
(i) $p \neq 0$, p is not a unit.
(ii) For every $a, b \in R$ if $p/ab \Rightarrow p/a$ or p/b.

* **Irreducible element:-** An element p of a commutative ring R with unity is called irreducible element if
(i) $p \neq 0$ and p is not a unit
(ii) p has no proper factors i.e whenever $p = ab$ then either a or b is a unit

* **Gaussian integer :-** A Gaussian integer is a complex number $a+ib$ where $a, b \in Z$.

* **Proper and Improper divisors:-** Let a be a non zero element of an integral domain R. Then the units of R and associates of a are always divisors of a. These are called trivial or improper divisors of a. Any other divisors of a are called non trivial or proper

divisors of a.

e.g: $\pm 1, \pm 6$ are improper divisors of 6.
$\pm 2, \pm 3$ are proper divisors of 6.

* Greatest Common divisor:- Let R be a commutative ring. An element $d \in R$ is a g.c.d of elements $a, b \in R$ if

(i) d/a, d/b.
(ii) whenever c/a, c/b then c/d.

$d = (a,b)$ is a g.c.d of a and b

* Relatively prime or coprime:- Two non zero elements a, b in an integral domain R, with unity are said to be relatively prime or coprime if g.c.d of a and b is a unit in R.

* Least common multiple:- Let R be a commutative ring. A non zero elt. $l \in R$ is a least common multiple of two elements $a \& b \in R$ if

(i) a/l, b/l
(ii) if a/c, b/c then l/c.

$l = [a,b]$ is the l.c.m of a and b

* Euclidean rings:- An integral domain R is said to be Euclidean ring if corresponding to every non zero

element $a \in R$ we can assign a non negative $d(a)$ s.t

(i) For all $a, b \in R$, $d(a) \leq d(ab)$
(ii) For all $a, b \in R$, $\exists$ q and r in R s.t $a = bq + r$ where $r = 0$ or $d(r) < d(b)$.

Ex:- The ring of Gaussian integers is an Euclidean domain.

Sol:- Let $Z[i] = \{a+ib ; a, b \in Z\}$ be the ring of Gaussian integers.

We know that $Z[i]$ is an integral domain.

Let us define a fn d on the non zero elts of $Z[i]$ by

$d(a+ib) = a^2+b^2 \quad \forall\ 0+i0 \neq a+ib \in Z[i]$

Let z_1, z_2 be two non zero elts of $Z[i]$ s.t $z_1 \neq 0$, $z_2 \neq 0$ & $z_1 = a+ib$, $z_2 = c+id$

Then $d(z_1, z_2) = d[(a+ib)(c+id)]$

$= d[(ac-bd) + i(ad+bc)]$

$= (ac-bd)^2 + (ad+bc)^2$

$= (a^2+b^2)(c^2+d^2)$

$= d(a+ib)\, d(c+id)$ — (1)

$\geq (a^2+b^2)$

$d(z_1, z_2) \geq d(z_1)$

or $d(z_1) \leq d(z_1, z_2)$ — (2)

Let $z_1, z_2 \in Z[i]$ be arbitrary

Consider $z = \frac{z_1}{z_2} = \frac{a+ib}{c+id} = \frac{(a+ib)(c+id)}{c^2+d^2}$

$= A+iB$

where A and B are rational numbers and z is not necessarily a Gaussian integer. Choose the integers nearest to A and B. Let these be A' and B' resp. Then $|A'-A| \le \frac{1}{2}$, $|B'-B| \le \frac{1}{2}$

Let $z' = A' + iB'$ be a Gaussian integer

$z = \frac{z_1}{z_2} \Rightarrow z_1 = zz_2$

$z_1 = z'z_2 + zz_2 - z'z_2$

$= z'z_2 + (z-z')z_2 \quad - (3)$

Since z_1, z_2, z' are Gaussian integers

$\therefore (z-z')z_2$ is also a Gaussian integer

Also $(z-z')z_2 = [(A+iB)-(A'+iB')](c+id)$

$= d[(A-A')+i(B-B')]d(c+id)$

$< [(A-A')^2 + (B-B')^2]\, d(z_2)$

$\le \left[\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right] d(z_2)$

$= \frac{1}{2} d(z_2) < d(z_2)$

Thus $d[(z-z')z_2] < d(z_2)$

Now if A and B are integers, then

$(z-z')z_2 = [(A-A')+i(B-B')](c+id)$

$= (0+i0)(c+id) = 0$

$\therefore (z-z')z_2 = 0$

Thus we have shown that

$z_1 = z'z_2 + (z-z')z_2$

and either $(z-z')z_2 = 0$ or

$d[(z-z')z_2] < d(z_2)$

Hence $\mathbb{Z}[i]$ is an Euclidean ring.

Theorem:- Every ideal of an Euclidean ring is a principal ideal.

Proof:- Let R be an Euclidean ring. Let S be any ideal of R. If $S = \{0\}$ i.e a null ideal, then obviously the theorem is proved.

Let $S \neq \{0\}$

then we have to prove that $S = \{a_0 r : r \in R\}$ which is a principal ideal.

$\exists$ atleast one non zero elt a in S.

Consider an element $a_0 \in S$ s.t $d(a_0)$ is minimal.

i.e $d(a_0) < d(a) \;\forall\; a_0 \neq a \in S$

Let $a \in S$ be arbitrary.

$\exists\, q, r \in R$ s.t

$a = a_0 q + r$ where $r = 0$ or $d(r) < d(a_0)$ — (1)

Now $q \in R, a_0 \in S \Rightarrow a_0 q \in S$

$a_0 q \in S, a \in S \Rightarrow a - a_0 q \in S$

$\Rightarrow r \in S$

$\Rightarrow d(a_0) < d(r)$

$\Rightarrow r = 0$

$\Rightarrow a = a_0 q$

$\therefore a \in S$ can be expressed as $a_0 q$

$\Rightarrow S \subseteq \{a_0 r : r \in R\}$

But $a_0 \in S \Rightarrow a_0 r \in S$

$\Rightarrow \{a_0 r : r \in R\} \subseteq S$.

Hence $S = \{a_0 r : r \in R\}$

Hence every ideal of an Euclidean ring is a principal ideal.

* Principal ideal domain (P.I.D) - An integral domain R with unity is a principal ideal domain if every ideal in R is a principal ideal.

Theorem: Show that an element a in an Euclidean ring R is a unit iff $d(a) = d(1)$

Proof: Let a be an element in an Euclidean ring s.t a is a unit in R.
Since a is a unit in R, therefore there exist a^{-1} s.t

$$aa^{-1} = 1$$
$$d(a) \le d(aa^{-1})$$
$$d(a) \le d(1)$$

Also $d(1) \le d(1 \cdot a)$
$\Rightarrow d(1) \le d(a)$
$\therefore d(a) = d(1)$

Conversely, Let $a \in R$ s.t $d(a) = d(1)$
We have to show that a is a unit in R.
If possible, let a is not a unit of R,

$$d(1 \cdot a) > d(1)$$
$$d(a) > d(1)$$ which is a contradiction.

Hence a is a unit of R.

Theorem:- Let R be an Euclidean R. Then any two elements a and b in R have a g.c.d.

Proof:- Let $S = \{ r_1 a + s_1 b : r_1, s_1 \in R \}$
We claim that S is an ideal of R.
Obviously $0 = 0 \cdot a + 0 \cdot b \in S \Rightarrow S \neq \phi$
Let $x, y \in S$ be arbitrary, then

$$x = r_1 a + s_1 b$$
$$y = r_2 a + s_2 b \text{ for some } r_1, r_2, s_1, s_2 \in R$$
$$x - y = (r_1 - r_2) a + (s_1 - s_2) b$$

Now $r_1, r_2, s_1, s_2 \in R$
$r_1 - r_2, s_1 - s_2 \in R$
$(r_1 - r_2) a + (s_1 - s_2) b \in S$
$x - y \in S$
$x, y \in S \Rightarrow x - y \in S.$

Also if $r \in R$ then $rx = r(r_1 a + s_1 b)$
$= (rr_1) a + (rs_1) b.$
Since $rr_1, rs_1 \in R \Rightarrow rx \in S$
Since R is commutative $rx = xr \in S.$
$\therefore$ S is an ideal of R. But every ideal of Euclidean ring R is a principal ideal.
$\Rightarrow$ S is a principal ideal of R and S is generated by some elt say d.
Since $d \in S$

$$d = ma + nb \text{ for some } m, n \in R$$
$$a = 1 \cdot a + 0 \cdot b \in S.$$

$b = 0.a + 1.b \in S$.

Now $a, b \in S$ & $S = \langle d \rangle$

$\Rightarrow a = d\lambda$ & $b = d\mu$ for some $\lambda, \mu \in R$

$\Rightarrow d/a$ and d/b.

Suppose that c/a and c/b

$\Rightarrow c/ma, c/nb \Rightarrow c/ma+nb$

$\Rightarrow c/d$

$\Rightarrow d = (a,b)$

i.e d is a g.c.d of a and b.

Hence the proof.

Theorem: An element in a P.I.D is prime element iff it is irreducible.

Proof:- Let R be a PID and $p \in R$ be a prime element.

Let $p = ab$. then we are to show that a or b is a unit.

Now $p = ab \Rightarrow p/ab$

$\Rightarrow p/a$ or p/b

If $p/a \Rightarrow a = pm$ for some m

$\therefore p = ab \Rightarrow p = (pm)b$

$\Rightarrow p(1-mb) = 0$

$\Rightarrow 1 - mb = 0$

$\Rightarrow mb = 1$

$\Rightarrow b$ is a unit

Similarly if p/b, then a is a unit.

Conversely, let p be a irreducible element s.t p/ab.

We are to show that p/a or p/b.

If p/a, then there is nothing to prove. so consider p/a.

Since p and $a \in$ PID, they must have a some gcd.

Let $(p,a) = d \Rightarrow d/p$, d/a.

$\Rightarrow p = dx$, $a = dy$ for some x, y

If d is not a unit, then $p = dx$

$\Rightarrow$ x is a unit $\Rightarrow x^{-1}$ exists

$$px^{-1} = d$$

$$a = dy = (px^{-1})y$$

$$a = p(x^{-1}y)$$

$\Rightarrow p/a$ which is a contradiction

Thus d must be a unit.

Also $d = (p,a) \Rightarrow d = up + va$

$\Rightarrow d^{-1}d = d^{-1}up + d^{-1}va$.

$\Rightarrow 1 = ud^{-1}p + vd^{-1}a$

$\Rightarrow b = ud^{-1}pb + vd^{-1}ab$

Also p/p. $p/ab \Rightarrow p/ud^{-1}pb$, $p/vd^{-1}ab$

$\Rightarrow p/ud^{-1}pb + vd^{-1}ab$

$\Rightarrow p/b$

Hence the result.

Theorem: Let R be a PID which is not a field. Then an ideal $S = \langle a \rangle$ is a maximal ideal iff a is an irreducible element.

Proof:- Let $S = \langle a_0 \rangle$ be a maximal ideal.
We shall show that

(i) $a_0 \neq 0$

(ii) a_0 is not a unit

(iii) a_0 has no proper factors i.e whenever $a_0 = bc$ then either b or c is a unit

Suppose $a_0 = 0$

Since R is not a field, therefore there exist atleast one non-zero element $b \in R$ s.t b^{-1} does not exist.

Let $T = \langle b \rangle$ and $a_0 = 0 \Rightarrow S = \langle 0 \rangle$

$$\langle 0 \rangle \subseteq T \subseteq R$$

$$S \subseteq T \subseteq R$$

But $T \neq S$ as $b \in T$, $b \neq 0$ and $S = \langle 0 \rangle$

Also $T \neq R$ as $1 \in R$ but $1 \notin T$ since

$1 \in T$

$\Rightarrow 1 \in \langle b \rangle \Rightarrow 1 = bx$ for some x

$\Rightarrow$ b is invertible, which is a contradiction

Hence $a_0 \neq 0$

Let us suppose that a_0 is a unit.

$a_0 a^{-1} = 1$.

Now $a_0 \in S$, $a_0^{-1} \in R \Rightarrow a_0 a^{-1} \in S$

$\Rightarrow 1 \in S$

$\Rightarrow S = R$ which is not possible

$\therefore$ a_0 is not a unit.

Finally, let $a_0 = bc$ for some $b, c \in R$

Since S is a maximal ideal.

$\therefore$ For any ideal $T \supseteq S$, either $T = S$ or $T = R$. Let $T = \langle b \rangle$

If $T = S$, then $b \in S \Rightarrow b \in \langle a_0 \rangle$

$\Rightarrow b = ma_0$ for some m

$\therefore$ $a_0 = bc \Rightarrow a_0 = ma_0 c$

$\Rightarrow a_0(1 - mc) = 0$

$\Rightarrow 1 - mc = 0$

$\Rightarrow mc = 1$

$\Rightarrow$ c is a unit.

If $T = R$ then $1 \in R \Rightarrow 1 \in T = \langle b \rangle$

$\Rightarrow 1 = nb$ for some n.

$\Rightarrow$ b is a unit.

Thus a_0 is an irreducible element.

Conversely, Let a_0 be an irreducible element s.t $S = \langle a_0 \rangle$

We have to prove that S is maximal.

Since a_0 being irreducible is not a unit element, therefore $S \neq R$

Let $T \supseteq S$ be an ideal of R.

Since R is a P.I.D.

$\therefore$ $T = \langle b \rangle$ for some $b \in R$ and $b \notin S$.

Also $\langle a_0 \rangle \subset \langle b \rangle$

$\Rightarrow a_0 = mb$ for some $m \in R$.

Since a_0 is irreducible elt, therefore either m is a unit or b is a unit.

If m is a unit, then $b = m^{-1} a_0 \in S$ which is a contradiction.

Thus we are left with the only

choice that b is a unit.
$\Rightarrow T = \langle b \rangle = R$
Hence S is a maximal ideal of R.
Hence the proof.

Ex:- Find all the units of $Z[\sqrt{-5}]$

Sol. Let $(a+\sqrt{-5}b)$ be a unit of $Z[\sqrt{-5}]$

$(a+\sqrt{-5}b)(c+\sqrt{-5}d) = 1+\sqrt{-5}\cdot 0$

$(a+\sqrt{-5}b)(c+\sqrt{-5}d) = 1$ — (1)

Taking conjugates on both sides, we get

$(a-\sqrt{-5}b)(c-\sqrt{-5}d) = 1$

$(a^2+5b^2)(c^2+5d^2) = 1$

$a^2+5b^2 = 1 \Rightarrow a = \pm 1, b = 0$

$\therefore (a+\sqrt{-5}b) = (\pm 1 + \sqrt{-5}0) = \pm 1$ are units in $Z[\sqrt{-5}]$

Ex:- Show that every non zero prime ideal of a PID is maximal.

Sol- Let $S = \langle a \rangle$, $a \neq 0$ be a non zero prime ideal in a PID R.

Let $T = \langle b \rangle$ be an ideal s.t. $T \supseteq S$ — (1)

Now $T \subseteq R$

$\langle b \rangle \subseteq R$.

$\therefore a \in S \Rightarrow a \in T$

$\Rightarrow a \in \langle b \rangle$

$\therefore a = mb$ for some $m \in R$

$\Rightarrow mb \in S \Rightarrow m \in S$ or $b \in S$

If $b \in S$ then all multiples of b are in S.
$\Rightarrow T \subseteq S$ — (2)
From (1) & (2), $T = S$.
If $m \in S$, then $m = na$ for some $n \in R$
$m = n(mb) = m(nb)$
$\Rightarrow m(1-nb) = 0$
Here $m \neq 0$ as $m = 0 \Rightarrow a = 0 \cdot b = 0$
$\Rightarrow S = \langle 0 \rangle$
$\therefore 1 - nb = 0 \Rightarrow nb = 1$.
But $b \in T$, $n \in R \Rightarrow nb \in T$
$\Rightarrow 1 \in T$.
$\Rightarrow T = R$
$\Rightarrow S$ is a maximal ideal.
Hence every non zero prime ideal in a PID is a maximal ideal.

—x—

Ch-9
Polynomial rings

Def: **Polynomial rings:-** Let R be a ring. Let $a_0, a_1, \ldots, a_n \in R$ be arbitrary. By a polynomial over R, we mean a finite formal sum

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = \sum_{i=0}^{n} a_i x^i$$

Any infinite sequence of elements of a ring R is said to be a polynomial over R if all except finite no. of its terms are equal to zero.

* **Degree of a polynomial:-** Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be any non zero polynomial in $R[x]$. We say that n is the degree of polynomial $f(x)$ iff $a_n \neq 0$ and $a_i = 0$ $\forall$ $i > n$.

Embedding of R into $R[x]$

Theorem:- Let R be an arbitrary ring and $R[x]$ the corresponding ring of polynomials over R. If R' is the set of constant polynomials in $R[x]$, then R' is isomorphic to R i.e R can be embedded in $R[x]$.

Proof:- We have $R' = [ax^0 + 0x + 0x^2 + \cdots ; a \in R]$

Define a mapping $f: R \to R'$ s.t $f(a) = ax^0 + 0x + 0x^2 + 0x^3 \cdots$ $\forall a \in R$

We claim that f is a one to one homomorphism as

$f(a) = f(b)$; $a, b \in R$ be arbitrary

$\Rightarrow$ $ax^0 + 0x + 0x^2 + \cdots = bx^0 + 0x + 0x^2 + \cdots$

$\Rightarrow$ $a = b$

$\Rightarrow$ f is one to one.

Obviously f is onto and

$f(a+b) = (a+b)x^0 + 0x + 0x^2 + \cdots$

$= (ax^0 + 0x + 0x^2 + \cdots) + (bx^0 + 0x + \cdots)$

$= f(a) + f(b)$

$f(ab) = abx^0 + 0x + 0x^2 + \cdots$

$= (ax^0 + 0x + 0x^2 + \cdots)(bx^0 + 0x + \cdots)$

$= f(a) f(b)$

Thus f is an isomorphism of R onto R'

Hence $R \cong R'$.

Theorem:- If F is a field, then $F[x]$ is a principal ideal ring.

Proof:- We know that $F[x]$ is an integral domain with unity.

Define the valuation d as

$d(f(x)) = \deg f(x)$ where $0 \neq f(x) \in F(x)$

≥ 0

Also for any $f(x), g(x) \in F(x)$

$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$

$\Rightarrow \deg f(x) \leq \deg(f(x)g(x))$

$\Rightarrow \deg f(x) \leq \deg(f(x)g(x))$

Next, we shall show that for any non zero $f(x), g(x) \in F[x]$, there exist $q(x)$ and $r(x)$ in $F[x]$ s.t

$f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$

or $\deg r(x) < \deg g(x)$ - ①

If $\deg f(x) < \deg g(x)$ then

$f(x) = 0 \cdot g(x) + f(x)$ & ① hold.

Let us assume that ① is true for all non zero polynomials $\in F[x]$ of degree less than $\deg f(x)$

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m$

$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$

We assume that $\deg f(x) \geq \deg g(x)$

Let $f_1(x) = f(x) - a_mb_n^{-1}x^{m-n}g(x)$

$= (a_0 + a_1x + \dots + a_mx^m) - a_mb_n^{-1}x^{m-n}$

$(b_0 + b_1x + b_2x^2 + \dots + b_nx^n)$

The coeff of x^m in $f_1(x)$ is

$a_m - a_mb_n^{-1}b_n = a_m - a_m = 0$

$\Rightarrow$ either $f_1(x) = 0$ or $\deg(f_1(x)) < m$

Now $f_1(x) = 0$

$\Rightarrow f(x) - a_mb_n^{-1}x^{m-n}g(x) = 0$

$\Rightarrow f(x) = a_mb_n^{-1}x^{m-n}g(x) + 0$.

If we take $q(x) = a_mb_n^{-1}x^{m-n}$ & $r(x) = 0$, Then ① is true.

If $f_1(x) \neq 0$ then $\deg f_1(x) < m$

$\deg f_1(x) < \deg f(x)$

By induction hypothesis,

$f_1(x) = q_1(x)g(x) + r(x)$ where $r(x) = 0$

or $\deg r(x) < \deg g(x)$

Thus $f(x) - a_mb_n^{-1}x^{m-n}g(x) = q_1(x)g(x) + r(x)$

Thus both the conditions for Euclidean domain are satisfied. Hence $F[x]$ is an Euclidean domain.

Hence the proof.

Division Algorithm for $F(x)$

Statement:- Let $f(x), g(x) \neq 0$ be two elts of $F[x]$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ s.t

$f(x) = g(x) \cdot q(x) + r(x)$ where $r(x) = 0$

or $\deg r(x) < \deg g(x)$

Proof:- Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m, a_m \neq 0$

& $g(x) = b_0 + b_1x + \dots + b_nx^n, b_n \neq 0$

s.t $\deg(f(x) = m, \deg g(x) = n$.

If $f(x) = 0$ then we can take $q(x) = 0$, $r(x) = 0$ and the result holds trivally.

Let $f(x)$ is non zero. If $\deg f(x) < \deg g(x)$ then we can write $f(x) = 0 \cdot g(x) + f(x)$

So in this case the theorem is true for $q(x) = 0$ and $r(x) = f(x)$

We now assume that $m \geq n$

We shall prove the theorem by induction

or deg $f(x)$ i.e m.
If $m=0$ then $m \geq n \Rightarrow n=0$
$\Rightarrow$ $f(x)$ and $g(x)$ are both non zero constt polynomial.
For $f(x) = a_0 \neq 0$, $g(x) = b_0 \neq 0$ we have
$f(x) = a_0 = (a_0 b_0^{-1}) b_0 + 0 = (a_0 b_0^{-1}) g(x) + 0$
$\Rightarrow$ The theorem is true for $m=0$ i.e for the case when deg $f(x) < 1$.
We now assume that the theorem is true for every polynomial of degree less than m.
Consider $f_1(x) = f(x) - (a_m b_n^{-1}) x^{m-n} g(x)$
deg $f_1(x) < m$
deg $f_1(x) <$ deg $f(x)$
Thus by our assumption, there exist polynomials $q_1(x), r_1(x)$ s.t
$f_1(x) = q_1(x) g(x) + r_1(x)$
$\Rightarrow f(x) - (a_m b_n^{-1}) x^{m-n} g(x) = q_1(x) g(x) + r(x)$
$f(x) = [(a_m b_n^{-1}) x^{m-n} + q_1(x)] g(x) + r_1 x$
Setting $q(x) = (a_m b_n^{-1}) x^{m-n} + q_1(x)$
$r(x) = r_1(x)$
$f(x) = q(x) \cdot g(x) + r(x)$
where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$
which proves the existence of $q(x)$ & $r(x)$
Uniqueness:- If possible, let
$f(x) = q_1(x) g(x) + r_1(x)$.
$f(x) = q_2(x) g(x) + r_2(x)$
where $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$

and $r_2(x) = 0$ or deg $r_2(x) <$ deg $g(x)$
$\Rightarrow [q_1(x) - q_2(x)] g(x) = r_2(x) - r_1(x)$
Since deg $[r_2(x) - r_1(x)] <$ deg $g(x)$
$\therefore$ If $q_1(x) - q_2(x) = 0$
$\Rightarrow q_1(x) = q_2(x)$
Thus $r_2(x) = r_1(x)$
which shows that the polynomials $q(x)$ and $r(x)$ are unique.
Hence the proof.

Unique Factorization domain:-

Let R be an integral domain with unity. Then R is called a unique factorization domain if
(i) every element of R that is neither 0 nor unit can be expressed as a product of finite number of irreducible elements of R.
(ii) If $a = p_1 p_2 p_3 \ldots p_r$ and $a = q_1 q_2 \ldots q_s$ are two factorizations of the same element a, Then $r = s$ and each p_i is an associate of some q_j i.e factorization is unique upto the order and associates of irreducible elements.

Theorem: Every principal ideal domain is a unique factorization domain.

Proof:- Let a be any non zero, non unit element

of R.
If a is irreducible, then $a = a$
$\therefore$ a can be expressed as a finite product of irreducible elements.
If a is not irreducible, then there exists an irreducible element p_1, s.t p_1 / a
$\Rightarrow a = a_1 p_1$ for some $a_1 \in R$
If a_1 is irreducible
$\Rightarrow$ a is expressible as finite product of irreducible elements.
If a_1 is not irreducible, we claim that $a_1 \neq 0$ and a_1 is a non unit element.
This is so because $a_1 = 0 \Rightarrow a = 0$ which is not possible.
Also if a_1 is a unit element, then
$a = a_1 p_1$
$\Rightarrow$ a and p_1 are associates.
$\Rightarrow$ a is irreducible.
But a_1 is not irreducible.
Again, for non zero, non unit element a_1 which is not irreducible, there exist an irreducible element p_2 s.t
p_2 / a_1
$\Rightarrow a_1 = a_2 p_2$ for some $a_2 \in R$
$\therefore$ We have $a = a_2 p_1 p_2$
If a_2 is irreducible we stop otherwise we continue
$a_2 = a_3 p_3$

where p_3 is some irreducible element
Proceeding in this way,
$a = p_1 p_2 p_3 \dots p_n a_n$
Thus a is expressed as a finite product of irreducible elements.
Uniqueness:- Let $a = p_1 p_2 p_3 \dots p_n$ and $a = q_1 q_2 q_3 \dots q_m$ be two factorizations of the same element a into irreducibles.
$\therefore p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$
$p_1 (p_2 p_3 \dots p_n) = q_1 q_2 \dots q_m$
$p_1 / q_1 q_2 q_3 \dots q_m$
$\Rightarrow p_1 / q_1$ or q_2 or q_3 ... or q_m.
W.O.G, we assume that p_1 / q_1 so that
$q_1 = p_1 u_1$
Since p_1 is irreducible, u_1 is a unit, therefore p_1 and q_1 are associates.
Thus $p_1 p_2 \dots p_n = p_1 u_1 q_2 \dots q_m$
$p_2 p_3 \dots p_n = u_1 q_2 q_3 \dots q_m$
Proceeding in the same way, we get
$1 = u_1 u_2 \dots u_n q_{n+1} \dots q_m$
Since q_j's are irreducibles, therefore $m = n$, which proves the uniqueness.

Def:- Primitive polynomial:- Let R be a UFD. A non zero polynomial $f(x) = a_0 + a_1 x + \dots$ in $R[x]$ is said to be a primitive

primitive.

Eisenstein's Irreducibility Criterion

Theorem:- Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in $Z[x]$. If p is a prime element s.t

(i) $p/a_0, p/a_1, p/a_2, \cdots p/a_{n-1}$

(ii) $p \nmid a_n$ and $p^2 \nmid a_0$

then $f(x)$ is an irreducible polynomial in $Q[x]$.

Proof:- Since $Z[x]$ is an integral domain with unity.

$\therefore$ $Z[x]$ is a UFD and $Q[x]$ i.e field of polynomials over rationals. is its quotient field.

W.L.O.G, we assume that $f(x)$ is primitive for taking out the g.c.d of the coeff. does not disturb the hypothesis since $p \nmid a_n$.

We are to prove that $f(x)$ is irreducible in $Q[x]$

If possible, let $f(x)$ is irreducible in $Q[x]$ s.t

$f(x)$ = product of two polynomials of the degree in $Q[x]$

and thus $f(x)$ can be expressed as

$\therefore$ product of two polynomials $\in Z[x]$

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$

$= (b_0 + b_1x + \cdots + b_rx_r)(c_0 + c_1x + \cdots + c_sx^s)$ — (1)

where b_i, c_i are elts of Z and $r, s > 0$

Equating the coeff on both sides of (1), we get $a_0 = b_0c_0$, $a_n = b_rc_s$

Now $p/a_0 \Rightarrow p/b_0c_0$

$\Rightarrow$ p/b_0 or p/c_0.

Since $p^2 \nmid a_0$ therefore p cannot be a divisor of both b_0 and c_0.

Let p/b_0 then $p \nmid c_0$.

Also p cannot divide all the coeff $b_0, b_1, \cdots, b_r$.

This is so because if p/b_i for each $i = 1, 2, \cdots, r$, then p/a_i for each i which is a contradiction to cond.

(ii) as $p \nmid a_n$.

Let us assume that b_ℓ is the first among b's which is not div. by p. $1 \le \ell \le n$.

$\therefore$ p/b_i for each i where $0 \le i \le \ell - 1$ — (2)

and $p \nmid b_\ell$.

From (1), $a_\ell = b_0c_\ell + b_1c_{\ell-1} + b_2c_{\ell-2} + \cdots + b_\ell c_0$

$b_\ell c_0 = a_\ell - (b_0c_\ell + b_1c_{\ell-1} + \cdots + b_{\ell-1}c_1)$ — (3)

Since $\ell < n$

$\therefore$ p/a_ℓ

From (2), p/b_i for $0 \le i \le \ell - 1$

$\Rightarrow$ $P/b_0, P/b_1, P/b_2 \cdots P/b_{e-1}$

$\Rightarrow$ $P/b_0c_e, P/b_1c_{e-1}, P/b_2c_{e-2} \cdots P/b_{e-1}c_1$ — (5)

From (3), (4) & (5), we get $P/b_e c_0$

$\Rightarrow$ P/b_e or P/c_0

which is absurd, because according to our assumptions $P\nmid c_0$ and $P\nmid b_e$.

Hence $f(x)$ is irreducible over $\mathbb{Q}$.

Hence the proof.

Ex Let p be a prime and $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Show that $f(x)$ is irreducible over $\mathbb{Q}$.

Sol:- $(x-1)f(x) = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$

$= x^p - 1$

or $(x-1)f(x) = x^p - 1$ — (1)

Let $x - 1 = y \Rightarrow x = y + 1$

Using this value of x in (1), we get

$yf(y+1) = (y+1)^p - 1$

$yf(y+1) = (1+y)^p - 1$

$= 1 + {}^pC_1 y + {}^pC_2 y^2 + \cdots + {}^pC_p y^p - 1$

$= {}^pC_1 y + {}^pC_2 y^2 + \cdots + {}^pC_{p-1} y^{p-1} + y^p$

Dividing by y, we get

$f(y+1) = y^{p-1} + {}^pC_{p-1} y^{p-2} + \cdots + {}^pC_3 y^2 + {}^pC_2 y + {}^pC_1$ — (2)

where ${}^pC_r = \dfrac{p!}{r!(p-r)!}$

Eq (2) show that $f(y+1)$ is a polynomial with integral coeffs.

Also $P/{}^pC_1, P/{}^pC_2, \cdots, P/{}^pC_{p-1}$, P/p and $P\nmid 1$

i.e all the coeffs of $f(y+1)$ except that of y^{p-1} are div. by p

Also $p^2 \nmid p$ where $p = {}^pC_1$ is the const term of $f(y+1)$

Thus by Eisenstein irreducibility criterion, $f(y+1)$

i.e $f(x)$ is irreducible.

Ex Show that the polynomial $x^4 + 1$ is irreducible over $\mathbb{Q}$.

Sol:- Let $f(x) = x^4 + 1$

Replacing x by $x+1$, we have

$f(x+1) = (x+1)^4 + 1$

$= (x^4 + 4x^3 + 6x^2 + 4x + 1) + 1$

$= 2 + 4x + 6x^2 + 4x^3 + x^4$

$= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$ (say)

$\therefore$ $a_0 = 2, a_1 = 4, a_2 = 6, a_3 = 4, a_4 = 1$

Now $p = 2$ is a prime s.t

(i) $P/a_0, P/a_1, P/a_2, P/a_3$

and (ii) $P \nmid a_4$, $p^2 \nmid a_0$

By Eisenstein's criterion, $f(x+1)$ is irreducible over $\mathbb{Q}$.

If possible, let us assume that $f(x)$ is not irreducible over $\mathbb{Q}$.

$\therefore$ There exist $g(x), h(x) \in \mathbb{Q}[x]$ where $\deg g(x) > 1$, $\deg h(x) > 1$ s.t

$$f(x) = g(x)\,h(x)$$

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

As $\deg g(x+1) > 1$, $\deg h(x+1) > 1$

$\Rightarrow$ $f(x+1)$ is not irreducible over $\mathbb{Q}$ which is not possible and hence $f(x)$ is irreducible over $\mathbb{Q}$.
