[10 marks]

1) a] let G be a finite group, H and K subgroups of $G \ni K \subset H$. Show that $(G:K) = (G:H)(H:K)$

[Freshman theorem or third theorem on Isomorphism.]

Proof:-

Lemma:- If H and K are two normal subgroup of a group $G \ni K \subseteq H$ then $\frac{H}{K}$ is normal subgroup of $\frac{G}{K}$.

Proof:- $\frac{H}{K}$ is non ϕ set of $\frac{G}{K}$

--- $\{ \because K \in \frac{H}{K} \}$

for any $Kh_1, Kh_2 \in \frac{H}{K}$ --- $\{h_1, h_2 \in H$

$(Kh_1)(Kh_2)^{-1} = Kh_1 \cdot Kh_2^{-1} = Kh_1 h_2^{-1} \in \frac{H}{K}$

--- $\{ \because h_1 h_2^{-1} \in H$

$\therefore \frac{H}{K}$ is a subgroup.

for any $Kh \in \frac{H}{K}$ and $Kg \in \frac{G}{K}$, we have

$(Kg)^{-1}(Kh)(Kg)$

$= Kg^{-1}Kh\,Kg$

$= Kg^{-1}hg$

$\in KH$ --- $\{ \because H$ is normal in G $\therefore g^{-1}hg \in H \}$

$\therefore \frac{H}{K}$ is normal in $\frac{G}{K}$

$\therefore \dfrac{G/K}{H/K}$ is defined.

Scanned with CamScanner

Define a map

$f : \frac{G}{K} \to \frac{G}{H}$ $\ni$

$f(Ka) = Ha \quad \forall\, a \in G$

f is well defined.

$Ka = Kb$

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

but $K \subset H$

$\therefore ab^{-1} \in H$

$\Rightarrow Ha = Hb$

$\therefore f(Ka) = f(Kb)$

taking reversing step we can prove f is one-one.

f is homomorphism as

$f(KaKb) = f(Kab)$

$= Hab$

$= Ha \cdot Hb$

$= f(Ka) \cdot f(Kb)$

$\forall\, Ha \in \frac{G}{H}$ $\exists$ $Ka \in \frac{G}{K}$

$\ni f(Ka) = Ha$

hence f is onto.

using fundamental theorem on Group homomorphism.

$$\frac{G}{H} \cong \frac{G/K}{\ker f}$$

we claim $\ker f = \frac{H}{K}$

A member of $\ker f$ will be some member of $\frac{G}{K}$

now $Ka \in \ker f$

$\Leftrightarrow f(Ka) = H$

$\Leftrightarrow Ha = H$

$\Leftrightarrow a \in H$

$\Leftrightarrow Ka \in \frac{H}{K}$

here we find

$$\frac{G/K}{H/K} \cong \frac{G}{H}$$

or $(G:K) = (G:H) \cdot (H:K)$

here proved.

a] If G and H are finite groups whose orders are relatively prime, then prove that there is only one homomorphism from G to H, the trivial one. (10) marks

Proof:

let G and H are two finite groups
let $o(G) = m$, $o(H) = n$
Given, $(m, n) = 1$
assume $\exists$ homomorphism
$\phi : G \to H$ which is not trivial.
$\therefore \phi(G) \neq e'$ --- where $e' \in H$
$\Rightarrow \exists$ an element $x \in G \ni$
$\phi(x) = y'$ where $y' \in H$ & $y' \neq e'$
we know that in homomorphism
order of $f(a) \mid o(a)$
$\Rightarrow o(y') \mid o(x)$
$\Rightarrow o(\phi(x)) \mid o(x)$
but $o(y') = o(\phi(x))$ also divides $o(H)$
$\Rightarrow o(y') \mid o(G)$ and $o(y') \mid o(H)$
$\Rightarrow o(y')$ is g.c.d of (m, n)

but $(m, n) = 1 \Rightarrow o(y') = 1$
$\therefore$ our assumption that $y' \neq e'$ is wrong.
$\therefore$ There does not exist any homomorphism from $G \to H$ which is not trivial.
hence $\phi(G) = e'$ is only trivial homomorphism exist.

Scanned with CamScanner

2) b] write down all quotient group of group $\mathbb{Z}_{12}$. (10 marks).

proof:-

quotient group:- If G is a group and $H \leq G$. to define quotient group H must be normal subgroup of G

i.e. $Hg = gH \quad \forall g \in G$

$\because \mathbb{Z}_{12}$ is an abelian group and every subgroup of abelian group is normal subgroup. Hence following are normal subgroup of $\mathbb{Z}_{12}$

$\{\mathbb{Z}_{12} = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \bmod 12$

$H_1 = \{0\}$

$H_2 = \{0, 6\}$

$H_3 = \{0, 4, 8\}$

$H_4 = \{0, 3, 6, 9\}$

$H_5 = \{\mathbb{Z}_{12}\}$

let $G = \mathbb{Z}_{12}$

① $\frac{G}{H_1} = H_1 + \mathbb{Z}_{12}$

$= \mathbb{Z}_{12}$

② $\frac{G}{H_2} = a + H_2 \quad \ldots \quad a \in G$

$= [\{0, 6\}, \{1, 7\}, \{2, 8\}, \{3, 9\}$
$\{4, 10\}, \{5, 11\}]$

③ $\frac{G}{H_3} = [\{0, 4, 8\}, \{1, 5, 9\}, \{2, 6, 10\}$
$\{3, 7, 11\}]$

Scanned with CamScanner

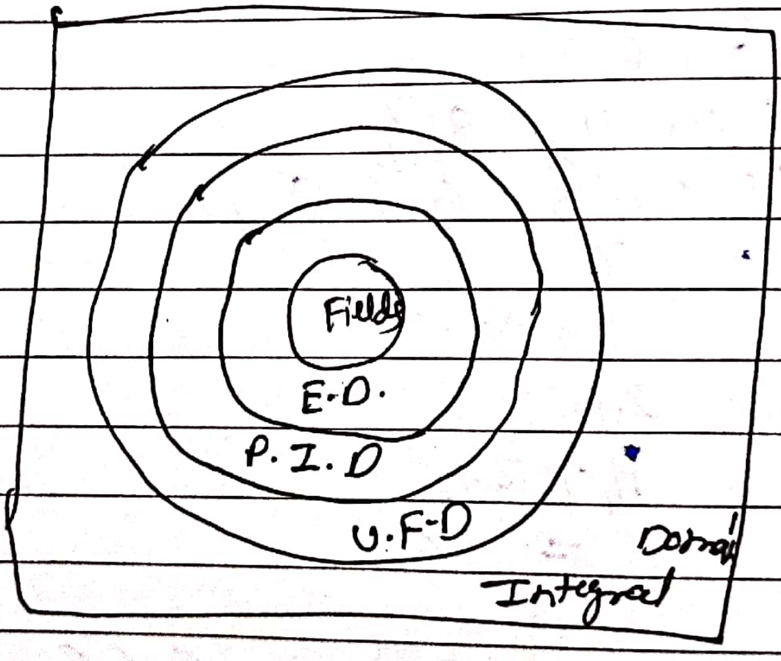
(4) $\frac{G}{H_4} = \{ a + H_4 : a \in G \}$

$= \{ \{0, 3, 6, 9\}, \{1, 4, 7, 10\}, \{2, 5, 8, 11\} \}$

(5) $\frac{G}{H_5} = \{ 0 \}$

3) d] let a be an irrudicible element of the Euclidean ring R, then prove that $\frac{R}{(a)}$ is a field.

Proof :



We know that If R is a commutative ring with unity and let A be an Ideal of R then R/A is a field iff A is maximal.

we are Given that $A = (a)$ where a is irreducible element

hence we have to show that
A is maximal Ideal of R.
let I be any Ideal of R $\ni$
$A \subseteq I \subseteq R$
by digaram $E.D. \Rightarrow P.I.D.$
$\therefore$ R is $P.I.D.$
In principal ideal domain every Ideal is principal ideal.
let $I = \langle d \rangle$ for some $d \in R$

$\Rightarrow$ let $d \in A$
as $A = \langle a \rangle$
$\therefore d = ax$ for some $a \in R$
for any $r \in I = (d)$
$r = dy, \; y \in R$
$r = axy$
$= a(xy)$ $\quad x.y \in R$
$\Rightarrow r \in A$
$\Rightarrow I \subseteq A$
but $A \subseteq I$
$\therefore A = I$
$\Rightarrow$ let $d \notin A$
now $a \in A \subseteq I = (d)$
$\therefore a = dP$ for some $P \in R$
$\because a$ is irreducible $\Rightarrow$ either d or P is unit.
let P is unit $\Rightarrow$ p^{-1} exist.
$\therefore ap^{-1} = dP.P^{-1}$
$\therefore d = a p^{-1}$
$p^{-1} \in R \quad a \in A$
$\therefore d \in A$ -- as A is ideal of R
but this is contradiction.

Scanned with CamScanner

hence d must be unit

$\therefore d^{-1}$ exist $d^{-1} \in R$

$\therefore d \in I, \quad d^{-1} \in R$

$d \cdot d^{-1} \in I$

$\Rightarrow 1 \in I$

$\Rightarrow I = R$

$\therefore$ if I is any ideal of $R \ni$

$A \subseteq I \subseteq R$

$\Rightarrow A = I$ or $I = R$

Hence A is maximal Ideal

$\Rightarrow \dfrac{R}{(a)}$ is field.