① Let G be a group of order n. Show that G is isomorphic to a subgroup of the permutation group S_n. (10)

Proof:-

$G = \{1, -1, i, -i\}$

let $G' = \{P_1, P_2, P_3, P_4\}$

$f : G \to G'$

$$P_1 = \begin{Bmatrix} 1 & -1 & i & -i \\ 1\cdot1 & -1\cdot1 & i\cdot1 & -i\cdot1 \end{Bmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}$$

$$= I$$

$$P_2 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot(-1) & (-1)(-1) & i(-1) & -i(-1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix} = (1\ -1)(i\ -i)$$

$$P_3 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot i & -1\cdot i & i\cdot i & -i\cdot i \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix} = (1\ i\ -1\ -i)$$

$$P_4 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot -i & -1\cdot -i & i\cdot(-i) & -i\cdot -i \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$$

$$= (1\ -i\ -1\ i)$$

Scanned with CamScanner

$G = \{1, -1, i, -i\}$

$G' = \{P_1, P_2, P_3, P_4\}$

$\phi : G \to G'$

$\phi(a) = P_a$

PROOF:- let G be the Given Group and $A(G)$ be the Group of all permutation of the set G.

For any $a \in G$, define a map

$f_a : G \to G \ni$

$f_a(x) = ax$

then as $x = y$

$\Rightarrow ax = ay$

$\Rightarrow f_a(x) = f_a(y)$

$\therefore f_a$ is well defined.

Again, $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$ -- {cancelli law}

$\Rightarrow f_a$ is one-one.

Also, for any $y \in G$, since $f_a(a^{-1}y)$

$= a.(a^{-1}y)$

$= (aa^{-1}).y$ ... associativity

$= ey = y$

we find $a^{-1}y$ is pre-image of y or that f_a is onto and hence a permutation on G.

thus $f_a \in A(G)$.

Scanned with CamScanner

let K be the set of all such permutations. We show K is a subgroup of $A(G)$.

$K \neq \phi$ as $f_e \in K$

let $f_a, f_b \in K$ be any numbers

then Since

$$f_b \circ f_{b^{-1}}(x) = f_b(f_{b^{-1}}(x))$$

$$= f_b(b^{-1}x) = b(b^{-1}x)$$

$$= ex = f_e(x) \text{ for all } x$$

we find

$$f_{b^{-1}} = (f_b)^{-1} \quad \text{--} \{ f_e = I \text{ of } A(G)$$

Also as

$$(f_a \circ f_b)x = f_a(bx) = a(bx)$$

$$= (ab)x$$

$$= f_{ab}(x) \quad \forall x$$

we find

~~fao~~ ~~ff~~

$$f_{ab} = f_a \circ f_b$$

now

$$f_a \circ (f_b)^{-1} = f_a \circ f_{b^{-1}}$$

$$= f_{ab^{-1}} \in K$$

$\therefore$ K is subgroup of $A(G)$.

Scanned with CamScanner

Define now a mapping
$\phi: G \to K \ni$
$\phi(a) = f_a$

then ϕ is well defined, 1-1 map as
$a = b$
$\Leftrightarrow ax = bx$
$\Leftrightarrow f_a(x) = f_b(x)$
$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \phi(a) = \phi(b)$
$\forall f_a \in K \ \exists a \in G$
$\ni \phi(a) = f_a$
$\therefore \phi$ is onto.

$\phi(ab) = f_{ab} = f_a \circ f_b$
$= \phi(a) \cdot \phi(b)$
ϕ is homomorphism and hence Isomorphism which proves our assertion.
$\therefore$ K is subgroup of a permutation group is a permutation group.
Hence proved.

Scanned with CamScanner

Q1. If F is a Field, then F[x] is a Euclidean domain.

Solⁿ:- F is Field ⇒

~~Suppose~~ F is an integral domain

let $f(x), g(x)$ be any two non zero members of $F[x]$. ∃

$$f(x) \cdot g(x) = 0$$

where $f(x) = a_0 + a_1 x + \cdots + a_m x^m$

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$

now both $f(x)$ and $g(x)$ can not be constant polynomial as then

$$a_0 \neq 0 , b_0 \neq 0$$

so $c_0 = a_0 \cdot b_0 \neq 0$

$\therefore f(x) g(x) \neq 0$

Since at least one of $f(x)$ and $g(x)$ ~~can not be~~ constant is non constant polynomial it's degree is ≥ 1

F being an integral domain

$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x) \geq 1$

which is a contradiction as it implies then $c_k \neq 0$ for some $k > 0$

where as $f(x) \cdot g(x) = 0$

hence $f(x) \cdot g(x) = 0$

$\Rightarrow f(x) = 0$ or $g(x) = 0$

⇒ F[x] is integral domain.

$f(x) = 1 + 0x + 0x^2 + \cdots$ is unity of $F[x]$.

∴ F[x] is an integral domain with unity.

For any $f(x) \in F[x]$, $f(x) \neq 0$

define

$d(f(x)) = \deg f(x)$ which is non-neg Integer

Since for any
$f(x), g(x) \in F[x]$, $f(x) \neq 0, g(x) \neq 0$

$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$

we get $\deg(f(x)) \leq \deg(f(x) \cdot g(x))$
as $\deg(g(x)) \geq 0$
$d(f(x)) \leq d(f(x)g(x))$

lastly we show for any non-zero $f(x), g(x)$ in $F[x]$, $\exists$ $q(x)$ and $r(x)$ in $F[x]$ $\ni$

$f(x) = q(x)g(x) + r(x)$
where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

If $\deg f(x) < \deg g(x)$
then $f(x) = 0 \cdot g(x) + f(x)$ gives the result.
Assume now the result is true for all (non zero) polynomials in $F[x]$ of deg less then $\deg f(x)$.

let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$

suppose $\deg f(x) \geq \deg g(x)$
~~the~~
Define $f_1(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$

then coefficient of x^m in $f_1(x)$ is
$a_m - a_m b_n^{-1} b_n = a_m - a_m = 0$

thus either $f_1(x) = 0$ (zero polynomial)
or $\deg f_1(x) < m$
If $f_1(x) = 0$ then

$0 = f(x) - a_m b_n^{-1} x^{m-n} g(x)$
gives $f(x) = a_m b_n^{-1} x^{m-n} g(x) + 0$
So by taking
$q(x) = a_m b_n^{-1} x^{m-n}$
and $r(x) = 0$
we get required result.
suppose $f_1(x) \neq 0$
then $\deg f_1(x) < m$
i.e. $\deg f_1(x) < \deg f(x)$
by induction hypothesis
$f_1(x) = q_1(x) g(x) + r(x)$
where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$\therefore f(x) - a_m b_n^{-1} x^{m-n} g(x) = q_1(x) \cdot g(x) + r(x)$

or $f(x) = [a_m b_n^{-1} x^{m-n} + q_1(x)] g(x) + r(x)$

$= q(x) \cdot g(x) + r(x)$
where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$
and hence $F[x]$ is a
Euclidean domain.

Euclidean domain:-

In integral domain R is called a Euclidean domain or Euclidean ring if for all $a \in R$ $a \neq 0$ there is defined a non-ve integer $d(a)$ $\ni$

(i) for all $a, b \in R$, $a \neq 0$, $b \neq 0$

$$d(a) \leq d(a b)$$

ii) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $\exists$ q and r in R $\ni$

$$a = tb + r$$

where either $r = 0$ or $d(r) < d(b)$.

eg:- $\langle \mathbb{Z}, +, \cdot \rangle$

$d(a) = |a|$

$d(a)$ is non-ve integer

Q-3) a] Show that the Group $\mathbb{Z}_5 \times \mathbb{Z}_7$ and $\mathbb{Z}_{35}$ are ~~an~~ isomorphic. (15)

<u>Sol^n:-</u> First of all we have to show that $\mathbb{Z}_5 \times \mathbb{Z}_7$ is cyclic group.

$\because (5,7)=1$

we will show that $\mathbb{Z}_5 \times \mathbb{Z}_7 = \langle 1,1 \rangle$

and $o(1,1) = 35 = |\mathbb{Z}_5 \times \mathbb{Z}_7|$

$\mathbb{Z}_5 = \langle 1 \rangle$, $\mathbb{Z}_7 = \langle 1 \rangle$

consider $(1,1)^{35}$

$$= (1,1)^{5\times 7}$$

$$= (1^{5\cdot 7}, 1^{5\cdot 7})$$

$$= ((1^5)^7, (1^7)^5)$$

$$= (0^7, 0^5) \quad \text{--} \left\{ \begin{array}{l} 1^5 = 1+1+1+1+1 \\ \quad = 0 \text{ in } \mathbb{Z}_5 \end{array} \right\}$$

$$= (0,0)$$

$$= \text{identity of } \mathbb{Z}_5 \times \mathbb{Z}_7 .$$

let $(1,1)^r = (0,0)$

$\Rightarrow (1^r, 1^r) = (0,0)$

$\Rightarrow \cancel{o(1)} = 1^r = 0, \quad 1^r = 0$

$\Rightarrow o(1) = 5 / r \qquad o(1) = 7/r$

$\Rightarrow 5\cdot 7 / r$, as $(m,n)=1$

$\Rightarrow 5\cdot 7 \le r$

$\Rightarrow 35 \le r$

$\therefore o(1,1) = 35 = o(\mathbb{Z}_5 \times \mathbb{Z}_7)$

hence $\mathbb{Z}_5 \times \mathbb{Z}_7 = \langle (1,1) \rangle$

we know any ~~two~~ cyclic group of order n is always isomorphic to $\mathbb{Z}_n$. Given by mapping,

$$\cancel{\phi : \mathbb{Z}_5 \times \mathbb{Z}_7 \to \mathbb{Z}_{35}}$$
$$\cancel{\phi[(1,1)^r] = r}$$

$$\phi : \mathbb{Z}_{35} \to \mathbb{Z}_5 \times \mathbb{Z}_7$$
$$\phi(r) = (1,1)^r$$

let $r = s$

$$\Leftrightarrow (1,1)^r = (1,1)^s$$
$$\Leftrightarrow \phi(r) = \phi(s).$$

$\forall$ $(x,y) \in \mathbb{Z}_5 \times \mathbb{Z}_7$

$$(x,y) = (1,1)^r$$

$\therefore$ $\forall$ $(x,y) \in \mathbb{Z}_5 \times \mathbb{Z}_7$ $\exists r \in \mathbb{Z}_{37}$ $\ni f(r) = (1,1)^r$

$\therefore$ f is onto.

$$\phi(r+s) = (1,1)^{r+s}$$
$$= (1,1)^r \cdot (1,1)^s$$
$$= \phi(r) \cdot \phi(s).$$

$\therefore$ ϕ is homomorphism

$\therefore$ ϕ is isomorphism.