IFOS - 2016

Date / /

① Prove that the set of all bijective function from a non-empty set X onto itself is a group with respect to usual composition of functions. (8)

Sol:- Let f, g be any two elements of A(X). Then f and g are both one-to-one mapping of X onto itself. By the defination of composite of two function f and g denoted by $fg: X \to X$ given by

$$(fg)(x) = f[g(x)] \quad \forall x \in X$$

Closure property:-

We know that If f, g are two bijective mapping of X onto itself then the composite mapping fg is also bijective on X.

$\therefore fg \in A(X) \quad \forall \; f, g \in A(X)$

Associativity:-

Let f, g and h be any three elements of A(X). then (fg)h and f(gh) are both bijective mapping on X.

We have

$$[(fg)h]x = (fg)[h(x)]$$
$$= f[g(h(x))]$$
$$= f[(gh)(x)]$$
$$= [f(gh)](x)$$

$\therefore (fg)h = f(gh)$ by def^n of equality of mapping

Existence of identity:- let e be the identity function on X. i.e. $e(x) = x \quad \forall x \in X$.

$\therefore e$ is bijective

$\Rightarrow e \in A(X)$.

if $f \in A(X)$ then $\forall x \in X$

we have $(ef)(x) = e[f(x)]$.

$= f(x)$

$\therefore ef = f$

thus e is identity element.

Existence of inverse:-

let $f \in A(X)$. then f is one-one and onto.

let $y \in X$ be arbitary. $\Rightarrow \exists\ x \in X \ni$

$f(x) = y$ also x is unique $\because f$ is one-one

now define a mapping

$f^{-1} : X \to X \ni$

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

$\therefore f^{-1}$ is bijective

$\therefore f^{-1} \in A(X)$.

$\therefore [f^{-1}f](x) = f^{-1}[f(x)] = f^{-1}(y) = x$

$\therefore f^{-1}f$ is identity mapping of X

$\therefore f^{-1}f = e$

$\therefore A(X)$ which is set of all bijective mapping on X is Group

5) Show that any non abelian Group of order 6 is isomorphic to Symmetric group S_3. (15)

Sol:- by lagrange's theorem
we know $\forall a \in G$, $o(a) / o(G)$.
∴ for a non-abelian Group G. where $o(G) = 6$ the possible order of elements are 1, 2, 3, and 6.
only identity element $e \in G$ has order 1
if G has element of order 6 then it is cyclic hence abelian ∴ contradiction
∴ G has in G order of every non-identity element is either 2 or 3.

Suppose $\forall a \in G$, $o(a) = 2$
then G will be abelian
∴ G must have $a \in G$ for which $o(a) = 3$.
let G have an element a
∋ $o(a) = 3$
let $b \notin \langle a \rangle$ then order of $\langle a \rangle \cap \langle b \rangle = 1$
else if $o(\langle a \rangle \cap \langle b \rangle) = 3$
then $\langle a \rangle = \langle b \rangle$ ∴ $o(a) = 3$
but $b \notin \langle a \rangle$
∴ $o(\langle a \rangle \cap \langle b \rangle) = 1$

Suppose $o(b) = 3$

$\therefore |\langle a \rangle \cap \langle b \rangle| = 1$

$\Rightarrow |\langle a \rangle \langle b \rangle| = 9$

which is contradict^{n}.

$\therefore o(b) = 2$

The six elements of G_1 are

e, a, a^2, b, ba, ba^2

as $G_1 = \langle a \rangle \cup b\langle a \rangle$

the product ab must be one of the elements above.

ab can not be e as $b \notin \langle a \rangle$

ab can not be a as $b \neq e$.

ab can not be a^2 as $b \neq a$

ab can not be b as $a \neq e$

ab can not be ba as then all the elements of G_1 will commute.

$\therefore$ only possibility is

$ab = ba^2$

$\therefore G_1$ has generator a, b with relation $a^3 = e, b^2 = e, ab = ba^2$.

$\therefore$ any map from $G_1 \to S_3$ which maps a to 3-cycle and b to a 2-cycle would be an isomorphism.

6] Let G be a group of order pq, where p and q are prime nb. ∋ p > q, and q ∤ (p-1). then prove G is cyclic. (18)

:- Note:-

1] Let G and H be finite cyclic groups. Then G ⊕ H is cyclic iff |G| and |H| are relatively prime.

2] If a Group G is the internal direct product of a finite number of subgroup $H_1, H_2, \dots H_n$ then $G \cong H_1 \oplus H_2 \oplus \dots \oplus H_n$.

i.e. $H_1 \times H_2 \times \dots \times H_n \cong H_1 \oplus H_2 \oplus \dots \oplus H_n$

:- We are Given that $o(G) = pq$

p and q are prime and $p > q$ and $q \nmid p-1$

∵ p is prime $p \mid o(G)$

$p^2 \nmid o(G)$

Here G has a sylow-p subgroup of order p.

no. of sylow p-subgroup is $1+kp \mid o(G)$

$\Rightarrow 1+kp \mid q$

Here $k=0$ is only possibility because if $k=1$ then $1+p \mid q$

but $p > q$

∴ contradiction

∴ Sylow-p subgroup is unique hence normal subgroup of G.

Similarly q is prime
$q \mid o(G)$
$q^2 \nmid o(G)$
$\therefore$ G has q-sylow subgroup of order q.
no. of sylow q subgroup is $1+kq \mid o(G)$
$\therefore 1+kq \mid p$
If $k=0$ then sylow-q subgroup is normal if $k \neq 0$
$\Rightarrow$ ~~$1+kq = \epsilon$~~
~~$p = (1+kq)t$~~
$\Rightarrow p = 1+kq$ ... $\because p$ is prime.
$\Rightarrow p-1 = kq$
$\therefore$ q divides $p-1$
again contradiction
$\therefore$ sylow-q subgroup is normal.
Let $o(H)=p$ where H is Sylow p-subgroup
$o(K)=q$ where K is Sylow q-subgroup.
since H and K both are normal in G
and $o(H \cap K) = 1 = (p,q)$
$\Rightarrow H \cap K = \{e\}$
Let $H = \langle a \rangle \quad K = \langle y \rangle$
consider $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1}$
$= y_1 y^{-1}$ --- $\{\because K$ is normal in G
$\in K$ $\quad -y_1 \in K\}$ $\quad \therefore xyx^{-1} \in K\}$
$xyx^{-1}y^{-1} \in K$ -- $\{\because y_1 \in K, y^{-1} \in K \therefore y_1 y^{-1} \in K\}$

$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1})$
$= x x_2$ --- $x_2 \in H - \{H \text{ is } \triangleright G$
$= x_3$ $\quad -x_3 \in H \cdot \{H$ is Subgp
$\therefore xyx^{-1}y^{-1} \in H$

$\therefore xyx^{-1}y^{-1} \in HOK$

but $HOK = \{e\}$

$\therefore xyx^{-1}y^{-1} = e$ $\quad x \in H, y \in K$

$xy = yx$ $\quad \forall x, y \in G$

$\therefore o(xy) = o(x) \cdot o(y) = pq$

$\therefore G = \langle xy \rangle$ is cyclic.

2] Show that in the ring $R = \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$ the elements $\alpha = 3$ and $\beta = 1+2\sqrt{-5}$ are relatively prime, but $\alpha\beta$ and β^2 have no g.c.d in R where $\gamma = \pm(1+2\sqrt{-5})$ --- (10)

Sol? Defn:- G.C.D:- If $a,b \in R$ then an element $d \in R$ is called greatest common divisor of a and b if

i) $d \mid a$, $d \mid b$

ii) whenever $c \mid a$, $c \mid b$ then $c \mid d$

$\Rightarrow$ let $a+b\sqrt{-5}$ is g.c.d of 3 and $1+2\sqrt{-5}$

$\therefore a+b\sqrt{-5} \mid 3$ and $a+b\sqrt{-5} \mid 1+2\sqrt{-5}$

now $a+b\sqrt{-5} \mid 3$

$\Rightarrow \exists\ c+d\sqrt{-5} \in \{a+b\sqrt{-5}\}$

$\ni\ 3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$

taking conjugate

$\bar{3} = (a-b\sqrt{-5})(c-d\sqrt{-5})$

$\therefore 3\cdot\bar{3} = 9 = (a+b\sqrt{-5})(a-b\sqrt{-5})(c+d\sqrt{-5})(c-d\sqrt{-5})$

$\therefore 9 = (a^2+5b^2)(c^2+5d^2)$ --- $\{a+b\sqrt{-5} = 9 \Rightarrow b\sqrt{-5}i$

this is possible if

$a^2+5b^2 = 1$ and $c^2+5d^2 = 9$ --- (1)

or $a^2+5b^2 = 9$ and $c^2+5d^2 = 1$ --- (2)

or $a^2+5b^2 = 3$ and $c^2+5d^2 = 3$

but $a^2+5b^2 \neq 3$ because $a,b \in \mathbb{Z}$

$\therefore a^2+5b^2 = 1$ and $c^2+5d^2 = 9$

$\Rightarrow a = \pm 1$ and $b = 0$ and $c = \pm 3$, $d = 0$ --- (3)

similarly by (2)

$a = \pm 3$ and $b = 0$ and $c = \pm 1$, $d = 0$ (4)

$a+b\sqrt{-5} \mid 1+2\sqrt{-5}$

$\Rightarrow 1+2\sqrt{-5} = (a+b\sqrt{-5})(e+f\sqrt{-5})$

$1-2\sqrt{-5} = (a-b\sqrt{-5})(e-f\sqrt{-5})$

$\therefore 1+4(5) = (a^2+5b^2)(e^2+5f^2)$

$21 = (a^2+5b^2)(e^2+5f^2)$

possible choices $\quad 1 \quad\quad 21$

$21 \quad\quad 1$

$\therefore \quad a^2+5b^2 = 21 \quad\quad e^2+5f^2 = 1$

or $\quad a^2+5b^2 = 1 \quad\quad e^2+5f^2 = 21$

$\therefore$ Choices for $a+bi = 1 \pm 2\sqrt{-5}, -1 \pm 2\sqrt{-5}$

or $a = \pm 1, \; b = 0$

but from (4) $a \neq 1 \pm 2\sqrt{-5}$ or $-1 \pm 2\sqrt{-5}$

$\therefore \quad a \pm bi = 1 \pm 0 = 1$

$\therefore \gcd(3, 1+2\sqrt{-5}) = 1$

hence relatively prime.

$\alpha = 3, \quad \gamma = 7(1+2\sqrt{-5}) \Rightarrow \alpha\gamma = 21(1+2\sqrt{-5})$

$\beta = 1+2\sqrt{-5} \cdot \quad \gamma = 7(1+2\sqrt{-5})$

$\beta\gamma = (1+2\sqrt{-5})(7(1+2\sqrt{-5}))$

$= 7+2\sqrt{-5}+14\sqrt{-5}+20$

$\beta\gamma = 27+16\sqrt{-5}$

$\beta\gamma = 7(21)$

$\alpha\gamma = 21(1+2\sqrt{-5})$

$\beta\gamma = 7(1+2\sqrt{-5})(1+2\sqrt{-5})$

$= 7(1+2\sqrt{-5}+2\sqrt{-5}+4\times 5(-1))$

$= 7(1+4\sqrt{-5}-20)$

$= 7(-19+4\sqrt{-5})$

∴ we can see that
7 divides both $\alpha\nu$ and $\beta\nu$
also $1+2\sqrt{-5}$ divides
both $\alpha\nu$ and $\beta\nu$
but $1+2\sqrt{-5} \nmid 7$

∴ there is no g.c.d.