(IFOS - 2011)

Q-3) a) If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for some $a, b \in G$ find order of b. (10)

Sol^n:- Given $a^5 = e$

$$aba^{-1} = b^2$$

or $b^2 = aba^{-1}$

$$b^4 = b^2 \cdot b^2$$
$$= (aba^{-1})(aba^{-1})$$
$$= ab(a^{-1}a)(ba^{-1})$$
$$= ab\,e\,ba^{-1}$$
$$b^4 = ab^2a^{-1} = a\,aba^{-1}a^{-1} = a^2ba^{-2}$$
$$b^8 = b^4 \cdot b^4 = \cancel{ab^2}\ a^2ba^{-2}a^2ba^{-2}$$
$$= a^2b^2a^{-2}$$
$$b^8 = a^2aba^{-1}a^{-2}$$
$$b^8 = a^3ba^{-3}$$
$$b^{16} = b^8 \cdot b^8$$
$$= a^3ba^{-3} \cdot a^3ba^{-3}$$
$$= a^3b^2a^{-3}$$
$$= a^3aba^{-1}a^{-3}$$
$$b^{16} = a^4ba^{-4}$$
$$b^{32} = b^{16} \cdot b^{16} =$$
$$a^4 \cdot ba^{-4} \cdot a^4 \cdot ba^{-4}$$
$$= a^4 \cdot b^2a^{-4}$$
$$= a^4 \cdot aba^{-1}a^{-4}$$
$$= a^5 \cdot ba^{-5}$$
$$= ebe$$
$$\therefore b^{32} = b$$
$$\therefore b^{31} = e$$
$$\therefore o(b) = 31$$

same question was asked in IFOS 2011 just $Q(\sqrt{2}) = \{a+b\sqrt{2}\}$

1) Prove that the set $Q(\sqrt{5}) = \{a+b\sqrt{5}; a,b \in Q\}$ is commutative ring with identity. (15)

[IAS-2014]

Ring:-

A non-ϕ set R, together with two binary compositions + and $\cdot$ is said to form a Ring if the following axioms are satisfied.

(1) $a+(b+c) = (a+b)+c \quad \forall a,b,c \in R$

2) $a+b = b+a$ for $a,b \in R$

3) $\exists$ some element 0 in R $\ni a+0 = 0+a = a$ for all $a \in R$

4] For each $a \in R$ $\exists$ an element $(-a) \in R \ni a+(-a) = (-a)+a = 0$

5] $a.(b.c) = (a.b).c$ for all $a,b,c \in R$

6] $a.(b+c) = a.b + a.c$

7) $a.b = b.a$ -- commutative.

$x = a+b\sqrt{5}$, $a,b \in Q$
$y = c+d\sqrt{5}$, $c,d \in Q$

$x+y = (a+c)+(b+d)\sqrt{5}$
$a+c \in Q$ $\quad b+d \in Q$

$\therefore x+y \in Q\sqrt{5}$

$\therefore$ closure property holds.

$\Rightarrow (a+b\sqrt{5}) + (p+c\sqrt{5} + d+e\sqrt{5})$

$= (a+b\sqrt{5})(p+d + (c+e)\sqrt{5})$

$= (a+p+d) + (b+c+e)\sqrt{5}$

$= (a+p+(b+c)\sqrt{5}) + (d+e\sqrt{5})$

$= ((a+b\sqrt{5}) + p+c\sqrt{5}) + (d+e\sqrt{5})$

$\therefore$ associativity holds.

$\Rightarrow$ let $c+d\sqrt{5} \in Q$

$c = d = 0$

$\therefore$ 0 is additive identity.

$\Rightarrow$ let $x = a+b\sqrt{5} \in Q\sqrt{5}$ additive.

$c+d\sqrt{5}$ is inverse of x

$\therefore a+b\sqrt{5} + c+d\sqrt{5} = 0$

$\therefore (a+c) + (b+d)\sqrt{5} = 0+0\sqrt{5}$

$\therefore a+c=0 \quad b+d=0$

$\therefore c=-a, \; d=-b$

$\therefore -a-b\sqrt{5}$ is additive inver

$\Rightarrow x = a+b\sqrt{5}, \quad y = c+d\sqrt{5}$

$x \cdot y = (a+b\sqrt{5})(c+d\sqrt{5})$

$= ac + ad\sqrt{5} + bc\sqrt{5} + 5bd$

$= (ac+5bd) + (ad+bc)\sqrt{5}$

$\in Q(\sqrt{5})$

hence closure hold.

Scanned with CamScanner

$\Rightarrow \quad x = a+b\sqrt{5} \qquad y = c+d\sqrt{5} \qquad z = e+f\sqrt{5}$

$x \cdot (y \cdot z)$

$= (a+b\sqrt{5})((c+d\sqrt{5}) \cdot (e+f\sqrt{5}))$

$= (a+b\sqrt{5}) \cdot (ce + 5fd + \sqrt{5}(cf+ed))$

$= ace + 5afd + 5bcf + 5bed$

$\quad + \sqrt{5}(acf + aed + \underline{bce} + 5bfd)$ *

$(x \cdot y) \cdot z$

$= ((a+b\sqrt{5}) \cdot (c+d\sqrt{5})) (e+f\sqrt{5})$

$= (ac + 5bd + \sqrt{5}(ad+bc)$

$\quad + \quad (e+f\sqrt{5})$

$= (ace + 5bde + 5adf + 5bcf$

$\quad + \sqrt{5}(acf + 5bdf + ade + bce)$

associativity. holds.

$\Rightarrow (a+b\sqrt{5})(c+d\sqrt{5} + e+f\sqrt{5})$

$= (a+b\sqrt{5})((c+e) + (d+f)\sqrt{5})$

$= (a+b\sqrt{5})(c+e) + (a+b\sqrt{5})(d+f)\sqrt{5}$

$= ac + ae + bc\sqrt{5} + be\sqrt{5}$

$+ (ad+df)\sqrt{5} + (bd+bf)5$

$= ac + 5bd + \sqrt{5}(ad+bc)$

$\quad + ae + 5bf + \sqrt{5}(af+be)$

$= (a+b\sqrt{5})(c+d\sqrt{5}) + (a+b\sqrt{5})(e+f\sqrt{5})$

Scanned with CamScanner

$\Rightarrow$ $(a+b\sqrt{5})\,(c+d\sqrt{5})$
$= ac+bd5 + \sqrt{5}(ad+bc)$
$= ca+5db + \sqrt{5}(da+cb)$
$= (c+d\sqrt{5})\,(a+b\sqrt{5})$

Here commutative.

let $x = a+b\sqrt{5}$ is arbitrary element of $Q(\sqrt{5})\setminus\{0\}$
$y = c+d\sqrt{5}$ is multiplicative identity.

$x \cdot y = x$
$(a+b\sqrt{5})\,(c+d\sqrt{5}) = a+b\sqrt{5}$
$(ac+5bd) + (ad+bc)\sqrt{5} = a+b\sqrt{5}$

$\Rightarrow ac+5bd = a$
$ad+bc = b$
$a(c-1)+5bd = 0$ $\quad\quad$ $b(c-1)+ad=0$
$c-1 = -\dfrac{5bd}{a} = -\dfrac{ad}{b}$
$\Rightarrow 5b^2d = a^2d$
$d(5b^2-a^2)=0$
$5b^2 \neq a^2$
$\therefore d=0$
$a(c-1)+5b0=0$
$a(c-1)=0$
$a\neq 0 \;\therefore c=1$
$\therefore$ identity $=1$ exist.

Scanned with CamScanner

3) let G be group of non-zero complex number under multiplication, and let N be the set of complex number of absolute value 1. Show that $\frac{G}{N}$ is isomorphic to the group of all positive real no. under multiplich.

(13)

Solⁿ:- Define $\phi: G \to R^+$ by
$$\phi(a+ib) = a^2+b^2$$
clearly ϕ is onto.

consider,
$$\phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i)$$
$$= (ac-bd)^2 + (ad+bc)^2$$
$$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2$$
$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$
$$= a^2(c^2+d^2) + b^2(c^2+d^2)$$
$$= (a^2+b^2)(c^2+d^2)$$
$$= \phi(a+bi)\,\phi(c+di)$$

$\therefore$ ϕ is onto homomorphism.

$\ker\phi = \{x \in G : \phi(x) = 1\}$

$\therefore$ $a+bi \in G$: $a^2+b^2 = 1$

$\therefore$ $\ker\phi = N$

$\therefore$ $\frac{G}{N} \cong R^+$

by first theorem on homomorphism.

(b) let G be a Group of order $2p$, p is prime. show that either G is cyclic or G is generated by $\{a, b\}$ with relations
$a^p = e = b^2$
and $bab = a^{-1}$ (13)

Sol^n: let $o(G) = 2p$, p is prime.

$\therefore$ by lagrange's theorem
$\forall a \in G$ $o(a) \mid o(G)$

$\therefore$ possible order of a are, 1, 2, p and $2p$

if $\exists a \in G \ni$ ~~o~~ $o(a) = 2p$
then $G = \langle a \rangle$
$\Rightarrow G$ is cyclic.

we know that only identity $e \in G$ has order 1.

$\therefore$ if G is not cyclic
then possible orders are 2 and p.

assume that ~~$\forall a \in G$~~ $a \neq e$ $o(a) = 2$
$\therefore$ G is abelian — (1)
let $a, b \in G$ $a \neq b$
$o(a) = 2$ $o(b) = 2$
let $H = \langle a \rangle$, $K = \langle b \rangle$
$\therefore$ HK is subgroup, $\because HK = KH$ — $\{G$ is abelian from (1)$\}$

& $H \cap K = \{e\}$ — $\{\because a \neq b\}$

$$\therefore \quad o(HK) = \frac{o(H)\cdot o(K)}{o(H\cap K)}$$

$$= \frac{2\cdot 2}{1} = 4$$

$\therefore$ HK is Subgroup having order 4
it is contradiction by
~~but~~ ~~to~~ lagrange's theorem

$\therefore \exists$ an element $a \in G \ni a^P = e$

let $b \notin \langle a \rangle$
we claim $o(b) = 2$
if not then $o(b) = P$
and $\langle a \rangle \cap \langle b \rangle = \{e\}$ --{$\because b \notin \langle a \rangle$

$$\therefore \quad o(ab) = \frac{o(\langle a \rangle)\, o(\langle b \rangle)}{\langle a \rangle \cap \langle b \rangle}$$

$$= \frac{P\cdot P}{e} = P^2$$

but $P^2 \nmid 2P$

$\therefore \quad o(b) = 2$
$\therefore$ G is Generated by $a^P = e$, $b^2 = e$ i.e.
$e, a, a^2, \ldots a^{P-1}, b, ba, ba^2, \ldots ba^{P-1}$

consider ab. $\because ab \notin \langle a \rangle$
$\therefore |ab| = 2$

Scanned with CamScanner