(1)

1 a) True

Theorem : A non empty subset H of the group G is a subgroup of G iff

(i) $a, b \in H$ implies $a * b \in H$

(ii) $a \in H$ implies $a^{-1} \in H$

$\Rightarrow \{e\}$ is a subset of G.

$\Rightarrow e \in H$ implies $e * e \in H$ [Closure property is satisfied since $e \in G$]

$\Rightarrow$ The inverse of e is 'e' itself. $e^{-1} \in H$.

$\Rightarrow \therefore \{e\}$ is subgroup of G (½ Marks)

b) True

Theorem : A non empty subset H of the group G is a subgroup of G iff

(i) $a, b \in H$ implies $a * b \in H$.

(ii) $a \in H$ implies $a^{-1} \in H$.

$\Rightarrow G$ is a subset of $(G, *)$.

$\Rightarrow a, b \in G$ implies $a * b \in G$ [Closure property is satisfied since $a, b \in G$].

$\Rightarrow$ For each $a \in G$, we have $a^{-1} \in G$ [since $a \in G$]

$\Rightarrow \therefore G$ is a subgroup of G. (½ Mark)

(1 Mark)

2) False

⇒ Assume that Z_{10} is a field under addition and multiplication modulo 10.

⇒ This implies that Z_{10} is a commutative group under multiplication modulo 10.

⇒ For Z_{10} to be a commutative group

1) For all $a, b \in Z_{10}$ $(a \times b) \bmod 10 = (b \times a) \bmod 10$.

2) For all $a, b \in Z_{10}$ $(a \times b) \bmod 10 \in Z_{10}$.

3) For all $a, b, c \in Z_{10}$,
$[(a \times b) \times c] \bmod 10 = [a \times (b \times c)] \bmod 10$.

4) There should exist an $e \in Z_{10}$ such that $(a \times e) \bmod 10 = a$ for all $a \in Z_{10}$

5) There should exist an $a^{-1} \in Z_{10}$ for all $a \in Z_{10}$ such that $(a \times a^{-1}) \bmod 10 = e$.

⇒ $(a \times a^{-1}) \bmod 10 = e = 1$.

⇒ For a^{-1} to exist $(a, 10) = 1$ for all $a \in Z_{10}$.

⇒ But $(a, 10) \neq 1$ for all $a \in Z_{10}$. ∴ Inverse element is not existing for all elements of Z_{10}.

∴ It's not a group under multiplication modulo 10.

This contradicts the assumption that Z_{10} is a field under addition and multiplication modulo 10.

3) Let $(R, +, *)$ be a ring.

⇒ Cancellation laws of multiplication.

I $a*b = a*c$ implies $b=c$.

II $b*a = c*a$ implies $b=c$.

⇒ We can prove that cancellation laws of multiplication will hold in ring's iff there exists an identity element 'u' and an inverse element for each element $a \in R$ w.r.t to the IInd binary operation in rings.

Proof

I $a*b = a*c$.

$\Rightarrow a^{-1}*(a*b) = a^{-1}*(a*c)$

$\Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c$ [Since associativity holds]

$\Rightarrow u*b = u*c$

$b = c$ [since u is the identity element]

Proof

II $b*a = c*a$.

$(b*a)*a^{-1} = (c*a)*a^{-1}$

$b*(a*a^{-1}) = c*(a*a^{-1})$ [Since associativity holds]

$b*u = c*u$

$b = c$. [Since u is the identity element]

⇒ The proof will stand iff we can guarantee the existence of identity element and inverse w.r.t to the IInd binary operation in rings.

4) Let $(G, *)$ be a group

Let S be any collection of subgroup's H_α of G.

Let $S = \{ H_\alpha \setminus \alpha = 1, 2 \ldots\ldots k$ and H_α is a subgroup of $G \}$

where k is the order of G.

$\Rightarrow$ Each H_α is a subgroup.

$\Rightarrow e \in H_\alpha$ for all H_α

$\Rightarrow \therefore e \in \bigcap_{\alpha=1}^{k} H_\alpha$

$\therefore \bigcap_{\alpha=1}^{k} H_\alpha \neq \phi$ (1 Mark)

<u>Theorem</u> : A non empty finite subset of a group G is a subgroup of G, if its closed under the binary operation in G.

$\Rightarrow$ Next we have to prove that $\bigcap_{\alpha=1}^{k} H_\alpha$ is

closed under the binary operation $*$.

$\Rightarrow$ Let $a, b \in \bigcap_{\alpha=1}^{k} H_\alpha$

$\Rightarrow$ Let $a * b = c$

$\Rightarrow$ Then $c \in H_\alpha$ for all H_α [From defn of subgroup's]

$$\Rightarrow c \in \bigcap_{\alpha=1}^{k} H_\alpha$$

$\Rightarrow \therefore \bigcap_{\alpha=1}^{k} H_\alpha$ is closed under the operation $*$.

$\Rightarrow \bigcap_{\alpha=1}^{k} H_\alpha$ is a subgroup of G.

5

5. $G = \langle a \rangle$, $\operatorname{ord}(G) = 30$.

a) $o(a) = o(G) = 30$. (1 Mark)

$\therefore a^{30} = e$.

$\therefore (a^5)^6 = e$.

$\therefore o(a^5) = 6$.

$\therefore \langle a^5 \rangle = \{ (a^5)^0, (a^5)^1, (a^5)^2, (a^5)^3, (a^5)^4, (a^5)^5 \}$

$= \{ e, a^5, a^{10}, a^{15}, a^{20}, a^{25} \}$

b) $a^{30} = e$. (1 Mark)

$\therefore (a^6)^5 = e$.

$\therefore o(a^6) = 5$.

$\therefore \langle a^6 \rangle = \{ (a^6)^0, (a^6)^1, (a^6)^2, (a^6)^3, (a^6)^4 \}$

$= \{ e, a^6, a^{12}, a^{18}, a^{24} \}$

(B)

6. Theorem : Multiplicative group's are cyclic iff $n = 1, 2, 4, p^\alpha$ or $2p^\alpha$ where p is an odd prime.

$\therefore$ Z_{19}^* is cyclic since n is of the form p^α.

$\Rightarrow \phi(19) = 18$.

No: of generators $= \phi(\phi(n)) = \phi(\phi(18))$

$= 6$.

$\Rightarrow q = 2, 3$ [Primes dividing $\phi(n)$]

$\Rightarrow a^{\phi(n)/q} \bmod n \neq 1$.

$\rightarrow a^9 \bmod 19 \neq 1$ $\quad a^6 \bmod 19 \neq 1$.

$Z_{19}^* = \{1, 2, \ldots\ldots 18\}$.

$2^9 \bmod 19 \neq 1$ $\quad 2^6 \bmod 19 \neq 1$.

$\therefore$ one of the generators is 2. (1 Mark)

$a^i \bmod n$ will generate next primitive roots where $2 < i < n-1$ and $\gcd(i, n-1) = 1$.

$i = 5, 7, 11, 13, 17$.

$2^5 \bmod 19 = 13$.

$2^7 \bmod 19 = 14$

$2^{11} \bmod 19 = 15$.

$2^{13} \bmod 19 = 3$

$2^{17} \bmod 19 = 10.$ (1 Mark)

generators = $\{2, \cancel{\ }\ 3, 10, 13, 14, 15\}$

7) $Z_4 = \{0, 1, 2, 3\}$.

$Z_{10}^* = \{1, 3, 7, 9\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

x	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\Rightarrow$ Two groups are isomorphic if there is one to one correspondence between the elements of groups.

$0 \in Z_4 \iff 1 \in Z_{10}^*$.

$1 \in Z_4 \iff 3 \in Z_{10}^*$.

$2 \in Z_4 \iff 9 \in Z_{10}^*$.

$3 \in Z_4 \iff 7 \in Z_{10}^*$.

$\therefore Z_4$ & Z_{10}^* are isomorphic.

(2 Marks)

8) Let $(G, *)$ be such a group.

Let $\forall\, a, b \in G \quad (a*b)^n = a^n * b^n \quad (1)$

$$(a*b)^{n+1} = a^{n+1} * b^{n+1} \quad (2)$$

$$(a*b)^{n+2} = a^{n+2} * b^{n+2} \quad (3)$$

(In the explanation, $*$ is termed multiplication for clarity of writing)

$(a*b)^{n+1} = a^{n+1} * b^{n+1}$ — by (2)

$\Rightarrow (a*b)^n (a*b) = a^{n+1} * b^{n+1}$ — definition

$\Rightarrow a^n * b^n * a * b = a^n * a * b^n * b$ — by (1) & definition

$\Rightarrow (a^n)^{-1} (a^n * b^n * a * b) = (a^n)^{-1} * (a^n * a * b^n * b)$

— multiplying by $(a^n)^{-1}$

$\Rightarrow b^n * a * b = a * b^n * b$ [Associativity & identity & property of inverses]

$\Rightarrow b^n * a * b * b^{-1} = a * b^n * b * b^{-1}$ [Multiply by b^{-1}]

$\Rightarrow b^n * a = a * b^n$ —— (4)

Ily $(a*b)^{n+2} = a^{n+2} * b^{n+2}$ —— by (3)

$\Rightarrow (a*b)^{n+1}\, a*b = a^{n+1} * a * b^{n+1} * b$ [Definition].

$\Rightarrow a^{n+1} * b^{n+1} * a * b = a^{n+1} * a * b^{n+1} * b$ [By (1) & definition]

$$\Rightarrow (a^{n+1})^{-1} * a^{n+1} * b^{n+1} * a * b$$

$$= (a^{n+1})^{-1} * a^{n+1} * a * b^{n+1} * b$$

[Multiply by $(a^{n+1})^{-1}$]

$\Rightarrow b^{n+1} * a * b = a * b^{n+1} * b$ [Associativity, prop of inverse, prop of identity]

$\Rightarrow b^{n+1} * a * b * b^{-1} = a * b^{n+1} * b * b^{-1}$ [Mult by b^{-1}]

$\Rightarrow b^{n+1} * a = a * b^{n+1}$

$\Rightarrow b * b^{n} * a = a * b * b^{n}$

$\Rightarrow b * a * b^{n} = a * b * b^{n}$ [Applying (4)]

$\Rightarrow b * a * b^{n} * (b^{n})^{-1} = a * b * b^{n} * (b^{n})^{-1}$

[Multiply by $(b^{n})^{-1}$]

$\Rightarrow b * a * e = a * b * e$ [property of inverses and property of identity element]

$\Rightarrow b * a = a * b.$

Thus we have proved that $\forall a, b \in G$ if $(a*b)^{n} = a^{n} * b^{n}$ for any three consecutive integers, $a * b = b * a$

$\Leftrightarrow G$ is commutative.

Scheme : 1/2 for formulating (1), (2) & (3)

1 for deriving (4)

1 for applying (4) as required & deriving $b*a = a*b$.

1/2 for concluding properly.