Unit 4 Groups
Part A

Define Algebraic structure.
The operations and relations on the set S define a structure on the elements of S, an algebraic system is called an algebraic structure.

Define Semi-group
Let S be a nonempty set and o be a binary operation on S. The algebraic system $(S,.)$ is called a semigroup if the operation . is associative. In other words $(S,.)$ is a semigroup if for any $x, y, z \in S$,

$$(x.y).z = x.(y.z).$$

Define Monoid
A semigroup (M,.) with an identity element with respect to the operation o is called a monoid. In other words, an algebraic system (M,.) is called a monoid if for any $x, y, z \in M$, $(x.y).z = x.(y.z)$ and there exists an element $e \in M$ such that for any $x \in M$, $e.x = x.e = x$

Define semigroup homomorphism.
Let $(S,*)$ and (T,Δ) be any two semigroups. A mapping $g: S \to T$ such that for any two elements $a, b \in S$, $g(a * b) = g(a)\,\Delta\, g(b)$ is called a semigroup homomorphism.

Define direct product
Let $(S,*)$ and (T,Δ) be two semigroups. The direct product of $(S,*)$ and (T,Δ) is the algebraic system $(S \times T,.)$ in which the operation . on $S \times T$ is defined by
$(s_1, t_1).(s_2, t_2) = (s_1 * s_2, t_1 \Delta\, t_2)$ for any (s_1, t_1) and $(s_2, t_2) \in S \times T$.

Show that the set N of natural numbers is a semigroup under the operation $x * y = max\{x, y\}$. Is it monoid?
Given the operation $x * y = max\{x, y\}$ for any $x, y \in N$.
Clearly $(N,*)$ is closed because $x * y = max\{x, y\} \in N$ and $*$ is associative as

$$(x * y) * z = max\{x * y, z\}$$
$$= max\{max\{x, y\}, z\}$$
$$= max\{x, y, z\}$$
$$= max\{x, max\{y, z\}\}$$
$$= max\{x, \{y * z\}\}$$
$$= x * (y * z)$$

Therefore, $(N,*)$ is a semi-group. The identity e of $(N,*)$ must satisfy the property that $x * e = e * x = x$. But $x * e = e * x = max\{x, e\}$
$= max\{e, x\} = x$.

Prove that " A semi-group homomorphism preserves the property of associativity.
$Let\ a, b, c \in S,$

$$g([(a*b)*c] = g(a*b).g(c)$$
$$= [\big(g(a).g(b)\big).g(c)] \quad \dots (1)$$
$$g[a*(b*c)] = g(a).g(b*c)$$
$$= g(a).[g(b).g(c)] \quad \dots (2)$$
$$But\ in\ S, (a*b)*c = a*(b*c), \forall\, a,b,c \in S$$
$$\therefore\ g[(a*b)*c] = g[a*(b*c)]$$
$$\Rightarrow\ [g(a).g(b)].g(c) = g(a).[g(b).g(c)]$$

∴ The property of associativity is preserved.

Prove that a semi group homomorphism preserves idem potency.

Let $a \in S$ be an idempotent element.

$\therefore\ a*a = a$

$$g(a*a) = g(a).g(a) = g(a)$$
$$\therefore g(a*a) = g(a).$$

This shows that $g(a)$ is an idempotent element in T.

The property of idem potency is preserved under semi group homomorphism.

Prove that A semigroup homomorphism preserves commutativity.

Let $a, b \in S$

Assume that $a*b = b*a$

$$g(a*b) = g(b*a)$$
$$g(a).g(b) = g(b).g(a).$$

This means that the operation . is commutative in T

The semigroup homomorphism preserves commutativity.

Define group.

A non-empty set G, together with a binary operation * is said to be a group if it satisfies the following axioms.

i) ∀a,b ∈G ⇒ a*b ∈ G (Closure Property)

ii) For any $a, b, c \in G, (a*b)*c = a*(b*c)$ (Associative property)

iii) There exists an element $e\ in\ G$ such that $a*e = e*a = a$, $\forall a \in G$ (Identity)

iv) For all $a \in G$ there exists an element $a-1 \in G$ such that $a*a^{-1} = a^{-1}*a = e$ (Inverse Property)

Define Abelian group

A Group $(G,*)$ is said to be abelian if $a*b = b*a$ for all $a, b \in G$

Define Left coset of H in G

Let $(H,*)$ be a subgroup of $(G,*)$. For any $a \in G$, the set aH defined by

$aH = \{a*h\ /\ h \in H\}$ is called the left coset of H in G determined by the element $a \in G$.

The element a is called the representative element of the left coset aH.

State Lagrange's theorem
The order of a subgroup of a finite group divides the order of the group. Or If G is a finite group, then $O(H) \setminus O(G)$, for all sub-group H of G.

If $(G,*)$ is a finite group of order n, then for any $a \in G$, we have $a^n = e$, where e is the identity of the group G.
Let $O(G) = n$ and Let $a \in G$ Then order of the subgroup $< a >$ is the order of the element a. If $O(< a >) = m$, then $a^m = e$ and by Lagrange's theorem , we get $m \setminus n$.Let $n = mk$ Then $a^m = a^{mk} = (a^m)^k = e^k = e$.

Let $G = \{1, a, a^2, a^3\}$ *where* $(a^4 = 1)$ be a group and $H = \{1, a^2\}$ is a subgroup of G under multiplication . Find all the cosets of H.
Let us find the right cosets of H in G.

$$H1 = \{1, a^2\} = H$$
$$Ha = \{a, a^3\}$$
$$Ha^2 = \{a^2, a^4\} = \{a^2, 1\} = H$$
$$and\ Ha^3 = \{a^3, a^5\} = \{a^3, a\} = Ha$$

$\therefore H.1 = H = Ha^2 = \{1, a^2\}\ and\ Ha = Ha^3 = \{a, a^3\}$ are distinct right cosets of H in G. Similarly, we can find the left cosets of H in G.

Find the left cosets of $\{[0],[2]\}$ in the group $(Z_4, +_4)$.
Let $Z_4 = \{[0],[1],[2],[3]\}$ be a group and $H = \{[0],[2]\}$ be a sub-group of Z_4 under $+_4$.
The left cosets of H are

$$[0] + H = \{[0],[2]\}$$
$$[1] + H = \{[1],[3]\}$$
$$[2] + H = \{[2],[4]\} = \{[2],[0]\} = \{[0],[2]\} = H$$
$$[3] + H = \{[3],[5]\} = \{[3],[1]\} = \{[1],[3]\} = [1] + H$$

$[0] + H = [2] + H = H\ and\ [1] + H = [3] + H$ are the two distinct left cosets of H in Z_4.

Define subgroup
Let $(G,*)$ be a group and let H be a non-empty subset of G. Then H is said to be a subgroup of G if H itself is a group with respect to the operation $*$.

Define normal subgroup
A subgroup $(H,*)$ of $(G,*)$ is called a normal sub-group if for any $a \in G$, $aH = Ha$. (i.e.) Left coset = Right coset

Prove that every subgroup of an abelian group is normal subgroup.
Let $(G,*)$ be an abelian group and $(N,*)$ be a subgroup of G.
Let g be any element in G and let $n \in N$.
Now $g * n * g^{-1} = (n * g) * g^{-1}$ [Since G is abelian]

$$= n * e = n \in N$$

$$\therefore \forall\, g \in G \; and \; n \in N, g * n * g^{-1} \in N$$

$\therefore$ $(N,*)$ is a normal subgroup.

Define direct product on groups

Let $(G,*)$ and (H,Δ) be two groups. The direct product of these two groups is the algebraic structure $(\, G \times H\,,.)$ in which the binary operation . on $G \times H$ is given by $(g_1, h_1).(g_2, h_2) = (g_1 * g_2, h_1\Delta\, h_2)$
for any $(g_1, h_1), (g_2, h_2) \in G \times H$.

If S denotes the set of positive integers ≤ 100, for any $x, y \in S$, define $x * y = min\{x, y\}$. Verify whether $(S,*)$ is a monoid assuming that $*$ is associative.

The identity element is $e = 100$ exists.
Since for $x \in S, min\,(x, 100) = x \Rightarrow x * 100 = x, \forall x \in S$

If H is a subgroup of the group G, among the right cosets of H in G. Prove that there is only one subgroup viz., H.

Let Ha be a right coset of H in G where $a \in G$. If Ha is a subgroup of G then $e \in Ha$, where e is the identity element in G. Ha is an equivalence class containing a with respect to an equivalence relation.

$e \in Ha \Rightarrow H.e = Ha$. But $He = H$

$\therefore Ha = H.\ This\ shows\ H\ is\ only\ subgroup.$

Give an example of sub semi-group

For the semi group $(N, +)$, where N is the set of natural number, the set E of all even non-negative integers $(E, +)$ is a sub semi-group of $(N, +)$.

Find the subgroup of order two of the group $(Z_8, +_8)$

$H = \{[0], [4]\}$ is a subgroup of order two of the group $G = (Z_8, +_8)$.

$+_8$	$[0]$	$[4]$
$[0]$	$[0]$	$[4]$
$[4]$	$[4]$	$[0]$

Define Ring

An algebraic system $(S, +, .)$ is called a ring if the binary operations $+$ and . on S satisfy the following three properities.

i)$(S, +)$ is an abelian group

ii)$(S, .)$ is a semigroup

iii) The operation . is distributive over $+$, i.e. , for any $a, b, c \in S$,

$$a.(b + c) = a.b + a.c \; and \; (b + c).a = b.a + c.a$$

Define Subring

A commutative ring $(S, +, .)$ is a ring is called a subring if $(R, +, .)$ is itself with the operations $+$ and $.$ restricted to R.

Define Ring homomorphism

Let $(R, +, .)$ and $(S, \oplus, \odot)$ be rings. A mapping g:R∈S is called a ring homomorphism from $(R, +, .)$ to $(S, \oplus, \odot)$ if for any $a, b \in R$.

$$g(a+b) = g(a) \oplus g(b) \text{ and } g(a.b) = g(a) \odot g(b)$$

If $(R, +, .)$ be a ring then prove that $a\,.\,0 = 0$ for every $a \in R$

Proof:

Let $a \in R$ then $a.0 = a.(0+0) = a.0 + a.0$ [by Distributive Law]

$a.0 = 0$ [Cancellation Law]

Give an example of an ring with zero-divisors.

The ring $(Z_{10}, +_{10}, ._{10})$ is not an integral domain.

Since $5 ._{10} 2 = 0, (5 \neq 0, 2 \neq 0 \; in \; Z_{10})$

Define Field.

The commutative ring $(R, +, \times)$ with unity is said to be a Field if it has inverse element under the binary operation $\times$. $(a^{-1} \times a = a \times a^{-1} = 1, \forall a \in R)$.

Part B

State and Prove Lagrange's theorem for finite groups.

Statement:

The order of a subgroup of a finite group is a divisor of the order of the group.

Proof:

Let aH and bH be two left cosets of the subgroup $\{H,*\}$ in the group $\{G,*\}$.

Let the two cosets aH and bH be not disjoint.

Then let c be an element common to aH and bH i.e., $c \in aH \cap bH$

$$\because c \in aH, c = a * h_1, for\ some\ h_1 \in H \ldots (1)$$

$$\because c \in bH, c = b * h_2, for\ some\ h_2 \in H \ldots (2)$$

From (1) and (2), we have

$$a * h_1 = b * h_2$$

$$a = b * h_2 * h_1^{-1} \ldots (3)$$

Let x be an element in aH

$x = a * h_3, for\ some\ h_3 \in H$

$= b * h_2 * h_1^{-1} * h_3, using\ (3)$

Since H is a subgroup, $h_2 * h_1^{-1} * h_3 \in H$

Hence, (3) means $x \in bH$

Thus, any element in aH is also an element in bH. $\therefore aH \subseteq bH$

Similarly, we can prove that $bH \subseteq aH$

Hence $aH = bH$

Thus, if aH and bH are disjoint, they are identical.

The two cosets aH and bH are disjoint or identical. …(4)
Now every element $a \in G$ belongs to one and only one left coset of H in G,
For,
$a = ae \in aH, since\ e \in H \Rightarrow a \in aH$

$a \notin bH$, since aH and bH are disjoint i.e., a belongs to one and only left coset of H in G i.e., aH … (5)
From (4) and (5), we see that the set of left cosets of H in G form the partition of G. Now let the order of H be m.
Let $H = \{h_1, h_2, \dots, h_m\}, where\ h_i's$ are distinct
Then $aH = \{ah_1, ah_2, \dots, ah_m\}$
The elements of aH are also distinct, for, $ah_i = ah_j \Rightarrow h_i = h_j$, which is not true.
Thus H and aH have the same number of elements, namely m.
In fact every coset of H in G has exactly m elements.
Now let the order of the group $\{G,*\}$ be n, i.e., there are n elements in G
Let the number of distinct left cosets of H in G be p.
∴ The total number of elements of all the left cosets $= pm$ $=$ the total number of elements of G. i.e., $n = pm$
i.e., m, the order of H is adivisor of n, the order of G.

Find all non-trivial subgroups of $(\boldsymbol{Z_6}, +_6)$
Solution: $(Z_6, +_6), S = \{[0]\}\ under\ binary\ operation\ +_6$ are trivial subgroups

$+_6$	**[0]**	**[1]**	**[2]**	**[3]**	**[4]**	**[5]**
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$S_1 = \{[0], [2], [4]\}$

$+_6$	**[0]**	**[2]**	**[4]**
[0]	[0]	[2]	[4]
[2]	[2]	[4]	[0]
[4]	[4]	[0]	[2]

From the above cayley's table,
All the elements are closed under the binary operation $+_6$
Associativity is also true under the binary operation $+_6$
[0] is the identity element.
Inverse element of [2] is [4] and vise versa

Hence $S_1 = \{[0],[2],[4]\}$ is a subgroup of $(Z_6, +_6)$
$S_2 = \{[0],[3]\}$

$+_6$	**[0]**	**[3]**
[0]	[0]	[3]
[3]	[3]	[0]

From the above cayley's table,
All the elements are closed under the binary operation $+_6$
Associativity is also true under the binary operation $+_6$
[0] is the identity element.
Inverse element of [3] is itself.
Hence $S_2 = \{[0],[3]\}$ is a subgroup of $(Z_6, +_6)$
Therefore $S_1 = \{[0],[2],[4]\}$ and $S_2 = \{[0],[3]\}$ are non trivial subgroups of $(Z_6, +_6)$

Show that the mapping $g: (S, +) \to (T, *)$ defined by $g(a) = 3^a$, where S is the set of all rational numbers under addition operation $+$ and T is the set of non-zero real numbers under multiplication operation $*$ is a homomorphism but not isomorphism.

Solution:

For any $a, b \in S$,

$$g(a+b) = 3^{a+b} = 3^a * 3^b = g(a) * g(b)$$

$\therefore g$ is a homomorphism.
To prove g is one to one:
For any $a, b \in S$,
Let $g(a) = g(b) \Rightarrow 3^a = 3^b \Rightarrow a = b$
$\therefore g$ is one to one
To prove g is onto:

$$b = 3^a \Rightarrow \log b = \log 3^a \Rightarrow \log b = \mathrm{a} \log 3 \Rightarrow a = \frac{\log b}{\log 3}$$

$$\therefore a = g\left(\frac{\log a}{\log 3}\right), \forall a \in T$$

$\therefore \forall a \in T$, there is a pre-image $\frac{\log a}{\log 3} \notin S$
$\left[\because \log 3 \text{ is irratioinal} \Rightarrow \frac{\log a}{\log 3} \text{ is irratioinal}\right]$
$\therefore g$ is not onto.
$\therefore g$ is not an isomorphism.

The intersection of any two subgroups of a group G is again a subgroup of G. –Prove.

Proof:
Let H_1 and H_2 be two normal subgroups of a group $(G, *)$.
Then H_1 *and* H_2 are subgroups.

$e \in H_1$ and $e \in H_2 \Rightarrow e \in H_1 \cap H_2$. Since e is the identity element of G and it is unique.

$$\therefore H_1 \cap H_2 \text{ is non empty}.$$

$$\forall a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1 \text{ and } a, b \in H_2 \Rightarrow a * b^{-1} \in H_1 \text{ and } a * b^{-1} \in H_2$$

Since H_1 and H_2 are subgroups.

$$\Rightarrow a * b^{-1} \in H_1 \cap H_2$$

$$\therefore H_1 \cap H_2 \text{ is a subgroup}$$

Show that monoid homomorphism preserves the property of invertibility.

Solution:

If $\{M,*,e\}$ and $\{T,\cdot,e'\}$ be any two $monoids, where$ e and e' are $identity$ elements of M and T with respect to the operations $*$ and . respectively, then a mapping $g: M \rightarrow T$ such that, for any two elements $a, b \in M$,

$g(a * b) = g(a).g(b)$ and $g(e) = e'$ is called monoid homomorphism.

Let $a^{-1} \in M$ be the inverse of $a \in M$

Then $g(a * a^{-1}) = g(e) = e'$ by $definition$.

Also $g(a * a^{-1}) = g(a).g(a^{-1})$ by $definition$

$$g(a).g(a^{-1}) = e'$$

Hence the inverse of $g(a) = g(a^{-1}) = (g(a))^{-1}$

$\therefore$ Monoid homomorphism preserves the property of invertibility.

Prove that the intersection of two normal subgroup of a group will be a normal subgroup.

Solution:

Let H_1 and H_2 be two normal subgroups of a group $(G,*)$.

Then H_1 and H_2 are subgroups.

Since $e \in H_1$ and $e \in H_2 \Rightarrow e \in H_1 \cap H_2$

$$\therefore H_1 \cap H_2 \text{ is non empty}.$$

$$\forall a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1 \text{ and } a, b \in H_2 \Rightarrow a * b^{-1} \in H_1 \text{ and } a * b^{-1} \in H_2$$

Since H_1 and H_2 are subgroups.

$$\Rightarrow a * b^{-1} \in H_1 \cap H_2$$

$$\therefore H_1 \cap H_2 \text{ is a subgroup}$$

$$\forall a \in G, \forall h \in H_1 \cap H_2 \Rightarrow h \in H_1 \text{ and } h \in H_2,$$

$\Rightarrow a^{-1} * h * a \in H_1$ and $a^{-1} * h * a \in H_2$ Since H_1 and H_2 are normal subgroups.

$$\Rightarrow a^{-1} * h * a \in H_1 \cap H_2$$

$$\therefore H_1 \cap H_2 \text{ is a normal subgroup}$$

Let S be a non-empty set and $P(S)$ denote the power set of S. Verify that $(P(S),\cap)$ is a group.

Solution:

$\because P(S)$ denote the power set of S

$\forall A, B \in P(S) \Rightarrow A \cap B \in P(S)$

$\therefore P(S)$ is closed.

$\forall A, B, C \in P(S) \Rightarrow A \cap (B \cap C) = (A \cap B) \cap C$

$\therefore P(S)$ is associative
$\forall A \in P(S)$, we have $A \cap S = A = S \cap A$
$\therefore S \in P(S)$ be the identity element.
$\forall A \in P(S)$, there exists some $B \in P(S)$ such that

$$A \cap B \neq S$$

$\therefore$ Inverse does not exists for any subset except S
$(P(S), \cap)$ is not a group but it is a monoid.

Let $(G, *)$ and (H, Δ) be groups and $g: G \to H$ be a homomorphism. Then prove that kernel of g is a normal sub-group of G.

Solution:
Let $K = ker(g) = \{g(a) = e' \backslash a \in G, e' \in H\}$
To prove K is a subgroup of G:
We know that $g(e) = e' \Rightarrow e \in K$
$\therefore K$ is a non-empty subset of G.
By the definition of homomorphism $g(a * b) = g(a) \, \Delta \, g(b), \forall a, b \in G$
Let $a, b \in K \Rightarrow g(a) = e' \; and \; g(b) = e'$
Now $g(a * b^{-1}) = g(a) \, \Delta \, g(b^{-1}) = g(a) \, \Delta \left(g(b)\right)^{-1} = e' \Delta \, (e')^{-1}$

$$= e' \Delta \, e' = e'$$
$$\therefore a * b^{-1} \in K$$

$\therefore K$ is a subgroup of G
To prove K is a normal subgroup of G:
For any $a \in G \; and \; k \in K$,

$$g(a^{-1} * k * a) = g(a^{-1}) \, \Delta \, g(k) \Delta g(a) = g(a^{-1}) \Delta \, g(k) \, \Delta \, g(a)$$
$$= g(a^{-1}) \Delta \, e' \Delta \, g(a) = g(a^{-1}) \, \Delta \, g(a) = g(a^{-1} * a) = g(e) = e'$$
$$a^{-1} * k * a \in K$$

$\therefore K$ is a normal subgroup of G

State and Prove Fundamental theorem of homomorphism.

Statement:
Let g be a homomorphism from a group $(G, *)$ to a group (H, Δ), and let K be the kernel of g and $H' \subseteq H$ be the image set of g in H. Then G/K is isomorphic to H'.
Proof:
Since K is the kernel of homomorphism, it must be a normal subgroup of G. Also we can define a mapping $f: (G, *) \to (G/K, \otimes)$ where $\otimes$ is defined as $(a * b)H = aH \otimes bH, \forall a, b \in G$ ... (1)
i.e., $f(a) = aK \qquad for \; any \; a \in G$ ... (2)
Let us define a mapping $h: G/K \to H'$ such that $h(aK) = g(a)$ ... (3)
To prove that h is well defined:
For any $a, b \in G$,

$$\therefore aK = bK$$
$$a * b^{-1} \in K \Rightarrow a \in Kb$$
$$g(a * b^{-1}) = e' \; [since \; k \; is \; kernel \; of \; homomorphism \; from \; G \; to \; H \,]$$

$$g(a)\Delta\, g(b^{-1}) = e' \ \ [since\ g\ is\ homomorphism\ from\ G\ to\ H\ ]$$
$$g(a)\Delta\left(g(b)\right)^{-1} = e' \ \left[\because \left(g(b)\right)^{-1} = g(b^{-1})\ \right]$$
$$g(a)\Delta\left(g(b)\right)^{-1}\Delta\ g(b) = e'\Delta\ g(b)$$
$$g(a)\Delta\, e' = g(b) \Rightarrow g(a) = g(b)$$
$$h(aK) = h(bK)$$
$$aK = bK \Rightarrow h(aK) = h(bK)$$

$\therefore h$ is well defined.

To prove that h is homomorphism:

$$h(aK \otimes bK) = h\left((a*b)K\right) \ \ [from(1)]$$
$$= g(a*b)[from(3)]$$
$$= g(a)\ \Delta\ g(b)\ \ [since\ g\ is\ homomorphism\ from\ G\ to\ H\ ]$$
$$= h(aK)\ \Delta\ h(bK)\ [from(3)]$$

$\therefore h$ is homomorphism

To prove that h is on to:

The image set of the mapping h is the same as the image set of the mapping g, so that $h: G/K \to H'$ is on to.

To prove that h is one to one:

For any $a, b \in G$,

$$h(aK) = h(bK)$$
$$g(a) = g(b)$$
$$g(a)\Delta\left(g(b)\right)^{-1} = g(b)\Delta\left(g(b)\right)^{-1}$$
$$g(a)\Delta\, g(b^{-1}) = e' \quad \left[\left(g(b)\right)^{-1} = g(b^{-1})\ \ \&\ \ g(b)\Delta\left(g(b)\right)^{-1} = e'\right]$$
$$g(a*b^{-1}) = e' \ \ [since\ g\ is\ homomorphism\ from\ G\ to\ H\ ]$$
$$a*b^{-1} \in K \Rightarrow a \in Kb$$
$$\therefore aK = bK$$

$\therefore h$ is one to one

$\therefore h: G/K \to H'$ is isomorphic.

Show that every subgroup of a cyclic group is cyclic.

Proof:

Let G be the cyclic group generated by the element a and let H be a subgroup of G. If $H = G\ or\ \{e\}$, H is cyclic. If not the elements of H are non-zero integral powers of a, since, if $a^r \epsilon H$, its inverse $a^{-r} \epsilon H$.

Let m be the least positive integer for which $a^m \epsilon H$

Now let a^n be any arbitrary element of H. Let q be the quotient and r be the remainder when n is divided by m.

Then $n = mq + r, where\ 0 \le r < m$

Since, $a^m \epsilon H, (a^m)^q \epsilon H, by\ closure\ property$

$$a^{mq} \epsilon H \Rightarrow (a^{mq})^{-1} \epsilon H, by\ existence\ of\ inverse, as\ H\ is\ a\ subgroup$$

$$a^{-mq} \epsilon H.$$

Now since, $a^n \epsilon H\ and\ a^{-mq} \epsilon H \Rightarrow a^{n-mq} \epsilon H \Rightarrow a^r \epsilon H$

$$r = 0\ \ \therefore n = mq$$
$$\therefore a^n = a^{mq} = (a^m)^q$$

Thus, every element $a^n \epsilon H$ is of the form $(a^m)^q$.

Hence H is a cyclic subgroup generated by a^m.

State and prove Cayley's theorem on permutation groups.

Statement:

Every group G is isomorphic to a subgroup of the group of permutation S_A for some set A.

Proof:

We know that $P \subseteq S_G$ is the subgroup of permutation group S_G. We prove the result by choosing A to be G.

In fact, we prove that the mapping $\varphi: (G,*) \to (P, o)$ given by $\varphi(a) = p_a$ is an isomorphism from G on to P.

To prove φ is homomorphism:

Let $a, b \in G$, then

$$\varphi(a * b) = p_{a*b} = p_a o p_b = \varphi(a) o \varphi(b)$$

$\therefore$ φ is homomorphism

To prove φ is one to one:

$$\varphi(a) = \varphi(b)$$
$$p_a = p_b \Rightarrow p_a(e) = p_b\,(e)$$
$$e * a = e * b$$
$$a = b$$

$\therefore$ φ is one to one

To prove φ is on to:

$\because$ $\varphi(a) = p_a$, For every image p_a in P there is a pre image a in G.

$\therefore$ φ is on to.

$\therefore$ φ is isomorphism.

Prove that every finite integral domain is a field.

Proof:

Let $\{D, +, .\}$ be a finite integral domain. Then D has a finite number of distinct elements, say, $\{a_1, a_2, \dots, a_n\}$.

Let $a \neq 0$ be an element of D.

Then the elements $a.a_1, a.a_2, \dots, a.a_n \epsilon D$, since D is closed under multiplication. The elements $a.a_1, a.a_2, \dots, a.a_n$ are distinct, because if $a.a_i = a.a_j, then$ $a.(a_i - a_j) = 0$. But $a \neq 0$. Hence $a_i - a_j = 0$, since D is an integral domain i.e., $a_i = a_j$, which is not true, since $a_1, a_2, \dots, a_n$ are distinct elements of D.

Hence the sets $\{a.a_1, a.a_2, \dots, a.a_n\}$ and $\{a_1, a_2, \dots, a_n\}$ are the same.

Since $a \epsilon D$ is in both sets, let $a.a_k = a$ for some k ... (1)

Then a_k is the unity of D, detailed as follows

Let $a_j = a.a_i$ ... (2)

Now $a_j.a_k = a_k.a_{j,}$ $by\ commutativity$

$= a_k.(a.a_i)$ by (2)

$= (a_k.a).a_i$

$= (a.a_k).a_i$

$= a.a_i\ by\ (1)$

$$= a_j \ by \ (2)$$

Since, a_j is an arbitrary element of D

a_k is the unity of D

Let it be denoted by 1.

Since $1 \epsilon D$, there exist $a \neq 0$ and $a_i \epsilon D$ such that $a. a_i = a_i. a = 1$

a has an inverse.

Hence $(D, +, .)$ is a field.