STUDY MATERIAL
Semester -2, Course: CC-4

Topic: Group Theory
(Some important problems with solutions)

1. Let G be a group and H be a non-empty subset of G. Prove that, if H is a subgroup of G, then $HH = H$.

Proof: Let x be an arbitrary element in HH.

Now, $x \in HH \Rightarrow x = ab, a, b \in H$.

Since H be a subgroup and $a, b \in H$, so $ab \in H$.

Therefore, $x \in HH \Rightarrow x \in H$. So, $HH \subseteq H$ (1)

Again, let h be an arbitrary element in H.

Now, $h = he \in HH$ since $h \in H, e$ is the identity element of H.

Therefore, $h \in H \Rightarrow h \in HH$. So, $H \subseteq HH$ (2)

From (1) and (2), we have $HH = H$.

2. Suppose a group contains element a, b such that $o(a) = 4, o(b) = 2$ and $a^3b = ba$. Find $o(ab)$.

Solution: $o(a) = 4 \Rightarrow a^4 = e$ and $o(b) = 2 \Rightarrow b^2 = 2$.

Now, $a^3b = ba \Rightarrow a^4b = aba \Rightarrow eb = aba \Rightarrow b = aba \Rightarrow bb = abab$

$\Rightarrow b^2 = (ab)^2 \Rightarrow e = (ab)^2$.

Therefore, $o(ab) \leq 2$.

Since $o(a) \neq o(b)$, so $a \neq b^{-1}$ [since $o(b) = o(b^{-1})$]

i.e. $ab \neq e$. So, $o(ab) > 1$. i.e. $1 < o(ab) \leq 2$.

Therefore, $o(ab) = 2$.

3. Let (G, o) be group. Prove that a non-empty subset H of G forms a subgroup of (G, o) if and only if $a \in H, b \in H \Rightarrow aob^{-1} \in H$.

Proof: S.K. Mapa, Th.2.11.3.

4. Prove that the semigroup (G, o) is a non-commutative group where $G = \{(a, b) \in Q \times Q : a \neq 0\}$ and the composition 'o' is defined by $(a, b)o(c, d) = (ac, ad + b)$ for $(a, b), (c, d) \in G$. Q is the set of rational numbers.

Proof: Since (G, o) is a semigroup, so G is closed under the binary operation 'o' and 'o' is associative in the algebraic structure (G, o).

$(1,0) \in G$.

Now, $(a,b)o(1,0) = (a,b)$ and $(1,0)o(a,b) = (a,b)\ \forall\ (a,b) \in G$.

Therefore, $(1,0)$ is the identity element in G under the binary composition 'o'.

Let for any element (a,b) in G, $\exists$ an element (c,d) in G such that $(a,b)o(c,d) = (1,0)$

i.e. $(ac, ad + b) = (1,0) \Rightarrow ac = 1,\ ad + b = 0$.

Therefore, $c = \frac{1}{a}$ and $d = -\frac{b}{a}$, since $a \neq 0$. So, $(c,d) = \left(\frac{1}{a}, -\frac{b}{a}\right) \in Q \times Q$.

Therefore, $(a,b)o\left(\frac{1}{a}, -\frac{b}{a}\right) = (1,0)$. Also $\left(\frac{1}{a}, -\frac{b}{a}\right)o(a,b) = (1,0)$.

So, $\left(\frac{1}{a}, -\frac{b}{a}\right)$ be the inverse of (a,b). i.e. inverse property is satisfied.

Commutativity: Let $(a,b),(c,d) \in G$.

Now, $(a,b)o(c,d) = (ac, ad + b)$ and $(c,d)o(a,b) = (ca, bc + d)$.

But $ab + b \neq bc + d$ in general.

For example, let $(1,2),(3,4) \in G$.

Now, $(1,2)o(3,4) = (3,6)$ and $(3,4)o(1,2) = (3,10)$.

Therefore, $(a,b)o(c,d) \neq (c,d)o(a,b)\ \forall\ (a,b),(c,d) \in G$.

5. Let G be an abelian group. Prove that the subset $H = \{g \in G: g^2 = e$ (identity element$\}$ forms a subgroup of G.

Proof: Since $e \in G$ and $e^2 = e$, so $e \in H$.

Therefore, H is non-empty.

Let a, b be two arbitrary element in H.

So, $a, b \in G$ and $a^2 = e, b^2 = e$.

$a, b \in G \Rightarrow ab^{-1} \in G$, since G is a group.

Now, $(ab^{-1})^2 = (ab^{-1})(ab^{-1}) = a(b^{-1}a)b^{-1} = a(ab^{-1})b^{-1}$, since G is abelian

$= a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = e$.

So, $a, b \in H \Rightarrow ab^{-1} \in H$.

Therefore, H is a subgroup of G.

6. Prove that a finite semigroup in which both the cancellation laws hold is a group. Does the theorem hold if the semigroup be infinite?

Proof: S.K. Mapa, Th. 2.7.7.

7. Let P be the set of all real numbers except the integer 1. Let the operation '$*$' be defined by $a * b = a + b - ab$ for all $a, b \in P$. Show that $(P,*)$ is a group.

Solution: (i) **Closure Property:** Let $a, b \in P$.

So, a and b are two real numbers and $a \neq 1, b \neq 1$.

Now, $a * b = a + b - ab$ which is a real number and $a + b - ab \neq 1$, because

$a + b - ab = 1 \Rightarrow b(1 - a) = 1 - a \Rightarrow b = 1$, since $a \neq 1$. But $b \neq 1$.

Therefore, $a * b$ is a real number and $a * b \neq 1$. So, $a * b \in P\ \ \forall\, a, b \in P$.

Hence P is closed under t6he binary operation '$*$'.

(ii) **Associative Property:** Let $a, b, c \in P$, where $a, b, c \in R$ and $a \neq 1, b \neq 1, c \neq 1$.

Now, $a * (b * c) = a * (b + c - bc) = a + b + c - bc - a(c + c - bc)$

$$= a + b + c - bc - ab - ac + abc.$$

$(a * b) * c = (a + b - bc) * c = a + b - bc + c - (a + b - ab)c$

$$= a + b + c - ab - ac - bc + abc.$$

Therefore, $a * (b * c) = (a * b) * c\ \ \forall\ a, b, c \in P$.

So, associative property is satisfied w.r.t. the binary operation '$*$'.

(iii) **Identity Property:** $0 \in P$.

Now, $0 * a = 0 + a - 0.a = a\ \forall\, a \in P$.

So 0 is the left identity element in P under the binary operation '$*$'.

(iv) **Inverse Property:** Let b be an element in P such that $b * a = 0$.

Now, $b * a = 0 \Rightarrow b + a - ba = 0 \Rightarrow b(1 - a) = -a \Rightarrow b = \frac{a}{a-1}$, since $a \neq 1$.

Since $\frac{a}{a-1}$ is a real number as $a \neq 1$ and $\frac{a}{a-1} \neq 1$, so $b = \frac{a}{a-1} \in P$.

Therefore, for any element a in P, $\exists$ an element $\frac{a}{a-1}$ in P such that $\frac{a}{a-1} * a = 0$.

So, $\frac{a}{a-1}$ is the left 0-inverse in P under the binary operation '$*$'.

Therefore, $(P,*)$ is a group.

8. Let (G, o) be a group and $a, b \in G$. If $o(a) = 3$ and $aoboa^{-1} = b^2$, find the order of b if b is not the identity element of G.

Solution: $aoboa^{-1} = b^2 \Rightarrow a^2oboa^{-2} = aob^2oa^{-1}$

$= (aoboa^{-1})o(aoboa^{-1})$, since '$o$' is associative.

$= b^2ob^2 = b^4$

$\Rightarrow a^3oboa^{-3} = aob^4oa^{-1} = (aoboa^{-1})o(aoboa^{-1})o(aoboa^{-1})o(aoboa^{-1})$

$$= b^2ob^2ob^2ob^2 = b^8$$

or, $\ b = b^8 \Rightarrow b^7 = e$.

Since $b \neq e$ and 7 is prime, so $o(b) = 7$.

9. Prove that the union of two subgroup H, K of a group $(G,*)$ forms a subgroup if and only if either $H \subset K$ or $K \subset H$.

Proof: S.K. Mapa, Th. 2.11.6.

10. Let G be a group. Let $Z(G)$ be a subset of G defined by $Z(G) = \{a \in G: xa = ax \ \forall\ x \in G\}$. Prove that $Z(G)$ is a subgroup of G.

Proof: S.K. Mapa, Example: 1, Page-111.

11. Let $(S,.)$ be a semigroup. If for $x, y \in S$, $x^2y = y = yx^2$, prove that $(S,.)$ is an abelian group.

Proof: S.K. Mapa, Example: 3, Page-83.

12. Prove that in a groupoid $(Z,-)$ there is no left identity, but 0 is a right identity.

Solution: Let $a, b \in Z$.

Now, $a, b \in Z \Rightarrow a - b \in Z\ \ \forall\ a, b \in Z$.

So, $(Z,-)$ is a groupoid.

Again, $a - 0 = a\ \forall a \in Z$. So 0 is the right identity in Z with respect to the binary operation '$-$'.

Now, $b - a = a \Rightarrow b = 2a$. So for different a in Z, $\exists$ different b in Z such that $b - a = a$. So b is not the left identity in $(Z,-)$. i.e. $(Z,-)$ has no left identity.

13. Show that the set of complex numbers $a + ib$ (where $i^2 = -1$) for $a^2 + b^2 = 1$ is a group under the multiplication of complex numbers.

Solution: Let $C = \{z = a + ib: a^2 + b^2 = 1\ i.e.\ |z| = 1\}$.

(i) **Closure Property:** Let $z_1, z_2 \in C$. So $|z_1| = 1, |z_2| = 1$.

Therefore, z_1z_2 is also a complex number and $|z_1z_2| = |z_1||z_2|$.

So, $z_1z_2 \in C\ \forall\ z_1, z_2 \in C$. i.e. C is closed under the multiplication of complex numbers.

(ii) **Associative Property:** Multiplication of complex numbers is associative.

(iii) **Identity Property:** $1 = 1 + 0.i \in C$ and $1.z = z.1 = z\ \ \forall z\ \in C$.

Therefore, 1 is the multiplicative identity element in C.

(iv) **Inverse Property:** Let z be an arbitrary element in C. So $z \neq 0$ and $|z| = 1$.

Since $z \neq 0$, so $\frac{1}{z}$ is also a complex number and $\left|\frac{1}{z}\right| = 1$. Therefore, $\frac{1}{z} \in C$.

Now, $z.\frac{1}{z} = \frac{1}{z}.z = 1$.

Therefore, $\frac{1}{z}$ is the multiplicative inverse of z in C.

Since z is arbitrary, so each element in C has a multiplicative inverse in C. So inverse property is satisfied.

Therefore, the set of complex numbers $a + ib$ for $a^2 + b^2 = 1$ is a group under the multiplication of complex numbers.

14. If b be an element of a group and order of b is 20, find the order of b^{15}.

Solution: $o(b^{15}) = \frac{o(b)}{gcd(20,15)} = \frac{20}{5} = 4$.

15. Give an example of a finite group whose each element other than the identity has the same order and also the order of the group is not a prime number.

Solution: The Klein's 4-group is a finite group of order 4 which is not prime and the order of each non-identity element is two.

16. Prove or disprove: The set D of all odd integers forms a commutative group with respect to the binary operation 'o' defined by $aob = a + b - 1$ for $a, b \in D$.

Solution:

i) **Closure property:** Let $a, b \in D$. Since a and b are odd integers, so $a + b - 1$ is also an odd integer.

Therefore, $aob = a + b - 1 \in D,\ \forall\, a, b \in D$. i.e. D is closed with respect to the binary operation 'o'.

(ii) **Associative property:** Let $a, b, c \in D$.

Now, $ao(boc) = ao(b + c - 1) = a + b + c - 1 - 1 = a + b + c - 2$

$(aob)oc = (a + b - 1)oc = a + b - 1 + c - 1 = a + b + c - 2$

Therefore, $ao(boc) = (aob)oc \quad \forall a, b, c \in D$. So the binary operation 'o' is associative in D.

(iii) **Identity property:** $1 \in D$.

Now, $ao1 = a + 1 - 1 = a = 1oa\ \forall a \in D$.

So 1 is the identity element in D under the binary operation 'o'.

(iv) **Inverse property:** If $a \in D$, then $2 - a \in D$, since $2 - a$ is odd as a is odd.

Now, $ao(2 - a) = a + 2 - a - 1 = 1$ and $(2 - a)oa = 2 - a + a - 1 = 1$.

Therefore, for each element $a \in D$, there exists an element $2 - a$ in D such that $ao(2 - a) = (2 - a)oa = 1$. So $2 - a$ is the inverse of a under the binary operation 'o'.

(v) **Commutativity:** Let $a, b \in D$.

$aob = a + b - 1 = b + a - 1 = boa \quad \forall a, b \in D$.

Therefore, (D, o) is a commutative group.

17. Give an example of an infinite group whose every element is of finite order.

Solution: Let Z be the set of integers and $P(Z)$ be the power set of Z.

Therefore, $P(Z)$ is an infinite set.

Now, define the binary operation '$*$' as $A * B = A \Delta B, A, B \in P(Z)$.

Then $(P(Z),*)$ be a group under the binary operation '$*$'. (Proof of this part is discussed in the class).

Here, $\emptyset \in P(Z)$ and $\emptyset$ be the identity element in $P(Z)$ under the operation '$*$' because

$A * \emptyset = A \Delta \emptyset = A = \emptyset \Delta A = \emptyset * A \, \forall \in P(Z)$.

Also $A * A = A \Delta A = \emptyset$. So every element is the self inverse with respect to the operation '$*$'.

i.e. $A^2 = A * A = \emptyset,\ A \neq \emptyset$.

Therefore, $o(A) = 2\ \forall\, A(\neq \emptyset) \in P(Z)$ and $o(\emptyset) = 1$.

Hence $(P(Z),*)$ is an infinite group whose every element is of finite order.

18. Show that A_3, the set of even permutations of $\{1,2,3\}$ is a cyclic group with respect to the product of permutations. Find a generator of this cyclic group. Answer with reason.

Solution: The set of even permutations of $\{1,2,3\}$ is $A_3 = \{\rho_0, \rho_1, \rho_2\}$ where

$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$

Find the composition table and prove that the set A_3, the set of even permutations of $\{1,2,3\}$ is a commutative group with respect to the product of permutations.

The order of this group is 3 and since 3 is a prime number, so A_3 is a cyclic group.

Since $o(\rho_1) = 3$ and $o(A_3) = 3$, so ρ_1 is a generator of this group.

19. Let $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$. Find the smallest positive integer k such that $a^k = e$ in S_4.

Solution: S_4 is the symmetric group with respect to the multiplication of permutations of the set $\{1,2,3,4\}$ and e be the identity element in S_4.

Now, $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1 \quad 3 \quad 2)$ which is a cycle of length 3.

So $o(a) = 3$.

Therefore, 3 is the least positive integer such that $a^3 = e$ in S_4.

20. Define permutation group. Give an example.

Definition: Let $S = \{a_1, a_2, a_3, \dots \dots \dots, a_n\}$ be a finite set.

A bijective mapping $f: S \to S$ is said to be a permutation on S. The number of such bijective mappings is $n!$. Let S_n be the set of all such permutations. Then the set S_n forms a group with respect to the multiplication of permutations. This group is called permutation group.

Example: Let $S = \{1, 2\}$. Therefore, $S_2 = \{\rho_0,\ \rho_1\}$ where $\rho_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $\rho_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

Consider the composition table and verify that $(S_2, .)$ is a permutation group.