classmate

Date
Page

# DS Assignment - 4

Q1

**Given:** $\left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} : a, b \in R, \ a+b \neq 0 \right\}$; R real No's.

**To Prove:**
(a) G is a semigroup under matrix multiplication.
(b) G has a left identity.
(c) Each element of G has a right inverse.
(d) G is a group.

**Proof:** (a) $A_1 \in G$ which is $\begin{pmatrix} a_1 & b_1 \\ a_1 & b_1 \end{pmatrix}$

$A_2 \in G$ which is $\begin{pmatrix} a_2 & b_2 \\ a_2 & b_2 \end{pmatrix}$

$$A_1 \times A_2 = \begin{pmatrix} a_1 & b_1 \\ a_1 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ a_2 & b_2 \end{pmatrix} = \begin{pmatrix} a_2(a_1+b_1) & b_2(a_1+b_1) \\ a_2(a_1+b_1) & b_2(a_1+b_1) \end{pmatrix}$$

Let $a_2(a_1+b_1) = c$ $\quad b_2(a_1+b_1) = d$

$$A_1 \times A_2 = \begin{pmatrix} c & d \\ c & d \end{pmatrix}$$

which is also in G. Hence G is closed under matrix multiplication.

$A_i \in G$ : $A_1 = \begin{pmatrix} a_1 & b_1 \\ a_1 & b_1 \end{pmatrix}$ $\quad A_2 = \begin{pmatrix} a_2 & b_2 \\ a_2 & b_2 \end{pmatrix}$ $\quad A_3 = \begin{pmatrix} a_3 & b_3 \\ a_3 & b_3 \end{pmatrix}$

we need to prove associativity i.e.

$$(A_1 \times A_2) \times A_3 = A_1 \times (A_2 \times A_3)$$

$A_1 \times A_2$

$$LHS = \begin{pmatrix} a_1 & b_1 \\ a_1 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ a_2 & b_2 \end{pmatrix} = \begin{pmatrix} a_2(a_1+b_1) & b_2(a_1+b_1) \\ a_2(a_1+b_1) & b_2(a_1+b_1) \end{pmatrix}$$

$$(A_1 \times A_2) \times A_3 = \begin{pmatrix} a_2(a_1+b_1) & b_2(a_1+b_1) \\ a_2(a_1+b_1) & b_2(a_1+b_1) \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ a_3 & b_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_3(a_1+b_1)(a_2+b_2) & b_3(a_1+b_1)(a_2+b_2) \\ a_3(a_1+b_1)(a_2+b_2) & b_3(a_1+b_1)(a_2+b_2) \end{pmatrix} \quad \text{--- (1)}$$

RHS: $A_2 \times A_3$

$$\begin{pmatrix} a_2 & b_2 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ a_3 & b_3 \end{pmatrix} = \begin{pmatrix} a_3(a_2+b_2) & b_3(a_2+b_2) \\ a_3(a_2+b_2) & b_3(a_2+b_2) \end{pmatrix}$$

$$A_1 \times (A_2 \times A_3) = \begin{pmatrix} a_1 & b_1 \\ a_1 & b_1 \end{pmatrix} \begin{pmatrix} a_3(a_2+b_2) & b_3(a_2+b_2) \\ a_3(a_2+b_2) & b_3(a_2+b_2) \end{pmatrix}$$

$$= \begin{pmatrix} a_3(a_2+b_2)(a_1+b_1) & b_3(a_2+b_2)(a_1+b_1) \\ a_3(a_2+b_2)(a_1+b_1) & b_3(a_2+b_2)(a_1+b_1) \end{pmatrix} \quad \text{--- (2)}$$

(1) = (2)

Hence G is associative.

Hence G is a semigroup under matrix multiplication.

Hence, Proved.

(b) Let left identity matrix be $A = \begin{pmatrix} c & d \\ c & d \end{pmatrix}$ and left identity exists.

$A_I \times A = A$ for left identity.

$$\begin{pmatrix} c & d \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ a & b \end{pmatrix} = \begin{pmatrix} a(c+d) & b(c+d) \\ a(c+d) & b(c+d) \end{pmatrix} \quad \text{--- (3)}$$

(3) matrix should be equal to A

$$\begin{pmatrix} a(c+d) & b(c+d) \\ a(c+d) & b(c+d) \end{pmatrix} = \begin{pmatrix} a & b \\ a & b \end{pmatrix}$$

by comparing we get $c+d=1$

So left identity matrix of $A$ is $A_I =$

$$\begin{pmatrix} c & d \\ c & d \end{pmatrix} \quad \text{s.t.} \quad c+d=1$$

left identity exists.

$$A_I = \begin{pmatrix} c & 1-c \\ c & 1-c \end{pmatrix} \quad - \quad (5)$$

Hence left identity exists

(c) ~~Ex~~ let Right inverse exists and be $= \begin{pmatrix} c & d \\ c & d \end{pmatrix} = A^{-1}$

$$A \times A^{-1} = \cancel{D}\, I$$

$$\begin{pmatrix} a & b \\ a & b \end{pmatrix} \begin{pmatrix} c & d \\ c & d \end{pmatrix} = \begin{pmatrix} e & 1-e \\ e & 1-e \end{pmatrix}$$

$$\begin{pmatrix} c(a+b) & d(a+b) \\ c(a+b) & d(a+b) \end{pmatrix} = \begin{pmatrix} e & 1-e \\ e & 1-e \end{pmatrix}$$

By comparing:

$$c(a+b) = e$$
$$d(a+b) = 1-e$$

Adding above eqn's

$$(a+b)(c+d) = 1$$

$$\cancel{a+b} \quad \boxed{c+d = \frac{1}{a+b}}$$

$$A^{-1} = \begin{pmatrix} c & \frac{1}{a+b} - c \\ c & \frac{1}{a+b} - c \end{pmatrix} \quad - (7)$$

Right inverse exists

Hence, Proved.

(d) G is a group i.e. ~~group~~ G should have following properties

(1) Closure
(2) Associative
(3) Existence of identity
(4) Existence of inverse.

As proofed in part (a), G is a semigroup.
Thus G is closed and associative.

But as shown in part (b), left identity is not unique. Since there is not a unique identity (left) existence of identity fails.
Hence G is not a group.
Hence, proved.

Q2 **Given:** $\langle G, \circ \rangle$ is a semigroup. $\forall a \; \exists$ unique $b$ s.t.

$a \circ b \circ a = a$

**To Prove:** $G$ is a group.

**Proof:** As $G$ is a semigroup, it satisfies the properties of

① closure

② Associativity

Now we need to prove,

① $\exists e$ s.t. $e \circ a = a \circ e = a \;\; \forall \; a \in G$.

② $\forall a \in G$, $\exists a^{-1}$ s.t. $a \circ a^{-1} = e$.

**Identity:** ~~a∘b is the left identity e~~ $e_l$

$(a \circ b) \circ a = a$

$a \circ b$ is the left identity

$= e_l$

$a \circ (b \circ a) = a$

$b \circ a$ is the right identity

$= e_r$

$e_l \circ e_r = e_l$

$e_l \circ e_r = e_r$

$e_l \circ e_r = e_l = e_r$

$\therefore$ The identity exists and is the ~~[illegible]~~ simplification of $a \circ b$ or $b \circ a$

Inverse:

$a \circ b \circ a = a$ — (1)

Post multiply b in (1)

$(a \circ b \circ a) \circ b = a \circ b$

$a \circ b = e$ (Proved in identity)

$a \circ (b \circ a \circ b) = e$.

From above $b \circ a \circ b$ is right inverse.

$i_r = b \circ a \circ b$

Pre multiply b in (1)

$b \circ (a \circ b \circ a) = b \circ a$

$b \circ a = e$ (Proved in identity).

$(b \circ a \circ b) \circ a = e$

From above $b \circ a \circ b$ is left inverse.

$i_l = b \circ a \circ b$

$i_l = i_r = i$

Therefore inverse exists and it is unique for all a ∈ G

$i =$ simplified version of $(b \circ a \circ b)$

∴ existence of group and identity both is satisfied.

∴ G is a group.

Hence, Proved.

Q3 Given:→ A finite cyclic group $\langle G \rangle$ with more than one element.

To Prove:→ $G$ must have an element of prime order.

Proof:→ $G$ is a cyclic group so it must contain an identity $\langle e \rangle$ and a generator $g$

$|G|$ be 'k'

$\therefore$ $g^k = e$ s.t. $\exists$ no $l < k$ s.t. $g^l \in G$ & $= e$

Now either $k$ is prime or composite.

Case I) $k$ is prime

$\therefore$ we proved there exists an element of prime order.

Case II:→ $k$ is composite.

$\therefore$ By fundamental theorem of arithematic.

$k = a \cdot b \longrightarrow$ prime

↳ prime / comp.

$\therefore g^k = (g^b)^a$

Now if $g^b \in G$, then an element of prime order exists

we know $g^k \in G$ & $g^k = e$

classmate
Date
Page

<u>By using Theorem's</u>

if $g^k \in G$ & $g^k = e$ & $\exists$ no. $l < k$, st. $g^l = e \in G$.

then $g^i \in G$ $\forall i \in [1, k]$

$\therefore$ as $k = a \cdot b$, $k > b$, $\therefore g^b \in G$, $\therefore$ by statement ①

Elements of prime order exists.

Hence, Proved.

classmate

Date
Page

Q4 **Given:** Group $G \langle G, \circ \rangle$. $H$ is subgroup of $G$.

$N = \bigcap_{x \in G} x \circ H \circ x^{-1}$.

**To Prove:** $N$ is a normal subgroup of $G$.

**Proof:** For a given ~~set~~ $x \in G$, let $P = x \circ H \circ x^{-1}$

For any $P_1, P_2 \in P$ if $P_1 P_2^{-1} \in P$ then $P$ is a subgroup of $G$.

Let $P_1 = x h_1 x^{-1}$ $\quad P_2 = x h_2 x^{-1}$

$$P_1 P_2^{-1} = (x h_1 x^{-1}) \cdot (x h_2 x^{-1})^{-1}$$
$$= x h_1 x^{-1} x h_2^{-1} x^{-1}$$
$$= x h_1 h_2^{-1} x^{-1}$$
$$= x h' x^{-1}$$

$h_1 h_2^{-1} \in H$
bcoz $H$ is subgrp of
Let $h_1 \circ h_2^{-1} = h'$

So $P_1 P_2^{-1} \in P$

$\therefore$ $P$ is a subgroup of group $G$.

Also, we know that intersection of subgroups is als a subgroup.

$\therefore$ $N$ is also a subgroup.

Proof: We have to prove that

$$g^{-1} \circ x \circ g \in N \quad \forall \; x \in N \;\&\; g \in G.$$

We know $x = y h y^{-1}$ $\quad y \in G \;\&\; h \in H.$

$$g^{-1} \circ x \circ g = g^{-1} \circ y \circ h \circ y^{-1} \circ g \quad \text{--- (1)} \quad \forall \; x, y \in G.$$

We also know that

$\forall \; y, g \in G \Rightarrow y^{-1}, g^{-1} \in G.$

$g^{-1} \circ y \in G$ and $y^{-1} \circ g \in G$ [Closure Property]

Let $g^{-1} \circ y = z$ — (2) (where $z \in G$ as $g^{-1} y \in G$)

$$z^{-1} = (g^{-1} \circ y)^{-1} = y^{-1} \circ (g^{-1})^{-1} = y^{-1} \circ g \quad \text{--- (3)}$$

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$$

From (1), (2) & (3),

$$g^{-1} \circ x \circ g = a \circ h \circ a^{-1} \quad \forall \; a \in G$$

We know $a \circ h \circ a^{-1} \in N$

$\Rightarrow g^{-1} \circ y \circ g \in N \quad \forall g \in G$ and $y \in N$.

$\Rightarrow$ N satisfies the property for normal subgroup

Hence, Proved.

Q5 Given: A Group $\{G, \circ\}$. Two normal subgroups $H$ and $K$ of group $G$.

To prove: Their intersection is a normal subgroup.

Proof: Since $H$ and $K$ are normal subgroups. By theorem that intersection of 2 subgroup is also a subgroup.

$\therefore$ $H \cap K$ is also a subgroup.

Let $H \cap K = T$.

For $T$ to be normal

we need to prove that: $g \circ T \circ g^{-1} \subseteq T \quad \forall g \in G$

Take arbitrary element $t \in T$.

$t \in H$ & $t \in K$.

Since $H$ and $K$ are normal subgroups.

$g \circ t \circ g^{-1} \subseteq H \quad \forall g \in G$

$g \circ t \circ g^{-1} \subseteq K \quad \forall g \in G$.

Since $g \circ t \circ g^{-1}$ is both in $H$ and $K$.

$\therefore$ $g \circ t \circ g^{-1} \in H \cap K \quad \forall g \in G$

$\Rightarrow$ $g \circ t \circ g^{-1} \subseteq T \quad \forall g \in G$.

Since we took arbitrary $t \in T$.

This is true $\forall t \in T$.

$\therefore$ $g \circ T \circ g^{-1} \subseteq T$.

Hence, $T$ is a normal subgroup or $H \cap K$ is a normal subgroup.

Hence, Proved.

Q6

**Given:** A subgroup $H$ of group $G$.

**To Prove:** $H$ is a normal subgrp. iff. $g^{-1} \cdot H \cdot g \subseteq H$ $\forall g \in G$.

**Proof:** Forward proof:

$H$ is a normal subgroup.

$\therefore$ $g \circ H = H \circ g$

Pre multiply $g^{-1}$ both sides.

$g^{-1} \circ g \circ H = g^{-1} \circ H \circ g$

$H = g^{-1} \circ H \circ g$

$\therefore \; g^{-1} \circ N \circ g \subseteq N \quad \forall g \in G$

Backward Proof:-

$$g^{-1} \cdot H \cdot g \subseteq H \quad - (1)$$

Pre multiply with $g$.

$$H \cdot g \subseteq g \cdot H \quad - (2)$$

Post multiply (1) with $g^{-1}$

$$g^{-1} \cdot H \subseteq H \cdot g^{-1}$$

we can also say that

as $g^{-1} \in G$ & $g \in G$ $\quad g \cdot H \subseteq H \cdot g \quad - (3)$

From (2) & (3)

$$g \cdot H = H \cdot g$$

Since left cosets and rights coset induced by $H$ are equal.

$H$ is a normal subgroup.

Hence, Proved.

classmate

Date

Page

07

**Given:** $H$ is a normal subgroup of a Group $\langle G, \circ \rangle$

**To Prove:** $\langle G/H, \bullet \rangle$ is abelian iff $g_1 \circ g_2 \circ g_1^{-1} \circ g_2^{-1}$ is in $H$ $\forall$ $g_1, g_2 \in G$.

**Proof:** ① $\langle G/H, \bullet \rangle$ abelian

$\forall g_1, g_2 \in G \Rightarrow [g_1] \bullet [g_2] = [g_2] \bullet [g_1]$ — ①

$[g_1] \bullet [g_2] = [g_1 \circ g_2]$ — ② (by defn of Quotient Group).

$\Rightarrow [g_1 \circ g_2] = [g_2 \circ g_1]$

$g_1 \circ g_2 \circ H = g_2 \circ g_1 \circ H$ — ③

Pre multiply $g_1^{-1} \circ g_2^{-1} \circ$ in ③

$g_1^{-1} \circ g_2^{-1} \circ g_1 \circ g_2 \circ H = g_1^{-1} \circ g_2^{-1} \circ g_2 \circ g_1 \circ H$

$g_1^{-1} \circ g_2^{-1} \circ g_1 \circ g_2 \circ H = g_1^{-1} \circ e \circ g_1 \circ H$

$g_1^{-1} \circ g_2^{-1} \circ g_1 \circ g_2 \circ H = g_1^{-1} \circ g_1 \circ H$

$\Rightarrow g_1^{-1} \circ g_2^{-1} \circ g_1 \circ g_2 \circ H = H$ — ④

By Thm of cosets;

$h \circ H = H \circ h = H$ — ⑤ , $\forall h \in H$.

From ④ & ⑤;

$g_1^{-1} \circ g_2^{-1} \circ g_1 \circ g_2 \in H$ , $\forall g_1, g_2 \in G$

$g_1, g_2 \in G \Rightarrow g_1^{-1}, g_2^{-1} \in G$ (Inverse exists in a group).

replacing $g_1$ by $g_1^{-1}$ & $g_2$ by $g_2^{-1}$;

$\Rightarrow (g_1^{-1})^{-1} \circ (g_2^{-1})^{-1} \circ g_1^{-1} \circ g_2^{-1} \in H$ $\forall g_1, g_2 \in G$ $\{(a^{-1})^{-1} = a\}$

$\Rightarrow g_1 \circ g_2 \circ g_1^{-1} \circ g_2^{-1} \in H$

Hence, Proved.

$\forall\ g_1, g_2 \in G$

(2) $g_1 \circ g_2 \circ g_1^{-1} \circ g_2^{-1} \in H$

By Theorem of Cosets,

$h \circ H = H \circ h = H \quad \forall\ h \in H.$

$H \circ g_1 \circ g_2 \circ g_1^{-1} \circ g_2^{-1} = H \quad -(1) \quad \forall\ g_1, g_2 \in G.$

Multiplying $g_2 \circ g_1$ on right sides of (1);

$H \circ g_1 \circ g_2 \circ g_1^{-1} \circ g_2^{-1} \circ g_2 \circ g_1 = H \circ g_2 \circ g_1$ $\left( \begin{array}{l} a \circ a^{-1} = e \ (\forall\ a \in G) \\ a \circ e = e \circ a = a \ \forall\ e \in G \end{array} \right)$

$H \circ g_1 \circ g_2 \circ g_1^{-1} \circ e \circ g_1 = H \circ g_2 \circ g_1$

$H \circ g_1 \circ g_2 \circ g_1^{-1} \circ g_1 = H \circ g_2 \circ g_1$

$H \circ g_1 \circ g_2 \circ e = H \circ g_2 \circ g_1$

$\Rightarrow H \circ g_1 \circ g_2 = H \circ g_2 \circ g_1 \quad -(2)$

From (2) and definition of $[g] = H \circ g$ with respect to right coset operation;

$[g_1 \circ g_2] = [g_2 \circ g_1]$

$[g_1] \bullet [g_2] = [g_2] \bullet [g_1]$

$\langle G/H, \bullet \rangle$ is an abelian group.

Hence, Proved.

Q8 **Given:** A cyclic group $G$.

**To Prove:** Cyclic group is necessarily abelian, but converse is not True.

**Proof:** $G = \{ g^k : k > 0 \quad k \in \mathbb{Z} \quad \& \; g \in G \}$

$g$ is fixed and is called generator of group $G$.

$a, b \in G$: Let $a = g^p$ where $p > 0 \quad p \in \mathbb{Z}$

$b = g^q$ where $q > 0 \quad q \in \mathbb{Z}$.

$\therefore a \circ b = g^p \cdot g^q = g^{p+q}$ — (1)

$b \cdot a = g^q \cdot g^p = g^{q+p} = g^{p+q}$ — (2)

(1) = (2)

So $a \cdot b = b \cdot a$

So cyclic group is commutative.

Hence it's an an abelian.

Converse Part: (counter example)

Let group $G = \langle \mathbb{Z}, + \rangle$

$G$ is a group bcoz $G$ is closed, associative, existence of identity and existence of inverse.

$G$ is abelian as $\forall a, b \in G$.
$a + b = b + a$.
$G$ is an abelian.
But $G$ is not a cyclic group as there is not a fixed $g \in G$ which can generate all the elements of $G$.

If $g \neq 0$, we cannot generate $0$.
If $g = 0$, we cannot generate any other no's.
Hence it is not a cyclic group.

Hence, Proved.

Q9 Given: H and K be 2 normal subgroups of group G.
Product set $H \cdot K$ is the set of all products of form $h \cdot k$
$h$ in $H$ and $k$ in $K$.

To Prove: Product set $H \cdot K$ is normal subgroup of group G

Proof:- Let $h_1, h_2 \in H$ & $k_1, k_2 \in K$

$h_1 \circ k_1 \in H \cdot K$ $\quad$ $h_2 \circ k_2 \in H \cdot K$

$h_1 \circ h_2^{-1} \in H$ $\quad$ $k_1 \circ k_2^{-1} \in K$

For $H \cdot K$ to be a subgroup.

$(h_1 \cdot k_1) \circ (h_2 \cdot k_2)^{-1} \in H \cdot K$

$\Rightarrow (h_1 \circ k_1) \circ (k_2^{-1} \circ h_2^{-1})$

$\Rightarrow h_1 \circ (k_1 \circ k_2^{-1}) \circ h_2^{-1}$

[using $H \cdot K = K \cdot H$ as H is a normal subgroup]

$\Rightarrow (h_1 \circ h_2^{-1}) \circ (k_1 \circ k_2^{-1})$

$\Rightarrow h_1 \circ h_2^{-1} = h_0 \in H$

$\Rightarrow k_1 \circ k_2^{-1} = k_0 \in K$

$h_0 k_0 \in H \cdot K$

Thus $H \cdot K$ is a normal subgroup of group G.

For $H \cdot K$ to be a normal subgroup.

$g^{-1} \circ (H \cdot K) \circ g \subseteq H \cdot K$

Since H and K both are normal subgroup:

$g^{-1} \circ h \circ g \subseteq H$ $\quad$ $g^{-1} \circ k \circ g \subseteq K$

$\forall g \in G, \forall h \in H$ $\quad$ $\forall g \in G, \forall k \in K$

$$(g^{-1} \circ h \cdot g) \circ (g^{-1} \circ k \cdot g) \subseteq H \circ K$$

$$(g^{-1} \circ h) \circ (g \circ g^{-1}) \circ (k \cdot g) \subseteq H \circ K$$

$$(g^{-1} \circ h) \circ e \circ (k \cdot g) \subseteq H \cdot K$$

$$g^{-1} \circ (h \circ k) \circ g \subseteq H \cdot K$$

$\forall g \in G$, $\forall h \in H$, $\forall k \in K$

$\therefore$ $H \cdot K$ is a normal subgroup of group $G$.

Hence, proved.

Q10 Let group of order 12 be
$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
and binary operation be $(a+b) \bmod 12$

This is a group because :
① closed ③ Existence of identity (0)
② Associative ④ Existence of inverse.

Now to make a subgroup of order 6
first element we need is 0.

Now to choose other elements we need pair wise inverses (1, 11) (2, 10) (3, 9) (4, 8) (5, 7) (6, 0).

Now as 6 is the inverse of itself we need to choose 6 as 2nd element
Now we can choose 2 pairs to make 6 elements.

For eg: Subgroup of order 6 = $\{0, 6, 1, 11, 2, 10\}$

But this subgroup is not closed as
$(6+1) \bmod (12) \Rightarrow 7$

∴ we make a subgrp. of order 6, but this subgroup is not closed.

∴ we cannot make a subgroup of order 6

Hence, proved.