Institute: University of Basrah

College of Sciences

Department of Mathematics

Email: mohna_l@yahoo.com

mohammed.ibrahim@uobasrah.edu.iq

Date: October 8, 2022

Mohammed Alabbood

MOHAMMED ALI IBRAHIM

Half of knowledge is to say "I do not know"

Contents

GROUP THEORY: PART I

Binary operations

Definition: A **binary operation** $\star$ on a non empty set G is a map

$$\star : G \times G \longrightarrow G$$

$$(g, g') \longmapsto g \star g'.$$

That is, $\star(g, g') = g \star g' \in G$.

In this case, we say $(G, \star)$ a **mathematical system**.

Example:

1. $(\mathbb{N}, +)$ is a mathematical system, where

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} = \text{ set of natural numbers.}$$

2. $(\mathbb{Z}, +)$ is a mathematical system, where

$$\mathbb{Z} = \{0, \mp 1, \mp 2, \mp 3, \ldots\} = \text{ set of integer numbers.}$$

3. $(\mathbb{Q}, +)$ is a mathematical system, where

$$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\} = \text{ set of rational numbers.}$$

4. $(\mathbb{R}, +)$ is a mathematical system, where $\mathbb{R}$ is the set of real numbers.

5. $(\mathbb{C}, +)$ is a mathematical system, where

$$\mathbb{C} = \left\{a + bi : a, b \in \mathbb{R}\right\} = \text{ set of complex numbers.}$$

6. $(\mathbb{N}, -)$ is not mathematical system. In fact,

$$a = 2, b = 7 \text{ are elements in } \mathbb{N}, \text{ but } a - b = 2 - 7 = -5 \notin \mathbb{N}.$$

Note that: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

PROBLEMS: Which of the following is a mathematical system:

1. $(\mathbb{Z}, \star)$, where $a \star b = a \cdot b$.
2. $(\mathbb{Z}, \star)$, where $a \star b = a \div b$.
3. $(\mathbb{Z}, \star)$, where $a \star b = a + b - 2022$.
4. $(\mathbb{Q}, \star)$, where $a \star b = a \div b$.
5. $(\mathbb{Q}\backslash\{0\}, \star)$, where $a \star b = a \div b$.
6. $(\mathbb{R}, \star)$, where $a \star b = a^b$.

What is a group?

DEFINITION: A mathematical system $(G, \star)$ is said to be a **group** if

1. For all $a, b, c \in G : (a \star b) \star c = a \star (b \star c)$; [**Associativity**]
2. There is an element $e \in G$, called the **identity element of** G, such that
$$a \star e = e \star a = a \text{ for all } a \in G.$$
3. For all $a \in G$, there is an element $a^{-1} \in G$, called the **inverse of** a, such that
$$a \star a^{-1} = a^{-1} \star a = e.$$

EXAMPLE:

1. $(\mathbb{Z}, +)$ is a group. Note that $e = 0$ and $a^{-1} = -a$.
2. $(\mathbb{Q}, +)$ is a group. Note that $e = 0$ and $a^{-1} = -a$.
3. $(\mathbb{Q}\backslash\{0\}, \cdot)$ is a group. Note that $e = 1$ and $a^{-1} = 1/a$.
4. $(\mathbb{Z}, \cdot)$ is not group. Note that $a = 0$ has no inverse in $\mathbb{Z}$.
5. $(\mathbb{Z}\backslash\{0\}, \cdot)$ is not group. Note that $a = 2$ has no inverse in $\mathbb{Z}$.

Example: Define operation $\star$ on $\mathbb{Z}$ as follows:

$$a \star b = a + b - 7.$$

Prove that $(\mathbb{Z}, \star)$ is a group.

Proof It is clear that $\mathbb{Z} \neq \emptyset$ since $-7 \in \mathbb{Z}$. Also, $a \star b = a + b - 7 \in \mathbb{Z}$ for every $a, b \in \mathbb{Z}$. So, $\star$ is a binary operation on $\mathbb{Z}$.

1. For all $a, b, c \in \mathbb{Z}$:

$$\begin{aligned} \textbf{L.H.S} :&= (a \star b) \star c = (a + b - 7) \star c \\ &= (a + b - 7) + c - 7 = a + b + c - 14. \end{aligned}$$

$$\begin{aligned} \textbf{R.H.S} :&= a \star (b \star c) = a \star (b + c - 7) \\ &= a + (b + c - 7) - 7 = a + b + c - 14 = \textbf{L.H.S}. \end{aligned}$$

2. Assume that $e \in \mathbb{Z}$ such that $a \star e = e \star a = a$ for all $a \in \mathbb{Z}$. Then

$$\begin{aligned} e \star a = e &\Longrightarrow e + a - 7 = a \\ &\Longrightarrow e = a - a + 7 = 7. \end{aligned}$$

Hence, $e = 7 \in \mathbb{Z}$ is the identity of $\mathbb{Z}$.

3. Let $a^{-1} \in \mathbb{Z}$ is an inverse of $a \in \mathbb{Z}$. Then $a \star a^{-1} = a^{-1} \star a = e = 7$ and

$$\begin{aligned} a^{-1} \star a = 7 &\Longrightarrow a^{-1} + a - 7 = 7 \\ &\Longrightarrow a^{-1} = 14 - a. \end{aligned}$$

Hence, $a^{-1} = 14 - a \in \mathbb{Z}$ is the inverse of a.

The group of integers modulo n

Consider the finite set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, where n some positive integer. Let us define a binary operation on $\mathbb{Z}_n$ as follows:

$$a + b = \text{ the reminder when } a + b \text{ is divided by } n.$$

For example, if $n = 7$ and $5, 6 \in \mathbb{Z}_7$, then $5 + 6 = 11 = 4$ since $11 = 7 \cdot 1 + \mathbf{4}$.

In fact, $(\mathbb{Z}_n, +)$ forms a group. This group is called the **group of integers modulo** n.

What is the identity of $(\mathbb{Z}_n, +)$?

Answer: $e = 0$.

What is the inverse of $a \in \mathbb{Z}_n$?

Answer: $a^{-1} = n - a$.

Example: Let us give the group table for $(\mathbb{Z}_4, +)$:

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

Note that: $0^{-1} = 0$,$1^{-1} = 4 - 1 = 3$,$2^{-1} = 4 - 2 = 2$,$3^{-1} = 4 - 3 = 1$.

The symmetric group on n letters

Let $X = \{1, 2, \ldots, n\}$. The set of all bijection maps $\sigma : X \to X$, denoted by S_n, is called the **symmetric group** on X. An element $\sigma \in S_n$, called **permutation**, can be written as:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

How we composite two permutations?

Answer: Let $X = \{1, 2, 3, 4\}$ and let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Then

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

In fact, $(S_n, \circ)$ forms a group, called the **symmetric group or permutation group on n letters**.

What is the identity of $(S_n, \circ)$?

Answer: $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ (send everything to itself).

What is the inverse of $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \in S_n$?

Answer: $\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$.

Let us find the inverse of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ in S_4:

$$\sigma^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \qquad \text{(rearrangement)}.$$

For $i_1, i_2, \dots, i_k \in \{1, 2, \dots, n\}$, a k-**cycle** or **cycle of length** k

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{pmatrix} = (i_1\, i_2 \dots i_k)$$

where $i_1, i_2, \dots, i_k \in X = \{1, 2, \dots, n\}$ is a permutation $\sigma \in S_n$ such that

$$\sigma(i_m) = \begin{cases} i_{m+1} & \text{if } \; m \in \{1, 2, \ldots, k-1\}, \\ i_1 & \text{if } \; m = k, \\ i_m & \text{if } \; i_m \in X - \{1, 2, \ldots, k-1\}. \end{cases}$$

In particular, a 2-cycle in S_n is called a **transposition**.

In fact, every nonidentity permutation $\sigma \in S_n, n \geq 2$ can be uniquely expressed (up to the order of the factors) as a composition of disjoint cycles, where each cycle is of length at least 2.

Note that every k-cycle $(i_1\, i_2 \ldots i_k)$ can be written as a composition of transpositions:

$$(i_1\, i_2 \ldots i_k) = (i_1\, i_k) \circ (i_1\, i_{k-1}) \circ \ldots \circ (i_1\, i_2).$$

Hence, every permutation $\sigma \in S_n, n \geq 2$ can be expressed as a composition of transpositions.

Example:

1. We can write the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 5 & 1 & 6 & 2 \end{pmatrix}$ in S_7 as a composition of disjoint cycles as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 5 & 1 & 6 & 2 \end{pmatrix} = (1\,3\,4\,5) \circ (2\,7).$$

2. Consider the permutation $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 5 & 1 & 6 & 8 & 9 & 2 \end{pmatrix}$ in S_9.

Now, we can write σ as a composition of transpositions as follows:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 5 & 1 & 6 & 8 & 9 & 2 \end{pmatrix} = (1\,3\,4\,5) \circ (2\,7\,8\,9)$$

$$= (1\,5) \circ (1\,4) \circ (1\,3) \circ (2\,9) \circ (2\,8) \circ (2\,7).$$

DEFINITION: A permutation $\sigma \in S_n$ is said to be **even**(**odd**) permutation if it is written as the composition of even(odd) number of transpositions respectively.

Note that the permutation τ in the above example is an even permutation.

The Klein 4-group

The **Klein 4-group** is a group with four elements, namely $K = \{e, a, b, c\}$, which has the following group table:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note that $a \cdot a = b \cdot b = c \cdot c = e =$ identity of K.

What is the inverse of each element in $(K, \cdot)$?

Answer: $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$.

DEFINITION: The **order** of a group $(G, \star)$ is the number of elements in G. If the number of elements in a group G is finite and equal to n, then G is called **finite group**, and we write $|G| = n$. Otherwise, G is called **infinite group**, and we write $|G| = \infty$.

EXAMPLE: I. The group $(\mathbb{Z}_n, +)$ is finite and $|\mathbb{Z}_n| = n$.

Example: II. The group $(S_n, \circ)$ is finite. Note that

$$|S_n| = n! = n(n-1)(n-2)\dots 1.$$

Example: III. The The Klein 4-group $(K, \cdot)$ is finite and $|K| = 4$.

Example: IV. All the groups $(\mathbb{Z}, +)$,$(\mathbb{Q}, +)$,$(\mathbb{R}, +)$,$(\mathbb{C}, +)$ are infinite groups.

Orders of elements in groups

Definition: An element g in group $(G, \star)$ with identity e is called **of finite order** n, written $o(g) = n$, if n is the smallest positive integer such that

$$g^n = g \cdot g \cdot \dots \cdot g(n - \text{times}) = e \text{ “multiplicative notation” or}$$

$$ng = g + g + \dots + g(n - \text{times}) = e \text{ “additive notation”.}$$

Otherwise, g is called **of infinite order**, and we write $o(g) = \infty$.

Theorem: Let a be an element in a group $(G, \star)$ with identity e and $o(a) = n$. Then

1. $a^m = e, m \in \mathbb{Z}^+ \Longrightarrow n|m$.
2. $t \in \mathbb{Z}^+$ and $\gcd(t, n) = d \Longrightarrow o(a^t) = \frac{n}{d}$.

Proof

1. Using division algorithm, we get $m = nq + r$ where $0 \leq r < n$. Now,

$$a^r = a^{m-nq} = a^m \star (a^n)^q = e \star e = e.$$

So, $r = 0$ (minimality of n). Hence, $m = nq$, in other words, $n|m$.

2. Since $\gcd(t, n) = d$, there are two integers u, v such that $n = vd; t = ud$ and $\gcd(u, v) = 1$.

   Suppose that $o(a^t) = k$. Want to prove that $k = \frac{n}{d}$.

   Note that, $a^{kt} = e$ implies $n|kt$ (by assertion 1). So, $kt = nr$ for some integer r.

$$kt = nr \Longrightarrow kdu = vdr \Longrightarrow ku = vr.$$

   In this case, $v|ku$ and $\gcd(u, v) = 1 \Longrightarrow v|k \Longrightarrow \frac{n}{d}|k$. On the other hand,

$$(a^t)^{\frac{n}{d}} = a^{\frac{nt}{d}} = a^{\frac{ndu}{d}} = a^{nu} = (a^n)^u = e.$$

   Thus, $o(a^t) = k|\frac{n}{d}$ (by assertion 1). Finally, since $k, \frac{n}{d}$ are positive integers, we get $o(a^t) = \frac{n}{d}$.

Example: I. In group $(\mathbb{Z}_6, +)$, the order of elements are shown in the following table:

element	order		
0	**1**	since	$\mathbf{1}(0) = 0$
1	**6**	since	$\mathbf{6}(1) = 6 = 0$
2	**3**	since	$\mathbf{3}(2) = 6 = 0$
3	**2**	since	$\mathbf{2}(3) = 6 = 0$
4	**3**	since	$\mathbf{3}(4) = 12 = 0$
5	**6**	since	$\mathbf{6}(5) = 30 = 0.$

Example: II. What is the order of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ in ($S_4, \circ$)?

Answer:

$$\sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e.$$

So, $o(\sigma) = 2$.

Example: III. In the Klein 4-group $(K, \cdot)$, the order of elements are shown in the following table:

element	order		
e	**1**	since	$e^{\mathbf{1}} = e$
a	**2**	since	$a^{\mathbf{2}} = a \cdot a = e$
b	**2**	since	$b^{\mathbf{2}} = b \cdot b = e$
c	**2**	since	$c^{\mathbf{2}} = c \cdot c = e.$

Example: IV. In the groups $(\mathbb{Z}, +)$, $o(0) = 1$ and the other integers have infinite orders.

Abelian groups

Definition: A group $(G, \star)$ is said to be **abelian** if $a \star b = b \star a$ for all $a, b \in G$.

Example: I.

1. All the groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups.
2. $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$ and $(\mathbb{C}\backslash\{0\}, \cdot)$ are abelian groups.

Example: II.

1. The Klein 4-group K is an abelian group. From the table of the Klein 4-group, we have
$$ab = ba, ac = ca, bc = cb, ea = ae, eb = be \text{ and } ec = ce.$$
2. The symmetric group $(S_3, \circ)$ is not abelian group. Note that $(1\ 2)$ and $(2\ 3)$ are two permutations in S_3 and
$$(1\ 2) \circ (2\ 3) = (1\ 2\ 3) \text{ while } (2\ 3) \circ (1\ 2) = (1\ 3\ 2).$$
So, $(1\ 2) \circ (2\ 3) \neq (2\ 3) \circ (1\ 2)$.

External direct product of groups

Let $(G_j; \star_j)$ be groups with identity e_j; $j = 1, \ldots, k$. Let $G = \prod_{j=1}^{k} G_j$. Then $(G; \star)$ is a group with identity $e = (e_1, e_2, \ldots, e_k)$ under the operation
$$(a_1, a_2, \ldots, a_k) \star (b_1, b_2, \ldots, b_k) = (a_1 \star_1 b_1, a_2 \star_2 b_2, \ldots, a_k \star_k b_k).$$
This group is called the **external direct product of the groups** G_j; $j = 1, \ldots, k$.

Note that $G = \prod_{j=1}^{k} G_j$ is an abelian group if all the groups G_j; $j = 1, \ldots, k$ are abelian groups. Moreover, the inverse of $(a_1, a_2, \ldots, a_k)$ in G is
$$(a_1, a_2, \ldots, a_k)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1})$$
where a_j^{-1} is the inverse of a_j in G_j.

Example: Let us find the group table of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ under componentwise addition.

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Here, $(0,0)$ acts as the identity of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Moreover, every non identity element has order 2:

$o(0,1) = 2$ since $(0,1)+(0,1) = (0,2) = (0,0)$ modulo 2. Similarly, $o(1,0) = o(1,1) = 2$.

Problems: I.

1. Prove that the identity in a group $(G, \star)$ is unique.
2. Prove that the inverse of an element in a group $(G, \star)$ is unique.
3. In a group $(G, \star)$ with identity e, prove that
   (a). Both $a \star b = a \star c$ and $b \star a = c \star a$ implies $b = c$ [These are called the **cancellation laws** in group].
   (b). $(a^{-1})^{-1} = a$.
   (c). $(a \star b)^{-1} = b^{-1} \star a^{-1}$.
   (d). $(a_1 \star a_2 \star \ldots \star a_n)^{-1} = a_n^{-1} \star a_{n-1}^{-1} \star \ldots \star a_1^{-1}$ for every $a_1, a_2, \ldots, a_n$ in G.

Problems: II.

1. In a group $(G, \star)$ with identity e, define $a^0 = e$ and
$$a^n = a \star a \star \ldots \star a \ (n - \text{times})$$
$$a^{-n} = a^{-1} \star a^{-1} \star \ldots \star a^{-1} \ (n - \text{times})$$
for any positive integer n. Prove that
(a). $a^n \star a^m = a^{n+m}$,
(b). $(a^n)^m = a^{nm}$
for any integers n, m.
2. In abelian group $(G, \star)$, prove that $(a \star b)^n = a^n \star b^n$ for any integer n. In particular, $(a \star b)^{-1} = a^{-1} \star b^{-1} \Leftrightarrow G$ is an abelian group.
3. In a group $(G, \star)$, prove that there is unique solution $x(y)$ for the equations $a \star x = b$ $(y \star a = b)$ respectively.
4. Find all even permutations in $(S_3, \circ)$.
5. Find inverse and order of each element in $(\mathbb{Z}_{12}, +)$.
6. What is the order of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ in $(\mathrm{S}_4, \circ)$? What is the inverse of σ?.
7. Write $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 5 & 3 & 7 & 6 \end{pmatrix}$ in $(S_7, \circ)$ as a composition of transpositions. What is the inverse of τ?.

Subgroups

Definition: An non empty subset H of group $(G,\star)$ is said to be **subgroup** of G, written $H \leq G$ if

1. $e \in H$,
2. $x \star y^{-1} \in H$ for all $x, y \in H$.

If $H \leq G$ and $H \neq G$, we say H **proper subgroup** of G, and we write $H < G$.

Theorem: Given a group $(G,\star)$ with identity e. The intersection of any family of subgroups of G is again subgroup of G.

Proof Assume that $H_\lambda \leq G$ for all $\lambda \in \Lambda$. Let $H = \bigcap\limits_{\lambda\in\Lambda} H_\lambda$. Want to prove that $H \leq G$.

1. Since $e \in H_\lambda$ for all $\lambda \in \Lambda \Longrightarrow e \in \bigcap\limits_{\lambda\in\Lambda} H_\lambda = H \Longrightarrow e \in H$.
2. Let $x, y \in H = \bigcap\limits_{\lambda\in\Lambda} H_\lambda$. Then $x, y \in H_\lambda$ for every $\lambda \in \Lambda \Longrightarrow$
   $x \star y^{-1} \in H_\lambda$ for every $\lambda \in \Lambda$ since $H_\lambda \leq G \Longrightarrow$
   $x \star y^{-1} \in \bigcap\limits_{\lambda\in\Lambda} H_\lambda = H \Longrightarrow x \star y^{-1} \in H$.
   Hence, by definition $H \leq G$.

Question: Are the union of two subgroups of a group again subgroup?

Example: I.

1. Given a group $(G, \star)$ with identity e. The sets $\{e\}$ and G itself form subgroups of G [**Trivial subgroups**].
2. $\{0\} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ under usual addition.
3. $\{1\} < \mathbb{Q}\backslash\{0\} < \mathbb{R}\backslash\{0\} < \mathbb{C}\backslash\{0\}$ under usual multiplication.
4. The subsets $\{e, a\}$, $\{e, b\}$ and $\{e, c\}$ form proper subgroup of Klein 4-group K.
5. $\mathbb{Z}_o$ = set of odd integers is not subgroup of $(\mathbb{Z}, +)$. Note that $3 - 1 = 2 \notin \mathbb{Z}_o$.

Example: II. Let H be a subgroup of a group $(G, \star)$ with identity e and let $a \in G$. Show that the subset

$$a \star H \star a^{-1} = \{a \star h \star a^{-1} : h \in H\}$$

is again subgroup of G.

Proof Since $H \leq G$, we have $e \in H$.

1. $e \in a \star H \star a^{-1}$ since $e = a \star a^{-1} = a \star e \star a^{-1}$ "$e \in H$".
2. Let $x, y \in a \star H \star a^{-1}$. Then $x = a \star h \star a^{-1}$ and $y = a \star h' \star a^{-1}$ for some $h, h' \in H$.

$$\begin{aligned} x \star y^{-1} &= (a \star h \star a^{-1}) \star (a \star h' \star a^{-1})^{-1} \\ &= (a \star h \star a^{-1}) \star ((a^{-1})^{-1} \star h'^{-1} \star a^{-1}) \\ &= (a \star h \star a^{-1}) \star (a \star h'^{-1} \star a^{-1}) \\ &= a \star (h \star a^{-1} \star a \star h'^{-1}) \star a^{-1} = a \star (h \star e \star h'^{-1}) \star a^{-1} \\ &= a \star (h \star h'^{-1}) \star a^{-1} = a \star h'' \star a^{-1} \in a \star H \star a^{-1} \end{aligned}$$

where $h'' = h \star h'^{-1} \in H$.

DEFINITION: Let S be any subset of a group $(G, \star)$. The **subgroup generated by** S, denoted by $\langle S\rangle$ is the intersection of all subgroup of G containing S. In fact, $\langle S\rangle$ is the smallest subgroup of G that containing S. If $S = \{a\}$, we write $\langle S\rangle = \langle a\rangle$ which is called the **cyclic subgroup** generated by a. In particular, if there is an element $a \in G$ such that $G = \langle a\rangle$, we say G **cyclic group**. More precisely:

$$\langle a\rangle = \{a^n : n \in \mathbb{Z}\} \qquad \text{(multiplicative notation)}$$

or

$$\langle a\rangle = \{na : n \in \mathbb{Z}\} \qquad \text{(additive notation).}$$

EXAMPLE: I. Let us consider the **dihedral group of degree** n, denoted by D_n, where

$$D_n = \{e, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$$

and $a^n = b^2 = e;\ aba = b$. This group has order $2n$. The subgroup of D_n generated by a is

$$\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

The subgroup of D_n generated by b is

$$\langle b\rangle = \{e, b\}.$$

EXAMPLE: II. Let us find all cyclic subgroups of the group $(\mathbb{Z}_6, +)$. Using the additive notation, we get all cyclic subgroups of $(\mathbb{Z}_6, +)$:

$$\langle 0\rangle = \{0\}$$
$$\langle 1\rangle = \{1,2,3,4,5,6=0\} = \mathbb{Z}_6$$
$$\langle 2\rangle = \{2,4,6=0\}$$
$$\langle 3\rangle = \{3,6=0\}$$
$$\langle 4\rangle = \{4,8=2,6=0\} = \langle 2\rangle$$
$$\langle 5\rangle = \{5,10=4,9=3,8=2,7=1,6=0\} = \mathbb{Z}_6$$

So, we have only 4 distinct cyclic subgroups of $(\mathbb{Z}_6,+)$, namely $\langle 0\rangle$, $\langle 1\rangle$, $\langle 2\rangle$ and $\langle 3\rangle$.

Example: III.

1. The group $(\mathbb{Z},+)$ is cyclic group with two generators.

   In fact, $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$.

2. The group $(\mathbb{R},+)$ is not cyclic group. In fact, there is no real number α such that $\mathbb{R} = \langle \alpha\rangle$.

3. The cyclic subgroups of the Klein 4-group K are:

$$\langle e\rangle,\ \langle a\rangle,\ \langle b\rangle,\ \langle c\rangle.$$

   However, K is not cyclic.

EXERCISES

1. If $(G,\star)$ a group such that $a^2 = e$ for all $a \in G$. Prove that G is abelian.

2. Define an operation $\star$ on $G = \mathbb{R}\times\mathbb{R}\backslash\{0\}$ as follows:

$$(a,b)\star(c,d) = (a+bc, bd) \text{ for all } (a,b),(c,d) \in G.$$

   Show that $(G,\star)$ is a group. Is G abelian?

3. Define an operation $\star$ on $G = \mathbb{R}\backslash\{0\} \times \mathbb{R}$ as follows:

$$(a,b) \star (c,d) = (ac, bc + d) \text{ for all } (a,b),(c,d) \in G.$$

Show that $(G,\star)$ is a group which has infinitely many element of order 2.

4. Let $(G,\star)$ be a group and $a,b \in G$. Show that
   (a). $o(a) = o(a^{-1})$,
   (b). $o(a) = o(b^{-1} \star a \star b)$,
   (c). $o(a \star b) = o(b \star a)$.

5. Show that the set of all even permutations forms a subgroup of the symmetric group $(S_n, \circ)$. This group is denoted by A_n which is called the **alternating group** on n letters. What is the order of A_n?

6. Consider the subset $H = \{2^n : n \in \mathbb{Z}\}$ of the group $(\mathbb{Q}\backslash\{0\}, \cdot)$. Prove that $H \leq \mathbb{Q}\backslash\{0\}$.

7. Let $(G,\star)$ be a group and let $a \in G$. Define

   $C(a) = \{b \in G : ab = ba\}$ **[This is called the centralizer of a]**

   $Z(G) = \{b \in G : ab = ba \text{ for all } a \in G\}$ **[This is called the center of G].**

   Prove that
   (a). $C(a) \leq G$,
   (b). $Z(G) \leq G$,
   (c). $Z(G) = \bigcap_{a \in G} C(a)$,
   (d). G abelian $\Longleftrightarrow Z(G) = G$.

8. Let $(G,\star)$ be a group, and let H,K be subgroups of G. Define

$$H \star K = \{h \star k : h \in H, k \in K\}.$$

Show that $H \star K \leq G \Longleftrightarrow H \star K = K \star H$.

9. Show that $(\mathbb{Z}_{12}, +)$ is a cyclic group. Find the number of its genera-

tors.

10. Prove that any cyclic group is abelian.

11. Prove that any subgroup of a cyclic group is cyclic.

12. Let $(G, \star)$ be cyclic group of finite order n. Prove that for any $d|n$ there is a subgroup of G of order d.

13. Let $(G, \star)$ be cyclic group of finite order n and let $a \in G$. Prove that a^k is a generator of G if and only if $\gcd(k, n) = 1$.

14. Find all subgroups of D_4. Is D_4 abelian group? How many element of order 2 in D_4?

15. Find all subgroups of $(\mathbb{Z}, +)$.

16. True or False:

    (a). Every element in a cyclic group $(G, \star)$ is a generator of G.

    (b). A group $(G, \star)$ is abelian if and only if $(G, \star)$ is a cyclic group.

    (c). Any subgroup of an abelian group is abelian.

    (d). Every group $(G, \star)$ of order ≤ 4 is cyclic.

    (e). Every proper subgroup of $(\mathbb{Z}, +)$ has infinite order.

    (f). There is a subgroup of $(S_4, \circ)$ of order 6.

17. Let σ be a k-cycle in $(S_n, \circ)$. Show that $o(\sigma) = k$.

18. Let σ, τ be disjoint cycles in $(S_n, \circ)$ such that $o(\sigma) = r$ and $o(\tau) = s$. Prove that $\sigma \circ \tau = \tau \circ \sigma$ and $o(\sigma \circ \tau) = \mathsf{lcm}(r, s)$.

19. Write $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 3 & 9 & 7 & 4 & 1 & 10 & 6 & 8 \end{pmatrix}$ as a composition of disjoint cycles in $(S_{10}, \circ)$. What is the order of σ? Is σ even or odd?