Abstract Algebra I
Chapter 1
Group Theory

Dr. Sanhan M. S. Khasraw

Salahaddin University-Erbil
College of Basic Education
Department of Mathematics
Third Year
Fall 2021-2022

Two Important Groups

1. The Group of Integers Modulo n

Definition 1.2.1: Let n be a fixed positive integer. Two integers a and b are said to be **congruent modulo** n, written

$$a \equiv b(mod\ n),$$

if and only if the difference $a - b$ is divisible by n. That is, $a \equiv b(mod\ n)$ if and only if $a - b = kn$ for some integer k.

Two Important Groups

1. The Group of Integers Modulo n

Definition 1.2.1: Let n be a fixed positive integer. Two integers a and b are said to be **congruent modulo** n, written

$$a \equiv b(mod\ n),$$

if and only if the difference $a - b$ is divisible by n. That is, $a \equiv b(mod\ n)$ if and only if $a - b = kn$ for some integer k.

Example 1.2.2:

If $n = 7$, we have

1. $3 \equiv 24 \pmod 7$,

1. The Group of Integers Modulo n

Definition 1.2.1: Let n be a fixed positive integer. Two integers a and b are said to be **congruent modulo** n, written

$$a \equiv b(mod\ n),$$

if and only if the difference $a - b$ is divisible by n. That is, $a \equiv b(mod\ n)$ if and only if $a - b = kn$ for some integer k.

Example 1.2.2:

If $n = 7$, we have

1. $3 \equiv 24 \pmod 7$,
2. $-5 \equiv 2 \pmod 7$,

Two Important Groups

1. The Group of Integers Modulo n

Definition 1.2.1: Let n be a fixed positive integer. Two integers a and b are said to be **congruent modulo** n, written

$$a \equiv b(mod\ n),$$

if and only if the difference $a - b$ is divisible by n. That is, $a \equiv b(mod\ n)$ if and only if $a - b = kn$ for some integer k.

Example 1.2.2:

If $n = 7$, we have

1. $3 \equiv 24 \pmod 7$,
2. $-5 \equiv 2 \pmod 7$,
3. $-8 \equiv -50 \pmod 7$, etc.

Two Important Groups

If $a - b$ is not divisible by n, we say that a is incongruent to b modulo n and, in this case, write $a \not\equiv b (\text{mod } n)$.

Two Important Groups

If $a - b$ is not divisible by n, we say that a is incongruent to b modulo n and, in this case, write $a \not\equiv b (\text{mod } n)$.

Example 1.2.3:

1. $7 \not\equiv 2 \ (\text{mod } 4)$,

Two Important Groups

If $a - b$ is not divisible by n, we say that a is incongruent to b modulo n and, in this case, write $a \not\equiv b (\text{mod } n)$.

Example 1.2.3:

1. $7 \not\equiv 2 \pmod 4$,
2. $17 \not\equiv 3 \pmod 5$.

Two Important Groups

Theorem 1.2.4: Let n be a fixed positive integer and a, b be arbitrary integers. Then $a \equiv b(mod\ n)$ if and only if a and b have the same remainder when divided by n.

Two Important Groups

Theorem 1.2.4: Let n be a fixed positive integer and a, b be arbitrary integers. Then $a \equiv b(mod\ n)$ if and only if a and b have the same remainder when divided by n.

Example: $15 \equiv 7 \pmod 4$ because $15 = 4 \cdot 3 + 3$ and $7 = 4 \cdot 1 + 3$

Two Important Groups

Theorem 1.2.5: Let n be a fixed positive integer and a, b, c, d be arbitrary integers. Then

(1) $a \equiv a (mod\ n)$,

Two Important Groups

Theorem 1.2.5: Let n be a fixed positive integer and a, b, c, d be arbitrary integers. Then

(1) $a \equiv a (mod\ n)$,

(2) if $a \equiv b (mod\ n)$, then $b \equiv a (mod\ n)$,

Two Important Groups

Theorem 1.2.5: Let n be a fixed positive integer and a, b, c, d be arbitrary integers. Then

(1) $a \equiv a (mod\ n)$,

(2) if $a \equiv b (mod\ n)$, then $b \equiv a (mod\ n)$,

(3) if $a \equiv b (mod\ n)$ and $b \equiv c (mod\ n)$, then $a \equiv c (mod\ n)$,

Two Important Groups

Theorem 1.2.5: Let n be a fixed positive integer and a, b, c, d be arbitrary integers. Then

(1) $a \equiv a (mod\ n)$,

(2) if $a \equiv b (mod\ n)$, then $b \equiv a (mod\ n)$,

(3) if $a \equiv b (mod\ n)$ and $b \equiv c (mod\ n)$, then $a \equiv c (mod\ n)$,

(4) if $a \equiv b (mod\ n)$ and $c \equiv d (mod\ n)$, then
$a + c \equiv b + d (mod\ n)$, $ac \equiv bd (mod\ n)$,

Two Important Groups

Theorem 1.2.5: Let n be a fixed positive integer and a, b, c, d be arbitrary integers. Then

(1) $a \equiv a (mod\ n)$,

(2) if $a \equiv b (mod\ n)$, then $b \equiv a (mod\ n)$,

(3) if $a \equiv b (mod\ n)$ and $b \equiv c (mod\ n)$, then $a \equiv c (mod\ n)$,

(4) if $a \equiv b (mod\ n)$ and $c \equiv d (mod\ n)$, then
$a + c \equiv b + d (mod\ n)$, $ac \equiv bd (mod\ n)$,

(5) if $a \equiv b (mod\ n)$, then $ac \equiv bc (mod\ n)$,

Two Important Groups

Theorem 1.2.5: Let n be a fixed positive integer and a, b, c, d be arbitrary integers. Then

(1) $a \equiv a (mod\ n)$,

(2) if $a \equiv b (mod\ n)$, then $b \equiv a (mod\ n)$,

(3) if $a \equiv b (mod\ n)$ and $b \equiv c (mod\ n)$, then $a \equiv c (mod\ n)$,

(4) if $a \equiv b (mod\ n)$ and $c \equiv d (mod\ n)$, then $a + c \equiv b + d (mod\ n)$, $ac \equiv bd (mod\ n)$,

(5) if $a \equiv b (mod\ n)$, then $ac \equiv bc (mod\ n)$,

(6) if $a \equiv b (mod\ n)$, then $a^k \equiv b^k (mod\ n)$ for every positive integer k.

Two Important Groups

Note 1.2.6: The converse of part (5) fails to be true. For instance, $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, yet $4 \not\equiv 1 \pmod{6}$.

Two Important Groups

Note 1.2.6: The converse of part (5) fails to be true. For instance, $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, yet $4 \not\equiv 1 \pmod{6}$.

Theorem 1.2.7: If $ca \equiv cb \pmod{n}$ and c is relatively prime to n, then $a \equiv b \pmod{n}$.

Two Important Groups

Definition 1.2.8: For an arbitrary integer a, let $[a]$ denote the set of all integers congruent to a modulo n:

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a(mod\ n)\}$$

$$= \{x \in \mathbb{Z} \mid x = a + kn \text{ for some integer } k\}.$$

We call $[a]$ the **congruence class**, modulo n, determined by a and refer to a as a **representative** of this class.

Two Important Groups

Example 1.2.9: If we deal with congruence modulo 3, then

$$[0] = \{x \in \mathbb{Z} \mid x = 3k \text{ for some } k \in \mathbb{Z}\}$$
$$= \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}.$$

Two Important Groups

Example 1.2.9: If we deal with congruence modulo 3, then

$$[0] = \{x \in \mathbb{Z} \mid x = 3k \text{ for some } k \in \mathbb{Z}\}$$
$$= \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}.$$

Also

$$[1] = \{x \in \mathbb{Z} \mid x = 1 + 3k \text{ for some } k \in \mathbb{Z}\}$$
$$= \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}.$$

Two Important Groups

Example 1.2.9: If we deal with congruence modulo 3, then

$$[0] = \{x \in \mathbb{Z} \mid x = 3k \text{ for some } k \in \mathbb{Z}\}$$
$$= \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}.$$

Also

$$[1] = \{x \in \mathbb{Z} \mid x = 1 + 3k \text{ for some } k \in \mathbb{Z}\}$$
$$= \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}.$$

Similarly,

$$[2] = \{x \in \mathbb{Z} \mid x = 2 + 3k \text{ for some } k \in \mathbb{Z}\}$$
$$= \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}.$$

Two Important Groups

Observe that every integer lies in one of these three classes. Integers in the same congruence class are congruent modulo 3, while integers in different classes are incongruent modulo 3. In the above illustration, for instance,

$$[-7] = [2] = [11] = [35] = \cdots$$

For convenience, one often selects the smallest nonnegative integer from each class to represent it.
For the general case of congruence modulo n, we write

$$\mathbb{Z}_n = \{[0], [1], [2], \cdots, [n-1]\}.$$

Two Important Groups

Theorem 1.2.10: Let n be a positive integer and $\mathbb{Z}_n$ be as defined before. Then

(1) for each $[a] \in \mathbb{Z}_n$, $[a] \neq \phi$,

Two Important Groups

Theorem 1.2.10: Let n be a positive integer and $\mathbb{Z}_n$ be as defined before. Then

(1) for each $[a] \in \mathbb{Z}_n$, $[a] \neq \phi$,

(2) if $[a] \in \mathbb{Z}_n$ and $b \in [a]$, then $[b] = [a]$.

Two Important Groups

Theorem 1.2.10: Let n be a positive integer and $\mathbb{Z}_n$ be as defined before. Then

(1) for each $[a] \in \mathbb{Z}_n$, $[a] \neq \phi$,

(2) if $[a] \in \mathbb{Z}_n$ and $b \in [a]$, then $[b] = [a]$.

(3) for any $[a], [b] \in \mathbb{Z}_n$ where $[a] \neq [b]$, $[a] \cap [b] = \phi$,

Two Important Groups

Theorem 1.2.10: Let n be a positive integer and $\mathbb{Z}_n$ be as defined before. Then

(1) for each $[a] \in \mathbb{Z}_n$, $[a] \neq \phi$,

(2) if $[a] \in \mathbb{Z}_n$ and $b \in [a]$, then $[b] = [a]$.

(3) for any $[a], [b] \in \mathbb{Z}_n$ where $[a] \neq [b]$, $[a] \cap [b] = \phi$,

(4) $\cup\{[a] \mid a \in \mathbb{Z}\} = \mathbb{Z}$.

Two Important Groups

Definition 1.2.11: A binary operation $+_n$ may be defined on $\mathbb{Z}_n$ as follows: for each $[a], [b] \in \mathbb{Z}_n$, let $[a] +_n [b] = [a + b]$.

Two Important Groups

Definition 1.2.11: A binary operation $+_n$ may be defined on $\mathbb{Z}_n$ as follows: for each $[a], [b] \in \mathbb{Z}_n$, let $[a] +_n [b] = [a + b]$.

Prove that $+_n$ is well defined.

Two Important Groups

Example 1.2.12: Suppose we consider congruence modulo 7. Then

$$[3] +_7 [6] = [3 + 6] = [9] = [2],$$

and

Two Important Groups

Example 1.2.12: Suppose we consider congruence modulo 7. Then

$$[3] +_7 [6] = [3 + 6] = [9] = [2],$$

and

$$[10] +_7 [-15] = [10 - 15] = [-5] = [2].$$

The Group of Integers Modulo n

Theorem 1.2.13: For each positive integer n, the mathematical system $(\mathbb{Z}_n, +_n)$ forms a commutative group, known as the *group of integers modulo n*.

Example 1.2.14: The operation table for $(\mathbb{Z}_4, +_4)$ is

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The Group of Integers Modulo n

For simplicity, we often write $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$. With this notation, the above operation table assumes the form

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2. The Symmetric Group on n Symbols

Definition 1.2.15: By a **permutation** of the set N is meant any one-to-one mapping of N onto itself.

2. The Symmetric Group on n Symbols

Definition 1.2.15: By a **permutation** of the set N is meant any one-to-one mapping of N onto itself.

We can represent f in a two-line form

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}.$$

The Symmetric Group on n Symbols

Example 1.2.17: If $N = \{1, 2, 3\}$, then there are $3! = 6$ permutations in S_3, namely,

The Symmetric Group on n Symbols

Example 1.2.17: If $N = \{1, 2, 3\}$, then there are $3! = 6$ permutations in S_3, namely,

$$i = f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \; f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \; f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \; f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \; f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

The Symmetric Group on n Symbols

Example 1.2.17: If $N = \{1, 2, 3\}$, then there are $3! = 6$ permutations in S_3, namely,

$$i = f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \; f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \; f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \; f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \; f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Thus, $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.

The Symmetric Group on n Symbols

A typical multiplication, say $f_4 \circ f_6$, proceeds as follows:

$$f_4 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_2.$$

The Symmetric Group on n Symbols

A typical multiplication, say $f_4 \circ f_6$, proceeds as follows:

$$f_4 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_2.$$

On the other hand, we have

$$f_6 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_3,$$

so that multiplication of permutations is not commutative.

The Symmetric Group on n Symbols

Theorem 1.2.18: The pair $(S_n, \circ)$ forms a group, known as the **symmetric group on n symbols**, which is noncommutative for $n \geq 3$.

The Symmetric Group on n Symbols

Theorem 1.2.18: The pair $(S_n, \circ)$ forms a group, known as the **symmetric group on n symbols**, which is noncommutative for $n \geq 3$.

The identity for $(S_n, \circ)$ is the permutation $i = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ and the inverse of any permutation $f \in S_n$ is described by

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Definition 1.2.19: Let $n_1, n_2, \cdots, n_k$ be k distinct integers between 1 and n. If a permutation $f \in S_n$ is such that

$$\begin{aligned} f(n_i) &= n_{i+1} \text{ for } 1 \leq i < k, \\ f(n_k) &= n_1, \text{ and} \\ f(n) &= n \text{ for } n \notin \{n_1, n_2, \cdots, n_k\}, \end{aligned}$$

then f is said to be a $k-$**cycle**, or a **cycle of length** k.

The Symmetric Group on n Symbols

Definition 1.2.19: Let $n_1, n_2, \cdots, n_k$ be k distinct integers between 1 and n. If a permutation $f \in S_n$ is such that

$$\begin{aligned} f(n_i) &= n_{i+1} \text{ for } 1 \leq i < k, \\ f(n_k) &= n_1, \text{ and} \\ f(n) &= n \text{ for } n \notin \{n_1, n_2, \cdots, n_k\}, \end{aligned}$$

then f is said to be a $k-$**cycle**, or a **cycle of length** k.

Remark 1.2.20: Any two-line form can be written in the form $(n_1 \;\; n_2 \;\; \cdots \;\; n_k)$.

The Symmetric Group on n Symbols

Example 1.2.21: In the symmetric group $(S_5, \circ)$, for example, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = (2\ \ 5\ \ 3).$$

The Symmetric Group on n Symbols

Example 1.2.21: In the symmetric group $(S_5, \circ)$, for example, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = (2\ \ 5\ \ 3).$$

Example 1.2.22: Write all elements of $(S_3, \circ)$ in cycle form.

The Symmetric Group on n Symbols

Theorem 1.2.23: Every permutation $f \in S_n$ can be written as a commutative product of cycles, no two of which have an element in common.

The Symmetric Group on n Symbols

Theorem 1.2.23: Every permutation $f \in S_n$ can be written as a commutative product of cycles, no two of which have an element in common.

Example 1.2.24: In the symmetric group $(S_5, \circ)$,

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

Definition 1.2.25: Any cycle of length two is called a **transposition**.

The Symmetric Group on n Symbols

Definition 1.2.25: Any cycle of length two is called a **transposition**.

Example 1.2.26: List all transpositions in the group $(S_3, \circ)$.

Corollary 1.2.27: Every permutation may be expressed as the product of transpositions.

Corollary 1.2.27: Every permutation may be expressed as the product of transpositions.

A $k-$cycle $(1 \;\; 2 \;\; \cdots \;\; k)$ can be written as a product of $k-1$ transpositions in the following manner:

$$(1 \;\; 2 \;\; \cdots \;\; k) = (1 \;\; k) \circ (1 \;\; k-1) \circ \cdots \circ (1 \;\; 2).$$

Corollary 1.2.27: Every permutation may be expressed as the product of transpositions.

A $k-$cycle $(1 \;\; 2 \;\; \cdots \;\; k)$ can be written as a product of $k-1$ transpositions in the following manner:

$$(1 \;\; 2 \;\; \cdots \;\; k) = (1 \;\; k) \circ (1 \;\; k-1) \circ \cdots \circ (1 \;\; 2).$$

Example 1.2.28:
In $(S_3, \circ)$, $(1 \;\; 2 \;\; 3) = (1 \;\; 3) \circ (1 \;\; 2)$.

The Symmetric Group on n Symbols

Definition 1.2.29: A permutation is **even** if it can be written as a product of even number of transpositions, and is **odd** if it can be written as a product of odd number of transpositions.

The Symmetric Group on n Symbols

Definition 1.2.29: A permutation is **even** if it can be written as a product of even number of transpositions, and is **odd** if it can be written as a product of odd number of transpositions.

Example 1.2.30: List all even and odd permutations in the group $(S_3, \circ)$.

The Symmetric Group on n Symbols

Definition 1.2.31: The subset of S_n consisting of all even permutations of n letters with the operation $\circ$ is called the **alternating group** and denoted by $(A_n, \circ)$.

The Symmetric Group on n Symbols

Definition 1.2.31: The subset of S_n consisting of all even permutations of n letters with the operation $\circ$ is called the **alternating group** and denoted by $(A_n, \circ)$.

Example 1.2.32: $A_3 = \{i, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$.

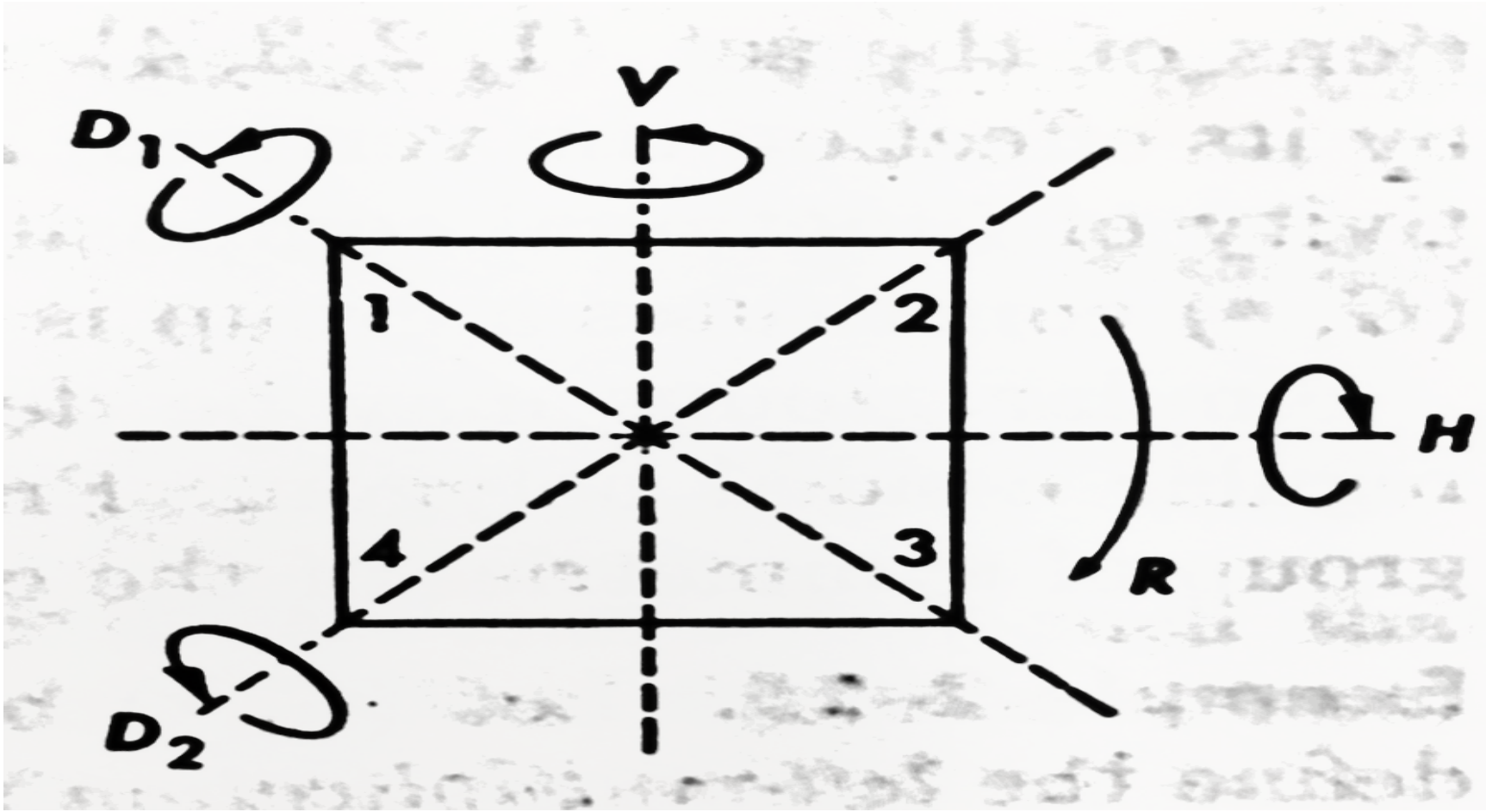
The Symmetric Group on n Symbols

Definition 1.2.31: The subset of S_n consisting of all even permutations of n letters with the operation $\circ$ is called the **alternating group** and denoted by $(A_n, \circ)$.

Example 1.2.32: $A_3 = \{i, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$.

Example 1.2.33: The elements of A_4 are:

Dihedral Group of Order 8(D_8)



Dihedral Group of Order 8(D_8)

$*$	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
R_{90}	R_{180}	R_{270}	R_{360}	R_{90}	D_1	D_2	V	H
R_{180}	R_{270}	R_{360}	R_{90}	R_{180}	V	H	D_2	D_1
R_{270}	R_{360}	R_{90}	R_{180}	R_{270}	D_2	D_1	H	V
R_{360}	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
H	D_2	V	D_1	H	R_{360}	R_{180}	R_{270}	R_{90}
V	D_1	H	D_2	V	R_{180}	R_{360}	R_{90}	R_{270}
D_1	H	D_2	V	D_1	R_{90}	R_{270}	R_{360}	R_{180}
D_2	V	D_1	H	D_2	R_{270}	R_{90}	R_{180}	R_{360}