Cyclic Groups

Defn:- A group G is called <u>cyclic</u> if there is an element $a \in G$ such that $G = \{a^n : n \in \mathbb{Z}\}$.

→ Such an element 'a' is called <u>generator</u> of G.

→ Notation: $G = \langle a \rangle$

→ ~~A group m~~ A cyclic group may have more than one generators.

<u>Examples:-</u>

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

$$n = \underbrace{1+1+\cdots+1}_{n \text{ terms}} \quad \text{when } n > 0$$

$$n = \underbrace{(-1)+(-1)+\cdots+(-1)}_{|n| \text{ times}} \quad \text{when } n < 0$$

2. The set $\mathbb{Z}_n = \{0, 1, 2 \ldots n-1\}$ for $n \geq 1$. is cyclic under addtn modulo n. Again 1 and $-1 = n-1$ are generators.

3. $U(n) = \{x \in \mathbb{N} : x < n \;\&\; (x, n) = 1\}$

eg:- $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^2, 3^3\}$

$\because$ $3^0 \equiv 1 \pmod{10}$

$3^1 \equiv 1 \pmod{10}$

$3^2 \equiv 9 \pmod{10}$

$3^2 = 27 \equiv 7 \pmod{10}$

$\therefore U(10) = \langle 3 \rangle = \langle 7 \rangle$ also.

Scanned by PDF Scanner

Important Results

1. Let G be a group, $a \in G$. If a has infinite order, then $a^i = a^j$ iff $i = j$. If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ iff $n \mid i-j$

2. For any group element a, $|a| = |\langle a \rangle|$

   i.e., Order of an element a is the order of the cyclic subgroup generated by a.

3. Let G be a group and let a be an element of order n in G. If $a^k = e$, the $n \mid k$.

4. Let a be element of order n in a group and let k be a +ve integer, then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and

$$|\langle a^k \rangle| = \frac{n}{\gcd(n,k)}$$

5. In a finite cyclic group, the order of an element divides the order of the group.

6. Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ iff $\gcd(n,j) = 1$

7. An integer $k \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $(n,k) = 1$.

Scanned by PDF Scanner

8. Fundamental Theorem of Cyclic Groups

Every subgroup of a cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n, and for each +ve divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k — namely, $\langle a^{n/k} \rangle$.

9. Subgroups of Z_n:

For each +ve divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n.

10 Results:-

* If d is +ve divisor of n, the no. of elements of order d in a cyclic group of order n is $\phi(n)$.

Problems:-

1. Find all generators of Z_6.

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

By result 7: generators of Z_6 are those k such that $\gcd(6, k) = 1 \Rightarrow Z_6 = \langle 1 \rangle = \langle 5 \rangle$

List elements of the subgroups $\langle 20 \rangle$ & $\langle 10 \rangle$ in Z_{30}

$$\langle 20 \rangle = \{20, 20+20, 20+20+20, \ldots\}$$

$$= \{20, 40, 60, \ldots\} = \{20, 10, 0\} \text{ in } Z_{30}$$

$\|^{ly}$ $\langle 10 \rangle = \{10, 20, 0\}$

Scanned by PDF Scanner

3. List the elements of the subgroups $\langle 3 \rangle$ & $\langle 7 \rangle$ in $U(20)$?

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\langle 3 \rangle = \{3, 3*3, 3*3*3, \ldots\}$ (here $*$ is multiplication)

$= \{3, 3^2, 3^3, \ldots\}$ $\quad 3, 9, 27, 81, \ldots$

$= \{3, 9, 7, 1\}$

$3^4 = 3^3 \cdot 3$
$= 7 \times 3 = 21 \equiv 1 \pmod{20}$

$3^5 = 3^4 \cdot 3 = 1 \cdot 3 = 3$
(again repeating)

$\langle 7 \rangle = \{7, 7^2, 7^3, \ldots\}$

$= \{7, 49, \ldots\}$ $\quad 7^3 = 7^2 \cdot 7 = 9 \cdot 7 = 63 \equiv 3 \pmod{20}$

$7^4 = 7^3 \cdot 7 = 3 \cdot 7 \equiv 1$

$= \{7, 9, 3, 1\}$ (in modulo 20)

4. Let a be an element of a group and $|a| = 15$. Compute the order of the following elements of G.

* a^3, a^6, a^9, a^{12} (Use result. 4)

$$|a^3| = \frac{15}{\gcd(3, 15)} = \frac{15}{3} = 5$$

(think how many times we operate a^3 to get a^{15} or a multiple of 15. We know $\underbrace{3 + 3 + 3 + 3 + 3}_{5 \text{ times}} = 15$. (or use result. 4)

So $|a^3| = 15$)

* $|a^6| \Rightarrow \underbrace{6 + 6 + \cdots + 6}_{?} \neq 15$

But $5 \cdot 6 = 30$ (multiple of 15) $\Rightarrow |a^6| = 5$

Sol: $\frac{15}{(15, 6)} = \frac{15}{3} = 5$

* $|a^9| \Rightarrow \frac{15}{(15, 9)} = \frac{15}{3} = \underline{\underline{5}}$

* $|a^{12}| = \frac{15}{(15, 12)} = 5$

Scanned by PDF Scanner

? How many subgroups does $\mathbb{Z}_{20}$ have?

for each of these subgroups:-

Use Result 9.

No: of subgroups = No: of divisors of 20

We've $20 = 2^2 \cdot 5^1$

$\Rightarrow$ No: of divisors $= (2+1)(1+1) = 3 \times 2 = 6$

$\Rightarrow$ No: of subgroups $= 6$

Divisors $= \{1, 2, 4, 5, 10, 20\}$; orders of subroups.

By Result 9:- K-order subgroup $= \langle n/k \rangle$

$\therefore$ $k = 1 \Rightarrow$ generator 20 $\quad \langle 20 \rangle = \{0\}$

$k = 2 \Rightarrow$ " 10 $\quad \langle 10 \rangle = \{0, 10\}$

$k = 4 \Rightarrow$ " $\frac{20}{4} = 5$ $\quad \langle 5 \rangle = \{0, 5, 10, 15\}$

$k = 5 \Rightarrow$ " $\frac{20}{5} = 4$ $\quad \langle 4 \rangle = \{0, 4, 8, 12, 16\}$

$k = 10 \Rightarrow$ " $\frac{20}{10} = 2$ $\quad \langle 2 \rangle = \{0, 2, 4, 6, 8, \ldots 18\}$

$k = 20 \Rightarrow$ " $\frac{20}{20} = 1$ $\quad \langle 1 \rangle = \mathbb{Z}_{20}$

Scanned by PDF Scanner

Permutation Groups

Defn:- A permutation of a set A is a function from A to A that is <u>both one-one and onto</u>. The set of all permutations on a set A is form a group under composition, called <u>permutation group</u>.

Example:- Let $A = \{1, 2, 3, 4\}$, we define a permutation α, as $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$, $\alpha(4) = 4$

It express like;

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

: here $\alpha(j)$ is placed directly below j for each j.

~~cycle notation~~ **Cycle notation:-**

$$\alpha = (1\ 2\ 3)(4) \quad \text{i.e., } (1 \to 2,\ 2 \to 3,\ 3 \to 1)\ \&\ (4 \to 4)$$

Composition of permutation:-

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$$

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$$

Then $\tau\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$

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

OR

$(1\ 4\ 3)$ (we may omit single cycles)

Single element cycles: maps the element to itself.

Scanned by PDF Scanner

Defn:- The length of a cycle is the no: of elements in a cycle.

~~Properties of per~~

Example:- Symmetric group S_3.

Let S_3 denotes the set of all one-to-one fns on $\{1, 2, 3\}$.

$\rightarrow |S_3| = 3! = 6$

$\rightarrow$ elements:- $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$

Cyclic notn:- $\{(1)(2)(3), (1\ 3\ 2), (1\ 2\ 3), (1)(2\ 3), (1\ 3)(2), (1\ 2)(3)$

Symmetric group S_n:-

The set of all permutations on $A = \{1, 2, \ldots, n\}$ is called symmetric group of degree n, denoted by S_n.

Elements of S_n of the form:-

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \ldots & \alpha(n) \end{bmatrix}$$

$$|S_n| = n!$$

Scanned by PDF Scanner

Properties of permutations:-

1. Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

2. If the pair of cycles $\alpha = (a_1\ a_2 \ldots a_m)$ and $\beta = (b_1\ b_2 \ldots b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

   → i.e., disjoint cycles commute each other.

   → In general S_n is non-abelian, when $n \geq 3$.

3. Order of a permutation:- The order of a permutation on a finite set written in disjoint cycles form is the lcm of the lengths of the cycles.

   Eg:-

   $$|(1\,3\,2)(4\,5)| = 6$$

   $$|(1\,4\,3\,2)(5\,6)| = 4$$

   $$|(1\,2\,3)(4\,5\,6)(7\,8)| = 6$$

   $$|\underset{\alpha}{(1\,2\,3)}\underset{\beta}{(1\,4\,5)}| = |(1\,4\,5\,3\,2)| = 5.$$

   ~~Eg:-~~ 1 ~~[illegible]~~

4. Every permutation in S_n; $n > 1$, is a product of 2-cycles.

   → When we write a permutation α, as a product of 2-cycles then it contains even no: of 2-cycles, we call α is an even permutation. or it contains odd no: of 2-cycles, then α is an odd permutation.

Scanned by PDF Scanner

Defn:- The set of all even permutations on $A = \{1, 2, \ldots n\}$ form a subgroup of S_n, denoted by A_n - called alternating group of degree n.

5. For $n > 1$, A_n has order $\frac{n!}{2}$.

Problems:-

1. $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$

1. $\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$ ~~Just write in new~~

i.e., $\alpha = (1\ 2)(4\ 5)(3)(6)$ → product of disjoint cycles

$\alpha^{-1} = (1\ 2)(4\ 5)(3)(6)$

Here $\alpha = \alpha^{-1}$

2. Write each permutations as a product of disjoint cycles.

1. $(1\ 2\ 3\ 5)(4\ 1\ 3) = (4\ 2\ 3)(1\ 5)$

OR

Verification

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{bmatrix}$$

$= (1\ 5)(2\ 3\ 4)$

2. $(1\ 3\ 2\ 5\ 6)(2\ 3)(4\ 6\ 5\ 1\ 2) = (4\ 1\ 2)(6)(5\ 3)($

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{bmatrix}$$

Scanned by PDF Scanner

3. Find the order of the following permutations:-

1. $(1\ 2\ 4)(3, 5\ 7)$

↳ product of disjoint cycles

→ order = lcm of lengths of cycles

= lcm $(3, 3) = 3$

2. $(1\ 2\ 4)(3\ 5\ 6\ 7)$ = lcm $(3, 4) = 12$

(∵ product of disjoint cycles)

3. $(1\ 2\ 3\ 5)(2\ 4\ 5\ 6\ 7)$

↳ cycles are not disjoint

↳ First convert it to product of disjoint cycles

↳ ~~(1 2 4 7)(5 6 7)~~

↳ ~~(1 2 4 7)(5 6 7~~

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 5 & 4 & 1 & 6 & 7 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 5 & 6 & 7 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 6 & 7 & 3 \end{bmatrix}$$

$= (1\ 2\ 4)(3\ 5\ 6\ 7)$

↳ order = lcm $(3, 4) = 12$.

4. What are the possible orders for the elements of S_7 & A_7?

Scanned by PDF Scanner

Q) Find an element in A_{12} of order 30.

→ order of an element in A_{12} is the lcm of lengths of disjoint cycle (here A_{12} contains even permutations)

→ lcm

(i.e.)

→ lcm (2, 3, 2, 5) = 30

element :- $(1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9\ 10)(11, 12)$

2 transp 1 4 1

Clearly it is an even permutat^n $\in A_{12}$

Q Let $\beta = (1\ 3\ 5\ 7\ 9\ 8\ 6)(2\ 4\ 10)$. What is the smallest +ve integer n for which $\beta^n = \beta^{-5}$?

$$\beta^n = \beta^{-5} \Rightarrow \beta^{n-5} = e$$

⇒ The smallest +ve integer n st $\beta^n = \beta^{-5}$ means smallest +ve integer n st $n-5 = \text{Order}(\beta)$

We've order $(\beta) = \text{lcm}(7, 3)$

$= 21$

i.e., $n - 5 = 21$

$\Rightarrow \underline{\underline{n = 26}}$

Scanned by PDF Scanner

Q) Let $\beta = (1\ 2\ 3)(1\ 4\ 5)$. Write β^{99} in disjoint cycle form?

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{bmatrix} = (1\ 4\ 5\ 2\ 3)$$

$$\text{order}(\beta) = 5 \implies \beta^5 = e$$

$$\beta^{99} = \beta^{100} \cdot \beta^{-1}$$

$$= (\beta^5)^{20} \beta^{-1}$$

$$= e^{20} \beta^{-1}$$

$$= \beta^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{bmatrix} = (1\ \underline{3\ 2\ 5\ 4})$$

(~~solution~~ ~~order(β) = order(β⁻¹)~~

Q) Find five subgroups of S_5 of order 24.

order = lcm (lengths of orbits)

Scanned by PDF Scanner