Permutation Group

k-cycle : $1 \le k \le n$, in S_n → group of permutions of n elements

Eg: $(1\ 2\ 3\ \dots\ k) \in S_n$ is the permutation that takes 1 to 2, 2 to 3, ..., k-1 to k, and k to 1 ; any other symbol is fixed by this cycle.

$(1\ 3\ 2)$ is a 3-cycle $\qquad 1 \to 3 \to 2$

- $(1\ 2)(3\ 4)$ not a cycle

  Product of two cycle — disjoint cycles

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

- $(1\ 2)(3\ 4)$ takes
  1 to 2
  2 to 1
  3 to 4
  4 to 3
  k to k if $n \geqslant k > 4$ in S_n

- $(1\ 2\ 3\ 4) \neq (1\ 3\ 2\ 4)$

In S_4, $(1\ 2\ 3)(2\ 4) = (1\ 2\ 4\ 3)$

Eg $(1\ 4\ 2)(3\ 2\ 1)$ → Product of non-disjoint

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

Write the following permutations as two product of disjoint cycles

Eg: $(1\ 3\ 4\ 5)(1\ 2\ 6) = (1\ 2\ 6\ 3\ 4\ 5)$

Eg: $(2\ 6\ 1)(4\ 5\ 6\ 2)(1\ 2\ 3) = (1\ 4\ 5)(2\ 3)(6)$

PROPOSITION

Disjoint cycles commute

In S_n; every permutation is a product of disjoint cycles.

→ Elements of S_2 : $\{1, (1,2)\}$

$S_1 = \{1\}$

$S_3 : \{1, (1,2), (1,3), (2,3), (1\ 2\ 3), (1\ 3\ 2)\}$

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

cyclic shifting

$S_4 : \{1, (1,2), (1,3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2),$
$(1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), \underbrace{(1\ 2)(3\ 4)},$
$(1\ 2)(4\ 3), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 2\ 4) \ldots \}$

Complete this

Recall: Lagrange's theorem: If $|G| < \infty$ and $H < G$ then $|H|$ divides $|G|$.

- The number of elements in a group is called the order of group.
- Notation for order of G: $|G|$ or $\# G$

Motivation for next theorem:

$$(1\ 2\ 3)^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$$
$$(1\ 2\ 3)^3 = (1\ 3\ 2)(1\ 2\ 3) = 1 \longrightarrow \text{identity permutation}$$

If the operation is multiplicative then:

$$\underbrace{g \cdot g \cdot g \cdots g}_{n \text{ times}} = g^n$$

If additive, $\underbrace{g + g + \cdots + g}_{n \text{ terms}} = ng$

The smallest natural number n, if any, s.t. $g^n = 1$ (multiplicative)

for [$ng = 0$ (additive grouping)] identity notation

is called the order of g.

If there is no n s.t. $g^n = 1$ (or $ng = 0$)

then we say order of g is infinity.

Denote order of g by $O(g)$

Eg: $|S_3| = 6$

$O(1\ 2) = 2$

$O(1\ 2\ 3) = 3$

The order of any 3 cycle is 3

" " 2 " " 2

The order of any n cycle is n

What is the order of $(1\ 2\ 3)(4\ 6\ 5\ 7)$? Answer:- 12

Proposition: If $\sigma_1, \sigma_2, \dots, \sigma_k$ are disjoint cycles (so that $\sigma_i \sigma_j = \sigma_j \sigma_i$, for $1 \le i, j \le k$)

the order of product of $\sigma_1 \sigma_2 \dots \sigma_k$ is $LCM(O(\sigma_1), O(\sigma_2) \dots, O(\sigma_k))$

- Suppose G is a group & $g \in G$.

Then $\langle g \rangle := \{ g^n : n \in \mathbb{Z} \} < G$

& $O(g) = |\langle g \rangle|$

Notation:

$x < \infty$

$\Rightarrow x$ is finite

Observe if $O(g) < \infty$

Then $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$, where $n = O(g)$

$\langle g \rangle$ is called the cyclic subgroups of G generated by g.

Eg: In $\mathbb{Z}$ under addition, let $g = 3$

- $\langle 3 \rangle = \{ n.3 : n \in \mathbb{Z} \} = \{0, \pm 3, \pm 6, \dots\}$

Eg: In S_4, let $g = (1\ 2\ 3\ 4)$

$\langle g \rangle = \{ 1, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2) \}$

Eg: In $\mathbb{Z}_n$ with addition, let $g = [1]_n$

$$\langle g \rangle = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$
$$= \mathbb{Z}_n$$

Cyclic Group

Def^n: A group G is called a cyclic group if $\exists g \in G$ s.t. $G = \langle g \rangle$

Eg: $G = \mathbb{Z}$ $\quad G = \langle 1 \rangle = \langle -1 \rangle$ generators $\quad \therefore$ is cyclic

$G = S_3$ $\quad$ ✗ not cyclic

$\mathbb{Z}_n$ is cyclic & $\mathbb{Z}_n = \langle [1]_n \rangle$

$$\mathbb{Z}_6 = \langle [1]_6 \rangle = \langle [5]_6 \rangle$$
$$\mathbb{Z}_9 = \langle [1]_9 \rangle = \langle [2]_9 \rangle = \langle [4]_9 \rangle$$

is a generator

$$\langle n[4_9] \rangle = \{[0]_9, [4]_9, \ldots, [5]_9\}$$

$$\boxed{\text{If } \gcd(r, n) = 1, \text{ then } \langle [r]_n \rangle = \mathbb{Z}_n}$$

We are done if we can show $[1]_n \in \langle [r_n] \rangle$

$\exists\, x, y \in \mathbb{Z}$ s.t. $xr + yn = 1$

$$[xr]_n + [yn]_n = [1]_n$$
$$[xr]_n + [0]_n = [1]_n$$
$$x[r]_n = [1]_n \implies \langle [r]_n \rangle = \mathbb{Z}_n$$

x can be replaced by $kn + x$

since $n[r]_n = [0]_n$

$[1]_n = m[r_n]$ for $m \in \mathbb{N}$

Corollary

Proposition: If G is finite group & $g \in G$ then $O(g) \mid |G|$.

Proof: $O(g) = |\langle g \rangle|$ $\qquad \langle g \rangle < G$ s.t.

$|\langle g \rangle|$ divides $|G|$ (Lagrange's theorem)

so $O(g)$ divides $|G|$

What are possible orders of an elements in S_3?

Ans: possible orders: $1, 2, 3, \cancel{4}, \cancel{5}, \cancel{6}$ (by Lagrange's theorem)

since S_3 is not cyclic

Remark: G has an element g of order $|G|$, then G is cyclic.

Infact $G = \langle g \rangle$.