22/08

Recall

If $G = \langle x \rangle$, then $o(x^a) = \dfrac{n}{\gcd(a,n)}$ and $|G| = n$

Corollary

Let $G = \langle x \rangle$ be a finite cyclic group of order n. Then x^a generates G. $\iff$ $\gcd(a,n) = 1$

Proof

x^a generates G

$\Rightarrow o(x^a) = n$

$\Rightarrow \gcd(a,n) = 1$

Generators of $\mathbb{Z}/n\mathbb{Z}$ are all such $\bar{a}$ such that $\gcd(a,n) = 1$. This is the set $U(n)$.

Proposition

Let $G = \langle x \rangle$ be an infinite cyclic group. Then x^a generates G. $\iff$ $a = \pm 1$

Proof

Suppose $G = \langle x^a \rangle$

since $x \in G$, there exists n such that $(x^a)^n = x$

$\Rightarrow an - 1 = 0$

$\Rightarrow an = 1 \Rightarrow a \mid 1 \Rightarrow a = \pm 1$

Converse is trivial

(Exercise !!)

- Let G be a cyclic group.
  If G is infinite, then any subgroup of G is of the form $\langle x^m \rangle$ where $m \in \mathbb{Z}$

- If $|G| = n < \infty$, then there is a bijection

  $\{ d \mid n, d > 0 \} \longrightarrow \{ K \leq H \}$

  For every divisor, there is a subgroup with that number as the order.

Define $\{d \mid d \mid n\} \longrightarrow \{K \leq G\}$

$$d \longmapsto \langle x^{n/d} \rangle$$

- $o(x^{n/d}) = \dfrac{n}{\gcd(n, n/d)} = \dfrac{n}{(n/d)} = d$

Suppose $o(x^b) = d$

$\Rightarrow d = \dfrac{n}{\gcd(b,n)} \Rightarrow \gcd(b,n) = \dfrac{n}{d}$

$\Rightarrow \dfrac{n}{d} \mid b$

$\Rightarrow \exists\, k \in \mathbb{Z}$ such that $b = k\dfrac{n}{d}$

$\Rightarrow x^b = (x^{n/d})^k \in \langle x^{n/d} \rangle$

$\Rightarrow \langle x^b \rangle \leq \langle x^{n/d} \rangle$

Note

- Each cyclic group of order n has $\varphi(n)$ generators.
- $n = \sum_{d \mid n} \varphi(d)$

Permutation groups

Definition

Let X be a non-empty set.

We define

$$S_X = \{ f : X \to X \mid f \text{ is bijective} \}$$

Notation

$[n] = \{1, \dots, n\}$ for $n \in \mathbb{N}$

If $X = [n]$, the bijection is denoted by $S_{[n]}$

S_n is a group under composition of maps.

S_n is called the symmetric group on $[n]$

$|S_n| = n!$

- Is S_n abelian?

No, S_3 is not abelian

Example :- $(2\ 1\ 3) \circ (3\ 2\ 1) \neq (3\ 2\ 1) \circ (2\ 1\ 3)$

where $(a\ b\ c) \Rightarrow f(1) = a,\ f(2) = b,\ f(3) = c$

Notation

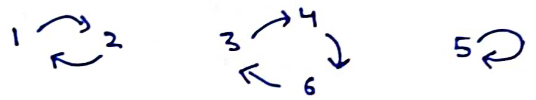
Let $\sigma \in S_n$

We will denote σ as $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

For $n = 4$, we will see composition

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

Let $\sigma \in S_6$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$



$(1\ 2)$ $(3\ 4\ 6)$ (5) $\longrightarrow$ Notation in terms of cycles

Definition

Let n be a positive integer. An element $\sigma \in S_n$ is called a k-cycle if there exist $a_1, \ldots, a_k \in [n]$ such that $\sigma = (a_1 \ldots\ldots a_k)$ where

$$(a_1\ a_2 \cdots a_k)(x) = \begin{cases} a_{i+1} & \text{if } x = a_i \quad (i = 1, \ldots, k-1) \\ a_1 & \text{if } x = a_k \\ x & \text{if } x \notin \{a_1, \ldots, a_k\} \end{cases}$$

Two cycles $(a_1 \ldots\ldots a_r)$ and $(b_1 \ldots\ldots b_s)$ are said to be distinct if $\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \emptyset$

Proposition

If $\sigma, \tau \in S_n$ are disjoint cycles, then

$\sigma\tau = \tau\sigma$

Proof

Let $x \in [n]$. We need to show that $\sigma\tau(x) = \tau\sigma(x)$

Let $\sigma = (a_1 \dots a_r)$, $\tau = (b_1 \dots b_s)$

Case - (i)

If $X \in \{a_1, \dots, a_r\}$

$$\sigma\tau(X) = \sigma(X) = \begin{cases} a_{i+1} & \text{if } i \le r-1 \\ a_1 & \text{if } i = r \end{cases}$$

$$\tau\sigma(X) = \begin{cases} \tau(a_{i+1}) & \text{if } i \le r-1 \\ \tau(a_1) & \text{if } i = r \end{cases} = \begin{cases} a_{i+1} & \text{if } i \le r-1 \\ a_1 & \text{if } i = r \end{cases}$$

Case - (ii)

If $y \in \{b_1, \dots, b_s\}$

$$\tau\sigma(y) = \tau(y) = \begin{cases} b_{i+1} & \text{if } i \le s-1 \\ b_1 & \text{if } i = s \end{cases}$$

$$\sigma\tau(y) = \begin{cases} \sigma(b_{i+1}) & \text{if } i \le s-1 \\ \sigma(b_1) & \text{if } i = s \end{cases} = \begin{cases} b_{i+1} & \text{if } i \le s-1 \\ b_1 & \text{if } i = s \end{cases}$$

Case - (iii)

If $y \notin \{a_1, \dots, a_r\}$ and $y \notin \{b_1, \dots b_s\}$

$\Rightarrow \tau\sigma(y) = \sigma\tau(y) = y$

Hence pooved.

Theorem

Any permutation $\sigma \in S_n$ can be written as a product of disjoint cycles.

Proof

Let $a \in [n]$ and we define the σ- orbit of a denoted by

$$O_{\sigma(a)} = \{\sigma^i(a) \mid i \in \mathbb{N}\}$$

Since $O_{\sigma(a)} \subseteq [n]$, $O_{\sigma(n)}$ is a finite set.

For some $i < j$, $\sigma^i(a) = \sigma^j(a)$

$\Rightarrow a = \sigma^{j-i}(a)$

If $m_1 = \min\{ l \mid \sigma^l(a) = a \}$

then $O_{\sigma(a)} = \{ a, \sigma(a), \dots, \sigma^{m_1 - 1}(a) \}$

If $O_\sigma(a) = [n]$, then $\sigma = (a \ \sigma(a) \ \dots \ \sigma^{n-1}(a))$

If $O_\sigma(a) \neq [n]$, then there exists

$b \in [n] \setminus O_{\sigma(a)}$. Construct σ-orbit of b.

<u>Claim</u>: $O_{\sigma(a)} \cap O_\sigma(b) = \emptyset$

<u>Proof</u>: Let $\exists x$ such that $x \in O_\sigma(a) \cap O_\sigma(b)$

$\Rightarrow x = \sigma^m(a)$ and $x = \sigma^l(b)$

If $m < l$

$\Rightarrow \sigma^{l-m}(b) = a \Rightarrow b = \sigma^{m-l}(a) \in O_\sigma(a)$

$(\Rightarrow\Leftarrow)$

If $m = l$

contradiction