Lecture 23: 27th Sep 2022

Note Title 9/27/2022

§ Generators of S_n:

Let X = set of all the 2-cycles of S_n

Then, $|X| = \frac{{}^nP_2}{2} = \frac{n(n-1)}{2}$

Since every $f \in S_n$ can be expressed as a product of 2-cycles, so S_n is generated by the set of all the 2-cycles, that is, $S_n = \langle X \rangle$.

We would like to find a smallest generating set for S_n.

(1) S_n is generated by the $(n-1)$ 2-cycles $(1\ 2), (1\ 3), \ldots, (1\ n)$.

<u>Proof:</u> Let $Y = \{(1\ 2), (1\ 3), \ldots, (1\ n{-}1), (1\ n)\}$.

Since S_n is generated by the set of all the 2-cycles of S_n, so it is enough to prove that every 2-cycle can be expressed as a product of 2-cycles from the set Y.

We have $(i\ j) = (1\ i)(1\ j)(1\ i)$.

Note that $(i\ j) \in X$ and $(1\ i), (1\ j), (1\ i) \in Y$.

$\therefore\ S_n = \langle Y \rangle$. #

(2) $S_n = \langle \{(1\ 2), (2\ 3), \ldots, (n-1\ n)\} \rangle$.

<u>Proof:</u> We have $(1\ j) = (1\ j-1)(j-1\ j)(1\ j-1)$

$(1\ 2) = (1\ 2) \in Z$

$(1\ 3) = \underbrace{(1\ 2)(2\ 3)(1\ 2)}_{\in Z}$

Let $Z = \{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$

$(1\ 4) = (1\ 3)(3\ 4)(1\ 3) = \underbrace{(1\ 2)(2\ 3)(1\ 2)(3\ 4)(1\ 2)(2\ 3)(1\ 2)}_{\in Z}$

Hence, from (1), we have $S_n = \langle Z \rangle$.

#

(3) $S_n = \langle (1\ 2),\ (1\ 2\ 3 \cdots n) \rangle$.

<u>Proof</u>: We first prove that if $\sigma = (i_1\ i_2 \cdots i_r) \in S_n$ and $\tau \in S_n$, then $\tau\sigma\tau^{-1} = (\tau(i_1)\ \tau(i_2) \cdots \tau(i_r))$.

$(\tau\sigma\tau^{-1})(\tau(i_1)) = (\tau\sigma)(i_1) = \tau(\sigma(i_1)) = \tau(i_2)$

$\vdots$

$(\tau\sigma\tau^{-1})(\tau(i_r)) = (\tau\sigma)(i_r) = \tau(\sigma(i_r)) = \tau(i_1)$.

Also, if $j \neq \tau(i_k)$, $1 \leq k \leq r$, then $\tau^{-1}(j) \neq i_k\ \forall k$

$\Rightarrow \sigma(\tau^{-1}(j)) = \tau^{-1}(j) \Rightarrow (\tau\sigma\tau^{-1})(j) = j$.

$\therefore \tau\sigma\tau^{-1} = (\tau(i_1)\ \tau(i_2) \cdots \tau(i_r))$. #

We will now use the above information to prove that

$$S_n = \langle (1\ 2),\ (1\ 2\ 3 \cdots n) \rangle.$$

Let $\sigma_1 = (1\ 2)$ and $\tau = (1\ 2\ 3 \cdots n)$.

Then $\sigma_2 = \tau \sigma_1 \tau^{-1} = (\tau(1)\ \ \tau(2)) = (2\ 3)$

$\sigma_3 = \tau \sigma_2 \tau^{-1} = (\tau(2)\ \ \tau(3)) = (3\ 4)$

$\vdots$

$\sigma_{n-1} = \tau \sigma_{n-2} \tau^{-1} = (n-1\ \ n)$

Thus, $(1\ 2) = \sigma_1 \in \langle \sigma_1, \tau \rangle$, $(2\ 3) \in \tau \sigma_1 \tau^{-1} \in \langle \sigma_1, \tau \rangle$

$\cdots, (n-1\ \ n) \in \langle \sigma_1, \tau \rangle$.

Since $S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1\ \ n) \rangle$, so

$$S_n = \langle \sigma_1, \tau \rangle = \langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle.$$

This completes the proof.

#

Theorem: A_n $(n \geq 3)$ is generated by the set of all 3-cycles.

Proof: Let $f \in A_n$. Then, f can be expressed as a product of even number of 2-cycles.

Let $f = \alpha_1 \alpha_2 \cdots \alpha_i \alpha_{i+1} \cdots \alpha_{2k-1} \alpha_{2k}$, where each α_i is a 2-cycle.

we have the following cases:

(i) $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$

(ii) $(a\ b)(a\ c) = (a\ c\ b)$

$\therefore$ A_n is generated by all the 3-cycles of S_n.

---

§ <u>Cayley's Theorem:</u> Every group G is isomorphic to a group of permutations. If $|G| = n$, then G is isomorphic to a subgroup of S_n.

<u>Proof</u>: Given a group G, we will first construct a group of permutations

For $g \in G$, define a function T_g on G by

$$T_g : G \longrightarrow G, \quad T_g(x) = gx \quad \forall x \in G.$$

Easy to check that T_g is 1-1 and onto, that is, T_g is a permutation on G.

Let $\overline{G} = \{T_g : g \in G\}$. We now prove that $\overline{G}$ is a group under composition of functions.

(i) $(T_g \circ T_h)(x) = T_g(hx) = g(hx) = (gh)(x) = T_{gh}(x) \quad \forall x \in G$

$\therefore \; T_g \circ T_h = T_{gh} \in \overline{G}$.

(ii) T_e plays the role of identity of $\overline{G}$, where e is the identity of G.

(iii) $T_{g^{-1}}$ is the inverse of T_g.

(iv) $T_g \circ (T_h \circ T_k) = (T_g \circ T_h) \circ T_k \quad \forall\, g, h, k \in G$.

$\therefore$ $\bar{G}$ is a group under composition of function.

We now prove that $G \cong \bar{G}$. We define

$\psi : G \longrightarrow \bar{G}$ by $\psi(g) = T_g$.

① $\psi(gh) = T_{gh} = T_g \circ T_h = \psi(g)\psi(h)$. Hence, ψ is a homomorphi

(2) $\psi(g) = \psi(h) \Rightarrow T_g = T_h \Rightarrow T_g(e) = T_h(e) \Rightarrow g = h$

$\therefore$ ψ is one-to-one.

(3) It is clear that ψ is onto.

$\therefore$ $G \cong \bar{G}$.

2nd part: If $|G| = n$, then the element of $\overline{G}$ are permutations on a set of n-elements.

$\therefore \overline{G} \subseteq S_n$.

Since $\overline{G}$ is a group, so $\overline{G} \leq S_n$.

$\therefore G$ is isomorphic to a subgroup of S_n.

Ex: Let $G = U(8) = \{1, 3, 5, 7\}$ is a group under multiplication modulo 8.

$T_1 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{bmatrix}$ $\qquad$ $T_5 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{bmatrix}$

$T_3 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 3 & 1 & 7 & 5 \end{bmatrix}$ $\qquad$ $T_7 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 7 & 5 & 3 & 1 \end{bmatrix}$

$\therefore \quad \overline{U(8)} = \{ T_1, T_3, T_5, T_7 \}.$

We find a subgroup of S_4 which is isomorphic to $U(8)$.

S_4 is a group of all the permutations on $\{1, 2, 3, 4\}$, a four elements set.

We have, $\quad T_1 \longleftrightarrow (1), \quad T_3 \longleftrightarrow (1\,2)(3\,4), \quad T_5 \longleftrightarrow (1\,3)(2\,4)$

$\therefore U(8) \cong \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq S_4. \quad T_7 \longleftrightarrow (1\,4)(2\,3).$

#