Class: Symmetric Groups - 2022/10/19

Symmetric Groups S_n

Symmetric Groups S_n

S_n : consists of all bijections $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Recall: a <u>k-cycle</u> in S_n is an element of the form

$\tau = (a_1\ a_2 \cdots a_k) \in S_n$. $\tau(a_1) = a_2$, $\tau(a_2) = a_3$, ..., $\tau(a_{k-1}) = a_k$

$\tau(a_k) = a_1$.

$a_1, \ldots, a_k$ are distinct integers among $\{1, 2, \ldots, n\}$

$\tau(b) = b$ if $b \notin \{a_1, \ldots, a_k\}$

Prop. Disjoint cycles commute.

$(a_1\, a_2 \dots a_k)$ & $(b_1\, b_2 \dots b_l)$ are disjoint if
$a_1, a_2, \dots a_k, b_1, b_2, \dots, b_l$ are all distinct.

Pf. Given disjoint cycles $\tau = (a_1\, a_2 \dots a_k)$, $\sigma = (b_1\, b_2 \dots b_l)$.
Take $x \in \{1, 2, \dots, n\}$.

- If $x = a_i$

$$\tau\cdot\sigma(x) = \tau\cdot\sigma(a_i) = \tau(a_i) = \begin{cases} a_{i+1}, & i<k \\ a_1, & i=k. \end{cases}$$

$$\sigma\cdot\tau(x) = \sigma\cdot\tau(a_i) = \begin{cases} \sigma(a_{i+1}), & i<k \\ \sigma(a_1), & i=k \end{cases} = \begin{cases} a_{i+1}, & i<k \\ a_1, & i=k \end{cases}$$

so $\tau\cdot\sigma = \sigma\cdot\tau$ on $\{a_1, a_2, \dots, a_k\}$.

- If $x = b_i$.
- If $x \notin \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_l\}$

} similarly discussed. to conclude $\tau\cdot\sigma = \sigma\cdot\tau$ for any choice of x.

Prop. Every $\sigma \in S_n$ can be expressed as a product of disjoint cycles in a unique way, up to reordering these cycles.

Pf. Take any $a_1 \in \{1, 2, \dots, n\}$.

consider $a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{m_1}(a_1)$

$\sigma^{m_1+1}(a_1) = a_1$

$(a_1\, \sigma(a_1) \dots \sigma^{m_1}(a_1))$ is a cycle.

Take $a_2 \notin \{a_1, \sigma(a_1), \dots, \sigma^{m_1}(a_1)\}$, repeat the process to obtain another cycle $\underbrace{(a_2, \sigma(a_2), \dots, \sigma^{m_2}(a_2))}$

"should be disjoint from the first cycle".

Then continue the process.

To make the argument rigorous, we define a relation on $\{1, 2, \dots, n\}$ by $i \sim j$ if $\exists\, m \in \mathbb{Z}$. $j = \sigma^m(i)$

You can verify it's an equivalence relation.

Then within each equivalence class, we can pick an element a_i.

Form the cycle $(a_i \ \sigma(a_i) \ \sigma^2(a_i) \ \dots \ \sigma^{m_i}(a_i))$

m_i is the smallest positive integer that $\sigma^{m_i+1}(a_i) = a_i$

Then we can verify

$$\sigma = \prod_i (a_i \ \sigma(a_i) \ \underbrace{\sigma^2(a_i)}_{b} \ \dots \ \sigma^{m_i}(a_i))$$

Also it's unique because the number after b has to be $\sigma(b)$ in the cycle that contains b.

- Cycle Decomposition

Def. $\tau \in S_n$. $\tau = c_1 c_2 \cdots c_\ell$ is the cycle decomposition.

with c_i an k_i-cycle, and $k_1 \le k_2 \le k_3 \le \dots \le k_\ell$.

$(k_1 + k_2 + \dots + k_\ell = n)$

(so if $\tau(m) = m$, we consider (m) as a "1-cycle")

Then $(k_1, k_2, \dots, k_\ell)$ or written as $k_1 + k_2 + \dots + k_\ell$ is called the cycle type of τ.

e.g. $\tau = (1\ 2)(3\ 4) \in S_4$. cycle type is $(2,2)$ or $2+2$

$\sigma = (1\ 2\ 3) \in S_4$. cycle type is $(1,3)$ or $1+3$.

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

$\sigma = (1\ 2\ 3)(4\ 5) \in S_7$ cycle type is $(1,1,2,3)$.

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

Lemma. $\sigma \in S_n$. $\sigma(a_1\, a_2 \dots a_k)\sigma^{-1} = (\sigma(a_1)\, \sigma(a_2) \dots \sigma(a_k))$

Pf. Let $\tau = \sigma(a_1\, a_2 \dots a_k)\sigma^{-1}$.

$$\tau(\underline{\sigma(a_i)}) = \begin{cases} \sigma(a_{i+1}), & i<k \\ \sigma(a_1), & i=k. \end{cases}$$

$b \notin \{\sigma(a_1), \dots, \sigma(a_k)\}$

$\tau(b) = b$ since $b \neq \sigma(a_i) \Rightarrow \sigma^{-1}(b) \neq a_i \Rightarrow \underbrace{(a_1 \dots a_k)(\sigma^{-1}(b))}_{= \sigma^{-1}(b)}$

$\Rightarrow \sigma(\sigma^{-1}(b)) = b$

- Conjugacy

Prop. Two elements of S_n are conjugate if and only if they are of the same cycle type.

Pf. "$\Rightarrow$" If $\sigma' = \tau\sigma\tau^{-1}$.

$\sigma = C_1 C_2 \cdots C_\ell$ is the cycle decomposition.

Then $\sigma' = \tau\sigma\tau^{-1} = \tau C_1 C_2 \cdots C_\ell \tau^{-1}$

$$= \tau C_1 \tau^{-1}\tau C_2 \tau^{-1} \cdots \tau C_\ell \tau^{-1}$$

$$= (\tau C_1 \tau^{-1})(\tau C_2 \tau^{-1}) \cdots (\tau C_\ell \tau^{-1})$$

by the Lemma, $\tau C_i \tau^{-1}$ is a cycle that has the same length as C_i.

so σ' has the same cycle type as σ.

"$\Leftarrow$": If $\sigma' = c_1' c_2' \cdots c_l'$ and $\sigma = c_1 c_2 \cdots c_l$ have the same cycle type. Then we can find $\tau \in S_n$ to make $\tau c_i \tau^{-1} = c_i'$ for all i.

$$\left.\begin{aligned} c_i &= (a_1 \cdots a_{k_i}) \\ c_i' &= (b_1 \cdots b_{k_i}) \end{aligned}\right\} \text{ let } \tau(a_m) = b_m$$

Then $\sigma' = \tau \sigma \tau^{-1}$

e.g. $\sigma = (1\ 2)(3\ 4\ 5) \in S_7$. $\sigma' = (3\ 4)(1\ 6\ 7) \in S_7$

Find ~~a~~ $\tau \in S_7$, $\sigma' = \tau \sigma \tau^{-1}$

$\sigma = (1\ 2)(3\ 4\ 5)$ $\quad \tau\sigma\tau^{-1} = (\tau(1)\ \tau(2))(\tau(3)\ \tau(4)\ \tau(5))$

$\sigma' = (3\ 4)(1\ 6\ 7)$

Let $\tau(1) = 3$, $\tau(2) = 4$. $\tau(3) = 1$, $\tau(4) = 6$ $\tau(5) = 7$.

$\tau(6) = 2$, $\tau(7) = 5$

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

Note the choice of τ is not unique.

In particular, if N is a normal subgroup of S_n, then N is made up from all elements in some of the cycle types.

Signature Functions and Alternating Groups

$\boxed{\text{Lemma. } \underbrace{(a_1\ a_2 \dots a_k)}_{\sigma} = \underbrace{(a_1\ a_k)(a_1\ a_{k-1})(a_1\ a_{k-2})\dots(a_1\ a_2)}_{\tau}}$

Pf. If $b \notin \{a_1, \dots, a_k\}$. Then

$\sigma(b) = b.\quad \tau(b) = b \Rightarrow \sigma(b) = \tau(b).$

If $b = a_k$. then $\sigma(b) = a_1$, $\tau(b) = a_1 \Rightarrow \sigma(b) = \tau(b)$.

If $b = a_i$. $1 < i < k$

then $\sigma(a_i) = a_{i+1}$

$$\tau(a_i) = (a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_i)(\underbrace{\dots (a_1\ a_2)}(a_i))$$

$$= (a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_{i+1})\underline{(a_1\ a_i)(a_i)}$$

$$= (a_1\ a_k)(a_1\ a_{k-1}) \dots \underline{(a_1\ a_{i+1})(a_1)}$$

$$= \underline{(a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_{i+2})}(a_{i+1})$$

$$= a_{i+1}.$$

If $b = a_1$. $\sigma(a_1) = a_2$. $\tau(a_1) = a_2$.

- Prop

We'll show that the number of 2-cycles (mod 2) in this decomposition is independent of the 2-cycle decomposition we choose for a given $\sigma \in S_n$.

Consider the function $T: S_n \longrightarrow GL_n(\mathbb{R})$

Define $T(\sigma)$ to be the $n \times n$ matrix, whose j-th column is

$e_{\sigma(j)}$. $\qquad e_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i\text{-th}$

e.g. $T: S_3 \to GL_3(\mathbb{R})$

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

$$T(\sigma) = \begin{bmatrix} e_{\sigma(1)} & e_{\sigma(2)} & e_{\sigma(3)} \end{bmatrix}$$

$$= \begin{bmatrix} e_2 & e_3 & e_1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Recall: For a matrix M.

$Me_j = j\text{-th column of } M$

$$\left(M = \begin{bmatrix} \vec{v}_1 & \vec{v}_2 & \dots & \vec{v}_n \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1 \vec{v}_1 + \dots + x_n \vec{v}_n \right)$$

$\begin{matrix} 0 & 1 & 0 \end{matrix}$

T defined above is a homomorphism:

$\forall\ \sigma, \tau \in S_n$.

$\boxed{T(\sigma \cdot \tau)} \cdot e_j = e_{\sigma \cdot \tau(j)}$

$\boxed{T(\sigma) \cdot T(\tau)} \cdot e_j = T(\sigma)\left(T(\tau) e_j\right) = T(\sigma)\left(e_{\tau(j)}\right) = e_{\sigma(\tau(j))} = e_{\sigma \cdot \tau(j)}$

j-th column

so T is a homomorphism.

Im(T) consists of elements of form $\underbrace{\left[e_{\sigma(1)}\ e_{\sigma(2)} \cdots e_{\sigma(n)} \right]}_{}\!\!\overset{T(\sigma)}{\shortparallel}$

which is a permutation of the rows of $\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$

so for any $M \in \operatorname{Im}(T)$. $\det(M) = \pm 1$.

Define: $\quad \operatorname{sgn}: S_n \xrightarrow{T} GL_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\}$

called the <u>signature function</u> of S_n. which is a homomorphism.

so If $\sigma = c_1 c_2 \cdots c_k$, a product of 2-cycles.

$\operatorname{sgn}(\sigma) = \prod \operatorname{sgn}(c_i) = (-1)^k$