GroupAction3

2023年2月18日 星期六 下午12:19

permutation.

symmetry group

k - cycle.

conjugate

Definition: Let S be a set. A bijection $S \to S$ is called a permutation of S and the set of permutations of S is denoted $Sym(S)$. Group.

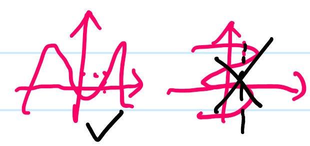
If n is integer (positive) we write S_n for $Sym(\{1,2,\cdots n\})$.

$k \in \{1,2\cdots n\}$.

$\sigma, \tau \in S_n$. $S \to S$

$$\boxed{\begin{aligned} k\sigma &= \sigma(k) \\ k\sigma\tau &= \tau(\sigma(k)) \end{aligned}}$$

$\sigma k = \sigma(k)$ ✗.



$y = f(x)$. function.

$\forall x.\ \exists$ unique y

$\forall y.\ \exists x.$

$\forall y.\ \exists$ unique x

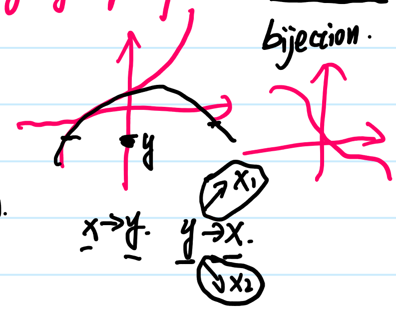
bijection.

Theorem: Let S be a set.

i) $Sym(S)$ forms a group under composition. Symmetry group of S

ii) If $|S| \geq 3$ the $Sym(S)$ is non-abelian.

iii). The cardinality of S_n is $n!$.



proof: i). the composition of two bijections is bijection.

composition. $\circ$ is ineed a binary operation.

$x \in S$. $f, g, h \in Sym(S)$.

$x((fg)h) = (x(fg))h = ((xf)g)h = (xf)(gh) = x(f(gh))$. associative

$id_S(x) = x \quad \forall x \in S$. identity.

$f^{-1}(f(x)) = id$. inverse.

$x \to y$

$y \to x \Rightarrow x \to x$.

ii) $S = \{x_1, x_2, x_3 \ldots\}$ $|S| \geq 3$

$\underset{y \to x}{\cdots} \sigma \Rightarrow x \to x.$

ii). $S = \{x_1, x_2, x_3, \cdots\}$ $\quad |S| \geq 3.$

f: $x_1 \to x_1$, $x_2 \to x_3$, $x_3 \to x_2$, $x \to x$ for other x

g: $x_1 \to x_2$, $x_2 \to x_1$, $x_3 \to x_3$, $x \to x$ for other x.

fg: $x_1 \to x_2$ $x_2 \to x_3$. $x_3 \to x_1$ $x \to x$ for other x

gf: $x_1 \to x_3$ $x_2 \to x_1$. $x_3 \to x_2$. $x \to x$ for other x.

$\neq$. non-abelian. do not commute.

iii). $f \in S_n$. $\underline{1f}$ $\quad f(1) \to k$. $\quad n$ possibilities.

$2f$. $\quad n-1$ possibilities.

$3f$. $\quad n-2$

$n \times (n-1) \times (n-2) \times \cdots \times 1 = n!$ permutations of $\{1, 2, \cdots n\}$ $\square$

$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1\sigma & 2\sigma & 3\sigma & 4\sigma & & n\sigma \end{pmatrix}$. $\sigma \in S_n$. cycle.

Example. S_2. group of order 2. $\underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}_{\text{identity}}$ $\quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ $\quad 2! = 2$

$D_{6} \underset{\uparrow}{\cong} S_3$.
isomorphism.

e. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad \sigma$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad \sigma^2$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad \tau$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\quad \sigma\tau$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\sigma^2\tau$. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$3! = 3 \times 2 \times 1 = 6$

$*$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$.
e	e	σ	σ^2	$\cdots$		
σ		σ^2				
σ^2			σ			
τ						
$\sigma\tau$						
$\sigma^2\tau$						

$\underline{\sigma} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad \underline{\tau} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

$\sigma^3 = \sigma^2\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \underline{e}$. $\quad \tau\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\tau^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$

Example. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \cdots \end{pmatrix}$ $\quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \cdots \end{pmatrix}$ $\quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \cdots \end{pmatrix} \in S_5$

Example. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$ $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$ $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$ $\in S_5$

$\alpha\beta\gamma$. β^{-1}. order of γ. $\gamma^2\ \gamma^3\ \gamma^4\ \gamma^5.\ \gamma^6 \cdots = e$

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

$\beta \cdot \beta^{-1} = e$. $\beta^{-1} \cdot \beta$

Definition: A permutation $\sigma \in S_n$ is a cycle if there are distinct elements $a_1, a_2, \cdots a_k$ in $\{1, 2, \cdots n\}$ such that.

$$a_i\sigma = a_{i+1} \text{ for } 1 \le i < k \qquad a_k\sigma = a_1.$$

and $x\sigma = x$ for $x \notin \{a_1, \cdots a_k\}$.

$(a_1 \cdots a_k)$ k. $(a_k\ a_1)$ k.

length of such a cycle is k. σ: k-cycle. order is k

$$(a_1, a_2, \ a_k). = (a_2 \cdots a_k\, a_1) = \cdots$$

Example. $\alpha = (1, 2, 4)$ 3-cycle. $\beta = (1\ 3\ 5\ 2\ 4)$. 5-cycle. $\gamma = (1\ 2\ 5)(3\ 4)$ is not a cycle

Definition: Two cycles. $(a_1 \cdots a_k)$ and $(b_1, \cdots b_l)$ are said to be disjoint if. $a_i \ne b_j$ for all i, j.

Proposition: Disjoint cycles. commute.

$\alpha\beta = \beta\alpha$.

proof. $\alpha = (a_1 \cdots a_k)$. $\beta = (b_1 \cdots b_l)$. Then.

$a_i\alpha\beta = a_{i+1}\beta = a_{i+1}$ $\quad a_i\beta\alpha = a_i\alpha = a_{i+1}$. $\quad i < k$.

$a_k\alpha\beta = a_1\beta = a_1$ $\quad a_k\beta\alpha = a_k\alpha = a_1$

$b_i\alpha\beta = b_i\beta = b_{i+1}$ $\quad b_i\beta\alpha = b_{i+1}\alpha = b_{i+1}$ $\quad i < l$

$b_l\alpha\beta = b_l\beta = b_1$. $\quad b_l\beta\alpha = b_1\alpha = b_1$.

$x\alpha\beta = x\beta = x$. $\quad x\beta\alpha = x\alpha = x$. $\quad$ for $x \notin \{a_1, \cdots a_k.\ b_1, \cdots b_l\}$.

$\square$.

Theorem: Every permutation can be written as a product of disjoint cycles..

$\square$

Theorem: Every permutation can be written as a product of disjoint cycles.
This expression is unique up to the cycling of elements within cycles and permuting the order of cycles.

$\alpha\beta\gamma = \beta\gamma\alpha = \gamma\alpha\beta$
$= \gamma\beta\alpha$.

proof: let $\sigma \in S_n$ $a_1 \in \{1, 2, \cdots n\}$.

$a_1, a_1\sigma, a_1\sigma^2, \cdots a_1\sigma^{j-1}$ $\in \{1, 2, \cdots n\}$

$a_1\sigma^i = a_1\sigma^j$. $i<j$. (repetition) occurs at j.

$a_1 = a_1\sigma^i \cdot \sigma^{-i} = a_1\sigma^{j-i}$ a_1 repetition occurs at $j-i$.

(first element to repeat).

$a_1\sigma^{k_1} = a_1$.

σ acts on the set $\{a_1, a_1\sigma, a_1\sigma^2 \cdots a_1\sigma^{k_1-1}\}$. $a_1\sigma^{k_1} = a_1$ is called the orbit of a_1.
as the cycle $(a_1\ a_1\sigma\ a_1\sigma^2 \cdots a_1\sigma^{k_1-1})$.

If $k_1 = n$, then σ is a cycle
If not. we take second element a_2 not in the orbit of a_1
σ acts as a second cycle on the orbit of a_2.

contradiction.

They are not disjoint, if $a_1\sigma^i = a_2\sigma^j$. for some i, j.
$a_1\sigma^{i-j} = a_2$. a_2 was in the orbit of a_1

They are disjoint.

$\{1, 2, \cdots n\}$. is finite. these orbits eventually exhaust the set.

$$\sigma = (a_1, a_1\sigma, \cdots a_1\sigma^{k_1-1})(a_2, a_2\sigma, \cdots a_2\sigma^{k_2-1}) \cdots (a_r, a_r\sigma, \cdots a_r\sigma^{k_r-1}).$$

r was the number of different orbits.

Suppose. $\sigma = \rho_1\rho_2 \cdots \rho_k = \tau_1\tau_2 \cdots \tau_l$. disjoint cycles.

1 appears in ρ_i. τ_j. (reordering) we assume. 1 appears in ρ_1, τ_1

$\rho_1 = (1\ 1\sigma\ 1\sigma^2 \cdots 1\sigma^{k-1}) = \tau_1$. $\Rightarrow \rho_2 = \tau_2 \Rightarrow \cdots$
orbit. k is the size of orbit of 1. $\square$

Definition: permutation $\Rightarrow$ cycle (decomposition) type

Example. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 9 & 7 & 3 & 2 & 4 & 8 & 1 \end{pmatrix}$.

$\begin{pmatrix} 1 & 5 & 3 & 9 \\ 5 & 3 & 9 & 1 \end{pmatrix}$

$\alpha = (1\,5\,3\,9)(2\,6)(4\,7)\cancel{(8)}$

$\alpha^{-1} = (1\,9\,3\,5)(2\,6)(4\,7)\cancel{(8)}$.

$\begin{pmatrix} 5 & 3 & 9 & 1 \\ 1 & 5 & 3 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 & 9 \\ 9 & 5 & 1 & 3 \end{pmatrix}$.

$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 7 & 5 & 1 & 3 & 6 & 2 & 8 \end{pmatrix}$

$\beta = (1\,4\,5)(2\,9\,8)(3\,7\,6)$ $\quad \beta^{272} = ?$

$$\beta^k = (1\,4\,5)^k(2\,9\,8)^k(3\,7\,6)^k = \begin{cases} e & k \text{ is multiple of } 3 \\ \beta & k-1 \;\cdots\; 3 \\ \beta^2 & k-2 \;\cdots\; 3. \end{cases}$$

$\beta^{272} = \beta^2 = (1\,5\,4)(2\,8\,9)(3\,6\,7)$.

Proposition: Let $\sigma = \rho_1 \cdots \rho_k$ be an expression for σ as disjoint cycles of lengths $l_1 \cdots l_k$. The order of σ is $\underline{lcm}(l_1, \cdots l_k)$.

least common multiple.

Example: (i) How many 5-cycles are there in S_{11}?
(ii) How many permutations in S_8 have a cycle decomposition type of two 3-cycles and one 2-cycle.

(i) $\overbrace{(\underset{11}{a}\,\underset{10}{b}\,c\,d\,e)}$ $\quad S_{11}$

$(b\,c\,d\,e\,a)$ ≥ 5.

$\dfrac{11 \times 10 \times 9 \times 8 \times 7}{5} = 11088$.

Proposition: In S_n, there are.

$$\frac{n!}{\underbrace{(l_1^{k_1} \times l_2^{k_2} \times \cdots l_r^{k_r})}\underbrace{(k_1! \times k_2! \times \cdots k_r!)}}.$$

$$\underbrace{(l_1^{k_1} \times l_2^{k_2} \times \cdots l_r^{k_r})}\underbrace{(k_1! \times k_2! \times \cdots k_r!)}.$$

permutations with a cycle type of k_1 of length l_1.

k_2 l_2

$\vdots$

k_r l_r.

This decomposition includes 1-cycles.: $k_1l_1 + k_2l_2 + \cdots k_rl_r = n$.

proof: $\underbrace{(\quad)}_{k_1}\underbrace{(\quad)}_{k_2}(\quad)\cdots\underbrace{(\quad)}_{k_r}$ $\sum k_i$.

$n!$ with number $1 \ldots n$.

l_i ways of cycling the elements of each cycle of length l_i.

$k_i!$ of permuting the cycles of length l_i. $\square$.

Example: How many permutations of each cycle type are there in S_7.

7	$7!/7$	720
6	$7!/6$	840.
5+2	$7!/5\times 2$	504
5	$7!/5$	504
4+3	$\vdots$	$\vdots$
4+2		
4		
$\vdots$		

Definition: Two permutations $\sigma, \tau \in S_n$ are said to be conjugate in S_n if there exists $\rho \in S_n$ such that.

$$\sigma = \rho^{-1}\tau\rho.$$

Theorem: Two permutations $\sigma, \tau \in S_n$ are conjugate iff. they have the same cycle type.

Lemma: For any cycle $(a_1, a_2, \cdots a_k)$, and any $\rho \in S_n$. we have

$$\rho^{-1}(a_1, \cdots a_k)\rho = (a_1\rho, a_2\rho \cdots a_k\rho)$$

$$\rho^{-1}(a_1, \cdots a_k)\rho = (a_1\rho, a_2\rho \cdots a_k\rho)$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \quad \rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}. \qquad (2\ 4).$$

$$\rho^{-1}(2\ 4)\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} = (4\ 1). \quad (2\rho, 4\rho).$$

proof (Theorem): $\Rightarrow$ Suppose $\tau = \rho^{-1}\sigma\rho \quad \sigma = \psi_1\psi_2\cdots\psi_r$. disjoint.

$$\tau = \rho^{-1}(\psi_1\cdots\psi_r)\rho = \underbrace{(\rho^{-1}\psi_1\rho)}(\rho^{-1}\psi_2\rho)\cdots(\rho^{-1}\psi_r\rho)$$

same cycle type as ψ_i (Lemma)

$\Leftarrow$: σ, τ have the same cycle decomposition type.

$$\sigma = (a_1, a_2 \cdots a_k)(b_1, b_2, \cdots b_l)(c_1 c_2 \cdots c_m)\cdots$$

$$\downarrow\rho \qquad \downarrow\rho \qquad \downarrow\rho \qquad \text{conjugate.}$$

$$\tau = (\alpha_1, \alpha_2 \cdots \alpha_k)(\beta_1, \beta_2, \cdots \beta_l)(\gamma_1, \gamma_2 \cdots \gamma_m)\cdots$$

$a_i\rho = \alpha_i$. $b_i\rho = \beta_i$. $c_i\rho = \gamma_i$.

$$\alpha_i(\rho^{-1}\sigma\rho) = a_i\sigma\rho = a_{i+1}\rho = \alpha_{i+1} = \alpha_i\tau \qquad 1 \le i < k$$

$$\alpha_k(\rho^{-1}\sigma\rho) = a_1\sigma\rho = a_1\rho = \alpha_1 = \alpha_k\tau. \qquad \square$$

Example: Let $\sigma = (12)(34)(567)$ $\in S_8$.
$\tau = (28)(17)(345)$

i). How many ρ are there in S_8 s.t. $\sigma = \rho^{-1}\tau\rho$?

ii). How many $\rho \in S_8$ are there which commutes with σ?
$\rho\sigma = \sigma\rho$.

24.

4. March. 2023.
4pm (+8)