Lecture 13: The Permutation group.

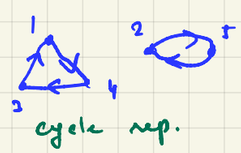
Def. A permutation is a bijection $\sigma: I_n \to I_n$; ie an n-permutation on n letters.

$S_n := \{\sigma: I_n \to I_n \mid \sigma \text{ a bijection}\}$

Example.

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

i, $\sigma(i)$



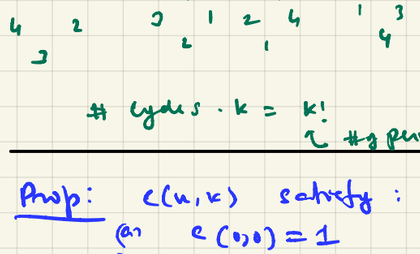
cycle rep.

Def: A k-cycle is a cyclic arrangement of k numbers from I_n.

Example. (143), (25).

Ex: # of cyclic arrangements of k objects is $(k-1)!$

cycle → rotate by $\frac{2\pi}{k}$ to get a permutation.



$\sigma \sim \tau$ if τ can be obtained by cyclic shifting.

$(1234) \to (4123) \to \cdots$

$\sim$ = equivalence relation → each has k

permutations = $\sum$ # [σ] = (# cyclic arr) k

cycles $\cdot\, k = k!$

↑ # of permutations

We can think of permutations as a "product" of disjoint cycles

Ex $(143)(25) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$

$(23)(41)(5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$

Def: (Product) $\sigma \cdot \tau := \sigma \circ \tau$

$\sigma = (154)$, $\tau = (243)$

$(154)(243) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$

↳ not disjoint.

- Product of disjoint cycles is very easy.

Prop: Any permutation can be written as a product of disjoint cycles.

proof: Let $\sigma \in S_n$. Consider $(\sigma(1), \sigma^2(1), \sigma^3(1), \dots)$. Here $\sigma^k(i) = \sigma^{k-1}(\sigma(i))$. This is a cycle. Its finite because either all elements of I_n are hit, or it starts repeating. If all are covered, then done. Else there is an $i \in I_n$ s.t. $\sigma^k(1) \neq i$ for any k. Now consider $(\sigma(i), \sigma^2(i), \dots)$. Carry on until all I_n are covered. ∎.

Ex $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \to (1, 5, 4, 3, 2)$

Def. The cycle #s $c(n,k)$ (unsigned stirling #s of first kind) is # of ways of decomposing I_n into k disjoint cycles.

n\k	0	1	2	3	4
0	() ← empty cycle.				
1	–	(1) ①			
2	–	(1,2) ①	(1)(2) ①		
3	–	(1,2,3), (1,3,2) ②	(1,2)(3), (1,3)(2), (2,3)(1) ③	(1)(2)(3) ①	
4	–	(1,2,3,4), (1,2,4,3), (1,3,2,4), (1,3,4,2), (1,4,2,3), (1,4,3,2) ⑥	(1,2,3)(4), (1,3,2)(4), (1,2)(3,4), (1,2,4)(3), (1,4,2)(3), (1,3)(2,4), (1,2,4)(3), (1,4,3)(2), (2,3)(1,4), (2,3,1)(4), (2,4,3)(1)	(1,2)(3)(4), (1,3)(2)(4), (2,3)(1)(4), (1)(2)(3,4), (1,3)(4)(2), (1,4)(2)(3)	(1)(2)(3)(4) ①

Prop: $c(n,k)$ satisfy:

(a) $c(0,0) = 1$

(b) $c(n,0) = 0$ for $n > 0$

(c) $c(n,k) = 0$ for $k > n$

(d) $c(n+1,k) = c(n,k-1) + n\,c(n,k)$ for $k > 0$.

The $c(n,k)$ are determined by numbers above.

Proof: – Given cyclic decomposition of I_{n+1} into k cycles

Either $(n+1)$ is a cycle → # $c(n,k-1)$

$n+1$ is in another cycle. Can be obtained by placing $n+1$ after $1, 2, 3, \dots, n$ → # $n\,c(n,k)$

– initial conditions – obvious.

– determined → induction ∎.

Ex. $c(n,k) = (-1)^{n+k} s(n,k)$

show this satisfies recurrence relation.

Ex. Make a table using above.

Prop: S_n is a group under composition. (mult := composition).

Proof: Associative → prop of composition of functions (calc.)

identity $\mathrm{Id}: x \mapsto x$ for each $x \in I_n$

inverse: Every σ has inverse.

ex: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ $\sigma^{-1} = \begin{pmatrix} 4 & 5 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

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

Remarks. ① S_n is non-commutative group. (Ex. Find ex)

② $(1,2,3,4,5)^{-1} = (5,4,3,2,1)$ ← inverse of cycles.

③ Disjoint cycles commute.

④ Any permutation can be written as a product of transpositions. (transposition := cycle of length 2).

Ex $(1,2,3,4,5) = (1,2)(2,3)(3,4)(4,5) = (1,5)(3,4)(1,3)(1,2)$

⑤ Ex: Show $\{(i, i+1)\}$ generate S_n, ie any permutation is a product of these transpositions (⇒ any permutation can be sorted by swapping neighbours)

⑥ If σ is a transposition, $\sigma^{-1} = \sigma$

⑦ If $\sigma_1, \dots, \sigma_k$ are transpositions, $(\sigma_1 \cdots \sigma_k)^{-1} = \sigma_k \sigma_{k-1} \cdots \sigma_1$.

Def: Given $\sigma \in S_n$, an inversion is a pair (i,j) s.t. $i < j$ and $(\sigma(i) > \sigma(j))$. The inversion # $\mathrm{INV}(\sigma)$ is the # of inversions of σ.

The sign of σ ($\mathrm{sgn}(\sigma) = (-1)^{\mathrm{INV}(\sigma)}$

Ex: List S_2 and S_3 (done earlier) and find $\mathrm{INV}(\sigma)$ for each σ.

eg. $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ Inversions: $(1,2)$, $(2,3)$, $(1,3)$, $\mathrm{sgn} = (-1)^3 = -1$

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $(2,3)$ $\mathrm{sgn} = -1$.

Ex What are inversions of $(1,2,\dots,n)$?

Thm (Lagrange's thm) Let G be any finite group. Let H be a subgroup, ie a subset of G which is also a group. Then $\#H \mid \#G$.

Proof: Let H, G be given. We define an equivalence relation on G. Let $a, b \in G$. We say $a \sim b$ if $ab^{-1} \in H$. To verify eq. relation: $\sim a a^{-1} = \mathrm{id} \in H$ (since H a group)

– if $ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow (b^{-1})^{-1} a^{-1} \in H \Rightarrow ba^{-1} \in H$ (since $(b^{-1})^{-1} = b$).

– $ab^{-1} \in H$, $bc^{-1} \in H \Rightarrow ab^{-1} \cdot bc^{-1} = a(b^{-1}b)c^{-1} = a \cdot (\mathrm{id})\, c^{-1} = ac^{-1} \in H$.

So by prop in lecture 12, the equivalence classes partition G. So $\#G = \sum_{[a] \text{ disjoint eq. classes}} [a]$

NB: $[a] = Ha := \{ha \mid h \in H\}$

$ab^{-1} \in H \Leftrightarrow ab^{-1} = h \Leftrightarrow a = hb \Leftrightarrow b = h^{-1}a \in Ha$

Further: $\#Ha = \#Hb$ (1-1 corr. $ha \leftrightarrow hb$)

So $\#G = \sum_{\text{disjoint eq. classes}} (\#H) = \#H \cdot C$

↑ # of conjugacy classes

$\Rightarrow \#H \mid \#G$. ∎.

Def: Let $a \in G$. The set $\{1, a, a^2, a^3, \dots\}$ is called the cyclic group generated by a. If $a^n = 1$, n smallest, we say order of a is n

Cor: For any group $a^{\#G} = 1$ (since order $\mid \#G$)

Cor: ① Group $= \mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$. $a^{p-1} \equiv 1 \pmod p$ ← Fermat

② $\mathbb{Z}_m^* = \{a \mid (a,m) = 1\}$ $a^{\phi(m)} \equiv 1 \pmod m$ ← Euler.

Note: For $(\mathbb{Z}_m, \cdot)$ when is $a^m = ?$ ($ma \equiv 0 \pmod m$)

$\#S_n = n!$ Every $k < n$ divides $n!$

Thm (Cayley) Any group π a subgroup of S_n for some n.

Proof: I will outline in P.S.