Group Vaction

Recall:

$$S_n := \{\text{bijections } \mathbb{N}_n \circlearrowright\}$$

i.e S_n is the grp of permutations of $\{1, \dots, n\}$ with bin op of composition

S_n is non abelian for $n \geq 3$ & $|S_n| = n!$

Recall Cycle Notation

in S_7 (123) represents

$1 \to 2 \to 3$ 4 5 6 7 $\to$ 3 1 2 4 5 6 7

Defn Cycle of length 2 / swap is called a transposition

It is of the form (ij) for $1 \leq i < j \leq n$

Remark S_n has $\binom{n}{2}$ transpositions!

Remark Transpositions are self inverting

$(12)(12) = e$

Lemma For $n \geq 2$. $\forall \sigma \in S_n$

σ is the product of trans

PF Base case: $n = 2$

$S_2 = \{e, (12)\}$

$e = (12)(12)$, $(12) = (12)$ so done

Another base case: $n = 3$

$(123) = (12)(23)$ $(132) = (23)(12)$

let $n \geq 4$. Spose the result holds for $n-1$

Case (1)

$\sigma(n) = n$ — doesn't effect the last ell

grp action

Then $\sigma|_{\mathbb{N}_{n-1}}$ gives a permutation in $n-1$

$\therefore \sigma|_{\mathbb{N}_{n-1}}$ is a product of trans in S_{n-1}

These 'same' transpositions exist in S_n and the product gives σ!

Case 2)

$\sigma(n) = i \neq n \Rightarrow i < n, \; i \in \mathbb{N}_{n-1}$

By above, $(in)\sigma$ is a product of trans as

$[(in)\sigma](n) = [(in)]\sigma(n) = (in)(i) = n$

So, $(in)\sigma = t_1 \cdots t_n$

$\Rightarrow \sigma = (in) t_1 \cdots t_n$ ☐

Defn let G be a grp. let $g \in G$

$\langle g \rangle := \{ g^n \mid n \in \mathbb{Z} \}$

Eg. $g^1 = g \quad g^2 = g \cdot g \quad g^{-1} = g^{-1} \quad g^{-2} = g^{-1} g^{-1}$

$g^0 = e$

Claim $\langle g \rangle$ is a subgrp of G.

Remark it is the smallest (by containment) grp that contains g

PF ① let $g^m, g^n \in \langle g \rangle \quad g^m \cdot g^n = g^{m+n} \in G$

(any case works)

② $g^n \in \langle g \rangle$, consider g^{-n}. $g^n g^{-n} = g^0 = e \in G$

$\Rightarrow \langle g \rangle \leq G$

Defn The subgrp $\langle g \rangle \leq G$ is the **cyclic grp generated by g**.

e.g let $G = (\mathbb{Z}, +)$

fix $m \in \mathbb{Z}$, $\langle m \rangle = m\mathbb{Z}$

Defn Let G be a grp.

we say G is **cyclic** p.t $\exists g \in G$ s.t $\langle g \rangle = G$.

In this case, g is a **generator**.

e.g. $(\mathbb{Z}, +) = \langle -1 \rangle = \langle 1 \rangle$

$(\mathbb{Z}/4\mathbb{Z}, +)$ is gen by $\langle \bar{1} \rangle, \langle \bar{3} \rangle$

non.eg. S_3 is not cyclic → check by cases.

$(\mathbb{R}, +)$ → **countability contradiction**

Cool | Space G is a finite grp & $|G|$ is prime.

Thm: **Lagrange says**

for $H \leq G$ $\Rightarrow |H| = 1$ or $|H| = |G|$

fix $g \neq e$ in G, $|\langle g \rangle| \neq 1$ so $|\langle g \rangle| = |G|$

$\Rightarrow \langle g \rangle = G$

looks like $\mathbb{Z}/p\mathbb{Z}$

So all **finite, prime grps are cyclic**

Usual on Hw, we showed if $|G| = n$ & G is **cyclic**,

$G \cong \mathbb{Z}/n\mathbb{Z}$ $\Rightarrow$ if $|G|$ is **prime**

it is hard to understand $\langle g \rangle$ as if is over $\mathbb{Z}$. let's see what we can do

→

Lemma Let G be finite grp.

If $g \in G$, $\exists n \in \mathbb{N}$ s.t. $g^n = e$

Pf $\{g, g^2, \dots\} \subseteq G$

$\exists i, j$, $i < j$ s.t. $g^i = g^j$ then $g^{i-j} = e$

G If this isn't true, not finite

Defn The order of g in the finite grp G is

$$\mathcal{O}(g) = \min_{n \in \mathbb{N}} (g^n = e)$$

well ordered

e.g. $\mathcal{O}(12)$ is 2 in S_{75}

Lemma Let G be fin gen. Let $g \in G$. Then,

$|\langle g \rangle| = \mathcal{O}(g)$. Specifically

$\langle g \rangle = \{g^n \mid n \in \mathbb{N}_{\mathcal{O}(g)}\}$

Pf for the sake of brevity $d = \mathcal{O}(g)$

$A = \{g^n \mid n \in \mathbb{N}_d\}$

Show $\langle g \rangle = A$ $\supseteq$ is free

Observe $g^d = e$

$\forall \ell > 0$ $\exists!$ $d \in \mathbb{N}$ and r s.t. $0 \le r \le d-1$

So, $\ell = d \cdot q + r$

$g^\ell = g^{dq+r} = (g^d)^q g^r = g^r \in A$

for $\ell < 0$, 2 ways

① Show A is closed under inverses $\Rightarrow$ if $g^\ell \in A \Rightarrow g^{-\ell} \in A$

② Show A is a subgrp of G. We have $\langle g \rangle$ is the smallest subgrp containing g and we're done!

Now, we showed $|\langle g \rangle| = k$. But we don't know about repeats. So, we can't conclude

$$|\langle g \rangle| = o(g)$$

If $g^i = g^j$ for $i, j \in \mathbb{N}_{\geq 1}$, $i \neq j$

WLOG $i < j$

$\Rightarrow g^{j-i} = e$ and $j - i < o(g)$ oops

Defn Let G be a grp. G is simple pt the only normal subgrps are:

- $\{e\}$ & G

E.g. $\mathbb{Z}/p\mathbb{Z}$ as the only subgrps are $\{e\}$ & G

Recall Let G be a grp. Let $H \leq G$ then H is normal pt

$\forall g \in G \quad gH = Hg$

This is nice since

$G/H = \{gH \mid g \in G\}$

is a grp where

$(aH)(bH) = (ab)H$

∴ Quotient grps of a simple grp are

$G/\{e\} \equiv G$, $G/G \equiv e$

Fact The only simple abelian grps are $\mathbb{Z}/p\mathbb{Z}$

↳ abelian $\Rightarrow$ all subgrps are normal

Recall Lagrange Says

if G is a finite grp & $H \leq G$ $|H| \mid |G|$

does the converse hold? ——→ Fails

↳ for $n \in \mathbb{N}$ s.t. $n \mid |G| \Rightarrow \exists\ H \leq G$ s.t. $|H| = n$

Cauchy Thm

Let G be a finite grp. Let p be a prime factor of $|G|$.

$\exists\ H \leq G$ s.t. $|H| = p$

Pf Not done here. But case where $p=2$ is ez.

Suppose $|G|$ is even

Consider the pairs $\{g, g^{-1}\}$ where $g \neq g^{-1}$

The elements that don't belong to such a pair are interesting, i.e. $g \in G$ s.t. $g^2 = e$

Considering $|G| \equiv 0 \pmod 2$.

If we ignore pairs $\{g, g^{-1}\}$ ← 2 elt at a time

$|G| \equiv |\{g \in G \mid g^2 = e\}| \pmod 2$

But $e \in$ ↗

But $|G| \equiv 0 \bmod 2$.

$\therefore \exists\ g \in G$ s.t. $g \neq e$ but $g^2 = e$.

$\{g, e\}$ is the subgrp we seek!

↳ $\langle g \rangle$

Idea We know that every permutation can be written as a product of transpositions → non-unique

Suppose $\sigma = T_1 \cdots T_\ell$

$\sigma = S_1 \cdots S_k$ → parity is fixed

We will show, $k - \ell$ is even. Once we have this defn

$\operatorname{sgn} : S_n \longrightarrow \{\pm 1\}$

$\sigma \mapsto$ 1 if σ is 'even'

-1 if σ is 'odd'

Then $\text{sgn}: S_n \to \{\pm 1\}$ is a grp homomorphism
$\{\pm 1\}$ with mult
↳ $\cong$ to $\mathbb{Z}/2\mathbb{Z}$

Define $A_n := \ker(\text{sgn})$

↳ normal subgrp & consists of all even perms

A_n is the alt grp. It is a normal subgp of S_n.

How big is A_n?

Guess: $\frac{n!}{2}$ as $|S_n| = n!$

We can show this by showing:

If $B_n :=$ odd perms

$A_n \cap B_n = \emptyset$ (Follows if sgn is well def)

Cook up bij between A_n & B_n e.g $\sigma \mapsto (12)\sigma$

$\therefore |A_n| = |B_n|$ & $A_n \cup B_n = S_n$

Claim: A_4 is the special grp from earlier

$$|A_4| = \frac{4!}{2} = \frac{24}{2} = 12$$

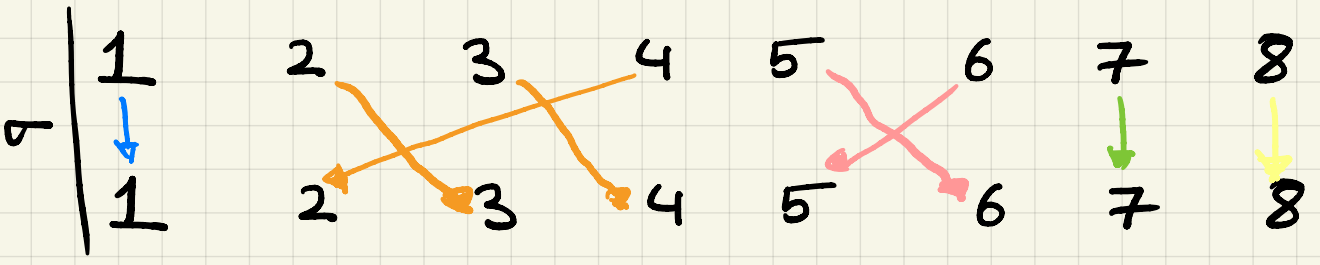
But $\nexists\ H \leq G$ s.t. $|H| = 6$!

But we gotta show that stuff abt parity!

Recall: S_n acts on $\mathbb{N}_n$ by def

e.g $\sigma = (234)(56) \in S_8$

consider $\langle \sigma \rangle$ acting on $\mathbb{N}_8$ and two orbits!



So since $\langle\sigma\rangle$ → powers of σ

$\mathbb{N}_8 / \sim = \{\{1\}, \{2,3,4\}, \{5,6\}, \{7\}, \{8\}\}$

↳ 5 orbits

$|\langle\sigma\rangle| = \Theta(\sigma) = 6$ ↗ lcm of all these!

More generally $T \in S_n$ & $T^k(k) = k$ for some $k \in \mathbb{N}_n$

$\Rightarrow k \mid \Theta(\langle T \rangle)$

Lemma if $1 \le i < j \le n$

Fix $\sigma \in S_n$. Then no of $\langle\sigma\rangle$ orbits in $\mathbb{N}_n$

$= (\#$ of $\langle(ij)\sigma\rangle$ orbits in $\mathbb{N}_n) \pm 1$

e.g $\sigma \in S_n$ orbs from earlier. Take $i=2, j=7$

↳ $(234)(56)$

$(27)\sigma$

1	2	3	4	5	6	7	8
↓							
1	2	3	4	5	6	7	8

We lost 1 orbit. In some sense, we joined 2 orbits!

e.g 2 Let $i = 2, j = 3$

$(23)\sigma$

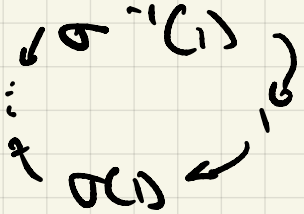
1	2	3	4	5	6	7	8
↓							
1	2	3	4	5	6	7	8

We gained 1 orbit. In some sense, we broke an orbit!

Sketch of proof

Fix $\sigma \in S_n$ and $1 \le i < j \le n$

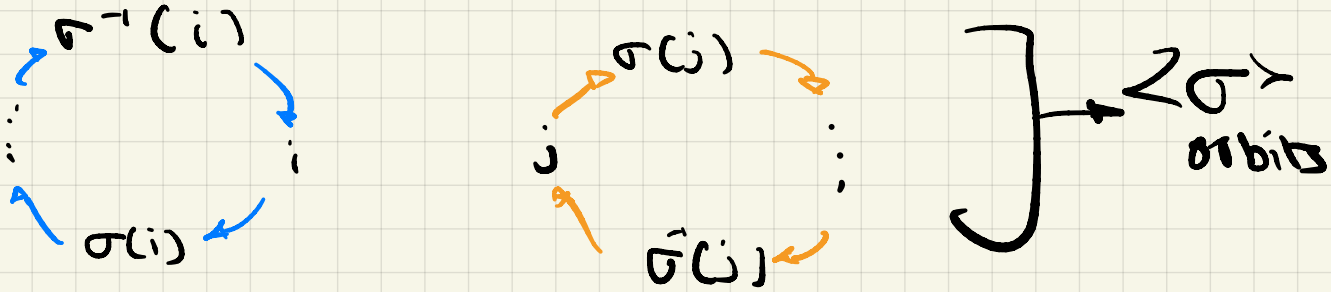
Lets draw an orbit



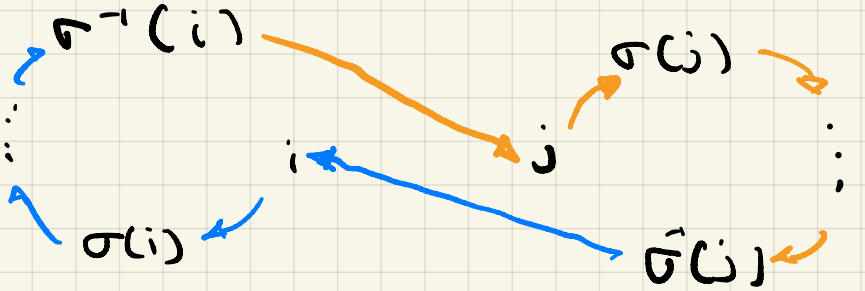
An orbit of $\langle\sigma\rangle$ is an orbit of $\langle (ij), \sigma \rangle$ iff that orbit doesn't contain i or j

What if they do?

(I) i, j are in distinct orbits

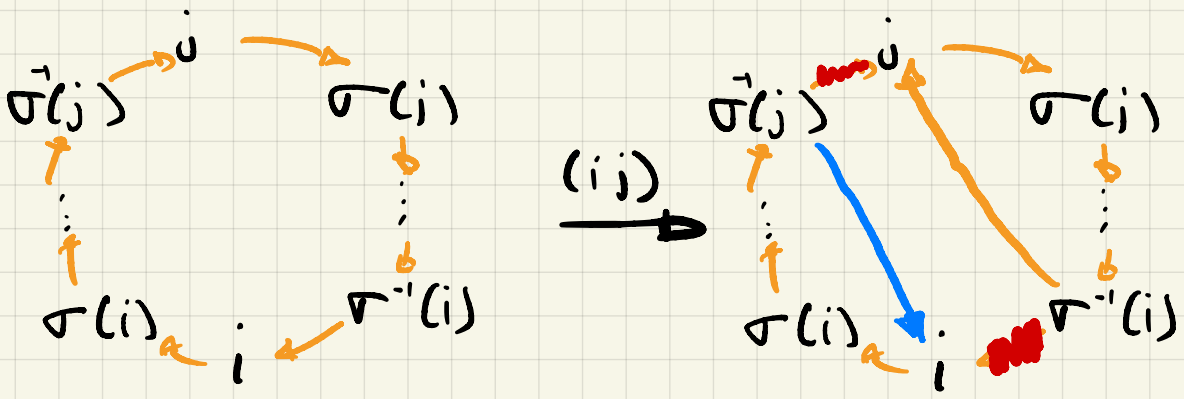


What happens in $\langle (ij), \sigma \rangle$



So in this case, we removed an orbit.

(II) i, j are in same $\langle\sigma\rangle$ orbit



So here, we added an orbit

□

Corr fix $n \in \mathbb{N}$ & $\sigma \in S_n$. Suppose

$\exists\, t_1, t_2 \cdots t_k \in S_n$ s.t $\sigma = t_1 t_2 \cdots t_k$

$\exists\, t_1', t_2' \cdots t_\ell' \in S_n$ s.t $\sigma = t_1' t_2' \cdots t_\ell'$

$\ell - k$ is even.

Pf we are done if we can show that the identitiley is the product of only an even no of Things.

Why?

$$t_1 \cdots t_k = t_1' \cdots t_\ell'$$

$$\Rightarrow e = \underbrace{(t_1 \cdots t_k)(t_\ell' \cdots t_1')}_{k+\ell}$$ ↷ as trans are self inv

if $k+\ell$ is even $\Rightarrow$ $k-\ell$ is even!

So lets do it.

Consider $\mathbb{N}_n = \{1 \cdots n\}$ and $\langle e \rangle$ acting on it.

we have n orbits.

Suppose $\exists\, t_1 \cdots t_r$ s.t $e = t_1 \cdots t_r e$

$\langle e \rangle \to n$ orbits

$\langle t_r e \rangle \to n \pm 1$ orbits

$\langle t_{r-1} t_r e \rangle \to \pm 1$ orbits

$\vdots$

$\langle t_1 \cdots t_r e \rangle \to n - p + q$ orbits ↷ $(p+q = r)$

where p is # of (-1)'s and q is no of $(+1)$'s

But $\langle t_1 \cdots t_r e \rangle = \langle e \rangle$

$\Rightarrow n - p + q = n \Rightarrow p = q.$

$\Rightarrow r = p + q = 2p \Rightarrow$ r is even ↷

Defn The Rmc

$$\text{sgn}: S_n \longrightarrow \{-1, 1\}$$

$$\sigma \longmapsto \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{otherwise} \end{cases}$$

Defn We call $\sigma \in S_n$ **even** p.t

it can be written as an even no of trans

otherwise it is **odd**.

Defn We define $A_n \leq S_n$ as the set of even perms!

This is called the **Alternating grp**

The fact that it is a subgrp comes from

$A_n = \ker(\text{sgn})$

Defn $B_n \subseteq S_n$ is the set of odd perms

It isn't a subgrp obviously

Lemma $|A_n| = |B_n|$ For $n \geq 2$

Pf We will **cook up a bij**

Fix $1 \leq i < j \leq n$ → valid as $n \geq 2$

Define.

$$A_n \longrightarrow B_n$$
$$\sigma \longmapsto (ij)\sigma$$

Check bijectivity. ▷

Corr $S_n = A_n \sqcup B_n$

$\Rightarrow |S_n| = |A_n| + |B_n| \Rightarrow |A_n| = |B_n| = \frac{n!}{2}$

Cor $(ij)A_n = A_n(ij) = B_n \Rightarrow$ it is normal (almost, we only check trans) & also a ker

$S_n / A_n = \{A_n, B_n\} \cong \mathbb{Z}/2\mathbb{Z}$