March2

Tuesday, March 2, 2021 12:39 PM

Takehome 1 Graded

* I will review regrade requests submitted before 3/8.

Main Comment:

$|G| =$ order of G = # elts in G.

$|G| \neq \max\{|x| : x \in G\}$ $\longleftarrow$ If $x \in G$ w/ $|x| = |G|$ $\rightsquigarrow G = \langle x \rangle$.

Ex $G = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ times}}$

$\rightsquigarrow |G| = 2^n$ $\quad x \in G \rightsquigarrow |x| \leq 2.$

Last time

$G \circlearrowleft G$ by conjugation.

$$g * a = gag^{-1}$$

Obersavrions / Def^n_s

① Given $a \in G$, orbit of a is

$$G * a = \{gag^{-1} \mid g \in G\}$$

called conjugacy class of a

Rmk Unlike cosets, vary in size as a varies.

② $G*a=\{a\} \iff ga=ag \quad \forall g\in G$

$\iff a\in Z(G)$

③ The stabilizer of a:

$$G_a := \{g\in G \mid ga=ag\}$$

$$= C_G(a).$$

④ Orbit Stabilizer

$$|G*a| = |G:G_a| = |G:C_G(a)|$$

Consequences

TH 1(c)

The conjugacy classes of G partition G

$$|G| = |O_1|+|O_2|+\dots+|O_n|$$

But by above know $(g\in O_i)$

$$|O_i| = \begin{cases} 1 & \text{if } g\in Z(G) \\ |G:C_G(g)| \end{cases}$$

Theorem (Class Equation)

Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ orbits not in $Z(G)$

Let $g_i \in \mathcal{O}_i$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Examples

① G abelian. $|G| = |Z(G)|$

$(G = Z(G))$ boring.

② Compute conjugacy classes of S_3

$$\{(1)\}, \quad \underline{\{(1\,2),(1\,3),(2\,3)\}}, \leftarrow$$

$$\underset{\in Z(S_3)}{\uparrow} \qquad \{(1\,2\,3),(1\,3\,2)\}$$

$$C_{S_3}((1\,2)) = \langle (1\,2) \rangle$$

$$|S_3 : C_{S_3}(1\,2)| = 6/2 = 3$$

$$C_{S_3}(1\,2\,3) = \langle (1\,2\,3) \rangle$$

$$|S_3 : C_{S_3}(1\,2\,3)| = 6/3 = 2$$

↙

$$|Z(S_3)| + |S_3 : C_{S_3}(1\,2)| + |S_3 : C_{S_3}(1\,2\,3)|$$

$= 1 + 3 + 2 = 6$ ✓

Class Equation... in action

Theorem Let p a prime number.
Let G a group. $|G| = p^d$. $d > 0$
Then $Z(G) \neq \{1\}$

Proof

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Notice

① $|G : C_G(g_i)| \cdot \underline{|C_G(g_i)|} = |G|$ (Lagrange)

$= p^d$

By def, $g_i \notin Z(G)$ so

$$p \mid |G : C_G(g_i)|$$

$$\underbrace{|G|}_{\text{div by } p} = \underbrace{|Z(G)|}_{\text{Div by } p.} + \underbrace{\sum_{i=1}^{r} |G : C_G(g_i)|}_{\text{div. by } p}$$

$|Z(G)| \geq 1$ & div by p so $\geq p$

we win

Theorem (Classification of groups of order p^2)

(Generalizes TH1 4(d))

If $|G| = p^2$ then

1) G abelian ← HW 6 2(c) ✓

2) $G \simeq \mathbb{Z}_{p^2}$ or $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof

1) Know $Z(G) \neq 1$. So $|Z(G)| = p$ or p^2.

If $|Z(G)| = p^2$ we win.

Else $|Z(G)| = p$.

⟶ ⇝ HW 6 2(a) $Z(G) \trianglelefteq G$.

So $G/Z(G)$ ← group of order p.

⇝ TH1 4a ← $G/Z(G) \simeq \mathbb{Z}_p$

⟶ ⇝ HW6 2b ← $G/Z(G)$ cyclic

⟹ G abelian.

Done!

Prove part 2 Suppos $G \not\simeq \mathbb{Z}_{p^2}$.

Show $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

Pick $x \in G \setminus \{1\}$. Then $|x| = p$

Pick $y \in G \setminus \langle x \rangle$. Then $|y| = p$.

Define

$$\begin{aligned} \mathbb{Z}_p \times \mathbb{Z}_p &\longrightarrow G \\ (a^i, b^j) &\longmapsto x^i y^j \end{aligned}$$

1) Well defined.

$(a^i, b^j) = (a^{i'}, b^{j'})$

$\rightsquigarrow i \equiv i' \mod p \qquad j \equiv j' \mod$

$\Rightarrow x^i y^j = x^{i'} y^{j'}$ b/c $|x| = p = |y|$ + abelian.

2) Homom! (adding exponents on each side).

3) $x^i y^j = 1$.

$\rightsquigarrow (x^i)^{-1} = y^j$ But $\langle x \rangle \cap \langle y \rangle = \{1\}$

so $x^i = 1$, $y^j = 1$

$\Rightarrow a^i = 1$ & $b^j = 1$

Get injectivity.

4) Surjectivity.

Injection btwn 2 sets of order p^2 $\Longrightarrow$ Surjection

HW1 . ∅

Remark

Class equation allows us to extract lots of info about the internal structure of a group from its order.

Special Case:

Conjugacy in S_n.

The example of S_3 suggests that the shape of cycle decomp. informs the conjugacy classes.

$\uparrow$ determines.

Goal

Give $\tau, \sigma \in S_n$. How do

σ & $\tau * \sigma = \tau \sigma \tau^{-1}$

relate?

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

$$\sigma(i) = j \iff (\tau * \sigma)(\tau(i)) = \tau(j)$$

Rmk

Consider analogy w/ changing bases in lin. alg.

Pf/ $(\tau * \sigma)(\tau(i)) = \tau \sigma \tau^{-1}(\tau(i))$

$= \tau\sigma(i)$

$= \tau(j)$

Corollary (Conjugation preserves cycle type).

σ have cycle decomp

$$(a_1\ \underline{a_2 \cdots a}_{n_a})(b_1\ b_2 \cdots b_{n_b})\cdots(z_1\ z_2 \cdots z_{n_z})$$

Then

$$\tau * \sigma = \tau \sigma \tau^{-1}$$

$$= (\tau a_1\ \underline{\tau a_2 \cdots} \tau a_{n_a})(\tau b_1 \cdots \tau b_{n_b})\cdots(\tau z_1 \cdots \tau z_{n_z})$$

Pf/ Follows from lemma.

$$\begin{array}{ccc} \tau * \sigma(\tau(a_i)) & = & \tau(a_{i+1}) \\ \| & = & \\ \tau(\sigma(a_i)) & & \end{array}$$

Ex $\sigma = (1\ 2)(3\ 4\ 5)$

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

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

$$= (2\ \ 3)(4\ \ 1\ \ 5) = \gamma$$

Check

$\tau\sigma\tau^{-1}(1) = \tau\sigma(4) = \tau(5) = 5$ ✓

$\gamma(1) = 5$

Observe

$\sigma = (\cdots n_1 \text{ terms})(\cdots n_2 \text{ terms}) \cdots (n_t \text{ terms})$

$\tau * \sigma = (\cdots n_1 \text{ terms} \cdots)(n_2 \text{ terms}) \cdots (n_t \text{ terms})$

Def^{n}

If $\sigma \in S_n$ decomposes into $\sigma_1\sigma_2\cdots\sigma_m$ w/ disjoint n_i cycles (including 1-cycles)

① $n_1 \leq n_2 \leq \cdots \leq n_m$

② $\sum n_i = n$.

The cycle type of σ is $(n_1, n_2, \dots, n_m)$

Ex in S_5 — Cycle type

$(1\ \ 2)(3\ \ 4\ \ 5) \leftarrow (2, 3)$

$(5)(1\ \ 2\ \ 3\ \ 4) \leftarrow (1, 4)$

Theorem A 2 elts of S_n are conjugate $\iff$ they have the same cycle type.

Pf/ $\Longrightarrow$ (done, corollary).

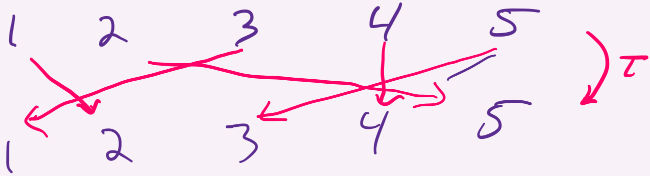
$\Longleftarrow$ First an example.

$\sigma_1 = (1\ 2)(3\ 4\ 5)$

→ $\sigma_2 = (2\ 5)(1\ 4\ 3)$

Goal

Find τ w/ $\tau\sigma_1\tau^{-1} = \sigma_2$



$\tau\sigma_1\tau^{-1} = (\tau(1)\ \ \tau(2))(\tau(3)\ \ \tau(4)\ \ \tau(5))$

$(2\ \ 5)(1\ \ 4\ \ 5)$

$= \sigma_2.$

In general

$\sigma_1 = (a_1 \cdots a_{n_a}) \cdots (z_1 \cdots z_{n_z})$

$\sigma_2 = (\hat{a}_1 \cdots \hat{a}_{n_a}) \cdots (\hat{z}_1 \cdots \hat{z}_{n_z})$ ←

Define $\tau(a_1) = \hat{a}_1$
$\tau(a_2) = \hat{a}_2$
$\vdots$
$\tau(z_{n_t}) = \hat{z}_{n_t})$

$\Longrightarrow \tau \sigma_1 \tau^{-1} = \sigma_2$ by corollary. $\emptyset$

Slogan

Congugacy classes of S_n are shapes of permutations.

Rmk τ above need not be unique

$\sigma_1 = (14)$ $\sigma_2 = (23)$

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

$$\left\{ \begin{matrix} (1\ 2)(3\ 4) \\ (1\ 2\ 3\ 4) \end{matrix} \right\} \ni \tau$$

Def$^{\underline{n}}$ Let $n \in \mathbb{N}$, a partition of n is a set $\{n_1, n_2, \ldots, n_t\} \subseteq \mathbb{N}$ s.t. $\sum n_i = n$.

Theorem $\exists$ a bijection

$$\left\{\begin{array}{c}\text{conjugacy}\\ \text{classes}\\ \text{in } S_n\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{partions of}\\ n\end{array}\right\}$$

$$S_n * \sigma \xmapsto{\text{well defined by thm A}} \text{Cycle type of } \sigma.$$

$$\begin{array}{l}(1\,2 \cdots n_1)\\ (n_1+1, \ldots, n_1+n_2)\\ \quad\vdots\\ (n_1+\cdots+n_{r-1}+1, \ldots, n_1+\cdots+n_r) = \sigma\end{array} \longleftarrow\!\!\!\!\dashv (n_1, \ldots, n_t)$$

Take $S_n * \sigma$.

Upshot

Enumerating conjugacy classes in S_n boils down to enumerating partitions of n.

Example Conjugacy Classes in S_5

Partitions of 5	Conj rep
$1+1+1+1+1$	$(1)(2)(3)(4)(5) = (1)$ ←
→ $1+1+1+2$	$(1\ 2)$ ←
$1+1+3$	$(1\ 2\ 3)$ ←
$1+4$	$(1\ 2\ 3\ 4)$ ←
5	$(1\ 2\ 3\ 4\ 5)$

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

$2+3$ $(1\ 2)(3\ 4\ 5)$

Observe $Z(S_5) = \{1\}$. (Exercise). $\leftarrow$

Application Compute Centralizer of an m-cycle in S_n.

Let $\sigma = (a_1\ a_2\ \cdots\ a_m)$

List elts that commute w/ σ

$\longrightarrow$ 1) $1, \sigma, \sigma^2, \ldots, \sigma^{m-1} \in C_{S_n}(\sigma)$

2) $\tau \in S_n$ & $\tau(a_i) = a_i$. (τ disjoint from σ $\Longrightarrow \tau\sigma = \sigma\tau$ (Hw 2 or 3))

τ a permutation of

$$\{1, \ldots, n\} \setminus \{a_1, \ldots, a_m\} \longleftrightarrow \{1, \ldots, n-m\}$$

$\rightsquigarrow$ "$\tau \in S_{n-m}$."

Get $\sigma^i \tau \in C_{S_n}(\sigma)$

How many? $\tau \in S_{n-m}$ $\leftarrow (n-m)!$

m σ^i's

Enumerated $m(n-m)!$ elts of $C_{S_n}(\sigma)$.

Lemma $|C_{S_n}(\sigma)| = m(n-m)!$

Pf/
$$|S_n * \sigma| = |S_n : C_{S_n}(\sigma)| = \frac{|S_n|}{|C_{S_n}(\sigma)|} = \frac{n!}{\underset{\substack{\uparrow \\ \text{Solve for } x}}{x}}$$

$$\uparrow$$

$$= \#(m\text{-cycles})$$

$$= \frac{n(n-1)(n-2)\cdots(n-m+1)}{\underset{\substack{\uparrow \\ \text{rotate}}}{m}}$$

Solve for $x = \dfrac{n! \cdot m}{n(n-1)(\cdots(n-m+1)} = m(n-m)!$ $\emptyset$

Consequence σ an m-cycle
Then

$$C_{S_n}(\sigma) = \left\{ \sigma^i \tau \;\middle|\; \begin{array}{l} i = 0, \dots, m-1 \\ \text{“}\tau \in S_{n-m}\text{”} \end{array} \right\}$$

$$\begin{tikzcd} C_{S_n}(\sigma) & \sigma^i\tau \\ \mathbb{Z}_m \times S_{n-m} \arrow[u, "\cong", "\text{exercise}"'] & (i,\tau) \arrow[u, mapsto] \end{tikzcd}$$

To finish

Goal A_5 is a simple group.

Recall

A_5 = even permutations in S_5.

G is simple if $H \trianglelefteq G$
$\implies H = 1$ or $H = G$.

Lemma Let $H \trianglelefteq G$. Let $\mathcal{K} \subseteq G$ be a conjugacy class. Then either

$\mathcal{K} \cap H = \emptyset$ or $\mathcal{K} \subseteq H$.

Pf/ Suppose $x \in \mathcal{K} \cap H$.

H normal $\implies gxg^{-1} \in H \quad \forall g$.

But $\mathcal{K} = \{gxg^{-1} \mid g \in G\} \subseteq H$

Slogan

A normal subgroup is a union of conjugacy classes.

Warning / Rmk

$$\sigma_1 \,\&\, \sigma_2 \text{ conjugate in } A_5 \;\underset{\cancel{\Longleftarrow}}{\Longrightarrow}\; \sigma_1 \,\&\, \sigma_2 \text{ are conjugate in } S_5$$

$\tau \sigma_1 \tau^{-1} = \sigma_2$

BUT $\tau \notin A_5$ (odd).

Theorem

A_5 is a simple group.

Proof Strategy

- Enumerate all conjugacy classes in A_5 w/ warning in mind
- Sums of orders of conj classes never divides 60 unless 60 or 1.

Cycle types in A_5

$(1,1,1,1,1)$, $(1,1,3)$, (5), $(1,2,2)$ ←

Not $(1,1,1,2)$ ← 2 cycle odd

$(1,4)$ ← 4-cycle odd

$(2,3)$ ← odd

$(ab)(cde)$

$1\ 1\ 1\ 1\ 1 \longleftarrow (1),\ K_0$ order 1

$1\ 1\ 3 \longleftarrow K_1$ order 20

$5 \Longleftarrow K_2, K_3$ order 12 each.

$1\ 2\ 2 \longleftarrow K_4$ order 15

Classes of type (1,1,3)

$$C_{S_5}(1\ 2\ 3) = \{(1\ 2\ 3)^i \underset{\text{odd}}{\tau} \mid \tau \in S_{\{4,5\}}\}$$

$$C_{A_5}(1\ 2\ 3) = \langle (1\ 2\ 3) \rangle \leftarrow \text{order } 3$$

Orbit stab

$$|A_5 * (1\ 2\ 3)| = \frac{|A_5|}{|C_{A_5}(1\ 2\ 3)|} = \frac{60}{3} = 20$$

How many 3 cycles?

$$(a\ b\ c) = \frac{5 \cdot 4 \cdot 3}{3} = 20.$$

$\rightsquigarrow A_5 * (1\ 2\ 3) =$ all 3 cycles.

5 cycles

$$C_{S_5}((1\,2\,3\,4\,5)) = \langle \overset{\sigma}{(1\,2\,3\,4\,5)} \rangle$$

$$\parallel$$

$$C_{A_5}(\sigma) \leftarrow \text{order } 5$$

$$|A_5 * \sigma| = \frac{60}{5} = 12 \leftarrow \text{half}$$

5 cycles.

How many 5-cycles??

$$(a\ b\ c\ d\ e) = \frac{5!}{5} = 24.$$

$$\sigma' = (1\ 2\ 3\ 5\ 4) = (4\,5)\,\sigma\,(4\,5)$$

conjugate is S_n but by something odd.

$$|A_5 * \sigma'| = 12$$

2 conjugacy classes of 5 cycles!

Accounted for

$|K_0|+|K_1|+|K_2|+|K_3| = 45$ elts.

Cycle type $(2,2)$

Lemma

$\rightarrow C_G(\overbrace{(12)(34)}^{\sigma}) = \left\{ \begin{matrix} 1, (12)(34) \\ (13)(24), (14)(23) \end{matrix} \right\}$ ✓

Pf/ $\supseteq$ check directly

$\subseteq$ ① $\tau\sigma\tau^{-1}$ $\qquad \tau = (ab)(c\ 5)$

$\uparrow$ acts nontrivially on 5 so cannot be σ.

② $|\tau| = 1, 3, 5$

If $\sigma\tau = \tau\sigma$ $\qquad \leftarrow \sigma^2 = 1$

$$(\sigma\tau)^n = (\tau\underbrace{\sigma)(\sigma}\tau)(\tau\sigma)(\sigma\tau)\ldots$$

$$= \begin{cases} \tau^n & n \text{ even} \\ \tau^n\sigma & n \text{ odd.} \end{cases}$$

$|\tau| = \text{odd}$ top never 1

Bottom never 1 $\lightning$

$|\sigma\tau| < \infty$ $\varnothing$

Upshot

$$|A_5 * \sigma| = \frac{60}{4} = 15$$

all remaining $(2,2)$ elts.

$H \trianglelefteq A_5$ then

$$H = \bigcup \mathcal{K}_i$$

$$\rightsquigarrow |H| = \sum |\mathcal{K}_i|$$

$$= 1 + \delta_1(20) + \delta_2(12) + \delta_3(12) + \delta_4(15)$$

$$\delta_i = 0, 1.$$

Also $|H|$ divide 60.

Only happen if $\delta_i = 0 \ \forall i$

$\delta_i = 1 \ \forall i$

QED ∅

Consequence

A_5 has no subgroup of order 30.

Such a sub have to be normal

A converse to Lagrange is false. ∅