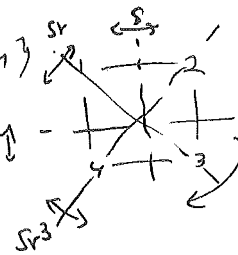
EXAMPLE: $G = D_4$ acting on vertices $\{1,2,3,4\}$



gives a subgroup im φ of S_4 isomorphic to D_4, namely

$$\{1, \underset{r}{(1234)}, \underset{r^2}{(13)(24)}, \underset{r^3}{(1432)}, \underset{s}{(12)(34)}, \underset{sr}{(1)(3)(24)}, \underset{sr^2}{(14)(23)}, (13)(2)(4)\}$$

---

§7.2 The class equation

Note that whenever a <u>finite</u> group G acts on a <u>finite</u> set S, if the G-orbits are $\mathcal{O}_{s_1}, \mathcal{O}_{s_2}, \ldots, \mathcal{O}_{s_t}$

then $S = \mathcal{O}_{s_1} \sqcup \mathcal{O}_{s_2} \sqcup \cdots \sqcup \mathcal{O}_{s_t}$

$$\Rightarrow |S| = |\mathcal{O}_{s_1}| + |\mathcal{O}_{s_2}| + \cdots + |\mathcal{O}_{s_t}| = \sum_{\text{orbits } \mathcal{O}_s} |\mathcal{O}_s|$$

and each $|\mathcal{O}_s| = \dfrac{|G|}{|G_s|}$, so

$$\boxed{|S| = \sum_{\text{orbits } \mathcal{O}_s} \frac{|G|}{|G_s|}}$$

<u>NOTE</u>: <u>Every</u> term $\frac{|G|}{|G_s|}$ divides into $|G|$!

10/24/2018 > In the special case where $S = G$ itself with G-action via <u>conjugation</u>

$$g * h := ghg^{-1}$$

then everything gets a special name:

$$\mathcal{O}_h = \{ghg^{-1} : g \in G\} = \text{the } \underline{\text{conjugacy class}} \text{ of } h \text{ in } G =: C(h) \text{ or } C_G(h)$$

$$G_h = \{g \in G : \underbrace{ghg^{-1} = h}_{\text{i.e. } gh = hg}\} = \text{the } \underline{\text{centralizer}} \text{ of } h \text{ in } G =: Z(h) \text{ or } Z_G(h)$$

and

$$\boxed{|G| = \sum_{\substack{\text{conjugacy} \\ \text{classes } C(h)}} |C(h)| = \sum_{\substack{\text{conjugacy} \\ \text{classes } C(h)}} \frac{|G|}{|Z(h)|}}$$

is called the <u>class equation</u> of G

EXAMPLES: ① We've seen for $G = S_3$, there are 3 conjugacy classes:

$C(e) = \{e\}$, $Z(e) = S_3$

$C((12)) = C((13)) = C((23)) = \{(12),(13),(23)\}$, $Z((12)) = \langle (12) \rangle = \{e,(12)\}$

$$\left(|C((12))| = \frac{|S_3|}{|Z((12))|} = \frac{3!}{2} = \frac{6}{2} = 3 \checkmark \right)$$

$C((123)) = C((132)) = \{(123),(132)\}$, $Z((123)) = \langle (123) \rangle = \{e,(123),(132)\}$

So S_3 has class equation

$$3! = |C(e)| + |C((12))| + |C((123))|$$
$$= 1 + 3 + 2$$
$$= \frac{3!}{3!} + \frac{3!}{2} + \frac{3!}{3}$$

② In general for S_n, who are the conjugacy classes?

PROPOSITION: If $p \in S_n$ has cycle decomposition

$$p = (a_1\, a_2 \cdots a_\alpha)(b_1\, b_2 \cdots b_\beta) \cdots (z_1\, z_2 \cdots z_\zeta)$$

then $qpq^{-1} = (q(a_1)\, q(a_2) \cdots q(a_\alpha))(q(b_1)\, q(b_2) \cdots q(b_\beta)) \cdots (q(z_1)\, q(z_2) \cdots q(z_\zeta))$

of the same cycle type (:= the list of cycle sizes).

Hence p, p' are conjugate in S_n $\iff$ they have the same cycle type

e.g. $p = (18)(36)(2475)$

and $p' = (74)(2381)(65)$

are conjugate in S_8, by $p' = qpq^{-1}$ where $q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 6 & 3 & 1 & 5 & 8 & 4 \end{pmatrix}$

proof of proposition: Since $p(a_j) = a_{j+1}$ as $p = (\cdots a_j\, a_{j+1} \cdots)\cdots$

$$qpq^{-1}(q(a_j)) = qp(a_j)$$
$$= q(a_{j+1}) \quad \text{i.e. } qpq^{-1} = (\cdots q(a_j)\, q(a_{j+1}) \cdots)\cdots \quad \blacksquare$$

e.g. for S_4 one has...

cycle types	$C(h)$	$Z(h)$
$(\cdot)(\cdot)(\cdot)(\cdot)$	$\{e\}$	$Z(e) = S_4$
$(\cdot\cdot)(\cdot)(\cdot)$	$\{(12),(13),(14),(23),(24),(34)\}$	$Z((12)) = \langle (12),(34)\rangle = \{e,(12),(34),(12)(34)\}$
$(\cdot\cdot\cdot)(\cdot)$	$\{(123),(132),(124),(142),(134),(143),(234),(243)\}$	$Z((123)) = \langle (123)\rangle = \{e,(123),(132)\}$
$(\cdot\cdot)(\cdot\cdot)$	$\{(12)(34),(13)(24),(14)(23)\}$	$Z((12)(34)) = \{e,(12)(34),(13)(24),(14)(23),(12),(34),(1324),(1423)\} \cong D_4$
$(\cdot\cdot\cdot\cdot)$	$\{(1234),(1243),(1324),(1342),(1423),(1432)\}$	$Z((1234)) = \langle (1234)\rangle = \{e,(1234),(13)(24),(1432)\}$

So the class equation for S_4 is

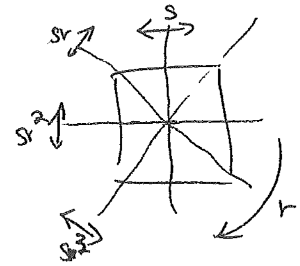
$$\underset{\overset{\shortparallel}{4!}}{24} = 1 + 6 + 8 + 3 + 6$$
$$= \frac{4!}{4!} + \frac{4!}{4} + \frac{4!}{3} + \frac{4!}{8} + \frac{4!}{4}$$

DEF'N: The center $Z(G) = \{g \in G : \underset{\text{i.e. } ghg^{-1} = h}{gh = hg} \ \forall g \in G\} = \bigcap_{h \in G} Z(h)$

(= the kernel K for the action of G on itself by conjugation)

So $Z(G) = \{g \in G : \underset{\text{or } |C(g)|=1}{C(g) = \{g\}}\} \Rightarrow |Z(G)| = \#$ ones in the class equation for G

EXAMPLE: $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$



has $Z(G) = \{e, r^2\}$

and conjugacy classes
$\{e\}$
$\{r, \underset{r^{-1}}{\underset{\shortparallel}{r^3}}\}$ since $srs^{-1} = srs = r^3 = r^{-1}$
$\{r^2\}$
$\{s, sr^2\}$ since $rsr^{-1} = sr^3r^{-1} = sr^2$
$\{sr, sr^3\}$

and class equation $\underset{|D_4|}{\underset{\shortparallel}{8}} = \underbrace{\underset{\{e\}}{1} + 2 + \underset{\{r^2\}}{1}}_{Z(D_4)} + 2 + 2$

§7.3 p-Groups

The class equation has an interesting consequence for **p-groups** G, defined to be groups G with $|G| = p^k$ a prime power, $k \geq 1$.

10/26/2018 >

PROPOSITION: A p-group G always has center $Z(G) \neq \{1\}$,
(PROP 7.3.1) i.e. a nontrivial subgroup

proof: Assume for the sake of contradiction that G has $|G| = p^k$ and trivial center $Z(G) = \{1\}$. Then its class equation looks like

$$p^k = |G| = \sum_{\substack{\text{Conjugacy}\\ \text{class } C(h)}} |C(h)| = 1 + \sum_{\substack{\text{Conj.}\\ \text{classes } C(h) \neq \{1\}}} |C(h)|$$

p^k: equals 0 mod p (since $k \geq 1$)

1: equals 1 mod p

$|C(h)|$: equals 0 mod p since $|C(h)| = \frac{|G|}{|Z(h)|} = \frac{p^k}{p^{k'}} = p^{k-k'}$, $1 \neq p^{k'}$ as $h \notin Z(G)$

$1 + \sum |C(h)|$: equals 1 mod p

CONTRADICTION

∎