Groups acting by conjugation

Recall that a group G acts on itself by conjugation as follows:

$$g \cdot a = gag^{-1} \quad \forall\, g, a \in G.$$

This satisfies the axioms for a group action:

$1 \cdot a = 1a1^{-1} = a$, and

$(gh) \cdot a = (gh)a(gh)^{-1} = ghah^{-1}g^{-1} = g \cdot (h \cdot a)$.

Def: Elements $a, b \in G$ are <u>conjugate</u> if $\exists\, g$ s.t. $b = gag^{-1}$, i.e. if they are in the same orbit under the conjugation action. The orbits in this case are called the <u>conjugacy classes</u> of G.

Ex: If $a \in Z(G)$, then a is the only element in its conjugacy class. If $a \notin Z(G)$, then there is some g s.t. $gag^{-1} \neq a$, so there are at least two elements in its conjucacy class.

Note: If G is nontrivial, the action of conjugation can't be transitive, since the conjugacy class of 1 is always just $\{1\}$.

We can also act on subsets of G by conjugation:

Recall that $\mathcal{P}(G) := \{ S \mid S \subseteq G \}$ is the <u>power set</u> of G, i.e. the set of all subsets of G.

Define an action on $\mathcal{P}(G)$ by

$$g \cdot S = gSg^{-1} = \{gsg^{-1} \mid s \in S, g \in G\}.$$

Again, it's straightforward to check that this is in fact a group action.

We say that two subsets S and T are conjugate if $\exists$ $g \in G$ s.t. $T = gSg^{-1}$!

Recall that if G acts on A, and $a \in A$, we showed that the number of elts in its orbit will be equal to $|G : G_a|$, i.e. the index of its stabilizer in G.

In the case where G acts on its power set by conjugation, and $S \subseteq G$, $G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$.

When G acts on itself by conjugation, and $h \in G$,
$G_h = \{g \in G \mid ghg^{-1} = h\} = C_G(S)$.

That is,

Prop: The number of conjugates of a subset $S \subseteq G$ is the index of the normalizer of S, $|G : N_G(S)|$.

In particular, the number of conjugates of an element $s \in G$. is $|G : C_G(s)|$.

We know that the orbits of an action partition the set being acted on, so in particular, if we add up the # of elements in all the orbits, we get the following:

<u>Thm</u>: (The Class equation) Let G be a finite group, and $g_1, g_2, \dots, g_r$ representatives of the distinct conjugacy classes not contained in the center of G. Then

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

<u>Pf</u>: Each orbit in the center has exactly one element. If the other orbits are $K_1, \dots, K_r$ and g_i a representative from K_i, then $|K_i| = |G : C_G(g_i)|$.

Since the orbits partition G, summing up their cardinalities gives us the desired equation. $\square$

<u>Ex</u>: In D_8, the center is $\{1, r^2\}$.

The centralizer of r contains $\langle r \rangle$, so it has order ≥ 4. Thus, $|G : C_G(r)| \leq \frac{8}{4} = 2$. But $srs = r^3$, so its conjugacy class is $\{r, r^3\}$.

$C_G(s) = \{1, s, r^2, sr^2\}$, so $|G : C_G(s)| = 2$, and $rsr^{-1} = sr^2$, so its conj. class is $\{s, sr^2\}$.

Note that the two remaining elts are conjugate: $r(sr)r^{-1} = sr^3$, so $\{sr, sr^3\}$ is the final conjugacy class.

Note that all of the summands in the class group divide the order of the group. This helps us classify some finite groups.

Theorem: If p is prime, and G is a group of order p^α, some $\alpha \geq 1$, then G has nontrivial center.

Pf: Let $g_1, \ldots, g_r$ be representatives from the conjugacy classes not contained in the center (if there are any).

Then for each g_i, its conjugacy class has at least 2 elements, so $1 < |G : C_G(g_i)|$, and Lagrange's Thm says that the index must divide p^α. Thus, for each g_i, $p \,\big|\, |G : C_G(g_i)|$.

The class equation says that

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

Thus $p \,\big|\, |Z(g)|$, so $Z(G)$ is not trivial. $\square$

Cor: If $|G| = p^2$ for some prime p, then G is abelian, and

G is cyclic or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Pf: $|Z(G)| = p$ or p^2 by the above. Thus $|G/Z(G)| = 1$ or p, so it's cyclic. Thus, by a HW problem, G is abelian.

The nontrivial elements of G have orders p or p^2. If G has any element of order p^2, then G is cyclic. Thus, assume all nontrivial elements have order p.

Let $x \in G$ s.t. $x \neq 1$. Then $|x| = p$, so we can find $y \in G - \langle x \rangle$.

Then $\langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Define $\varphi : \langle x \rangle \times \langle y \rangle \to G$ by $(x^a, y^b) \longmapsto x^a y^b$. It is straightforward to check this is a homomorphism.

If $(x^a, y^b) \in \ker \varphi$, then $x^a y^b = 1 \Rightarrow x^a = y^{-b} \in \langle x \rangle \cap \langle y \rangle$. But $\langle x \rangle \cap \langle y \rangle \lneq \langle x \rangle$, and the order divides p, so $a = b = 0$.

Thus, $\ker \varphi = 1$, so φ is injective. Both groups have the same order, so it must also be a bijection and thus an isomorphism. $\square$

Conjugacy in S_n

How can you tell based on the cycle decomposition of an element of S_n which elements are in its conjugacy class?

Consider a cycle $\sigma = (a_1 \dots a_m)$, and $\tau \in S_n$.

Then what is $\tau\sigma\tau^{-1}$?

If $k \in \{1, \dots, n\}$, then $\tau\sigma\tau^{-1}(\tau(k)) = \tau(\sigma(k))$. We have 2 cases:

Case 1: $k \neq a_i$ for any i (i.e. k doesn't appear in the cycle σ).

Then $\tau\sigma\tau^{-1}(\tau(k)) = \tau(k)$, so $\tau(k)$ doesn't appear in the cycle decomposition of $\tau\sigma\tau^{-1}$!

Case 2: $k = a_i$, then $\tau\sigma\tau^{-1}(\tau(a_i)) = \tau\sigma(a_i) = \tau(a_{i+1})$

That is, σ sends a_i to $a_{i+1} \iff \tau\sigma\tau^{-1}$ sends $\tau(a_i)$ to $\tau(a_{i+1})$

So $\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2) \dots \tau(a_m))$.

This leads to the following theorem:

Theorem: If $\sigma \in S_n$ has cycle decomposition

$$\sigma = (a_1 \dots a_m)(a_{m+1} \dots) \dots (\dots a_k)$$

then $\tau\sigma\tau^{-1}$ has cycle decomp. $(\tau(a_1)\tau(a_2) \dots \tau(a_m)) \dots (\dots \tau(a_k))$.

Pf: $\tau\sigma\tau^{-1} = \tau(a_1 \dots a_m)\tau^{-1}\tau(a_{m+1} \dots)\tau^{-1}\tau \dots \tau^{-1}\tau(\dots a_k)\tau^{-1}$,

so the cycle decomposition follows from above discussion.

Note that the cycles are disjoint since τ is a bijection:

$$a_i \neq a_j \iff \tau(a_i) \neq \tau(a_j). \quad \square$$

Thus, two elements of S_n can only be conjugate if their cycle decompositions have the same # of cycles of each length. In fact the converse holds!

Theorem: $\sigma = (a_1 \cdots a_{m_1})(a_{m_1+1} \cdots a_{m_2}) \cdots (\cdots a_{m_k})$ is conjugate to $\sigma' = (b_1 \cdots b_{m_1})(b_{m_1+1} \cdots b_{m_2}) \cdots (\cdots b_{m_k})$.

Pf: Let τ be the bijection sending each a_i to b_i and every other element to itself. Then $\tau \sigma \tau^{-1} = \sigma'$! $\square$

Ex: S_4 has 5 conjugacy classes, w/ representatives $1, (1\,2), (1\,2\,3), (1\,2\,3\,4), (1\,2)(3\,4)$, respectively.