6.3 Action of $G \curvearrowright G$ by left multiplication

Recall that we can define an action of G on $S = G$ itself by left multiplication:

$$\mu : G \times G \to G$$
$$(g, x) \mapsto gx.$$

In other words, we are putting group multiplication into the framework of a group action.
This action is both transitive and free:

- (Transitive) It suffices to show that there is just one orbit, so we will show that every $g \in G$ is in the orbit of the identity. Indeed, $\mu(g, 1) = g \cdot 1 = g$.
- (Free) If $gx = x$, then by cancellation we have $g = 1$.

Observation 6.28. For any group action $G \curvearrowright S$, we can view the map

$$G \times S \to S$$
$$(g, s) \mapsto g * s$$

satisfying the identity and associativity axioms equivalently as a map

$$G \to \mathrm{Perm}(S)$$
$$g \mapsto [g* : S \to S]$$

where $\mathrm{Perm}(S)$ is the group of permutations of the elements of S. (For example, $\mathrm{Perm}(\{1, 2, \ldots, n\})S_n$; this is the more general construction.)

We can view the action $G \curvearrowright G$ by left multiplication as a map

$$G \to \mathrm{Perm}(G)$$
$$g \mapsto m_g$$

where m_g is "multiply by g on the left", i.e. $m_g(h) = gh$.

- This map is an injective group homomorphism: $m_g(x) = x$ for all $x \in G$ iff $g = 1$. In other words, this action is *faithful*. But we already knew this, since we showed that the action was in fact *free*. See Remark 6.8.

Using this action, can prove that every finite group lives inside a symmetric group S_n; this is another reason why it's so important to understand symmetric groups.

Theorem 6.29 (Cayley's Theorem)**.** Every finite group G is isomorphic to a subgroup of some symmetric group S_n.

Proof. Let $n = |G|$. Then $\mathrm{Perm}(G) \cong S_n$. The homomorphism $\varphi : G \to \mathrm{Perm}(G) \cong S_n$ is injective, so $G \cong \mathrm{img}(\varphi)$. □

Note that it's an entirely different question to ask for the *smallest* n such that $G \hookrightarrow S_n$.

6.4 Action of $G \curvearrowright G$ by conjugation

We can define a different action of G on itself by conjugation; this will tell us more about the structure of the group.

The action of G on itself by conjugation is given by $(g, x) \mapsto gxg^{-1}$. In this section, we will write $g * x := gxg^{-1}$ to emphasize the action.

Definition 6.30. Let $x \in G$. The **centralizer** of x, denoted $Z(x)$, is the stabilizer of x under the conjugation action $G \curvearrowright G$:

$$Z(x) = \{g \in G \mid gxg^{-1} = x\}.$$

These are precisely the elements of G that commute with x.

Exercise 6.31. Prove that $Z(G)$ is a subgroup of G.

Remark 6.32. Recall that the **center** $Z(G)$ of a group G is the set of elements that commute with *all* $x \in G$. Therefore $Z(G) = \bigcap_{x \in G} Z(x)$.

If G is abelian, then for all $x \in G$, $Z(x) = G$. (And $Z(G) = G$.)

Definition 6.33. The **conjugacy class** of $x \in G$ is the orbit of x under the conjugation action of $G \curvearrowright G$.

We will write $C(x)$ for the conjugacy class of x, though I don't believe there is standard notation for this. Here are some immediate observations:

- The Counting Formula tells us that

$$|G| = |G_x||O_x| = |Z(x)||C(x)|$$

- For any $x \in G$, $\langle x \rangle \subseteq Z(x)$.
- $Z(G) \leq Z(x)$
- An element $x \in G$ is in $Z(G)$ iff $Z(x) = G$ iff $C(x) = \{x\}$. Think through this.

Definition 6.34. For a finite group G, the **class equation of** G is the equation describing how the group G is decomposed into conjugacy classes:

$$|G| = \sum_{\text{conj. classes } C} |C| = |C_1| + |C_2| + \ldots + |C_k|.$$

By convention, we let $C_1 = C(1) = \{1\}$ (the conjugacy class of the identity element).

Some more quick observations:

- For all $x \in Z(G)$, $C(x) = \{x\}$, so there will be $|Z(G)|$ ones in the class equation for G.
- For every conjugacy class C_i, by the counting formula we know $|C_i| \mid |G|$.

Example 6.35. The class equation of $S_3 \cong D_3$ is $6 = 1 + 2 + 3$, because

$$S_3 = \{1\} \cup \{(123), (132)\} \cup \{(12), (23), (13)\}.$$

Observe that since A_3 is a *normal* subgroup of S_3, it must be a union of conjugacy classes. Indeed, A_3 is the union of the first two conjugacy classes shown above.

Exercise 6.36. Determine the class equation of $D_4 = \langle \rho, \tau \mid \rho^4 = \tau^2 = \rho\tau\rho\tau = 1 \rangle$. Solution: Instead of directly computing conjugacy classes, you can instead compute the size of centralizers; this way, you can use the counting formula to know when you've found all the elements in the conjugacy class. For example, consider ρ. We know $\rho \notin Z(D_4)$ since $\tau\rho\tau = \rho^{-1}$ (i.e. ρ^{-1} is in the conjugacy class of ρ). Then $Z(\rho) = \langle \rho \rangle$, which contains 4 elements. So $|C(\rho) = 2$. This means we've already found the entire conjugacy class of ρ: $C(\rho) = \{\rho, \rho^{-1}\}$. There are many different ways to arrive at the final answer, which is that $8 = 1+1+2+2+2$.