1 Group Presentations

We start out with an important (somewhat trivial) fact:

Fact. *Every group is the quotient of a free group.*

If G is a group, then we can surject

$$\begin{aligned} F(G) &\twoheadrightarrow G \\ g_1g_2g_3 &\longmapsto g_1 \times g_2 \times g_3. \end{aligned}$$

This sucks. We can do better. Often times, there exists a smaller set $A \subseteq G$ such that

$$\begin{aligned} F(A) &\twoheadrightarrow G \\ a &\longmapsto a \\ a_1a_2a_3 &\longmapsto a_1 \times a_2 \times a_3. \end{aligned}$$

If this is a surjection, A is a set of generators, and if A is finite, then G is *finitely generated.* Now let

$$R \longrightarrow F(A) \longrightarrow\!\!\!\!\!\rightarrow G$$

Be exact at $F(A)$, then R is a *normal* subgroup.

So let $\mathcal{R}$ be the set of words such that $\langle\langle \mathcal{R} \rangle\rangle$

So we define $B \subseteq G$ to be

$$\begin{aligned} \langle\langle B \rangle\rangle_G &:= \bigcap N : N \trianglelefteq G \text{ and } B \subseteq N \\ \langle\langle \mathcal{R} \rangle\rangle &= \text{The smallest normal subgroup that contains } \mathcal{R}. \end{aligned}$$

Example 1.1. Okay, so, like, don't worry about the fact that we haven't defined presentations yet.

$$D_{10} = \left\langle r, s \;\middle|\; r^5 = 1, s^2 = 1, sr = r^4 s \right\rangle$$

Being the dihedral group on 10 elements, and

$$\langle\langle r^5, s^2, srsr \rangle\rangle \longrightarrow F(r, s) \longrightarrow\!\!\!\!\!\rightarrow D_{10}$$

Definition 1.2. G has a presentation

$$\langle A \mid \mathcal{R} \rangle$$

if $F(A) \twoheadrightarrow G$ is a surjection and $\langle\langle \mathcal{R} \rangle\rangle_{F(A)}$ is the kernel.

If the kernel $\langle\langle \mathcal{R} \rangle\rangle$ is written with $\mathcal{R}$ a finite list of words and A is finite, then $G = \langle A \mid \mathcal{R} \rangle$

If p is prime and $|G| = p$, what is G? $\exists x : x^p = 1$, and $G = \langle x | x^p = 1 \rangle = \mathbb{Z}/p\mathbb{Z}$

Theorem 1.3 (Cauchy's Theorem.). *If $p \mid |G|$ and p is prime, then there exists an element of order p in G.*

2 Group Actions

Let A be a set, and G be a group. Then take a homomorphism $G \to \mathrm{Aut}(A)$. Every group is a subgroup of a permutaton gp. G acts on G by left multiplication.

Definition 2.1. $G \curvearrowright A$ is *transitive* if $\forall a, b \in A$, $\exists g \in G$ such that $g(a) = b$.

Example 2.2. $G \curvearrowright G$ by conjugation is **not** a transitive action... especially clear in abelian groups. Notice that $gag^{-1} = a$ in any abelian group, so the action is not transitive.

Definition 2.3. The *orbit* of $a \in A$ under G is the set

$$O_G(a) = \{ga \mid g \in G\} \subseteq A.$$

Orbits partition the set A.

Definition 2.4. The *stabilizer subgroup* of $a \in A$ is

$$\mathrm{Stab}_G(a) = \{g \in G \mid g(a) = a\} \leq G.$$

We make a brief return to categories to make a few statements.

Let G be a group, call sets with a group action G-sets. Then consider the category whose objects are (ρ, A), $\rho : G \times A \to A$ such that

$$\begin{tikzcd}
G \times A_1 \arrow[r, "(\mathrm{Id},\varphi)"] \arrow[d, "\rho_1"] & G \times A_2 \arrow[d, "\rho_2"] \\
A_1 \arrow[r, "\varphi"] & A_2
\end{tikzcd}$$

commutes. Such a φ is called a G-equivariant function if $\forall g \in G$, $g\varphi(a) = \varphi(ga)$.

Two G sets are called isomorphic if there is an equivariant bijection.

Proposition 2.5. *Every transitive left action of G on a set is isomorphic to*

$$\rho G \times G/H \to G/H$$
$$\rho(g_1, g_2H) = g_1 g_2 H,$$

Where H is the stabilizer of any $a \in A$.

Proof. $G \curvearrowright A$ transitively. $H = \text{Stab}_G(a)$.
Then let

$$\varphi : G/\text{Stab}(a) \to A$$
$$\varphi : gH \to ga.$$

We claim that φ is a G-equivariant bijection, but first that it is well defined.
Suppose that $g_1H = g_2H$. then $g_2^{-1}g_1H = H$, so $g_2^{-1}g_1 \in H = \text{Stab}(a)$.
Then $g_2(a) = g_2(g_2^{-1}g_1a) = g_1a$. △
Then we aught show it's a bijection.
Well $a' \in A \Rightarrow a' = ga$ for some $g \in G$ by the action of G being transitive. so take

$$a' \longrightarrow gH.$$

if $a' = g_1a$ and $a' = g_2a$, then

$$g_1a = g_2a \Rightarrow g_2^{-1}g_1(a) = a$$
$$g_2^{-1}g_1 \in H = \text{Stab}(a)$$
$$g_1H = g_2H.$$

△

Then also φ is equivariant by definition. Namely

$$\varphi(g'gH) = g'g(a)$$
$$g'\varphi(gH) = g'(ga) = g'ga.$$

□

Now we introduce a thoerem that is incredibly useful for counting things in groups.

Corollary 2.6 (The Orbit-Stabilizer Theorem)**.** *Let $G \curvearrowright A$.*
If O_a is the orbit of $a \in A$, then

$$|O_a| \cdot |\text{Stab}_G(a)| = |G|$$

Corollary 2.7. *$|O_a|$ divides $|G|$*

Proof. G acts transitibely on O_a for any a by definition. So

$$|G/\text{Stab}_G(a)| = |O|$$

Notice that the left hand side is the number of left cosets. In other words,

$$|O_a| = [G : \text{Stab}_G(a)]$$

so

$$|O_a| \cdot |\mathrm{Stab}_G(a)| = |G|$$

$\square$

Now we introduce a small theorem that is not so difficult to prove.

Theorem 2.8. *If $G \curvearrowright A$, $g(a) = b$, then*

$$\mathrm{Stab}_G(b) = g\mathrm{Stab}_G(a)g^{-1}.$$

In other words

Proof. **Admitted.** I dunno, just work this diagram and work by conjugation. You should be able to track elements via conjugatoin to get both containments.

$$\begin{tikzcd} a \arrow[loop left] \arrow[r, bend left, "g"] & b \arrow[loop right] \end{tikzcd}$$

$\square$

Therefore, these stabilizers are the same size.

Proposition 2.9. *Let S be a finite set, $G \curvearrowright S$. Then*

$$|S| = \sum_{a \in A} [G : G_a], \quad G_a = \mathrm{Stab}(a)$$

Where A contains exactly one element from from each orbit.

Proof. The orbits partition S.

$$|S| = \sum_{a \in A} |O|, \quad |G| = |O| \cdot |\mathrm{Stab}(a)|$$

Now let's pull out the things with one orbit.

$$\begin{aligned} Z = \text{Number of elements with one on element in it's orbit} \\ Z = \{a \mid [G : G_a] = 1\}. \\ |S| = |Z| + \sum_{a \in A} [G : G_a] \end{aligned}$$

Where A has one element from each non-trivial orbit. When the action is conjugation...

Let $Z(G)$ denote the center of G, namely

$$\begin{aligned} Z(G) = \{g \in G : ga = ag \ \forall a \in G\} \\ Z(a) = \{g \in G \mid ga = ag\} \end{aligned}$$

Then the center is a subgroup.

$$|G| = |Z(G)| + \sum_{a \in A-1} [G : Z(a)]$$

Where A contains exactly one element from each nontrivial orbit. $\square$

In particular,

$$|G| = \sum a_i \quad \text{where each } a_i \mid |G|$$

Example 2.10. When $|G| = 6$, we only have the options $6 = 6$, and $6 = 1 + 2 + 3$, and in particular, $p = p$ where p is prime.