Week 3

Types of Subgroups and Group Functions

3.1 Subgroups and Generators

10/10:

- Defining **subgroups**.
  - Let $G = (G, *)$ be a group, and let $H \subseteq G$ be a subset.
  - What properties do we want H to satisfy to consider it a "subgroup?"
    - H should inherit the binary operation from G.
    - H should be closed under multiplication using said binary operation.
    - H should be nonempty.
    - H should contain the inverses of every element — this is automatic if G is finite since the inverse of an element g of order n is g^{n-1} and $g^{n-1} \in H$ by closure under multiplication.
    - H should also be associative; we also inherit this for free from G.
- Easy way to construct a subgroup.
  - Let G be a group, and let $x_1, x_2, \dots \in G$. We can let $H = \langle x_1, x_2, \dots \rangle$, i.e., H is the group **generated** by $x_1, x_2, \dots$. In other words, H is the set of all finite products $x_1, x_1^{-1}, x_2, x_2^{-1}, \dots$.
  - This construction does give you all possible subgroups, but when you write it down, it's very hard to say what group you get.
- Example: If you have $H \subset G$ a subgroup, then $H = \langle h|_{h \in H} \rangle$.
- **Cyclic** (group): A group G for which there exists $g \in G$ such that $G = \langle g \rangle$.
- Examples:
  - If $1 < n < \infty$, then $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$.
  - However, the generator isn't always unique — $\mathbb{Z}/7\mathbb{Z} = \langle 3 \rangle$.
  - If G is generated by an element, it's also generated by its inverse. For example, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- Proposition: Let G be a cyclic group. It follows that
  1. If $|G| = \infty$, then G is isomorphic to $\mathbb{Z}$;
  2. If $|G| = n < \infty$, then G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Proof. Assertion 1: Let $G = \langle g \rangle$. Then

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}$$

Now suppose for the sake of contradiction that $g^a = g^b$ for some $a, b \in \mathbb{Z}$. Then $g^{a-b} = e$, so $|G| \leq a-b$, a contradiction. Therefore, $G = \{G^{\mathbb{Z}}\}$. In particular, we may define $\phi : \mathbb{Z} \to G$ by $k \mapsto g^k$. This map has the property that $a + b \mapsto g^a g^b$, i.e., $\phi(a)\phi(b) = \phi(ab)$[1].

Assertion 2: Let $G = \langle g \rangle$. Then

$$G = \{e, g, g^2, \dots, g^{n-1}\}$$

Now suppose for the sake of contradiction that $g^a = g^b$. Then $g^{a-b} = e$, so $|G| \leq a - b < n$, a contradiction. Therefore, we may once again define $\phi : \mathbb{Z}/n\mathbb{Z} \to G$ as above. Note that $a + b \mapsto g^{(a+b) \mod n}$. This is still a homomorphism, though. □

- Claim: Any subgroup of a cyclic group is also cyclic.
- Example: $G = \mathbb{Z}$, $H = \langle 2002, 686 \rangle$.
  - $H = \{2002x + 686y \mid x, y \in \mathbb{Z}\}$.
  - To say that H is cyclic is to say that it is equal to the integer multiples of some $d \in \mathbb{Z}$, i.e., there exists d such that $G = \{zd \mid z \in \mathbb{Z}\}$.
  - We can take $d = \gcd(2002, 686)$.
  - (Nonconstructive) proof: Let d be the smallest positive integer in H. Suppose for the sake of contradiction that $md + k$ is in the group for some $1 \leq k < d$. Then adding $-d$ m times, we get that $k \in H$, a contradiction since we assumed d was the smallest positive integer in H.
- Let $G = \langle x, y \rangle$ be a group that is generated by two elements. Find a subgroup $H \subset G$ such that H *must* be generated by more than 2 elements.
  - Let's work with $S_n = \langle (1, 2, \dots, n), (1, 2) \rangle$.
  - The subgroup $H = \langle (1, 2), (3, 4), (5, 6) \rangle$ will work.
    - $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
    - Suppose $H = \langle a, b \rangle$. We can get e, a, b, ab. But because everything commutes, we can rearrange any product to $a^i b^j$ and cancel.
- When you want to answer questions like, "Is $\mathbb{Z}/180180\mathbb{Z}$ a subgroup of S_n for some n," you need some more information on the structure of S_n.
- Group **presentations** allow us to describe a group really easily. Seems useful at first but isn't really.

3.2 Blog Post: Subgroups

From Calegari (2022).

10/24:

- Relevant section from Dummit and Foote (2004): 2.1.
- **Subgroup**: A subset H of a group G for which the binary operation $\cdot$ on G restricts to a binary operation (which we can also call $\cdot$) on H and $(H, \cdot)$ is a group.
- Lemma: $H \subset G$ iff the following three conditions are satisfied.
  1. H is nonempty.
  2. H is closed under multiplication, that is, if $x, y \in H$, then $x \cdot y \in H$.
  3. H has inverses, that is, if $x \in H$, then $x^{-1} \in H$.

  Proof. Calegari gives a totally rigorous proof of this. □
- Rigorous definitions of the notation x^n as well as proving that the usual properties of exponents hold.

[1] We all know that this is a **homomorphism**; Calegari just doesn't want to call it that yet.

3.3 Homomorphisms

10/12:

- We've studied groups a lot at this point. But as with vector spaces, we don't have a complete theory of groups until we consider maps between them.
- Today: Homomorphisms.
- Let H, G be groups.
- What qualities do we want a map of groups to have?
  - Maps between vector spaces preserve linearity, so maps between groups should probably preserve the group operation.
  - Bijection? As with linear maps, the bijective case is interesting, but we don't want to be this restrictive.
  - In fact, that first quality is the only one we want.
- **Homomorphism**: A map $\phi : H \to G$ of sets such that $\phi(x *_H y) = \phi(x) *_G \phi(y)$.
- Lemma: Let $\phi : H \to G$ be a homomorphism. Then...
  1. $\phi(e_H) = e_G$.
  2. $\phi(x^{-1}) = \phi(x)^{-1}$.

  Proof. Claim 1:

  $$\begin{aligned} e_G\phi(x) = \phi(x) &= \phi(xe_H) = \phi(x)\phi(e_H) \\ e_G &= \phi(e_H) \end{aligned}$$

  Claim 2:

  $$e_G = \phi(e_H) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

  □

- **Image** (of ϕ): The subset of G such that for all $h \in H$, $\phi(h) = g$. *Denoted by* $\textbf{im}\,\boldsymbol{\phi}$.
- **Kernel** (of ϕ): The subset of H containing all $h \in H$ such that $\phi(h) = e_G$. *Denoted by* $\textbf{ker}\,\boldsymbol{\phi}$.
- Lemma:
  1. $\operatorname{im}\phi \subset G$ is a subgroup.
  2. $\ker\phi \subset H$ is a subgroup.

  Proof. Claim 1: We know that $\phi(e_H) = e_G$, so

  $$\operatorname{im}\phi \neq \emptyset$$

  as desired. Next, let $g_1, g_2 \in \operatorname{im}\phi$. Suppose $g_1 = \phi(h_1)$ and $g_2 = \phi(h_2)$. Then since H is closed under multiplication as a subgroup, $h_1h_2 \in H$. It follows that

  $$g_1g_2 = \phi(h_1)\phi(h_2) = \phi(h_1h_2) \in \operatorname{im}\phi$$

  as desired. Lastly, let $g \in \operatorname{im}\phi$. Suppose $g = \phi(h)$. Then since H is closed under inverses as a subgroup, $h^{-1} \in H$. It follows that

  $$g^{-1} = \phi(h)^{-1} = \phi(h^{-1}) \in \operatorname{im}\phi$$

  as desired.

Claim 2: We know that $\phi(e_H) = e_G$, so

$$\ker\phi \neq \emptyset$$

as desired. Next, let $g_1, g_2 \in \ker\phi$. Then

$$e_G = e_G e_G = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$$

so $g_1 g_2 \in \ker\phi$, as desired. Lastly, let $g \in \ker\phi$. Then

$$e_G = \phi(e_H) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = e_G\phi(g^{-1}) = \phi(g^{-1})$$

□

- Examples:

H	G	ϕ	$\operatorname{im}\phi$	$\ker\phi$
H	G	$\phi(h) = e$	$\{e\}$	H
$H \leq G$	G	inclusion	H	$\{e\}$
$\mathbb{Z}$	$\mathbb{Z}/n\mathbb{Z}$	$k \mapsto k \mod n$	$\mathbb{Z}/n\mathbb{Z}$	$n\mathbb{Z}$
$\mathrm{O}(n)$	$\mathbb{R}^*$	det	$\{\pm 1\}$	$\mathrm{SO}(n)$
$\mathrm{GL}_n\mathbb{R}$	$\mathbb{R}^*$	det	$\mathbb{R}^*$	$\mathrm{SL}_n\mathbb{R}$

Table 3.1: Examples of images and kernels.

  - The first example shows that there is always at least one homomorphism between two groups.
  - $\mathbb{R}^*$ is the group of nonzero real numbers with multiplication as the group operation.
  - The $\mathrm{O}(n)$ example expresses the fact that $\det(AB) = \det(A)\det(B)$, i.e., that the determinant is a homomorphism.
    - The kernel is $\mathrm{SO}(n)$ since 1 is the multiplicative identity of $\mathbb{R}^*$ and all matrices in $\mathrm{SO}(n) \subset \mathrm{O}(n)$ get mapped to 1 by the determinant.
  - $\mathrm{GL}_n\mathbb{R}$ is the set of all $n \times n$ invertible matrices over the field $\mathbb{R}$.

- **Isomorphism**: A bijective homomorphism from $H \to G$.
  - If an isomorphism exists between H and G, we say, "H is isomorphic to G."

- Lemma: H is isomorphic to G implies G is isomorphic to H.

Proof. $\phi : H \to G$ a bijection implies the existence of $\phi^{-1} : G \to H$. Claim: This is an isomorphism. We can formalize the notion, or just think of ϕ as relabeling elements of H and ϕ^{-1} as unrelabeling them. □

- Lemma: A homomorphism $\phi : H \to G$ is **injective** iff $\ker\phi = \{e_H\}$.

Proof. Suppose ϕ is injective. We know that $\phi(e_H) = e_G$ from a previous lemma; this implies that $e_H \in \ker\phi$. Now let $x \in \ker\phi$ be arbitrary. Then $\phi(x) = e_G = \phi(e_H)$. But since ϕ is injective, we have that $x = e_H$. Thus, we have proven that $e_H \in \ker\phi$, and any $x \in \ker\phi$ is equal to e_H; hence, we know that $\ker\phi = \{e_H\}$, as desired.

Now suppose that $\ker\phi = \{e_H\}$. Let $\phi(x) = \phi(y)$. It follows that

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = \phi(x)\phi(x)^{-1} = e_G$$

But this implies that

$$xy^{-1} = e_H$$
$$x = y$$

as desired. □

- Problem: Is there a surjective homomorphism $\phi : S_5 \to S_4$?
  - Proposal 1: Send 5-cycles to the identity and everything else to itself.
  - Proposal 2: "Drop 5" $(1,2)(3,4,5) \mapsto (1,2)(3,4)$.
    - Counterexample: $(1,2,3,4,5) \mapsto (1,2,3,4)$.
  - Proposal 3: If it doesn't do something to everything, send it to e.
- Lemma: Let $\phi : H \mapsto G$ be a homomorphism. If $|h| = n$, then $|\phi(h)|$ divides n, i.e., n is a multiple of $|\phi(h)|$.

  Proof. If $h^n = e$, then $\phi(h^n) = e = \phi(h)^n$. □
- Equipped with this lemma, let's return to the previous problem.
  - Suppose for the sake of contradiction that such a surjective homomorphism ϕ exists.
  - Consider a 5-cycle $h \in S_5$; obviously, $|h| = 5$.
  - It follows by the lemma that $\phi(h) \in S_4$ has order which divides 5. But since the maximum order of an element in S_4 is 4, this means that $|\phi(h)| = 1$, so $\phi(h) = e$.
- If one 5-cycle maps to the identity, then all of their products must, too.
- What can map to an order 3 element in S_4?
- If $\psi(g) = (1,2,3)$, then $|g|$ is divisible by 3.
- In fact, no surjective map exists!
- In order for homomorphisms to exist, there must be some reason. If there aren't any (nontrivial ones), proving this can be easy.
- Now consider $S_4 \mapsto S_3$.
  - 4-cycles to e or 2-cycles.
  - 3-cycles to 3-cycles.
- Idea: $S_4 \cong \text{Cu} \cong S_3$.
  - 3 pairs of opposite faces and 4 diagonals.

3.4 Blog Post: Homomorphisms and Isomorphisms

From Calegari (2022).

10/24:

- Relevant section from Dummit and Foote (2004): 1.7.
- Additional homomorphism examples:
  - Let Cu be the cube group. Then the action of this group on vertices, faces, edges, diagonals, and pairs of opposite faces gives homomorphisms $\psi : \text{Cu} \to S_n$ for $n = 8, 6, 12, 4, 3$, respectively.
  - Let $G = \mathbb{Z}/6\mathbb{Z}$ and $H = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $\psi : G \to H$ sending $n \mod 6 \mapsto (n \mod 2, n \mod 3)$ is a homomorphism.
- Lemma: If $\psi : G \to H$ is an injection, then $\tilde{\psi} : G \to \text{im}(\psi)$ is an isomorphism.

3.5 Cosets

10/14:

- Asking, "what's the intuition for this question?" in OH.
  - Calegari: Intuition is borne of experience. You get intuition from grubby computations, and then you finally recognize the structure. If you don't know what's going on, it's good to struggle. Start with the simplest possible example and then struggle until you develop intuition.
- Last time, we discussed the fact that there is no surjective homomorphism from $S_5 \to S_4$, but there is a surjective homomoprhism from $S_4 \to S_3$. How about the case $S_{n+1} \to S_n$ for arbitrary n?
- Teaser theorem: Let $n > m$ and $\phi : S_n \twoheadrightarrow S_m$. Then
  1. $m = 1$.
  2. $m = 2$.
  3. $m = 3$.
- Think about the problem of maps from $G \to \Gamma$, where Γ is another group. What we know:
  - Let $K = \ker \phi$. Recall that ϕ is injective iff $\ker \phi = \{e\}$. But there is some additional structure: If $\phi(g) = x$, then $\phi(gK) = x$ where $gK = \{gk \in G \mid k \in K\}$. Another way of phrasing this: If $\phi(g') = x$, then $g' = gk$ for some $k \in K$.
  - This motivates the following definition.
- **Left coset**: The set defined as follows, where $g \in G$ and H is a subgroup of G. *Denoted by* $\boldsymbol{gH}$. *Given by*

$$gH = \{gh \mid h \in H\}$$

  - You can define cosets for H a subset (not a subgroup) of G, but we will not be interested in these cases.
- Claim: Let $x, y \in G$ be arbitrary. Then either $xH \cap yH = \emptyset$ or $xH = yH$.
- Example: $G = S_3$, $H = \langle e, (1,2) \rangle$.

g	gH
e	$\{e, (1,2)\}$
$(1,2)$	$\{e, (1,2)\}$
$(1,3)$	$\{(1,3), (1,2,3)\}$
$(1,2,3)$	$\{(1,3), (1,2,3)\}$
$(2,3)$	$\{(2,3), (1,3,2)\}$
$(1,3,2)$	$\{(2,3), (1,3,2)\}$

Table 3.2: Cosets of $\langle e, (1,2) \rangle$ in S_3.

  - Observations: Cosets are pairwise disjoint. $x \in gH$ implies $xH = gH$.
- $\boldsymbol{G/H}$: The set of all left cosets of H in G.
- Proposition:
  1. Any two cosets in G/H are either (i) the same or (ii) disjoint.
  2. All $g \in G$ lie in a unique coset (in particular, gH).
  3. $|gH| = |H|$.

Proof. Claim 1: Let $C_1, C_2 \in G/H$. We divide into two cases ($C_1 \cap C_2 = \emptyset$ and $C_1 \cap C_2 \neq \emptyset$). In the first case, C_1, C_2 are disjoint, as desired. In the latter case, they are not disjoint, so we need to prove that they are the same. Suppose $g \in C_1 \cap C_2$. Let $C_1 = \gamma H$. We will prove that $gH = \gamma H$ via a bidirectional inclusion argument. It will follow by similar logic that $gH = C_2$, from which transitivity will imply that $C_1 = gH = C_2$, as desired. Let's begin. Let $x \in gH$. Then $x = gh$ for some $h \in H$. Additionally, we know that $g \in \gamma H$ by hypothesis, so $g = \gamma h'$ for some $h' \in H$. It follows by combining the last two equations that $x = \gamma h'h$. But since $h'h \in H$, $x \in \gamma H$ as desired. A symmetric argument works in the other direction.

Claim 2: We know that $g \in gH$ since $e \in H$ and $g = ge$. Additionally, if $g \in \gamma H$, we have by part (1) that $\gamma H = gH$, so g does lie in a *unique* coset.

Claim 3: Suppose there exist $h, h' \in H$ such that $gh = gh'$. Then $h = h'$ by the cancellation lemma. Thus, every distinct $h \in H$ induces a distinct $gh \in gH$. Therefore, $|gH| = |H|$, as desired. □

- Notice that so far, general statements we've made about groups have been very easy to prove; it's only in particular instances that things become tricky.
- Decomposition of a group into equivalence classes: Cosets and conjugacy both do this.
- Corollary: Let H be a subgroup of G. Then

$$|G| = |G/H| \cdot |H|$$

Proof. Sketch: Partition G into cosets, each of order $|H|$. But there are $|G/H|$ of these. Thus, the number of elements in G is $|G/H| \cdot |H|$. □

- **Index** (of H in G): The number of cosets into which H partitions G. *Denoted by* $\boldsymbol{[G : H]}$. *Given by*

$$[G : H] = |G/H|$$

- If $|G| < \infty$, then $[G : H] = |G|/|H|$. If $|G| = \infty$, then we can still define the concept $|G/H|$, but we don't have a nice formula for it.
- Example: Let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$ (i.e., H is the set of even integers).
  - Then the orbits are all even and all odd numbers. The index of H in G is 2.
- Theorem (Lagrange):
  1. Let G be a finite group, $H \subset G$. Then $|H|$ divides $|G|$.
  2. Let G be a finite group. Let $g \in G$. Then $|g|$ divides $|G|$.
- Example: Let p be prime. If $|G| = p$, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. Take $g \in G$ such that $g \neq e$. By Lagrange's theorem, $|g|$ divides p. But this means that $|g| = 1$ or $|g| = p$. But it's not the first case because $g \neq e$. Thus, $G = \langle g \rangle \cong \mathbb{Z}/p\mathbb{Z}$, as desired. □

- **Right coset**: The set defined as follows, where $g \in G$ and H is a subgroup of G. *Denoted by* $\boldsymbol{Hg}$. *Given by*

$$Hg = \{hg \mid h \in H\}$$

- $\boldsymbol{H/G}$: The set of all right cosets of H in G.
- The theories of left and right cosets are very similar, but they are not entirely equivalent.
  - For example, $H = \langle e, (1,2) \rangle$ implies

$$(1,3)H = \{(1,3), (1,2,3)\} \qquad H(1,3) = \{(1,3), (1,3,2)\}$$

3.6 Blog Post: Dihedral Groups

From Calegari (2022).

10/24:

- Moving on from the cube group as a subset of SO(3), we can talk about 2-dimensions.
- In 2-dimensions, we choose to admit both rotations and reflections of a given geometric object.
  - This is because reflections in 2D are equal to rotations in 3D. Mathematically, there is a homomorphism $\psi : \mathrm{O}(2) \to \mathrm{SO}(3)$ given by

$$A \mapsto \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{A}} & 0 \\ & & 0 \\ \hline 0 & 0 & \det(A) \end{array}\right)$$

- **Dihedral group**: The subgroup of O(2) consisting of elements which preserve the regular n-gon ($n \geq 3$) centered at the origin. *Denoted by* $\boldsymbol{D_{2n}}$.
- We can study $D_{2n} \subset S_n$ by labeling the vertices of the n-gon from 1 through n.
  - Similarly to in the cube group, any two nonopposite vertices are linearly independent, and the transformation is uniquely determined by any two such vertices.
  - In particular, we can move vertex 1 anywhere we want (say m), but then since vertex 2 must remain a neighbor, it can either move to $m \pm 1$ (addition modulo n).
  - Thus, we get an injective homomorphism from $D_{2n} \to S_n$.
- We can write down the elements of D_{2n} explicitly in terms of S_n. For example...
  - A rotation r of $2\pi/n$ is sent to $(1, 2, \dots, n)$.
  - A reflection s through the edge connecting 1 and n is sent to $(1, n)(2, n-1)(3, n-2)\cdots$.
    - Note that depending on whether n is odd or even (i.e., depending on the **parity** of n), s may or may not (respectively) fix one vertex.
- We can easily write out all of the elements of D_{2n} and the multiplication table; this is rather rare.
- Lemma: The elements of D_{2n} are as follows.
  1. The powers of r, given by $e, r, r^2, \dots, r^{n-1}$.
  2. The elements $s, sr, sr^2, \dots, sr^{n-1}$.

  The multiplication table is given by

$$\begin{aligned} r^i \cdot r^j &= r^{i+j} \\ sr^i \cdot r^j &= sr^{i+j} \\ r^i \cdot sr^j &= sr^{-i+j} \\ sr^i \cdot sr^j &= r^{-i+j} \end{aligned}$$

- All rotations are distinct.
- All elements sr^i are distinct: If $sr^i = r^j$, then $s = r^{j-i}$, but r is a reflection not a rotation.
- To check the multiplication table, we use the identity

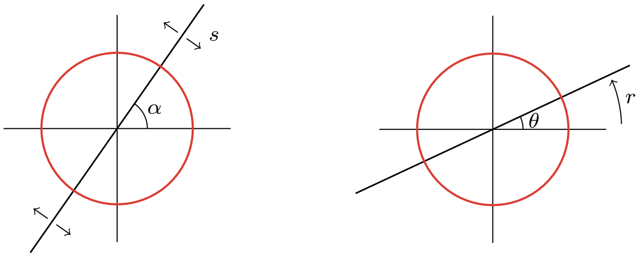
$$rs = sr^{-1}$$

  - This identity has the alternate form

$$srs = s^{-1}rs = r^{-1}$$

    since s has order 2.

- Claim: The above identity is true for any rotation and reflection.



(a) Reflection.

(b) Rotation.

Figure 3.1: Commuting rotations and reflections.

Proof. Let's consider the plane to be the complex plane, and represent points on the unit circle using the complex numbers $z = \mathrm{e}^{i\gamma}$. In this case, we have that

$$s : \mathrm{e}^{i\gamma} \mapsto \mathrm{e}^{i(2\alpha-\gamma)} \qquad r : \mathrm{e}^{i\gamma} \mapsto \mathrm{e}^{i(\gamma+\theta)} \qquad r^{-1} : \mathrm{e}^{i\gamma} \mapsto \mathrm{e}^{i(\gamma-\theta)}$$

It follows that for any $\mathrm{e}^{i\gamma}$ on the unit circle,

$$[srs](\mathrm{e}^{i\gamma}) = [sr](\mathrm{e}^{i(2\alpha-\gamma)}) = s(\mathrm{e}^{i(2\alpha-\gamma+\theta)}) = \mathrm{e}^{i(2\alpha-(2\alpha-\gamma+\theta))} = \mathrm{e}^{i(\gamma-\theta)} = r^{-1}(\mathrm{e}^{i\gamma})$$

meaning that

$$srs = r^{-1}$$

as desired. □

- The identity $r^i \cdot sr^j = sr^{-i+j}$ follows inductively.
- Lemma: The conjugacy classes of D_{2n} are as follows.
  1. The identity.
  2. If $n = 2m$, the element r^m.
  3. For all other $0 < m < n$, the pair $\{r^m, r^{-m}\}$.
  4. If n is odd, then all reflections are conjugate.
  5. If $n = 2m$, then the reflections divide into two conjugacy classes of size m, consisting of elements of the form sr^{2i} and sr^{2i+1}, respectively.

Proof. Consider the rotation r^i and, more specifically, gr^ig^{-1} for $g \in D_{2n}$. We divide into two cases. If g is a rotation, then it commutes with r^i. Thus,

$$gr^ig^{-1} = r^igg^{-1} = r^i$$

If g is a reflection, then since the inverse of a reflection is itself and $r^{j+i}s = sr^{-i-j}$, we have that

$$gr^ig^{-1} = sr^jr^i(sr^j)^{-1} = sr^{j+i}sr^j = ssr^{-i-j}r^j = r^{-i}$$

Therefore, the only elements in the conjugacy class of r^i are r^i and r^{-i}. This validates claims 1-3, above.

Now consider the reflection sr^i and, more specifically, gsr^ig^{-1} for $g \in D_{2n}$. Once again, we divide into two cases. If g is a rotation, then

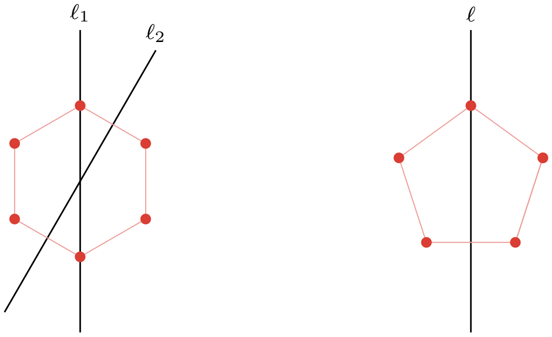
$$gsr^ig^{-1} = r^jsr^ir^{-j} = sr^{-j}r^ir^{-j} = sr^{i-2j}$$

If g is a reflection, then since $sr^is = r^{-i}$ as proven above, we have that

$$gsr^ig^{-1} = sr^jsr^isr^j = sr^j(sr^is)r^j = sr^jr^{-i}r^j = sr^{2j-i}$$

Therefore, either way, sr^i is only conjugate to reflections with the same parity of a power of a rotation. If n is odd, then we will be able to get to all reflections using different values of j, but if n is even, then we will only be able to get to half at a time. This validates claims 4-5, above. □

- Geometric intuition for the relation between the reflection conjugacy classes and n.



(a) n even. (b) n odd.

Figure 3.2: Reflection conjugacy classes for n even or odd.

  - If n is even, there are two "flavors" of reflection: Those in which the line of reflection passes through two opposite vertices (e.g., ℓ_1 in Figure 3.2a), and those in which the line of reflection passes through the midpoints of two opposite edges (e.g., ℓ_2 in Figure 3.2a).
  - If n is odd, all lines of reflection pass through one vertex and through the middle of the opposite edge (e.g., ℓ in Figure 3.2b).

3.7 Blog Post: Cosets and Lagrange's Theorem

From Calegari (2022).

10/24:

- **Left coset**: The following subset of G, where $g \in G$ and H is a subgroup of G. *Denoted by* $\boldsymbol{gH}$, $[\boldsymbol{g}]$. *Given by*

$$[g] = gH = \{gh \mid h \in H\}$$

- Additional coset examples:
  - If $H = G$, then $[g] = gH = G$ for any $g \in G$.
  - If $H = \{e\}$, then $[g] = gH = \{e\}$ for any $g \in G$.
  - If $G = \mathbb{Z}$ and $H = 10\mathbb{Z}$, then

$$[7] = \{\dots, -13, -3, 7, 17, 27, 37, 47, \dots\} = [17] = [-3]$$

    for instance.
- Calegari does want us to attempt to prove the claims in the blog by ourselves.

- Calegari offers two proofs of the fact claim that either $xH \cap yH = \emptyset$ or $xH = yH$.
- Lemma: If $g \in G$ is arbitrary, then there is a bijection between H and gH.

  Proof. The bijection is given by $h \mapsto gh$; the fact that this is a bijection follows from the cancellation lemma. Explicitly,
  $$gh = gh' \iff h = h'$$
  and gh in the codomain is mapped to by h in the domain. □

- Theorem: There is an equality
  $$|G| = |G/H| \cdot |H|$$
  for all subgroups H of G, where when $|G| = \infty$ the above statement is interpreted to mean that at least one of the quantities on the RHS is also infinite.

  Proof. We count the elements of G in two ways. The first is to say that there are $|G|$ elements in G. The second is to say that $G = \bigcup_{g \in G} gH$. But by the previous lemma, $|gH| = |H|$ so the size of G is the product of the size of each coset $|H|$ and the number of cosets $|G/H|$. Therefore, via transitivity, we have the desired result. □