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 $x_1, x_2, \cdots \in G$. We can let $H = \langle x_1, x_2, \ldots \rangle$, i.e., H is the group **generated** by $x_1, x_2, \ldots$. In other words, H is the set of all finite products $x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots$.
  - 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* $\mathbf{im}\,\boldsymbol{\phi}$.
- **Kernel** (of ϕ): The subset of H containing all $h \in H$ such that $\phi(h) = e_G$. *Denoted by* $\mathbf{ker}\,\boldsymbol{\phi}$.
- 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

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

- **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 $(1, 2, \ldots, n)$.
  - 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 $e, r, r^2, \ldots, r^{n-1}$.
  2. The elements $s, sr, sr^2, \ldots, sr^{n-1}$.

  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

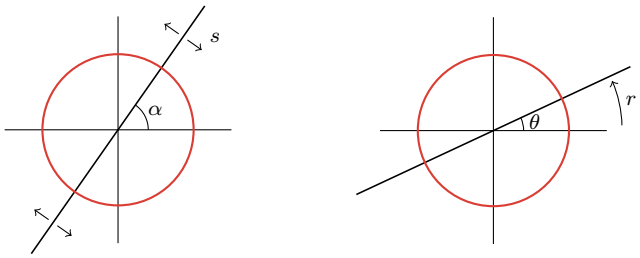
$$rs = sr^{-1}$$

– 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

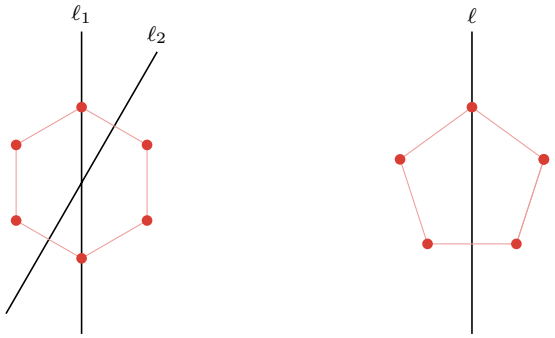
$$gsr^ig^{-1} = r^jsr^ir^{-j} = sr^{-j}r^ir^{-j} = sr^{i-2j}$$

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

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

    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. □

3.8 Chapter 1: Introduction to Groups

From Dummit and Foote (2004).

Matrix Groups

12/5:

- Used for illustrative purposes in Part I, and studied in detail with vector spaces later on.
- **Field**: A set F together with two binary operations $+$ and $\cdot$ on F such that $(F, +)$ is an abelian group with identity 0, $(F - \{0\}, \cdot)$ is an abelian group, and the following **distributive law** holds:
  $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
  for all $a, b, c \in F$.
  - The "smallest" mathematical structure in which we can perform all the arithmetic operations $+$, $-$, $\times$, and $\div$ (division by nonzero elements).
  - Fields will be studied more thoroughly later; for now, it suffices to know $\mathbb{Q}$, $\mathbb{R}$, and the finite fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime.
- $\boldsymbol{F^\times}$: The set $F - \{0\}$ where F is a field.
- Linear algebra (vector space theory, matrices and linear transformations, and determinants) over $\mathbb{R}$ is true *mutatis mutandis*[2] over an arbitrary field F.
- **General linear group of degree n**: The set of all $n \times n$ matrices, where $n \in \mathbb{Z}^+$, whose entities come from the field F and whose determinant is nonzero. *Denoted by* $\boldsymbol{GL_n(F)}$.
  - We can compute the determinant $\det(A)$ of a matrix A with entries in F using the same formulas applied when $F = \mathbb{R}$.
  - The product of two matrices A, B with entries in F is also computed by using the familiar formula.
  - $\det(AB) = \det(A) \cdot \det(B)$ implies that for $A, B \in GL_n(F)$ (i.e., $\det(A) \neq 0 \neq \det(B)$), AB will also have nonzero determinant and hence $AB \in GL_n(F)$ as well. Thus, $GL_n(F)$ is closed under matrix multiplication.

[2] Def: Making the necessary adjustments while not affecting the main point.

  - $\det(A) \neq 0$ still implies the existence of A^{-1}.
  - Compute inverses can be done with the same familiar adjoint formula.

- Useful results (proven in Part III).
  - If F is a field and $|F| < \infty$, then $|F| = p^m$ for some prime p and integer m.
  - If $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.

Exercises

The next exercise introduces the **Heisenberg group** over the field F and develops some of its basic properties. When $F = \mathbb{R}$, this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally, for example, with entries in $\mathbb{Z}$.

11. Let

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in F \right\}$$

be the **Heisenberg group** over F. Let

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \qquad\qquad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

be elements of $H(F)$.

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

The Quaternion Group

- **Quaternion group**: The group defined as follows. *Denoted by* $\boldsymbol{Q_8}$. *Given by*

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

where the product $\cdot$ is described by

$$1 \cdot a = a \cdot 1 = a \qquad \text{for all } a \in Q_8$$
$$(-1) \cdot (-1) = 1$$
$$(-1) \cdot a = a \cdot (-1) = -a \qquad \text{for all } a \in Q_8$$

$$i \cdot i = j \cdot j = k \cdot k = -1$$

$i \cdot j = k$	$j \cdot k = i$	$k \cdot i = j$
$j \cdot i = -k$	$k \cdot j = -i$	$i \cdot k = -j$

- Associativity can be tediously checked by explicit computation, or by less computational means later on.

- Q_8 is a non-abelian group of order 8.

Homomorphisms and Isomorphisms

- Goal: Quantify when two groups "look the same."
  - We say this happens when there exists an **isomorphism** between them. We'll first define a **homomorphism**, though. This latter concept we'll discuss in much greater detail later.
- **Homomorphism**: A map $\varphi : G \to H$ such that the following equality holds for all $x, y \in G$, where $(G, \star)$ and $(H, \diamond)$ are groups.
$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$$
  - Without explicit group operations, we have the form $\varphi(xy) = \varphi(x)\varphi(y)$. This form will commonly show up, but it is important to remember the distinction between group operations.
  - Intuitively, a map is a homomorphism if it "respects the group structures of its domain and codomain" (Dummit & Foote, 2004, p. 37).
- **Isomorphism**: A bijective homomorphism.
  - If an isomorphism exists from G to H, we write that G and H are **isomorphic**, are of the same **isomorphism type**, and that $\boldsymbol{G \cong H}$.
  - Intuitively, such a map implies that G and H are the same group; the elements have simply been relabeled from one to the other.
- The existence of an isomorphism between two groups implies that any property of G that can be derived from the group axioms also holds for H, and vice versa.
- Isomorphisms formally justify writing all group actions as $\cdot$ since groups $(G, \star)$ and $(G, \cdot)$ where $\star, \cdot$ are defined the same are isomorphic.
- $\cong$ is an equivalence relation.
- **Isomorphism class**: An equivalence class of a nonempty collection $\mathcal{G}$ of groups under $\cong$.
- $\exp : \mathbb{R} \to \mathbb{R}^+$ defined by $\exp(x) = \mathrm{e}^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.
  - $\mathrm{e}^{x+y} = \mathrm{e}^x \mathrm{e}^y$.
- $|\triangle| = |\Omega| \iff S_\triangle \cong S_\Omega \iff |S_\triangle| = |S_\Omega|$.
- We will define new notions of isomorphisms for other algebraic structures (e.g., rings, fields, vector spaces, etc.).
- **Classification theorem**: A theorem stating what properties of a structure specify its isomorphism type.
  - Finding classification theorems is a central problem in mathematics.
  - A general classification theorem would assert that if G is an object with some structure (such as a group) and G has property $\mathcal{P}$, then any other similarly structured object (group) X with property $\mathcal{P}$ is isomorphic to G.
- Example: Any non-abelian group of order 6 is isomorphic to S_3.
  - Utility: Allows us to obtain $D \cong S_3$ and $GL_2(\mathbb{F}_2) \cong S_3$ without having to find explicit maps between said groups.
- **Classification**: A theorem stating what properties of a structure specify that it is isomorphic to one of more than one distinct objects.
  - Less specific conclusions, but simpler property $\mathcal{P}$ to check compared to a classification theorem.
- Example: Any group of order 6 is isomorphic to S_3 or $\mathbb{Z}/6\mathbb{Z}$.

  - We don't get an isomorphism type, but we can check "$|G| = 6$" more easily than "$|G| = 6$ and non-abelian."

- Conditions that allow us to rule out two groups G, H being isomorphic: If $\varphi : G \to H$ is an isomorphism, then

  1. $|G| = |H|$.
  2. G is abelian iff H is abelian.
  3. For all $x \in G$, $|x| = |\varphi(x)|$.

- "Let G be a finite group of order n for which we have a presentation and let $S = \{s_1, \ldots, s_m\}$ be the generators. Let H be another group and $\{r_1, \ldots, r_m\}$ be elements of H. Suppose that any relation satisfied in G by the s_i is also satisfied in H when each s_i is replaced by r_i. Then there is a unique homomorphism $\varphi : G \to H$ which sends $s_i \mapsto r_i$" (Dummit & Foote, 2004, pp. 38–39).

  - If $\{r_1, \ldots, r_m\}$ generate H, then φ is surjective. If in addition $|G| = |H| < \infty$, then φ is injective, and φ is an isomorphism.
  - Intuitively, we can map the generators of G to any elements of H and obtain a homomorphism provided that the relations in G are still satisfied.

- Examples:

  - Let $k \geq 3$ be such that $k \mid n$. Then since $a^k = 1$ implies $a^n = 1$, and we can obtain a homomorphism $\varphi : D_{2n} \to D_{2k}$.
  - Mapping $r \in D_6$ to (1 2 3) $\in S_3$ and $s \in D_6$ to (1 2) $\in S_3$ yields an isomorphism.

- Corresponding statement from vector spaces: Let V, W be vector spaces and S a basis for V. Then we can specify $T : V \to W$ a linear transformation by its action on S. If $\dim W = \dim V$ and $T(S)$ spans W, then T is a vector space isomorphism.

Group Actions

- **Group action** (of a group G on a set A): A map $\cdot : G \times A \to A$ such that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and such that $1 \cdot a = a$ for all $a \in A$.

- Let G act on A, and for each $g \in G$, define $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then

  1. For each fixed $g \in G$, σ_g is a permutation of A;

     Proof. We prove that σ_g has a two-sided inverse; it follows that σ_g is a permutation by Proposition 1. Let $g \in G$ be arbitrary. Then by Axiom (iii), there exists g^{-1}. Therefore,

     $$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1} \cdot g) \cdot a \\ &= 1 \cdot a \\ &= a\end{aligned}$$

     We can prove something similar in the other direction. □

  2. The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

     Proof. Let $\varphi : G \to S_A$ be defined by $\varphi(g) = \sigma_g$ for all $g \in G$. To prove that φ is a homomorphism, it will suffice to show that $\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all $g_1, g_2 \in G$. To verify the equality

of functions, we must show that for all $a \in A$, $\varphi(g_1 \cdot g_2)(a) = (\varphi(g_1) \circ \varphi(g_2))(a)$. Let a be an arbitrary element of A. Then

$$\begin{aligned}\varphi(g_1 \cdot g_2)(a) &= \sigma_{g_1 \cdot g_2}(a) \\ &= (g_1 \cdot g_2) \cdot a \\ &= g_1 \cdot (g_2 \cdot a) \\ &= g_1 \cdot \sigma_{g_2}(a) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= (\sigma_{g_1} \circ \sigma_{g_2})(a) \\ &= (\varphi(g_1) \circ \varphi(g_2))(a)\end{aligned}$$

□

- Intuitively, a group action of G on A means that every element $g \in G$ acts as a permutation on A in a manner consistent with the group operations in G.
- **Permutation representation** (associated to the group action $\cdot$): The homomorphism $\varphi : G \to S_A$ defined by $\varphi(g)(a) = \sigma_g(a) = g \cdot a$ for all $g \in G$, $a \in A$.
- **Left** (action): A group action where the elements of G act on the elements of A from the left.
  - Group actions, as we have defined them, are left actions.
- **Right** (action): A group action where the elements of G act on the elements of A from the right.
- **Trivial action**: The group action defined by $g \cdot a = a$ for all $g \in G$, $a \in A$.
  - G is said to **act trivially** on A.
  - The associated permutation representation is the **trivial homomorphism**.
- **Trivial homomorphism**: The homomorphism $\varphi : G \to H$ sending all $g \in G$ to $1 \in H$.
- **Faithful** (group action): A group action for which distinct elements of G induce distinct permutations of A.
  - The associated permutation representation is injective.
- **Kernel** (of a group action): The set of $g \in G$ that fix all elements of A.
- Examples:
  - If V is a vector field taken over F, then scalar multiplication can be described as the action of $F^\times$ on V.
  - S_A acts on A by $\sigma \cdot a = \sigma(a)$; the associated permutation representation is the identity map from S_A to itself.
  - D_{2n} acts on $[n]$ in a manner consistent with the geometric picture. This action is faithful (since, geometrically, distinct symmetries induce distinct permutations of the vertices).
  - The **left regular action** of G on itself. This action is faithful (by the cancellation lemma).
  - Further examples appear in the exercises.
- **Left regular action** (of G on itself): The group action where $A = G$ defined by $g \cdot a = ga$, i.e., where the group operation is left multiplication within the group. *Also known as* **left translation** [when G is additive and thus $a \mapsto g + a$].

3.9 Chapter 2: Subgroups

From Dummit and Foote (2004).

Definition and Examples

- Two way of unraveling the structure of an axiomatically defined mathematical object are to study subsets of the object that satisfy the same axioms, and to study quotients (which, roughly speaking, collapse one group onto a smaller one).
  - Here, we study subgroups and quotient groups. Later, we will study subrings and quotient rings of a ring, subspaces and quotient spaces of a vector space, etc.
- **Subgroup** (of G): A nonempty subset $H \subset G$ that is closed under products and inverses. *Denoted by* $\boldsymbol{H \leq G}$.
  - In other words, we require that $x^{-1} \in H$ for all $x \in H$, and $xy \in H$ for all $x, y \in H$.
  - Alternatively, a subgroup of $(G, \cdot)$ is a subset of G that is a group in its own right under $\cdot$.
  - It is possible for a subset $H \subset G$ to have the structure of a group with respect to some operation other than the one on G (e.g., $(\mathbb{Q}, +)$ and $(\mathbb{Q} \setminus \{0\}, \times)$), but we do not refer to this subset as a *subgroup*.
  - Any equation in the elements of H may be viewed as an equation in the elements of G. Consequences:
    - Every subgroup must contain 1, the identity of G.
    - The inverse of $x \in G$ is the same as the inverse of $x \in H$, i.e., x^{-1} is indeed unambiguous notation.
- $H \leq G$ and $H \neq G$ imply $H < G$.
- Examples of groups and some of their subgroups given.
- **Trivial subgroup**: The subgroup $H = \{1\}$. *Denoted by* $\mathbf{1}$.
- $\leq$ is transitive: $K \leq H \leq G \implies K \leq G$.
- Let G be a group.

  Proposition 1 (The Subgroup Criterion)**.** A subset $H \subset G$ is a subgroup iff

  1. $H \neq \emptyset$;
  2. For all $x, y \in H$, $xy^{-1} \in H$.

  Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

  Proof. Given. □

Centralizers and Normalizers, Stabilizers and Kernels

- Goal: Introduce important families of subgroups for an arbitrary group G.
- Let A be a nonempty subset of G.
- **Centralizer** (of A in G): The set defined as follows. *Denoted by* $\boldsymbol{C_G(A)}$. *Given by*

$$C_G(A) = \{g \in G \mid gag^{-1} = a \ \forall \ a \in A\}$$

  - $C_G(A)$ is the set of all elements in G which commute with every element of A, since $gag^{-1} = a$ is an equivalent condition to $ga = ag$.
  - If $A = \{a\}$, we write $C_G(a)$ instead of $C_G(\{a\})$.
    - In this case, $a^n \in C_G(a)$ for all $n \in \mathbb{Z}$.
- $C_G(A) \leq G$.

Proof. Use the subgroup criterion (Proposition 1).

Criterion 1: Since $1a1^{-1} = 1a1 = a$ for all $a \in A$, $1 \in C_G(A)$. Thus, $C_G(A)$ is nonempty.

Criterion 2: Let $x, y \in C_G(A)$ be arbitrary. To prove that $xy^{-1} \in C_G(A)$, it will suffice to show that for all $a \in A$, $(xy^{-1})a(xy^{-1})^{-1} = a$. Let a be an arbitrary element of A. Since $x, y \in C_G(A)$, we know that $xax^{-1} = a$ and $yay^{-1} = a$. It follows from the latter condition via multiplication on the left by y^{-1} and multiplication on the right by y that $a = y^{-1}ay$. Combining the last two results, we have that

$$\begin{aligned}(xy^{-1})a(xy^{-1})^{-1} &= x(y^{-1}ay)x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

as desired. □

- Examples.
  - $C_{Q_8}(i) = \{\pm 1, \pm i\}$.
- **Center** (of G): The set defined as follows. *Denoted by* $\boldsymbol{Z(G)}$. *Given by*

$$Z(G) = \{g \in G \mid gx = xg \ \forall \ x \in G\}$$

  - Observe that $Z(G) = C_G(G)$.
  - Thus, $Z(G) \leq G$ by the above argument.
- **Normalizer** (of A in G): The set defined as follows, where $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. *Denoted by* $\boldsymbol{N_G(A)}$. *Given by*

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

  - $g \in C_G(A)$ implies $g \in N_G(A)$.
  - Thus, $C_G(A) \leq N_G(A)$.
  - We can prove $N_G(A) \leq G$ analogously to how we proved $C_G(A) \leq G$.
- Examples.
  - G abelian implies $C_G(A) = Z(G) = N_G(A) = G$ for all $A \subset G$.
  - Let $A = \{1, r, r^2, r^3\}$ be the rotational subgroup of D_8. Then $C_{D_8}(A) = A$, $N_{D_8}(A) = D_8$, and $Z(D_8) = \{1, r^2\}$.
  - Let $A = \{1, (1\ 2)\}$ be a subgroup of S_3. Then $C_{S_3}(A) = N_{S_3}(A) = A$ and $Z(S_3) = 1$.
- We deduce that the fact that the normalizer, centralizer, and center are subgroups is a special case of a more general result about group actions (this will be discussed further in Chapter 4).
- Define the following two subgroups of G for an arbitrary group action.
- **Stabilizer** (of s in G): The set defined as follows. *Denoted by* $\boldsymbol{G_s}$. *Given by*

$$G_s = \{g \in G \mid g \cdot s = s\}$$

  - $G_s \leq G$. Dummit and Foote (2004) proves this.
  - "Notice how the steps take to prove G_s is a subgroup are the same as those to prove $C_G(A) \leq G$ with axiom (1) of an action taking the place of the associative law" (Dummit & Foote, 2004, p. 51).
- **Kernel** (of the action of G on S): The set defined as follows. *Given by*

$$\{g \in G \mid g \cdot s = s \ \forall \ s \in S\}$$

  - The kernel is a subgroup of G as well.

- **Power set** (of A): The set of all subsets of A, where A is any set. *Denoted by* $\boldsymbol{\mathcal{P}(G)}$.
- Consider the action of G on $S = \mathcal{P}(G)$ by conjugation, i.e., $g \cdot B = gBg^{-1}$.
  - By definition, $N_G(A) = G_s$ where $s = A \in S$. Thus, the stabilizer being a subgroup implies that the normalizer is a subgroup of G.
- Consider the action of $N_G(A)$ on A by conjugation, i.e., $g \cdot a = gag^{-1}$.
  - By definition, $C_G(A)$ is the kernel of this action. Thus, the kernel being a subgroup implies that the centralizer is a subgroup of the normalizer, which in turn is a subgroup of G.
- Consider the action of G on $S = G$ by conjugation, i.e., $g \cdot s = gsg^{-1}$.
  - By definition, $Z(G)$ is the kernel of this action. Thus, the kernel being a subgroup implies that the center is a subgroup of G.

Cyclic Groups and Cyclic Subgroups

- One type of subgroup of G is to pick $x \in G$ and let H be the set of all integer powers of x, guaranteeing closure under inverses and products. We study groups like H in this section.
- **Cyclic** (group): A group H that can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where, as usual, the operation is multiplication).
  - Additive notation: $H = \{nx \mid n \in \mathbb{Z}\}$.
  - We write $H = \langle x \rangle$ and say "H is **generated** by x (and x is a **generator** of H)."
  - A cyclic group may have more than one generator (e.g., we have $H = \langle x \rangle = \langle x^{-1} \rangle$ since $(x^{-1})^n = x^{-n}$ and as n runs over all integers so does $-n$).
  - Cyclic groups are abelian.
- Examples:
  - Rotational subgroup of D_{2n}.
  - $(\mathbb{Z}, +)$.
- Relating the order of H and its generator x.

  Proposition 2. If $H = \langle x \rangle$, then $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically,

  1. If $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H;
  2. If $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.

  Proof. Given. □

- Important note on the above proof: The Division Algorithm is used to reduce arbitrary powers of a generator in a finite cyclic group to the "least residue" powers.
  - The use of this algorithm suggests a similarity between finite cyclic groups and groups of the form $\mathbb{Z}/n\mathbb{Z}$. Theorem 4 will formalize this notion, noting that a finite cyclic group H and $\mathbb{Z}/n\mathbb{Z}$ are the same up to isomorphism as long as $n = |H|$.
  - Before we can prove this, though, we need another proposition.
- Properties of $|x|$ given that $x^n = x^m = 1$.

Proposition 3. Let G be an arbitrary group, let $x \in G$, and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.

Proof. If $d = (m, n)$, then by the Euclidean Algorithm, there exist integers r, s such that $d = mr + ns$. Thus,

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1$$

as desired.

We divide into two cases for the second assertion ($m = 0$ and $m \neq 0$). If $m = 0$, then clearly $|x|$ divides $0 = m$, as desired. On the other hand, if $m \neq 0$, then we continue. Let $d = (m, |x|)$. By the first part, $x^d = 1$. By definition, $0 < d \leq |x|$. But since $|x|$ is the smallest positive integer such that $x^{|x|} = 1$, we must have $d = |x|$. Thus, by the definition of d, $d \mid m$ so $|x| \mid m$. □

- Cyclic group structure.

  Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

  1. If $n \in \mathbb{Z}$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

     $$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

     is well defined and is an isomorphism.

     Proof. To prove that φ is well defined, it will suffice to show that if $x^r = x^s$, then $\varphi(x^r) = \varphi(x^s)$. Let $x^r = x^s$. Then $x^{r-s} = 1$. Thus, by Proposition 3, $n \mid r - s$. It follows that $r - s = nt$, i.e., that $r = nt + s$ for some $t \in \mathbb{Z}$. Consequently,

     $$\varphi(x^r) = \varphi(x^{tn+s}) = y^{tn+s} = (y^n)^t y^s = y^s = \varphi(x^s)$$

     as desired.

     To prove that φ is an isomorphism, it will suffice to show that it is a homomorphism and a bijection. The following shows that φ is a homomorphism.

     $$\varphi(x^a x^b) = \varphi(x^{a+b}) = y^{a+b} = y^a y^b = \varphi(x^a)\varphi(x^b)$$

     As to proving that φ is a bijection, we have by hypothesis that $\langle x \rangle$ and $\langle y \rangle$ are finite groups of the same order, and we know that φ is a surjection since each y^k is the image of an x^k. These two facts prove that it is a bijection by Proposition 1. □

  2. If $\langle x \rangle$ is an infinite cyclic group, the map

     $$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

     is well defined and is an isomorphism.

     Proof. φ is automatically well-defined since $\mathbb{Z}$ is well-defined (i.e., there is no ambiguity in the representation of elements in the domain).

     By Proposition 2, $a \neq b$ implies $x^a \neq x^b$ for all distinct $a, b \in \mathbb{Z}$. Thus, φ is injective. By the definition of a cyclic group, φ is surjective. Thus, it is bijective. Additionally, laws of exponents prove that it is a homomorphism, as above. □

- **Cyclic group of order n**: The cyclic group of order n written multiplicatively. *Denoted by* $\boldsymbol{Z_n}$.
  - We liken Z_n more to $\langle r \rangle \leq D_{2n}$ than $\mathbb{Z}/n\mathbb{Z}$ so that we can use multiplication as the group operation.

- Up to isomorphism, Z_n is the unique cyclic group of order n.
- We will occasionally say "let $\langle x \rangle$ be the infinite cyclic group written multiplicatively," but we do not introduce any special notation for this; indeed, we always use $\mathbb{Z}$ (additively) to *represent* the infinite cyclic group.

- How to determine all generators for a given cyclic group H.

Proposition 5. Let G be a group, let $x \in G$, and let $a \in \mathbb{Z} \setminus \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$.

   Proof. Suppose for the sake of contradiction that $|x^a| = m < \infty$. Then $x^{am} = (x^a)^m = 1$ and $x^{-am} = ((x^a)^m)^{-1} = 1^{-1} = 1$. Thus, since either am or $-am$ is a positive integer (neither are 0 since $a \neq 0 \neq m$), $|x| = \pm am < \infty$, a contradiction. □

2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.

   Proof. Given. □

3. In particular, if $|x| = n < \infty$, and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$.

   Proof. Given. □

Proposition 6. Let $H = \langle x \rangle$.

1. Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ iff $a = \pm 1$.
2. Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ iff $(a, n) = 1$. In particular, the number of generators of H is $\varphi(n)$ (where φ is Euler's φ-function).

Proof. Given. □

- Example of applying Proposition 6.
  - $\varphi(12) = 4$, so we should not be surprised to find that there are four residue classes $\bar{a}$ mod n with $(a, n) = 1$: Namely, these are $\bar{1}$, $\bar{5}$, $\bar{7}$, and $\bar{11}$. Thus, these four residue classes are the generators of $\mathbb{Z}/12\mathbb{Z}$.

- Complete subgroup structure of a cyclic group.

Theorem 7. Let $H = \langle x \rangle$ be a cyclic group.

1. Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = 1$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.
2. If $|H| = \infty$, then for any distinct nonnegative integers a, b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m, so that the nontrivial subgroups of H corresponds bijectively with the integers in $\mathbb{Z}^+$.
3. If $|H| = n < \infty$, then for each positive integer a dividing n, there is a unique subgroup H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = n/a$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n.

Proof. Given. □

- Example:
  - We can use Proposition 6 and Theorem 7 to list all the subgroups of $\mathbb{Z}/n\mathbb{Z}$ for any given n. Continuing with $n = 12$, for instance, we have

  - $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \left\langle \overline{7} \right\rangle$ (order 12).
  - $\langle \bar{2} \rangle = \left\langle \overline{10} \right\rangle$ (order 6).
  - $\langle \bar{3} \rangle = \langle \bar{9} \rangle$ (order 4).
  - $\langle \bar{4} \rangle = \langle \bar{8} \rangle$ (order 3).
  - $\langle \bar{6} \rangle$ (order 2).
  - $\langle \bar{0} \rangle$ (order 1).
- The inclusions between the subgroups are given by

$$\langle \bar{a} \rangle \leq \left\langle \bar{b} \right\rangle \quad \iff \quad (b, 12) \mid (a, 12), \quad 1 \leq a, b \leq 12$$

- Example: Centralizers and normalizers of cyclic groups.