Week 3

???

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 write and describe a group really easily.
  - Seems useful at first, but isn't really that useful once you see it more.

3.2 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.

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

- **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

  $$e_G = e_Ge_G = \phi(g_1)\phi(g_2) = \phi(g_1g_2)$$

  so $g_1g_2 \in \ker\phi$, 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:
  - 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.

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 $\mathrm{O}(n)$ 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

  $$\begin{aligned} xy^{-1} &= e_H \\ x &= y \end{aligned}$$

  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.