Week 3

???

3.1 Introduction to 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

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

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

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

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 $S_n = \langle (1, 2, \ldots, n), (1, 2) \rangle$.
  - 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.

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