Section 6: Cyclic Groups

Where we ended last time (we'll prove it this time!):

Theorem 0.1. *Let G be a group and let $a \in G$. Then, $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and it is the smallest subgroup of G containing a.*

Proof. To show this is a subgroup, we check the three criteria: this is closed under the operation in G because, if $a^n \in H$ and $a^m \in H$, then $a^n a^m = a^{n+m}$ is also in H. This contains the identity element because $a^0 = e \in H$ and, for any $a^n \in H$, the inverse is $a^{-n} \in H$.

To see that this is the smallest subgroup containing a, we observe that, because H is closed under the operation in G, if $a \in H$, then all powers of a must be in H. In particular, if $a \in H$, $a^n \in H \forall n \in \mathbb{Z}$. □

Note that these subgroups do not have to be infinite: as soon as n is equal to the order of a (if the order is finite), then $a^n = e$, so we stop getting new elements.

Definition 0.2. Let G be a group and $a \in G$. Then, $\{a^n \mid n \in \mathbb{Z}\}$ is called the **cyclic subgroup of G generated by** a. We denote this by $\langle a \rangle$.

Definition 0.3. An element a of a group G **generates** G if $\langle a \rangle = G$. A group G is **cyclic** if there is some element a that generates G.

Example 0.4. $\mathbb{Z}$ is cyclic generated by 1 or -1. $\mathbb{Z}_n$ is cyclic generated by 1 or $n-1$.

Example 0.5. The group $\langle 3 \rangle \subset \mathbb{Z}$ is the group $\ldots, -3, 0, 3, 6, \ldots$: $\langle 3 \rangle = 3\mathbb{Z}$.

Example 0.6. Consider the symmetry group of a non-square rectangle. There are four elements: e do nothing, a flip across the vertical axis, b flip across the horizontal axis, and c rotate 180 degrees without flipping. These satisfy $a^2 = b^2 = c^2 = e$.

This group is called the **Klein** 4-group, denoted by V. It is isomorphic to the group $(\{1, -1, i, -i\}, \times)$. It is **not** cyclic because none of its elements are generators.

Some properties that you might already expect:

Theorem 0.7. *All cyclic groups are abelian.*

Proof. If G is cyclic, then $G = \langle a \rangle$ and the elements of G are all of the form a^n for various n. Let g_1 and g_2 be arbitrary elements of G, so $g_1 = a^n$ and $g_2 = a^m$ for some integers n, m. We must show that $g_1 g_2 = g_2 g_1$, but this is clear because

$$g_1 g_2 = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = g_2 g_1.$$

□

Theorem 0.8. *Any subgroup of a cyclic group is cyclic.*

The proof will be rather intuitive: if H is a subgroup of a cyclic choose the element $a^m \in H$ with minimal value of m, and show that this generates H. However, there is a technical detail we need to complete the proof called the **division algorithm** (or *Euclidean algorithm*).

Definition 0.9 (Division Algorithm)**.** If m is a positive integer and n is any integer, there exist unique integers q and r such that

$$n = mq + r$$

such that $0 \leq r < m$. We say q is the *quotient* and r is the *remainder*. This is called the division algorithm because it says

$$\frac{n}{m} = q + \frac{r}{m}.$$

Example 0.10. Find the quotient and remainder when 38 is divided by 7. Find the quotient and remainder when -38 is divided by 7. Answer: 5, 3 and $-6, 4$.