MATH 3311, FALL 2025: LECTURE 6, SEPTEMBER 8

Video: `https://youtu.be/iNN3AeOVgGk`

Definition 1. A group G is **cyclic** if there exists $g \in G$ such that

$$G = \{g^n : \ n \in \mathbb{Z}\}.$$

In this case, we say that g is **generator** for the cyclic group G or that g **generates** G.

In Homework 2, you will show the following:

Fact 1. $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are cyclic.

Fact 2. Every cyclic group is isomorphic to either $\mathbb{Z}$ (if infinite) or to $\mathbb{Z}/n\mathbb{Z}$ (if finite of order n).

Definition 2. A group G is **abelian** if for all $g, h \in G$, we have $g * h = h * g$.

Observation 1. Every cyclic group is abelian.

Proof. This just amounts to seeing that $g^n * g^m = g^{n+m} = g^{m+n} = g^m * g^n$. □

The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$

In Homework 1, you checked using Bezout's lemma that, when p is a prime, the set $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ of non-zero bins mod-p is a group under multiplication. The main point is that every non-zero bin admits a multiplicative inverse, which is a translation of the fact that, for $p \nmid a$, we can find integers s and t such that

$$1 = \gcd(a, p) = sa + tp.$$

This ensures that sa is in the same bin as 1 mod-p and so s functions as the multiplicative inverse for a mod-p.

Suppose that we replace p with any integer n (not necessarily prime). Then the same reasoning works *as long as* $\gcd(a, n) = 1$. In other words:

Fact 3. When $\gcd(a, n) = 1$, the bin of a mod-n admits a multiplicative inverse. Therefore, the set

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \ \gcd(a, n) = 1\}$$

forms a group under multiplication.

Example 1. One really has to discard all the elements *not* relatively prime to n to get multiplicative invertibility. If, for instance, we work with $n = 4$, then the non-zero entries in $\mathbb{Z}/4\mathbb{Z}$ are represented by $1, 2, 3$. Recall the multiplication table for these elements:

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Note that the second row and column have two features you wouldn't want in a group: Repetitions and an entry from *outside* the set being considered, in this case, the element 0. If we threw away 2 however (note that 2 is not relatively prime to 4), the remaining elements $1, 3$ do give a multiplicative group of order 2.

Example 2. Consider the group $(\mathbb{Z}/8\mathbb{Z})^\times$. This is a group of order 4. However, note that we have

$$3^2 = 5^2 = 7^2 = 1 \in (\mathbb{Z}/8\mathbb{Z})^\times.$$

It turns out that we can set up an isomorphism of groups

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\simeq} (\mathbb{Z}/8\mathbb{Z})^\times$$
$$(1,1) \mapsto 1$$
$$(1,0) \mapsto 3$$
$$(0,1) \mapsto 5$$
$$(1,0) \mapsto 7$$

Here, the left hand side is a *direct product*, which we will see next.

Definition 3. Given groups G and H, their **direct product** $G \times H$ is the group whose underlying set is the Cartesian product $G \times H$ of sets equipped with the structure of a group as follows:

- The operation is $(g_1, h_1) * (g_2, h_2) = (g_1 * g_2, h_1 * h_2)$.
- The identity is (e_G, e_H).
- Inverses are given by $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Observation 2. The direct product of abelian groups is also abelian.

This is because you can check the condition for being abelian in each co-ordinate separately.

Example 3. If $n, m \in \mathbb{Z}$, then we can consider the direct product $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$: this is an *abelian* group of order nm by the previous observation. The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is therefore abelian of order 4, but it is *not* cyclic, because every element in it is its own inverse, and so its multiples can never give the whole group.

Dihedral groups

Definition 4. The **dihedral group** D_{2n} is the group consisting of the *rigid* symmetries of the regular n-gon: These consist of the rotations through multiples of $2\pi/n$, as well as reflections across medians. It is a finite group of order $2n$: There are n rotations (through each multiple of $2\pi/n$) and n reflections (across each of the medians).

Example 4. Let us look at the case where $n = 3$, which gives us a group of order 6 that you already considered in homework 2.

We have two particular elements of D_6: σ, which is rotation counterclockwise by $\frac{2\pi}{3}$; and τ, which is reflection across the median through the vertex 1. We see that τ fixes the vertex 1 and switches vertices 2 and 3.

Consider $\sigma \circ \tau$: you can check that this fixes the vertex 3 and switches vertices 1 and 2. Therefore, it is reflection across the median through the vertex 3.

Similarly, $\tau \circ \sigma$ is reflection across the median through the vertex 2. In particular, we have $\sigma \circ \tau \neq \tau \circ \sigma$, which shows that D_6 is *non-abelian*.

Now, we also have σ^2, which is rotation counterclockwise by $\frac{4\pi}{3}$. It satisfies:

$$\sigma^2 : 1 \mapsto 3 \mapsto 2 \mapsto 1.$$

You can now check that $\sigma^2 \circ \tau$ fixes the vertex 2 and switches 1 and 3. In other words, it is equal to $\tau \circ \sigma$.

So we can write down every element of D_6 in terms of σ and τ:

- We have the three rotations e, σ, σ^2 (the first being the trivial rotation).
- We have the three reflections $\tau, \sigma \circ \tau, \sigma^2 \circ \tau$.

What happens when we compose them? We have to use the equality $\tau \circ \sigma = \sigma^2 \circ \tau$ to get back an element in the form above. For instance, we have

$$(\sigma^2 \circ \tau) \circ \sigma = \sigma^2 \circ (\tau \circ \sigma) = \sigma^2 \circ (\sigma^2 \circ \tau) = \sigma^4 \circ \tau = \sigma \circ \tau.$$

Here, in the last equality I'm using the fact that $\sigma^3 = e$.