MATH 3311, FALL 2025: LECTURE 8, SEPTEMBER 12

Video: `https://youtu.be/PuCQG9xYc5A`
Recall what being a subgroup means:

Definition 1. A subset $H \subset G$ of a group G is a **subgroup** if the following conditions hold:
(1) (Closure under operation) If $h_1, h_2 \in H$, then $h_1 * h_2 \in H$.
(2) (Identity) $e \in H$.
(3) (Closure under inverse) If $h \in H$, then $h^{-1} \in H$

We denote this by writing $H \leq G$.

Example 1 (Trivial subgroup). For any group G, $\{e\} \leq G$ is a subgroup. This is the **trivial** subgroup.

Example 2. Again, for any group G, $G \leq G$ is a subgroup.

Usually, we'll be interested in subgroups that are not one of these examples: That is, we'll want to look at *non-trivial*, *proper* (that is, $\neq G$) subgroups.

Example 3 (Cyclic subgroups). For any element $g \in G$, the subset $\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \leq G$ is a subgroup, and is called the **cyclic subgroup generated** by g.

Definition 2. If G is a group, then an element $g \in G$ has **finite order** if there exists some $m \in \mathbb{Z}\backslash\{0\}$ such that $g^m = e$. In this case, the **order of** g, denoted $|g|$, is the smallest $m \geq 1$ such that $g^m = e$.

Observation 1. For $g \in G$, the cyclic subgroup $\langle g \rangle \leq G$ is finite if and only if g has finite order. In this case, we have $|\langle g \rangle| = |g|$: that is, the order of a cyclic subgroup (which is a notion of *size*) is equal to the order of its generator (which is a notion involving the group operation).

Example 4. By order considerations, $D_{2n} \leq S_n$ is a proper non-trivial subgroup for $n \geq 4$.

Example 5. The subset $\{0, 1, \ldots, n-1\} \subset \mathbb{Z}$ with mod n addition is not a subgroup, even though it is a group in its own right. The problem here is that the operation on $\mathbb{Z}$ does not agree with the one on the subset: $1 + (n-1)$ is 0 with mod n addition, but is $n \in \mathbb{Z}$ if we think of them as integers. Note for instance that, in $\mathbb{Z}/4\mathbb{Z}$, every element goes to 0 when multiplied by 4, while in $\mathbb{Z}$, *no* non-zero element has this property.

Example 6. Consider the subgroup $\langle 3 \rangle \leq \mathbb{Z}/6\mathbb{Z}$: Since $2 \cdot 3 = 0$, 3 has order 2 here, and so this is a subgroup of order 2. By Homework 2, it has to be isomorphic to $\mathbb{Z}/2\mathbb{Z}$. In other words, we have a subgroup of $\mathbb{Z}/6\mathbb{Z}$ *isomorphic* to $\mathbb{Z}/2/\mathbb{Z}$. However, the naïve subset $\{0, 1\} \subset \mathbb{Z}/6\mathbb{Z}$ is *not* a subgroup.

Group actions

Definition 3. A **group action** or simply **action** of a group G on a set X is a group homomorphism

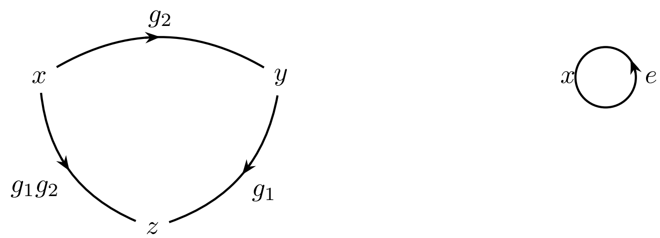
$$\rho : G \to \mathrm{Bij}(X).$$

We will use the notation $G \curvearrowright X$ (read 'G acting on X') to denote that we have an action of G on X.

While this is a very compact definition, it packs a lot of information! To see this, define a function

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto \rho(g)(x) = g \cdot x. \end{aligned}$$

Then this function has several properties that fall out of the homomorphism condition, which we see in the following picture, where, for fixed $x \in X$, we view every element $g \in G$ as being a path from x to $g \cdot x$.



(1) For all $x \in X$, $g_1, g_2 \in G$, $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.[1] This is because we have
$$(g_1 g_2) \cdot x = \rho(g_1 g_2)(x) = (\rho(g_1) \circ \rho(g_2))(x) = \rho(g_1)(\rho(g_2)(x)) = g_1 \cdot (g_2 \cdot x).$$
Here, we have used the homomorphism property $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$.

(2) For all $x \in X$, $e \cdot x = \rho(e)(x) = \mathrm{Id}(x) = x$. This is because $\rho(e) = \mathrm{Id}$.

[1] From now on, we will, like in high school algebra, use concatenation of symbols (like gh) instead of bringing in the group operation every time (like $g * h$). This doesn't imply that the group operation is necessarily multiplication: For instance, it could be composition of functions, or it could be addition in a group like $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$.