**MATH 3311, FALL 2025: LECTURE 12, SEPTEMBER 22**

Video: `https://youtu.be/yTUTPX3aK8A`
Cosets

**Definition 1.** Given a subgroup $H \leq G$ and $g \in G$, the **left coset** for $g$ with respect to $H$ is the subset

$$gH = \{gh : \; h \in H\}.$$

*Remark* 1. There is an action of $H$ on $G$ by *right* multiplication, given by $h \cdot g = gh^{-1}$. The introduction of the inverse here is to ensure that associativity works as expected: $(h_1h_2) \cdot g = g(h_1h_2)^{-1} = gh_2^{-1}h_1^{-1} = h_1 \cdot (h_2 \cdot g)$. The left cosets of $H$ are precisely the *orbits* in $G$ for this action.

This remark combined with general facts about orbits tells us:

**Fact 1.** $G$ is a *disjoint* union of left cosets for $H$: $G = \bigsqcup_{\text{distinct cosets } gH} gH$.

**Fact 2.** If $G$ is finite, then $|G| = \sum_{\text{distinct cosets } gH} |gH| = m \cdot |H|$, where $m$ is the number of distinct cosets for $H$ in $G$.

**Definition 2.** We will set $G/H$ to be the set of left cosets of $H$ in $G$: Equivalently, this is the set of orbits for the right multiplication action of $H$ on $G$.

We can reinterpret Fact 2 now as follows:

**Proposition 1** (Lagrange's theorem)**.** *Suppose that we have a subgroup $H \leq G$ of a finite group $G$. Then:*

*(1) $|G| = |G/H| \cdot |H|$, where $|G/H|$.*
*(2) In particular, $|H|$ is a divisor of $|G|$.*
*(3) For any element $g \in G$, $|g| = |\langle g \rangle|$ is a divisor of $|G|$.*

*Remark* 2. Point (3) above tells you that the order of an element of finite group $G$ has to divide $|G|$. We've already used this a few times, but now we have shown it rigorously via the theory of group actions, orbits and cosets.

*Remark* 3. Note that the *converse* to point (3) is not always true: If a number $d$ divides $|G|$, it is not necessary for there to exist an element of order $d$ in $G$. However, *Cauchy's theorem*, shown on the homework, tells us that this is true if $d$ is a *prime* number.

**Definition 3.** A subgroup $H \leq G$ has **finite index** if $G/H$ is a finite set. In this case, we set $[G : H] = |G/H|$.

*Example* 1. Any subgroup of a finite group has finite index, but infinite groups can also have subgroups of finite index: $d\mathbb{Z} \leq \mathbb{Z}$ for $d \neq 0$ is an example. In fact, one can check that, in this case $\mathbb{Z}/d\mathbb{Z}$ as a set of cosets for $d\mathbb{Z}$ in $\mathbb{Z}$ is the *same* as our original definition for $\mathbb{Z}/d\mathbb{Z}$ in terms of congruence mod-$d$. We will see this more carefully next time, but the point is that being in the same coset for $d\mathbb{Z}$ is the *same* as having the same remainder under division by $d$.