LECTURE 20
(Monday Nov. 18, 2019)
**Reminder**: $(\mathbb{Z}, +)$ additive group. Fix $N > 0$. For $a, b \in \mathbb{Z}$,

$$a \equiv b \ (\text{mod } N) \iff b - a \in N \mathbb{Z}.$$ 

gives equivalence relation on $\mathbb{Z}$, whose classes are residue classes:

$$[a] = \{ b \in \mathbb{Z} : b \equiv a \ (\text{mod } N) \} = \{ a + Nq : q \in \mathbb{Z} \} = a + N \mathbb{Z}.$$ 

Partition $\mathbb{Z}$ into $N$ "boxes of numbers"

$$\mathbb{Z}_N = \{ [0], [1], \ldots, [N-1] \} \quad (\text{has addition & multiplication}).$$

Also,

$$[a] = [b] \iff a \equiv b \ (\text{mod } N).$$

--- **Goal** is to generalize this to any group $G$ with a subgroup $H \leq G$.

(above: $G = \mathbb{Z}$ and $H = N \mathbb{Z}$)
Def. For $a, b \in G$,

$$a \sim b \iff a^{-1} \ast b \in H.$$ 

This defines an equivalence relation on $G$:

1. Reflexive: $a \sim a$
   (indeed $a^{-1} \ast a = e \in H$)

2. Symmetric: $a \sim b \implies b \sim a$
   (knowing $a^{-1} \ast b \in H$ implies its inverse lies in $H$:
   $$(a^{-1} \ast b)^{-1} = b^{-1} \ast a$$)

3. Transitive: $a \sim b$ and $b \sim c \implies a \sim c$.
   (we're assuming $a^{-1} \ast b \in H$ and $b^{-1} \ast c \in H$.
   Since $H$ is closed under $\ast$, their composition still lies in $H$:
   $$(a^{-1} \ast b) \ast (b^{-1} \ast c) = a^{-1} \ast c.$$)

Def. The equivalence class of $a \in G$ is the subset

$$[a] = \{ b \in G : b \sim a \}$$

$$= \{ a \ast h : h \in H \}$$

$$= a \ast H$$

Note: $[e] = e \ast H = H$.

This is known as the (left) **coset** containing $a$. 
Remark: \( a \equiv b \iff a \ast b^{-1} \in H \)
also def. an equivalence relation on \( G \), with classes
\[ [a] = \{ h \ast a : h \in H \} = H \ast a \]
- the right coset containing \( a \).
- Usually we take left cosets unless otherwise specified.

Lemma: For \( a, b \in G \),
(i) \([a] = [b] \iff a \sim b\).
(ii) \([a] \cap [b] \neq \emptyset \implies [a] = [b] \).

PF: Standard argument, cf. congruence \( \mod N \).
(omit)

In particular the cosets \([a]\) form a partition of \( G \).

Remark: \([a] = a \ast H\) is not a subgroup unless \( a \in H \).
\( (e \in [a] \iff a \ast e \iff a \in H) \)

Def: \( G/H = \{ a \ast H : a \in G \} \)
- family of all left cosets.
- The index of \( H \) in \( G \) is the number of cosets:

- Ex: \( \mathbb{Z}/\mathbb{Z} = \mathbb{Z}_N \)
- Equality! (not just isomorphic)
Index:

\[ [G : H] = \frac{|G|}{|H|}. \quad (\leq \infty). \]

**LAGRANGE'S Theorem:** Suppose \(|G| < \infty\).

("index formula")

Let \(H \leq G\) be any subgroup. Then \(|H|\) divides \(|G|\), and

\[ \frac{|G|}{|H|} = [G : H]. \]

Proof. First observe that all cosets have the same size, namely \(|H|\):

\[ H \rightarrow a \cdot H \]

\[ h \mapsto a \cdot h \]

is a bijection (surjective by very def. of \(a \cdot H\), injective by the cancellation law):

- Follows that the sets must have the same cardinality:

\[ |H| = |a \cdot H|. \]

Now, decompose \(G\) into (disjoint) cosets:

\[ G = a_1 \cdot H \cup a_2 \cdot H \cup \ldots \cup a_n \cdot H \]

(compare to \( \mathbb{Z} = [0] \cup [1] \cup \ldots \cup [N-1]. \))
Here \( N = \# \text{cosets} = |G/H| = [G:H] \) (index).

**Count:**

\[
|G| = \sum_{i=1}^{N} |a_i + H| = \sum_{i=1}^{N} |H| = N \cdot |H|.
\]

- verifies that 1st obs.

|H| divides |G|, and

\[
|G| = [G:H] \cdot |H|.
\]

**Ex.** \( G = \mathbb{R}^2 \) with addition. Fix \( v \neq 0 \)

\[
H = \text{span}(v) \text{ line}.
\]

For \( a \in \mathbb{R}^2 \) its coset

\[
[a] = a + \text{span}(v)
\]

is the "line, through \( a \) parallel to \( H \)."

(they partition the plane into parallel lines)