Abstract Algebra
Lecture 5 by Gross
§ Equivalence relation on a set $S$

Very important topic today
Equivalent relation $\Rightarrow$ partition means union of disjoint subsets

Defining properties:
- $a \sim a$ reflective property
- $a \sim b \Rightarrow b \sim a$ symmetric property
- $a \sim b$ and $b \sim c \Rightarrow a \sim c$ transitive property

We can also understand this as a subset of pairs $S \times S : \{(a,b): a \sim b\}$

Define $a \sim b$ if $a, b$ are in the same subset. We have disjoint subsets, everything belong to some set. Two subsets containing $a$ and $b$ with $a \sim b$ must be equal.

\[
\{S \mapsto \overline{S} = \{\text{equivalence classes in } S\} \\
a \mapsto \overline{a} = \text{the equivalence class containing } a
\]
Conversely if you have a map \( f : S \to T \), this gives an equivalence relation (or partition) on \( S \) (with \( \overline{S} = \text{Image}(f) \)): \( a \sim b \iff f(a) = f(b) \) in \( T \)

\[
\begin{array}{cccccccc}
1 & 1 & 2 & 2 & 0 & 1 & 2 \\
\leftrightarrow \end{array}
\]

\( S = \mathbb{R} \)

\[
\begin{array}{cccccccc}
-2 & -1 & 0 & 1 & 2 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\end{array}
\]

\[
f(t) = e^{2\pi it}
\]

\( T = \text{circle in } \mathbb{C} \)

\[
f^{-1}(1) = \{ \cdots, -2, -1, 0, 1, 2, \cdots \}
\]

Line \( \mathbb{R} \) moves down to a circle \( S^1 = T = \overline{S} \). This map is surjective.
A group homomorphism $f(a+b)=f(a)f(b)$ and satisfies a differential equation $f'=2\pi if$. The Homomorphism $f$ preserves not only group structure but also topological structure. Such a group is a continuous group, or Lie group.

**Example:**
Suppose $f: G \to G'$ be a group homomorphism. Let $H \leq G$ be the kernel of $f$. We get an equivalence relation on $G$, where $H$ is one of the equivalence classes. Why?

Because the definition of $H$ is $H=f^{-1}(e')=\{a \in G: f(a)=f(e)=e'\}$

**Proposition** The other equivalence classes have the form $aH=\{ah: h \in H\}$ for some $a \in G$

**Proof** Say $f(a)=f(b) \in G'$ (i.e. $a \sim b$). Then $f(a^{-1}b)=e'$ because $f$ is homomorphism and $e'=f(a)^{-1}f(b)=f(a^{-1})f(b)=f(a^{-1}b)$. Hence $a^{-1}b \in H$, i.e. $a^{-1}b=h \in H$ for some element $h$. So $b=ah$. If $b$ is equivalent to $a$, then we can write $b=ah$ for some $h \in H$.

Conversely, any element $b \in aH$ is equivalent to $a$, as by homomorphism property $f(b)=f(ah)=f(a)f(h)=f(a)e'=f(a)$.

What so good about that is the number of elements of every cosets are same.

**Fact:** The map $a \mapsto ah$ gives a bijection of sets $H \to aH$. In particular if $|H|$ is finite, then $|H|=|aH|$ for all $a$. So for a **group homomorphism**, the equivalence classes are of the form $aH$, $H=\ker f$ and have the same size.

bijection: 1-1 because if $ah=ah'$ then $h=h'$, onto, clear.
Note: This is not true for a general map of sets.

**Corollary** Assume $G$ is finite, and $f : G \to G'$ is a homomorphism with kernel $H$. Then $|G| = |\ker f| \cdot |\text{Image } f| = |H| \cdot |\text{Image } f|$

This is similar to a result in Linear algebra: If $T : V \to W$ is a linear map, then $\dim V = \dim(\ker T) + \dim(\text{Image } T)$.

**Example:** $|S_n| = n!$. For $n \geq 2$, $|A_n| = \frac{n!}{2}$.

**Proof of Corollary** Let homomorphism $f : S_n \to \{\pm 1\}$ (sign map) is surjective for $n \geq 2$ and kernel is $A_n$. $\blacksquare$

$|A_3| = 3$, $|A_4| = 12$, $|A_5| = 60$ we will study this later.

More generally, let $H \subset G$ be any subgroup (not necessarily normal). We define the (left) coset of $a \in G$ by $aH = \{ah : h \in H\}$.

**Proposition:** These subsets are disjoint and partition of $G$. Furthermore, they are in set-theoretic bijection with $H$. 
Define “the index of $H$”, which might be infinite, (denoted by $[G:H]$) as the number of distinct left cosets (i.e. equivalence classes).

**Corollary** $|G|=|H|\cdot[G:H]$

This is very famous identity

**Lagrange’s Theorem** If $|G|$ is finite, and $g \in G$, then the order of $g$ divides $|G|$, where the order of element $g$ is defined by the smallest number $m$ such that $g^m=e$.

(Example: you can’t have an element of order 3 in a group of order 4).

**Proof** Let $H=\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ where $n$ is the order of $g$. Since $|H|$ divides $|G|$ by the above corollary, the result follows.

Where is $g^{-1}$? Yeah $g^{n-1}$.

**Example** Let $G$ be a finite group with $|G|=p$ for a prime number. Then $G$ is cyclic generated by any $g \in G$ with $g \neq e$. Furthermore, the only subgroups of $G$ are $\{e\}$ and $G$.

**Proof of Example** Let $g \neq e$ in $G$. Order of $g$ divides $p$ and not 1. Since $p$ is prime, order of $g$ must be $p$ and $\langle g \rangle \subset G$. The comparison of orders, we conclude $\langle g \rangle = G$ (Finite groups of the same order are equal).
Can we show this is a strong result by exhibiting a non-cyclic group of order $p^2$ or $pq$? Yes: Klein4-group has order $2^2$ and is not cyclic.
Similarly: $S_3$ has order $6 = 2 \cdot 3$, is not abelian (and certainly not cyclic).
But all groups of order $p^2$ are abelian! (This is a beautiful result. We will see this later.)

**Definition:** A group $G$ is **simple** if its only normal subgroups $H$ are $\{e\}$ and $G$.

**Examples:** of Simple groups:
1) Any $G$ of prime order $p$ is cyclic (these are the only abelian simple groups)
2) Later we’ll see $A_n$ for $n \geq 5$
3) (Feit-Thompson theorem): Any finite non-abelian simple group has even order.

Complete list of finite simple groups is provided which is the great achievement in group theory. See you Monday.