Lecture 7: Groups, Order, Equivalence Relations

Summary:
We begin by studying the order of elements in groups, defining both finite and infinite order and establishing properties about powers of elements. We prove that the order of an element equals the size of its cyclic subgroup. Building on this foundation, we introduce equivalence relations and their fundamental properties. We show that equivalence relations naturally partition sets into equivalence classes.

Topics Covered: equivalence relation, group, order

Proposition (last time):

Let G be a group and let $a \in G$. Then,

1. $\langle a \rangle$ is a group
2. If K is a subgroup of G and $a \in K$, then $\langle a \rangle \subseteq K$

Definition:

Let G be a group and let $a \in G$. If there exists a positive integer $n \in \mathbb{Z}^+$ such that $a^n = e$, then a has **finite order** and the smallest positive integer n such that $a^n = e$ is called the order of a. If there does not exist a positive integer $n \in \mathbb{Z}^+$ such that $a^n = e$, then a is said to have **infinite order**.

Example:

Consider the group $(\mathbb{Z}, +)$. In this group, the identity element is 0. In this group, any element other than 0 has infinite order.

Proposition:

Let G be a group and let $a \in G$. If a has infinite order, then

1. $k \neq m \implies a^k \neq a^m$
   - Suppose not. Then, we have that $a^{k-m} = e$, which contradicts that a has infinite order. Therefore, it must hold that $a^k \neq a^m$.
2. If a has finite order and $k \in \mathbb{Z}$, then $a^k = e \iff \sigma(a) \mid k$
   - This means $\sigma(a)$ divides k
3. If a has finite order $\sigma(a) = n$, then $\forall k, m \in \mathbb{Z}\ a^m = a^k \iff k \equiv m \pmod{n}$
   - Furthermore, $|\langle a \rangle| = \sigma(a)$

Lagrange's Theorem:

If H is a subgroup of a finite group G, then $|H| \mid |G|$.

In other words, if H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Definition:

Let S be a set. A collection $\mathcal{P}$ of nonempty subsets of S is called a partition of S when each element of S belongs to exactly one set in $\mathcal{P}$.

For example

$$\begin{aligned} S &= \{1, 2, \star, \circ, ?, !\} \\ &= \{1\} \sqcup \{2, \circ\} \sqcup \{\star\} \sqcup \{?, !\} \end{aligned}$$

Definition: Let S be a set. A subset $R \subseteq S \times S$ is an equivalence relation on S means

1. $\forall a \in S.\ (a, a) \in R$

- Reflective

2. $\forall a, b \in S.\ (a, b) \in S \implies (b, a) \in S$
   - Symmetric
3. $\forall a, b, c \in S.\ (a, b), (b, c) \in S \implies (a, c) \in S$
   - Transitive

Equivalence class of $a \in S$: $[a] = \{x \in S \mid x \sim a\}$

Theorem: Let $\sim$ be an equivalence relation on S, Then, the distinct equivalence classes partition S into nonempty sets. Moreover, given any partition of S, there is an equivalence relation on S whose equivalence classes are the parts of the partition.

Example:

Let $f : S \to T$ be a function. Define $x_1, x_2 \in S$.

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2)$$

Claim: $\sim_f$ is an equivalence relation on S.

Example 2:

$\mathbb{Z}$, fix $n \in \mathbb{Z}_{\geq 0}$. $a \sim b \iff n \mid a - b$ is an equivalence relation.

Proof of theorem 1:

Note that $a \in [a]$, so none of the equivalence classes are empty. Moreover, $\forall a \in S$ appears in an equivalence class.

Suppose $a, b \in S$ and $[a] \cap [b] \neq \emptyset$. $c \in [a] \cap [b] \implies c \sin a$ and $c \sim b \implies a \sim b$.

$$x \in [a] \iff x \sim a$$

and we have $a \sim b \implies x \sim b \implies x[b].\ a \sim c$.

$$\implies [a] \subseteq [b]$$

Doing the same we get $[b] \subseteq [a]$.

$$\implies [a] = [b]$$

$$QED$$

Example:

$$H = \langle (1, 2) \rangle = \{\mathrm{id}, (1, 2)\} = H\ \mathrm{id}$$

Let $a \in G$

$$H\ a = \{h\ a \mid h \in H\}$$

$$H\ (1, 2) = H$$

$$H\ (1, 3) = \{(1, 3), (1, 3, 2)\}$$

$$H\ (1, 3, 2) = \{(1, 3, 2), (1, 3)\}$$

$$H\ (2, 3) = \{(2, 3), (1, 2, 3)\} = H\ (1, 2, 3)$$

Lemma:

Let H be a subgroup of G. For $a, b \in G$, define $a \sim b \iff ab^{-1} \in H$. Then, $\sim$ is an equivalence relation.

Proof:

1. Reflexive
   - $a \sim a \implies a^{-1} = e \in H$
2. Symmetric

- $a \sim b \iff b \sim a$

3. Transitivity
   - $a \sim b, b \sim c \implies a \sim c$