Lecture 6: More on Monoids and Groups, Lagrange's Theorem, Cyclic Groups

Summary:
We explore further properties of monoids and groups. We examine examples of monoids that are not groups, such as integers under multiplication and matrices under multiplication. We prove that the set of invertible elements in a monoid forms a group. We introduce subgroups and Lagrange's theorem, which states that the order of a subgroup divides the order of the group, when the group is finite. We define cyclic groups and prove that they are the smallest subgroups containing a given element.

Topics Covered: cyclic group, group, Lagrange's theorem, monoid

Recall that a group is a monoid where every element is invertible.

Examples of monoids (but not groups, since not every element is invertible):

- $(\mathbb{Z}, \cdot)$
- $(\mathcal{M}_n(\mathbb{R}), \cdot)$

Examples of groups:

- $(\{-1, 1\}, \cdot)$
- $(\{M \in \mathcal{M}_n(\mathbb{R}) : \det M \neq 0\}, \cdot)$
  - Note that this follows because $\det AB = \det A \cdot \det B$
  - This group is called $\mathrm{GL}_n(\mathbb{R})$
- Given a monoid $(M, \cdot)$, we denote M^x the set of invertible elements of M.

Proposition: Given a monoid $(M, \cdot)$, then $(M^\times, \cdot)$ is a group

Proof: We need to show the following things

1. Closure
   - $\forall a, b \in M^\times.\ a \cdot b \in M^\times$
2. $e \in M$ is invertible $\implies e \in M^\times$
3. Associativity
4. Every element is invertible in $M^\times$

Lemma:

$a, b \in M^\times$ where $(M, \cdot)$ is a monoid.

Then, $a \cdot b \in M^x$ and

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Proof:

The inverse, if it exists, is unique.

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$$
$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = e$$

Definition:

Let $(G, \cdot)$ be a group. Let $H \subseteq G$. If $(H, \cdot)$ is a group, then we say it is a subgroup of G under the operation induced by G.

Lagrange's theorem:

If G is a finite group and H is a subgroup of G, then the cardinality of H divides the cardinality of G.

Proposition:

Let G be a group with identity element e, and $H \subseteq G$.

H is a subgroup of $G \iff G$ satisfies

1. $a, b \in H \implies ab \in H$
2. $e \in H$.
3. $a \in H \implies a^{-1} \in H$

$\implies$ **proof:**

Let G be a group and let $H \subseteq G$ be a subgroup of G.

Since H is a group, closure holds, which means the first condition has to hold.

Since H is a group, we know that H has an identity element $e' \in H \in G$.

Since e' is an identity element of H, we know that

$$e'e' = e' = e'e$$

We have that, in G

$$e'e' = e'e$$

So, by the cancellation property,

$$e' = e$$

Therefore, $e \in H$, so the second condition holds.

Since $a \in H$ and H is a subgroup, meaning it is a group, $\exists b \in H$ such that $ab = e = ba$. This is in H, therefore, this also holds in G.

Therefore, in G, we also have

$$aa^{-1} = a^{-1}a = e$$

Therefore, the third condition holds.

$$QED$$

$\impliedby$ **proof:**

Let G be a group with $H \subseteq G$ and H satisfies 1, 2, and 3.

We want to show that H is a subgroup of G.

For H to be a group we need closure by 1.

Need identity $\implies$ e is an identity in H

Associativity

Need inverses, a^{-1} is an inverse, so third holds.

$$QED$$

Note that for a group G, G itself is always a subgroup of G, and $(\{e\}, \cdot)$ is called the trivial subgroup.

Corollary: Let G be a group and $H \subseteq G$. Note that H is a subgroup of $G \iff H \neq \emptyset$ and $\forall a, b \in H.\ ab^{-1} \in H$.

$\implies$ **proof:**

Let H be a subgroup of G. Using proposition ii, we know that $e \in H \implies H \neq \emptyset$.

$a, b \in H \implies ab^{-1} \in H.$

$$QED$$

$\impliedby$ **proof:**

$H \neq \emptyset$ and $\forall a, b \in H \implies ab^{-1} \in H.$

Since $H \neq \emptyset$, $\exists a \in G$ such that $a \in H \implies a, a^{-1} \in H \implies aa^{-1} \in H, \implies e \in H.$

$e, a \in H$

$e, a \in H \implies a^{-1} = ea^{-1} \in H.$

Corollary:

Let G be a group, let H be a finite nonempty subset of G.

Then, H is a subgroup of $G \iff \forall a, b \in H. ab \in H.$

$\implies$ proof is trivial

$\impliedby$ **proof:**

We know that

$$\forall a, b \in H \implies ab \in H$$

We also know that $H \neq \emptyset$ and $|H| < \infty$.

Let $b \in H$ be finite.

Then, we know that $b, b^2, b^3, \ldots$.

$$\implies m > n \in \mathbb{Z}_{\geq 0}.\ b^n = b^m$$
$$\implies e = b^{m-n}$$
$$\implies b^{-1} = b^{m-n-1}$$
$$\implies b^{-1} \in H$$

Definition:

Let G be a group with $a \in G$.

Define

$$\langle a \rangle = \{a^n \in G \mid n \in \mathbb{Z}\}$$

This is called the cyclic subgroup generated by a.

Moreover, a group H is called cyclic when $\exists a \in H$ such that $H = \langle a \rangle$.

Note that S_3 is not cyclic.

Proposition:
Let G be a group with $a \in G$.

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

Proof:

1. Closure
   - $a^m \cdot a^n = a^{m+n}$

$$(a^n)^{-1} = (a^{-1})^n = a^{-n}$$

2. By closure