Lecture 8: Equivalence Relations, Lagrange's Theorem, Groups, Isomorphisms, Homomorphisms

Summary:
We continue our study of equivalence relations and groups. We prove Lagrange's theorem using cosets and equivalence relations. We use Lagrange's theorem to show that any group of prime order is cyclic. We introduce group isomorphisms and homomorphisms, proving that they preserve important group properties. We demonstrate that isomorphic groups have the same structure and prove that the order of elements is preserved under isomorphisms. We show that isomorphisms map identity elements to identity elements and that the inverse of an isomorphism is also an isomorphism.

Topics Covered: equivalence relation, group, homomorphism, isomorphism, Lagrange's theorem

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

Lagrange's theorem: Given a finite group G and subgroup H, the cardinality of H divides G.

Proof:

Recall that, given any element $a \in G$, we can define $H\ a \subseteq G$

$$Ha = \{ha \mid h \in H\}$$

Note that for $h, a \in G$, ha is the product $h \cdot a$ in H.

For example

$$S_3 = G$$
$$H = \langle (1,2) \rangle = \{e, (1,2)\} = He = H(1,2)$$
$$a = (1,2,3)$$
$$Ha = \{e(1,2,3), (1,2)(1,2,3)\}$$
$$= \{(1,2,3), (1)(2,3)\}$$

To prove claim 1, we will show that

1. $[a] \subseteq Ha$
2. $[a] \supseteq Ha$

We have

1. $x \in [a] : x \sim a \iff xa^{-1} \in H \iff ax^{-1}$
2. $x \in Ha \implies x = ha$ for some $h \in H : xa^{-1} = haa^{-1} = h \in H$

We need to prove that $x \sim a \iff xa^{-1} \in H$.

Claim 1: $[a] = Ha$

Claim 2: $|Ha| = |H|$, because of the cancellation property - $\forall a \in G.\ (\forall b, c \in G.\ ab = ac) \implies \forall b, c \in G.\ b = c$

Corollary:

Let G be a finite group of order n (this means $|G| = n$). Then,

1. $\forall a \in G.\ \sigma(a) \mid n$
2. $\forall a \in G.\ a^n = e$

Proof:

Let $a \in G$ and let $H = \langle a \rangle$ be the cyclic group generated by a. We showed last time that $|\langle a \rangle| = \sigma(a)$.

Thus, since $\langle a \rangle$ is a subgroup of $G \implies \sigma(a) \mid |G| = n$

1. $\forall k \in \mathbb{Z}.\ \left(a^{\sigma(a)}\right)^k = e$

Corollary:

Any group of prime order is cyclic.

Proof:

Let G be a group with prime order $|G| = p$. This means

$$\forall a \in G.\ \sigma(a) \mid p \implies \sigma(a) = 1 \text{ or } \sigma(a) = p$$

Only e is of order 1 means

$$\exists a \in G.\ \sigma(a) = p \implies |\langle a \rangle| = p, \langle a \rangle \subseteq G \implies G = \langle a \rangle$$

$$QED$$

$$G = \{e, a, a^2, a^3, a^4, a^5, a^6\}$$

$$a^7 = e$$

- $\sigma(a^2) = 7$
- $\sigma(a^3) = 7$
- $\sigma(a^4) = 7$
- $\sigma(a^5) = 7$
- $\sigma(a^6) = 7$

This is because 7 is prime. Therefore, every element in G except for e is a generator of G.

Definition:

Let G_1 and G_2 be groups and let $\phi : G_1 \to G_2$ be a function. ϕ is a group isomorphism means

1. ϕ is a bijection
2. $\phi(ab) = \phi(a)\phi(b)$
   - On the left, multiplication is in G_1
   - On the right, multiplication is in G_2

When such a ϕ exists, we say that G_1 is isomorphic to G_2 and we write $G_1 \cong G_2$. This essentially means the groups G_1 and G_2 are the same group with the same structure, but with differently-named elements.

Example:

$$G = \langle a \rangle,\ \ \sigma(a) = 7$$

$$\phi : G \to \langle (1,2,3,4,5,6,7) \rangle$$

$$\phi(a) = (1,2,3,4,5,6,7)$$

$$\phi(a)^2 = (\phi(a))^2$$

Here, ϕ is a group isomorphism.

Definition:

Let G_1, G_2 be groups. A homomorphism is a function $\phi : G_1 \to G_2$ such that $\forall a, b \in G_1.\ \phi(ab) = \phi(a)\phi(b)$.

$\cdot$	e	a	a^2	b	ab	a^2b
e	$(1)(2)(3)$	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
a						

$\cdot$	e	a	a^2	b	ab	a^2b
a^2						
b						
ab						
a^2b						

This creates an isomorphism.

Proposition:

Let $\phi : G_1 \to G_2$ be a group isomorphism. Then,

1. $\forall a \in G.\ \sigma_{G_1}(a) = \sigma_{G_2}(\phi(a))$
2. If G_1 is abelian (commutative), so is G_2
3. If G_1 is cyclic, then G_2 is cyclic

Note that for an isomorphism $\phi : G_1 \to G_2$ with $e_1 \in G_1$ and $e_2 \in G_2$ identity elements, we have $\phi(e_1) = e_2$. This is shown by verifying that $\phi(e_1) \in G_2$ is an identity element of G_2. Then, by the uniqueness of identity elements, we know that $e_2 = \phi(e_1)$, so they are indeed the same element.

Since ϕ is an isomorphism, there exists an inverse isomorphism that maps $\phi(a) \mapsto a$.

Therefore,

$$\sigma(\phi(a)) \mid \sigma(a)$$

and

$$\sigma(a) \mid \sigma(\phi(a))$$

Therefore,

$$\sigma(a) = \sigma(\phi(a))$$