Note Title 9/12/2022

Lecture 19:

Monday, Sep 12, 2022

Theorem 1: If $\phi: G_1 \to G_2$ is an isomorphism, then $\phi^{-1}: G_2 \to G_1$ is also an isomorphism.

Proof: Let $x, y \in G_2$. Then, there exist unique a and b in G_1 such that $\phi(a) = x$ and $\phi(b) = y$.

Then, $a = \phi^{-1}(x)$ and $b = \phi^{-1}(y)$

Now, $xy = \phi(a)\,\phi(b) = \phi(ab) \Rightarrow ab = \phi^{-1}(xy)$

$\Rightarrow \phi^{-1}(xy) = ab = \phi^{-1}(x)\,\phi^{-1}(y) \quad \forall\, x, y \in G_2.$

#

Theorem 2: If $\phi: G_1 \to G_2$ and $\psi: G_2 \to G_3$ are group isomorphisms, then $\psi \circ \phi: G_1 \to G_3$ is also a group isomorphism.

Proof: For $x, y \in G_1$, we have

$$(\psi \circ \phi)(xy) = \psi(\phi(xy)) = \psi(\phi(x) \cdot \phi(y))$$
$$= \psi(\phi(x))\, \psi(\phi(y))$$
$$= (\psi \circ \phi)(x)\, (\psi \circ \phi)(y)$$

$\therefore$ $\psi \circ \phi$ is a group homomorphism. Since ϕ and ψ are bijectives, so $\psi \circ \phi$ is a bijective. Hence, $\psi \circ \phi$ is an isomorphism.

#

__Ex1:__ If G is a finite and $f: G \to \mathbb{Z}$ is a homomorphism, then f is the __trivial__ homomorphism, that is, $f(x) = 0 \ \forall x \in G$.

__Ex2:__ Find all the group homomorphisms $f: \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$

__Solution:__ $f(k) = k f(1)$, so f is determined by the value of $f(1)$. Hence, $f(k) = a \cdot k$ for some fixed $a \in \mathbb{Z}_m$.

For $a \in \mathbb{Z}_m$, let $f_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ be defined by

$$f_a(x) = ax \quad \forall x \in \mathbb{Z}_n$$

If $f_a : \mathbb{Z}_n \to \mathbb{Z}_m$ is a group homomorphism, then

$$0 \equiv f_a(0) \equiv f_a(n) \equiv n \cdot f_a(1) \equiv n \cdot a \pmod{m}.$$

By Theorem 1 ($b = 0$ case) of Lecture 8, we have the congruence $nx \equiv 0 \pmod{m}$ has $d = \gcd(n, m)$ solutions, namely, $x = \frac{m}{d} k$, $k = 0, 1, 2, \cdots, d-1$.

For each solution $x = a$, we have a homomorphism

$$f_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m.$$

Hence, the set of homomorphisms $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ is

$$\left\{ f_a \;\middle|\; a = \frac{m}{d} k, \quad k = 0, 1, \ldots, d-1 \right\}.$$

Here $f_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ is the map defined by

$$f_a(x) = ax \quad \forall \, x \in \mathbb{Z}_n.$$

#

§ Automorphisms:

$\mathrm{Aut}(G) = \{\phi : G \to G \mid \phi$ is an automorphism$\}$ is a group under composition of functions.

Ex 1: $\mathrm{Aut}(\mathbb{Z}) = \{I, \phi\} \cong \mathbb{Z}_2$, here $\phi(x) = -x \;\forall\, x \in \mathbb{Z}$.

In fact, if G is an infinite cyclic group, then

$$\mathrm{Aut}(G) \cong \mathbb{Z}_2.$$

Ex 2: If G is a finite cyclic group of order n, then $G \cong (U(n), \cdot)$.

Ex 3: $\operatorname{Aut}(\mathbb{Q}) \cong (\mathbb{Q}^*, \cdot)$

Let $x = \frac{p}{q}$, $x \neq 0$, $q > 0$.

Then, if $f: \mathbb{Q} \to \mathbb{Q}$ is a homomorphism, we have

$$q \cdot f(x) = f(q \cdot x) = f(p) = p\, f(1)$$

$$\Rightarrow f(x) = \frac{p}{q} f(1) = x\, f(1).$$

If $x = 0$, then $f(x) = 0 = x \cdot f(1)$.

$\therefore f(x) = x\, f(1) \quad \forall x \in \mathbb{Q}$.

Thus, $\operatorname{Aut}(\mathbb{Q}) = \{ f_a \mid a \in \mathbb{Q}, a \neq 0 \} \cong (\mathbb{Q}^*, \cdot)$. #