Lecture Notes: Abstract Algebra — Properties of Isomorphisms (Course By: Alvaro Lozano-Robledo)

Thobias K. Høivik

March 11, 2025

Theorems

Let $\phi : G \to H$ be a group isomorphism.
Then:

Theorem 1. *$\phi^{-1} : H \to G$ is also an isomorphism.*

Proof. Since $\phi : G \to H$ is an isomorphism $\Rightarrow \phi$ is a bijection and therefore there exists an inverse map $\phi^{-1} : H \to G$ and since ϕ is a bijection we know ϕ^{-1} is a bijection. Observe

$$\begin{gathered} h, k \in H \Rightarrow \exists a, b, \in G : \phi(a) = h \wedge \phi(b) = k \\ \therefore \phi^{-1}(hk) = \phi^{-1}(\phi(a)\phi(b)) \\ = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(h)\phi^{-1}(k) \end{gathered}$$

thus ϕ^{-1} is an isomorphism. □

Theorem 2. *$|G| = |H|$, the cardinalities of G and H are the same.*

Proof. ϕ is an isomorphism $\Rightarrow \phi$ is a bijection and bijections between sets are how we define two sets to have the same cardinality. □

Theorem 3. *If G is abelian, then H is abelian.*

Proof. Take $h, k \in H$ arbitrary elements, then

$$\begin{gathered} \exists a, b \in G : \phi(a) = h \wedge \phi(b) = k \\ \phi(ab) = \phi(ba) \\ \phi(a)\phi(b) = \phi(b)\phi(a) \\ hk = kh \end{gathered}$$

Since we took h and k to be arbitrary elements of H, we have shown all elements of H commute, hence H is abelian. □

Theorem 4. *If G is cyclic, then H is cyclic.*

Proof. Let's assume $G =< a >$ and take $h \in H$ arbitrary.

$$\exists b \in G : h = \phi(b)$$
$$b \in G =< a > \Rightarrow b = a^n, n \in \mathbb{Z}^+$$
$$\phi(b) = \phi(a^n) = \phi(a)^n = \phi(a)\phi(a)\dots\phi(a)$$
$$\therefore h = \phi(a)^n$$

Since we took h to be arbitrary $h = \phi(a)^n \forall h \in H$, thus $H =< \phi(a) >$.

$\square$

Theorem 5. *If G has a subgroup of order n, then H has a subgroup of order n.*

Proof. Let $J \subseteq G$ be a subgroup with $|J| = n$, and consider its image under ϕ:

$$\phi[J] = \{\phi(a) \mid a \in J\} \subseteq H.$$

We verify that $\phi[J]$ is a subgroup of H: **Closure:** If $h, k \in \phi[J]$, then there exist $a, b \in J$ such that $h = \phi(a)$ and $k = \phi(b)$. Since J is a subgroup, $ab^{-1} \in J$. Applying ϕ, we get

$$hk^{-1} = \phi(a)\phi(b)^{-1} = \phi(ab^{-1}) \in \phi[J].$$

So, $\phi[J]$ is closed under the group operation. **Identity:** Since J is a subgroup, it contains the identity element e_G. Applying ϕ, we obtain

$$\phi(e_G) = e_H \in \phi[J].$$

Thus, $\phi[J]$ contains the identity element of H. **Inverses:** If $h \in \phi[J]$, then $h = \phi(a)$ for some $a \in J$. Since J is a subgroup, $a^{-1} \in J$, so

$$\phi(a^{-1}) = \phi(a)^{-1} = h^{-1} \in \phi[J].$$

Hence, $\phi[J]$ contains inverses. Thus, $\phi[J]$ is a subgroup of H. Now, to show $|\phi[J]| = |J| = n$, we need ϕ to be injective on J, meaning $\ker\phi \cap J = \{e_G\}$. This holds if ϕ is injective or if J is mapped bijectively onto $\phi[J]$. In that case, $|\phi[J]| = |J| = n$, as required. Thus, if ϕ is injective on J, then H has a subgroup of order n, completing the proof. $\square$

Theorem 6. *All cyclic groups of infinite order are isomorphic to the integers under addition. Which means that there is only one infinite cyclic group structure.*

Proof. Let G be a group, $|G| = \infty$, and $G =< a >$. Let $\phi : \mathbb{Z} \to G, \phi(n) = a^n$. Then:

$$g \in G \Rightarrow g = a^m, m \in \mathbb{Z}$$

$$\Rightarrow \phi(m) = g$$

making ϕ surjective and

$$\phi(n) = \phi(m) \Rightarrow a^n = a^m$$
$$a^{n-m} = e \Rightarrow n - m = 0 (\because |G| = \infty) \Rightarrow n = m$$

thus ϕ is injective. Lastly

$$\phi(n + m) = a^{n+m} = a^n a^m = \phi(n)\phi(m)$$

$\square$