Isomorphism Theorems

Miliyon T.

October 7, 2013

1 Group Isomorphism

Definition .1. *Two groups $(G, \cdot)$ and $(H, \circ)$ are **isomorphic** if there exists a bijective map $\phi : G \to H$ such that the group operation is preserved; that is,*

$$\phi(a \cdot b) = \phi(a) \circ \phi(b) \qquad \forall a, b \in G.$$

*If G is isomorphic to H, we write $G \cong H$. The map ϕ is called an **isomorphism**.*

Theorem 1.1. *Let $\phi : G \to H$ be an isomorphism of two groups. Then the following statements are true.*

1. *$\phi^{-1} : H \to G$ is an isomorphism.*
2. *$|G| = |H|$.*
3. *If G is abelian, then H is abelian.*
4. *If G is cyclic, then H is cyclic.*
5. *If G has a subgroup of order n, then H has a subgroup of order n.*

Proof. Assertions (1) and (2) follow from the fact that ϕ is a bijection. We will prove (3) here and leave the remainder of the theorem to be proved in the exercises.

(3) Suppose that h_1 and h_2 are elements of H. Since ϕ is onto, there exist elements $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Therefore,

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1) = h_2 h_1.$$

□

We are now in a position to characterize all cyclic groups.

Theorem 1.2. *All cyclic groups of infinite order are isomorphic to $\mathbb{Z}$.*

Proof. Let G be a cyclic group with infinite order and suppose that a is a generator of G. Define a map $\phi : \mathbb{Z} \to G$ by $\phi : n \mapsto a^n$. Then

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

To show that ϕ is injective, suppose that m and n are two elements in $\mathbb{Z}$, where $m \neq n$. We can assume that $m > n$. We must show that $a^m \neq a^n$. Let us suppose the contrary; that is, $a^m = a^n$. In this case $a^{m-n} = e$, where $m - n > 0$, which contradicts the fact that a has infinite order. Our map is onto since any element in G can be written as a^n for some integer n and $\phi(n) = a^n$. □

Theorem 1.3. *If G is a cyclic group of order n, then G is isomorphic to $\mathbb{Z}_n$.*

Proof. Let G be a cyclic group of order n generated by a and define a map $\phi : \mathbb{Z}_n \to G$ by $\phi(k) = a^k$, where $0 \leq k < n$. The proof that ϕ is an isomorphism is one of the end-of-chapter exercises. □

Corollary 1.4. *If G is a group of order p, where p is a prime number, then G is isomorphic to $\mathbb{Z}_p$.*

Proof. The proof is a direct result of Corollary cosets-theorem7. □

The main goal in group theory is to classify all groups; however, it makes sense to consider two groups to be the same if they are isomorphic. We state this result in the following theorem, whose proof is left as an exercise.

Theorem 1.5. *The isomorphism of groups determines an equivalence relation on the class of all groups.*

Hence, we can modify our goal of classifying all groups to classifying all groups **up to isomorphism**; that is, we will consider two groups to be the same if they are isomorphic.

2 Isomorphism Theorem

Though at first it is not evident that factor groups correspond exactly to homomorphic images, we can use factor groups to study homomorphisms. We already know that with every group homomorphism $\phi : G \to H$ we can associate a normal subgroup of G, $\ker \phi$; the converse is also true. Every normal subgroup of a group G gives rise to homomorphism of groups.

Let H be a normal subgroup of G. Define the **natural** or **canonical homomorphism**

$$\phi : G \to G/H$$

by

$$\phi(g) = gH.$$

This is indeed a homomorphism, since

$$\phi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \phi(g_1)\phi(g_2).$$

The kernel of this homomorphism is H. The following theorems describe the relationships among group homomorphisms, normal subgroups, and factor groups.

Theorem 2.1 (First Isomorphism Theorem)**.** *If $\psi : G \to H$ is a group homomorphism with $K = \ker \psi$, then K is normal in G. Let $\phi : G \to G/K$ be the canonical homomorphism. Then there exists a unique isomorphism $\eta : G/K \to \psi(G)$ such that $\psi = \eta\phi$.*

Proof. We already know that K is normal in G. Define $\eta : G/K \to \psi(G)$ by $\eta(gK) = \psi(g)$. We first show that η is a well-defined map. If $g_1K = g_2K$, then for some $k \in K$, $g_1k = g_2$; consequently,

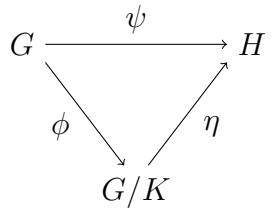
$$\eta(g_1K) = \psi(g_1) = \psi(g_1)\psi(k) = \psi(g_1k) = \psi(g_2) = \eta(g_2K).$$

Thus, η does not depend on the choice of coset representatives and the map $\eta : G/K \to \psi(G)$ is uniquely defined since $\psi = \eta\phi$. We must also show that η is a homomorphism, but

$$\begin{aligned}\eta(g_1Kg_2K) &= \eta(g_1g_2K) \\ &= \psi(g_1g_2) \\ &= \psi(g_1)\psi(g_2) \\ &= \eta(g_1K)\eta(g_2K).\end{aligned}$$

Clearly, η is onto $\psi(G)$. To show that η is one-to-one, suppose that $\eta(g_1K) = \eta(g_2K)$. Then $\psi(g_1) = \psi(g_2)$. This implies that $\psi(g_1^{-1}g_2) = e$, or $g_1^{-1}g_2$ is in the kernel of ψ; hence, $g_1^{-1}g_2K = K$; that is, $g_1K = g_2K$. □

Mathematicians often use diagrams called **commutative diagrams** to describe such theorems. The following diagram "commutes" since $\psi = \eta\phi$.



Example .1. *Let G be a cyclic group with generator g. Define a map $\phi : \mathbb{Z} \to G$ by $n \mapsto g^n$. This map is a surjective homomorphism since*

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

Clearly ϕ is onto. If $|g| = m$, then $g^m = e$. Hence, $\ker \phi = m\mathbb{Z}$ and $\mathbb{Z}/\ker \phi = \mathbb{Z}/m\mathbb{Z} \cong G$. On the other hand, if the order of g is infinite, then $\ker \phi = 0$ and ϕ is an isomorphism of G and $\mathbb{Z}$. Hence, two cyclic groups are isomorphic exactly when they have the same order. Up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}_n$.

Theorem 2.2 (Second Isomorphism Theorem)**.** *Let H be a subgroup of a group G (not necessarily normal in G) and N a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and*

$$H/H \cap N \cong HN/N.$$

Proof. We will first show that $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G. Suppose that $h_1n_1, h_2n_2 \in HN$. Since N is normal, $(h_2)^{-1}n_1h_2 \in N$. So

$$(h_1n_1)(h_2n_2) = h_1h_2((h_2)^{-1}n_1h_2)n_2$$

is in HN. The inverse of $hn \in HN$ is in HN since

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

Next, we prove that $H \cap N$ is normal in H. Let $h \in H$ and $n \in H \cap N$. Then $h^{-1}nh \in H$ since each element is in H. Also, $h^{-1}nh \in N$ since N is normal in G; therefore, $h^{-1}nh \in H \cap N$.

Now define a map ϕ from H to HN/N by $h \mapsto hN$. The map ϕ is onto, since any coset $hnN = hN$ is the image of h in H. We also know that ϕ is a homomorphism because

$$\phi(hh') = hh'N = hNh'N = \phi(h)\phi(h').$$

By the First Isomorphism Theorem, the image of ϕ is isomorphic to $H/\ker\phi$; that is,

$$HN/N = \phi(H) \cong H/\ker\phi.$$

Since

$$\ker\phi = \{h \in H : h \in N\} = H \cap N,$$

$HN/N = \phi(H) \cong H/H \cap N$. □

Theorem 2.3 (Correspondence Theorem)**.** *Let $N \lhd G$. Then $H \mapsto H/N$ is a 1-1 correspondence between the set of subgroups H containing N and the set of subgroups of G/N. Furthermore, the normal subgroups of G containing N correspond to normal subgroups of G/N.*

Proof. Let H be a subgroup of G containing N. Since N is normal in H, H/N makes sense. Let aN and bN be elements of H/N. Then $(aN)(b^{-1}N) = ab^{-1}N \in H/N$; hence, H/N is a subgroup of G/N.

Let S be a subgroup of G/N. This subgroup is a set of cosets of N. If $H = \{g \in G : gN \in S\}$, then for $h_1, h_2 \in H$, we have that $(h_1N)(h_2N) = h_1h_2N \in S$ and $h_1^{-1}N \in S$. Therefore, H must be a subgroup of G. Clearly, H contains N. Therefore, $S = H/N$. Consequently, the map $H \mapsto H/N$ is onto.

Suppose that H_1 and H_2 are subgroups of G containing N such that $H_1/N = H_2/N$. If $h_1 \in H_1$, then $h_1N \in H_1/N$. Hence, $h_1N = h_2N \subset H_2$ for some h_2 in H_2. However, since N is contained in H_2, we know that $h_1 \in H_2$ or $H_1 \subset H_2$. Similarly, $H_2 \subset H_1$. Since $H_1 = H_2$, the map $H \mapsto H/N$ is one-to-one.

Suppose that H is normal in G and N is a subgroup of H. Then it is easy to verify that the map $G/N \to G/H$ defined by $gN \mapsto gH$ is a homomorphism. The kernel of this homomorphism is H/N, which proves that H/N is normal in G/N.

Conversely, suppose that H/N is normal in G/N. The homomorphism given by

$$G \to G/N \to \frac{G/N}{H/N}$$

has kernel H. Hence, H must be normal in G. □

Notice that in the course of the proof of Correspond Theorem, we have also proved the following theorem.

Theorem 2.4 (Third Isomorphism Theorem)**.** *Let G be a group and N and H be normal subgroups of G with $N \subset H$. Then*

$$G/H \cong \frac{G/N}{H/N}.$$

Example .2. *By the Third Isomorphism Theorem* **??**,

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}).$$

Since $|\mathbb{Z}/mn\mathbb{Z}| = mn$ and $|\mathbb{Z}/m\mathbb{Z}| = m$, we have $|m\mathbb{Z}/mn\mathbb{Z}| = n$.