Group Homomorphisms

Recall that an isomorphism of a group G with a group G' is a 1-1 function mapping G onto G' such that:

$$\phi(xy) = \phi(x)\phi(y) \text{ for all } x, y \in G.$$

Isomorphic groups have the same group structure.

Def. A map $\phi: G \to G'$ is a **group homomorphism** if

$$\phi(xy) = \phi(x)\phi(y) \text{ for all } x, y \in G.$$

An isomorphism is a type of homomorphism that is 1-1 and onto.

For any groups G, G' there is always at least one homomorphism, $\phi: G \to G'$, given by $\phi(g) = e'$ for all $g \in G$. This is called the **trivial homomorphism**. However, this is not a very useful homomorphism because no information about the group structures of G and G' can be gained from this.

Ex. Let $\phi: G_1 \to G_2$ be a homomorphism of G_1 into G_2. Show that If G_1 is abelian and ϕ is onto then G_2 must be abelian. However, if ϕ is not onto then G_2 need not be abelian.

To show G_2 is abelian we must show given any $a_2, b_2 \in G_2$ that $a_2 b_2 = b_2 a_2$.

Since ϕ is onto, we know there is at least one $a_1 \in G_1$ and at least one $b_1 \in G_1$ such that $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$.

Since G_1 is abelian $a_1 b_1 = b_1 a_1$. So we know:

$$a_2 b_2 = \phi(a_1)\phi(b_1) = \phi(a_1 b_1) = \phi(b_1 a_1)$$
$$= \phi(b_1)\phi(a_1) = b_2 a_2$$

Thus, G_2 is abelian.

Notice that if ϕ is not onto then we can have the trivial homomorphism:

$$\phi: \mathbb{Z}_6 \to S_3, \quad \phi(k) = \rho_0 = identity.$$

Thus $G_1 = \mathbb{Z}_6$ is abelian but $G_2 = S_3$ is non-abelian.

Ex. Let $r \in \mathbb{Z}$. Consider two mappings from $\mathbb{Z}, +$ to $\mathbb{Z}$,+ :

$\phi_1: \mathbb{Z} \to \mathbb{Z};\ \phi_1(n) = rn$ for all $n \in \mathbb{Z}$

$\phi_2: \mathbb{Z} \to \mathbb{Z};\ \phi_2(n) = rn + 1$ for all $n \in \mathbb{Z}$.

Show that $\phi_1$is a homomorphism but that ϕ_2 is not.

$$\phi_1(m+n) = r(m+n) = rm + rn = \phi_1(m) + \phi_1(n)$$

so ϕ_1 is a homomorphism.

$$\phi_2(m+n) = r(m+n) + 1 = rm + rn + 1$$
$$\phi_2(m) + \phi_2(n) = rm + 1 + rn + 1 = rm + rn + 2.$$

Thus $\phi_2(m+n) \neq \phi_2(m) + \phi_2(n)$.

So ϕ_2 is not a homomorphism.

Ex. Let $\phi: GL(2,\mathbb{R}) \to \mathbb{R}^*$ by $\phi(A) = detA.$ Show ϕ is a homomorphism.

For $A, B \in GL(2,\mathbb{R})$,

$\phi(AB) = det(AB) = (detA)(detB) = \phi(A)\phi(B).$

Note: $GL(2,\mathbb{R})$ is non-abelian and $\mathbb{R}^*$ is abelian. So you can have a homomorphism from a non-abelian group onto an abelian group.

Ex. Let F be the group of all real valued functions on $\mathbb{R}$ under addition.

Show $\phi: F \to \mathbb{R}$ by $\phi(f) = f(3)$ is a homomorphism.

$$\phi(f+g) = (f+g)(3) = \big(f(3)\big) + \big(g(3)\big) = \phi(f) + \phi(g).$$

Ex. Let S_n be the symmetric group on n letters.

Let $\phi: S_n \to \mathbb{Z}_2$ be defined by $\phi(\sigma) = 0$ if σ is an even permutation

$= 1$ if σ is an odd permutation.

Show ϕ is a homomorphism.

We must show $\phi(\sigma\tau) = (\ \phi(\sigma) + \ \phi(\tau))\ (mod\ 2)$ for all $\sigma, \tau\ \in S_n$.

There are 4 cases:

1) σ even and τ even
2) σ odd and τ even
3) σ even and τ odd
4) σ odd and τ odd

Case		$\phi(\sigma\tau)$		$\phi(\sigma)+\phi(\tau)$
1	$\sigma\tau$ is even	0	$=$	$0+\ 0$
2	$\sigma\tau$ is odd	1	$=$	$1+\ 0$
3	$\sigma\tau$ is odd	1	$=$	$0+\ 1$
4	$\sigma\tau$ is even	0	$=$	$1+\ 1=0\ mod\ 2.$

Note: ϕ is not 1-1, but it is onto.

Ex. $\phi: \mathbb{Z} \to \mathbb{Z}_n$, where $\phi(m) = m\ (mod\ n)$ is a homomorphism.

This follows from the fact that:

$$(r+s)\ (mod\ n) = [r\ (mod\ n) + s\ (mod\ n)]\ \ (mod\ n).$$

Note: This homomorphism is very useful and we will use it later.

Ex. Let F_1 be the group of infinitely differentiable functions on $\mathbb{R}$ under addition and F_2 be the group of infinitely differentiable functions on $\mathbb{R}$, such that $f(x) \neq 0$ for any $x \in \mathbb{R}$ under multiplication.

Let $\phi_1: F_1 \to F_1$ by $\phi_1(f) = f'(x)$.

Let $\phi_2: F_1 \to F_2$ by $\phi_1(f) = 2^{f(x)}$.

Show that ϕ_1 and ϕ_2 are homomorphisms and determine if they are 1-1 or onto.

$$\phi_1(f+g) = (f+g)'(x) = f'(x) + g'(x) = \phi_1(f) + \phi_1(g).$$

$$\phi_2(f+g) = 2^{(f(x)+g(x))} = 2^{f(x)} \cdot 2^{g(x)} = \phi_2(f) \cdot \phi_2(g).$$

ϕ_1 is not 1-1 because $\phi_1(f) = \phi_1(g) \Longrightarrow f'(x) = g'(x)$,

but that only implies that $f(x) = g(x) + C$, not $f(x) = g(x)$.

ϕ_1 is onto because given any $g(x) \in F_2$, by the fundamental theorem of Calculus, if $f(x) = \int_0^x g(t)dt$, then $\phi_1(f) = f'(x) = g(x)$.

ϕ_2 is 1-1 because $\phi_2(f) = \phi_2(g) \Longrightarrow 2^{f(x)} = 2^{g(x)} \Longrightarrow f = g$.

ϕ_2 is not onto since $\phi_1(f) = 2^{f(x)} > 0$. So, for example, $g(x) = -1$ is not in the image of ϕ_2.

Def: Let $A \subseteq X, B \subseteq Y$, $\phi: X \to Y$.

The **image** $\phi[A]$ of A in Y under ϕ is $\{\phi(a) | \ a \in A\}$.

$\phi[X]$ is the **range** of ϕ.

The **inverse image** $\phi^{-1}[B]$ of B in X is $\{x \in X | \ \phi(x) \in B\}$.

Theorem: Let ϕ be a homomorphism of a group G into a group G'.

1) If e is the identity element in G then $\phi(e) = e'$, the identity element of G'.
2) If $a \in G$, then $\phi(a^{-1}) = (\phi(a))^{-1}$.
3) If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.
4) If K' is a subgroup of $G' \cap \phi[G]$, then $\phi^{-1}[K']$ is a subgroup of G.

So ϕ preserves the identity, inverses, and subgroups.

Proof 1,2 and 3:

1) $\phi(a) = \phi(ae) = \phi(a)\phi(e)$. Multiply both sides by $\left(\phi(a)\right)^{-1}$.

$$e' = \phi(e).$$

2) $e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$.

Multiply by $\left(\phi(a)\right)^{-1}$ on the left $\Longrightarrow$ $(\phi(a))^{-1} = \phi(a^{-1})$.

3) $H \leq G$. Let $\phi(a), \phi(b) \in \phi[H]$.

$\phi(a)\phi(b) = \phi(ab) \in \phi[H]$, so $\phi[H]$ is closed under multiplication.

By 2, $\phi(a^{-1}) = (\phi(a))^{-1} \implies (\phi(a))^{-1} \in \phi[H]$

so $\phi[H] \leq G'$.

Notice that $\{e'\}$ is a subgroup of G', so $\phi^{-1}(e')$ is a subgroup of G.

Def. Let $\phi: G \to G'$ be a homomorphism of groups.

The subgroup $\phi^{-1}(e') = \{x \in G \mid \phi(x) = e'\}$ is the **kernel** of ϕ, denoted $\ker(\phi)$.

Theorem: Let $\phi: G \to G'$ be a group homomorphism, and

let $H = \ker(\phi)$. Let $a \in G$. Then the set:

$$\phi^{-1}[\phi(a)] = \{x \in G|\, \phi(x) = \phi(a)\}$$

is the left coset aH of H, and is also the right coset Ha of H.

So the two partitions of G into left cosets and into right cosets of H are the same.

Ex. Let F be the group of infinitely differentiable functions on $\mathbb{R}$ under addition.

Let $\phi: F \to F$ be the homomorphism $\phi(f) = f'(x)$.

What is the kernel of ϕ?

The identity element of F is the function $f(x) = 0$.

So $\ker(\phi) = \{f \in F|\, \phi(f) = f'(x) = 0\}$,

So $\ker(\phi) = \{f \in F|\, f(x) = \text{constant}\}$.

Corollary: A group homomorphism $\phi: G \to G'$ is 1-1 if, and only if,

$\ker(\phi) = \{e\}$.

Proof: If $\ker(\phi) = \{e\}$ then by our theorem for every $a \in G$, the elements that get mapped to $\phi(a)$ is the coset $a\{e\} = \{a\}$. Thus ϕ is 1-1.

If ϕ is 1-1, we know $\phi(e) = e'$ so e is the only element that gets mapped to e' and hence, $\ker(\phi) = e$.

So when we want to prove $\phi: G \to G'$ is an isomorphism:

Step 1: Show ϕ is a homomorphism.

Step 2: Show $\ker(\phi) = \{e\}$ (which implies ϕ is 1-1)

Step 3: Show ϕ is onto.

Our theorem shows that the kernel of a homomorphism is a subgroup whose left cosets and right cosets coincide, $gH = Hg$ for all $g \in G$.

Def. A subgroup H of a group G is **normal** if its left and right cosets coincide,

i.e. $gH = Hg$ for all $g \in G$.

Corollary: If $\phi: G \to G'$ is a group homomorphism, then $\ker(\phi)$ is a normal subgroup of G.

Notice also that for any abelian group G, any subgroup H is a normal subgroup.

Ex. Suppose $\phi: \mathbb{Z} \to \mathbb{Z}_{12}$ is a homomorphism with $\phi(1) = 9$.

Find a) $\ker(\phi)$ and b) $\phi(19)$.

a) $\phi(1) = 9$

$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = (9+9) \ (mod\ 12) = 6$

$\phi(3) = \phi(1+2) = \phi(1) + \phi(2) = (9+6) \ (mod\ 12) = 3$

$\phi(4) = \phi(1+3) = \phi(1) + \phi(3) = (9+3) \ (mod\ 12) = 0$

So $4 \in \ker(\phi)$.

But notice:

$\phi(4+4) = \phi(4) + \phi(4) = 0$

$\phi(4+4+4) = \phi(4) + \phi(4) + \phi(4) = 0$

etc, so any multiple of 4 is in $\ker(\phi)$.

$\ker(\phi)$ is a subgroup of $\mathbb{Z}$, so it must be of the form $n\mathbb{Z}$.

So $\ker(\phi) = 4\mathbb{Z}$.

b) $\phi(19) = \phi(16+3) = \phi(16) + \phi(3) = 0 + 3 = 3.$

Or we could say:

$$\begin{aligned} \phi(19) &= \phi(1+1+\cdots+1) = 19(\phi(1)) \\ &= 19(9) \ \ (mod\ 12) \\ &= 171 \ \ (mod\ 12) = 3. \end{aligned}$$

Ex. Find all homomorphisms from $\mathbb{Z}$ into $\mathbb{Z}_3$.

A homomorphism is completely defined by that it does to a generator of a cyclic group. So we just need to find $\phi(1)$.

There are three possibilities:

$\phi(1) = 0$ in which case $\phi(n) = 0$,

$\phi(1) = 1$ in which case $\phi(n) = n \ \ (mod\ 3)$, or

$\phi(1) = 2$ in which case $\phi(n) = 2n \ \ (mod\ 3)$.

So there are only three different homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_3$.

Ex. Show that A_n, the alternating group on n letters (i.e. the even permutations in S_n) is a normal subgroup of S_n.

We saw earlier that

$$\phi: S_n \to \mathbb{Z}_2 \text{ by } \phi(\sigma) = 0 \text{ if } \sigma \text{ is even}$$
$$= 1 \text{ if } \sigma \text{ is odd}$$

is a homomorphism.

$\ker \phi = A_n$, thus A_n is a normal subgroup of S_n.