HW 4

Charles Liu
Elementary Modern Algebra - Dr. Ben Clark
February 8th, 2024

---

1. Explain why the mapping $f(x) = 3x \bmod 10$ from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{10}$ is not a homomorphism.

Theorem. $f(x) = 3x \bmod 10$ from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{10}$ is *NOT* a homomorphism.
Proof:
If $f(x)$ from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{10}$ is a homomorphism, then $f(a) + f(b) = f(a+b)$ for $a, b \in \mathbb{Z}_{12}$. This is not the case however.
Take $a = 4 \in \mathbb{Z}_{12}$ and $b = 8 \in \mathbb{Z}_{12}$. We can solve that $f(a) + f(b) = (12 + 24) \bmod 10 = 6$ and $f(a+b) = f(12) = f(0) = 0$. Since $f(a) + f(b) = 6 \neq f(a+b) = 0$, the mapping $f(x)$ is not a homomorphism.

---

1. Prove that the mapping from $\mathbb{R}^*$ to, $\mathbb{R}^*$ defined by $\varphi(x) = |x|$, is a homomorphism with $\operatorname{Ker} \varphi = \{1, -1\}$.

Theorem. $\varphi(x) = |x|$ where $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ is a homomorphism with $\operatorname{Ker} \varphi = \{1, -1\}$.
Proof:
We can solve that $\varphi(ab) = |ab| = |a||b| = \varphi(a)\varphi(b)$, so φ is a homomorphism.

To find the kernel, we set $|x| = 1$. This means $x = \pm 1$, so $\operatorname{Ker} \varphi = \{1, -1\}$.

---

2. Prove that $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.

Theorem. $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.
Proof:
BWOC, assume that $\mathbb{Z}$ under addition is isomorphic to $\mathbb{Q}$ under addition. This means there

exists an isomorphic map $\varphi : \mathbb{Z} \to \mathbb{Q}$ with addition operation. This means there must also exist isomorphism $\phi : \mathbb{Q} \to \mathbb{Z}$.

Since ϕ is an isomorphism, the identity element 0 must map to itself. This means $\phi(0) = 0$.

Since ϕ is one-to-one, $\phi(1) \neq 0$.

Let $b \in \mathbb{N}$ where $b \neq 0$. Using the fact that ϕ is a homomorphism, we can solve that $\phi(1) = \phi(b \cdot \frac{1}{b}) = \phi(\frac{1}{b} + \frac{1}{b} \ldots + \frac{1}{b}) = b\phi(\frac{1}{b})$

This means $\phi(\frac{1}{b}) = \frac{1}{b}\phi(1)$
Take $b = |\phi(1)| + 1$. $\frac{1}{b}\phi(1)$ cannot be an integer, but $\phi(\frac{1}{b})$ must be an integer, a contradiction.

Thus, an isomorphism ϕ cannot exist, meaning φ cannot exist, and $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.

---

3. Prove that $\mathbb{Q}^+$ (positive rational numbers) under multiplication is isomorphic to a proper subgroup of itself.

Let $\phi(x) = x^2$ be a map from $\mathbb{Q}^+$ to H.

H is a proper subgroup, as rational elements which have irrational square roots are not contained, but H only has rational numbers.
$2 \notin H$ since $\sqrt{2} \notin \mathbb{Q}^+$, but $2 \in \mathbb{Q}^+$. This means H is proper.
If $x \in \mathbb{Q}^+$, then $x = \frac{p}{q}$ and $x > 0$. $x^2 = \frac{p^2}{q^2} \in \mathbb{Q}^+$, so $H \leq G$.

Let $a, b \in \mathbb{Q}^+$. We can solve that $\phi(a \times b) = ab \times ab = a^2 \times b^2 = \phi(a) \times \phi(b)$, so ϕ is a homomorphism.

Let $a, b \in \mathbb{Q}^+$. If $\phi(a) = \phi(b)$, we get that $a^2 = b^2$. Since $a, b > 0$, $a = b$, so ϕ is one-to-one.

Let $y \in \mathbb{Q}^+$. We can find that $\phi(x) = y$ where $x = \sqrt{y}$ and $x \in \mathbb{Q}^+$, so ϕ is onto.

Thus, ϕ is an isomorphism. Since an isomorphism exists between $\mathbb{Q}^+$ and a proper subgroup of $\mathbb{Q}^+$, H, $\mathbb{Q}^+$ under multiplication is isomorphic to a proper subgroup of itself.

---

1. Prove that the set of automorphisms with function composition of a group G forms a group.

Theorem. $\mathrm{Aut}(G)$ under operation function composition is a group.

Proof:

Closure

Let ϕ_1, ϕ_2 be automorphisms of a group G. This means $\phi_1 : G \to G$ and $\phi_2 : G \to G$.

Since ϕ_1 and ϕ_2 are both automorphisms, $\phi_1 \circ \phi_2$ also maps from G to G.

Since ϕ_1 and ϕ_2 are bijective, $\phi_1 \circ \phi_2$ is also bijective.

Let $a, b \in G$.
$\phi_1 \circ \phi_2(ab) = \phi_1(\phi_2(ab)) = \phi_1(\phi_2(a)\phi_2(b)) = \phi_1(\phi_2(a))(\phi_1(\phi_2(b))$
$= (\phi_1 \circ \phi_2(a))(\phi_1 \circ \phi_2(b))$

This means $\phi_1 \circ \phi_2 \in \mathrm{Aut}(G)$

Identity

Take $e : G \to G$, where $e(x) = x$.

Let $a, b \in G$. Since $e(ab) = ab = e(a)e(b)$, e is a homomorphism. If $\phi(a) = \phi(b)$, $a = b$ so e is one-to-one. For $y \in G$, we can find $x \in G$ $x = y$ and $y = \phi(x)$, so e is onto.

Thus, e is an isomorphism.
Since e maps from G to G, e is an automorphism.

Let $\phi \in \mathrm{Aut}(G)$.
Since $e \circ \phi = e(\phi) = \phi = \phi(e) = \phi \circ e$, e is the identity element of $\mathrm{Aut}(G)$.

Associativity

Let ϕ_1, ϕ_2, ϕ_3 be automorphisms of a group G. This means $\phi_1 : G \to G$, $\phi_2 : G \to G$, and $\phi_3 : G \to G$.

Since function composition is associative, $(\phi_1\phi_2)\phi_3 = \phi_1(\phi_2\phi_3)$ and associativity among elements in $\mathrm{Aut}(G)$ holds.

Inverse

Let $\phi \in \mathrm{Aut}(G)$. Because ϕ is an automorphism and is thus bijective, ϕ^{-1} must exist.
Since ϕ maps from $G \to G$, ϕ^{-1} must also be a bijective map from $G \to G$.
Let $a, b \in G$. We want to show that $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$.

We can solve that $\phi(\phi^{-1}(ab)) = ab$.
On the other side, we get that $\phi(\phi^{-1}(a)\phi^{-1}(b) = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) = ab$.

Because ϕ is one-to-one, $\phi^{-1}(ab)) = \phi^{-1}(a)\phi^{-1}(b)$, which means ϕ^{-1} is an isomorphism.

Because $\phi^{-1} : G \to G$ is isomorphic, it is an automorphism and $\phi^{-1} \in \mathrm{Aut}(G)$.

Since closure, identity, associativity, and inverse all hold, the set $\mathrm{Aut}(G)$ must be a group.

---

2. Let $\mathbb{R}^*$ be the group of nonzero real numbers under multiplication, and let r be a positive integer.

(a) Show that the mapping that takes x to x^r is a homomorphism from $\mathbb{R}^*$ to $\mathbb{R}^*$.

Theorem. $\phi(x) = x^r$ is a homomorphism from $\mathbb{R}^*$ to $\mathbb{R}^*$.
Proof:
$\phi(a \times b) = (a \times b)^r = a^r \times b^r = \phi(a) \times \phi(b)$, so ϕ is a homomorphism.

(b) Determine the kernel of this homomorphism.

Theorem. $\mathrm{Ker}(\phi) = \{1\}$ when r is odd, and $\mathrm{Ker}(\phi) = \{1, -1\}$ when r is even.

The identity element in $\mathbb{R}^*$ is 1.
Case 1: r is odd
The only element to the rth power that equals 1 is 1, so
$\mathrm{Ker}(\phi) = \{1\}$.
Case 2: r is even.
Both 1 and -1 to the rth power equal 1, so
$\mathrm{Ker}(\phi) = \{1, -1\}$

(c) Which values of r yield an isomorphism?

Theorem. $\phi(x) = x^r$ is an isomorphism from $\mathbb{R}^*$ to $\mathbb{R}^*$ if r is odd.

Proof:
As proved in *(a)*, ϕ is a homomorphism.

When $\mathrm{Ker}(\phi) = e$, ϕ is one-to-one. As proved in *(b)*, this only occurs when r is odd.

Let $y \in \mathbb{R}^*$. We can find $x = y^{\frac{1}{r}}$ where $\phi(x) = y$ and $x \in \mathbb{R}^*$, so ϕ is onto.

Thus, r is an isomorphism if r is odd.
