Isomorphism Problems

Problem1: Find an isomorphism from the group of integers under addition to the group of even integers under addition.

Solution: Define $\phi : \mathbb{Z} \to 2\mathbb{Z}$ by $\phi(n) = 2n$

- **One-to-one:** If $\phi(m) = \phi(n)$, then $2m = 2n$, so $m = n$ ✓
- **Onto:** For any even integer $2k \in 2\mathbb{Z}$, we have $\phi(k) = 2k$ ✓
- **Operation-preserving:**
  $\phi(m+n) = 2(m+n) = 2m + 2n = \phi(m) + \phi(n)$ ✓

Therefore ϕ is an isomorphism and $\mathbb{Z} \cong 2\mathbb{Z}$.

Problem2: Find $\mathbf{Aut}(\mathbb{Z})$ and $\mathbf{Aut}(\mathbb{Z}_6)$.

Solution: $\mathbf{Aut}(\mathbb{Z})$**:** Any automorphism ϕ of $\mathbb{Z}$ is determined by $\phi(1)$.

- $\phi(n) = n\phi(1)$ for all $n \in \mathbb{Z}$
- For ϕ to be onto, $\phi(1)$ must generate $\mathbb{Z}$
- Therefore $\phi(1) \in \{\pm 1\}$

Thus $\mathbf{Aut}(\mathbb{Z}) = \{\mathbf{id}, \phi_{-1}\}$ where $\phi_{-1}(n) = -n$. Therefore $|\mathbf{Aut}(\mathbb{Z})| = 2$ and $\mathbf{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$

$\mathbf{Aut}(\mathbb{Z}_6)$: ϕ is determined by $\phi(1)$, which must generate $\mathbb{Z}_6$

- $\phi(1) \in U(6) = \{1, 5\}$ (elements relatively prime to 6)
- $\phi_1(k) = k$ and $\phi_5(k) = 5k \bmod 6$

Thus $\mathbf{Aut}(\mathbb{Z}_6) = \{\phi_1, \phi_5\}$ and $|\mathbf{Aut}(\mathbb{Z}_6)| = 2$

Problem4: Show that $U(8) \ncong U(10)$. Show that $U(8) \cong U(12)$.

Solution: Part 1: $U(8) = \{1, 3, 5, 7\}$ and $U(10) = \{1, 3, 7, 9\}$

- $U(8)$: All elements have order ≤ 2: $1^2 \equiv 1$, $3^2 \equiv 1$, $5^2 \equiv 1$, $7^2 \equiv 1 \pmod 8$
- $U(10)$: Element 3 has order 4: $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 7$, $3^4 \equiv 1 \pmod{10}$

Since $U(8)$ is not cyclic while $U(10)$ is, we have $U(8) \ncong U(10)$.

Part 2: $U(12) = \{1, 5, 7, 11\}$

Define $\phi : U(8) \to U(12)$ by $\phi(1) = 1$; $\phi(3) = 5$; $\phi(5) = 7$; $\phi(7) = 11$. To see that ϕ is operation preserving we observe that:

- $\phi(1 \cdot a) = \phi(a) = \phi(a) \cdot 1 = \phi(a)\phi(1)$ for all a;
- $\phi(3 \cdot 5) = \phi(7) = 11 = 5 \cdot 7 = \phi(3)\phi(5)$;
- $\phi(3 \cdot 7) = \phi(5) = 7 = 5 \cdot 11 = \phi(3)\phi(7)$;
- $\phi(5 \cdot 7) = \phi(3) = 5 = 7 \cdot 11 = \phi(5)\phi(7)$.

Problem6: Prove that $\cong$ is an equivalence relation on groups.

Proof:

Reflexive: $G \cong G$

- The identity map $\mathrm{id}_G : G \to G$ defined by $\mathrm{id}_G(g) = g$ is an isomorphism

Symmetric: $G \cong H \implies H \cong G$

- If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ exists and is a bijection
- ϕ^{-1} preserves operations: for $a, b \in H$ with $\phi(x) = a, \phi(y) = b$, $\phi^{-1}(ab) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(a)\phi^{-1}(b)$

Transitive: $G \cong H$ and $H \cong K \implies G \cong K$

- If $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms, then $\psi \circ \phi : G \to K$ is an isomorphism
- $(\psi \circ \phi)(xy) = \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) = (\psi \circ \phi)(x)(\psi \circ \phi)(y)$

Problem7: Give three reasons why S_4 is not isomorphic to D_{12}.

Solution:

Reason 1: D_{12} has elements of order 12 e.g., R_{30} and S_4 has maximum element order = 4.

Reason 2: D_{12} has elements of order 6 e.g., R_{60} and S_4 has maximum element order = 4.

Reason 3: Center structure

Problem12: Prove that the mapping $\alpha : G \to G$ defined by $\alpha(g) = g^{-1}$ is an automorphism if and only if G is Abelian.

Proof: (⇒) Assume α is an automorphism: Since α preserves the operation, for all $a, b \in G$:
$\alpha(ab) = \alpha(a)\alpha(b)$
$(ab)^{-1} = a^{-1}b^{-1}$

But we also know $(ab)^{-1} = b^{-1}a^{-1}$ (always true in any group). Therefore $b^{-1}a^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Taking inverses of both sides: $(b^{-1}a^{-1})^{-1} = (a^{-1}b^{-1})^{-1}$, which gives $ab = ba$. So G is Abelian.

(⇐) Assume G is Abelian:

- α is clearly a bijection (since $(g^{-1})^{-1} = g$)
- Need to verify $\alpha(ab) = \alpha(a)\alpha(b)$:
  $\alpha(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \alpha(a)\alpha(b)$
  (using commutativity in the third equality)

Therefore $\alpha \in \mathrm{Aut}(G)$ ✓

Problem13: If g and h are elements from a group, prove that $\phi_g \circ \phi_h = \phi_{gh}$.

Proof: Recall: ϕ_g denotes the inner automorphism induced by g, defined by $\phi_g(x) = gxg^{-1}$

For any $x \in G$:

$$(\phi_g \circ \phi_h)(x) = \phi_g(\phi_h(x)) = \phi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(h^{-1}g^{-1})$$
$$= (gh)x(gh)^{-1} = \phi_{gh}(x)$$

Therefore $\phi_g \circ \phi_h = \phi_{gh}$

Note: This shows that the map $g \mapsto \phi_g$ is a homomorphism from G to $\mathrm{Aut}(G)$.

Problem15: Prove that the inner automorphisms $\phi_{R_0}, \phi_{R_{90}}, \phi_H$ and ϕ_D of D_4 are distinct.

Proof: Done in class.

Problem17: If G is a group, prove that $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups.

Proof: Done in class.

Problem31: Let $r \in U(n)$. Prove that the mapping $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\alpha(s) = sr \bmod n$ is an automorphism of $\mathbb{Z}_n$.

Proof: Done in class.

Problem41: Prove that $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.

Proof: $\mathbb{Z} = \langle 1 \rangle$ is cyclic. $\mathbb{Q}$ is not cyclic: Suppose $\mathbb{Q} = \langle q \rangle$ for some $q \in \mathbb{Q}$. Then $\frac{q}{2} \in \mathbb{Q}$, but there is no integer n such that $nq = \frac{q}{2}$ (this would require $n = \frac{1}{2} \notin \mathbb{Z}$).

Since isomorphisms preserve the cyclic property, $\mathbb{Z} \ncong \mathbb{Q}$

Problem43: Let $M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$. Prove that $\mathbb{C} \cong M$ under addition and $\mathbb{C}^* \cong M^*$ under multiplication.

Proof: Define $\phi : \mathbb{C} \to M$ by $\phi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

- **Bijection:** Clear from the one-to-one correspondence between $(a, b) \in \mathbb{R}^2$.

Addition isomorphism: Operation-preserving: For $z_1 = a + bi$ and $z_2 = c + di$:

$$\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix}$$

$$= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \phi(a+bi) + \phi(c+di)$$

Multiplication isomorphism: Operation-preserving: For $z_1 = a + bi$ and $z_2 = c + di$:

- $z_1 z_2 = (ac - bd) + (ad + bc)i$
- $\phi(z_1 z_2) = \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix}$
- Matrix multiplication:
$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -ad - bc \\ bc + ad & -bd + ac \end{bmatrix} = \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix}$$

Therefore $\phi(z_1 z_2) = \phi(z_1)\phi(z_2)$, so $\mathbb{C}^* \cong \ M^*$.

Problem45: Consider: "The order of a subgroup divides the order of the group." If you could prove this for finite permutation groups, would it be true for all finite groups?

Solution: YES, by Cayley's Theorem, every finite group G is isomorphic to a subgroup of some symmetric group S_n (specifically, $n = |G|$). More precisely: Since there exists an embedding $\phi : G \to S_{|G|}$ such that ϕ is an injective homomorphism, **Proof strategy:**

1. Let G be a finite group and $H \leq G$
2. By Cayley's Theorem, $G \cong \phi(G) \leq S_n$ for some permutation subgroup $\phi(G)$
3. The restriction $\phi|_H : H \to S_n$ gives $\phi(H) \leq \phi(G) \leq S_n$
4. If we know "$|K| \mid |L|$ whenever $K \leq L \leq S_n$", then:
   $|\phi(H)| \mid |\phi(G)|$
5. Since isomorphisms preserve order: $|H| = |\phi(H)|$ and $|G| = |\phi(G)|$
6. Therefore $|H| \mid |G|$

Problem47: Let G be a group and $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g equals the inner automorphism induced by zg.

Proof: Need to show: $\phi_g = \phi_{zg}$ for any $z \in Z(G)$. For any $x \in G$:

$\phi_{zg}(x) = (zg)x(zg)^{-1}$
$= (zg)x(g^{-1}z^{-1})$
$= z(gxg^{-1})z^{-1}$ (associativity)
$= (gxg^{-1})z \cdot z^{-1}$ (since $z \in Z(G)$, z commutes with gxg^{-1})
$= (gxg^{-1}) \cdot e$
$= gxg^{-1}$
$= \phi_g(x)$

Therefore $\phi_g = \phi_{zg}$ for all $z \in Z(G)$

Problem49: Suppose g and h induce the same inner automorphism. Prove that $h^{-1}g \in Z(G)$. Combine with Problem 47 for an "if and only if" theorem.

Proof: Done in class. Theorem: $\phi_g = \phi_h$ if and only if $h^{-1}g \in Z(G)$.

Problem51: If α and β are elements in S_n ($n \geq 3$), prove that $\phi_\alpha = \phi_\beta$ implies $\alpha = \beta$.

Solution: From Problem 49: $\phi_\alpha = \phi_\beta \iff \beta^{-1}\alpha \in Z(S_n)$. **Key fact:** For $n \geq 3$, $Z(S_n) = \{e\}$. Since $\beta^{-1}\alpha \in Z(S_n) = \{e\}$, we have $\beta^{-1}\alpha = e$, so $\alpha = \beta$

Problem53: Suppose ϕ and ψ are isomorphisms from a group G to itself (i.e., automorphisms). Prove that $H = \{g \in G \mid \phi(g) = \psi(g)\}$ is a subgroup of G.

Proof: We use the subgroup test (or verify the subgroup axioms):

1. Non-empty: $e \in H$ since $\phi(e) = e = \psi(e)$. Therefore $H \neq \emptyset$.

2. Closed under operation: Let $a, b \in H$. Then $\phi(a) = \psi(a)$ and $\phi(b) = \psi(b)$. We have $\phi(ab) = \phi(a)\phi(b) = \psi(a)\psi(b) = \psi(ab)$. Therefore $ab \in H$.

3. Closed under inverses: Let $a \in H$, so $\phi(a) = \psi(a)$. Taking inverses on both sides: $[\phi(a)]^{-1} = [\psi(a)]^{-1}$. Since ϕ and ψ are isomorphisms:
$\phi(a^{-1}) = [\phi(a)]^{-1} = [\psi(a)]^{-1} = \psi(a^{-1})$. Therefore $a^{-1} \in H$.

Problem56: Let ϕ be an automorphism of D_8. What are the possibilities for $\phi(R_{45})$?

Solution: D_8 has 8 rotations and 8 reflections, for a total of 16 elements and $|R_{45}| = 8$. Since automorphisms preserve element order: $|\phi(R_{45})| = |R_{45}| = 8$. Elements of order 8 in D_8: Since all reflections have order 2 need only to check rotations: Since the rotations form a cyclic group generated by R_{45} which has order 8, so $|R_{45}^k| = 8 \iff \gcd(k, 8) = 1$. Therefore $k \in \{1, 3, 5, 7\}$, giving:

- $R_{45}^1 = R_{45}$
- $R_{45}^3 = R_{135}$
- $R_{45}^5 = R_{225}$
- $R_{45}^7 = R_{315}$

Answer: $\phi(R_{45}) \in \{R_{45}, R_{135}, R_{225}, R_{315}\}$