Chapter 6: Isomorphisms

Motivation Examples We've Already Seen

Example 1: Symmetries of a Square

- Chapter 1: Geometric description $(R_{90}, R_{180}, H, V, \ldots)$
- Chapter 5: Permutation description (permutations of corners)
- **Same underlying group!**

Example 2: Cyclic Groups

- A cyclic group $\langle a \rangle$ of order n satisfies: $a^r \cdot a^s = a^k$ where $k = (r+s) \bmod n$
- This is essentially addition modulo n
- Both $U(43)$ and $U(49)$ are cyclic of order 42
- Each has the form $\langle a \rangle$ where $a^r \cdot a^s = a^{(r+s) \bmod 42}$

Exercise:

Which of the following groups looks like Z_4?

A) $U(10)$

B) $U(8)$

C) A_4

D) D_4

Multiple Choice

The Concept of Isomorphism

Etymology:

- Greek: *isos* = "same" or "equal"
- Greek: *morphe* = "form"
- Introduced by Galois ~190 years ago

Colorful Definition (R. Allenby):

"An algebraist is a person who can't tell the difference between isomorphic systems."

Intuition: Isomorphic groups are "the same" group in different notation.

Definition - Group Isomorphism

An **isomorphism** ϕ from a group G to a group $\bar{G}$ is a one-to-one onto mapping (function) from G to $\bar{G}$ that preserves the group operation. That is,

$\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

If there is an isomorphism from G onto $\bar{G}$, we say that G and $\bar{G}$ are **isomorphic** and write $G \approx \bar{G}$.

Understanding the Definition

Key Points:

1. **One-to-one:** If $\phi(a) = \phi(b)$, then $a = b$
2. **Onto:** For every $\bar{g} \in \bar{G}$, there exists $g \in G$ such that $\phi(g) = \bar{g}$
3. **Operation-preserving:** $\phi(ab) = \phi(a)\phi(b)$

Implicit in the definition:

- Isomorphic groups have the same order
- The operation on the left side of $\phi(ab) = \phi(a)\phi(b)$ is from G
- The operation on the right side is from $\bar{G}$

Four Steps to Prove Isomorphism To prove $G \approx \bar{G}$:

Step 1: "Mapping" Define a candidate function $\phi : G \to \bar{G}$

Step 2: "1-1" (One-to-one). Assume $\phi(a) = \phi(b)$ and prove $a = b$

Step 3: "Onto". For any $\bar{g} \in \bar{G}$, find $g \in G$ such that $\phi(g) = \bar{g}$

Step 4: "O.P." (Operation-Preserving). Show $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$

Example 1: $G = \mathbb{R}$ under addition, $\bar{G} = \mathbb{R}^+$ under multiplication. Claim: $G \approx \bar{G}$ via $\phi(x) = 2^x$.

Proof: Step 1 (Mapping): $\phi : \mathbb{R} \to \mathbb{R}^+$ defined by $\phi(x) = 2^x$

Step 2 (One-to-one): Assume $\phi(x) = \phi(y)$. Then $2^x = 2^y$. Taking $\log_2$ of both sides: $x = y$ ✓

Step 3 (Onto): Let $y \in \mathbb{R}^+$ (arbitrary). Need to find $x \in \mathbb{R}$ such that $\phi(x) = y$
That is, $2^x = y$. Solving: $x = \log_2 y$ ✓

Step 4 (Operation-Preserving): For all $x, y \in \mathbb{R}$:
$\phi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \phi(x)\phi(y)$ ✓

Conclusion: $\mathbb{R}$ under addition $\approx \mathbb{R}^+$ under multiplication

Example 2a - Infinite Cyclic Groups

Any infinite cyclic group is isomorphic to $\mathbb{Z}$.

Proof: Let $\langle a \rangle$ be an infinite cyclic group. Define $\phi : \langle a \rangle \to \mathbb{Z}$ by $\phi(a^k) = k$

- **Well-defined and one-to-one:** By Theorem 4.1, distinct powers of a are distinct elements
- **Onto:** For any $k \in \mathbb{Z}$, we have $\phi(a^k) = k$
- **Operation-preserving:** $\phi(a^k \cdot a^m) = \phi(a^{k+m}) = k + m = \phi(a^k) + \phi(a^m)$ ✓

Example 2b - finite Cyclic Groups

Any finite cyclic group $\langle a \rangle$ of order n is isomorphic to $\mathbb{Z}_n$.

Proof: Define $\phi : \langle a \rangle \to \mathbb{Z}_n$ by $\phi(a^k) = k \bmod n$

- By Theorem 4.1 and properties of modular arithmetic, this is an isomorphism

Example 3: When Operation-Preservation Fails. Consider $\phi : \mathbb{R} \to \mathbb{R}$ (both under addition) defined by $\phi(x) = x^3$.

Check:

- **One-to-one:** If $x^3 = y^3$, then $x = y$ ✓
- **Onto:** For any $y \in \mathbb{R}$, we have $\phi(\sqrt[3]{y}) = y$ ✓
- **Operation-preserving:** Is $\phi(x+y) = \phi(x) + \phi(y)$?

$$\phi(x+y) = (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$
$$\phi(x) + \phi(y) = x^3 + y^3$$

Since $(x+y)^3 \neq x^3 + y^3$ in general, ϕ is **NOT** operation-preserving. **Conclusion:** ϕ is NOT an isomorphism.

Example 4: $U(10) \approx \mathbb{Z}_4$ and $U(5) \approx \mathbb{Z}_4$. **Verification:**

$U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10
$U(5) = \{1, 2, 3, 4\}$ under multiplication modulo 5

Key Observations:

- $|U(10)| = 4$ and $U(10)$ is cyclic (generated by 3 or 7)
- $|U(5)| = 4$ and $U(5)$ is cyclic (generated by 2 or 3)
- $|\mathbb{Z}_4| = 4$ and $\mathbb{Z}_4$ is cyclic

By Example 2: Any cyclic group of order 4 is isomorphic to $\mathbb{Z}_4$. Therefore: $U(10) \approx \mathbb{Z}_4$ and $U(5) \approx \mathbb{Z}_4$. **Transitive property:** $U(10) \approx U(5)$

Example 5: There is NO isomorphism from $\mathbb{Q}$ (addition) to $\mathbb{Q}^*$ (multiplication)

Proof by Contradiction: Suppose $\phi : \mathbb{Q} \to \mathbb{Q}^*$ is an isomorphism. Then there exists $a \in \mathbb{Q}$ such that $\phi(a) = -1$. Now consider:

$$-1 = \phi(a) = \phi\left(\frac{a}{2} + \frac{a}{2}\right) = \phi\left(\frac{a}{2}\right) \cdot \phi\left(\frac{a}{2}\right) = \left[\phi\left(\frac{a}{2}\right)\right]^2$$

This says $\left[\phi\left(\frac{a}{2}\right)\right]^2 = -1$

But $\phi\left(\frac{a}{2}\right) \in \mathbb{Q}^*$, and no rational number squared equals -1! **Contradiction!**

Conclusion: No such isomorphism exists.

Example 6: Conjugation as an Isomorphism

Let $G = SL(2, \mathbb{R})$ = $\{2 \times 2$ real matrices with determinant $1\}$
Let $M \in G$ (any fixed matrix with determinant 1)

Define $\phi_M : G \to G$ by $\phi_M(A) = MAM^{-1}$ for all $A \in G$

Claim: ϕ_M is an isomorphism from G to itself.

Step 1 (Well-defined - maps G to G): For any $A \in G$: $\det(\phi_M(A)) = \det(MAM^{-1})$
$= \det(M) \cdot \det(A) \cdot \det(M^{-1}) = 1 \cdot 1 \cdot 1 = 1$. So $\phi_M(A) \in G$ ✓

Step 2 (One-to-one): Assume $\phi_M(A) = \phi_M(B)$.

- Then $MAM^{-1} = MBM^{-1}$
- Left-multiply by M^{-1}: $AM^{-1} = BM^{-1}$
- Right-multiply by M: $A = B$ ✓

Step 3 (Onto): Let $B \in G$ (arbitrary)

- Need to find $A \in G$ such that $\phi_M(A) = B$
- That is, $MAM^{-1} = B$
- Solving for A: $A = M^{-1}BM$

Verify: Since $\det(M^{-1}BM) = \det(M^{-1}) \cdot \det(B) \cdot \det(M) = 1$, we have $A \in G$

And: $\phi_M(A) = M(M^{-1}BM)M^{-1} = B$ ✓

Step 4 (Operation-Preserving): Let $A, B \in G$:

$$\phi_M(AB) = M(AB)M^{-1}$$
$$= MA(M^{-1}M)BM^{-1}$$
$$= MA(I)BM^{-1}$$
$$= (MAM^{-1})(MBM^{-1})$$
$$= \phi_M(A)\phi_M(B) \checkmark$$

Conclusion: ϕ_M is an isomorphism from G to G

Definition: ϕ_M is called **conjugation by** M

Properties of Isomorphisms - Two Major Theorems:

Theorem 6.1: Properties of Isomorphisms Acting on **Elements**

- 7 properties about how isomorphisms affect individual elements

Theorem 6.2: Properties of Isomorphisms Acting on **Groups**

- 6 properties about how isomorphisms affect group structure

Key Insight: Isomorphic groups have **all** group-theoretic properties in common.

Theorem 6.1: Properties of Isomorphisms Acting on Elements

Suppose ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then:

1. ϕ carries the identity of G to the identity of $\bar{G}$
2. For every integer n and for every group element $a \in G$: $\phi(a^n) = [\phi(a)]^n$ (Additive form: $\phi(na) = n\phi(a)$)
3. For any elements $a, b \in G$: a and b commute iff $\phi(a)$ and $\phi(b)$ commute
4. $G = \langle a \rangle$ if and only if $\bar{G} = \langle \phi(a) \rangle$
5. $|a| = |\phi(a)|$ for all $a \in G$ (isomorphisms preserve orders)
6. For fixed integer k and fixed $b \in G$: the equation $x^k = b$ has the same number of solutions in G as does $x^k = \phi(b)$ in $\bar{G}$
7. If G is finite, then G and $\bar{G}$ have exactly the same number of elements of every order

Theorem 6.1 - Proof Strategy

Dependencies Among Properties:

- Property 5 follows from properties 1 and 2
- Property 6 follows from property 2
- Property 7 follows from property 5

We will prove: Properties 1, 2, and 4

Notation: e = identity in G and $\bar{e}$ = identity in $\bar{G}$

Property 1: ϕ carries the identity of G to the identity of $\bar{G}$

Proof: We know $\phi(e) \in \bar{G}$ and $e = e \cdot e$. Therefore:

- $\bar{e} \cdot \phi(e) = \phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e)$

By right cancellation in $\bar{G}$: $\bar{e} = \phi(e)$ ✓. **Conclusion:** Isomorphisms map identity to identity.

Property 2: For every integer n and element $a \in G$: $\phi(a^n) = [\phi(a)]^n$

Proof for $n > 0$: By induction on n:

Base case ($n = 1$): $\phi(a^1) = \phi(a) = [\phi(a)]^1$ ✓

Inductive step: Assume $\phi(a^k) = [\phi(a)]^k$ for some $k \geq 1$. Then:

$$\begin{aligned}
\phi(a^{k+1}) &= \phi(a^k \cdot a) \\
&= \phi(a^k) \cdot \phi(a) \\
&= [\phi(a)]^k \cdot \phi(a) \\
&= [\phi(a)]^{k+1} \checkmark
\end{aligned}$$

By induction, the property holds for all positive integers n.

Proof for $n = 0$: $\phi(a^0) = \phi(e) = \bar{e} = [\phi(a)]^0$ ✓ (using Property 1)

Proof for $n < 0$: If $n < 0$, then $-n > 0$. From Property 1 and the positive case:

$$\bar{e} = \phi(e) = \phi(a^n \cdot a^{-n}) = \phi(a^n) \cdot \phi(a^{-n}) = \phi(a^n) \cdot [\phi(a)]^{-n}$$

Multiplying both sides on the right by $[\phi(a)]^n$: $[\phi(a)]^n = \phi(a^n)$ ✓

Conclusion: Property 2 holds for all integers n.

Property 4: $G = \langle a \rangle$ if and only if $\bar{G} = \langle \phi(a) \rangle$

Proof ($\Rightarrow$): Assume $G = \langle a \rangle$. First, by closure: $\langle \phi(a) \rangle \subseteq \bar{G}$.

Now let $\boldsymbol{b} \in \bar{G}$ be arbitrary. Since $\boldsymbol{\phi}$ is onto, there exists $\boldsymbol{a^k} \in \boldsymbol{G}$ such that $\boldsymbol{\phi(a^k) = b}$

By Property 2: $\boldsymbol{b = \phi(a^k) = [\phi(a)]^k}$. So $\boldsymbol{b \in \langle \phi(a) \rangle}$

Since $\boldsymbol{b}$ was arbitrary: $\boldsymbol{\bar{G} \subseteq \langle \phi(a) \rangle}$

Conclusion: $\bar{G} = \langle \phi(a) \rangle$ ✓

Proof (⇐): Assume $\bar{G} = \langle \phi(a) \rangle$. Clearly, $\langle a \rangle \subseteq G$.

Let $b \in G$ be arbitrary. Then $\phi(b) \in \bar{G} = \langle \phi(a) \rangle$. So for some integer k: $\phi(b) = [\phi(a)]^k$

By Property 2: $[\phi(a)]^k = \phi(a^k)$. Therefore: $\phi(b) = \phi(a^k)$

Since ϕ is one-to-one: $b = a^k$. Thus $b \in \langle a \rangle$

Since b was arbitrary: $G \subseteq \langle a \rangle$

Conclusion: $G = \langle a \rangle$ ✓

Important Corollary: Isomorphisms map generators to generators.

Theorem 6.2: Properties of Isomorphisms Acting on Groups

Suppose ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then:

1. ϕ^{-1} is an isomorphism from $\bar{G}$ onto G
2. G is Abelian if and only if $\bar{G}$ is Abelian
3. G is cyclic if and only if $\bar{G}$ is cyclic
4. If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\bar{G}$
5. If $\bar{K}$ is a subgroup of $\bar{G}$, then $\phi^{-1}(\bar{K}) = \{g \in G \mid \phi(g) \in \bar{K}\}$ is a subgroup of G
6. $\phi(Z(G)) = Z(\bar{G})$

Proof Strategy:

- Properties 1 and 4 are left as exercises (Exercises 17 and 34)
- **Property 2** (Abelian): Direct consequence of Property 3 of Theorem 6.1
  If $ab = ba$ for all $a, b \in G$, then $\phi(ab) = \phi(ba)$, so $\phi(a)\phi(b) = \phi(b)\phi(a)$
- **Property 3** (Cyclic): Follows from Property 4 of Theorem 6.1 and Property 1 of Theorem 6.2
- **Property 5**: Follows from Properties 1 and 4 of Theorem 6.2
- **Property 6** (Center): Direct consequence of Property 3 of Theorem 6.1
  $a \in Z(G)$ means a commutes with everything; $\phi(a)$ commutes with everything in $\bar{G}$

Key Insight: These properties show that isomorphic groups are indistinguishable from a group-theoretic perspective.

Using Theorems to Prove Non-Isomorphism

Five Methods to Prove $G \not\approx \bar{G}$: Strategy: Look for the easiest structural difference!

1. Show $|G| \neq |\bar{G}|$
2. Show one is cyclic and the other is not
3. Show one is Abelian and the other is not
4. Show the largest order of any element differs
5. Show the number of elements of some specific order differs

Example: Consider $\mathbb{Z}_{12}$, D_6, and A_4 (all have order 12)

Method 1: Largest element order

- $\mathbb{Z}_{12}$: Largest order = 12 (e.g., $|1| = 12$)
- D_6: Largest order = 6 (rotations $R_{60}, R_{120}, \ldots$)
- A_4: Largest order = 3 (e.g., (123) has order 3)

Since $12 \neq 6 \neq 3$: **No two are isomorphic**

Method 2: Number of elements of order 2

- $\mathbb{Z}_{12}$: Only $\{6\}$ has order 2 → **1 element**
- D_6: Reflections and R_{180} → **7 elements**
- A_4: Elements like $(12)(34), (13)(24), (14)(23)$ → **3 elements**

Since $1 \neq 7 \neq 3$: **No two are isomorphic**

Exercise:

Which property can be used to prove that $\mathbb{Z}_6 \not\approx S_3$?

A) $\mathbb{Z}_6$ is abelian but S_3 is not

B) $\mathbb{Z}_6$ has 6 elements but S_3 has 5 elements

C) $\mathbb{Z}_6$ is cyclic but S_3 is infinite

D) $\mathbb{Z}_6$ has no elements of order 2

Multiple Choice

Example: $\mathbb{Q}$ under addition vs. $\mathbb{Q}^*$ under multiplication

Analysis:

In $\mathbb{Q}$ (addition):

- Every non-identity element has infinite order
- For any $x \neq 0$: $nx = 0$ iff $n = 0$ or $x = 0$
- So if $x \neq 0$, then $|x| = \infty$

In $\mathbb{Q}^*$ (multiplication):

- The element -1 has finite order: $|-1| = 2$
- Because $(-1)^2 = 1$

Conclusion: The groups have different element order structures. By Property 5 of Theorem 6.1: $\mathbb{Q} \not\approx \mathbb{Q}^*$

Two main applications of Isomorphisms:

1. Simplify difficult problems

- Question about complicated group G
- Find simpler isomorphic group $\bar{G}$
- Answer question about $\bar{G}$ instead
- Answer applies to G!

2. Provide concrete realizations

- Abstract group G
- Find concrete isomorphic group $\bar{G}$
- Better intuition and computation

Coming attractions: Chapters 8 and 11 will have many examples!

Definition: An isomorphism from a group G onto **itself** is called an **automorphism** of G.

Example (Complex Conjugation): Define $\phi : \mathbb{C} \to \mathbb{C}$ by $\phi(a + bi) = a - bi$. Show that ϕ is an automorphism of $\mathbb{C}$ under addition.

Proof:

- **One-to-one:** If $a - bi = c - di$, then $a = c$ and $b = d$
- **Onto:** For any $c + di$, we have $\phi(c - di) = c + di$
- **Operation-preserving:**
  $\phi((a + bi) + (c + di)) = \phi((a + c) + (b + d)i)$
  $= (a + c) - (b + d)i = (a - bi) + (c - di)$
  $= \phi(a + bi) + \phi(c + di)$

Example (Reflection Automorphism of $\mathbb{R}^2$): Let $\mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}$ under componentwise addition. Define $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ by $\phi(a,b) = (b,a)$. Show that ϕ is an automorphism of $\mathbb{R}^2$.

Proof:

- **One-to-one:** If $(b,a) = (d,c)$, then $b = d$ and $a = c$
- **Onto:** $\phi(b,a) = (a,b)$ for any (a,b)
- **Operation-preserving:** $\phi((a_1,b_1) + (a_2,b_2)) = \phi(a_1 + a_2, b_1 + b_2)$
  $= (b_1 + b_2, a_1 + a_2) = (b_1,a_1) + (b_2,a_2) = \phi(a_1,b_1) + \phi(a_2,b_2)$

General fact: Any reflection across a line through the origin or rotation about the origin is an automorphism of $\mathbb{R}^2$.

Linear algebra connection: Every invertible linear transformation of vector space V to itself is an automorphism

Definition (Inner Automorphism Induced by a): Let G be a group and $a \in G$. The function $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ for all $x \in G$ is called the **inner automorphism of G induced by a**.

Note: This is conjugation by a (generalization of Example 6)

Verification that ϕ_a is an automorphism: (Similar to Example 6)

- One-to-one: If $axa^{-1} = aya^{-1}$, then $x = y$ by cancellation
- Onto: For any $y \in G$, we have $\phi_a(a^{-1}ya) = y$
- Operation-preserving: $\phi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$

Example (Inner Automorphism of D_4 induced by R_{90}) Recall $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$. $\phi_{R_{90}}$ acts as follows:

x	$\phi_{R_{90}}(x) = R_{90} \cdot x \cdot R_{90}^{-1}$	**Result**
R_0	$R_{90}R_0R_{90}^{-1} = R_{90}R_0R_{270}$	R_0
R_{90}	$R_{90}R_{90}R_{90}^{-1} = R_{90}R_{90}R_{270}$	R_{90}
R_{180}	$R_{90}R_{180}R_{90}^{-1} = R_{90}R_{180}R_{270}$	R_{180}
R_{270}	$R_{90}R_{270}R_{90}^{-1} = R_{90}R_{270}R_{270}$	R_{270}
H	$R_{90}HR_{90}^{-1} = R_{90}HR_{270}$	V
V	$R_{90}VR_{90}^{-1} = R_{90}VR_{270}$	H
D	$R_{90}DR_{90}^{-1} = R_{90}DR_{270}$	D'
D'	$R_{90}D'R_{90}^{-1} = R_{90}D'R_{270}$	D

Observation: Rotations are fixed; reflections are permuted

Theorem 6.3: $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are Groups.

Proof: (Left as Exercise 17, but outline provided)

For $\mathrm{Aut}(G)$:

- **Closure:** If $\phi, \psi \in \mathrm{Aut}(G)$, then $\phi \circ \psi$ is an automorphism
- **Associativity:** Function composition is associative
- **Identity:** The identity function $\mathbf{id}(x) = x$ is in $\mathrm{Aut}(G)$
- **Inverses:** If $\phi \in \mathrm{Aut}(G)$, then $\phi^{-1} \in \mathrm{Aut}(G)$ (Property 1 of Theorem 6.2)

For $\mathrm{Inn}(G)$:

- Note that $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$ is not empty Identity: $\phi_e = \mathbf{id}$. So need to varify
  - Closed under composition: Follows from $\phi_a \circ \phi_b = \phi_{ab}$ (can be verified directly)
  - Closed under Inverses: $(\phi_a)^{-1} = \phi_{a^{-1}}$

Exercise:

Which of the following is **always** true about $\mathrm{Inn}(G)$?

A) $\mathrm{Inn}(G) = \mathrm{Aut}(G)$ for every group G
B) $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$
C) $\mathrm{Inn}(G)$ is empty if G is abelian
D) $\mathrm{Inn}(G)$ contains exactly $|G|$ distinct automorphisms

Multiple Choice

General Strategy for Computing $\mathrm{Inn}(G)$:

If $G = \{e, a, b, c, \ldots\}$, then $\mathrm{Inn}(G) = \{\phi_e, \phi_a, \phi_b, \phi_c, \ldots\}$. **But:** This list may have duplicates!

- ϕ_a may equal ϕ_b even though $a \neq b$
- This happens when $axa^{-1} = bxb^{-1}$ for all $x \in G$
- Equivalently: when $ab^{-1} \in Z(G)$

Task: Identify which distinct elements give distinct automorphisms

Note: Determining $\mathrm{Aut}(G)$ is generally much harder than determining $\mathrm{Inn}(G)$

General Strategy for Computing $\mathrm{Inn}(G)$:

If $G = \{e, a, b, c, \ldots\}$, then $\mathbf{Inn}(G) = \{\phi_e, \phi_a, \phi_b, \phi_c, \ldots\}$. **But:** This list may have duplicates! ϕ_a may equal ϕ_b even though $a \neq b$. This happens when

- $axa^{-1} = bxb^{-1}$ for all $x \in G$. Equivalently, $a^{-1}bxb^{-1}a = x$ for all $x \in G$.
- Equivalently, $(a^{-1}b)x(a^{-1}b)^{-1} = x$ for all $x \in G$. Equivalently, $(a^{-1}b)x = x(a^{-1}b)$ for all $x \in G$. Equivalently: when $a^{-1}b \in Z(G)$.
- **So**: $\phi_a = \phi_b$ ***iff*** there exists $z \in Z(G)$ such that $b = az$.

Task: Identify which distinct elements give distinct automorphisms

Note: Determining $\mathbf{Aut}(G)$ is generally much harder than determining $\mathbf{Inn}(G)$

Example: Computing $\mathrm{Inn}(D_4)$

Step 1: List all candidates. $\textbf{Candidates: } \phi_{R_0}, \phi_{R_{90}}, \phi_{R_{180}}, \phi_{R_{270}}, \phi_H, \phi_V, \phi_D, \phi_{D'}$.

Step 2: Compute $Z(D_4) = \{R_0, R_{180}\}$.

Step 3: Multiply by R_{180}

- Since $R_0 R_{180} = R_{180}$, then $\phi_{R_{180}} = \phi_{R_0}$
- Since $R_{90} \cdot R_{180} = R_{270}$, then $\phi_{R_{270}} = \phi_{R_{90}}$.
- Since $V R_{180} = H$, then $\phi_H = \phi_V$.
- Since $D R_{180} = D'$, then $\phi_{D'} = \phi_D$.

Therefore, $\mathrm{Inn}(D_4) = \{\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D\}$.

Exercise:

If G is an abelian group, then we must have

A) $\mathrm{Inn}(G) = \mathrm{Aut}(G)$

B) $\mathrm{Inn}(G) \approx Z(G)$

C) $|\mathrm{Inn}(G)| = 1$

D) $|\mathrm{Inn}(G)| = |G|$

Multiple Choice

Theorem 6.4: For every positive integer n: $\text{Aut}(\mathbb{Z}_n) \approx U(n)$.

Proof:

- Any $\alpha \in \text{Aut}(\mathbb{Z}_n)$ is determined by $\alpha(1)$
- We have $\alpha(k) = k\alpha(1)$ for all $k \in \mathbb{Z}_n$
- By Property 5 of Theorem 6.1: $|\alpha(1)| = |1| = n$
- So $\alpha(1) \in U(n)$ (elements of order n are exactly the generators)

Define: $T : \text{Aut}(\mathbb{Z}_n) \to U(n)$ by $T(\alpha) = \alpha(1)$

T **is one-to-one:** Suppose $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}_n)$ with $T(\alpha) = T(\beta)$. Then $\alpha(1) = \beta(1)$.

- For any $k \in \mathbb{Z}_n$: $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$. Therefore $\alpha = \beta$ ✓

T **is onto:** Let $r \in U(n)$ (arbitrary). Define $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\alpha(s) = sr \pmod{n}$ for all $s \in \mathbb{Z}_n$. **Claim:** $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$:

- **Well-defined:** If $s \equiv s' \pmod{n}$, then $sr \equiv s'r \pmod{n}$
- **One-to-one:** If $sr \equiv tr \pmod{n}$, then $s \equiv t \pmod{n}$ (since $\gcd(r, n) = 1$)
- **Onto:** For any $k \in \mathbb{Z}_n$, solve $sr \equiv k \pmod{n}$ for s (possible since $\gcd(r, n) = 1$)
- **Operation-preserving:** $\alpha(s + t) = (s + t)r = sr + tr = \alpha(s) + \alpha(t)$

So $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$ and $T(\alpha) = \alpha(1) = r$ ✓

T **is operation-preserving:** Let $\alpha, \beta \in \mathbf{Aut}(\mathbb{Z}_n)$. Then:

$$T(\alpha \circ \beta) = (\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1) \text{ times}})$$

$$= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1) \text{ times}} = \alpha(1) \cdot \beta(1) = T(\alpha) \cdot T(\beta)$$

(where the last multiplication is in $U(n)$)

Conclusion: T is an isomorphism, so $\mathbf{Aut}(\mathbb{Z}_n) \approx U(n)$

Exercise:

Using Theorem 6.4, what is $|\mathbf{Aut}(\mathbb{Z}_{10})|$?

A) 10

B) 5

C) 4

D) 2

Multiple Choice

Theorem 6.5 (Cayley's Theorem): Every group is isomorphic to a group of permutations.

Strategy of proof:

- Start with arbitrary group G
- Construct a specific group $\bar{G}$ of permutations
- Prove $G \approx \bar{G}$

Proof: Let G be any group.

Step 1: Construct permutations from G: For each $g \in G$, define a function

- $T_g : G \to G$ by $T_g(x) = gx$ for all $x \in G$. **In words:** T_g is "left multiplication by g"

Claim: Each T_g is a permutation of G (i.e., a bijection from G to G):

- One-to-one: If $gx = gy$, then $x = y$ by cancellation
- Onto: For any $y \in G$, we have $T_g(g^{-1}y) = g(g^{-1}y) = y$

Step 2: Form the group of permutations: Let $\bar{G} = \{T_g \mid g \in G\}$

Claim: $\bar{G}$ is a group under function composition:

- **Closure:** For any $g, h \in G$:
  $(T_g \circ T_h)(x) = T_g(T_h(x)) = T_g(hx) = g(hx) = (gh)x = T_{gh}(x)$ So $T_g \circ T_h = T_{gh} \in \bar{G}$
- **Identity:** T_e is the identity function (since $T_e(x) = ex = x$)
- **Inverses:** $(T_g)^{-1} = T_{g^{-1}}$ (because $T_g \circ T_{g^{-1}} = T_{gg^{-1}} = T_e$)
- **Associativity:** Function composition is always associative

Step 3: Define the isomorphism: Define $\phi : G \to \bar{G}$ by $\phi(g) = T_g$ for all $g \in G$

- **one-to-one:** Suppose $\phi(g) = \phi(h)$. Then $T_g = T_h$. So $T_g(e) = T_h(e)$. Thus $ge = he$, which gives $g = h$.
- **onto:** By construction, for every $T_g \in \bar{G}$, we have $\phi(g) = T_g$.
- **operation-preserving:** For any $a, b \in G$, $\phi(ab) = T_{ab}$. We showed earlier that $T_{ab} = T_a \circ T_b$. Therefore: $\phi(ab) = T_a \circ T_b = \phi(a) \circ \phi(b)$

Conclusion: ϕ is an isomorphism from G to $\bar{G}$, where $\bar{G}$ is a group of permutations.

Definition: The group $\bar{G}$ is called the **left regular representation** of G.

Explicit Computation $U(12) = \{1, 5, 7, 11\}$ under multiplication modulo 12. Compute permutations in array form:

$$T_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix}$$

$$T_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}$$

$$T_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}$$

$$T_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix}$$

Explanation: $T_5(1) = 5 \cdot 1 = 5$, $T_5(5) = 5 \cdot 5 = 25 \equiv 1 \pmod{12}$, etc.

Cayley Tables Comparison

Cayley Table for $U(12)$:

$\cdot$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Cayley Table for $\overline{U(12)}$:

$\circ$	T_1	T_5	T_7	T_{11}
T_1	T_1	T_5	T_7	T_{11}
T_5	T_5	T_1	T_{11}	T_7
T_7	T_7	T_{11}	T_1	T_5
T_{11}	T_{11}	T_7	T_5	T_1

Observation: The tables are identical (up to notation)!

Two sophisticated isomorphism results:

Theorem (advanced): $(\mathbb{R}, +) \approx (\mathbb{C}, +)$

The real numbers under addition are isomorphic to the complex numbers under addition!

Theorem (advanced): $(\mathbb{C}^*, \cdot) \approx (S^1, \cdot)$

The nonzero complex numbers under multiplication are isomorphic to the unit circle under multiplication.