CHAPTER 6

Isomorphisms

A while back, we saw that \( \langle a \rangle \) with \( |\langle a \rangle| = 42 \) and \( \mathbb{Z}_{42} \) had basically the same structure, and said the groups were “isomorphic,” in some sense the same.

**Definition** (Group Isomorphism). An **isomorphism** \( \phi \) from a group \( G \) to a group \( \overline{G} \) is a 1–1 mapping from \( G \) onto \( \overline{G} \) that preserves the group operation. That is,

\[
\phi(ab) = \phi(a)\phi(b) \quad \forall \ a, b \in G.
\]

If there is an isomorphism from \( G \) onto \( \overline{G} \), we say \( G \) and \( \overline{G} \) are **isomorphic** and write \( G \cong \overline{G} \).

**Note.** The operations in \( G \) and \( \overline{G} \) may be different. The operation to the left of “=” is in \( G \), while that on the right is in \( \overline{G} \).

<table>
<thead>
<tr>
<th>( G ) Operation</th>
<th>( \overline{G} ) Operation</th>
<th>Operation Preservation</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \cdot )</td>
<td>( \cdot )</td>
<td>( \phi(a \cdot b) = \phi(a) \cdot \phi(b) )</td>
</tr>
<tr>
<td>( \cdot )</td>
<td>( + )</td>
<td>( \phi(a \cdot b) = \phi(a) + \phi(b) )</td>
</tr>
<tr>
<td>( + )</td>
<td>( \cdot )</td>
<td>( \phi(a + b) = \phi(a) \cdot \phi(b) )</td>
</tr>
<tr>
<td>( + )</td>
<td>( + )</td>
<td>( \phi(a + b) = \phi(a) + \phi(b) )</td>
</tr>
</tbody>
</table>
To establish an isomorphism:

1. Define \( \phi : G \rightarrow \overline{G} \).
2. Show \( \phi \) is 1–1: assuming \( \phi(a) = \phi(b) \), show \( a = b \).
3. Show \( \phi \) is onto: \( \forall \overline{g} \in \overline{G} \). show \( \exists g \in G \implies \phi(g) = \overline{g} \).
4. Show \( \phi(ab) = \phi(a)\phi(b) \) \( \forall a, b \in G \).

**Example.** With \( |a| = 42 \), show \( \langle a \rangle \approx \mathbb{Z}_{42} \).

**Proof.**

Define \( \phi : \langle a \rangle \rightarrow \mathbb{Z}_{42} \) by \( \phi(a^n) = n \mod 42 \).

[Show 1–1.] Suppose \( \phi(a^n) = \phi(a^m) \). Then

\[
  n = m \mod 42 \implies 42 | n - m \implies a^n = a^m
\]

by Theorem 4.1. Thus \( \phi \) is 1–1.

[Show onto.] For all \( n \in \mathbb{Z}_{42} \), \( a^n \in \langle a \rangle \) and \( \phi(a^n) = n \), so \( \phi \) is onto.

[Show operation preservation.] For all \( a^n, a^m \in \langle a \rangle \),

\[
  \phi(a^n a^m) = \phi(a^{n+m}) = n + m \mod 42 = n \mod 42 + m \mod 42 = \phi(a^n) + \phi(a^m).
\]

Thus, by definition, \( \langle a \rangle \approx \mathbb{Z}_{42} \). \( \square \)

**Example.** Any finite cyclic group \( \langle a \rangle \) with \( |\langle a \rangle| = n \) is isomorphic to \( \mathbb{Z}_n \) under \( \phi(a^k) = k \mod n \). The proof of this is identical to that of the previous example.
EXAMPLE. Let $G$ be the positive real numbers with multiplication and $\overline{G}$ be the group of real numbers with addition. Show $G \cong \overline{G}$.

PROOF.

Define $\phi : G \to \overline{G}$ by $\phi(x) = \ln(x)$.

[Show 1–1.] Suppose $\phi(x) = \phi(y)$. Then

$$\ln(x) = \ln(y) \implies e^{\ln(x)} = e^{\ln(y)} \implies x = y,$$

so $\phi$ is 1–1.

[Show onto] Now suppose $x \in \overline{G}$. $e^x > 0$ and $\phi(e^x) = \ln e^x = x$, so $\phi$ is onto.

[Show operation preservation.] Finally, for all $x, y \in G$,

$$\phi(xy) = \ln(xy) = \ln x + \ln y = \phi(x) + \phi(y),$$

so $G \cong \overline{G}$.

[Question: is $\phi$ the only isomorphism?]

EXAMPLE. Any infinite cyclic group is isomorphic to $\mathbb{Z}$ with addition. Given $\langle a \rangle$ with $|a| = \infty$, define $\phi(a^k) = k$. The map is clearly onto. If $\phi(a^n) = \phi(a^m)$, $n = m \implies a^n = a^m$, so $\phi$ is 1–1. Also,

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

so $\langle a \rangle \cong \mathbb{Z}$.

Consider $\langle 2 \rangle$ under addition, the cyclic group of even integers. The $\langle 2 \rangle \cong \mathbb{Z} = \langle 1 \rangle$ with $\phi : \langle 2 \rangle \to \mathbb{Z}$ defined by $\phi(2n) = n$. 
EXAMPLE. Let $G$ be the group of real numbers under addition and $\overline{G}$ be the group of positive numbers under multiplication. Define $\phi(x) = 2^{x-1}$. $\phi$ is 1–1 and onto but

$$\phi(1+2) = \phi(3) = 4 \neq 2 = 1 \cdot 2 = \phi(1)\phi(2),$$

so $\phi$ is not an isomorphism.

Can this mapping be adjusted to make it an isomorphism?

Use $\phi(x) = 2^x$.

If $\phi(x) = \phi(y)$, $2^x = 2^y \implies \log_2 2^x = \log_2 2^y \implies x = y$, so $\phi$ is 1–1.

Given any positive $y$, $\phi(\log_2 y) = 2^{\log_2 y} = y$, so $\phi$ is onto.

Also, for all $x, y \in \mathbb{R}, \phi(x+y) = 2^{x+y} = 2^x2^y = \phi(x)\phi(y)$.

Thus $\phi$ is an isomorphism.

EXAMPLE. Are $U(8)$ and $U(12)$ isomorphic?

SOLUTION.

$U(8) = \{1, 3, 5, 7\}$ is noncyclic with $|3| = |5| = |7| = 2$.

$U(12) = \{1, 5, 7, 11\}$ is noncyclic with $|5| = |7| = |11| = 2$.

Define $\phi : U(8) \to U(12)$ by $1 \to 1, \ 3 \to 5, \ 5 \to 7, \ 7 \to 11$.

$\phi$ is clearly 1–1 and onto. Regarding operation preservation:

$\phi(3 \cdot 5) = \phi(7) = 11$ and $\phi(3)\phi(5) = 5 \cdot 7 = 11$.

$\phi(3 \cdot 7) = \phi(5) = 7$ and $\phi(3)\phi(7) = 5 \cdot 11 = 7$.

$\phi(5 \cdot 7) = \phi(3) = 5$ and $\phi(5)\phi(7) = 7 \cdot 11 = 5$.

$\phi(1 \cdot 3) = \phi(3) = 5$ and $\phi(1)\phi(3) = 1 \cdot 5 = 5$.

etc.

Since both groups are Abelian, we need only check each pair in a single order. Thus, $U(8) \cong U(12)$. 

$\square$
This group of order 4, with all non-identity element of order 2, is called the Klein 4 group. Any other group of order 4 must have an element of order 4, so is cyclic and isomorphic to $\mathbb{Z}_4$.

For orders 1, 2, 3, 5, there are only the cyclic groups $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_5$.

**Problem (Page 140 # 36).**

Let $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Q} \right\}$. Show that $G$ and $H$ are isomorphic under addition. Prove that $G$ and $H$ are closed under multiplication. Does your isomorphism preserve multiplication as well as addition? ($G$ and $H$ are examples of rings — a topic we begin in Chapter 12)

**Solution.**

Given $a + b\sqrt{2}, c + d\sqrt{2} \in G$.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in G$$

and

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in G$$

since $(a + c), (b + d), (ac + 2bd), (ad + bc) \in \mathbb{Q}$.

Also, if $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, $\begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \in H$,

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix}$$

and

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{bmatrix} \in H$$

since $(a + c), (b + d), (ac + 2bd), ad + bc \in \mathbb{Q}$.

Thus $G$ and $H$ are closed under both addition and multiplication. Also, $G$ and $H$ are groups under addition (you can prove this, if you desire).
Define $\phi : G \to H$ by $\phi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$.

Suppose $\phi(a + b\sqrt{2}) = \phi(c + d\sqrt{2})$. Then $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \implies a = c$ and $b = d \implies a + b\sqrt{2} = c + d\sqrt{2} \implies \phi$ is 1-1.

For $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \in H$, $a + b\sqrt{2} \in G$ and $\phi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, so $\phi$ is onto.

Now suppose $a + b\sqrt{2}, c + d\sqrt{2} \in G$. Then

$$
\phi((a + b\sqrt{2}) + (c + d\sqrt{2})) = \phi((a + c) + (b + d)\sqrt{2}) = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix} = \begin{bmatrix} a + c & 2b + 2d \\ b + d & a + c \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2}).
$$

Thus $\phi$ is an isomorphism under addition.

Also,

$$
\phi((a + b\sqrt{2})(c + d\sqrt{2})) = \phi((ac + 2bd) + (ad + bc)\sqrt{2}) = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{bmatrix} = \begin{bmatrix} ac + 2bd & 2ad + 2bc \\ ad + bc & ac + 2bd \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = (\phi(a + b\sqrt{2}))(\phi(c + d\sqrt{2})).
$$

So $\phi$ preserves multiplication also. (We will later see that this makes $\phi$ a ring homomorphism.)

\[\square\]
Problem (Page 141 # 54). Consider $G = \langle m \rangle$ and $H = \langle n \rangle$ where $m, n \in \mathbb{Z}$. These are groups under addition. Show $G \approx H$. Does this isomorphism also preserve multiplication?

Solution.

Define $\phi : G \to H$ by $\phi(x) = \frac{n}{m}x$. Suppose $\phi(x) = \phi(y)$. Then

$$\frac{n}{m}x = \frac{n}{m}y \implies x = y \implies \phi \text{ is } 1-1.$$

For $x \in H$, $x = rn$ where $r \in \mathbb{Z}$. Then $\frac{m}{n}x = \frac{m}{n}rn = rm \in G$. Then

$$\phi \left( \frac{m}{n}x \right) = \frac{n}{m} \left( \frac{m}{n}x \right) = x,$$

so $\phi$ is onto. Now, suppose $x, y \in G$. Then

$$\phi(x + y) = \frac{n}{m}(x + y) = \frac{n}{m}x + \frac{n}{m}y = \phi(x) + \phi(y),$$

so addition is preserved and $G \approx H$. But,

$$\phi(xy) = \frac{n}{m}(xy) \neq \left( \frac{n}{m}x \right) \left( \frac{n}{m}y \right) = \phi(x)\phi(y),$$

so multiplication is not preserved by $\phi$. \qed
Theorem (3). $\cong$ is an equivalence relation on the set $\mathcal{G}$ of all groups.

Proof.

(1) $G \cong G$. Define $\phi : G \to G$ by $\phi(x) = x$. This is clear.

(2) Suppose $G \cong H$. If $\phi : G \to H$ is the isomorphism and, for $g \in G$, $\phi(g) = h$, then $\phi^{-1} : H \to G$ where $\phi^{-1}(h) = g$ is 1–1 and onto.

Suppose $a, b \in H$. Since $\phi$ is onto, $\exists \alpha, \beta \in G \ni \phi(\alpha) = a$ and $\phi(\beta) = b$. Then $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta) = ab$, so

$$\phi^{-1}(ab) = \phi^{-1}(\phi(\alpha)\phi(\beta)) = \phi^{-1}(\phi(\alpha\beta)) = \alpha\beta = \phi^{-1}(\phi(\alpha))\phi^{-1}(\phi(\beta)) = \phi^{-1}(a)\phi^{-1}(b).$$

Thus $\phi^{-1}$ is an isomorphism and $H \cong G$.

(3) Suppose $G \cong H$ and $H \cong K$ with $\phi : G \to H$ and $\psi : H \to K$ the isomorphisms. Then $\psi\phi : G \to K$ is 1–1 and onto.

For all $a, b \in G$,

$$(\psi\phi)(ab) = \psi[\phi(ab)] = \psi[\phi(a)\phi(b)] = \psi[\phi(a)]\psi[\phi(b)] = [\psi\phi)(a)][(\psi\phi)(b)].$$

Thus $G \cong K$ and $\cong$ is an equivalence relation on $\mathcal{G}$. \hfill \Box

Note. Thus, when two groups are isomorphic, they are in some sense equal. They differ in that their elements are named differently. Knowing of a computation in one group, the isomorphism allows us to perform the analogous computation in the other group.
Example (Conjugation by $a$). Let $G$ be a group, $a \in G$. Define a function

$\phi_a : G \to G$ by $\phi_a(x) = axa^{-1}$.

Suppose $\phi_a(x) = \phi_a(y)$. Then $axa^{-1} = aya^{-1} \implies x = y$ by left and right cancellation. Thus $\phi_a$ is 1–1.

Now suppose $y \in G$. We need to find $x \in G$ s.t. $axa^{-1} = y$. But that will be so if $x = a^{-1}ya$, for then

$$\phi_a(x) = \phi_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = (aa^{-1})y(aa^{-1}) = eye = y,$$

so $\phi_a$ is onto.

Finally, for all $x, y \in G$,

$$\phi_a(xy) = axya^{-1} = axeya^{-1} = axa^{-1}aya^{-1} = \phi_a(x)\phi_a(y).$$

Thus $\phi_a$ is an isomorphism from $G$ onto $G$.

Recall $U(8) = \{1, 3, 5, 7\}$. Consider $\phi_7$. Since 7 is its own inverse,

$$\phi_7(1) = 7 \cdot 1 \cdot 7 = 1,$$

$$\phi_7(3) = 7 \cdot 3 \cdot 7 = 5 \cdot 7 = 3,$$

$$\phi_7(5) = 7 \cdot 5 \cdot 7 = 3 \cdot 7 = 5,$$

$$\phi_7(7) = 7 \cdot 7 \cdot 7 = 1 \cdot 7 = 7.$$

Conjugation by 7 turns out to be the identity isomorphism, which is not very interesting.
Theorem (6.1 — Cayley’s Theorem). Every group is isomorphic to a group of permutations.

Proof.
Let $G$ be any group. [We need to find a set $A$ and a permutation on $A$ that forms a group $\overline{G}$ that is isomorphic to $G$.] We take the set $G$ and define, for each $g \in G$, the function $T_g : G \rightarrow G$ by $T_g(x) = gx \ \forall x \in G$.

Now $T_g(x) = T_g(y) \implies gx = gy \implies x = y$ by left cancellation, so $T_g$ is 1–1.

Given $y \in G$, by Theorem 2 (solutions of equations) $\exists$ a unique solution $x \in G \ni gx = y$ or $T_g(x) = y$. Thus $T_g$ is onto and so is a permutation on $G$.

Now define $\overline{G}$ by $\{T_g | g \in G\}$. For any $g, h \in G$,

$$(T_gT_h)(x) = T_g(T_h(x)) = T_g(hx) = g(hx) = (gh)(x) = T_{gh}(x) \ \forall x \in G,$$

so $\overline{G}$ is closed under composition. Then $T_e$ is the identity and $T_g^{-1} = T_{g^{-1}}$.

Since composition is associative, $\overline{G}$ is a group.

Now define $\phi : G \rightarrow \overline{G}$ by $\phi(g) = T_g \ \forall g \in G$.

$$\phi(g) = \phi(h) \implies T_g = T_h \implies T_g(e) = T_h(e) \implies ge = he \implies g = h,$$

so $\phi$ is 1–1. $\phi$ is clearly onto by construction.

Finally, for $g, h \in G$,

$$\phi(gh) = T_{gh} = T_gT_h = \phi(g)\phi(h),$$

so $\phi$ is an isomorphism. \qed
**Example.** $U = \{1, 3, 5, 7\}$.

$T_1 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{bmatrix}, T_3 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 3 & 1 & 7 & 5 \end{bmatrix}, T_5 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{bmatrix}, T_7 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 7 & 5 & 3 & 1 \end{bmatrix}$.

Then $\overline{U(8)} = \{T_1, T_3, T_5, T_7\}$.

<table>
<thead>
<tr>
<th>$U(8)$</th>
<th>1 3 5 7</th>
<th>$\overline{U(8)}$</th>
<th>$T_1$</th>
<th>$T_3$</th>
<th>$T_5$</th>
<th>$T_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 3 5 7</td>
<td>$T_1$</td>
<td>$T_1$</td>
<td>$T_3$</td>
<td>$T_5$</td>
<td>$T_7$</td>
</tr>
<tr>
<td>3</td>
<td>3 1 7 5</td>
<td>$T_3$</td>
<td>$T_3$</td>
<td>$T_1$</td>
<td>$T_7$</td>
<td>$T_5$</td>
</tr>
<tr>
<td>5</td>
<td>5 7 1 3</td>
<td>$T_5$</td>
<td>$T_5$</td>
<td>$T_7$</td>
<td>$T_1$</td>
<td>$T_3$</td>
</tr>
<tr>
<td>7</td>
<td>7 5 3 1</td>
<td>$T_7$</td>
<td>$T_7$</td>
<td>$T_5$</td>
<td>$T_3$</td>
<td>$T_1$</td>
</tr>
</tbody>
</table>

**Theorem (6.2 — Properties of Elements Acting on Elements).** Suppose $\phi$ is an isomorphism from a group $G$ onto a group $\overline{G}$. Then

1. $\phi(e) = \overline{e}$.
   **Proof.**

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

   Also, since $\phi(e) \in \overline{G}$, $\phi(e) = \overline{e}\phi(e) \implies \overline{e}\phi(e) = \phi(e)\phi(e) \implies \overline{e} = \phi(e)$ by right cancellation.

2. For all $n \in \mathbb{Z}$ and for all $a \in G$, $\phi(a^n) = [\phi(a)]^n$.
   **Proof.**

   For $n \in \mathbb{Z}$, $n \geq 0$, $\phi(a^n) = [\phi(a)]^n$ from the definition of an isomorphism and induction. For $n < 0$, $-n > 0$, so

   $\overline{e} = \phi(e) = \phi(a^n a^{-n}) = \phi(a^n)\phi(a^{-n}) = \phi(a^n)[\phi(a)]^{-n} \implies [\phi(a)]^n = \phi(a^n)$.

3. For all $a, b \in G$, $ab = ba \iff \phi(a)\phi(b) = \phi(b)\phi(a)$.
   **Proof.**

   $ab = ba \iff \phi(ab) = \phi(ba) \iff \phi(a)\phi(b) = \phi(b)\phi(a)$.
(4) \( G = \langle a \rangle \iff \overline{G} = \langle \phi(a) \rangle \).

**Proof.**

Let \( G = \langle a \rangle \). By closure, \( \langle \phi(a) \rangle \subseteq \overline{G} \). Since \( \phi \) is onto, for any element \( b \in \overline{G} \), \( \exists a^k \in G \implies \phi(a^k) = b \). Thus \( b = \left[ \phi(a)^k \right] \implies b \in \langle \phi(a) \rangle \). Thus \( \overline{G} = \langle \phi(a) \rangle \).

Now suppose \( \overline{G} = \langle \phi(a) \rangle \). Clearly, \( \langle a \rangle \subseteq G \). For all \( b \in G \), \( \phi(b) \in \langle \phi(a) \rangle \).

Thus \( \exists k \in \mathbb{Z} \implies \phi(b) = \phi(a)^k = \phi(a^k) \). Since \( \phi \) is 1–1, \( b = a^k \). Thus \( \langle a \rangle = G \). \( \square \)

(5) \( |a| = |\phi(a)| \forall a \in G \) (Isomorphisms preserve order).

**Proof.**

\[ a^n = e \iff \phi(a^n) = \phi(e) \iff [\phi(a)]^n = e. \]

Thus \( a \) has infinite order \iff \( \phi(a) \) has infinite order, and \( a \) has finite order \( n \iff \phi(a) \) has infinite order \( n \). \( \square \)

(6) For a fixed integer \( k \) and a fixed \( b \in G \), \( x^k = b \) has the same number of solutions in \( G \) as does \( x^k = \phi(b) \) in \( \overline{G} \).

**Proof.**

Suppose \( a \) is a solution of \( x^k = b \) in \( G \), i.e., \( a^k = b \). Then

\[ \phi(a^k) = \phi(b) \implies [\phi(a)]^k = \phi(b), \]

so \( \phi(a) \) is a solution of \( x^k = \phi(b) \) in \( \overline{G} \).

Now suppose \( y \) is a solution of \( x^k = \phi(b) \) in \( \overline{G} \). Since \( \phi \) is onto, \( \exists a \in G \implies \phi(a) = y \). Then

\[ [\phi(a)]^k = \phi(b) \iff \phi(a^k) = \phi(b) \implies a^k = b \]

since \( \phi \) is 1–1. Thus \( a \) is a solution of \( x^k = b \) in \( G \).

Therefore, there exists a 1–1 correspondence between the sets of solutions. \( \square \)

(7) If \( G \) is finite, then \( G \) and \( \overline{G} \) have exactly the same number of elements of every order.

**Proof.** Follows directly from property (5). \( \square \)
Example. Is $\mathbb{C}^* \cong \mathbb{R}^*$ with multiplication the operation of both groups? Solution. $x^2 = -1$ has 2 solutions in $\mathbb{C}^*$, but none in $\mathbb{R}^*$, so by Theorem 6.2(6) no isomorphism can exist. \(\square\)

Theorem (6.3 — Properties of Isomorphisms Acting on Groups). Suppose that $\phi$ is an isomorphism from a group $G$ onto a group $\overline{G}$. Then

(1) $\phi^{-1}$ is an isomorphism from $\overline{G}$ onto $G$.

Proof. The inverse of $\phi$ is 1–1 since $\phi$ is. Let $g \in G$. $\phi^{-1}(\phi(g)) = g \implies \phi$ is onto. Now let $x, y \in \overline{G}$. Then

$$\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y) \iff \phi(\phi^{-1}(xy)) = \phi(\phi^{-1}(x)\phi^{-1}(y)) \iff xy = \phi(\phi^{-1}(x))\phi(\phi^{-1}(y)) = xy.$$ 

Thus operations are preserved and $\phi^{-1}$ is an isomorphism. \(\square\)

(2) $G$ is Abelian $\iff \overline{G}$ is Abelian.

Proof. Follows directly from Theorem 6.2(3) since isomorphisms preserve commutivity. \(\square\)

(3) $G$ is cyclic $\iff \overline{G}$ is cyclic.

Proof. Follows directly from Theorem 6.2(4) since isomorphisms preserve order. \(\square\)
(4) If $K \leq G$, then $\phi(K) = \{\phi(k) \mid k \in K\} \leq \overline{G}$.

**Proof.**

Follows directly from Theorem 6.2(4) since isomorphisms preserve order. \hfill \Box

(5) If $\overline{K} \leq \overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G \mid \phi(g) \in \overline{K}\} \leq G$.

**Proof.**

Follows directly from (1) and (4). \hfill \Box

(6) $\phi(Z(G)) = Z(\overline{G})$.

**Proof.**

Follows directly from Theorem 6.2(3) since isomorphisms preserve commutivity. \hfill \Box

**Definition (Automorphism).** An isomorphisms from a group $G$ onto itself is called an automorphism.

**Problem (Psge 140 # 35).** Show that the mapping $\phi(a + bi) = a - bi$ is an automorphism of $\mathbb{C}$ under addition. Show that $\phi$ preserves complex multiplication as well. (This means $\phi$ is an automorphisms of $\mathbb{C}^*$ as well.)

**Solution.**

$\phi$ is clearly 1–1 and onto. Suppose $a + bi, c + di \in \mathbb{C}$.

$\phi[(a + bi) + (c + di)] = \phi[(a + c) + (b + d)i] = (a + c) - (b + d)i$

$\phantom{\phi[(a + bi) + (c + di)]} = \phi(a + bi) + \phi(c + di)$,

so $\phi$ is an automorphism of $\mathbb{C}$ under addition.

Now suppose $a + bi, c + di \in \mathbb{C}^*$.

$\phi[(a + bi)(c + di)] = \phi[(ac - bd) + (ad + bc)i] = (ac - bd) - (ad + bc)i$

$\phantom{\phi[(a + bi)(c + di)]} = \phi(a - bi)(c - di) = \phi(a + bi)\phi(c + di)$,

so $\phi$ is an automorphism of $\mathbb{C}^*$ under multiplication. \hfill \Box
6. ISOMORPHISMS

**Example** (related to Example 10 on Page 135). Consider $\mathbb{R}^2$. Any reflection across a line through the origin or rotation about the origin is an automorphism under componentwise addition. For example, consider the reflection about the line $y = 2x$.

Consider $(a, b)$ not on $y = 2x$. The line through $(a, b) \perp y = 2x$ is $y - b = -\frac{1}{2}(x - a)$. To find $P$ (using substitution):

$$2x - b = -\frac{1}{2}(x - a) \implies \frac{5}{2}x = \frac{1}{2}a + b \implies x = \frac{1}{5}a + \frac{2}{5}b \implies y = \frac{2}{5}a + \frac{4}{5}b.$$  

Thus the direction vector $\mathbf{v} = P - (a, b)$ takes $(a, b)$ to $P$.

$$\mathbf{v} = \left( -\frac{4}{5}a + \frac{2}{5}b, \frac{2}{5}a - \frac{1}{5}b \right).$$

Define $\phi(a, b) = (b, a)$.

$\phi$ is clearly 1–1 and onto.
Finally,
\[
\phi \left[ (a, b) + (c, d) \right] = \phi(a + c, b + d) = (b + d, a + c) = (b, a) + (d, c) = \phi(a, b) + \phi(c, d),
\]
so \( \phi \) is an isomorphism.

**Definition** (Inner Automorphism Induced by \( a \)).

Let \( G \) be a group, \( a \in G \). The function \( \phi_a \) defined by \( \phi_a(x) = axa^{-1} \forall x \in G \) is called the **inner automorphism** of \( G \) induced by \( a \).

**Example.** The action of the inner automorphism of \( D_4 \) induced by \( R_{90} \) is given in the following table.

<table>
<thead>
<tr>
<th>( x )</th>
<th>( \phi_{R_{90}} )</th>
<th>( R_{90} x R_{90}^{-1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( R_0 )</td>
<td>( \rightarrow )</td>
<td>( R_{90}R_0R_{90}^{-1} = R_0 )</td>
</tr>
<tr>
<td>( R_{90} )</td>
<td>( \rightarrow )</td>
<td>( R_{90}R_{90}R_{90}^{-1} = R_{90} )</td>
</tr>
<tr>
<td>( R_{180} )</td>
<td>( \rightarrow )</td>
<td>( R_{90}R_{180}R_{90}^{-1} = R_{180} )</td>
</tr>
<tr>
<td>( R_{270} )</td>
<td>( \rightarrow )</td>
<td>( R_{90}R_{270}R_{90}^{-1} = R_{270} )</td>
</tr>
<tr>
<td>( H )</td>
<td>( \rightarrow )</td>
<td>( R_{90}HR_{90}^{-1} = V )</td>
</tr>
<tr>
<td>( V )</td>
<td>( \rightarrow )</td>
<td>( R_{90}VR_{90}^{-1} = H )</td>
</tr>
<tr>
<td>( D )</td>
<td>( \rightarrow )</td>
<td>( R_{90}DR_{90}^{-1} = D' )</td>
</tr>
<tr>
<td>( D' )</td>
<td>( \rightarrow )</td>
<td>( R_{90}D'R_{90}^{-1} = D )</td>
</tr>
</tbody>
</table>
Problem (Page 145 # 45). Suppose $g$ and $h$ induce the same inner automorphism of a group $G$. Prove $h^{-1}g \in Z(G)$.

Proof. Let $x \in G$. Then

$$\phi_g(x) = \phi_h(x) \implies gxg^{-1} = hxh^{-1} \implies h^{-1}gxg^{-1}h = x \implies (h^{-1}g)x(h^{-1}g)^{-1}h = x \implies (h^{-1}g)x = x(h^{-1}g) \implies h^{-1}g \in Z(G)$$ since $x$ is arbitrary.

Definition.

$\text{Aut}(G) = \{ \phi \mid \phi \text{ is an automorphism of } G \}$ and

$\text{Inn}(G) = \{ \phi \mid \phi \text{ is an inner automorphism of } G \}$.

Theorem (6.4 — $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups).

$\text{Aut}(G)$ and $\text{Inn}(G)$ are groups under function composition.

Proof.

From the transitive portion of Theorem 3, compositions of isomorphisms are isomorphisms. Thus $\text{Aut}(G)$ is closed under composition. We know function composition is associative and that the identity map is the identity automorphism.

Suppose $\alpha \in \text{Aut}(G)$. $\alpha^{-1}$ is clearly 1–1 and onto. Now

$$\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y) \iff (\iff \text{ by 1–1})$$

$$\alpha[\alpha^{-1}(xy)] = \alpha[\alpha^{-1}(x)\alpha^{-1}(y)] \iff xy = \alpha[\alpha^{-1}(x)]\alpha[\alpha^{-1}(y)] \iff xy = xy.$$ 

Thus $\alpha^{-1}$ is operation preserving, and $\text{Aut}(G)$ is a group.
Now let \( \phi_g, \phi_h \in \text{Inn}(G) \subseteq \text{Aut}(G) \). For all \( x \in G \),
\[
\phi_g \phi_h(x) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x),
\]
so \( \phi_{gh} = \phi_g \phi_h \in \text{Inn}(G) \), and \( \text{Inn}(G) \) is closed under composition.

Also, \( \phi_g^{-1} = \phi_{g^{-1}} \) since
\[
\phi_{g^{-1}} \phi_g(x) = \phi_{g^{-1}}(gxg^{-1}) = g^{-1}gxg^{-1}(g^{-1})^{-1} = g^{-1}gxg^{-1}g = exe = \phi_e(x),
\]
and so also \( \phi_{gg^{-1}} = \phi_e \). Thus \( \text{Inn}(G) \subseteq \text{Aut}(G) \) by the two-step test. \( \square \)

**Example.** Find \( \text{Inn}(\mathbb{Z}_{12}) \).

**Solution.**
Since \( \mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\} \), \( \text{Inn}(\mathbb{Z}_{12}) = \{\phi_0, \phi_1, \phi_2, \ldots, \phi_{11}\} \), but the second list may have duplicates. That is the case here. For all \( n \in \mathbb{Z}_{12} \) and for all \( x \in \mathbb{Z}_{12} \),
\[
\phi_n(x) = n + x + (-n) = n + (-n) + x = 0 + x = 0 + x + 0 = \phi_0(x),
\]
the identity automorphism. Thus \( \text{Inn}(\mathbb{Z}_{12}) = \{\phi_0\} \). \( \square \)
**Example.** Find $\text{Inn}(D_3)$.

**Solution.**

$D_3 = \{\varepsilon, (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3), (1\ 2)\}$ as permutations. Then $\text{Inn}(D_3) = \{\phi_\varepsilon, \phi_{(1\ 2\ 3)}, \phi_{(1\ 3\ 2)}, \phi_{(2\ 3)}, \phi_{(1\ 3)}, \phi_{(1\ 2)}\}$, but we need to eliminate repetitions.

$\phi_{(1\ 2\ 3)}(1\ 2\ 3) = (1\ 2\ 3)(1\ 2\ 3)(3\ 2\ 1) = (1\ 2\ 3)$.

$\phi_{(1\ 2\ 3)}(1\ 3\ 2) = (1\ 3\ 2)(1\ 2\ 3)(3\ 2\ 1) = (1\ 3\ 2)$.

$\phi_{(1\ 2\ 3)}(2\ 3) = (1\ 3\ 2)(2\ 3)(3\ 2\ 1) = (1\ 3)$.

$\phi_{(1\ 2\ 3)}(1\ 3) = (1\ 3\ 2)(1\ 3)(3\ 2\ 1) = (1\ 2)$.

$\phi_{(1\ 2\ 3)}(1\ 2) = (1\ 3\ 2)(1\ 2)(3\ 2\ 1) = (2\ 3)$. Thus $\phi_{(1\ 2\ 3)}$ is distinct from $\phi_\varepsilon$.

$\phi_{(1\ 3\ 2)}(2\ 3) = (1\ 3\ 2)(2\ 3)(2\ 3\ 1) = (1\ 2)$. Thus $\phi_{(1\ 3\ 2)}$ is distinct.

$\phi_{(2\ 3)}(2\ 3) = (2\ 3)(2\ 3)(2\ 3) = (2\ 3)$.

$\phi_{(2\ 3)}(1\ 3) = (2\ 3)(1\ 3)(2\ 3) = (1\ 2)$. Thus $\phi_{(2\ 3)}$ is distinct.

$\phi_{(1\ 3)}(2\ 3) = (1\ 3)(2\ 3)(1\ 3) = (1\ 2)$.

$\phi_{(1\ 3)}(1\ 3) = (1\ 3)(1\ 3)(1\ 3) = (1\ 3)$.

$\phi_{(1\ 3\ 2)}(1\ 3) = (1\ 3\ 2)(1\ 3)(2\ 3\ 1) = (2\ 3)$. Thus $\phi_{(1\ 3)}$ is distinct.

$\phi_{(1\ 2)}(2\ 3) = (1\ 2)(2\ 3)(1\ 2) = (1\ 3)$.

$\phi_{(1\ 2)}(1\ 3) = (1\ 2)(1\ 3)(1\ 2) = (2\ 3)$. Thus $\phi_{(1\ 2)}$ is distinct.

Therefore, there are no duplicates and $\text{Inn}(D_3) = \{\phi_\varepsilon, \phi_{(1\ 2\ 3)}, \phi_{(1\ 3\ 2)}, \phi_{(2\ 3)}, \phi_{(1\ 3)}, \phi_{(1\ 2)}\}$. 

□
**Theorem (6.5 – Aut(\(\mathbb{Z}_n\)) = U(n))**. For all \(n \in \mathbb{N}\), Aut(\(\mathbb{Z}_n\)) = U(n).

**Proof.**

Let \(\alpha \in \text{Aut}(\mathbb{Z}_n)\). Then

\[
\alpha(k) = \alpha(1 + 1 + \cdots + 1) = (\alpha(1) + \alpha(1) + \cdots + \alpha(1)) = k\alpha(1).
\]

Now \(|1| = n \implies |\alpha(1)| = n\), so \(\alpha(1)\) is a generator of \(\mathbb{Z}_n\) since \(1\) is also a generator. Now consider

\[
T : \text{Aut}(\mathbb{Z}_n) \to U(n) \quad \text{where} \quad T(\alpha) = \alpha(1).
\]

Suppose \(\alpha, \beta \in \text{Aut}(\mathbb{Z}_n)\) and \(T(\alpha) = T(\beta)\). Then \(\alpha(1) = \beta(1)\), so \(\forall k \in \mathbb{Z}_n\), \(\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)\). Thus \(\alpha = \beta\) and \(T\) is 1–1.

[To show \(T\) is onto.] Now suppose \(r \in U(n)\) and consider \(\alpha : \mathbb{Z}_n \to \mathbb{Z}_n\) defined by \(\alpha(s) = sr \mod n \quad \forall s \in \mathbb{Z}_n\).

[To show \(\alpha \in \text{Aut}(\mathbb{Z}_n)\).] Suppose \(\alpha(x) = \alpha(y)\). Then \(xr = yr \mod n\).

But \(r^{-1}\) exists modulo \(n\) \(\implies xr^{-1} = yr^{-1} \mod n \implies x \cdot 1 = y \cdot 1 \mod n \implies x = y \mod n\), so \(\alpha\) is 1–1.

Suppose \(x \in \mathbb{Z}_n\). By Theorem 2, \(\exists s \in \mathbb{Z}_n \ni \alpha(s) = sr = x\), so \(\alpha\) is onto.

Now suppose \(x, y \in \mathbb{Z}_n\).

\[
\alpha(x + y) = (x + y)r \mod n = (xr + yr) \mod n = xr \mod n + yr \mod n = \alpha(x) + \alpha(y),
\]

so \(\alpha \in \text{Aut}(\mathbb{Z}_n)\).

Since \(T(\alpha) = \alpha(1) = r\), \(T\) is onto.
Finally, let $\alpha, \beta \in \text{Aut}(\mathbb{Z}_n)$. Then
\[
T(\alpha \beta) = (\alpha \beta)(1) = \alpha[\beta(1)] = \alpha(1 + 1 + \cdots + 1)_\beta(1) \text{ terms}
\]
\[
\underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1) \text{ terms}} = \alpha(1)\beta(1) = T(\alpha)T(\beta),
\]
so $\text{Aut}(\mathbb{Z}_n) \approx U(n)$. 

**Example.** $\text{Aut}(\mathbb{Z}_{10}) \approx U(10)$. The multiplication tables for the two groups are given below:

<table>
<thead>
<tr>
<th>$U(10)$</th>
<th>1</th>
<th>3</th>
<th>7</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>1</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\text{Aut}(\mathbb{Z}_{10})$</th>
<th>$\alpha_1$</th>
<th>$\alpha_3$</th>
<th>$\alpha_7$</th>
<th>$\alpha_9$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_1$</td>
<td>$\alpha_1$</td>
<td>$\alpha_3$</td>
<td>$\alpha_7$</td>
<td>$\alpha_9$</td>
</tr>
<tr>
<td>$\alpha_3$</td>
<td>$\alpha_3$</td>
<td>$\alpha_9$</td>
<td>$\alpha_1$</td>
<td>$\alpha_7$</td>
</tr>
<tr>
<td>$\alpha_7$</td>
<td>$\alpha_7$</td>
<td>$\alpha_1$</td>
<td>$\alpha_9$</td>
<td>$\alpha_3$</td>
</tr>
<tr>
<td>$\alpha_9$</td>
<td>$\alpha_9$</td>
<td>$\alpha_7$</td>
<td>$\alpha_3$</td>
<td>$\alpha_1$</td>
</tr>
</tbody>
</table>

The isomorphism is clear.