ISOMORPHISMS OF GROUPS

**Definition:**
If \((G, \ast)\) and \((H, \circ)\) are groups, then a function \(f : G \rightarrow H\) is a **homomorphism** if

\[ f(x \ast y) = f(x) \circ f(y) \]

for all \(x, y \in G\).

**Example:**
Let \((G, \ast)\) be an arbitrary group and \(H = \{e\}\), then the function \(f : G \rightarrow H\) such that \(f(x) = e\) for any \(x \in G\) is a homomorphism. In fact,

\[ f(x \ast y) = e = e \circ e = f(x) \circ f(y). \]

**Definition:**
Let a function \(f : G \rightarrow H\) be a homomorphism. If \(f\) is also a one-one correspondence, then \(f\) is called an **isomorphism**. Two groups \(G\) and \(H\) are called isomorphic, denoted by

\[ G \cong H, \]

if there exists an isomorphism between them.

**Example:**
We show that \(\mathbb{R}^+ \cong \mathbb{R}^\times\). In fact, let

\[ f(x) = e^x. \]

To prove that this is an isomorphism, we should check that

\[ f : \mathbb{R}^+ \rightarrow \mathbb{R}^\times \]

is one-one correspondence and that

\[ f(x + y) = f(x)f(y) \]

for all \(x, y \in \mathbb{R}\). The first part is trivial, since \(f(x) = e^x\) is defined for all \(x \in \mathbb{R}\) and its inverse \(g(x) = \ln x\) is also defined for all \(x \in \mathbb{R}_{>0}\). The second part is also true, since

\[ f(x + y) = e^{x+y} = e^x e^y = f(x)f(y). \]
**Definition:**

Let \( G = \{ a_1, a_2, \ldots, a_n \} \) be a finite group. A multiplication table for \( G \) is an \( n \times n \) matrix whose \( ij \) entry is \( a_i a_j \): 

\[
\begin{array}{cccc}
  G & a_1 & a_2 & \ldots & a_j & \ldots & a_n \\
  a_1 & a_1 a_2 & a_1 a_2 & \ldots & a_1 a_j & \ldots & a_1 a_n \\
  a_2 & a_2 a_1 & a_2 a_2 & \ldots & a_2 a_j & \ldots & a_2 a_n \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
  a_i & a_i a_1 & a_i a_2 & \ldots & a_i a_j & \ldots & a_i a_n \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
  a_n & a_n a_1 & a_n a_2 & \ldots & a_n a_j & \ldots & a_n a_n \\
\end{array}
\]

We will also agree that \( a_1 = 1 \).

**Example:**

Multiplicative table for \( \mathbb{Z}^\times_5 \) is 

\[
\begin{array}{cccc}
  \mathbb{Z}^\times_5 & 1 & 2 & 3 & 4 \\
\end{array}
\]

**Remark:**

It is clear that two groups of the same order \( G = \{ a_1, a_2, \ldots, a_n \} \) and \( H = \{ b_1, b_2, \ldots, b_n \} \) are isomorphic if and only if it is possible to match elements \( a_1, a_2, \ldots, a_n \) with elements \( b_1, b_2, \ldots, b_n \) such that this one-one correspondence remains also for corresponding entries \( a_i a_j \) and \( b_i b_j \) of their multiplication tables.

**Example:**

1. The multiplication tables below show that \( \mathcal{P} \cong \mathbb{Z}^+_2 \cong \mathbb{Z}^\times_3 \):

\[
\begin{array}{cc}
  \mathcal{P} & \text{“even” “odd”} \\
  \text{“even” “even” “odd”} & \text{“odd” “odd” “even”} \\
\end{array}
\]

\[
\begin{array}{c|c|c}
  \mathbb{Z}^+_2 & 0 & 1 \\
  0 & 1 & 0 \\
  1 & 0 & 1 \\
\end{array}
\]

\[
\begin{array}{c|c|c}
  \mathbb{Z}^\times_3 & 1 & 2 \\
  1 & 1 & 2 \\
  2 & 2 & 1 \\
\end{array}
\]

2. The multiplication tables below show that \( \mathbb{Z}^+_4 \cong \mathbb{Z}^\times_5 \):

\[
\begin{array}{c|c|c|c|c}
  \mathbb{Z}^+_4 & 0 & 1 & 2 & 3 \\
  0 & 0 & 1 & 2 & 3 \\
  1 & 1 & 2 & 3 & 0 \\
  2 & 2 & 3 & 0 & 1 \\
  3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

\[
\begin{array}{c|c|c|c|c}
  \mathbb{Z}^\times_5 & 1 & 2 & 4 & 3 \\
  1 & 1 & 2 & 4 & 3 \\
  2 & 2 & 4 & 3 & 1 \\
  4 & 4 & 3 & 1 & 2 \\
  3 & 3 & 1 & 2 & 4 \\
\end{array}
\]
3. The multiplication tables below show that $\mathbb{Z}^+_6 \cong \mathbb{Z}^+_7$:

<table>
<thead>
<tr>
<th>$\mathbb{Z}^+_6$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\mathbb{Z}^+_7$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**Theorem 1:**

Let $f : G \longrightarrow H$ is a homomorphism of groups. Then

(i) $f(e) = e$;

(ii) $f(x^{-1}) = f(x)^{-1}$;

(iii) $f(x^n) = f(x)^n$ for all $n \in \mathbb{Z}$.

**Proof:**

(i) We have

$$e \cdot e = e \implies f(e \cdot e) = f(e) = f(e) \cdot f(e) = f(e).$$

Multiplying both sides by $[f(e)]^{-1}$, we get

$$[f(e)]^{-1}f(e)f(e) = [f(e)]^{-1}f(e) \implies e \cdot f(e) = e \implies f(e) = e.$$  

(ii) We have

$$x \cdot x^{-1} = e \implies f(x \cdot x^{-1}) = f(e) = f(x)f(x^{-1}) = f(e).$$

Since $f(e) = e$ by (i), we get

$$f(x)f(x^{-1}) = e.$$  

Similarly, from $x^{-1} \cdot x = e$ one can deduce that $f(x^{-1})f(x) = e$. So,

$$f(x)f(x^{-1}) = f(x^{-1})f(x) = e,$$

which means that $f(x^{-1}) = f(x)^{-1}$.

(iii) If $n \geq 1$, one can prove $f(x^n) = f(x)^n$ by induction. If $n < 0$, then

$$f(x^{-n}) = f((x^{-1})^n) = f(x^{-1})^n,$$

which is equal to $f(x)^{-n}$ by (ii). □

**Theorem 2:**

Any two cyclic groups $G$ and $H$ of the same order are isomorphic.

**Proof (Sketch):**

Suppose that $G = \langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\}$ and $H = \langle b \rangle = \{1, b, b^2, \ldots, b^{m-1}\}$. Then

$$f : G \longrightarrow H$$
with
\[ f(a^i) = b^i, \quad 0 \leq i \leq m - 1, \]
is an isomorphism and \( G \cong H. \) □

**Example:**

(a) We know that any group of the prime order is cyclic. Therefore by Theorem 2 any two groups of the same prime order are isomorphic.

(b) Let \( p \) be a prime number. We know that the group \( \mathbb{Z}_{p-1}^+ \) is cyclic, since \( \mathbb{Z}_{p-1}^+ = \langle [1] \rangle \). It is possible to prove that \( \mathbb{Z}_p^x \) is also cyclic. Also, \( |\mathbb{Z}_{p-1}^+| = |\mathbb{Z}_p^x| = p - 1 \). Therefore from Theorem 2 it follows that \( \mathbb{Z}_{p-1}^+ \cong \mathbb{Z}_p^x \).

**Problem:** Show that \( V \not\cong \mathbb{Z}_4^+ \).

**Solution:**

Assume to the contrary that \( V \cong \mathbb{Z}_4^+ \). Then there is a one-one correspondence \( f : V \to \mathbb{Z}_4^+ \).

From this, in particularly, follows that there exists \( x \in V \) such that
\[ f(x) = [1]. \]

This and (iii) of Theorem 1 give
\[ f(x^2) = [f(x)]^2 = [1]^2 = [1] + [1] = [2]. \]

We now recall that for any element \( x \in V \) we have
\[ x^2 = e. \]

By this and (i) of Theorem 1 we get
\[ f(x^2) = f(e) = e = [1]. \]

This is a contradiction. □

**Remark:**

One can show that any group of order 4 is isomorphic to \( \mathbb{Z}_4^+ \) or \( V \).
\[\begin{array}{|c|cccc|}
\hline
\times & I & II & III & IV \\
\hline
I & I & II & III & IV \\
II & II & IV & VI & VIII \\
III & III & VI & IX & XII \\
IV & IV & VIII & XII & XVI \\
\hline
\end{array}\]
<table>
<thead>
<tr>
<th>×</th>
<th>Ⅰ</th>
<th>Ⅱ</th>
<th>Ⅲ</th>
<th>Ⅳ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ⅰ</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Ⅱ</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Ⅲ</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Ⅳ</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>×</th>
<th>Ⅲ</th>
<th>Ⅱ</th>
<th>Ⅰ</th>
<th>Ⅳ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ⅱ</td>
<td>VI</td>
<td>IV</td>
<td>Ⅱ</td>
<td>VIII</td>
</tr>
<tr>
<td>Ⅳ</td>
<td>XII</td>
<td>VIII</td>
<td>IV</td>
<td>XVI</td>
</tr>
<tr>
<td>Ⅲ</td>
<td>IX</td>
<td>VI</td>
<td>Ⅲ</td>
<td>XII</td>
</tr>
<tr>
<td>Ⅰ</td>
<td>Ⅲ</td>
<td>Ⅱ</td>
<td>Ⅰ</td>
<td>Ⅳ</td>
</tr>
</tbody>
</table>
\[
\begin{array}{c|cc}
\mathbb{Z}_2^+ & [0] & [1] \\
[0] & 0 & 1 \\
[1] & 1 & 0 \\
\end{array}
\]

\[
\begin{array}{c|ccc}
[1] & 1 & 2 \\
[2] & 2 & 1 \\
\end{array}
\]
<table>
<thead>
<tr>
<th>$\mathbb{Z}_2^+$</th>
<th>[0]</th>
<th>[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[0]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\mathbb{Z}_3$</th>
<th>[1]</th>
<th>[2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[1]</td>
</tr>
</tbody>
</table>

$[0] \leftrightarrow [1]$  
$[1] \leftrightarrow [2]$
<table>
<thead>
<tr>
<th>$\mathbb{Z}_4^+$</th>
<th>[0]</th>
<th>[1]</th>
<th>[2]</th>
<th>[3]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[0]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[3]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
<tr>
<td>[3]</td>
<td>[3]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\mathbb{Z}_5^\times$</th>
<th>[1]</th>
<th>[2]</th>
<th>[3]</th>
<th>[4]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[4]</td>
<td>[1]</td>
<td>[3]</td>
</tr>
</tbody>
</table>

\[0\leftrightarrow 1\]
\[1\leftrightarrow 2\]
\[2\leftrightarrow 3\]
\[3\leftrightarrow 4\]
\[
\begin{array}{|c|c|c|c|}
\hline
\hline
\hline
\end{array}
\]

\[
\begin{array}{|c|c|c|c|}
\hline
\hline
\hline
\end{array}
\]

\[
\begin{align*}
[0] & \leftrightarrow [1] \\
\end{align*}
\]
<table>
<thead>
<tr>
<th>$\mathbb{Z}_6^+$</th>
<th>$[0]$</th>
<th>$[1]$</th>
<th>$[2]$</th>
<th>$[3]$</th>
<th>$[4]$</th>
<th>$[5]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[0]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
<td>$[4]$</td>
<td>$[5]$</td>
</tr>
<tr>
<td>$[1]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
<td>$[4]$</td>
<td>$[5]$</td>
<td>$[0]$</td>
</tr>
<tr>
<td>$[2]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
<td>$[4]$</td>
<td>$[5]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
</tr>
<tr>
<td>$[3]$</td>
<td>$[3]$</td>
<td>$[4]$</td>
<td>$[5]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
</tr>
<tr>
<td>$[4]$</td>
<td>$[4]$</td>
<td>$[5]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
</tr>
<tr>
<td>$[5]$</td>
<td>$[5]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
<td>$[4]$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\mathbb{Z}_7^\times$</th>
<th>$[1]$</th>
<th>$[2]$</th>
<th>$[3]$</th>
<th>$[4]$</th>
<th>$[5]$</th>
<th>$[6]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Z^+_6$</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
</tr>
<tr>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
<tr>
<td>[3]</td>
<td>[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
</tr>
<tr>
<td>[4]</td>
<td>[4]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
</tr>
<tr>
<td>[5]</td>
<td>[5]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$Z_4^+$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$V$</th>
<th>(1)</th>
<th>(12)(34)</th>
<th>(13)(24)</th>
<th>(14)(23)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>(1)</td>
<td>(12)(34)</td>
<td>(13)(24)</td>
<td>(14)(23)</td>
</tr>
</tbody>
</table>

$[0] \leftrightarrow (1)$
$[1] \leftrightarrow (12)(34)$
$[2] \leftrightarrow (13)(24)$
$[3] \leftrightarrow (14)(23)$
Definition:
If \((G, \ast)\) and \((H, \circ)\) are groups, then a function \(f : G \rightarrow H\) is a homomorphism if
\[
f(x \ast y) = f(x) \circ f(y)
\]
for all \(x, y \in G\).

Example:
Let \((G, \ast)\) be an arbitrary group and \(H = \{e\}\), then the function
\[
f : G \rightarrow H
\]
such that
\[
f(x) = e \quad \text{for any} \quad x \in G
\]
is a homomorphism. In fact,
\[
f(x \ast y) = e = e \circ e = f(x) \circ f(y).
\]
Definition:
Let a function \( f : G \longrightarrow H \) be a homomorphism. If \( f \) is also a one-one correspondence, then \( f \) is called an isomorphism. Two groups \( G \) and \( H \) are called isomorphic, denoted by
\[
G \cong H,
\]
if there exists an isomorphism between them.
Example:
We show that $R^+ \cong R_{>0}^\times$. In fact, let
$$f(x) = e^x.$$ 
To prove that this is an isomorphism, we should check that
$$f : R^+ \longrightarrow R_{>0}^\times$$ 
is one-one correspondence and that
$$f(x + y) = f(x)f(y)$$
for all $x, y \in R$. The first part is trivial, since $f(x) = e^x$ is defined for all $x \in R$ and its inverse $g(x) = \ln x$ is also defined for all $x \in R_{>0}$. The second part is also true, since
$$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y).$$
Definition:

Let $G = \{a_1, a_2, \ldots, a_n\}$ be a finite group. A multiplication table for $G$ is an $n \times n$ matrix whose $ij$ entry is $a_i a_j$:

<table>
<thead>
<tr>
<th></th>
<th>$a_1$</th>
<th>$a_2$</th>
<th>$\ldots$</th>
<th>$a_j$</th>
<th>$\ldots$</th>
<th>$a_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_1$</td>
<td>$a_1 a_2$</td>
<td>$a_1 a_2$</td>
<td>$\ldots$</td>
<td>$a_1 a_j$</td>
<td>$\ldots$</td>
<td>$a_1 a_n$</td>
</tr>
<tr>
<td>$a_2$</td>
<td>$a_2 a_1$</td>
<td>$a_2 a_2$</td>
<td>$\ldots$</td>
<td>$a_2 a_j$</td>
<td>$\ldots$</td>
<td>$a_2 a_n$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\ddots$</td>
<td>$\vdots$</td>
<td>$\ddots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$a_i$</td>
<td>$a_i a_1$</td>
<td>$a_i a_2$</td>
<td>$\ldots$</td>
<td>$a_i a_j$</td>
<td>$\ldots$</td>
<td>$a_i a_n$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\cdots$</td>
<td>$\vdots$</td>
<td>$\cdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$a_n$</td>
<td>$a_n a_1$</td>
<td>$a_n a_2$</td>
<td>$\ldots$</td>
<td>$a_n a_j$</td>
<td>$\ldots$</td>
<td>$a_n a_n$</td>
</tr>
</tbody>
</table>

We will also agree that $a_1 = 1$. 
Example:

Multiplicative table for $\mathbb{Z}_5^\times$ is

<table>
<thead>
<tr>
<th>$\mathbb{Z}_5^\times$</th>
<th>[1]</th>
<th>[2]</th>
<th>[3]</th>
<th>[4]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
<td>[3]</td>
<td>[4]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[4]</td>
<td>[1]</td>
<td>[3]</td>
</tr>
</tbody>
</table>
Remark:
It is clear that two groups of the same order

\[ G = \{ a_1, a_2, \ldots, a_n \} \]

and

\[ H = \{ b_1, b_2, \ldots, b_n \} \]

are isomorphic if and only if it is possible to match elements \( a_1, a_2, \ldots, a_n \) with elements \( b_1, b_2, \ldots, b_n \) such that this one-one correspondence remains also for corresponding entries \( a_ia_j \) and \( b_ib_j \) of their multiplication tables.
Example:
1. The multiplication tables below show that $\mathcal{P} \cong \mathbb{Z}_2^+ \cong \mathbb{Z}_3^\times$:

<table>
<thead>
<tr>
<th>$\mathcal{P}$</th>
<th>“even”</th>
<th>“odd”</th>
</tr>
</thead>
<tbody>
<tr>
<td>“even”</td>
<td>“even”</td>
<td>“odd”</td>
</tr>
<tr>
<td>“odd”</td>
<td>“odd”</td>
<td>“even”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\mathbb{Z}_2^+$</th>
<th>[0]</th>
<th>[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[0]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\mathbb{Z}_3^\times$</th>
<th>[1]</th>
<th>[2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[1]</td>
</tr>
</tbody>
</table>
2. The multiplication tables below show that $\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$:

<table>
<thead>
<tr>
<th>$\mathbb{Z}_4^+$</th>
<th>$[0]$</th>
<th>$[1]$</th>
<th>$[2]$</th>
<th>$[3]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[0]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
</tr>
<tr>
<td>$[1]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
<td>$[0]$</td>
</tr>
<tr>
<td>$[2]$</td>
<td>$[2]$</td>
<td>$[3]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
</tr>
<tr>
<td>$[3]$</td>
<td>$[3]$</td>
<td>$[0]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\mathbb{Z}_5^\times$</th>
<th>$[1]$</th>
<th>$[2]$</th>
<th>$[4]$</th>
<th>$[3]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[1]$</td>
<td>$[1]$</td>
<td>$[2]$</td>
<td>$[4]$</td>
<td>$[3]$</td>
</tr>
</tbody>
</table>
3. The multiplication tables below show that $\mathbb{Z}_6^+ \cong \mathbb{Z}_7^\times$:

\[
\begin{array}{c|cccccc}
\end{array}
\]

\[
\begin{array}{c|cccccc}
\end{array}
\]
Theorem 1:

Let \( f : G \rightarrow H \) is a homomorphism of groups. Then

(i) \( f(e) = e \);

(ii) \( f(x^{-1}) = f(x)^{-1} \);

(iii) \( f(x^n) = f(x)^n \) for all \( n \in \mathbb{Z} \).
(i) We have
\[ e \cdot e = e \quad \Rightarrow \quad f(e \cdot e) = f(e), \]
therefore
\[ f(e)f(e) = f(e). \]
Multiplying both sides by \([f(e)]^{-1}\), we get
\[ [f(e)]^{-1}f(e)f(e) = [f(e)]^{-1}f(e), \]
which gives
\[ e \cdot f(e) = e, \]
so
\[ f(e) = e. \]
(ii) We have

\[ x \cdot x^{-1} = e \quad \implies \quad f(x \cdot x^{-1}) = f(e), \]

so

\[ f(x)f(x^{-1}) = f(e). \]

Since \( f(e) = e \) by (i), we get

\[ f(x)f(x^{-1}) = e. \]

Similarly, from \( x^{-1} \cdot x = e \) one can deduce that \( f(x^{-1})f(x) = e \). So,

\[ f(x)f(x^{-1}) = f(x^{-1})f(x) = e, \]

which means that \( f(x^{-1}) = f(x)^{-1} \).
(iii) If $n \geq 1$, one can prove $f(x^n) = f(x)^n$ by induction. If $n < 0$, then

$$f(x^{-n}) = f((x^{-1})^n) = f(x^{-1})^n,$$

which is equal to $f(x)^{-n}$ by (ii). ■
Theorem 2:
Any two cyclic groups $G$ and $H$ of the same order are isomorphic.

Proof (Sketch):
Suppose that
\[ G = \langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\} \]
and
\[ H = \langle b \rangle = \{1, b, b^2, \ldots, b^{m-1}\}. \]
Then
\[ f : G \longrightarrow H \]
with
\[ f(a^i) = b^i, \quad 0 \leq i \leq m - 1, \]
is an isomorphism and $G \cong H$. ■.
Example:

(a) We know that any group of the prime order is cyclic. Therefore by Theorem 2 any two groups of the same prime order are isomorphic.

(b) Let $p$ be a prime number. We know that the group $\mathbb{Z}_{p-1}^+$ is cyclic, since

$$\mathbb{Z}_{p-1}^+ = \langle [1] \rangle.$$

It is possible to prove that $\mathbb{Z}_p^\times$ is also cyclic. Also,

$$|\mathbb{Z}_{p-1}^+| = |\mathbb{Z}_p^\times| = p - 1.$$

Therefore from Theorem 2 it follows that $\mathbb{Z}_{p-1}^+ \cong \mathbb{Z}_p^\times$. 
Problem: Show that $V \not\cong Z_4^+$. 

Solution:
Assume to the contrary that $V \cong Z_4^+$. Then there is a one-one correspondence $f : V \rightarrow Z_4^+$. From this, in particular, follows that there exists $x \in V$ such that

$$f(x) = [1].$$

This and (iii) of Theorem 1 give

$$f(x^2) = [f(x)]^2 = [1]^2 = [1] + [1] = [2].$$

We now recall that for any element $x \in V$ we have

$$x^2 = e.$$

By this and (i) of Theorem 1 we get

$$f(x^2) = f(e) = e = [1].$$

This is a contradiction. ■