HOMOMORPHISMS AND ISOMORPHISMS

Definition:

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

$$f(x * y) = f(x) \circ f(y)$$

for all $x, y \in G$.

Example:

Let $(G, *)$ be an arbitrary group and $H = \{e\}$, then the function $f : G \longrightarrow H$ such that

$$f(x) = e \quad \text{for any} \quad x \in G$$

is a homomorphism. In fact,

$$f(x * y) = e = e \circ e = f(x) \circ f(y).$$

Example:

Let $(G, *)$ be an arbitrary group, then the function $f : G \longrightarrow G$ such that

$$f(x) = x \quad \text{for any} \quad x \in G$$

is a homomorphism. In fact,

$$f(x * y) = x * y = f(x) * f(y).$$

Example:

Let $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}_2^+$ be a function such that $f(x) = \begin{cases} [0] \text{ if } x \text{ is even} \\ [1] \text{ if } x \text{ is odd} \end{cases}$. Then f is a homomorphism. In fact, if $x + y$ is even, then

$$f(x + y) = [0] = f(x) + f(y).$$

Similarly, if $x + y$ is odd, then

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

Example:

Let $f : GL(2, \mathbb{R}) \longrightarrow \mathbb{R}^{\times}_{\neq 0}$ be a function such that

$$f(M) = \det M \quad \text{for any} \quad M \in GL(2, \mathbb{R}).$$

Then f is a homomorphism. In fact,

$$f(M_1 M_2) = \det(M_1 M_2) = \det(M_1) \det(M_2) = f(M_1) f(M_2).$$

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 $\mathbb{R}^+ \cong \mathbb{R}^\times_{>0}$. In fact, let

$$f(x) = e^x.$$

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

$$f : \mathbb{R}^+ \longrightarrow \mathbb{R}^\times_{>0}$$

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 $a_i a_j$:

G	a_1	a_2	$\ldots$	a_j	$\ldots$	a_n
a_1	a_1a_2	a_1a_2	$\ldots$	a_1a_j	$\ldots$	a_1a_n
a_2	a_2a_1	a_2a_2	$\ldots$	a_2a_j	$\ldots$	a_2a_n
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	a_ia_1	a_ia_2	$\ldots$	a_ia_j	$\ldots$	a_ia_n
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	a_na_1	a_na_2	$\ldots$	a_na_j	$\ldots$	a_na_n

We will also agree that $a_1 = 1$.

Example:

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

$Z_5^\times$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Remark:

It is clear that two groups $G = \{a_1, a_2, \ldots, a_n\}$ and $H = \{b_1, b_2, \ldots, b_n\}$ of the same order 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 $\mathcal{P} \cong \mathbb{Z}_2^+ \cong \mathbb{Z}_3^\times$:

$\mathcal{P}$	"even"	"odd"
"even"	"even"	"odd"
"odd"	"odd"	"even"

Z_2^+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$Z_3^\times$	[1]	[2]
[1]	[1]	[2]
[2]	[2]	[1]

2. The multiplication tables below show that $\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$:

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]

$Z_5^\times$	[1]	[2]	[4]	[3]
[1]	[1]	[2]	[4]	[3]
[2]	[2]	[4]	[3]	[1]
[4]	[4]	[3]	[1]	[2]
[3]	[3]	[1]	[2]	[4]

3. The multiplication tables below show that $\mathbb{Z}_6^+ \cong \mathbb{Z}_7^\times$:

Z_6^+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$Z_7^\times$	[1]	[3]	[2]	[6]	[4]	[5]
[1]	[1]	[3]	[2]	[6]	[4]	[5]
[3]	[3]	[2]	[6]	[4]	[5]	[1]
[2]	[2]	[6]	[4]	[5]	[1]	[3]
[6]	[6]	[4]	[5]	[1]	[3]	[2]
[4]	[4]	[5]	[1]	[3]	[2]	[6]
[5]	[5]	[1]	[3]	[2]	[6]	[4]

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

$$e \cdot e = e \quad \Longrightarrow \quad f(e \cdot e) = f(e) \quad \Longrightarrow \quad f(e)f(e) = f(e).$$

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

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

(ii) We have

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

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:

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.

Example:

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 $\mathbf{V} \ncong \mathbb{Z}_{4}^{+}$.

Solution:

Assume to the contrary that $\mathbf{V} \cong \mathbb{Z}_{4}^{+}$. Then there is a one-one correspondence $f : \mathbf{V} \longrightarrow \mathbb{Z}_{4}^{+}$. From this, in particularly, follows that there exists $x \in \mathbf{V}$ 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 $x \in \mathbf{V}$ we have

$$x^2 = e.$$

By this and (i) of Theorem 1 we get

$$f(x^2) = f(e) = e = [0].$$

This is a contradiction. ■

Remark:

One can show that any group of order 4 is isomorphic to either $\mathbb{Z}_{4}^{+}$ or $\mathbf{V}$.

Definition:

If $f : G \longrightarrow H$ is a homomorphism, define

$$\ker f = \{x \in G : f(x) = 1\}.$$

Theorem 3:

Let $f : G \longrightarrow H$ be a homomorphism. Then $\ker f$ is a subgroup of G

Proof:

From (i) of Theorem 1 it follows that $1 \in \ker f$, since $f(1) = 1$. Next, if $x, y \in \ker f$, then

$$f(x) = 1 = f(y),$$

hence

$$f(xy) = f(x)f(y) = 1 \cdot 1 = 1,$$

so $xy \in \ker f$. Finally, if $x \in \ker f$, then $f(x) = 1$ and so

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

hence $x^{-1} \in \ker f$. Therefore $\ker f$ is a subgroup of G. ■

×	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

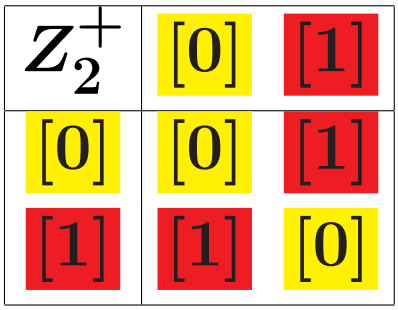
×	*I*	*II*	*III*	*IV*
I	*I*	*II*	*III*	*IV*
II	*II*	*IV*	*VI*	*VIII*
III	*III*	*VI*	*IX*	*XII*
IV	*IV*	*VIII*	*XII*	*XVI*

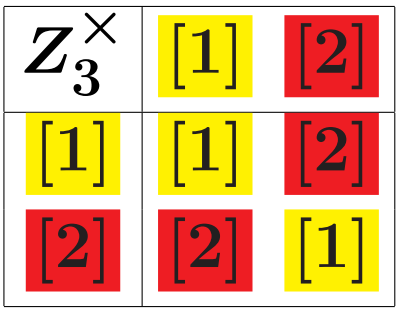
×	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

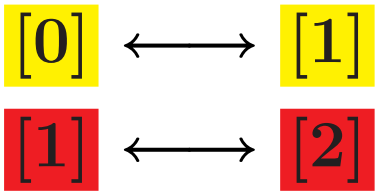
×	*III*	*II*	*I*	*IV*
II	*VI*	*IV*	*II*	*VIII*
IV	*XII*	*VIII*	*IV*	*XVI*
III	*IX*	*VI*	*III*	*XII*
I	*III*	*II*	*I*	*IV*

Z_2^+	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$Z_3^\times$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$
$[2]$	$[2]$	$[1]$

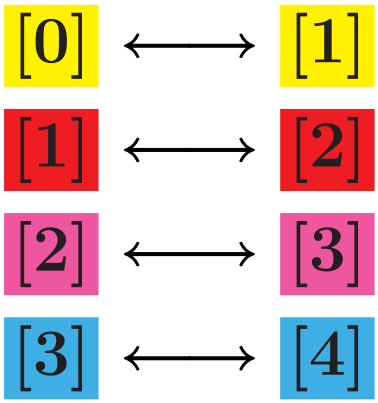

Z_2^+
[0]
[1]
[0]
[0]
[1]
[1]
[1]
[0]


$Z_3^\times$
[1]
[2]
[1]
[1]
[2]
[2]
[2]
[1]


[0]
[1]
[1]
[2]

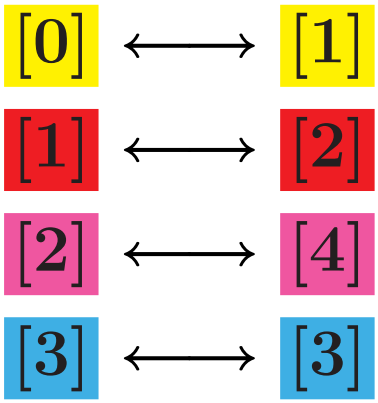
Z_4^+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$Z_5^\times$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]



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]

$Z_5^\times$	[1]	[2]	[4]	[3]
[1]	[1]	[2]	[4]	[3]
[2]	[2]	[4]	[3]	[1]
[4]	[4]	[3]	[1]	[2]
[3]	[3]	[1]	[2]	[4]



Z_6^+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$Z_7^\times$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

Z_6^+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$Z_7^\times$	[1]	[3]	[2]	[6]	[4]	[5]
[1]	[1]	[3]	[2]	[6]	[4]	[5]
[3]	[3]	[2]	[6]	[4]	[5]	[1]
[2]	[2]	[6]	[4]	[5]	[1]	[3]
[6]	[6]	[4]	[5]	[1]	[3]	[2]
[4]	[4]	[5]	[1]	[3]	[2]	[6]
[5]	[5]	[1]	[3]	[2]	[6]	[4]

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]

V	(1)	(12)(34)	(13)(24)	(14)(23)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)

$$[0] \longleftrightarrow (1)$$
$$[1] \longleftrightarrow (12)(34)$$
$$[2] \longleftrightarrow (13)(24)$$
$$[3] \longleftrightarrow (14)(23)$$

Definition:

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

$$f(x * y) = f(x) \circ f(y)$$

for all $x, y \in G$.

Example:

Let $(G, *)$ be an arbitrary group and $H = \{e\}$, then the function

$$f : G \longrightarrow H$$

such that

$$f(x) = e \quad \text{for any} \quad x \in G$$

is a homomorphism. In fact,

$$f(x * y) = e = e \circ e = f(x) \circ f(y).$$

Example:

Let $(G, *)$ be an arbitrary group, then the function $f : G \longrightarrow G$ such that

$$f(x) = x \quad \text{for any} \quad x \in G$$

is a homomorphism. In fact,

$$f(x * y) = x * y = f(x) * f(y).$$

Example:

Let $f : Z^+ \longrightarrow Z_2^+$ be a function such that

$$f(x) = \begin{cases} [0] \text{ if } x \text{ is even} \\ [1] \text{ if } x \text{ is odd} \end{cases}$$

Then f is a homomorphism. In fact, if $x + y$ is even, then

$$f(x + y) = [0] = f(x) + f(y).$$

Similarly, if $x + y$ is odd, then

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

Example:

Let $f : GL(2, R) \longrightarrow R^{\times}_{\neq 0}$ be a function such that

$$f(M) = \det M$$

for any $M \in GL(2, R)$. Then f is a homomorphism. In fact,

$$\begin{aligned} f(M_1 M_2) &= \det(M_1 M_2) \\ &= \det(M_1)\det(M_2) \\ &= f(M_1) f(M_2). \end{aligned}$$

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 $R^+ \cong R^\times_{>0}$. In fact, let

$$f(x) = e^x.$$

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

$$f : R^+ \longrightarrow R^\times_{>0}$$

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 $a_i a_j$:

G	a_1	a_2	$\ldots$	a_j	$\ldots$	a_n
a_1	a_1a_2	a_1a_2	$\ldots$	a_1a_j	$\ldots$	a_1a_n
a_2	a_2a_1	a_2a_2	$\ldots$	a_2a_j	$\ldots$	a_2a_n
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	a_ia_1	a_ia_2	$\ldots$	a_ia_j	$\ldots$	a_ia_n
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	a_na_1	a_na_2	$\ldots$	a_na_j	$\ldots$	a_na_n

We will also agree that $a_1 = 1$.

Example:

Multiplicative table for $Z_5^\times$ is

$Z_5^\times$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[4]$	$[3]$	$[2]$	$[1]$

Remark:

It is clear that two groups

$$G = \{a_1, a_2, \ldots, a_n\}$$

and

$$H = \{b_1, b_2, \ldots, b_n\}$$

of the same order 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 $\mathcal{P} \cong Z_2^+ \cong Z_3^\times$:

$\mathcal{P}$	"even"	"odd"
"even"	"even"	"odd"
"odd"	"odd"	"even"

Z_2^+	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$Z_3^\times$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$
$[2]$	$[2]$	$[1]$

2. The multiplication tables below show that $Z_4^+ \cong Z_5^\times$:

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]

$Z_5^\times$	[1]	[2]	[4]	[3]
[1]	[1]	[2]	[4]	[3]
[2]	[2]	[4]	[3]	[1]
[4]	[4]	[3]	[1]	[2]
[3]	[3]	[1]	[2]	[4]

3. The multiplication tables below show that $Z_6^+ \cong Z_7^\times$:

Z_6^+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$Z_7^\times$	[1]	[3]	[2]	[6]	[4]	[5]
[1]	[1]	[3]	[2]	[6]	[4]	[5]
[3]	[3]	[2]	[6]	[4]	[5]	[1]
[2]	[2]	[6]	[4]	[5]	[1]	[3]
[6]	[6]	[4]	[5]	[1]	[3]	[2]
[4]	[4]	[5]	[1]	[3]	[2]	[6]
[5]	[5]	[1]	[3]	[2]	[6]	[4]

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 $n \in Z$.

(i) We have

$$e \cdot e = e \quad \Longrightarrow \quad f(e \cdot e) = f(e),$$

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

$$x \cdot x^{-1} = e \quad \Longrightarrow \quad f(x \cdot x^{-1}) = f(e),$$

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 Z_{p-1}^{+} is cyclic, since

$$Z_{p-1}^{+} = \langle [1] \rangle.$$

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

$$|Z_{p-1}^{+}| = |Z_p^{\times}| = p - 1.$$

Therefore from Theorem 2 it follows that $Z_{p-1}^{+} \cong Z_p^{\times}$.

Problem: Show that $\mathbf{V} \ncong Z_4^+$.

Solution:

Assume to the contrary that $\mathbf{V} \cong Z_4^+$. Then there is a one-one correspondence $f : \mathbf{V} \longrightarrow Z_4^+$. From this, in particularly, follows that there exists $x \in \mathbf{V}$ 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 $x \in \mathbf{V}$ we have

$$x^2 = e.$$

By this and (i) of Theorem 1 we get

$$f(x^2) = f(e) = e = [0].$$

This is a contradiction. ■

Definition:

If $f : G \longrightarrow H$ is a homomorphism, define

$$\ker f = \{x \in G : f(x) = 1\}.$$

Theorem 3:

Let $f : G \longrightarrow H$ be a homomorphism. Then $\ker f$ is a subgroup of G

Proof:

From (i) of Theorem 1 it follows that $1 \in \ker f$, since $f(1) = 1$. Next, if $x, y \in \ker f$, then

$$f(x) = 1 = f(y),$$

hence

$$f(xy) = f(x)f(y) = 1 \cdot 1 = 1,$$

so $xy \in \ker f$. Finally, if $x \in \ker f$, then $f(x) = 1$ and so

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

hence $x^{-1} \in \ker f$. Therefore $\ker f$ is a subgroup of G.