MTH 4441 HW #5 - Isomorphisms - Solutions

FALL 2017

Pat Rossi Name _____

1. Show that $(\mathbb{Z}_n, +) = (\{0, 1, 2, \ldots, n-1\}, +)$, where "+" is addition modulo n, is a group.

   (a) First observe that $\mathbb{Z}_n$ is closed under addition modulo n, as the sum of *any* two integers modulo n is an element of the set $\{0, 1, 2, \ldots, n-1\} = \mathbb{Z}_n$.

   (b) Next, observe that $0 \in \mathbb{Z}_n$. (i.e., $\mathbb{Z}_n$ contains the *identity*, modulo n.)

   (c) To show that every element of $\mathbb{Z}_n$ has an additive inverse (modulo n) that is also contained in $\mathbb{Z}_n$, **observe that:**

      1. 0 is its own inverse

      2. If k is a non-zero element of $\mathbb{Z}_n$, then $(n-k) \in \mathbb{Z}_n$ is the inverse of k.

         To see this, note that if k is a non-zero element of $\mathbb{Z}_n$, then $1 \leq (n-k) \leq n-1$.

         (i.e., if k is a non-zero element of $\mathbb{Z}_n$, then $(n-k) \in \mathbb{Z}_n$ also.)

         In addition, $k + (n-k) \equiv 0 \bmod n$

         (i.e., $k + (n-k) = 0$ in the group $(\mathbb{Z}_n, +)$.)

         Hence, if k is a non-zero element of $\mathbb{Z}_n$, then $(n-k)$ is the inverse of k.

   (d) Finally, addition modulo n is associative.

2. Construct the group table for $(\mathbb{Z}_6, +)$

$(\mathbb{Z}_6, +)$

+	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

3. In the preceding example:

   (a) What is the inverse of 2?

   Observe that: $2 + 4 = 0$ (the identity)

   and that: $4 + 2 = 0$ (the identity)

   So 4 is the additive inverse of 2.

   (b) What is the inverse of 3?

   Observe that: $3 + 3 = 0$ (the identity)

   So 3 is its own inverse.

4. Construct the group table for $(\mathbb{Z}_4, +)$

$(\mathbb{Z}_4, +)$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

5. Construct the group table for $(U_5, \cdot)$

$(U_5, \cdot)$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

6. With reference to exercises 4 and 5, show that the two groups are isomorphic by defining an isomorphism $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$

   Since ϕ is an isomorphism, ϕ must map "identity to identity."

   i.e., $\phi(0) = 1$

   Also, Since ϕ is an isomorphism, ϕ must map "inverse to inverse."

   Since $2 \in (\mathbb{Z}_4, +)$ is its own inverse, ϕ must map 2 to an element in $(U_5, \cdot)$ that is its own inverse. Therefore, it must be the case that $\phi(2) = 4$

   We have a choice in assignments of $\phi(1)$ and $\phi(3)$

   We can either assign $\begin{cases} \phi(1) = 2 \\ \phi(3) = 3 \end{cases}$ or we can assign $\begin{cases} \phi(1) = 3 \\ \phi(3) = 2 \end{cases}$

Thus, the possibilities are:

$$\boxed{\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot), \text{ given by } \begin{cases} \phi(0) = 1 \\ \phi(1) = 2 \\ \phi(2) = 4 \\ \phi(3) = 3 \end{cases}} \quad \text{or} \quad \boxed{\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot), \text{ given by } \begin{cases} \phi(0) = 1 \\ \phi(1) = 3 \\ \phi(2) = 4 \\ \phi(3) = 2 \end{cases}}$$

7. Show that the function ϕ in the previous exercise is an isomorphism.

Case 1: $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$, given by $\begin{cases} \phi(0) = 1 \\ \phi(1) = 2 \\ \phi(2) = 4 \\ \phi(3) = 3 \end{cases}$

Clearly, $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$, as we have defined it, is one-to-one and onto.

We must also show that $\phi(x + y) = \phi(x) \cdot \phi(y)$ and that $\phi(y + x) = \phi(y) \cdot \phi(x)$, $\forall x, y \in \mathbb{Z}_4$

Note that since both groups are commutative (the group tables are symmetric about the "main diagonal"), it is only necessary to show that $\phi(x + y) = \phi(x) \cdot \phi(y)$ $\forall x, y \in \mathbb{Z}_4$

Observe:
$\phi(0 + y) = \phi(y) = 1 \cdot \phi(y) = \phi(0) \cdot \phi(y)$ $\forall y \in \mathbb{Z}_4$

i.e., $\phi(0 + y) = \phi(0) \cdot \phi(y)$ and $\phi(y + 0) = \phi(y) \cdot \phi(0)$, $\forall y \in \mathbb{Z}_4$

Observe: $\phi(1 + 1) = \phi(2) = 4$

and $\phi(1) \cdot \phi(1) = 2 \cdot 2 = 4$

i.e., $\phi(1 + 1) = \phi(1) \cdot \phi(1)$

Observe: $\phi(1 + 2) = \phi(3) = 3$

and $\phi(1) \cdot \phi(2) = 2 \cdot 4 = 8 \cong 3 \pmod 5$

i.e., $\phi(1 + 2) = \phi(1) \cdot \phi(2)$ and $\phi(2 + 1) = \phi(2) \cdot \phi(1)$

Observe: $\phi(1 + 3) = \phi(0) = 1$

and $\phi(1) \cdot \phi(3) = 2 \cdot 3 = 6 \cong 1 \pmod 5$

i.e., $\phi(1 + 3) = \phi(1) \cdot \phi(3)$ and $\phi(3 + 1) = \phi(3) \cdot \phi(1)$

Observe: $\phi(2 + 2) = \phi(0) = 1$

and $\phi(2) \cdot \phi(2) = 4 \cdot 4 = 16 \cong 1 \pmod 5$

i.e., $\phi(2 + 2) = \phi(2) \cdot \phi(2)$

Observe: $\phi(2+3) = \phi(1) = 2$

and $\phi(2) \cdot \phi(3) = 4 \cdot 3 = 12 \cong 2 \pmod 5$

i.e., $\phi(2+3) = \phi(2) \cdot \phi(3)$ and $\phi(3+2) = \phi(3) \cdot \phi(2)$

Observe: $\phi(3+3) = \phi(2) = 4$

and $\phi(3) \cdot \phi(3) = 2 \cdot 2 = 4$

i.e., $\phi(3+3) = \phi(3) \cdot \phi(3)$

This exhausts all possibilities. In each case, $\phi(x+y) = \phi(x) \cdot \phi(y)$ and $\phi(y+x) = \phi(y) \cdot \phi(x)$ $\forall x, y \in G$

Hence, $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$, given by $\begin{cases} \phi(0) = 1 \\ \phi(1) = 2 \\ \phi(2) = 4 \\ \phi(3) = 3 \end{cases}$ is an isomorphism.

Case 2: $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$, given by $\begin{cases} \phi(0) = 1 \\ \phi(1) = 3 \\ \phi(2) = 4 \\ \phi(3) = 2 \end{cases}$

Clearly, $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$, as we have defined it, is one-to-one and onto.

We must also show that $\phi(x+y) = \phi(x) \cdot \phi(y)$ and that $\phi(y+x) = \phi(y) \cdot \phi(x)$, $\forall x, y \in \mathbb{Z}_4$

Note that since both groups are commutative (the group tables are symmetric about the "main diagonal"), it is only necessary to show that $\phi(x+y) = \phi(x) \cdot \phi(y)$ $\forall x, y \in \mathbb{Z}_4$

Observe:

$\phi(0+y) = \phi(y) = 1 \cdot \phi(y) = \phi(0) \cdot \phi(y)$ $\forall y \in \mathbb{Z}_4$

i.e., $\phi(0+y) = \phi(0) \cdot \phi(y)$ and $\phi(y+0) = \phi(y) \cdot \phi(0)$, $\forall y \in \mathbb{Z}_4$

Observe: $\phi(1+1) = \phi(2) = 4$

and $\phi(1) \cdot \phi(1) = 3 \cdot 3 = 9 \cong 4 \pmod 5$

i.e., $\phi(1+1) = \phi(1) \cdot \phi(1)$

Observe: $\phi(1+2) = \phi(3) = 2$

and $\phi(1) \cdot \phi(2) = 3 \cdot 4 = 12 \cong 2 \pmod 5$

i.e., $\phi(1+2) = \phi(1) \cdot \phi(2)$ and $\phi(2+1) = \phi(2) \cdot \phi(1)$

Observe: $\phi(1+3) = \phi(0) = 1$

and $\phi(1) \cdot \phi(3) = 3 \cdot 2 = 6 \cong 1 \pmod 5$

i.e., $\phi(1+3) = \phi(1) \cdot \phi(3)$ and $\phi(3+1) = \phi(3) \cdot \phi(1)$

Observe: $\phi(2+2) = \phi(0) = 1$

and $\phi(2) \cdot \phi(2) = 4 \cdot 4 = 16 \cong 1 \pmod 5$

i.e., $\phi(2+2) = \phi(2) \cdot \phi(2)$

Observe: $\phi(2+3) = \phi(1) = 3$

and $\phi(2) \cdot \phi(3) = 4 \cdot 2 = 8 \cong 3 \pmod 5$

i.e., $\phi(2+3) = \phi(2) \cdot \phi(3)$ and $\phi(3+2) = \phi(3) \cdot \phi(2)$

Observe: $\phi(3+3) = \phi(2) = 4$

and $\phi(3) \cdot \phi(3) = 2 \cdot 2 = 4$

i.e., $\phi(3+3) = \phi(3) \cdot \phi(3)$

This exhausts all possibilities. In each case, $\phi(x+y) = \phi(x) \cdot \phi(y)$ and $\phi(y+x) = \phi(y) \cdot \phi(x)$ $\forall x, y \in G$

Hence, $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$, given by $\begin{cases} \phi(0) = 1 \\ \phi(1) = 3 \\ \phi(2) = 4 \\ \phi(3) = 2 \end{cases}$ is an isomorphism.

8. As incredible as it seems, the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$, where "+" and "$\cdot$" are the usual addition and multiplication of real numbers, are isomorphic. Show that $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, given by $\phi(x) = e^x$, is an isomorphism. (the function e^x is the exponential function (that we all know and love) from Calculus.)

First, we must show that $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, given by $\phi(x) = e^x$, is one-to-one and onto.

ϕ is one to one

Suppose that $\phi(x_1) = \phi(x_2)$

$\Rightarrow e^{x_1} = e^{x_2}$

$\Rightarrow \ln(e^{x_1}) = \ln(e^{x_2})$

$\Rightarrow x_1 = x_2$

i.e., $\phi(x_1) = \phi(x_2) \Rightarrow x_1 = x_2$

Hence, ϕ is one to one

ϕ is onto

Suppose that $y \in \mathbb{R}^+$

Let $x \in \mathbb{R}$ be given by $x = \ln(y)$

Observe: $\phi(x) = \phi(\ln(y)) = e^{\ln(y)} = y$

i.e., Given $y \in \mathbb{R}^+$, $\exists\, x \in \mathbb{R}$ (namely $x = \ln(y)$) such that $\phi(x) = y$

Hence, ϕ is onto

Next, we must show that $\phi(x + y) = \phi(x) \cdot \phi(y)$

Observe: $\phi(x + y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$

i.e., $\phi(x + y) = \phi(x) \cdot \phi(y)$

Hence, $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, given by $\phi(x) = e^x$, is an isomorphism.

Relating to Exercises 9-11, Given sets S_1 and S_2, the **product** of S_1 and S_2, denoted $S_1 \times S_2$, is given by:

$$S_1 \times S_2 = \{(x, y) : x \in S_1 \text{ and } y \in S_2\}$$

Addition of elements in $S_1 \times S_2$ is done component-wise: $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

9. Construct the group table for $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, starting with:

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

10. Recall from class lectures that $(G_3, *_3)$ was not isomorphic to either $(G_1, *_1) = (U_5, \cdot)$ or $(G_2, *_2)$ (all shown below). Show that $(G_3, *_3)$ IS isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ of the previous exercise by exhibiting an isomorphism $\phi : (G_3, *_3) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

$(G_1, *_1) = (U_5, \cdot)$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(G_2, *_2)$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$(G_3, *_3)$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Observe: An Isomorphism $\phi : (G_3, *_3) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ must be such that "identity maps to identity."

Thus, $\phi(e) = (0,0)$

Also: An Isomorphism $\phi : (G_3, *_3) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ must be such that "inverse maps to inverse."

In $(G_3, *_3)$ and in $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, EVERY element is its own inverse.

The ramifications of this fact are that ANY non-identity element in $(G_3, *_3)$ can be mapped to ANY non-identity element in $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

Arbitrarily, we will make the following assignments:

$\phi(a) = (1,0)$

$\phi(b) = (0,1)$

$\phi(c) = (1,1)$

Thus, we have: $\phi : (G_3, *_3) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ given by: $\begin{cases} \phi(e) = (0,0) \\ \phi(a) = (1,0) \\ \phi(b) = (0,1) \\ \phi(c) = (1,1) \end{cases}$

(**Note:** ANY one-to-one and onto function $\phi : (G_3, *_3) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, such that $\phi(e) = (0,0)$ will be an isomorphism.)

11. Show that $(G_3, *_3) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, as defined in the previous exercise, IS an isomorphism.

Clearly, $\phi : (G_3, *_3) \to (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ given by: $\begin{cases} \phi(e) = (0,0) \\ \phi(a) = (1,0) \\ \phi(b) = (0,1) \\ \phi(c) = (1,1) \end{cases}$ is **one-to-one and onto.**

We must also show that $\phi(x+y) = \phi(x) \cdot \phi(y)$ and that $\phi(y+x) = \phi(y) \cdot \phi(x)$, $\forall x, y \in \mathbb{Z}_4$

Note that since both groups are commutative (the group tables are symmetric about the "main diagonal"), it is only necessary to show that $\phi(x *_3 y) = \phi(x) + \phi(y)$ $\forall x, y \in G_3$

Observe:

$\phi(e *_3 y) = \phi(y) = (0,0) + \phi(y) = \phi(e) + \phi(y)$ $\forall y \in G_3$

i.e., $\phi(e *_3 y) = \phi(e) + \phi(y)$ and $\phi(y *_3 e) = \phi(y) + \phi(e)$, $\forall y \in \mathbb{Z}_4$

Observe: $\phi(a *_3 a) = \phi(e) = (0,0)$

and $\phi(a) + \phi(a) = (0,0) + (0,0) = (0,0)$

i.e., $\phi(a *_3 a) = \phi(a) + \phi(a)$

Observe: $\phi(a *_3 b) = \phi(c) = (1,1)$

and $\phi(a) + \phi(b) = (1,0) + (0,1) = (1,1)$

i.e., $\phi(a *_3 b) = \phi(a) + \phi(b)$ and $\phi(b *_3 a) = \phi(b) + \phi(a)$

Observe: $\phi(a *_3 c) = \phi(b) = (0,1)$

and $\phi(a) + \phi(c) = (1,0) + (1,1) = (0,1)$

i.e., $\phi(a *_3 c) = \phi(a) + \phi(c)$ and $\phi(c *_3 a) = \phi(c) + \phi(a)$

Observe: $\phi(b *_3 b) = \phi(e) = (0,0)$

and $\phi(b) + \phi(b) = (0,1) + (0,1) = (0,0)$

i.e., $\phi(b *_3 b) = \phi(b) + \phi(b)$

Observe: $\phi(b *_3 c) = \phi(a) = (1,0)$

and $\phi(b) + \phi(c) = (0,1) + (1,1) = (1,0)$

i.e., $\phi(b *_3 c) = \phi(b) + \phi(c)$ and $\phi(c *_3 b) = \phi(c) + \phi(b)$

Observe: $\phi(c *_3 c) = \phi(e) = (0,0)$

and $\phi(c) + \phi(c) = (1,1) + (1,1) = (0,0)$

i.e., $\phi(c *_3 c) = \phi(c) + \phi(c)$

This exhausts all possibilities. In each case, $\phi(x+y) = \phi(x) \cdot \phi(y)$ and $\phi(y+x) = \phi(y) \cdot \phi(x)$ $\forall x, y \in G$

Hence, $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$, given by $\begin{cases} \phi(0) = 1 \\ \phi(1) = 3 \\ \phi(2) = 4 \\ \phi(3) = 2 \end{cases}$ is an isomorphism.

12. From previous examples, list all algebraic properties that isomorphisms preserve and all properties that isomorphic groups have in common.

    (a) Finite groups that are isomorphic have the same order. (i.e., if $(G_1, *_1) \cong (G_2, *_2)$, then $|G_1| = |G_2|$.
    Contrapositively, if $|G_1| \neq |G_2|$, then $(G_1, *_1) \ncong (G_2, *_2)$

    (b) Isomorphisms "map identity to identity." (i.e. if e is the identity in $(G_1, *_1)$, then $\phi(e)$ is the identity in $(G_2, *_2)$)

    (c) Isomorphisms "map inverse to inverse." (i.e. if a^{-1} is the inverse of a in $(G_1, *_1)$, then $\phi\left(a^{-1}\right)$ is the inverse $\phi(a)$ of in $(G_2, *_2)$)

    (d) Isomorphic groups have the same number of elements that are their own inverses.

    (e) Isomorphisms "map subgroup to subgroup." (i.e., if $(G_1, *_1) \cong (G_2, *_2)$, then $(G_1, *_1)$ and $(G_2, *_2)$ have the same number of subgroups of order each order. (e.g. if $(G_1, *_1)$ has 3 subgroups of order 5, then $(G_2, *_2)$ has 3 subgroups of order 5.))

    (f) If $(G_1, *_1) \cong (G_2, *_2)$ and $(G_1, *_1)$ is **cyclic,** then $(G_2, *_2)$ must be **cyclic** also.
    Conversely, if $(G_1, *_1)$ and $(G_2, *_2)$ are **both cyclic and of the same order,** then $(G_1, *_1) \cong (G_2, *_2)$

    (g) If $(G_1, *_1) \cong (G_2, *_2)$ and the groups are cyclic, then if $\phi : (G_1, *_1) \to (G_2, *_2)$ is an isomorphism,then ϕ "maps generator to generator." (i.e., if $(G_1, *_1) = \langle a \rangle$, then $(G_2, *_2) = \langle \phi(a) \rangle$)