MTH 4441 Test #2 - Solutions

FALL 2021

Pat Rossi Name _____

1. Define - Cyclic group

   A group $(G, *)$ is a **cyclic group,** exactly when $\exists x \in G$ such that $G = \{nx : n \in \mathbb{Z}\}$ (additive notation), or $G = \{x^n : n \in \mathbb{Z}\}$ (multiplicative notation). In such a case, we write: $\langle x \rangle = (G, *)$, and we say that "$x$ is a generator of $(G, *)$,"or that "$(G, *)$ is generated by x."

2. Define - Direct Product of groups $(G, *_G)$ and $(H *_H)$

   Given groups $(G, *_1)$ and $(H, *_2)$, the **direct product of groups** $G \times H$, together with the inherited operations $*_1$ and $*_2$, form a group $(G \times H, *)$, where $*$ is the operation $*_1$ on the first coordinate and $*$ is the operation $*_2$ on the second coordinate.

3. Define - Isomorphism

   Given groups $(G, *_G)$ and $(H, *_H)$, and a function $f : (G, *_G) \to (H, *_H)$, the function f is said to be an **isomorphism** exactly when:

   1) f is one to one and onto, and

   2) $f(g_1 *_G g_2) = f(g_1) *_H f(g_2)$

   In this case, groups $(G, *_G)$ and $(H, *_H)$ are said to be **isomorphic,** and we write $(G, *_G) \cong (H, *_H)$.

4. **Prove or Disprove:** $(\mathbb{R}, +)$ is a cyclic group

   This is False.

   pf/ If $(\mathbb{R}, +)$ were a cyclic group, then $(\mathbb{Q}, +)$ would be cyclic also, since every subgroup of a cyclic group is cyclic also.

   But $(\mathbb{Q}, +)$ is NOT cyclic.

   Hence, $(\mathbb{R}, +)$ is not cyclic. ■

Alternatively:

Suppose, for the sake of deriving a contradiction, that $(\mathbb{R}, +)$ is cyclic.

Then $\exists r \in \mathbb{R}$ such that $\langle r \rangle = (\mathbb{R}, +)$

Thus every real number can be expressed as nr, for some $n \in \mathbb{Z}$.

Since $\mathbb{Z}$ is countably infinite, there are only countably infinitely many values of n, and hence only countably infinitely many values of nr.

This implies that $\mathbb{R}$ is countably infinite, contradicting the well known fact that $\mathbb{R}$ is uncountable.

Since the assumption that $(\mathbb{R}, +)$ is cyclic leads to a contradiction, the assumption must be false.

Hence, $(\mathbb{R}, +)$ is not cyclic.■

Alternatively:

Suppose, for the sake of deriving a contradiction, that $(\mathbb{R}, +)$ is cyclic.

Then $\exists r \in \mathbb{R}$ such that $\langle r \rangle = (\mathbb{R}, +)$

This means that every positive rational number must be of the form $n(r)$, for some $r \in \mathbb{R}$.

What about the real number $\frac{r}{2}$?

Since r generates $\mathbb{R}$, $\frac{r}{2} = nr$, for some $r \in \mathbb{R}$.

But $nr = \frac{r}{2} \Rightarrow n = \frac{1}{2}$. contradicting the fact that $n \in \mathbb{Z}$.

Since this contradiction is a consequence of our assumption that $(\mathbb{R}, +)$ is cyclic, the assumption must be false.

Hence, $(\mathbb{R}, +)$ is NOT cyclic ■

5. **Prove or Disprove:** $(\mathbb{Q}, +)$ is a cyclic group

   This is False.

   pf/ Suppose, for the sake of deriving a contradiction, that $(\mathbb{Q}, +)$ IS cyclic.

   Then $\exists\ a, b \in \mathbb{Z}$ such that $\left\langle \frac{a}{b} \right\rangle = (\mathbb{Q}, +)$

   This means that every positive rational number must be of the form $n\left(\frac{a}{b}\right)$, for some $n \in \mathbb{Z}$.

   What about the rational number $\frac{a}{2b}$?

   Since $\frac{a}{b}$ generates $\mathbb{Q}$, $\frac{a}{2b} = n\left(\frac{a}{b}\right)$, for some $n \in \mathbb{Z}$.

   But $n\left(\frac{a}{b}\right) = \frac{a}{2b} \Rightarrow n = \frac{1}{2}$. contradicting the fact that $n \in \mathbb{Z}$.

   Since this contradiction is a consequence of our assumption that $(\mathbb{Q}, +)$ is cyclic, the assumption must be false.

   Hence, $(\mathbb{Q}, +)$ is NOT cyclic ■

6. **Prove:** $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$

   pf/ We claim that: $f : \mathbb{R} \to \mathbb{R}^+$, given by $f(x) = e^x$ is our isomorphism.

   Note that $f^{-1} : \mathbb{R}^+ \to \mathbb{R}$, given by $f^{-1}(x) = \ln(x)$, is the inverse of f

   $(f \circ f^{-1}) : \mathbb{R}^+ \to \mathbb{R}^+$ is such that $(f \circ f^{-1}) = 1_{\mathbb{R}^+}$

   and

   $(f^{-1} \circ f) : \mathbb{R} \to \mathbb{R}$ is such that $(f^{-1} \circ f) = 1_{\mathbb{R}}$

   Hence, $f : \mathbb{R} \to \mathbb{R}^+$, given by $f(x) = e^x$ is one to one and onto.

   To show that f is an isomorphism and that $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$ isomorphic, we need to show that:

   $f(r_1 + r_2) = f(r_1) \cdot f(r_2)$

   Observe: $f(r_1 + r_2) = e^{r_1 + r_2} = e^{r_1} \cdot e^{r_2} = f(r_1) \cdot f(r_2)$

   Hence, $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$ are isomorphic. ■

Alternatively:

We can show that $f : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$, given by $f(x) = \ln(x)$ is an isomorphism.

Note that $g : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, given by $g(x) = e^x$, is such that $(g \circ f) : (\mathbb{R}^+, \cdot) \to (\mathbb{R}^+, \cdot)$ is the identity on $(\mathbb{R}^+, \cdot)$.

Hence, $f : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ is one to one and onto.

Next observe: $f(x_1 \cdot x_2) = \ln(x_1 \cdot x_2) = \ln(x_1) + \ln(x_2) = f(x_1) + f(x_2)$

Thus, f is an isomorphism. ■

In Exercises 7-10, determine whether the two groups are isomorphic. If they aren't, give at least one reason why. If they are, justify your answer either by exhibiting an isomorphism between the two groups, or by proving that they are isomorphic by some other method.

7. $(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$.

   ARE isomorphic.

   $f : \mathbb{Z} \to 2\mathbb{Z}$, given by $f(n) = 2n$ is clearly one to one and onto.

   $f(n_1 + n_2) = 2(n_1 + n_2) = 2n_1 + 2n_2 = f(n_1) + f(n_2)$

   i.e., $f(n_1 + n_2) = f(n_1) + f(n_2)$

   Thus, $(2\mathbb{Z}, +) \cong (3\mathbb{Z}, +)$.■

8. $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ and the group $(G, *)$ whose group table is given below:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

The group table for $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ is shown below:

$\oplus$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

They are NOT isomorphic.

Note that every element of $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ is its own inverse. This is not true for $(G, *)$. a and c are not their own inverses.

Alternatively, note that $(G, *)$ is cyclic with generators a and c. In $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$, every element has order 2 (or less), and therefore $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ can't be cyclic. ■

9. The groups $(G, *)$ and $(H, *)$, whose group tables are given below:

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

These groups ARE isomorphic.

$(G, *)$ is cyclic with generators a and c, and $(H, *)$ is cyclic with generators a and b.

Furthermore, both groups are of order 4. (i.e., $|G| = 4 = |H)|$

Since both groups are cyclic and of the same order, they are isomorphic. ■

10. The groups $(\mathbb{Z}_6, \oplus)$ and $(H, *)$, whose group tables are given below:

$\oplus$	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

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

These groups are NOT isomorphic.

Note that $(\mathbb{Z}_6, \oplus)$ is cyclic and the elements 1, 2, 3, 4, 5 are all generators.

$(H, *)$ is NOT cyclic, since $(H, *)$ is a group of order 6 and no element has order greater than 3.

Alternatively, note that $(\mathbb{Z}_6, \oplus)$ is abelian (commutative), whereas $(H, *)$ is NOT abelian (NOT commutative). For example, $d * f = b$ but $f * d = a$. ■

11. Given the group table for $(G, *)$, find all of the subgroups of $(G, *)$ and justify your answers. Draw a subgroup diagram for $(G, *)$.

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

To start off, we acknowledge that $(\{e\}, *)$ and $(G, *)$ are subgroups of $(G, *)$.

If there are other subgroups $(H, *)$, then $|H|$ must divide $|G|$.

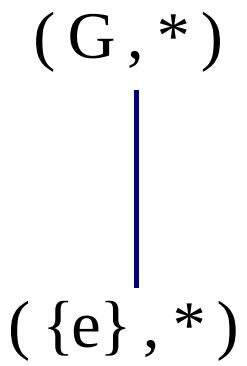
But $|G| = 5$

$\Rightarrow |H| = 1$ or $\Rightarrow |H| = 5$.

Thus, we have already accounted for all possible subgroups of $(G, *)$.

Hence $(\{e\}, *)$ and $(G, *)$ are the **only** subgroups of $(G, *)$.

Our subgroup diagram is below:



12. Construct the group table for $(\mathbb{Z}_4, \oplus)$, and then find all of the subgroups of $(\mathbb{Z}_4, \oplus)$ and justify your answers. Draw a subgroup diagram for $(\mathbb{Z}_4, \oplus)$.

Note that $(\mathbb{Z}_4, \oplus) = (\{0, 1, 2, 3\}, \oplus)$, where $\oplus$ is addition modulo 4

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

To start off, we acknowledge that $(\{0\}, \oplus)$ and $(\mathbb{Z}_4, \oplus)$ are subgroups of $(\mathbb{Z}_4, \oplus)$.

If there are other subgroups $(H, \oplus)$, then $|H|$ must divide $|\mathbb{Z}_4|$.

Since $|\mathbb{Z}_4| = 4$, this implies that $|H| = 1, 2$, or 4.

So we are looking for subgroups of order 2.

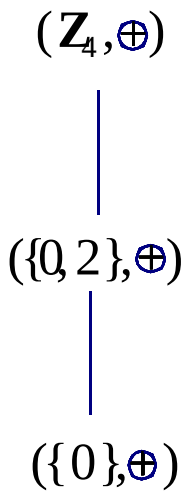
Such a subgroup would consist of the identity and an element of order 2 (i.e., an element that is its own inverse.)

From the group table, we can see that 2 is the only element, other than the identity, that fits this description.

Thus, $(\{0, 2\}, \oplus)$ is the only subgroup of order 2.

This exhausts all possibilities.

The subgroups of $(\mathbb{Z}_4, \oplus)$ are $(\{0\}, \oplus)$, $(\{0, 2\}, \oplus)$, and $(\mathbb{Z}_4, \oplus)$.



13. Calculate the order of the element $(4, 9)$ in the group $\mathbb{Z}_{18} \times \mathbb{Z}_{18}$

$o(4)$ is the order of 4 as an element of $\mathbb{Z}_{18}$

$o(4) = \frac{18}{\gcd(4,18)} = \frac{18}{2} = 9$

$o(9)$ is the order of 9 as an element of $\mathbb{Z}_{18}$

$o(9) = \frac{18}{\gcd(9,18)} = \frac{18}{9} = 2$

$o(4, 9)$ is the order of $(4, 9)$ as an element of $\mathbb{Z}_{18} \times \mathbb{Z}_{18}$

$o(4, 9) = \operatorname{lcm}(o(4), o(9)) = \operatorname{lcm}(9, 2) = \frac{9 \cdot 2}{\gcd(9,2)} = \frac{18}{1} = 18$

$\boxed{o(4, 9) = 18}$

(Note: $\operatorname{lcm}(a, b)$ is the least common multiple of a and b. $\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$)

(Note: $o(m)$ in $\mathbb{Z}_n$ is given by $\frac{n}{\gcd(m,n)}$the least common multiple of a and b. $\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$)

14. Calculate the order of the element $(8,6,4)$ in the group $\mathbb{Z}_{18} \times \mathbb{Z}_9 \times \mathbb{Z}_8$

$o(8)$ is the order of 8 as an element of $\mathbb{Z}_{18}$

$o(8) = \frac{18}{\gcd(8,18)} = \frac{18}{2} = 9$

$o(6)$ is the order of 6 as an element of $\mathbb{Z}_9$

$o(6) = \frac{9}{\gcd(6,9)} = \frac{9}{3} = 3$

$o(4)$ is the order of 4 as an element of $\mathbb{Z}_8$

$o(4) = \frac{8}{\gcd(4,8)} = \frac{8}{4} = 2$

$o(8,6,4)$ is the order of $(8,6,4)$ as an element of $\mathbb{Z}_{18} \times \mathbb{Z}_9 \times \mathbb{Z}_8$

$o(8,6,4) = \operatorname{lcm}(o(8), o(6), o(4)) = \operatorname{lcm}(9,3,2) = \operatorname{lcm}(\operatorname{lcm}(9,3),2)$

$\operatorname{lcm}(9,3) = \frac{9 \cdot 3}{\gcd(9,3)} = \frac{27}{3} = 9$

$\operatorname{lcm}(\operatorname{lcm}(9,3),2) = \operatorname{lcm}(9,2) = \frac{9 \cdot 2}{\gcd(9,2)} = \frac{18}{1} = 18$

$\boxed{o(8,6,4) = 18}$

(Note: $\operatorname{lcm}(a,b)$ is the least common multiple of a and b. $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$)

(note also: $\operatorname{lcm}(a,b,c) = \operatorname{lcm}(\operatorname{lcm}(a,b),c)$)

(Note: $o(m)$ in $\mathbb{Z}_n$ is given by $\frac{n}{\gcd(m,n)}$the least common multiple of a and b. $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$)