

MTH 4441 Test #2 - Solutions

FALL 2024

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

3. Define - Isomorphism

Given groups $(G, *G)$ and $(H, *H)$, and a function $f : (G, *G) \rightarrow (H, *H)$, 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 nr , 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 $n \in \mathbb{Z}$.

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 $\langle \frac{a}{b} \rangle = (\mathbb{Q}, +)$

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. Compute the sum of the elements $(5, 2)$ and $(4, 2)$ in the group $\mathbb{Z}_6 \times \mathbb{Z}_3$

The operation in (\mathbb{Z}_6, \oplus) is addition mod 6

The operation in (\mathbb{Z}_3, \oplus) is addition mod 3

The operation in $(\mathbb{Z}_6 \times \mathbb{Z}_3,)$ is addition mod 6 in the first component and addition mod 3 in the first component.

Thus, $(5, 2) \oplus (4, 2) = ((5 + 4) \bmod 6, (2 + 2) \bmod 2) = (3, 1)$

i.e., $(5, 2) \oplus (4, 2) = (3, 1)$

7. Find all of the subgroups of (\mathbb{Z}_7, \oplus) and justify your answers. Draw a subgroup diagram for (\mathbb{Z}_7, \oplus) .

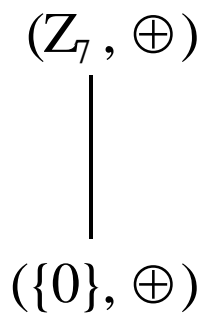
Ah! This is an easy one!

Observe that $|\mathbb{Z}_7| = 7$.

Since the order of a subgroup must divide the order of the group, any subgroups must either be of order 1 or 7.

Thus, our only subgroups are $(\{0\}, *)$ and $(\mathbb{Z}_7, *)$.

The subgroup diagram is shown below:



8. Construct the group table for (U_5, \odot) , and then find all of the subgroups of (U_5, \odot) and justify your answers. Draw a subgroup diagram for (U_5, \odot) . (Recall: $U_5 = \{1, 2, 3, 4\}$)

\odot	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Of course, every group has, as subgroups, itself and the group consisting of the identity.

i.e., (U_5, \odot) and $(\{1\}, \odot)$ are subgroups of order 4 and 1 respectively.

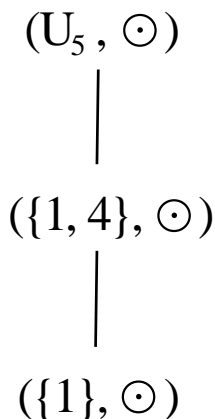
$|U_5| = 4$, so any subgroups would be such that their order must be a divisor of 4.

Since the divisors of 4 are 1, 2, 4; and since we have already accounted for all subgroups of order 1 and 4, we restrict our attention to prospective subgroups of order 2.

A subgroup of order 2 consists of the identity and itself. Since the inverse of each element of a subgroup must also be contained in the subgroup, each element of a group of order 2 must be its own inverse.

Looking at the group table, we can see that the only elements that are their own inverses are 1 and 4. Thus, $\{1, 4\}$ is the only subgroup of order 2.

The subgroup diagram for (U_5, \odot) is shown below.



9. Construct the group table for (\mathbb{Z}_6, \oplus) , and then find all of the subgroups of (\mathbb{Z}_6, \oplus) and justify your answers. Draw a subgroup diagram for (\mathbb{Z}_6, \oplus) .

(\mathbb{Z}_6, \oplus) is the set $\{0, 1, 2, 3, 4, 5\}$ under the operation of addition modulo 6.

\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

Of course, every group has, as subgroups, itself and the group consisting of the identity. i.e., (\mathbb{Z}_6, \oplus) and $(\{0\}, \oplus)$ are subgroups of order 6 and 1 respectively.

$|\mathbb{Z}_6| = 6$, so any subgroups would be such that their order must be a factor of 6.

Since the divisors of 6 are 1, 2, 3, 6; and since we have already accounted for all subgroups of order 1 and 6, we restrict our attention to prospective subgroups of order 2 and 3.

A subgroup of order 2 consists of the identity and itself. Since the inverse of each element of a subgroup must also be contained in the subgroup, each element of a group of order 2 must be its own inverse.

Looking at the group table, we can see that the only elements that are their own inverses are 0 and 3. Thus, $\{0, 3\}$ is the only subgroup of order 2.

In looking for a subgroup(s) of order 3, note that neither 1 nor 3 can be an element of such a group, because the order of an element must divide the order of any group/subgroup which contains it.

Considering elements 2 and 4, each element has order 3 and each element is the inverse of the other.

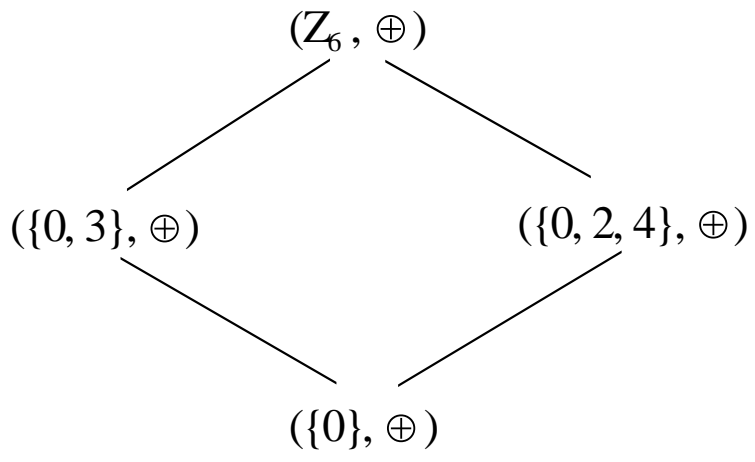
Hence, $\{0, 2, 4\}$ is a subgroup of order 3.

A quick consideration of the element 5 reveals that $o(5) = 6$.

Thus, we have exhausted all possibilities.

The subgroups of (\mathbb{Z}_6, \oplus) are $(\{0\}, \oplus)$, $(\{0, 3\}, \oplus)$, $(\{0, 2, 4\}, \oplus)$, and (\mathbb{Z}_6, \oplus) .

The subgroup diagram is shown below:



10. Construct the group table for $(\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$, and then find all of the subgroups of $(\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$ and justify your answers. Draw a subgroup diagram for $(\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$.

Note that since 2 and 3 are relatively prime, $\mathbb{Z}_3 \times \mathbb{Z}_2$ is cyclic. Its generators will be of the form: (m, n) where m is a generator of \mathbb{Z}_3 and where n is a generator of \mathbb{Z}_2 .

Thus, there are two generators of $\mathbb{Z}_3 \times \mathbb{Z}_2$, namely $(1, 1)$ and $(2, 1)$.

Note also that $(0, 0)$ is the identity of $\mathbb{Z}_3 \times \mathbb{Z}_2$.

Using $(1, 1)$ as the generator, we have:

\oplus	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$
$(0, 0)$	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$
$(1, 1)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$	$(0, 0)$
$(2, 0)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$	$(0, 0)$	$(1, 1)$
$(0, 1)$	$(0, 1)$	$(1, 0)$	$(2, 1)$	$(0, 0)$	$(1, 1)$	$(2, 0)$
$(1, 0)$	$(1, 0)$	$(2, 1)$	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$
$(2, 1)$	$(2, 1)$	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$

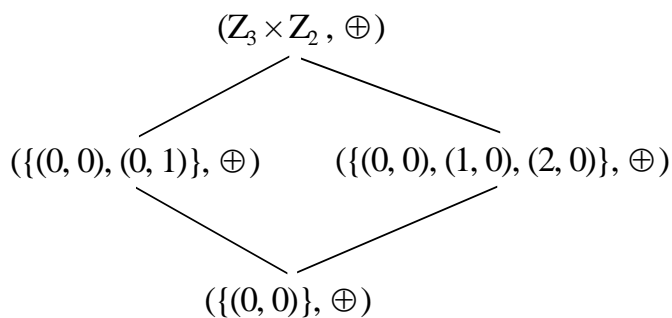
Since $|\mathbb{Z}_3 \times \mathbb{Z}_2| = 6$, any subgroups must have order 1, 2, 3, or 6, since these are the divisors of 6.

$$\langle (0, 0) \rangle = (\{(0, 0)\}, \oplus)$$

$$\langle (0, 1) \rangle = (\{(0, 0), (0, 1)\}, \oplus)$$

$$\langle (1, 0) \rangle = \langle (2, 0) \rangle = (\{(0, 0), (1, 0), (2, 0)\}, \oplus)$$

$$\langle (1, 1) \rangle = \langle (2, 1) \rangle = (\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$$



11. With reference to Exercises 9 and 10, Define an isomorphism from (\mathbb{Z}_6, \oplus) to $(\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$ and prove that $(\mathbb{Z}_6, \oplus) \cong (\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$

Observe that the function $f : (\mathbb{Z}_6, \oplus) \rightarrow (\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$, given by:

$$f(0) = (0, 0)$$

$$f(1) = (1, 1)$$

$$f(2) = (2, 0)$$

$$f(3) = (0, 1)$$

$$f(4) = (1, 0)$$

$$f(5) = (2, 1)$$

Yields the group table for $\mathbb{Z}_3 \times \mathbb{Z}_2$:

\oplus	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$
$(0, 0)$	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$
$(1, 1)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$	$(0, 0)$
$(2, 0)$	$(2, 0)$	$(0, 1)$	$(1, 0)$	$(2, 1)$	$(0, 0)$	$(1, 1)$
$(0, 1)$	$(0, 1)$	$(1, 0)$	$(2, 1)$	$(0, 0)$	$(1, 1)$	$(2, 0)$
$(1, 0)$	$(1, 0)$	$(2, 1)$	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$
$(2, 1)$	$(2, 1)$	$(0, 0)$	$(1, 1)$	$(2, 0)$	$(0, 1)$	$(1, 0)$

The group table for (\mathbb{Z}_6, \oplus) is shown 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

(Continued on the next page)

Note that the group table for $(\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$ can be obtained from the group table for (\mathbb{Z}_6, \oplus) , just by renaming the elements of \mathbb{Z}_6 as follows:

$$f(0) \text{ as } (0, 0)$$

$$f(1) \text{ as } (1, 1)$$

$$f(2) \text{ as } (2, 0)$$

$$f(3) \text{ as } (0, 1)$$

$$f(4) \text{ as } (1, 0)$$

$$f(5) \text{ as } (2, 1)$$

$$\text{Hence, } (\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus) \cong (\mathbb{Z}_6, \oplus)$$

12. (Extra - 5 pts) Calculate the order of the element $(4, 8)$ in the group $\mathbb{Z}_{18} \times \mathbb{Z}_{10}$

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

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

$o(8)$ is the order of 8 as an element of \mathbb{Z}_{10}

$$o(8) = \frac{10}{\gcd(8,10)} = \frac{10}{2} = 5$$

$o(4, 8)$ is the order of $(4, 8)$ as an element of $\mathbb{Z}_{18} \times \mathbb{Z}_{10}$

$$o(4, 8) = \text{lcm}(o(4), o(8)) = \text{lcm}(9, 5) = \frac{9 \cdot 5}{\gcd(9,5)} = \frac{45}{1} = 45$$

$o(4, 8) = 45$

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

(Note: $o(m)$ in \mathbb{Z}_n is given by $\frac{n}{\gcd(m,n)}$)

13. (Extra - 5 pts) 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 $\mathbb{Z}_{18} \times \mathbb{Z}_9 \times \mathbb{Z}_8$

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

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

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

$$o(8, 6, 4) = 18$$

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

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

(Note: $o(m)$ in \mathbb{Z}_n is given by $\frac{n}{\gcd(m,n)}$)