MTH 4441 Test #2 - Solutions

FALL 2022

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. **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 ■

4. **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 ■

5. 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., $\boxed{(5, 2) \oplus (4, 2) = (3, 1)}$

6. 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

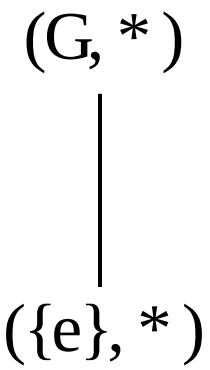
Ah! This is an easy one!

Observe that $|G| = 5$.

Since the order of a subgroup must divide the order of the group, any subgroups must either be of order 1 or 5.

Thus, our only subgroups are $(\{e\}, *)$ and $(G, *)$.

The subgroup diagram is shown below:



7. 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.

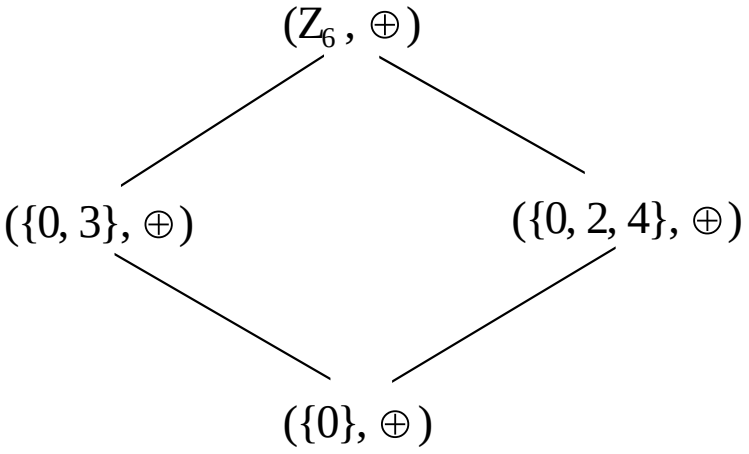
Hence, $\{0, 2, 4\}$ is a subgroup of order 3.

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:



8. Calculate the order of the element $(4, 9)$ in the group $\mathbb{Z}_{18} \times \mathbb{Z}_{12}$

   $o(4)$ 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 $\mathbb{Z}_{12}$

   $o(9) = \frac{12}{\gcd(9,12)} = \frac{12}{3} = 4$

   $o(4, 9)$ is the order of $(4, 9)$ as an element of $\mathbb{Z}_{18} \times \mathbb{Z}_{12}$

   $o(4, 9) = \operatorname{lcm}(o(4), o(9)) = \operatorname{lcm}(9, 4) = \frac{4 \cdot 9}{\gcd(9,4)} = \frac{36}{1} = 36$

   $\boxed{o(4, 9) = 36}$

9. 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. $\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$)

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

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

10. Construct the group table for $(U_7, \odot)$, and then find all of the subgroups of $(U_7, \odot)$ and justify your answers. Draw a subgroup diagram for $(U_7, \odot)$. (Recall: $U_7 = \{1, 2, 3, 4, 5, 6\}$) and the operation $\odot$ is multiplication mod 7)

$\odot$	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