MTH 4441 HW #6 - SUBGROUPS - Solutions

Fall 2021

Pat Rossi Name ______________________________

1. 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 $|G|$.

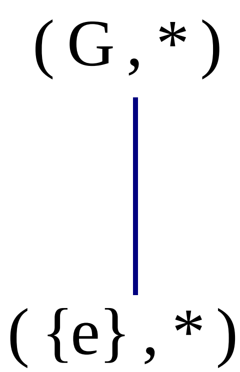
But $|G| = 5$

$\Rightarrow |H| = 1$ 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:



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

$*$	e	v	w	x	y	z
e	e	v	w	x	y	z
v	v	w	x	y	z	e
w	w	x	y	z	e	v
x	x	y	z	e	v	w
y	y	z	e	v	w	x
z	z	e	v	w	x	y

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

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

Since $|G| = 6$, this implies that $|H| = 1, 2, 3$, or 6.

So we are looking for subgroups of order 2 or order 3.

Since 2 and 3 are both prime numbers, any subgroups of order 2 or 3 must be cyclic, (because the order of an element in a group must divide the order of the group.)

Thus, to find the subgroups of order 2 or 3, we are looking for elements of order 2 or 3.

Observe: $v * v = w$, and $v * (v * v) = v * w = x$

Since $o(v) \neq 2, 3$; v is not a generator of a subgroup of order 2 or 3.

Observe: $w * w = y$, and $w * (w * w) = w * y = e$

Thus, $\langle w \rangle = (\{e, w, y\}, *)$

(Also note that $\langle y \rangle = (\{e, w, y\}, *)$ as well)

Observe: $x * x = e$

Thus, $\langle x \rangle = (\{e, x\}, *)$ (subgroup of order 2)

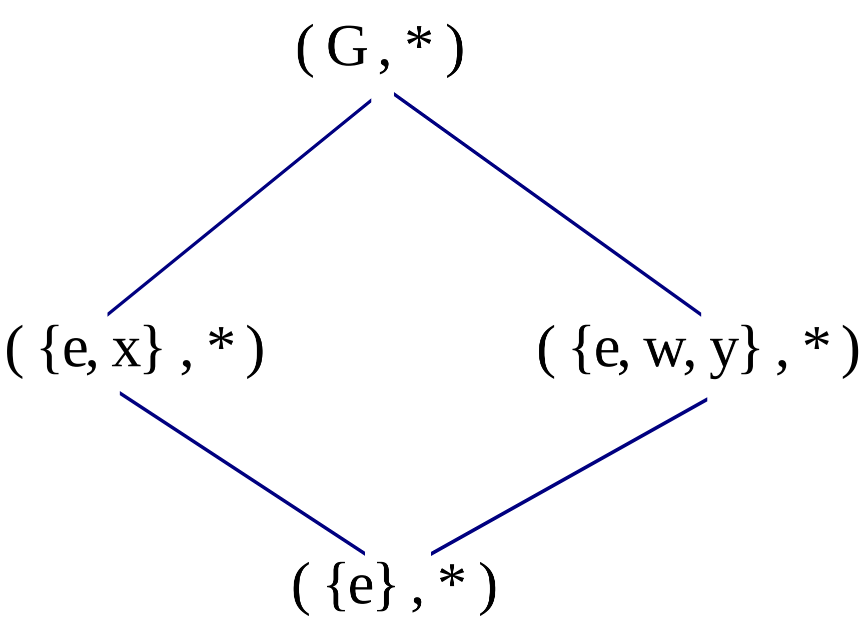
Observe: $z * z = y$, and $z * (z * z) = z * y = x$

Since $o(z) \neq 2, 3$; z is not a generator of a subgroup of order 2 or 3.

This exhausts all possibilities. We have accounted for all subgroups of $(G, *)$.

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

Our subgroup diagram is below:



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

$*$	e	v	w	x	y	z
e	e	v	w	x	y	z
v	v	e	x	z	w	y
w	w	x	e	y	z	v
x	x	z	y	e	v	w
y	y	w	z	v	e	x
z	z	y	v	w	x	e

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

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

Since $|G| = 6$, this implies that $|H| = 1, 2, 3$, or 6.

So we are looking for subgroups of order 2 or order 3.

Since 2 and 3 are both prime numbers, any subgroups of order 2 or 3 must be cyclic, (because the order of an element in a group must divide the order of the group.)

Thus, to find the subgroups of order 2 or 3, we are looking for elements of order 2 or 3.

Note, by looking at the group table for $(G, *)$, that every element is its own inverse. (The identity appears in every location on the main diagonal.)

Thus, the identity has order 1 and every other element has order 2.

There are 2 consequences of this observation:

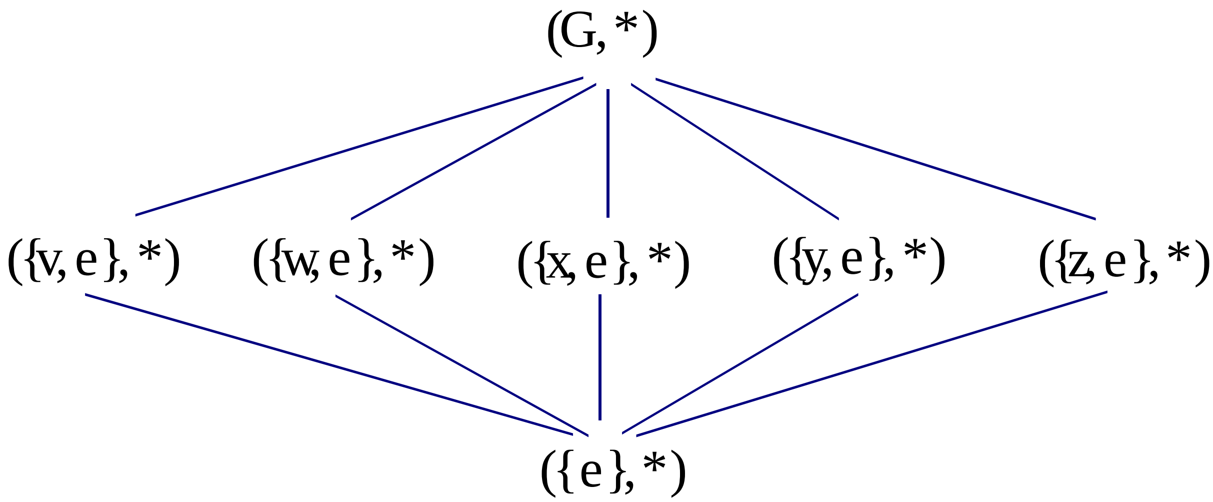
1. $(\{e\}, *), (\{e, v\}, *), (\{e, w\}, *), (\{e, x\}, *), (\{e, y\}, *), (\{e, z\}, *)$ are all subgroups of $(G, *)$.

2. There are no subgroups of order 3, since no element has order 3.

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

Hence $(\{e\}, *), (\{e, v\}, *), (\{e, w\}, *), (\{e, x\}, *), (\{e, y\}, *), (\{e, z\}, *)$, and $(G, *)$
are the subgroups of $(G, *)$.

Our subgroup diagram is below:



4. 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.

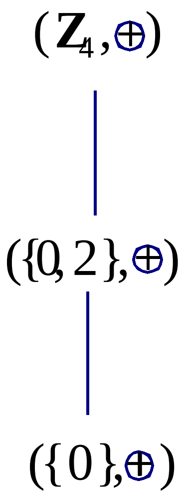
   Such a subgroup would consist of the identity and an element of order 2 (i.e., an element that is its own inverse.)

   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 $(\mathbb{Z}_4, \oplus)$.



5. Construct the group table for $(\mathbb{Z}_5, \oplus)$, and then find all of the subgroups of $(\mathbb{Z}_5, \oplus)$ and justify your answers. Draw a subgroup diagram for $(\mathbb{Z}_5, \oplus)$.

   Note that $(\mathbb{Z}_5, \oplus) = (\{0, 1, 2, 3, 4\}, \oplus)$, where $\oplus$ is addition modulo 5

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

   To start off, we acknowledge that $(\{0\}, \oplus)$ and $(\mathbb{Z}_5, \oplus)$ are subgroups of $(\mathbb{Z}_5, \oplus)$.

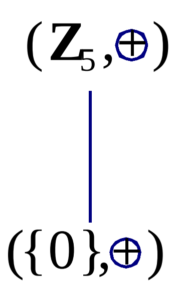
   If there are other subgroups $(H, \oplus)$, then $|H|$ must divide $|\mathbb{Z}_5|$.

   Since $|\mathbb{Z}_5| = 5$, this implies that $|H| = 1$ or 5.

   Thus, the only subgroups of $(\mathbb{Z}_5, \oplus)$ are $(\{0\}, \oplus)$ and $(\mathbb{Z}_5, \oplus)$.

   Thus, $(\mathbb{Z}_5, \oplus)$ are $(\{0\}, \oplus)$ are the only subgroups of $(\mathbb{Z}_5, \oplus)$.

   The subgroups of $(\mathbb{Z}_5, \oplus)$ are $(\{0\}, \oplus)$ and $(\mathbb{Z}_5, \oplus)$.



6. 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 $\odot$ is multiplication modulo 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

To start off, we acknowledge that $(\{1\}, \odot)$ and are subgroups of $(U_7, \odot)$.

If there are other subgroups $(H, \odot)$, then $|H|$ must divide $|U_7|$.

Since $|U_7| = 6$, this implies that $|H| = 1, 2$, or 3.

So we are looking for subgroups of order 2 or 3.

Subgroups of order 2 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 6 is the only element, other than the identity, that fits this description.

Thus, $(\{1,6\}, \odot)$ is the only subgroup of order 2.

To find subgroups of order 3, we look for elements $x \in U_7$ having the property that $x^3 = 1$.

Observe: $2^3 = 8 \equiv 1 \pmod 7$

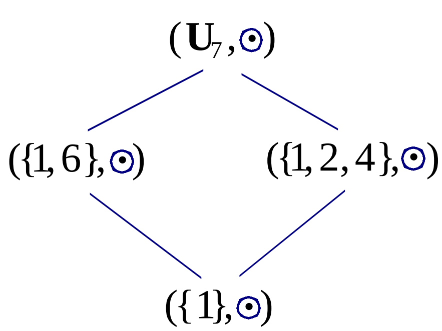
Also: $4^3 = 64 \equiv 1 \pmod 7$

Note that both 2 and 4 generate the same subgroup of order 3.

$\langle 2 \rangle = \langle 4 \rangle = (\{1,2,4\},) \odot$

This exhausts all possibilities.

The subgroups of $(U_7, \odot)$ are $(\{1\}, \odot), (\{1,6\}, \odot), (\{1,2,4\}, \odot)$, and $(U_7, \odot)$.



7. Given the group $(\mathbb{Z},+)$, list some of the subgroups of $(\mathbb{Z},+)$ and draw a subgroup diagram for the subgroups of $(\mathbb{Z},+)$.

Note that $\forall n\in\mathbb{N}$, n and $-n$ are generators of the subgroup $(n\mathbb{Z},+)$.

Note that $\langle n\rangle=(n\mathbb{Z},+)$ because:

i) $0\in n\mathbb{Z}$, $\forall n\in\mathbb{N}$ (0 is the identity)

ii) $-nz\in n\mathbb{Z}$, $\forall n\in\mathbb{N}$ ($-nz$ is the inverse of $nz\in n\mathbb{Z}$)

iii) $+$ is associative, as $+$ is associative for all real numbers.

iv) $+$ is closed, as $nz_1+nz_2=n(z_1+z_2)\in n\mathbb{Z}$

Here is a lattice diagram of some of the subgroups of $(\mathbb{Z},+)$