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 $|G|$.

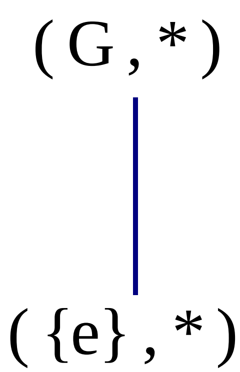
But $|G| = 5$

$\Rightarrow |H| = 1$ 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

Preferred Solution: 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)

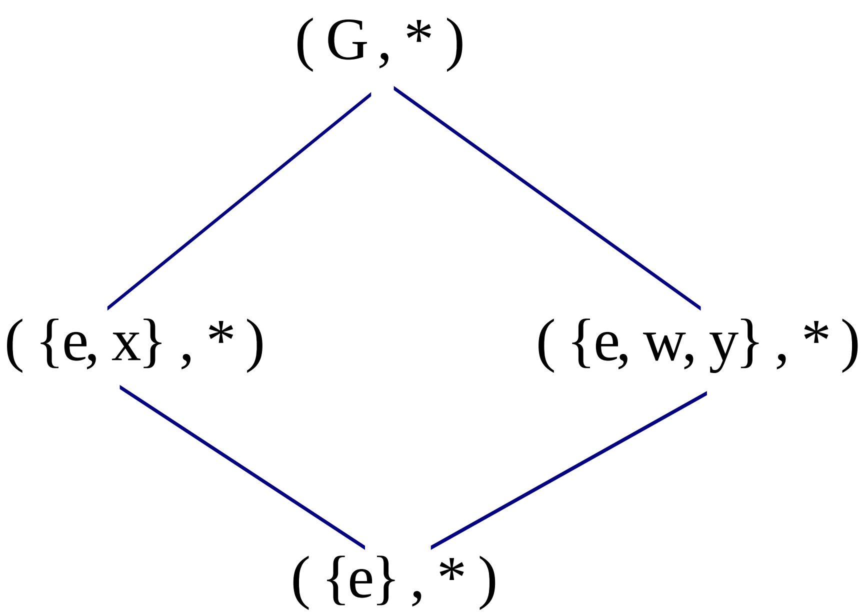
Observe: $z * z = y$, and $z * (z * z) = z * y = x$

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:



Alternative Solution: 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.

Let's see what happens when we take $(H,*)=(\{e\},*)$ and add a single element of G to H.

$v \in H$

If $(H,*)$ is a **subgroup** of $(G,*)$ and $v \in H$, then $(H,*)$ must also contain v^{-1}.

From the group table of $(G,*)$, $v^{-1}=z$.

Thus, $z \in H$.

Also, since $*$ must be closed on $(H,*)$, $v*v \in H$ and $v*(v*v) \in H$, etc.

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

i.e., if $v \in H$, then $(H,*)=(\{e,v,w,x,y,z\},*)=(G,*)$

$z \in H$

If $(H,*)$ is a **subgroup** of $(G,*)$ and $z \in H$, then $(H,*)=(G,*)$, for reasons similar to those given in the preceding case.

$w \in H$

If $(H,*)$ is a **subgroup** of $(G,*)$ and $w \in H$, then $(H,*)$ must also contain w^{-1}.

From the group table of $(G,*)$, $w^{-1}=y$.

Thus, $y \in H$.

Also, since $*$ must be closed on $(H,*)$, $w*w \in H$ and $w*(w*w) \in H$, etc.

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

Thus, $w,y \in (H,*)$.

A quick check shows that $*$ is closed on $\{e,w,y\}$, as $w*y=e$ and $y*w=e$ and $y*y=w$

Therefore, $(H,*)=(\{e,w,y\},*)$ is a subgroup of $(G,*)$ having order 3.

$y \in H$

Based on reasoning similar to the previous case, this yields the subgroup $(H, *) = (\{e, w, y\}, *)$ of order 3.

$x \in H$

If $(H, *)$ is a **subgroup** of $(G, *)$ and $x \in H$, then $(H, *)$ must also contain x^{-1}.

From the group table of $(G, *)$, $x^{-1} = x$.

Thus, $x \in H$.

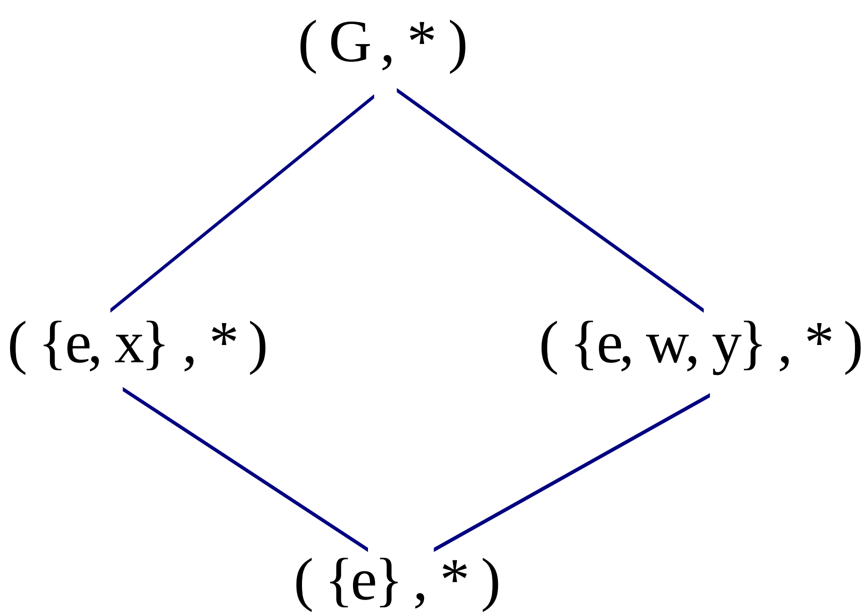
Also, since $x^{-1} = x$ $*$ is closed on $(H, *)$.

Therefore, $(H, *) = (\{e, x\}, *)$ is a subgroup of $(G, *)$ having order 2.

Thus, we have already accounted for all possible 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

Preferred Solution: 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:

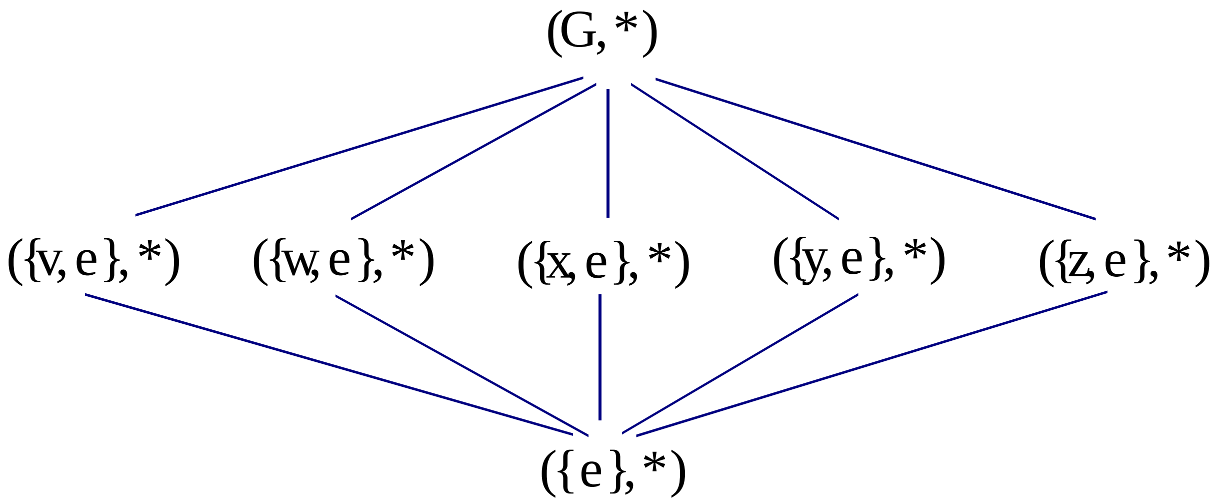
1. $(\{e\}, *), (\{e, v\}, *), (\{e, w\}, *), (\{e, x\}, *), (\{e, y\}, *), (\{e, z\}, *)$ are all subgroups of $(G, *)$.

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:



Alternative Solution #1: 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.

Let's see what happens when we take $(H, *) = (\{e\}, *)$ and add a single element of G to H.

Note that every element of $(G, *)$ is its own inverse.

Since each element in G is its own inverse:

(a) each of the prospective subgroups $(\{e, v\}, *)$; $(\{e, w\}, *)$; $(\{e, x\}, *)$; $(\{e, y\}, *)$; $(\{e, z\}, *)$ is such that each element has an inverse that is contained in the prospective subroup

(b) $*$ is closed on each of the prospective subgroups

Thus, $(\{e, v\}, *)$; $(\{e, w\}, *)$; $(\{e, x\}, *)$; $(\{e, y\}, *)$; $(\{e, z\}, *)$ are all subgroups (of order 2) of $(G, *)$.

Do we have any subgroups of order 3?

No. There cannot be any subgroups of order 3.

Here's how we arrive at this conclusion:

Observe that any subgroup of order 3 would have to be formed by taking one of the subgroups of order 2, $(\{e, v\}, *)$; $(\{e, w\}, *)$; $(\{e, x\}, *)$; $(\{e, y\}, *)$; $(\{e, z\}, *)$, and adding another element.

Thus, a subgroup $(H, *)$ of order 3 would have to contain one of the subgroups of order 2, $(\{e, v\}, *)$; $(\{e, w\}, *)$; $(\{e, x\}, *)$; $(\{e, y\}, *)$; $(\{e, z\}, *)$.

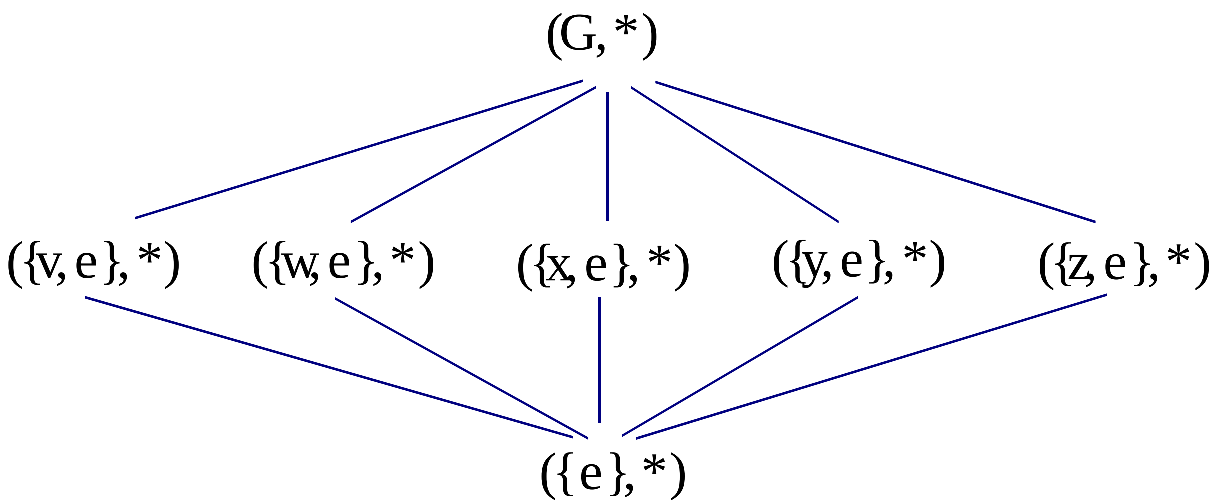
i.e., A subgroup $(H, *)$ of order 3 would, itself, have to have a subgroup of order 2.

But this can't happen, because 2 doesn't divide 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:



Alternate Solution #2: 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.

Let's see what happens when we take $(H,*)=(\{e\},*)$ and add a single element of G to H.

Note that every element of $(G,*)$ is its own inverse.

Since each element in G is its own inverse:

(a) each of the prospective subgroups $(\{e,v\},*)$; $(\{e,w\},*)$; $(\{e,x\},*)$; $(\{e,y\},*)$; $(\{e,z\},*)$ is such that each element has an inverse that is contained in the prospective subroup

(b) $*$ is closed on each of the prospective subgroups

Thus, $(\{e,v\},*)$; $(\{e,w\},*)$; $(\{e,x\},*)$; $(\{e,y\},*)$; $(\{e,z\},*)$ are all subgroups (of order 2) of $(G,*)$.

Do we have any subgroups of order 3?

If we do, then such a subgroup would have to contain the identity e, and one of the elements v, w, x, y, z.

Hence, a subgroup of order 3 would have to contain one of the subgroups $(\{e, v\}, *)$; $(\{e, w\}, *)$; $(\{e, x\}, *)$; $(\{e, y\}, *)$; $(\{e, z\}, *)$.

Any subgroup of order 3 would have to be formed by taking one of these subgroups and adding another element.

Let's see what happens if we do that.

Suppose that we add an element (we'll call it q) to the subgroup $(\{e, v\}, *)$.

In order for this to yield a subgroup of order 3, $\{e, v, q\}$ would have to be closed under $*$.

Thus, $q * v$ would have to be an element of $\{e, v, q\}$.

Hence, either $q * v = e$, or $q * v = v$, or $q * v = q$.

If $q * v = e$, then q is the inverse of v. But this can't happen, because v is it's own inverse.

If $q * v = v$, then q is the identity. But this can't happen, because e is the identity.

If $q * v = q$, then v is the identity. But this can't happen, because e is the identity.

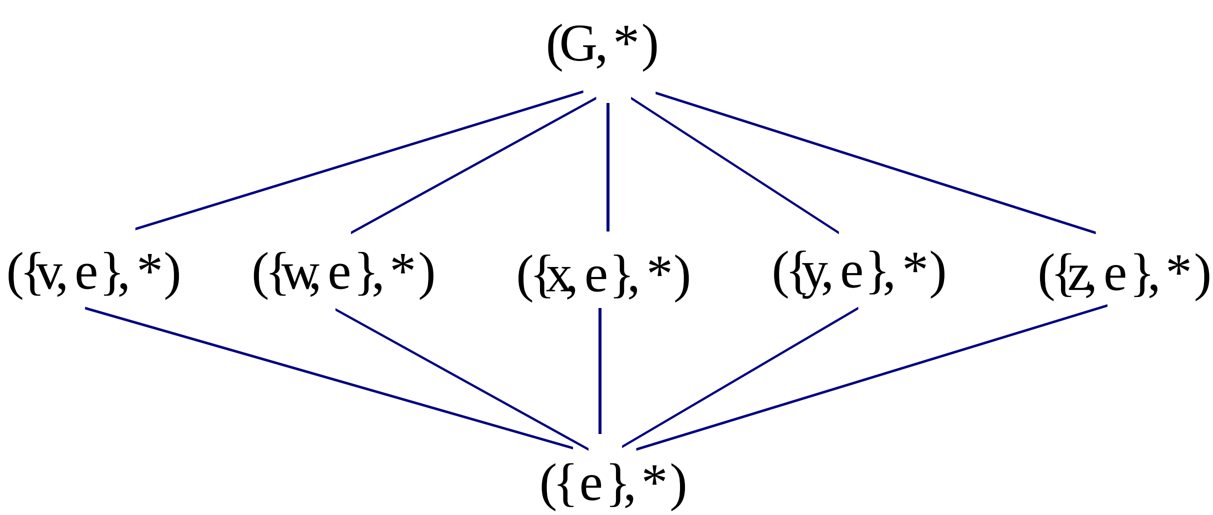
This means that we can't get a subgroup of order 3 by adding an element to the subgroup $(\{e, v\}, *)$.

The exact same line of reasoning tells us that we can't get a subgroup of order 3 by adding an element to **any** of the subgroups of order 2.

Thus, there are no subgroups of order 3.

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.

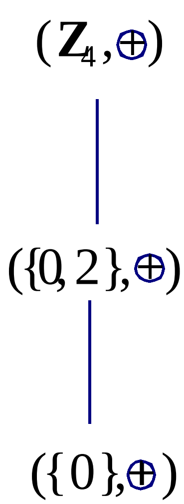
Such a subgroup would consist of the identity and an element of order 2 (i.e., an element that is its own inverse.)

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 $(\mathbb{Z}_5, \oplus)$.

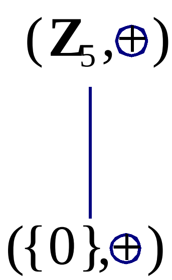
   If there are other subgroups $(H, \oplus)$, then $|H|$ must divide $|\mathbb{Z}_5|$.

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

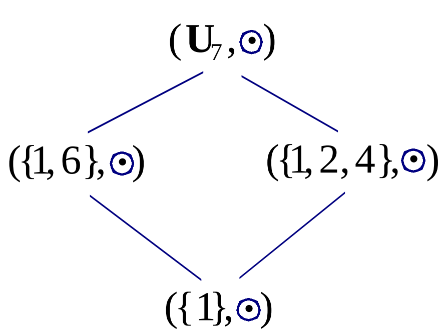
Also: $4^3 = 64 \equiv 1 \pmod 7$

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 $(\mathbb{Z},+)$