Section 6.4, Subgroups: Groups Inside a Group

1. **(True or False)**

a) The order of any subgroup always divides the order of the group.
Ans: true

b) Every subgroup of a group must contain the identity element of the group.
Ans: true

c) Some groups do not have any subgroups.
Ans: false, the identity alone is a subgroup

d) $\mathbb{Z}$ is a subgroup of $\mathbb{R}$ under the operation of addition.
Ans: true

e) The symmetric group S_2 has two subgroups.
Ans: true, the identity and the group itself are both subgroups of S_2

f) There are some groups where every subset is a subgroup.
Ans: false, the subsets must contain the identity element and some subsets fo not.

g) The set $\{e,h\}$ is a subgroup of the group of symmetries of a square, where e denotes the identity map, and h is the horizontal flip.
Ans: yes

h) There are 5 subgroups of order 2 of the group of symmetries of a square.
Ans: yes, and you should be able to envision them

2. **(Subgroups of $\mathbb{Z}_6$)** List all subgroups of $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ generated by the elements of the group. What is the order of each generator?
Ans:

$\langle 1\rangle = \mathbb{Z}_6$ order 6

$\langle 2\rangle = \{0,2,4\}$ order 3

$\langle 3\rangle = \{0,3\}$ order 2

$\langle 4\rangle = \{0,2,4\}$ order 3

$\langle 5\rangle = \mathbb{Z}_6$ order 6

3. Find the Cayley table for the subgroup $\{e, R_{180}, v, h\}$ of the group of symmetries of a square.

Ans:

$*$	e	R_{180}	v	h
e	e	R_{180}	v	h
R_{180}	R_{180}	e	h	v
v	v	h	e	R_{180}
h	h	v	R_{180}	e

4. Show that the group defined by the following Cayley table is a subgroup of S_3.

$*$	$(\ )$	(123)	(132)
$(\ )$	$(\ )$	(123)	(132)
(123)	(123)	(132)	$(\ )$
(132)	(132)	$(\ )$	(123)

Ans: By Theorem 1 all we need to do is verify that the subset $H = \{(\ ), (123), (132)\}$ is closed under the operation *, and that each member of H has an inverse. Clearly the operation * is closed since the table consists of these members. Also, (123) and (132) are inverses of each other, and of course the inverse of the identity $(\ )$ is itself.

5. **(Subgroup Geneated by** R_{240}**)** Find the subgroup of the dihedral group D_3 of symmetries of an equilateral triangle generated by R_{240}.
Ans: $\langle R_{240} \rangle = \{e, R_{120}, R_{240}\}$

6. **(Generated Groups of Symmetries of a Rectangle)** In the Klein 4-group $\{e, R_{180}, v, h\}$ of symmetries of a rectangle, find the subgroups generated by each element in the group. What is the order of each member?
Ans:

$\langle R_{180} \rangle = \{e, R_{180}\}$ $\quad R_{180}$ has order 2
$\langle v \rangle = \{e, v\}$ $\quad v$ has order 2
$\langle h \rangle = \{e, h\}$ $\quad h$ has order 2

7. **(Center of a Group)** The center $Z(G)$ of a group G consists of all elements of the group that commute with all elements of the group. That is

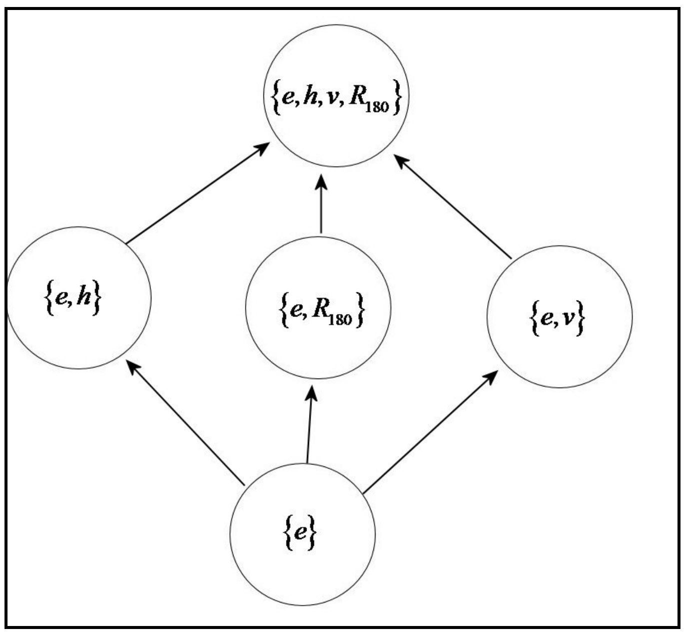
$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$$

It can be shown that the center of any group is a subgroup of the group. Find the center of the group of symmetries of a rectangle. Note: The center of a group is never empty since the identity element of a group always commutes with every element of the group. The question is, are there other elements that commute with every element of the group.

Ans: The center of the Klein 4-group is $\{e, R_{180}\}$

8.**(Hasse Diagram)** Draw a Hasse diagram for the subgroups of symmetries of a rectangle; i.e. the Klein 4-group.

Ans:



9. **(Subgroups of $\mathbb{Z}_8$)** Find the subgroups of the cyclic group $\mathbb{Z}_8$.
Ans: Systematically trying difference generators of $\mathbb{Z}_8$ we find

$$\langle 1\rangle = \{1,2,3,4,5,6,7,0\} = \mathbb{Z}_8$$
$$\langle 2\rangle = \{2,4,6,0\}$$
$$\langle 3\rangle = \{3,6,1,4,7,2,5\} = \mathbb{Z}_8$$
$$\langle 4\rangle = \{4,0\}$$
$$\langle 5\rangle = \{5,2,7,4,1,6,3,0\} = \mathbb{Z}_8$$
$$\langle 6\rangle = \{6,4,2,0\}$$
$$\langle 7\rangle = \{7,6,5,4,3,2,1,0\} = \mathbb{Z}_8$$

which gives us four subgroups $\{0\}$, $\{0,4\}$, $\{0,2,4,6\}$, and $\mathbb{Z}_8$.

10. **(Subgroups of $\mathbb{Z}_{11}$)** Find the subgroups of the cyclic group $\mathbb{Z}_{11}$.

Ans: Systematically trying difference generators of $\mathbb{Z}_{11}$ the only subgroups are the trivial group $\{0\}$ and $\mathbb{Z}_{11}$. Also, the order of the subgroup divides the order of the group and since $\mathbb{Z}_{11}$ has order 11 and the only two numbers that divide 11 are 1 and 11.

11. **Cryptographics** Using the subgroup

$$\langle 3\rangle = \{3,6,9,12,15\}$$

of the cyclic group Z_{16} where the group operation is addition, modulo 16, suppose Alice has the secret number 9, and Bob has a secret number of 15.

a) What is the secret number they share?

b) What if they both had the same secret number of 9. What secret number would they share then?

ΟΠΧΝΞΩΨ