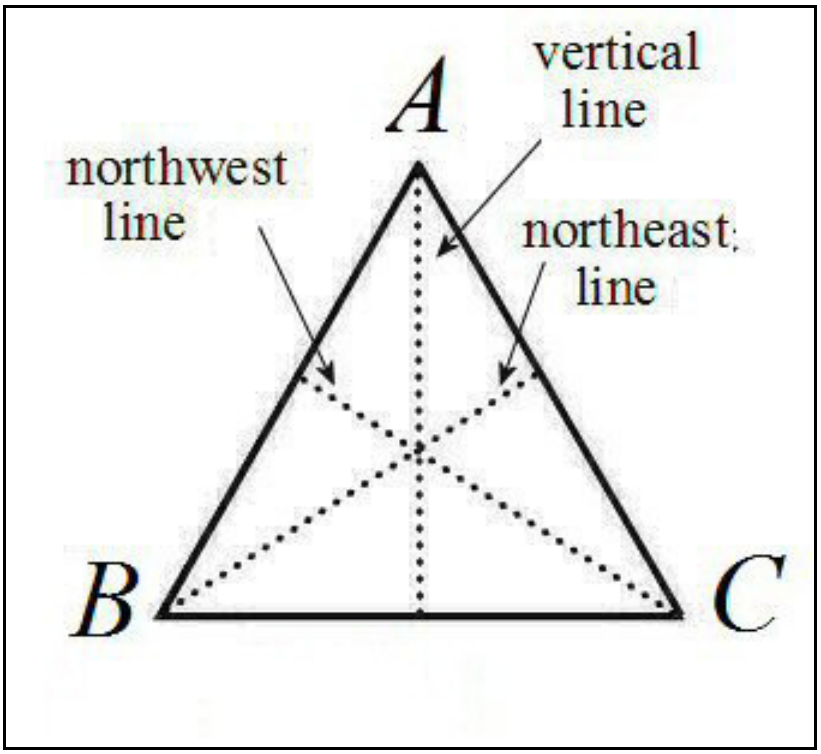
Section 6.4 Subgroups: Groups Inside a Group

Purpose of Section To introduce the concept of a **subgroup** and find the subgroups of various symmetry groups.

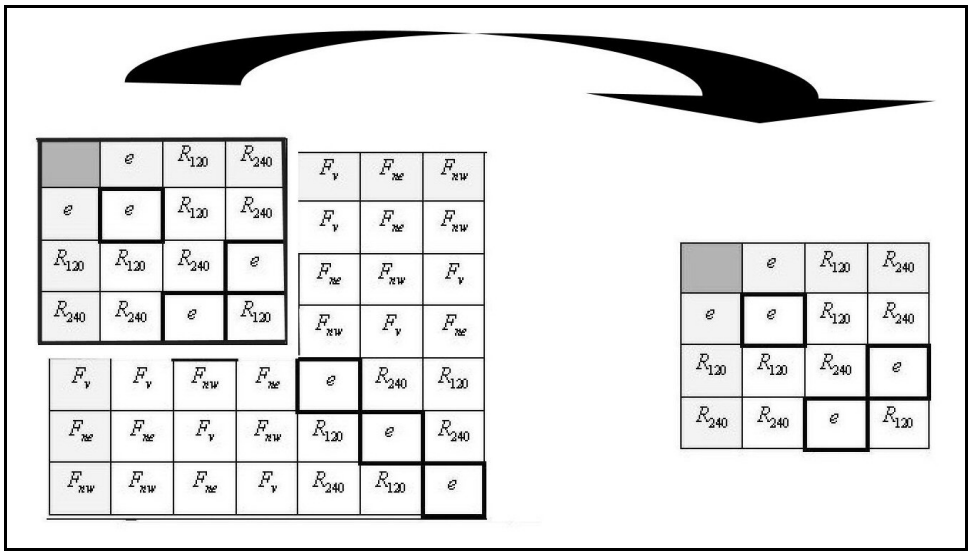
Introduction

Recall the six symmetries of an equilateral triangle; the identity map, three flips about the midlines through the vertices of the triangle, and two (counterclockwise) rotations of 120^0 and 240^0.



Symmetries of an equilateral triangle
Figure 1

These symmetries along with the group operation of composition of permutations forms an algebraic system called a group. But this group is only the outside of the shell. On the inside there may be smaller groups. For the dihedral group D_3 of six symmetries of an equilateral triangle, the subset of the three rotational symmetries is a group itself. The multiplication table for these symmetries $\{e, R_{120}, R_{240}\}$ is drawn in Figure 2, which can easily be verified to form a group.



Subgroup of rotations of symmetries of an equilateral triangle
Figure 2

This motivates the following definition of "groups within groups," or subgroups.

Definition: Let $\{G,*\}$ be a group with operation $*$. If a subset $H \subseteq G$ itself forms a group with the same operation $*$, then H is called a **subgroup** of G.

At Least Two Subgroups: All groups have two subgroups, the group itself and the trivial group consisting of only the identity $\{e\}$. We are mainly interested in the other subgroups, sometimes called the **proper subgroups**, although we will refer to them simply as subgroups.

Example 1 Subgroups of Symmetries Find the subgroups of the dihedral group D_3 of the symmetries of an equilateral triangle.

Solution: The Cayley table for the dihedral group D_3 of symmetries of an equilateral triangle and its subgroups are displayed below. There are four subgroups[1] of D_3; the rotational subgroup $\{e, R_{120}, R_{240}\}$ of order 3 and three "flip" subgroups $\{e, F_v\}, \{e, F_{ne}\}, \{e, F_{nw}\}$, each of order 2.

[1] Of course, $(G,*)$ is a subgroup of *itself*, but when we say subgroups we mean *proper* subgroups when $H \neq G$.

$*$	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
e	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
R_{120}	R_{120}	R_{240}	e	F_{ne}	F_{nw}	F_v
R_{240}	R_{240}	e	R_{120}	F_{nw}	F_v	F_{ne}
F_v	F_v	F_{nw}	F_{ne}	e	R_{240}	R_{120}
F_{ne}	F_{ne}	F_v	F_{nw}	R_{120}	e	R_{240}
F_{nw}	F_{nw}	F_{ne}	F_v	R_{240}	R_{120}	e

$H_1 = \{e, F_v\}$ flip around vertical axis

$*$	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
e	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
R_{120}	R_{120}	R_{240}	e	F_{ne}	F_{nw}	F_v
R_{240}	R_{240}	e	R_{120}	F_{nw}	F_v	F_{ne}
F_v	F_v	F_{nw}	F_{ne}	e	R_{240}	R_{120}
F_{ne}	F_{ne}	F_v	F_{nw}	R_{120}	e	R_{240}
F_{nw}	F_{nw}	F_{ne}	F_v	R_{240}	R_{120}	e

$H_2 = \{e, F_{nw}\}$ flip around the northwest axis

$*$	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
e	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
R_{120}	R_{120}	R_{240}	e	F_{ne}	F_{nw}	F_v
R_{240}	R_{240}	e	R_{120}	F_{nw}	F_v	F_{ne}
F_v	F_v	F_{nw}	F_{ne}	e	R_{240}	R_{120}
F_{ne}	F_{ne}	F_v	F_{nw}	R_{120}	e	R_{240}
F_{nw}	F_{nw}	F_{ne}	F_v	R_{240}	R_{120}	e

$H_3 = \{e, F_{ne}\}$ flip around the northeast axis.

$*$	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
e	e	R_{120}	R_{240}	F_v	F_{ne}	F_{nw}
R_{120}	R_{120}	R_{240}	e	F_{ne}	F_{nw}	F_v
R_{240}	R_{240}	e	R_{120}	F_{nw}	F_v	F_{ne}
F_v	F_v	F_{nw}	F_{ne}	e	R_{240}	R_{120}
F_{ne}	F_{ne}	F_v	F_{nw}	R_{120}	e	R_{240}
F_{nw}	F_{nw}	F_{ne}	F_v	R_{240}	R_{120}	e

Three rotations of a rectangle

We let the reader verify that each of these subgroups satisfy the required conditions to be a group. See Problem 1.

Subgroups of the Klein 4-Group

Recall that the group of symmetries of a rectangle form the Klein 4-group with elements

$$G = \{e, R_{180}, H, V\}$$

Figure 3 shows the Cayley table of these symmetries and three subgroups of order 2.

$*$	e	R_{180}	H	V
e	e	R_{180}	H	V
R_{180}	R_{180}	e	V	H
H	H	V	e	R_{180}
V	V	H	R_{180}	e

Group of symmetries of a rectangle.

$*$	e	R_{180}	H	V
e	e	R_{180}	H	V
R_{180}	R_{180}	e	V	H
H	H	V	e	R_{180}
V	V	H	R_{180}	e

Subgroup of horizontal flips

$*$	e	R_{180}	H	V
e	e	R_{180}	H	V
R_{180}	R_{180}	e	V	H
H	H	V	e	R_{180}
V	V	H	R_{180}	e

Subgroup of vertical flips

$*$	e	R_{180}	H	V
e	e	R_{180}	H	V
R_{180}	R_{180}	e	V	H
H	H	V	e	R_{180}
V	V	H	R_{180}	e

Subgroup of rotational symmetries

Symmetry group of a rectangle and three subgroups
Figure 3

Note that the order of a subgroup divides the order of the group. This fundamental property of subgroups is called Lagrange's Theorem after the French/Italian mathematician Joseph-Louis Lagrange (1736-1813).

Test of Subgroups

Although a subset H of a group G is a group only if it satisfies the requirements for a group, it is only necessary to verify that the group operation $*$ is closed in H and that every element of H has an inverse in H. There is no need to show the existence of an identity since the identity in G is also an identity in H. This result is summarized in the following theorem.

Theorem 1: Conditions for Being a Subgroup If $\{G,*\}$ is a group and H a (nonempty) subset of G, then H with operation $*$ is a **subgroup** of $\{G,*\}$, provided the following two conditions hold:

i) The operation $*$ is closed in H. That is,

$$\forall x, y \in H \Rightarrow x * y \in H$$

ii) Every element in H has an **inverse** $h^{-1} \in H$ such that $h * h^{-1} = e \in G$. That is,

$$(\forall h \in H)(\exists h^{-1} \in H)(h * h^{-1} = h^{-1} * h = e).$$

where "e" is the identity element in G.

Proof: We verify the conditions for $(H,*)$ to be a group.

Closure in *H*: This is assumed.

Identity in *H*: If $h \in H$, then by condition ii) there exists a $h^{-1} \in H$. But the closure assumption *i*) tells us that $e = h * h^{-1} \in H$.

Inverse in *H* This is assumed.

Associative condition: The associative law

$$(a * b) * c = a * (b * c)$$

holds for all $a,b,c \in H \subseteq G$ and we know it holds for all elements of G. ▌

Example 2 Test of Subgroup Let $G = \mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$ be the group of integers with addition $+$ as the group operation. Show that the set of even integers $2\mathbb{Z} = \{0, \pm 2, \pm 4, ...\}$ is a subgroup of G.

Solution We verify the two conditions for a subset of a group to be a subgroup.

Closure of Addition: If $m = 2k_1$ and $n = 2k_2$ are even integers, so is their sum, as can be seen from the equation

$$m + n = 2(k_1 + k_2) \in 2\mathbb{Z}.$$

Inverse in Subset: Every even integer $2k \in 2\mathbb{Z}$ has an inverse, namely $-2k \in 2\mathbb{Z}$, as can be seen from ∎

Example 3: Group of Infinite Order The points (a,b) in the Cartesian plane with group operation

$$(a,b) \oplus (c,d) = (a+c, b+d)$$

form a group. Show that the x-axis $H = \{(x,0) : x \in \mathbb{R}\}$ is a subgroup.

Solution We verify the two conditions which ensures a subset of a group to be a subgroup.

Closure: The x-axis is a subset of the plane and the operation $\oplus$ is closed in H since

$$\left.\begin{matrix}(x_1,0) \in H \\ (x_2,0) \in H\end{matrix}\right\} \Rightarrow (x_1,0) \oplus (x_2,0) = (x_1 + x_2, 0) \in H$$

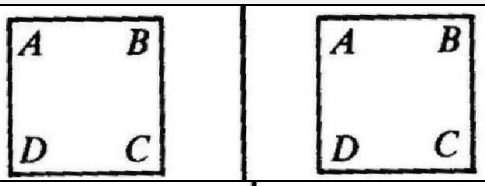
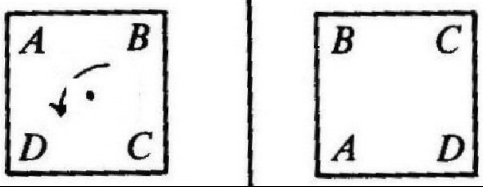
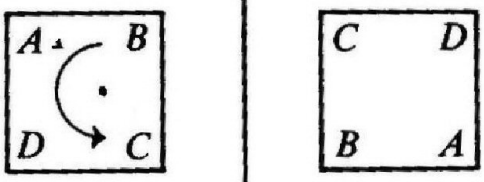
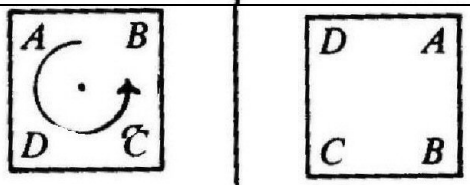
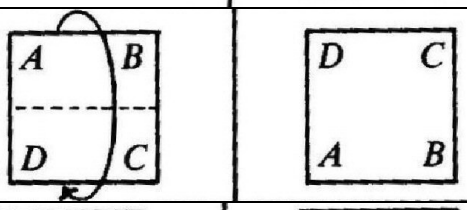
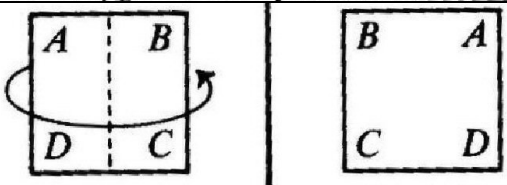
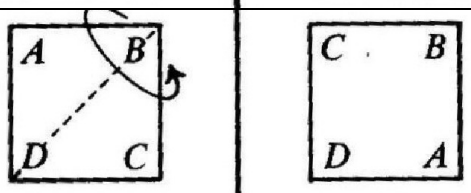
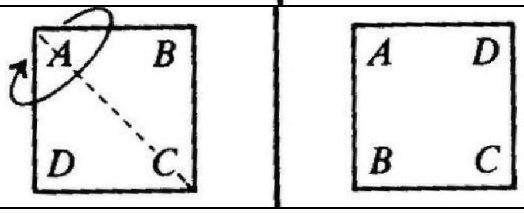
Identity: The identity of the Cartesian plane $(0,0) \in \mathbb{R}^2$ also belongs on the x-axis. ∎

Example 4 Subgroups of the Octic Group Figure 4 shows the individual symmetries of the dihedral group

$$D_4 = \{e, R_{90}, R_{180}\, R_{270}, F_V, F_H, F_{nw}, F_{ne}\}$$

which represent the eight symmetries of a square. This group is also called the **octic** group.

a) Does the group commute? Hint: Compare $R_{270}F_{ne}$ and $F_{ne}R_{270}$.
b) There are 9 subgroups of the octic group. Find them.

Motion	Symbol	First and Final Positions
No motion or Rotate 0^0	$e = R_0$	
Rotate 90° counterclockwise	R_{90}	
Rotate 180° counterclockwise	R_{180}	
Rotate 270° counterclockwise	R_{270}	
Horizontal flip	H	
Vertical flip	V	
Northeast flip	F_{ne}	
Northwest flip	F_{nw}	

Eight symmetries of a square
Figure 4

Solution

a) The reader can check that

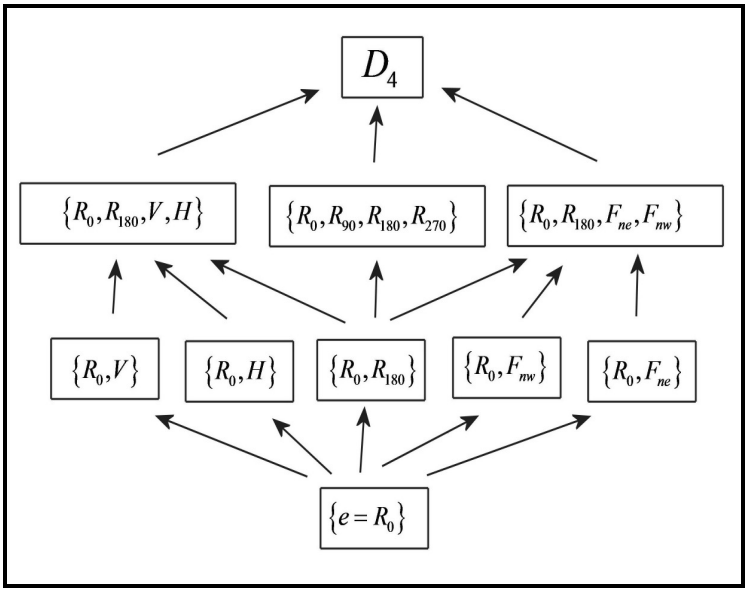
$$R_{270}F_{ne} \neq F_{ne}R_{270}.$$

Hence, the octic group is not commutative.

b) The 9 (proper) subgroups of the octic group D_4 are[2]

$$\{e\},\{e,V\},\{e,H\},\{e,F_{nw}\},\{e,F_{ne}\},\{e,R_{180}\},$$
$$\{e,R_{180},V,H\},\{e,R_{180},F_{nw},F_{ne}\}$$

The symmetry subgroups of a square form a partially ordered set, ordered by set inclusion, illustrated in Figure 5. The dihedral group D_4 is itself a subgroup of the group S_4 of 24 permutations of four elements.



Hasse diagram for the subgroups of the octic group D_4

Figure 5

Subgroups of Cyclic Groups

We have seen that the cyclic group Z_n is generated by an element in the group. That is, there exists a $g \in Z_n$ such that

$$\langle g \rangle \equiv \{e, g, g^2, g^3, ..., g^{n-1}\} = Z_n$$

To find the subgroups of Z_n we start with an arbitrary element $h \in Z_n$ and compute the set $\langle h \rangle$ generated by h. This set of elements generated by h may

[2] The octic group, which is a subgroup of itself, is not included here.

or may not be all of Z_n, but it *will* be a subgroup of Z_n. We then pick a new member $h' \in Z_n$ that is not in the first generated set $\langle h \rangle$ and compute $\langle h' \rangle$. This will yield another subset of Z_n. Continuing this process will eventually yield all subgroups of Z_n.

Let's apply this technique to find all the subsets of the cyclic group

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$$

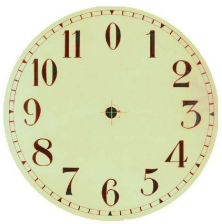
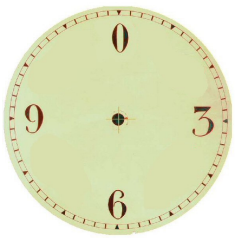
where the group operation is addition modulo 12. Starting with 1, we generate powers of $g = 1$, remembering that powers of one in this group are really adding 1. Hence, we have

$$\langle 1 \rangle = \{1,2,3,4,5,6,7,8,9,10,11,0\} \subseteq Z_{12}$$

which has generated the entire group $\mathbb{Z}_{12}$. We now select the element $g = 2$ which generates the subgroup

$$\langle 2 \rangle = \{0,2,4,6,8\} \subseteq Z_{12}.$$

Figure 6 shows the subgroups generated by $g = 1,2,3,4$. Do you see why $\langle 5 \rangle = \mathbb{Z}_{12}$ and $\langle 6 \rangle = \{0,6\}$.

	
$g = 1$ generates the entire group $\langle 1 \rangle = \mathbb{Z}_{12} = \{0,1,2,...,11\}$	$g = 2$ generates the subgroup $\langle 2 \rangle = \{0,2,4,6,8,10\}$
	
$g = 3$ generates the subgroup $\langle 3 \rangle = \{0,3,6,9\}$	$g = 4$ generates the subgroup $\langle 4 \rangle = \{0,4,8\}$

Four typical subgroups generated by elements of the group
Figure 6

Table 2 shows the subgroups generated by each element of the group and the order of the subgroup generated by the generator.

Generator	Order of the Generator
$\langle 1 \rangle = \mathbb{Z}_{12}$	$12 \ (1^{12} = 0)$
$\langle 2 \rangle = \{0,2,4,6,8,10\}$	$6 (2^6 = 0)$
$\langle 3 \rangle = \{0,3,6,9\}$	$4 (3^4 = 0)$
$\langle 4 \rangle = \{0,4,8\}$	$3 (4^3 = 0)$
$\langle 5 \rangle = \mathbb{Z}_{12}$	$12 (5^{12} = 0)$
$\langle 6 \rangle = \{0,6\}$	$2 (6^2 = 0)$
$\langle 7 \rangle = \mathbb{Z}_{12}$	$12 (7^{12} = 0)$
$\langle 8 \rangle = \{0,4,8\}$	$3 (8^3 = 0)$
$\langle 9 \rangle = \{0,3,6,9\}$	$4 (9^4 = 0)$
$\langle 10 \rangle = \{0,2,4,6,8,10\}$	$6 (10^6 = 0)$
$\langle 11 \rangle = \mathbb{Z}_{12}$	$12 (11^{12} = 0)$

Generators of subsets of $\mathbb{Z}_{12}$

Table 2

Cryptographics[3]

Cyclic groups play an important role in cryptographics using the Diffie-Hellman key-exchange protocol. Suppose Alice and Bob want to exchange a secret number. They agree on a (large) cyclic group generated by a number g known to the general public. Alice has a secret number a known only to herself, and Bob has his own secret number b .Alice computes g^a and sends this number to Bob, and Bob computes g^b and sends this number to Alice. Then

- Bob then computes $\left(g^a\right)^b = g^{ab}$
- Alice then computes $\left(g^b\right)^a = g^{ab}$

after which they share the secret number g^{ab} .

For example, suppose the cyclic group chosen is the subgroup of Z_8 generated by $g = 2$, or

$$\langle 2 \rangle \equiv \{0,2,4,6,8\}$$

[3] The following storyline is based on a lecture given by Carl Pomearance of Dartmouth College.

Suppose Alice's secret number is $a = 4$ and Bob's number is 2. Then

- Alice sends Bob $g^a = 2^4 = (2+2+2+2) \bmod 8 = 0$
- Bob sends Alice $g^b = 2^2 = (2+2) \bmod 8 = 4$

After receiving these numbers, each person then computes

- Alice computes $\left(g^b\right)^a = 4^4 = (4+4+4+4) \bmod 8 = 0$
- Bob computes $\left(g^a\right)^b = 0^2 = (0+0) \bmod 8 = 0$

after which they share the secret number 0. An eavesdropper listening to messages being transmitted might know g^a and g^b but cannot determine g^{ab} unless they know a or b.

Problems

1. **True or False**

a) The order of any subgroup divides the order of the group.
b) Every subgroup of a group contains an identity element.
c) Some groups do not have any subgroups.
d) $\mathbb{Z}$ is a subgroup of $\mathbb{R}$ under the operation of addition.
e) The symmetric group S_2 has two subgroups.
f) There are some groups where every subset is a subgroup.
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.
h) There are 5 subgroups of order 2 of the group of symmetries of a square.

2. **Subgroups of** $\mathbb{Z}_6$ List the subgroups of $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ generated by the different elements of the group. What is the order of each of these generated groups?

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

4. **Cayley Table** 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)

5. **Subgroup Generated by Rotations** Find the subgroup of the dihedral group D_3 of symmetries of an equilateral triangle generated by the rotation 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 repeated operations of each element in the group. What is the order of each member?

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.

8. **Hasse Diagram** Draw the Hasse diagram for the subgroups of symmetries of a rectangle.

9. **Subgroups of** $\mathbb{Z}_8$ Find the subgroups of $\mathbb{Z}_8$.

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

11. **Secret Number** 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?

ΓΣΘΨΞΠΩ