

Unit 3: Symmetry
Math 330B Spring 2006 (Barsamian)

1. Introduction to Symmetry	3
1.1. <i>Function terminology for fixing a set of points.....</i>	3
1.2. <i>Describing Symmetry using Terminology of Isometries</i>	5
1.3. <i>The Set of Symmetries of a Set of Points.....</i>	6
1.4. <i>Exercises.....</i>	8
2. Introduction to Groups.....	8
2.1. <i>Binary operations</i>	8
2.2. <i>Definition of a group</i>	12
2.3. <i>Exercises.....</i>	14
3. Symmetry Groups	15
3.1. <i>The Set of Symmetries a Set of Points is a Group.....</i>	15
3.2. <i>Examples of Symmetry Groups.....</i>	17
3.3. <i>Exercises.....</i>	18
4. Exploring Groups.....	19
4.1. <i>General properties.....</i>	19
4.2. <i>Order of group elements.....</i>	21
4.3. <i>Cyclic Groups.....</i>	23
4.4. <i>Subgroups.....</i>	24
4.5. <i>The lattice of subgroups of a group.....</i>	25
4.6. <i>Exercises.....</i>	26
5. Dihedral Groups.....	27
5.1. <i>Definition & Properties.....</i>	27
5.2. <i>Completely worked example: The Dihedral group with 6 elements.....</i>	28
5.3. <i>The subgroup generated by a subset.....</i>	31
5.4. <i>Exercises.....</i>	32

1. Introduction to Symmetry

Most of us probably first encountered the word *symmetric* sometime in grade school or junior high. At the time, it may have been used as a name for objects or pictures that look as if one side is a reversed copy of the other—a sort of mirror image. This kind of symmetry is sometimes called *bilateral symmetry*. Later, we learned that there are other kinds of symmetry, as well. For instance, the patterns on wallpaper are periodic in both the horizontal and vertical direction. This is called *translational symmetry*. Some objects or pictures have radial symmetry, meaning that the pattern is the same along any ray from the origin. Some have rotational symmetry, meaning that the pattern may not be identical along different rays from the origin, but the pattern does “repeat” in the sense that there is some angle of rotation about the origin that will cause the rotated pattern to lie on top of the original.

It is easy to see symmetry in pictures and objects. It is harder to describe symmetry in purely abstract mathematical terms, without reference to pictures. But such a description is worth the effort. It turns out that many powerful abstract mathematical concepts can be applied to an analysis of symmetry. These concepts give us a deeper understanding of symmetry and also a richer, more precise vocabulary for describing it. And conversely, by developing an abstract mathematical notion of symmetry, without reference to pictures, we become poised to find symmetry in abstract settings where there is no picture.

This unit will consider symmetry of sets in the Cartesian plane \mathbb{R}^2 from an abstract mathematical viewpoint. The discussion in Chapter 1 begins by defining symmetry in terms of isometries of the plane. Once the basic definitions and terminology has been established, we will see in later chapters that the concepts of abstract algebra can be used to analyze and describe symmetry.

1.1. Function terminology for fixing a set of points

In Unit 2, you were introduced to some basic terminology pertaining to maps of the Cartesian plane, including the idea of a *point* being *fixed* by a map of the plane. The goal of this first section of Unit 3 Chapter 1 is to introduce the notion of a *set of points* in the plane being fixed by a map. For our discussion, more terminology is useful, so we start with some definitions.

Definition 1 image of a point

- words: Q is the image of P under the mapping f .
- usage: $P \in \mathbb{R}^2$ is a point and $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a mapping.
- meaning in symbols: $f(P) = Q$
- meaning in words: when P is used as input to the mapping f , point Q is the resulting output.
- observation: The image of a point is a point.

Definition 2 preimage of a point

- words: the preimage of Q under the mapping f .
- symbol: $f^{-1}(Q)$
- usage: $Q \in \mathbb{R}^2$ is a point and $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a mapping.
- meaning in symbols: $f^{-1}(Q) = \{P \in \mathbb{R}^2 \text{ such that } f(P) = Q\}$
- meaning in words: The preimage of point Q under the mapping f is the set whose elements are all points P that have the property that the image of P is Q .
- observation: The preimage of a point is a set of points.

Example: Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be the map defined by $f(x, y) = (x^2, y)$.

Then $f^{-1}(4, 5) = \{(2, 5), (-2, 5)\}$, and $f^{-1}(0, 0) = \{(0, 0)\}$, and $f^{-1}(-4, 5) = \emptyset = \{ \}$, the empty set.

Note that $f^{-1}(4, 5)$ is a set containing two points because the mapping f is not one-to-one. Similarly, $f^{-1}(-4, 5)$ is the empty set because the mapping f is not onto. Clearly, if we decided to only deal with mappings that were bijections, this weird behavior would never happen: the preimage of a point would always be a set containing one point. So if we were dealing only with mappings that were bijections, we could simplify our definition of preimage:

Definition 3 preimage of a point when all maps are bijections

- words: P is the preimage of Q under the bijective mapping f .
- symbol: $P = f^{-1}(Q)$
- usage: $Q \in \mathbb{R}^2$ is a point and $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a bijective mapping.
- meaning in symbols: $f(P) = Q$
- meaning in words: The image of P is Q .
- observation: The preimage of a point is a point.

In this unit, we will be dealing exclusively with bijective mappings of the plane. So we adopt a common terminology, expressed in the following definition:

Definition 4 transformation of the plane

- words: f is a transformation of the plane
- meaning: $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a bijective mapping from the plane to itself.

Recall the following definition that was introduced in Unit 2:

Definition 5 fixed point

- Words: “ P is a fixed point of f ”, or “ f fixes P ”
- Usage: f is a map of the plane and P is a point of the plane
- Meaning: $f(P) = P$
- Meaning in words: To say that P is a fixed point of f means that when the point P is used as input to the function f , the resulting output is also point P .
- Special case: to say “ f fixes the origin ” means that $f(0, 0) = (0, 0)$.

Definition 6 image of a set of points

- symbol: $f(A)$
- words: the image of set A under the mapping f .
- usage: $A \subset \mathbb{R}^2$ is a set of points and $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a mapping.
- meaning in symbols: $f(A) = \{f(a) \text{ such that } a \in A\}$
- meaning in words: the image of a set A is the set of outputs that result when all of the elements of set A are (individually) used as inputs to the map f .

- observation: The image of a set of points is a set of points.

Definition 7 preimage of a set of points

- words: the preimage of set B under the mapping f .
- symbol: $f^{-1}(B)$
- usage: $B \subset \mathbb{R}^2$ is a set of points and $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a mapping.
- meaning in symbols: $f^{-1}(B) = \{P \in \mathbb{R}^2 \text{ such that } f(P) \in B\}$
- meaning in words: The preimage of point Q under the mapping f is the set whose elements are all points P that have the property that the image of P is an element of B .
- observation: The preimage of a set of points is a set of points.

Definition 8 a set of points fixed by a map of the plane

- Words: “ f fixes set A ”
- Usage: f is a map of the plane and $A \subset \mathbb{R}^2$ is a set of points.
- Meaning: $f(A) = A$.

Remark: to say that a set is fixed by a map does not mean that every point in the set is fixed by the map. Indeed, it is often the case that a set is fixed by a map even though not a single point in the set is fixed by the map. For example, let the set A be the unit circle centered at the origin, and consider the rotation $R_{(0,0),45^\circ}$. This map fixes the unit circle, but every point on the circle gets moved; not a single point of the circle is fixed.

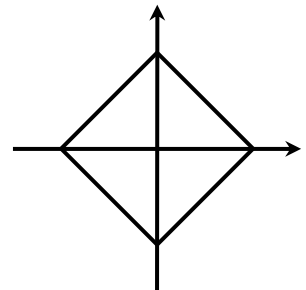
1.2. Describing Symmetry using Terminology of Isometries

Now that we have articulated the idea of a set being fixed by a map, we are ready to use it in an abstract definition of symmetry.

Definition 9 a symmetry of a set

- Words: “ f is a symmetry of A ”
- Usage: $A \subset \mathbb{R}^2$ is a set of points.
- Meaning: $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a Euclidean isometry and f fixes A . That is, $f(A) = A$.

Example: Let set A be a square centered at the origin, as shown in the picture at right. Observe that $R_{(0,0),45^\circ}$ is not a symmetry of set A , but $R_{(0,0),90^\circ}$ is a symmetry. Also note that the reflection $M_{x\text{-axis}}$ across the x -axis is a symmetry, as is M_L , where L is the line through the origin that makes a 45° angle with the positive x -axis.



Example: Let A be the endless set $\dots \mathbf{E} \mathbf{E} \mathbf{E} \mathbf{E} \dots$ whose characters are one unit apart. Then the translation $T_{\langle 1,0 \rangle}$ one unit to the right is a symmetry of A . So is the translation $T_{\langle 5,0 \rangle}$ five units to the

right. But the translation $T_{\langle \frac{1}{2}, 0 \rangle}$ one half unit to the right is not a symmetry of A . In fact, if $0 < b < 1$, then the translation $T_{\langle b, 0 \rangle}$ is not a symmetry.

The last couple of sentences capture the essence of what we will call a “frieze”. We will use the following definition. (This is not a standard definition, but it will work for us.)

Definition 10 Frieze

A *frieze* is a set of points $A \subset \mathbb{R}^2$ with the property that there is a real number $a > 0$ such that the translation $T_{\langle a, 0 \rangle}$ is a symmetry of A and if $0 < b < a$, then the translation $T_{\langle b, 0 \rangle}$ is not a symmetry of A .

Example: The x -axis has translational symmetry, but it is not a frieze. To see why, consider trying to find some number $a > 0$ to satisfy the requirement stated in the definition. Clearly, $T_{\langle a, 0 \rangle}$ is a symmetry of A . But we can let $b = \frac{a}{2}$. Then $0 < b < a$ and the translation $T_{\langle b, 0 \rangle}$ is also a symmetry of A .

Remark: Some friezes have other symmetries besides the translation along the x -axis. For example, the reflection $M_{x\text{-axis}}$ across the x -axis is an isometry for the frieze $\cdot \cdot \cdot \mathbf{E} \mathbf{E} \mathbf{E} \mathbf{E} \cdot \cdot \cdot$, but that same reflection is not an isometry for the frieze $\cdot \cdot \cdot \mathbf{e} \mathbf{e} \mathbf{e} \mathbf{e} \cdot \cdot \cdot$.

1.3. The Set of Symmetries of a Set of Points

In this unit, we will study the set of symmetries for a given set of points. It turns out that regardless of the set of points in question, the resulting set of symmetries will have certain algebraic properties. The study of those algebraic properties will begin in the next chapter. For now, we will just consider some examples of sets of points and their corresponding sets of symmetries.

Before considering the examples, we need to introduce an important map of the plane that will play an important role in the rest of the unit.

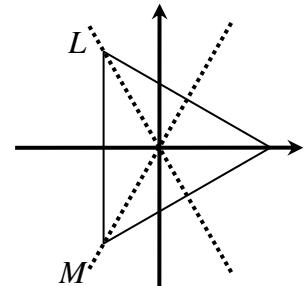
Definition 11 the identity map

- Words: “the identity map of set S ”, or “the identity of S ”
- symbol: id_S
- Usage: S is any set (not necessarily a set of points).
- Meaning: the function $id_S : S \rightarrow S$ defined by $id_S(x) = x$ for all $x \in S$.
- Special case: In this unit, we will be interested in “the identity map of the plane”, denoted by $id_{\mathbb{R}^2}$. It is the map that takes a point as input and spits out the same point as output. In symbols, we write $id_{\mathbb{R}^2}(x, y) = (x, y)$ for all points $(x, y) \in \mathbb{R}^2$. Often, we will omit the subscript \mathbb{R}^2 from the symbol $id_{\mathbb{R}^2}$, and instead denote this map simply as id .

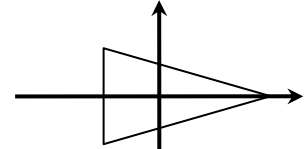
Observe that if the set S has a distance function d , then the map id_S will be an isometry for that distance function (regardless of the set S and regardless of the distance function d .) In particular, $id_{\mathbb{R}^2}$ will be a Euclidean isometry. Also note that given any set of points $A \subset \mathbb{R}^2$, the identity map $id_{\mathbb{R}^2}$ fixes A . That

is, $id_{\mathbb{R}^2}(A) = A$. These two observations tell us that given any set of points $A \subset \mathbb{R}^2$, the identity map $id_{\mathbb{R}^2}$ will be a symmetry of the set A .

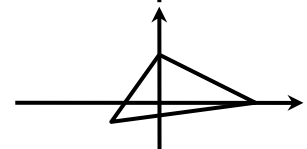
Example: Let set A be an equilateral triangle centered at the origin, as shown in the picture at right. The set A has six symmetries. They are $id_{\mathbb{R}^2}$, $R_{(0,0),120^\circ}$, $R_{(0,0),240^\circ}$, M_{x-axis} , M_L , and M_M , where L is the line through the origin that makes a 120° angle with the positive x -axis and M is the line through the origin that makes a 240° angle with the positive x -axis.



Example: Let set B be an isosceles triangle, as shown in the picture at right. The set B has only two symmetries. They are $id_{\mathbb{R}^2}$ and M_{x-axis} .



Example: Let set C be a scalene triangle, as shown in the picture at right. The set C has only one symmetry, the identity map $id_{\mathbb{R}^2}$.



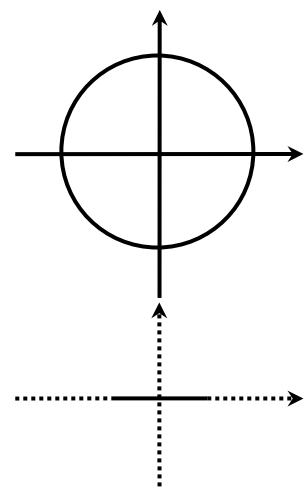
Example: Let set D be the frieze shown in the picture at right. The set of symmetries for this set is infinite, although the symmetries are all of two types: the translation $T_{\langle k,0 \rangle}$ where k is any integer, and the reflection M_{x-axis} across the axis. (Observe that the translation $T_{\langle 0,0 \rangle}$ corresponding to $k = 0$ is just the identity map, $id_{\mathbb{R}^2}$, in disguise.)



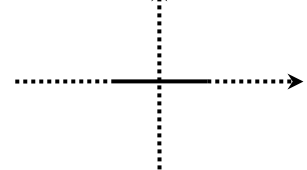
Example: Let set E be the frieze shown in the picture at right. The set of symmetries for this set is infinite, but the symmetries are all of one type: the translation $T_{\langle k,0 \rangle}$ where k is any integer. (Again note that the translation $T_{\langle 0,0 \rangle}$ is just the identity map, $id_{\mathbb{R}^2}$, in disguise.)



Example: Let set F be a circle centered at the origin, as shown in the picture at right. The set of symmetries for this set is infinite, but they can be classified as one of two types: The rotation $R_{(0,0),\varphi}$, where φ is any angle, and the reflection M_L , where L is any line through the origin. (Observe that the rotation $R_{(0,0),0}$ corresponding to the angle $\varphi = 0$ is just the identity map, $id_{\mathbb{R}^2}$, in disguise.)



Example: Let set G be the line segment $[-1,1]$ shown in the picture at right. The set G has four symmetries. They are $id_{\mathbb{R}^2}$, $R_{(0,0),180^\circ}$, M_{x-axis} , and M_{y-axis} .



Example G above brings up an interesting subtlety in the definition of a symmetry for a set. Observe that the reflection $M_{x\text{-axis}}$ does exactly the same thing to the line segment $[-1,1]$ that the identity map $id_{\mathbb{R}^2}$ does. That is, both maps do absolutely nothing to the line segment. Every point on the line segment is fixed by both operations. So aren't the two operations $M_{x\text{-axis}}$ and $id_{\mathbb{R}^2}$ the same? Why do we include both of them in the list of symmetries of set G ? The answer is that the two operations are not the same when considered as isometries of the plane. That is, even though they both fix the line segment $[-1,1]$, they do not both fix the point $P = (5,7)$, for example. Remember that a symmetry of set G is defined to be an isometry of the plane that fixes set G . Because the two operations $M_{x\text{-axis}}$ and $id_{\mathbb{R}^2}$ are distinct isometries of the plane, we list them as distinct symmetries of the set G . (Note also that $R_{(0,0),180^\circ}$ and $M_{y\text{-axis}}$ are distinct isometries of the plane but have identical effects on set G . They are both listed as symmetries of set G .)

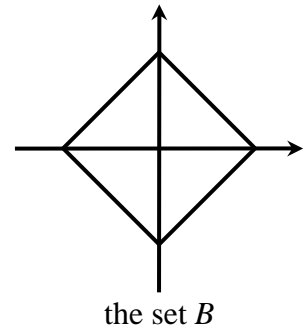
1.4. Exercises

[1] Let set A be the frieze $\dots \square \square \square \dots$. Describe the elements of the set of symmetries of A . Hint: the set is infinite, but the symmetries are all of three types.

[2] Example: Let set B be a square centered at the origin, as shown in the picture at right.

(a) Draw a picture of $R_{(0,0),45^\circ}(B)$. Is the set B fixed by the map $R_{(0,0),45^\circ}$?

(b) List the elements of the set of symmetries of B . Hint: the set has eight elements.



2. Introduction to Groups

In Chapter 1, a symmetry of a set of points in the plane was defined to be a mapping of the plane that had certain properties. By the end of the chapter (all six pages of it), the focus had turned to considering the set of symmetries for a given set of points. In Chapter 3, we will continue exploring the set of symmetries. We will see that the sets of symmetries have important algebraic properties. In this chapter, we will study the relevant algebraic concepts.

2.1. Binary operations

2.1.1. Definition of binary operation

We start the chapter by introducing the concept of a “binary operation on a set”, and then describing some properties that binary operations may or may not have.

Definition 12 Binary Operation on a Set

- Words: “ $*$ is a binary operation on S ”
- Usage: S is a set (not necessarily a set of points).
- Meaning in symbols: $* : S \times S \rightarrow S$
- Meaning in words: $*$ is a function that takes as input a pair of elements of S , and produces as output an element of S .

- Additional terminology: The fact that the output is always an element of the set S is sometimes referred to as the set S being “closed under the operation $*$ ”.

Example: Let A be the set of even integers and let $*$ be the operation of addition. Then $*$ is a binary operation for A , because when a and b are both even integers, $a + b$ is also an even integer. We could say that the set of even integers is closed under the operation of addition.

Example: Let B be the set of odd integers and let $*$ be the operation of addition. Then $*$ is not a binary operation for B , because when a and b are both odd integers, $a + b$ is not an odd integer. We could say that the set of odd integers is not closed under the operation of addition.

Example: Using the same sets A and B as above, let $*$ be the operation of multiplication. Then $*$ is a binary operation for A , and $*$ is a binary operation for B .

The two examples of binary operations that we have seen so far have both involved common mathematical operations. Operations will often be described by formulas involving mathematical operations. But remember that a binary operation is just a function, and there are many ways of describing functions. When the set S is a finite set, a binary operation can be described by simply giving a table showing every possible input pair (a, b) from the set $S \times S$, along with the resulting value of $a * b$. For example, the two tables shown below are both examples of binary operations on the set $S = \{a, b, c\}$. one of the operations is denoted by the symbol $*$; the other, by the symbol $\#$. The entries in the shaded column on the left of each table indicate the left element of the input pair; the entries in the shaded row along the top of each table indicate the right element of the input pair. The entries in the unshaded cells of the table indicate the corresponding output. For instance, $z * y = x$, and $y * z = x$, while $z \# y = z$, and $y \# z = y$.

		right input		
	*	x	y	z
left input	x	x	z	y
	y	z	y	x
	z	y	x	z

$z * y = x$ $y * z = x$

		right input		
	#	x	y	z
left input	x	x	y	z
	y	z	x	y
	z	y	z	x

$z \# y = z$ $y \# z = y$

2.1.2. Associative binary operations

We will now discuss four properties that a binary operation may or may not have. The first of these is the associative property.

Definition 13 associative binary operation

- Words: “the operation $*$ on S is associative”
- Usage: S is a set (not necessarily a set of points) and $*$ is a binary operation on S .
- Meaning in symbols: $\forall a, b, c \in S, (a * b) * c = a * (b * c)$.

Observation: For an associative operation $*$, we can write the symbol $a * b * c$ without having to specify whether we mean $(a * b) * c$ or $a * (b * c)$, because the placement of the parentheses does not matter.

This cannot be done when $*$ is not associative. That is, the symbol $a*b*c$ would be useless, because we don't know whether to interpret it as $(a*b)*c$ or $a*(b*c)$, and these two interpretations might give different results.

Example: Consider the set of real numbers, \mathbb{R} , with the operation of addition, $+$. This is a binary operation, because when a and b are real numbers, $a+b$ is also a real number. That this operation is associative is a fact that we all probably learned in grade school or junior high.

Example: Consider the set of real numbers, \mathbb{R} , with the operation of subtraction, $-$. This is a binary operation, because when a and b are real numbers, $a-b$ is also a real number. Let $a=b=c=1$. Then $(a-b)-c=(1-1)-1=-1$, while $a-(b-c)=1-(1-1)=1$. So for this example, $(a-b)-c \neq a-(b-c)$. Now let $a=b=1$, $c=0$. Then $(a-b)-c=(1-1)-0=0$, while $a-(b-c)=1-(1-0)=0$. For this example, $(a-b)-c = a-(b-c)$. What, then, should our conclusion be? Is the operation of subtraction associative or not? It seems that for some choices of numbers a , b , and c , the placement of the parentheses makes a difference, but for some other choices of numbers a , b , and c , the placement of the parentheses does not make a difference. For an answer, look back at the definition of associative. The definition says that an operation is called associative only when *for all choices* of numbers a , b , and c , the placement of the parentheses does not make a difference. If there is even a single example of three numbers a , b , and c for which the placement of the parentheses does make a difference, then we have to conclude that the operation is not associative. So, we conclude that the operation of subtraction is not associative.

Remark: If you type $1-1-1$ into a graphing calculator and hit enter, you will probably get an answer of -1 . The calculator is assuming that you meant $(1-1)-1$, not $1-(1-1)$. But this does not mean that it is okay for us to write the symbol $1-1-1$. Whenever we write expressions involving binary operations that are not associative, we should be sure to include parentheses to indicate exactly which pairs of numbers are to be processed first.

2.1.3. Binary operations with identity

The second property of binary operations that we will consider pertains to an "identity element".

Definition 14 binary operation with an identity element

- Words: "the operation $*$ on S has an identity element"
- Usage: S is a set (not necessarily a set of points) and $*$ is a binary operation on S .
- Meaning in symbols: $\exists e \in S, \forall a \in S, e*a = a$ AND $a*e = a$
- Additional terminology: The element $e \in S$ is called an *identity element* for the operation $*$.
- Comment on word choice: It is not hard to show that there can be only one identity element for a given binary operation on a set. For that reason, we will say *the* identity element, rather than *an* identity element, from now on.

Example: Consider the set of integers, \mathbb{Z} , with binary operation of addition, $+$. Observe that for any integer x , the following two equations are true: $0+x=x$ and $x+0=x$. Those two equations tell us that the number 0 is the identity element for the operation of addition. The number 0 is often called the additive identity element.

Example: Consider the set of integers, \mathbb{Z} , with binary operation of multiplication, \cdot . Observe that for any integer x , the following two equations are true: $1 \cdot x = x$ and $x \cdot 1 = x$. Those two equations tell us that the number 1 is the identity element for the operation of multiplication. The number 1 is often called the multiplicative identity element.

The two examples above show that the identity element depends on the choice of binary operation. We now return to two examples that we considered earlier.

Example: Let A be the set of even integers and let \cdot be the operation of multiplication. The operation \cdot is a binary operation on set A , but there is no identity element. That is, there is no even integer e with the property that for all even integers x , the two equations $e \cdot x = x$ and $x \cdot e = x$ are true. Put another way, the only integer that could possibly play the role of the multiplicative identity element is the number 1, but that number is not in the set of even numbers.

Example: Let B be the set of odd integers and let \cdot be the operation of multiplication. The operation \cdot is a binary operation on set B , with identity element $e = 1$.

2.1.4. Binary operations with inverses

The third property of binary operations that we will consider pertains to an “inverse” for each element.

Definition 15 binary operation with inverses

- Words: “the set S , with operation $*$, has inverses for each element”
- Usage: S is a set and $*$ is a binary operation on S with an identity element.
- Meaning in symbols: $\forall x \in S, \exists y \in S, x * y = e$ AND $y * x = e$
- Additional terminology: It is not hard to show that for a given element $x \in S$, there can be at most one element $y \in S$ as described above. The element y , if it exists, is called *the* inverse of x , and is denoted x^{-1}

Note that the definition of an inverse element involves a reference to the identity element. So it does not make sense to talk of inverses unless the binary operation has an identity element.

Example: Consider the set of integers, \mathbb{Z} , with binary operation of addition, $+$. Observe that for any integer x , the following two equations are true: $x + (-x) = 0$ and $(-x) + x = 0$. Those two equations tell us that the number $-x$ is qualified to be called the inverse of x . We would say more precisely that the number $-x$ is the additive inverse of x . We could use the usual notation for the inverse of an element and write $x^{-1} = -x$, but that would undoubtedly lead to some confusion for the reader, because we are used to interpreting the symbol x^{-1} to mean $\frac{1}{x}$. So when the binary operation is addition, we usually write the additive inverse as $-x$, rather than x^{-1} .

Example: Consider the set of integers, \mathbb{Z} , with binary operation of multiplication, \cdot . The multiplicative inverse of the element $x = 1$ is the number $x = 1$, because $1 \cdot 1 = 1$, and the multiplicative inverse of the element $x = -1$ is the number $x = -1$, because $(-1) \cdot (-1) = 1$. But no other elements of the set \mathbb{Z} have multiplicative inverses. For example, consider the integer $x = 5$. It is true that $5 \cdot \left(\frac{1}{5}\right) = \left(\frac{1}{5}\right) \cdot 5 = 1$. But

we cannot say that $y = \frac{1}{5}$ is the multiplicative inverse of $x = 5$ because the number $y = \frac{1}{5}$ is not an integer. So we have to conclude that the set of integers, \mathbb{Z} , with binary operation of multiplication, \cdot , does not have an inverse for every element.

2.1.5. Commutative binary operations

The final property of binary operations that we will consider pertains to whether or not order is important when performing the binary operation. The first issue is whether order is important for a particular pair of elements. That issue is addressed in the following definition.

Definition 16 commuting elements

- Words: “elements a and b commute”
- Usage: There is a set S and a binary operation $*$ in use, and a and b are elements of the set S .
- Meaning in symbols: $a * b = b * a$

Example: Let S be the set of invertible 2×2 matrices with real number entries. A common symbol for this set is $GL(2, \mathbb{R})$. Consider the operation of matrix multiplication. Recall from linear algebra that the product of two invertible 2×2 matrices with real number entries will be an invertible 2×2 matrix with real number entries. This tells us that the operation of matrix multiplication is a binary operation on the set $GL(2, \mathbb{R})$. Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 0 \\ 0 & -7 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, and $D = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. (It is not difficult to show

that these matrices are invertible. The easiest way is to observe that the determinant of each of them is non-zero.) We compute the products AB , BA , CD , and DC .

$$AB = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & -7 \end{bmatrix} = \begin{bmatrix} 10 & 0 \\ 0 & -21 \end{bmatrix} \quad BA = \begin{bmatrix} 5 & 0 \\ 0 & -7 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 10 & 0 \\ 0 & -21 \end{bmatrix}$$

$$CD = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \quad DC = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

Observe that $AB = BA$ and $CD \neq DC$. We say that *elements A and B commute* and that *elements C and D do not commute*.

Definition 17 commutative binary operation

- Words: “the operation $*$ on S is commutative”
- Usage: S is a set and $*$ is a binary operation on S .
- Meaning in symbols: $\forall a, b \in S, a * b = b * a$
- Meaning in words: every pair of elements commutes

We see that the binary operation of matrix multiplication on the set $GL(2, \mathbb{R})$ is not commutative, for though there are some pairs of matrices that do commute, there are also pairs of matrices that do not.

2.2. Definition of a group

The definitions of the previous section are key elements in the definition of a group, an important concept from abstract algebra that will play a central role in our study of symmetry.

Definition 18 group

- Symbol: $\langle G, * \rangle$
- Words: “the group G with operation $*$ ”
- Usage: G is a set and $*$ is a binary operation on G .
- Meaning: The operation $*$ on set G is associative, has an identity, and has inverses.
- Additional Terminology: A group $\langle G, * \rangle$ whose operation $*$ is commutative is called a *commutative group*, or an *abelian group*.

Example: $\langle \mathbb{Z}, + \rangle$ is a group. The operation of addition has been considered in earlier examples. That the operation is associative is a fact we all learn in grade school or junior high. The number 0 is the identity element, and given any integer x , the inverse of x is the number $-x$. We call $-x$ the *additive inverse* of x .

What is important to notice is that a group has only one operation. When we study the group $\langle \mathbb{Z}, + \rangle$, we focus on integer addition and its properties. Of course one can also multiply integers, and there is much to say about the multiplication operation and its interaction with the addition operation. But in studying $\langle \mathbb{Z}, + \rangle$, the goal is to isolate properties of integer arithmetic that arise purely from the addition operation.

Example: $\langle \mathbb{Z}, \cdot \rangle$ is not a group (and so the symbol $\langle \mathbb{Z}, \cdot \rangle$ is not actually a valid mathematical symbol). Multiplication is a binary operation, and it is associative, and there is an identity element. (The multiplicative identity element is the number 1.) But as we saw above, the operation does not have inverses. Remember the example of the integer $x = 5$. It is true that $5 \cdot \left(\frac{1}{5}\right) = \left(\frac{1}{5}\right) \cdot 5 = 1$. But we cannot say that $y = \frac{1}{5}$ is the multiplicative inverse of $x = 5$ because the number $y = \frac{1}{5}$ is not an integer.

One might suspect that if we consider a larger set, one that would contain numbers like $y = \frac{1}{5}$, then we might be able to have a group with the multiplication operation. The next two examples explore this.

Example: $\langle \mathbb{R}, \cdot \rangle$ is not a group (and so the symbol $\langle \mathbb{R}, \cdot \rangle$ is not actually a valid mathematical symbol). Multiplication is a binary operation, and it is associative, and there is an identity element. (The multiplicative identity element is the number 1.) But, the operation does not have inverses. Consider the example of the real number $x = 0$. There is no real number y such that $0 \cdot y = y \cdot 0 = 1$.

Example: $\langle \mathbb{R}^*, \cdot \rangle$ is a group. (\mathbb{R}^* is the set of non-zero real numbers.) Multiplication is a binary operation, and it is associative, and there is an identity element—the multiplicative identity element is the number 1—and every element has a multiplicative inverse. For any non-zero real number x , the multiplicative inverse of x will be the non-zero real number $\frac{1}{x}$. This multiplicative inverse is denoted x^{-1} . That is, $x^{-1} = \frac{1}{x}$.

Examples of finite groups: Remember that a group is a set with a binary operation that has three special properties. All of the examples of groups that we have seen so far involve infinite sets. But there are lots of groups involving finite sets. We saw earlier that binary operations on a finite set can be shown in a

table. So a finite group can also be shown in a table. Two examples of groups with four elements are shown in the tables below. The “V” in the name of the first group is short for *vier*, the German word for *four*. It refers to the fact that the group has four elements. The name of the cyclic group will make sense when we revisit this group later in the unit.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The Klein V-group

#	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

The cyclic group
with four elements

2.3. Exercises

[1] Remember that a *Binary Operation* on a set S is a map $*$: $S \times S \rightarrow S$. That is, $*$ is a function that takes as input a pair of elements of S , and produces as output an element of S . In class and in the notes, we discussed four properties that a binary operation on a set may or may not have:

Property	Words	meaning
1	$*$ is associative	$\forall a, b, c \in S, (a * b) * c = a * (b * c)$
2	$*$ has an identity element	$\exists e \in S, \forall a \in S, e * a = a$ AND $a * e = a$
3	$*$ has inverses	$\forall x \in S, \exists y \in S, x * y = e$ AND $y * x = e$
4	$*$ is commutative	$\forall a, b \in S, a * b = b * a$

Below is a table containing examples of sets, each with an accompanying operation, $*$, that may or may not be a binary operation. Fill in the table below by writing “yes” or “no” in each cell. If an example has an operation that turns out NOT be a *binary operation*, then , answer “no” to the “Binary Operation?” question, and skip the rest of the questions in that row, putting “X” in those boxes. Also, if an example is a binary operation but does not have an identity, then there is no way that it can have inverses. So, in that case, you can just put an “X” in the “inverse box”. (Remember that \mathbb{Z} is the set of integers, \mathbb{Z}^* is the set of non-zero integers, \mathbb{Z}^+ is the set of positive integers, \mathbb{R} is the set of real numbers, and \mathbb{R}^* is the set of non-zero real numbers.)

Example	Set	*	Binary Operation?	Associative?	Identity?	Inverses?	Commutative?
1	\mathbb{Z}	$a * b = a + b$					
2	\mathbb{Z}	$a * b = ab$					
3	\mathbb{Z}	$a * b = ab + 1$					
4	\mathbb{Z}^+	$a * b = b - a$					
5	\mathbb{Z}	$a * b = b - a$					
6	\mathbb{Z}	$a * b = \frac{a}{b}$					
7	\mathbb{Z}^*	$a * b = \frac{a}{b}$					
8	\mathbb{R}^*	$a * b = \frac{a}{b}$					
9	\mathbb{R}^*	$a * b = ab$					
10	\mathbb{R}^*	$a * b = \frac{ab}{2}$					

[2] Complete the table so as to define a commutative binary operation $*$ on the set $S = \{a, b, c, d\}$.

$*$	a	b	c	d
a	a	b	c	
b	b	d		c
c	c	a	d	d
d	d			a

[3] Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, and $D = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and let $*$ denote matrix

multiplication. Show that the set $\{A, B, C, D\}$, with the operation $*$, is a group. Hint: Show that $*$ is a binary operation (do this with a table!). Then, explain why $*$ is associative (just say that it is a fact of linear algebra that matrix multiplication is always associative). Then, present an element of the set that can play the role of the identity element. Then, for each element of the set, give an inverse element.

[4] Let $D = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $E = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $F = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, and $G = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ and let $*$ denote matrix

multiplication. Show that the set $\{D, E, F, G\}$, with the operation $*$, is not a group. Hint: Try to do the same steps that you did in exercise [3]. When something goes wrong, present that as evidence that the set is not a group.

3. Symmetry Groups

We have finally arrived at the core chapter of Unit 3. In this section, we establish the link between the geometric notion of symmetry and the algebraic notion of a group.

3.1. The Set of Symmetries a Set of Points is a Group

The following theorem needs no further introduction

Theorem 1 If $S \subset \mathbb{R}^2$ is a set of points, and G is the set symmetries of S , and the symbol \circ denotes the operation of function composition, then $\langle G, \circ \rangle$ is a group.

Proof:

Step 1 (Show that \circ is a binary operation on the set G):

Let f and g be two symmetries of S . That is, $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ and $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ are isometries and they both fix S . We must show that $f \circ g$ is also a symmetry of S . That is, we must show that $f \circ g$ is an isometry and that it fixes S . The fact that the composition of two isometries is another isometry was proven in Unit 2. To see that $f \circ g$ fixes S , observe that

$$\begin{aligned} f \circ g(S) &= f(g(S)) && \text{by definition of function composition} \\ &= f(S) && \text{because } g \text{ fixes } S \\ &= S && \text{because } f \text{ fixes } S \end{aligned}$$

Therefore, $f \circ g$ fixes S . Conclude that $f \circ g$ is a symmetry of S .

Step 2 (Show that the binary operation is associative):

We will show that function composition is associative, regardless of whether or not the functions in question are isometries. Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, and $h : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be any three maps of \mathbb{R}^2 , and let $P \in \mathbb{R}^2$ be any point. Then

$$(f \circ g) \circ h(P) = (f \circ g)(h(P)) = f(g(h(P)))$$

$$f \circ (g \circ h)(P) = f((g \circ h)(P)) = f(g(h(P)))$$

We see that $(f \circ g) \circ h(P) = f \circ (g \circ h)(P)$ for any point P . Therefore, $(f \circ g) \circ h = f \circ (g \circ h)$.

Step 3 (Show that the binary operation has an identity element):

Consider the map $id_{\mathbb{R}^2}$. Recall that we have seen that the map $id_{\mathbb{R}^2}$ is an isometry, and that it is a symmetry of set S . (Regardless of what the set S is.) Therefore, $id_{\mathbb{R}^2}$ is an element of the set G of symmetries of S . Now, let f be any element of G . Then f is a function, $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$. Observe that $id_{\mathbb{R}^2} \circ f = f$ and $f \circ id_{\mathbb{R}^2} = f$. This tells us that the element $id_{\mathbb{R}^2}$ can play the role of the identity element for set G with operation \circ .

Step 4 (Show that the binary operation has inverses):

Let f be an element of G . We must show that there is an inverse of f in G . Because f is an element of G , we know that it is a Euclidean isometry of \mathbb{R}^2 . Therefore, f is bijective, and so there is an inverse map $f^{-1} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ such that $f^{-1} \circ f = id_{\mathbb{R}^2}$ and $f \circ f^{-1} = id_{\mathbb{R}^2}$. So far, we know that f has an inverse, f^{-1} . We have not shown that the inverse is an element of G . To do that, we must show that f^{-1} is an isometry and that f^{-1} fixes S . To show that f^{-1} is an isometry, let $P \in \mathbb{R}^2$ and $Q \in \mathbb{R}^2$ be any two points. Observe that

$$\begin{aligned} d_2(f^{-1}(P), f^{-1}(Q)) &= d_2(f(f^{-1}(P)), f(f^{-1}(Q))) && \text{because } f \text{ is an isometry} \\ &= d_2(f \circ f^{-1}(P), f \circ f^{-1}(Q)) && \text{by definition of function composition} \\ &= d_2(id_{\mathbb{R}^2}(P), id_{\mathbb{R}^2}(Q)) && \text{because } f \text{ and } f^{-1} \text{ are inverses} \\ &= d_2(P, Q) && \text{by definition of the identity map} \end{aligned}$$

This confirms that f^{-1} is a Euclidean isometry. To show that f^{-1} fixes S , observe that

$$\begin{aligned} f^{-1}(S) &= f^{-1}(f(S)) && \text{because } f \text{ fixes } S \\ &= f^{-1} \circ f(S) && \text{by definition of function composition} \\ &= id_{\mathbb{R}^2}(S) && \text{because } f \text{ and } f^{-1} \text{ are inverses} \\ &= S && \text{by definition of the identity map} \end{aligned}$$

Therefore, f^{-1} fixes S .

End of proof

3.2. Examples of Symmetry Groups

We will revisit some examples that we investigated earlier:

Example: Let set A be an equilateral triangle centered at the origin, as shown in the picture at right, and let $\langle G, \circ \rangle$ be the group of symmetries of A . The group has six elements: $id_{\mathbb{R}^2}$, $R_{(0,0),120^\circ}$, $R_{(0,0),240^\circ}$, $M_{x\text{-axis}}$, M_L , and M_M , where L is the line through the origin that makes a 120° angle with the positive x -axis and M is the line through the origin that makes a 240° angle with the positive x -axis.

Example: Let set B be an isosceles triangle, as shown in the picture at right, and let $\langle G, \circ \rangle$ be the group of symmetries of B . The group has two elements: They are $id_{\mathbb{R}^2}$ and $M_{x\text{-axis}}$.

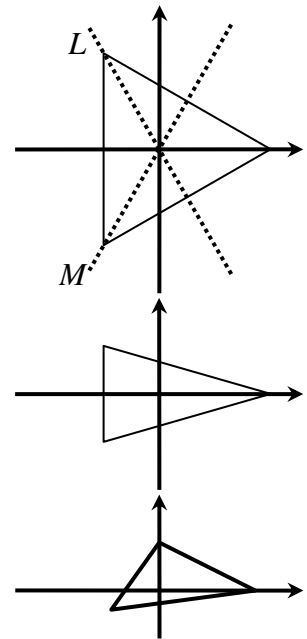
Example: Let set C be a scalene triangle, as shown in the picture at right and let $\langle G, \circ \rangle$ be the group of symmetries of C . The group has only one element: the identity map $id_{\mathbb{R}^2}$.

Example: Let set D be the frieze shown in the picture at right, and let $\langle G, \circ \rangle$ be the group of symmetries of D . The group G is infinite: all of the translations $T_{\langle k,0 \rangle}$, where k is any integer, are members, and the reflection $M_{x\text{-axis}}$ across the axis is a member. (Observe that the translation $T_{\langle 0,0 \rangle}$ corresponding to $k = 0$ is just the identity map, $id_{\mathbb{R}^2}$, in disguise. It is the identity element for the group G .)

Example: Let set E be the frieze shown in the picture at right, and let $\langle G, \circ \rangle$ be the group of symmetries of E . The group G is infinite: all of the translations $T_{\langle k,0 \rangle}$, where k is any integer, are members. (Again note that the translation $T_{\langle 0,0 \rangle}$ is just the identity map, $id_{\mathbb{R}^2}$, in disguise.)

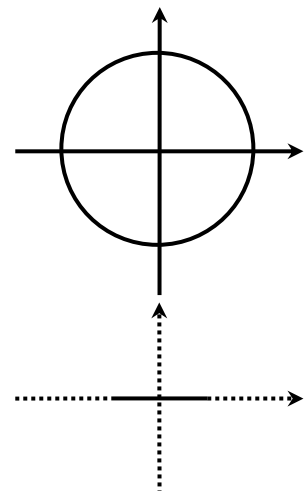
Example: Let set F be a circle centered at the origin, as shown in the picture at right, and let $\langle G, \circ \rangle$ be the group of symmetries of F . The group G is infinite: All of the rotations $R_{(0,0),\varphi}$, where φ is any angle, are members, and all of the reflection M_L , where L is any line through the origin, are members. (Observe that the rotation $R_{(0,0),0}$ corresponding to the angle $\varphi = 0$ is just the identity map, $id_{\mathbb{R}^2}$, in disguise.)

Example: Let set H be the line segment $[-1,1]$ shown in the picture at right, and let $\langle G, \circ \rangle$ be the group of symmetries of H . The group G has four members. They are $id_{\mathbb{R}^2}$, $R_{(0,0),180^\circ}$, $M_{x\text{-axis}}$, and $M_{y\text{-axis}}$.



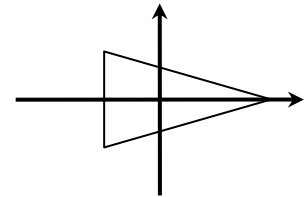
... E E E E ...

... e e e e ...



3.3. Exercises

[1] In this example, you will explore the group of symmetries of set B , where B is the isosceles triangle shown in the picture at right. Let $\langle G, \circ \rangle$ be the group of symmetries of B . The group has two elements: They are $id_{\mathbb{R}^2}$ and M_{x-axis} .



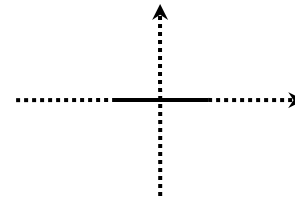
\circ	id	M_{x-axis}
id		
M_{x-axis}		

(a) Fill out the group table shown at right. For simplicity, the symbol $id_{\mathbb{R}^2}$ has been abbreviated to id .

(b) Is the group $\langle G, \circ \rangle$ abelian?

[2] In this example, you will explore the group of symmetries of set H , where H is the line segment $[-1,1]$ shown in the picture at right. Let $\langle G, \circ \rangle$ be the group of symmetries of H . The group G has four members.

They are $id_{\mathbb{R}^2}$, $R_{(0,0),180^\circ}$, M_{x-axis} , and M_{y-axis} .



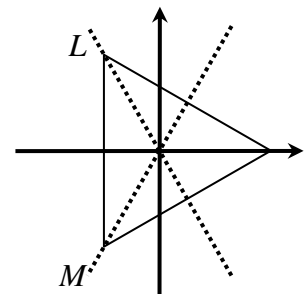
\circ	id	R_{180°	M_{x-axis}	M_{y-axis}
id				
R_{180°				
M_{x-axis}				
M_{y-axis}				

(a) Fill out the group table shown at right. For simplicity, the symbol $id_{\mathbb{R}^2}$ has been abbreviated to id , and the symbol $R_{(0,0),180^\circ}$ has been abbreviated to R_{180° .

(b) Is the group $\langle G, \circ \rangle$ abelian?

[3] In this exercise, you will explore the *dihedral group with six elements*, D_6 .

This is the group of symmetries of an equilateral triangle. If we orient the triangle with its center at the origin, and one of the vertices lying on the positive x -axis as shown in the figure at right, then the elements of this group are: $id_{\mathbb{R}^2}$, $R_{(0,0),120^\circ}$, $R_{(0,0),240^\circ}$, M_{x-axis} , M_L , and M_M , where L is the line



through the origin that makes a 120° angle with the positive x -axis and M is the line through the origin that makes a 240° angle with the positive x -axis.

In the figure, you should think of the coordinate axes and the dotted lines as being fixed to the table, while the triangle is the thing that gets rotated and flipped. For instance, the x -axis is always horizontal, and line L (the 120° line) always goes from upper left to lower right, as shown.)

(a) Fill out the group table shown at right. For simplicity, the symbol $id_{\mathbb{R}^2}$ has been abbreviated to id , and the symbols $R_{(0,0),120^\circ}$ and $R_{(0,0),240^\circ}$ have been abbreviated to R_{120° and R_{240° .

(b) Is the group D_6 abelian?

\circ	$id_{\mathbb{R}^2}$	R_{120°	R_{240°	M_{x-axis}	M_L	M_M
$id_{\mathbb{R}^2}$						
R_{120°						
R_{240°						
M_{x-axis}						
M_L						
M_M						

4. Exploring Groups

In this chapter, we will study some of the most basic properties of groups and investigate some of the simplest examples of groups.

4.1. General properties

The definition of a group is very short. But the three properties that define a group imply a host of other properties, as well. In this section, we look at a few properties that are as fundamental as the properties that are part of the group definition. But the properties are not included as part of the definition of a group because they don't need to be: they can be proven as theorems.

The first theorem fills in some details about group behavior.

Theorem 2 Basic facts about associativity, identity elements, and inverse elements

If $\langle G, * \rangle$ is a group then

- 1) for any $x_1, x_2, \dots, x_n \in G$, the value of $x_1 * x_2 * \dots * x_n$ does not depend on how parentheses are placed.
- 2) the identity element of G is unique
- 3) for each element $x \in G$, the inverse element x^{-1} is unique
- 4) for each element $x \in G$, the inverse of x^{-1} is x .
- 5) for each pair of elements $x, y \in G$, the inverse of $x * y$ is the element $y^{-1} * x^{-1}$.

The proof of statement (1) is a nuisance. It is straightforward to prove the statement by induction, but the proof is quite long, longer than I want you to deal with in this geometry course. (Remember that I tried to present the proof in class before I was drowned out by the sound of snoring.) At heart, the proof uses the fact that the associativity property holds for any collection of 3 elements. We will just use the fact that statement (1) is true, and skip its proof.

Proof of Statement 2)

Suppose that e_1 and e_2 are identity elements for group G . We must show that they are in fact the same element.

$$\begin{aligned} e_1 &= e_1 * e_2 && \text{because } e_2 \text{ is an identity element} \\ &= e_2 && \text{because } e_1 \text{ is an identity element} \end{aligned}$$

End of proof of Statement 2)

Proof of Statement 3)

Suppose that $x \in G$ and that a and b are inverses of x . We must show that a and b are in fact the same element.

$$\begin{aligned} a &= a * id && \text{by definition of how the identity element works} \\ &= a * (x * b) && \text{we know that } (x * b) \text{ is the identity, because } b \text{ is an inverse of } x. \\ &= (a * x) * b && \text{associativity} \\ &= id * b && \text{we know that } (x * a) \text{ is the identity, because } a \text{ is an inverse of } x. \\ &= b \end{aligned}$$

End of proof of Statement 3)

Proof of Statement 4)

Suppose that $x \in G$ and that the inverse of x is x^{-1} . We must show that the inverse of x^{-1} is x . But we know that the elements x and x^{-1} satisfy the two equations $x * x^{-1} = id$ and $x^{-1} * x = id$. By definition, any two elements a and b that satisfy two equations of the form $a * b = id$ and $b * a = id$ are inverses of each other.

End of proof of Statement 4)

Proof of Statement 5)

Let $x, y \in G$ be any two elements. Observe that the following two equations are true:

$$\begin{aligned}(x * y) * (y^{-1} * x^{-1}) &= x * (y * y^{-1}) * x^{-1} \text{ by associative law} \\ &= x * id * x^{-1} \\ &= x * x^{-1} \\ &= id\end{aligned}$$

and

$$\begin{aligned}(y^{-1} * x^{-1}) * (x * y) &= y^{-1} * (x^{-1} * x) * y \text{ by associative law} \\ &= y^{-1} * id * y \\ &= y^{-1} * y \\ &= id\end{aligned}$$

Because any two elements a and b that satisfy two equations of the form $a * b = id$ and $b * a = id$ are inverses of each other, we conclude that the inverse of $x * y$ is the element $y^{-1} * x^{-1}$.

End of proof of Statement 5)

Theorem 3 Left and Right Cancellation Laws

1) For any $a, x, y \in G$, if $a * x = a * y$ then $x = y$.

2) For any $a, x, y \in G$, if $x * a = y * a$ then $x = y$.

Proof of statement (1).

Let $a, x, y \in G$ be any three group elements.

$$\begin{aligned}a * x &= a * y && \text{assumption} \\ a^{-1} * a * x &= a^{-1} * a * y && \text{operated on the left with } a^{-1} \\ id * x &= id * y && \text{because } a^{-1} \text{ is the inverse of } a. \\ x &= y && \text{property of the identity element}\end{aligned}$$

End of proof

A similar proof can be used to prove statement (2). (This time, operate on the right with a^{-1} .)

The left and right cancellation laws have a very important implication for group tables for finite groups. Because of them we know that there cannot be any repeated elements in a row. If there were, it would tell us that $a * x = a * y$, which would in turn indicate that $x = y$ by the left cancellation law. Similarly, there cannot be any repeated elements in a column. If there were, it would tell us that $x * a = y * a$, which would in turn indicate that $x = y$ by the right cancellation law. Now consider the fact that a finite group with n elements will have an $n \times n$ group table. (Not counting the heading row across the top and the heading column down the left.) That means that each row will contain n elements. Since there cannot be any repeated elements (because of the left cancellation law), we conclude that in each row of the

table, every one of the n elements of the group must appear exactly once. Similarly, in every column of the table, every group element must appear exactly once.

The fact that each element of a finite group must appear exactly once in each row and in each column of the group table can be exploited to save time when filling out group tables. Given a partially-filled-out table for a group $\langle G, * \rangle$, it is often possible to fill in empty cells in the table even without knowing anything about the group or its operation. You will do this in the exercises. Those of you who have played the number puzzle game called “Sudoku” will find the exercises to be very easy. Even if you do know what the group $\langle G, * \rangle$ is and how its operation $*$ works, the best way to fill out a group table is usually to fill out a few entries using what you know about the group operation, and then fill in the rest using the fact that each row and each column should contain each group element exactly once.

Another basic fact about groups and their tables has to do with abelian groups. In exercise [2.3#2] you were asked to fill in a table in order to define a commutative binary operation. No explanation was given before the exercise, but most likely, none was needed. It is easy to understand that if a binary operation on a finite set is commutative, then the table presentation of the binary operation must be symmetric across the main diagonal. The converse is also true: if the table presentation of a binary operation is symmetric across the main diagonal, then the binary operation is commutative. Extending this to groups, we see that if a finite group is abelian (commutative), then its group table will be symmetric across the main diagonal, and vice-versa.

4.2. Order of group elements

Definition 19 order of an element of a group

- words: The order of x .
- usage: $x \in G$ where $\langle G, * \rangle$ is some group
- meaning:
 - If there exists a positive integer n such that $x^n = id$, then there will exist some smallest positive integer k such that $x^k = id$. We say “The order of x is k ”, denoted $|x| = k$.
 - If there does not exist a positive integer n such that $x^n = id$, then we say that “element x is of infinite order,” denoted $|x| = \infty$.

Example: Consider the additive group $\langle \mathbb{R}, + \rangle$. The identity element of this group is the number 0.

Because $0^1 = 0$, we conclude that the order of the element 0 is 1. That is, $|0| = 1$. On the other hand, suppose that x is some non-zero element of the group. Then observe the list of powers:

$$x^1 = x \neq 0$$

$$x^2 = x + x = 2x \neq 0$$

$$x^3 = x + x + x = 3x \neq 0$$

⋮

We see that the list of powers of x will never include the identity element, 0. Therefore, x is of infinite order. That is, $|x| = \infty$. So we see that the group $\langle \mathbb{R}, + \rangle$ contains one element of order 1, and all the rest are of infinite order.

Example: Consider the multiplicative group $\langle \mathbb{R}^*, \cdot \rangle$. The identity element of this group is the number 1.

Because $1^1 = 1$, we conclude that the order of the element 1 is 1. That is, $|1| = 1$.

Now consider the list of powers of the element $x = -1$.

$$(-1)^1 = (-1) \neq 1$$

$$(-1)^2 = (-1) * (-1) = (-1) \cdot (-1) = 1 = id$$

We conclude that the order of the element $x = -1$ is 2. That is, $|-1| = 2$.

On the other hand, suppose that x is some element of the group that is neither 1 nor -1. Then observe the list of powers:

$$x^1 = x \neq 1$$

$$x^2 = x \cdot x \neq 1$$

$$x^3 = x \cdot x \cdot x \neq 1$$

$$\vdots$$

We see that the list of powers of x will never include the identity element, 1. Therefore, x is of infinite order. That is, $|x| = \infty$. So we see that the group $\langle \mathbb{R}^*, \cdot \rangle$ contains one element of order 1, one element of order 2, and all the rest are of infinite order.

Before proceeding with the next example of a group, it would be useful to identify some notation used for describing certain sets of integers. The next two definitions do that.

Definition 20 the set of multiples of n

- Symbol: $n\mathbb{Z}$
- Spoken: the set of multiples of n
- Usage: n is an integer. (Usually, the notation is used in cases where $n \geq 2$.)
- Meaning: the set $n\mathbb{Z} = \{kn \text{ such that } k \in \mathbb{Z}\} = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$

Examples: $5\mathbb{Z}$ is the set $\{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$.

$2\mathbb{Z}$ is the set $\{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$. (Note that this is the set of even numbers!)

Definition 21 the set of the first n non-negative integers

- Symbols: $\frac{\mathbb{Z}}{n\mathbb{Z}}$ or \mathbb{Z}_n
- Spoken: the set of the first n non-negative integers
- Usage: n is a non-negative integer. That is, $n \geq 0$.
- Meaning: the set $\mathbb{Z}_n = \{0, 1, 2, \dots, n-2, n-1\}$

Remark: Notice that the set \mathbb{Z}_n contains n elements, starting with 0 and ending with $n-1$.

Examples: \mathbb{Z}_5 is the set $\{0, 1, 2, 3, 4\}$.

\mathbb{Z}_2 is the set $\{0, 1\}$. (Note that this is the set of even numbers!)

\mathbb{Z}_1 is the set $\{0\}$.

\mathbb{Z}_0 is the empty set, $\{\}$.

The set of the first n non-negative integers can be used to define a common group that is useful for exploring the concept of the order of group elements:

Definition 22 the group of integers mod n

- symbol: group $\langle \frac{\mathbb{Z}}{n\mathbb{Z}}, * \rangle$, or $\langle \mathbb{Z}_n, * \rangle$
- spoken: the group of integers mod n
- usage: n is some positive integer.
- meaning: the set $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$, with operation $*$ defined by $a * b = (a + b) \bmod n$.

In class, we discussed the fact that this operation is a binary operation, that it is associative, that it has an identity element, and that it has inverses for each element.

Example: Consider the group $\langle \mathbb{Z}_4, * \rangle$. The set of elements is $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. An example of the group operation at work is the calculation $2 * 3 = (2 + 3) \bmod 4 = (5) \bmod 4 = 1$. The identity element for this group is the number 0. We can determine the order of each of the four elements of this group by considering the list of powers of each of them.

powers of 0: $0^1 = 0 = id$, so the order of 0 is 1. That is, $|0| = 1$.

powers of 1: $1^1 = 1$

$$1^2 = 1 * 1 = (1 + 1) \bmod 4 = 2$$

$$1^3 = 1 * 1 * 1 = (1 * 1) * 1 = 2 * 1 = (2 + 1) \bmod 4 = (3) \bmod 4 = 3$$

$$1^4 = 1 * 1 * 1 * 1 = (1 * 1 * 1) * 1 = 3 * 1 = (3 + 1) \bmod 4 = (4) \bmod 4 = 0 = id$$

So the order of 1 is 4. That is, $|1| = 4$.

powers of 2: $2^1 = 2$

$$2^2 = 2 * 2 = (2 + 2) \bmod 4 = (4) \bmod 4 = 0 = id$$

So the order of 2 is 2. That is, $|2| = 2$.

powers of 3: $3^1 = 3$

$$3^2 = 3 * 3 = (3 + 3) \bmod 4 = (6) \bmod 4 = 2$$

$$3^3 = 3 * 3 * 3 = (3 * 3) * 3 = 2 * 3 = (2 + 3) \bmod 4 = (1) \bmod 4 = 1$$

$$3^4 = 3 * 3 * 3 * 3 = (3 * 3 * 3) * 3 = 1 * 3 = (1 + 3) \bmod 4 = (4) \bmod 4 = 0 = id$$

So the order of 3 is 4. That is, $|3| = 4$.

4.3. Cyclic Groups

Notice that in the example of $\langle \mathbb{Z}_4, * \rangle$ given above, the list of powers of the element 1 was actually a complete list of all of the group elements. The same was true for the element 3, but it was not true of the

elements 0 and 2. Not all groups have such elements like 1 and 3. Those groups that do are called *cyclic groups*.

Definition 23 cyclic group

- words: $\langle G, * \rangle$ is cyclic
- meaning: there is some element $g \in G$ such that the list of all the powers of element g (that is, all positive, negative, and zero powers of g) includes all of the elements in the group G .
- additional terminology: We say that g is a *generator of G* , and that g *generates G* .

As we saw in the example of the group $\langle \mathbb{Z}_4, * \rangle$, it is possible for a cyclic group to have more than one generator.

Example: Consider the group $\langle \mathbb{Z}, + \rangle$. The identity element in this group is the number 0. Let's examine the positive, negative, and zero powers of the element $x = 1$

positive powers of 1:	$1^1 = 1$
	$1^2 = 1 * 1 = 1 + 1 = 2$
	$1^3 = 1 * 1 * 1 = (1 * 1) * 1 = 2 * 1 = 2 + 1 = 3$
	and so on...
zero power of 1:	1^0 means the identity element, which is 0. That is, $1^0 = 0$
negative powers of 1:	1^{-1} means the additive inverse of the element $1^1 = 1$. Therefore, $1^{-1} = -1$.
	1^{-2} means the additive inverse of the element $1^2 = 2$. Therefore, $1^{-2} = -2$.
	1^{-3} means the additive inverse of the element $1^3 = 3$. Therefore, $1^{-3} = -3$.
	and so on...

We see that the list of powers of the element $x = 1$ is the entire set \mathbb{Z} . So $x = 1$ is a generator of the group $\langle \mathbb{Z}, + \rangle$. We conclude that the group $\langle \mathbb{Z}, + \rangle$ is cyclic. In the exercises, you will look for other generators for this group.

4.4. Subgroups

A subgroup is essentially a “group within a group”.

Definition 24 subgroup

- symbol: $\langle H, * \rangle < \langle G, * \rangle$
- usage: $\langle G, * \rangle$ is a group
- meaning: $H \subset G$ (that is, H is a subset of G) and $\langle H, * \rangle$ is a group.

Example: We can say $\langle \{0, 2\}, * \rangle < \langle \mathbb{Z}_4, * \rangle$. Notice that in the subgroup $\langle \{0, 2\}, * \rangle$, there is an identity element (the number 0), and every element has an inverse. (The inverse of 0 is 0 and the inverse of 2 is 2).

Example: We can say $\langle \{0\}, * \rangle < \langle \mathbb{Z}_4, * \rangle$. In the subgroup $\langle \{0\}, * \rangle$, there is an identity element (the number 0), and every element has an inverse.

Remark: In any group $\langle G, * \rangle$, we can always say $\langle \{id\}, * \rangle < \langle G, * \rangle$. The subgroup $\langle \{id\}, * \rangle < \langle G, * \rangle$ is called a *trivial subgroup*. We can also say $\langle G, * \rangle < \langle G, * \rangle$. In some books, the subgroup $\langle G, * \rangle < \langle G, * \rangle$ is also called a *trivial subgroup*.

Example: In the group $\langle \mathbb{Z}_4, * \rangle$, the set $\{0, 1, 2\}$ is not closed under the group operation. That is, $1 * 2 = 3$, which is not in the set $\{0, 1, 2\}$. So the set $\{0, 1, 2\}$ is not a subgroup of the group $\langle \mathbb{Z}_4, * \rangle$.

Example: Consider the group $\langle \mathbb{Z}, + \rangle$.

- The set of positive integers, $\mathbb{Z}^+ \subset \mathbb{Z}$, is closed under the group operation because if a and b are positive, then $a + b$ is also positive. But the set \mathbb{Z}^+ does not contain an identity element. So the set \mathbb{Z}^+ is not a subgroup of the group $\langle \mathbb{Z}, + \rangle$.
- The set of non-negative integers, $\mathbb{Z}^{nonneg} \subset \mathbb{Z}$, is closed under the group operation because if a and b are nonnegative, then $a + b$ is also nonnegative. And the set \mathbb{Z}^{nonneg} contains an identity element, $x = 0$. But the set \mathbb{Z}^{nonneg} does not have inverse elements. For example, there is no inverse for the number $x = 5$. So the set \mathbb{Z}^{nonneg} is not a subgroup of the group $\langle \mathbb{Z}, + \rangle$.
- The set of even integers, $2\mathbb{Z} \subset \mathbb{Z}$, is closed under the group operation because if a and b are even, then $a + b$ is also even. And the set $2\mathbb{Z}$ contains an identity element, $x = 0$. And the set $2\mathbb{Z}$ has an inverse element for each of its element: If x is an even integer, then the number $-x$ will also be an even integer, and $-x$ will be the additive inverse of x . So the set $2\mathbb{Z}$ is a subgroup of the group $\langle \mathbb{Z}, + \rangle$. We write $\langle 2\mathbb{Z}, + \rangle < \langle \mathbb{Z}, + \rangle$.

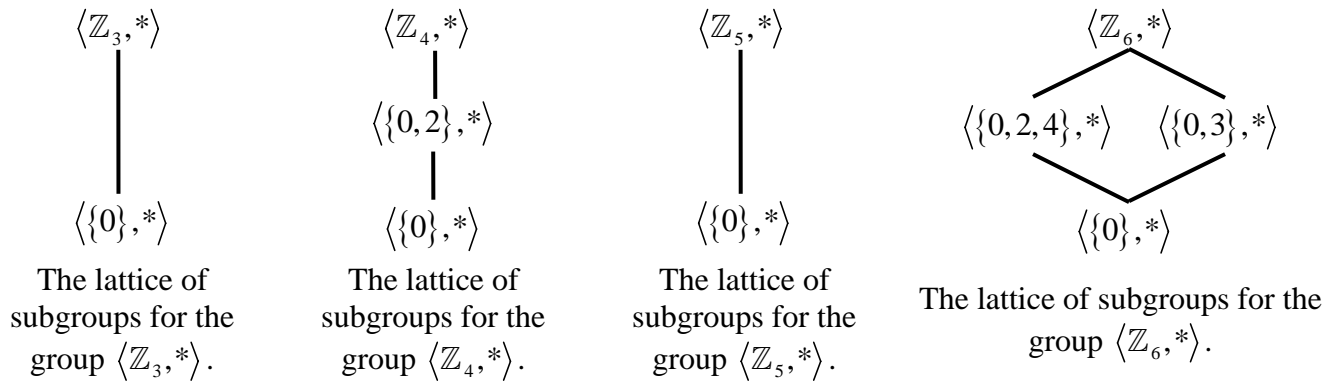
Observe that a subgroup is a group, and so a subgroup can have subgroups of its own. For example, $\langle \{0\}, * \rangle < \langle \{0, 2\}, * \rangle < \langle \mathbb{Z}_4, * \rangle$.

4.5. The lattice of subgroups of a group

There is a wonderful way of illustrating the relationship between the various subgroups of a group $\langle G, * \rangle$ in a diagram. The diagram can be produced by following a simple algorithm:

- 1) put the trivial subgroup $\langle G, * \rangle$ at the top of the diagram
- 2) put the trivial subgroup $\langle \{id\}, * \rangle$ at the bottom of the diagram.
- 3) Put other subgroups on the diagram in the following manner. If $\langle A, * \rangle < \langle B, * \rangle$, and there is no other subgroup $\langle C, * \rangle$ “in between them”, in the sense $\langle A, * \rangle < \langle C, * \rangle < \langle B, * \rangle$, then put the $\langle A, * \rangle$ and $\langle B, * \rangle$ on the diagram, with $\langle B, * \rangle$ above $\langle A, * \rangle$, and draw a line segment between them. If there are no other subgroups, then simply draw a vertical line from $\langle \{id\}, * \rangle$ to $\langle G, * \rangle$.

The figure below shows some examples of subgroup lattices for groups of type $\langle \mathbb{Z}_n, * \rangle$. Notice that increasing the size of the group does not necessarily increase the complexity of the lattice of subgroups.



4.6. Exercises

[1] In a group $\langle G, * \rangle$, prove that $x * y = y * x$ iff $y^{-1} * x * y = x$ iff $x^{-1} * y^{-1} * x * y = id$.

[2] The goal of this exercise is to prove the following statement.

“For all integers $n \geq 1$, if a and b are commuting elements of a group $\langle G, * \rangle$, then $(a * b)^n = a^n * b^n$.”

The strategy is to do a proof by induction. Let $P(n)$ be the following statement:

“If a and b are commuting elements of a group $\langle G, * \rangle$, then $(a * b)^n = a^n * b^n$.”

With the symbol $P(n)$ defined as we have defined it, the goal of the problem can be re-stated:

We want to prove that $\forall n \geq 1, P(n)$.

- Preliminary work: Write down the statement $P(1)$. (Don't prove it.)
- Preliminary work: Write down the statement $P(k)$. (Don't prove it.)
- Preliminary work: Write down the statement $P(k+1)$. (Don't prove it.)
- Basis Step: Prove that $P(1)$ is true.
- Induction Step: Prove that if $P(k)$ is true, then $P(k+1)$ is true.
- Write a conclusion of the proof.

[3] (a) Show that the number $x = -1$ is a generator of the group $\langle \mathbb{Z}, + \rangle$.

(b) Show that the number $x = 2$ is not a generator of the group $\langle \mathbb{Z}, + \rangle$.

Hint: In both (a) and (b), make a list of the positive, zero, and negative powers of the element, as was done in the example in Section 4.3.

[4] In this exercise, you will explore the group $\langle \mathbb{Z}_8, * \rangle$, where the operation $*$ is addition mod 8.

- For each element of the group, make a list of the powers of that element.
- Find the order of each of the elements of the group.
- Draw a subgroup lattice diagram for the group.
- Make a group table for the group.

[5] Shown at right is a partially-filled-out table for an unknown group $\langle G, * \rangle$.

- (a) What is the identity element?
 (b) Is the group abelian?
 (c) Fill in the empty cells.

Hint: Start by considering each cell by itself. Write down all the possible letters for that cell in the cell. Do this for all the cells. Then cross out letters that cause conflicts.

You should be left with only one letter in each cell.

- (d) Make a list of the powers of each of the elements.
 (e) Draw a subgroup lattice diagram for the group.

*	a	b	c	d	e	f	g	h
a			c	d	e			h
b						e	h	g
c	c					h	f	e
d	d			b	h	g	e	f
e	e			g	b	a	c	d
f		e	g	h	a	b	d	c
g		h	e	f	d	c	b	a
h		g	f	e	c	d	a	b

5. Dihedral Groups

5.1. Definition & Properties

Definition: the Dihedral group of order $2n$

- symbol: D_{2n} , or $\langle D_{2n}, \circ \rangle$
- spoken: the dihedral group of order $2n$
- usage: n is an integer and $n \geq 3$.
- meaning: $\langle D_{2n}, \circ \rangle$ is the group consisting of the set of symmetries of a regular n -gon (that is, a polygon with n sides of equal length), with the operation of function composition.

Example: The symbol D_6 can be written $D_{2 \cdot 3}$. In this symbol, the number n is 3. The symbol represents the group of symmetries of a polygon with 3 sides of equal length. In other words, an equilateral triangle. You investigated this group in Homework 5.

Theorem 4 The group $\langle D_{2n}, \circ \rangle$ has $2n$ elements.

Proof

Let set A be a regular n -gon, with sides of length 1, oriented so that it is centered at the origin and one of its vertices is on the positive x -axis. Label the vertices of set A with the numbers 1, 2, ..., n by starting with the vertex that is on the positive x -axis and proceeding counterclockwise. We will consider the number of ways of defining a symmetry of set A .

First, we can choose where vertex 1 will go. We have n choices, because vertex 1 must end up at one of the spots where there was a vertex before.

Once we have chosen a destination for vertex 1, we get to choose a destination for vertex 2. We don't have so many choices this time. Vertex 2 was initially adjacent to vertex 1, a distance of 1 unit from vertex 1. The map that we are trying to define is a symmetry, and all symmetries are isometries. That means that because vertex 2 was initially 1 unit from vertex 1, it must end up 1 unit from vertex 1. So, wherever vertex 1 ended up, vertex 2 must end up someplace that is 1 unit away. There are only 2 choices: vertex 2 can land either 1 unit counterclockwise or 1 unit clockwise from the spot where vertex 1 lands.

Once we have chosen the destinations of vertices 1 and 2, the destinations of all of the other vertices are automatically determined.

Since we had n choices of a destination for vertex 1 and two choices of a destination for vertex 2, we conclude that we have $2n$ possibilities when defining a symmetry of set A .

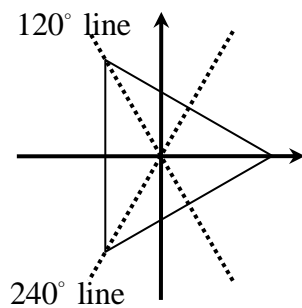
End of proof.

5.2. Completely worked example: The Dihedral group with 6 elements.

In this section, we will investigate the group D_6 using some of the tools that we have developed in the previous chapters.

The symbol D_6 can be written $D_{2,3}$, indicating that the symbol represents the group of symmetries for a 3-sided regular polygon. Such a polygon would be an equilateral triangle. In Homework 6, you explored the group of symmetries of an equilateral triangle. In that assignment, the group was called D_6 , but the name was not explained.

If we orient the triangle with its center at the origin, and one of the vertices lying on the positive x -axis, as shown in the figure below, then the elements of this group as shown in the list to the right.



Elements of the group D_6

$\rho_0 = \text{identity} = id$

$\rho_1 = \text{counterclockwise rotation through } 120^\circ$

$\rho_2 = \text{counterclockwise rotation through } 240^\circ$

$M_1 = \text{flip across the } 0^\circ \text{ line}$

$M_2 = \text{flip across the } 120^\circ \text{ line}$

$M_3 = \text{flip across the } 240^\circ \text{ line}$

(In the figure above, you should think of the degree lines as being fixed to the table, while the triangle is the thing that gets rotated and flipped. For instance, the 0° is always horizontal, and the 120° line always goes from lower left to upper right, as shown.)

Two of the tools that we know are the group table and the list of powers of each element. Here they are.

\circ	id	ρ_1	ρ_2	M_1	M_2	M_3	element	list of powers of that element
id	id	ρ_1	ρ_2	M_1	M_2	M_3	id	$id^1 = id$
ρ_1	ρ_1	ρ_2	id	M	M	M	ρ_1	$\rho_1^1 = \rho_1, \rho_1^2 = \rho_2, \rho_1^3 = id$
ρ_2	ρ_2	id	ρ_1	M	M	M	ρ_2	$\rho_2^1 = \rho_2, \rho_2^2 = \rho_1, \rho_2^3 = id$
M_1	M_1	M_2	M_3	id	ρ_1	ρ_2	M_1	$M_1^1 = M_1, M_1^2 = id$
M_2	M_2	M_3	M_1	ρ_2	id	ρ_1	M_2	$M_2^1 = M_2, M_2^2 = id$
M_3	M_3	M_1	M_2	ρ_1	ρ_2	id	M_3	$M_3^1 = M_3, M_3^2 = id$

We see that the group D_6 is not cyclic, because there is not an element that generates the entire group.

Now let's build the lattice of subgroups for D_6 . Of course the group $\langle D_6, \circ \rangle$ will be at the top, and the subgroup $\langle \{id\}, \circ \rangle$. What will be in between?

Notice that the set $\{id, \rho_1, \rho_2\}$ contains the identity, is closed under the group operation, and contains inverses for every element. Therefore, $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$ is a subgroup. Now we must figure out where to put this subgroup in the lattice of subgroups.

We know that the subgroup $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$ fits in between the two trivial subgroups. That is, $\langle \{id\}, \circ \rangle < \langle \{id, \rho_1, \rho_2\}, \circ \rangle < \langle D_6, \circ \rangle$. But are there any other subgroups in between these? For instance, is there a subgroup between $\langle \{id\}, \circ \rangle$ and $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$? To answer that question, consider omitting one of the elements of the set $\{id, \rho_1, \rho_2\}$. If we omitted the element ρ_1 , then the resulting set $\{id, \rho_2\}$ would not be a subgroup because it would not be closed under the group operation (because $\rho_2 \circ \rho_2 = \rho_1$, and ρ_1 is not in the set). A similar thing would happen if we tried to omit the element ρ_2 from the set $\{id, \rho_1, \rho_2\}$.

The conclusion is that there is no subgroup between $\langle \{id\}, \circ \rangle$ and $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$.

Therefore, $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$ will appear above $\langle \{id\}, \circ \rangle$ on the subgroup diagram, and there will be a line segment drawn between them. So far, the subgroup lattice diagram has progressed to the state shown at right.

$$\langle D_6, \circ \rangle$$

$$\begin{array}{c} \langle \{id, \rho_1, \rho_2\}, \circ \rangle \\ | \\ \langle \{id\}, \circ \rangle \end{array}$$

We must also ask if there is a subgroup between $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$ and $\langle D_6, \circ \rangle$. To answer that question, consider adding an element to the set $\{id, \rho_1, \rho_2\}$. If we added just the element M_1 , then the resulting set $\{id, \rho_1, \rho_2, M_1\}$ would not be a subgroup because it would not be closed under the group operation. To see why, note that $M_1 \circ \rho_1 = M_2$, and M_2 is not in the set. Also note that $M_1 \circ \rho_2 = M_3$, and M_3 is not in the set. We see that if we want a set that contains the set $\{id, \rho_1, \rho_2\}$ and any of the reflections $M_1, M_2, \text{ or } M_3$, and if we want that set to be a group, then the set will have to contain all of the reflections. That is, the set would have to be all of D_6 .

The conclusion is that there is no subgroup between $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$ and $\langle D_6, \circ \rangle$.

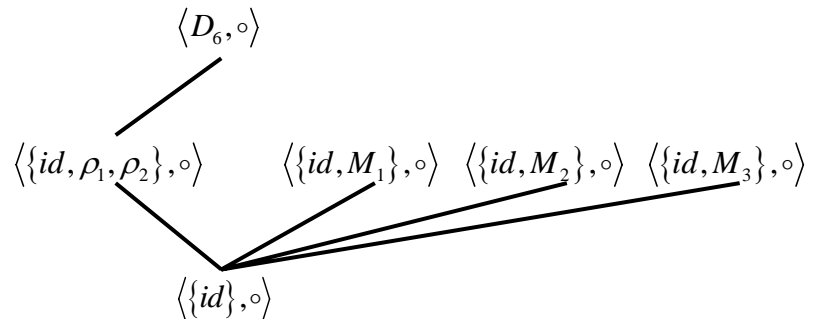
Therefore, $\langle D_6, \circ \rangle$ will appear above $\langle \{id, \rho_1, \rho_2\}, \circ \rangle$ on the subgroup diagram, and there will be a line segment drawn between them. So far, the subgroup lattice diagram has progressed to the state shown at right. But we are not done with the subgroup lattice, because there are more subgroups to be added to it.

$$\langle D_6, \circ \rangle$$

$$\begin{array}{c} | \\ \langle \{id, \rho_1, \rho_2\}, \circ \rangle \\ | \\ \langle \{id\}, \circ \rangle \end{array}$$

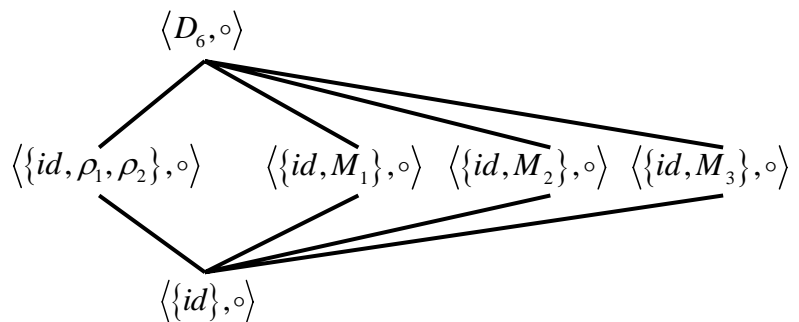
Notice that the set $\{id, M_1\}$ contains the identity, is closed under the group operation, and contains inverses for every element. Therefore, $\langle\{id, M_1\}, \circ\rangle$ is a subgroup. Now we must figure out where to put this subgroup in the lattice of subgroups. Clearly, there can be no subgroup between $\langle\{id\}, \circ\rangle$ and $\langle\{id, M_1\}, \circ\rangle$, because there is only one element different between the sets. Therefore, $\langle\{id, M_1\}, \circ\rangle$ will appear above $\langle\{id\}, \circ\rangle$ on the subgroup diagram, and there will be a line segment drawn between them. The same goes for two other similar subgroups, $\langle\{id, M_2\}, \circ\rangle$ and $\langle\{id, M_3\}, \circ\rangle$.

So far, our subgroup diagram looks like the drawing shown at right. We are still not done with the subgroup lattice, because we have not shown how the subgroups $\langle\{id, M_1\}, \circ\rangle$, $\langle\{id, M_2\}, \circ\rangle$ and $\langle\{id, M_3\}, \circ\rangle$ are related to $\langle D_6, \circ\rangle$.



Are there any subgroups between $\langle\{id, M_1\}, \circ\rangle$ and $\langle D_6, \circ\rangle$? To answer this question, consider adding an element to the set $\{id, M_1\}$ in a way that the new set is a new subgroup. If we add either of the rotations, ρ_1 or ρ_2 , then our earlier analysis tells us that we will also have to add the other rotation and the other two reflections. The resulting set would be all of D_6 . Suppose, instead, that we added just the reflection M_2 to the set $\{id, M_1\}$. The resulting set would not be a subgroup unless we also added ρ_1 , because $M_1 \circ M_2 = \rho_1$. But then we would also have to add the other rotation and the other reflection. Either way, the resulting set would be all of D_6 . The conclusion is that there is no subgroup between $\langle\{id, M_1\}, \circ\rangle$ and $\langle D_6, \circ\rangle$. Similarly, there is no subgroup between $\langle\{id, M_2\}, \circ\rangle$ and $\langle D_6, \circ\rangle$, and there is not one between $\langle\{id, M_3\}, \circ\rangle$ and $\langle D_6, \circ\rangle$. Therefore, we can draw line segments from each of the subgroups $\langle\{id, M_1\}, \circ\rangle$, $\langle\{id, M_2\}, \circ\rangle$ and $\langle\{id, M_3\}, \circ\rangle$ upward to $\langle D_6, \circ\rangle$.

Our subgroup lattice now looks like the drawing to the right. And we realize that we are done! That is, our consideration of the various subgroups has been thorough enough to convince ourselves that we have indeed found all of the subgroups of $\langle D_6, \circ\rangle$, and we have figured out exactly how they should be related on the subgroup lattice diagram.



5.3. The subgroup generated by a subset

In our study of the subgroups of the group $\langle D_6, \circ \rangle$ in the previous section, we repeatedly considered subsets of the set D_6 , asking whether or not a given subset was in fact a subgroup. If the subset was not a subgroup, we sometimes considered what elements would have to be added to the subset in order to make it a subgroup. For example, we saw that the subset $\{id, \rho_2\}$ was not a subgroup, but if we added the element ρ_1 , then the resulting subset $\{id, \rho_1, \rho_2\}$ was a subgroup. We also saw that the subset $\{id, M_1, \rho_1\}$ was not a subgroup, and that the only way to turn it into a subgroup by adding elements to it was to add all the remaining elements of the group D_6 .

This notion of considering enlarging subsets that are not subgroups to obtain subsets that are subgroups is a useful tool when studying groups. The tool is used so much that is given a precise definition, as follows.

Definition 25 The closure of a subset

- Symbol: \bar{A}
- Spoken: “The closure of A ”
- Usage: There is some group $\langle G, * \rangle$ in use, and A is a subset of G . That is, $A \subset G$. But A may or may not be a subgroup of G .
- Meaning in symbols: \bar{A} is the smallest set such that A is a subset of \bar{A} and \bar{A} is a subgroup of G .
- Meaning in words: \bar{A} is the smallest set such that $A \subset \bar{A}$ and $\langle \bar{A}, * \rangle < \langle G, * \rangle$.

Example: In the group $\langle D_6, \circ \rangle$, we would say that $\overline{\{id, \rho_2\}} = \{id, \rho_1, \rho_2\}$, and we would say that $\overline{\{id, M_1, \rho_1\}} = D_6$. Also note that $\overline{\{id, \rho_1, \rho_2\}} = \{id, \rho_1, \rho_2\}$, illustrating that the closure of a subset can be the same as the subset.

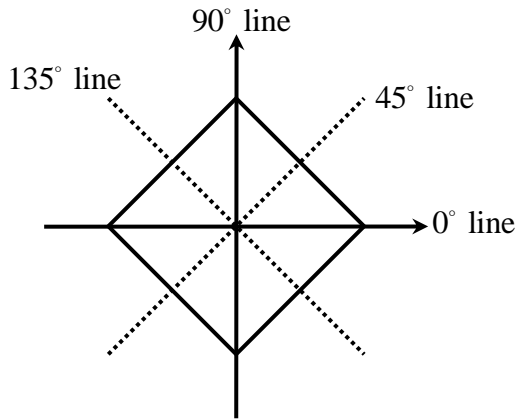
Definition 26 The subgroup generated by a subset

- Words: “The subgroup generated by A ”
- Usage: There is some group $\langle G, * \rangle$ in use, and A is a subset of G . That is, $A \subset G$. But A may or may not be a subgroup of G .
- Meaning in symbols: $\langle \bar{A}, * \rangle$
- Meaning in words: The subgroup generated by a subset A is the smallest subgroup that contains set A . In other words, it is just the set that is the closure of set A , together with the group operation, considered as a subgroup of the group.

Example: In the group $\langle D_6, \circ \rangle$, the subgroup generated by the subset $\{id, \rho_2\}$ is $\langle \overline{\{id, \rho_2\}}, * \rangle$, which is just the subgroup $\langle \{id, \rho_1, \rho_2\}, * \rangle$.

5.4. Exercises

[1] In this exercise, you will explore the *dihedral group with eight elements*, D_8 . This is the group of symmetries of a square. If we orient the square with its center at the origin and one of the vertices lying on the positive x -axis as shown in the figure below, then the elements of the group are as shown in the list to the right.



Elements of the group D_8

$$\rho_0 = \text{identity} = e$$

$$\rho_1 = \text{counterclockwise rotation through } 90^\circ$$

$$\rho_2 = \text{counterclockwise rotation through } 180^\circ$$

$$\rho_3 = \text{counterclockwise rotation through } 270^\circ$$

$$M_1 = \text{flip across the } 0^\circ \text{ line}$$

$$M_2 = \text{flip across the } 45^\circ \text{ line}$$

$$M_3 = \text{flip across the } 90^\circ \text{ line}$$

$$M_4 = \text{flip across the } 135^\circ \text{ line}$$

(In the figure above, you should think of the degree lines as being fixed to the table, while the square is the thing that gets rotated and flipped. For instance, the 0° line is always horizontal, and the 45° line always goes from lower left to upper right, as shown.)

(a) Fill out the group table below.

\circ	id	ρ_1	ρ_2	ρ_3	M_1	M_2	M_3	M_4
id								
ρ_1								
ρ_2								
ρ_3								
M_1								
M_2								
M_3								
M_4								

(b) Fill out the table below showing the list of powers of each element.

element	list of powers of that element
id	
ρ_1	
ρ_2	
ρ_3	
M_1	
M_2	
M_3	
M_4	

(c) What is $\overline{\{\rho_1\}}$?

(d) What is $\overline{\{\rho_2\}}$?

(e) What is $\overline{\{\rho_1, M_1\}}$?

(f) What is $\overline{\{\rho_2, M_1\}}$?

(g) Make a subgroup lattice diagram for the group D_8 .

Hint: The results of part (e) and (f) show that it will not be enough to simply consider the subgroups generated by single elements of the group. In order to find all of the subgroups, you will need to consider subgroups generated by various subsets.