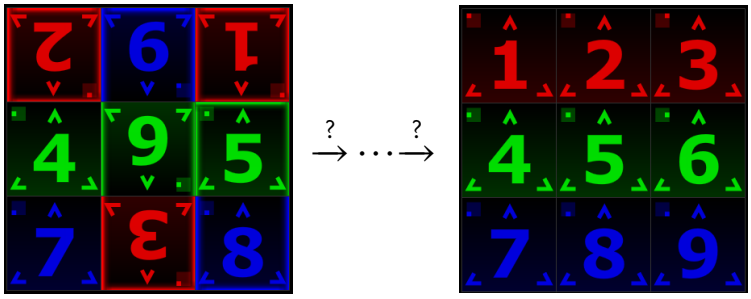
# Chapter 2

# An Introduction to Groups

One of the major topics of this course is **groups**. The area of mathematics that is concerned with groups is called **group theory**. Loosely speaking, group theory is the study of symmetry, and in my opinion is one of the most beautiful areas in all of mathematics. It arises in puzzles, visual arts, music, nature, the physical and life sciences, computer science, cryptography, and of course, throughout mathematics.

## 2.1 A First Example

Let's begin our study by developing some intuition about what groups actually are. To get started, we will explore the game Spinpossible$^{TM}$, which used to be available for iOS and Android devices*. The game is played on a $3 \times 3$ board of scrambled tiles numbered 1 to 9, each of which may be right-side-up or up-side-down. The objective of the game is to return the board to the standard configuration where tiles are arranged in numerical order and right-side-up. This is accomplished by a sequence of "spins", where a spin consists of rotating an $m \times n$ subrectangle by 180°. The goal is to minimize the number of spins used. The following figure depicts a scrambled board on the left and the solved board on the right. The sequence of arrows is used to denote some sequence of spins that transforms the scrambled board into the solved board.




Let's play with an example. Suppose we start with the following scrambled board.

*If you'd like to play the game, try going here: https://www.kongregate.com/games/spinpossible.

| | | |
|---|---|---|
| 2 | 6 | 1 |
| 4 | 9 | 5 |
| 7 | 3 | 8 |

The underlines on the numbers are meant to help us tell whether a tile is right-side-up or up-side-down. Our goal is to use a sequence of spins to unscramble the board. Before we get started, let's agree on some conventions. When we refer to *tile n*, we mean the actual tile that is labeled by the number $n$ regardless of its position and orientation on the board. On the other hand, *position n* will refer to the position on the board that tile $n$ is supposed to be in when the board has been unscrambled. For example, in the board above, tile 1 is in position 3 and tile 7 happens to be in position 7.

It turns out that there are multiple ways to unscramble this board, but I have one particular sequence in mind. First, let's spin the rectangle determined by the two rightmost columns. Here's what we get. I've shaded the subrectangle that we are spinning.

| | | |
|---|---|---|
| 2 | 6 | 1 |
| 4 | 9 | 5 |
| 7 | 3 | 8 |

$\rightarrow$

| | | |
|---|---|---|
| 2 | 8 | 3 |
| 4 | 5 | 6 |
| 7 | 1 | 9 |

Okay, now let's spin the middle column.

| | | |
|---|---|---|
| 2 | 8 | 3 |
| 4 | 5 | 6 |
| 7 | 1 | 9 |

$\rightarrow$

| | | |
|---|---|---|
| 2 | 1 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

Hopefully, you can see that we are really close to unscrambling the board. All we need to do is spin the rectangle determined by the tiles in positions 1 and 2.

| | | |
|---|---|---|
| 2 | 1 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

$\rightarrow$

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

Putting all of our moves together, here is what we have.

| | | |
|---|---|---|
| 2 | 6 | 1 |
| 4 | 9 | 5 |
| 7 | 3 | 8 |

$\rightarrow$

| | | |
|---|---|---|
| 2 | 8 | 3 |
| 4 | 5 | 6 |
| 7 | 1 | 9 |

$\rightarrow$

| | | |
|---|---|---|
| 2 | 1 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

$\rightarrow$

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

In this case, we were able to solve the scrambled board in 3 moves. It's not immediately obvious, but it turns out that there is no way to unscramble the board in fewer than 3 spins. However, there is at least one other solution that involves exactly 3 spins.

**Problem 2.1.** How many scrambled $3 \times 3$ Spinpossible boards are there? To answer this question, you will need to rely on some counting principles such as factorials. In this context, we want to include the solved board as one of the scrambled boards—it's just not very scrambled.

**Problem 2.2.** How many spins are there?

It's useful to have some notation. Let $s_{ij}$ (with $i \leq j$) denote the spin that rotates the subrectangle that has position $i$ in the upper-left corner and position $j$ in the lower-right corner. As an example, the sequence of spins that we used above to unscramble our initial scrambled board is

$$s_{29} \to s_{28} \to s_{12}.$$

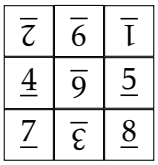
As you noticed in Problem 2.2, we can also rotate a single tile. Every spin of the form $s_{ii}$ is called a *toggle*. For example, $s_{44}$ toggles the tile in position 4.

We can think of each spin as a function and since we are doing spins on top of spins, every sequence of spins corresponds to a composition of functions. We will follow the standard convention of function composition that says the function on the right goes first. In this case, our previous sequence of spins becomes $s_{12} \circ s_{28} \circ s_{29}$, which we abbreviate as $s_{12}s_{28}s_{29}$. This might take some getting used to, but just remember that it is just like function notation—stuff on the right goes first. We will refer to expressions like $s_{12}s_{28}s_{29}$ as **words** in the alphabet $\{s_{ij} \mid i \leq j\}$. Our words will always consist of a finite number of spins.

Every word consisting of spins corresponds to a function that takes a scrambled board as input and returns a scrambled board. We say that the words "act on" the scrambled boards. For each word, there is an associated net action. For example, the word $s_{12}s_{23}s_{12}$ corresponds to swapping the positions but not orientation of the tiles in positions 1 and 3. You should take the time to verify this for yourself. Sometimes it is difficult to describe what the net action associated to a word is, but there is always some corresponding net action nonetheless.

It is worth pointing out that $s_{12}s_{23}s_{12}$ is not itself a spin. However, sometimes a composition of spins will yield a spin. For example, the net action of $s_{12}s_{11}s_{12}$ is toggling the tile in position 2. That is, $s_{12}s_{11}s_{12}$ and $s_{22}$ are two different words that correspond to the same net action. In this case, we write $s_{12}s_{11}s_{12} = s_{22}$, where the equality is referring to the net action as opposed to the words themselves. The previous example illustrates that multiple words may represent the same net action.

**Problem 2.3.** Find a sequence of 3 spins that is different from the one we described earlier that unscrambles the following board. Write your answer as a word consisting of spins.



**Problem 2.4.** What is the net action that corresponds to the word $s_{23}s_{12}s_{23}$? What can you conclude about $s_{23}s_{12}s_{23}$ compared to $s_{12}s_{23}s_{12}$?

We can also use exponents to abbreviate. For example, $s_{23}^2$ is the same as $s_{23}s_{23}$ (which in this case is the net action of doing nothing) and $(s_{12}s_{23})^2$ is the same as $s_{12}s_{23}s_{12}s_{23}$.

**Problem 2.5.** It turns out that there is an even simpler word (i.e., a shorter word) that yields the same net action as $(s_{12}s_{23})^2$. Can you find one?

Define $\text{Spin}_{3\times3}$ to be the collection of net actions that we can obtain from words consisting of spins. We say that the set of spins **generates** $\text{Spin}_{3\times3}$ and we refer to the set of spins as a **generating set** for $\text{Spin}_{3\times3}$.

**Problem 2.6.** Suppose $s_{x_1}s_{x_2}\cdots s_{x_n}$ and $s_{y_1}s_{y_2}\cdots s_{y_m}$ are both words consisting of spins. Then the corresponding net actions, say $u$ and $v$, respectively, are elements of $\text{Spin}_{3\times3}$. Prove that the composition of the actions $u$ and $v$ is an element of $\text{Spin}_{3\times3}$.

The previous problem tells us that the composition of two net actions from $\text{Spin}_{3\times3}$ results in another net action in $\text{Spin}_{3\times3}$. Formally, we say that $\text{Spin}_{3\times3}$ is **closed** under composition.

It is clear that we can construct an infinite number of words consisting of spins, but since there are a finite number of ways to rearrange the positions and orientations of the tiles of the $3\times3$ board, there are only a finite number of net actions arising from these words. That is, $\text{Spin}_{3\times3}$ is a finite set of functions.

**Problem 2.7.** Verify that $\text{Spin}_{3\times3}$ contains an **identity** function, i.e., a function whose net action is "do nothing." What happens if we compose a net action from $\text{Spin}_{3\times3}$ with the identity?

A natural question to ask is whether every possible scrambled Spinpossible board can be unscrambled using only spins. In other words, is $\text{Spin}_{3\times3}$ sufficient to unscramble every scrambled board? It turns out that the answer is yes.

**Problem 2.8.** Verify that $\text{Spin}_{3\times3}$ is sufficient to unscramble every scrambled board by describing an algorithm that will always unscramble a scrambled board. It does not matter whether your algorithm is efficient. That is, we don't care how many steps it takes to unscramble the board as long as it works in a finite number of steps. Using your algorithm, what is the maximum number of spins required to unscramble any scrambled board?

In a 2011 paper, Alex Sutherland and Andrew Sutherland (a father and son team) present a number of interesting results about Spinpossible and list a few open problems. You can find the paper at http://arxiv.org/abs/1110.6645. As a side note, Alex is one of the developers of the game and his father, Andrew, is a mathematics professor at MIT. Using a brute-force computer algorithm, the Sutherlands verified that every scrambled $3\times3$ Spinpossible board can be solved in at most 9 moves. However, a human readable mathematical proof of this fact remains elusive. By the way, mathematics is chock full of open problems and you can often get to the frontier of what is currently known without too much trouble. Mathematicians are in the business of solving open problems.

Instead of unscrambling boards, we can act on the solved board with an action from $\text{Spin}_{3\times3}$ to obtain a scrambled board. Problem 2.8 tells us that we can use $\text{Spin}_{3\times3}$ to get from the solved board to any scrambled board. In fact, starting with the solved board makes it clear that there is a one-to-one correspondence between net actions and scrambled boards.

**Problem 2.9.** What is the size of $\text{Spin}_{3\times3}$? That is, how many net actions are in $\text{Spin}_{3\times3}$?

Let's make a couple more observations. First, every spin is reversible. That is, every spin has an **inverse**. In the case of Spinpossible, we can just apply the same spin again to undo it. For example, $s_{12}^2$ is the same as doing nothing. This means that the inverse of $s_{12}$, denoted $s_{12}^{-1}$, is $s_{12}$ itself. Symbolically, we write $s_{12}^{-1} = s_{12}$. Remember that we are exploring the game Spinpossible—it won't always be the case that repeating an action will reverse the action.

In the same vein, every sequence of spins is reversible. For example, if we apply $s_{12}s_{23}$ (i.e., do $s_{23}$ first followed by $s_{12}$), we could undo the net action by applying $s_{23}s_{12}$ because

$$(s_{12}s_{23})^{-1} = s_{23}^{-1}s_{12}^{-1} = s_{23}s_{12}$$

since $s_{23}^{-1} = s_{23}$ and $s_{12}^{-1} = s_{12}$. Notice that the first equality is an instantiation of the "socks and shoes theorem", which states that if $f$ and $g$ are functions with compatible domain and codomain, then

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

The upshot is that the net action that corresponds to a word consisting of spins can be reversed by applying "socks and shoes" and is itself an action.

**Problem 2.10.** Imagine we started with the solved board and then you scrambled the board according to some word consisting of spins. Let's call this word $w$. How could you obtain the solved board from the scrambled board determined by $w$? How is this related to $w^{-1}$?

There is one detail we have been sweeping under the rug. Notice that every time we wrote down a word consisting of two or more spins, we didn't bother to group pairs of adjacent spins using parentheses. Recall that the composition of functions with compatible domains and codomains is **associative** (see Theorem 2.29). That is, if $f$, $g$, and $h$ are functions with compatible domains and codomains, then

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

Since composition of spins is really just function composition, composition of spins is also associative. And since the spins generate $\text{Spin}_{3\times3}$, the composition of net actions from $\text{Spin}_{3\times3}$ is associative, as well.

**Problem 2.11.** Does the order in which you apply spins matter? Does it always matter? Let's be as specific as possible. If the order in which we apply two spins does not matter, then we say that the spins **commute**. However, if the order does matter, then the spins do not commute. When will two spins commute? When will they not commute? Provide some specific examples.

In the previous problem, you discovered that the composition of two spins may or may not commute. Since the spins generate $\text{Spin}_{3\times3}$, the composition of two net actions may or may not commute. We say that $\text{Spin}_{3\times3}$ is not commutative.

Let's collect our key observations about $\text{Spin}_{3\times3}$.

(1) **Generating Set:** The set of spins generates $\text{Spin}_{3\times3}$. That is, every net action from $\text{Spin}_{3\times3}$ corresponds to a word consisting of spins.[†]

(2) **Closure:** The composition of any two net actions from $\text{Spin}_{3\times3}$ results in a net action from $\text{Spin}_{3\times3}$.

(3) **Associative:** The composition of net actions from $\text{Spin}_{3\times3}$ is associative.

(4) **Identity:** There is an identity in $\text{Spin}_{3\times3}$ whose corresponding net action is "do nothing".

(5) **Inverses:** Every net action from $\text{Spin}_{3\times3}$ has an inverse net action in $\text{Spin}_{3\times3}$. Composing a net action and its inverse results in the identity.

(6) The composition of two net actions from $\text{Spin}_{3\times3}$ may or may not commute.

It turns out that $\text{Spin}_{3\times3}$ is an example of a group. Loosely speaking, a **group** is a set together with a method for combining two elements together that satisfies conditions (2), (3), (4), and (5) above. More formally, a group is a nonempty set together with an associative binary operation such that the set contains an identity element and every element in the set has an inverse that is also in the set. As we shall see, groups can have a variety of generating sets, possibly of different sizes. Also, some groups are commutative and some groups are not.

Before closing out this section, let's tackle a few more interesting problems concerning Spinpossible. We say that a generating set $S$ for a group is a **minimal generating set** if $S \setminus \{x\}$ is no longer a generating set for the group for all $x \in S$.

**Problem 2.12.** Determine whether the set of spins is a minimal generating set for $\text{Spin}_{3\times3}$.

It's not too difficult to prove—but we will omit the details—that we can generate $\text{Spin}_{3\times3}$ with the following subset of 9 spins:

$$T = \{s_{11}, s_{12}, s_{23}, s_{36}, s_{56}, s_{45}, s_{47}, s_{78}, s_{89}\}.$$

That is, every net action in $\text{Spin}_{3\times3}$ corresponds to a word consisting of the spins from $T$. Try to take a moment to convince yourself that this is at least plausible.

**Problem 2.13.** For each of the following spins, find a word consisting of spins from the set $T$ that yields the same net action.

(a) $s_{33}$

(b) $s_{13}$

(c) $s_{14}$

**Problem 2.14.** Taking for granted that $T$ is a generating set for $\text{Spin}_{3\times3}$, determine whether $T$ is a minimal generating set.

[†]The case of Spinpossible is a little misleading. Since each spin is its own inverse, we never need to write words consisting of spins with inverses. However, as we shall see later, there are situations outside the context of Spinpossible where we will need to utilize inverses of elements from a generating set.

## 2.2 Binary Operations

Before beginning our formal study of groups, we need have an understanding of binary operations. After learning to count as a child, you likely learned how to add, subtract, multiply, and divide with natural numbers. As long as we avoid division by zero, these operations are examples of binary operations since we are combining two objects to obtain a single object. More formally, we have the following definition.

**Definition 2.15.** A **binary operation** $*$ on a set $A$ is a function from $A \times A$ into $A$. For each $(a, b) \in A \times A$, we denote the element $*(a, b)$ via $a * b$. If the context is clear, we may abbreviate $a * b$ as $ab$.

Don't misunderstand the use of $*$ in this context. We are not implying that $*$ is the ordinary multiplication of real numbers that you are familiar with. We use $*$ to represent a generic binary operation.

Notice that since the codomain of a binary operation on a set $A$ is $A$, binary operations require that we yield an element of $A$ when combining two elements of $A$. In this case, we say that $A$ is **closed** under $*$. Binary operations have this closure property by definition. Also, since binary operations are functions, any attempt to combine two elements from $A$ should result in a *unique* element of $A$. In this case, we say that $*$ is **well-defined**. Moreover, since the domain of $*$ is $A \times A$, it must be the case that $*$ is defined for *all* pairs of elements from $A$.

**Example 2.16.** Here are some examples of binary operations.

(a) The operations of $+$ (addition), $-$ (subtraction), and $\cdot$ (multiplication) are binary operations on the real numbers. All three are also binary operations on the integers. However, while $+$ and $\cdot$ are both binary operations on the set of natural numbers, $-$ is not a binary operation on the natural numbers since $1 - 2 = -1$, which is not a natural number.

(b) The operation of $\div$ (division) is not a binary operation on the set of real numbers because all elements of the form $(a, 0)$ are not in the domain $\mathbb{R} \times \mathbb{R}$ since we cannot divide by 0. Yet, $\div$ is a suitable binary operation on $\mathbb{R} \setminus \{0\}$.

(c) Let $A$ be a nonempty set and let $F$ be the set of functions from $A$ to $A$. Then $\circ$ (function composition) is a binary operation on $F$. We utilized this fact when exploring the game Spinpossible.

(d) Let $M_{2\times 2}(\mathbb{R})$ be the set of $2 \times 2$ matrices with real number entries. Then matrix multiplication is a binary operation on $M_{2\times 2}(\mathbb{R})$.

**Problem 2.17.** Let $M(\mathbb{R})$ be the set of matrices (of any size) with real number entries. Is matrix addition a binary operation on $M(\mathbb{R})$? How about matrix multiplication? What if you restrict to square matrices of a fixed size $n \times n$?

**Problem 2.18.** Let $A$ be a set. Determine whether $\cup$ (union) and $\cap$ (intersection) are binary operations on $\mathcal{P}(A)$ (i.e., the power set of $A$).

**Problem 2.19.** Consider the closed interval $[0,1]$ and define $*$ on $[0,1]$ via $a*b = \min\{a,b\}$ (i.e., take the minimum of $a$ and $b$). Determine whether $*$ is a binary operation on $[0,1]$.

**Problem 2.20.** Consider a square puzzle piece that fits perfectly into a square hole. Let $R_4$ be the set of net actions consisting of the rotations of the square by an appropriate amount so that it fits back into the hole. Assume we can tell the corners of the square apart from each other so that if the square has been rotated and put back in the hole we can notice the difference. Each net action is called a **symmetry** of the square.

(a) Describe all of the distinct symmetries in $R_4$. How many distinct symmetries are in $R_4$?

(b) Is composition of symmetries a binary operation on $R_4$?

The set $R_4$ is called the rotation group for the square. For $n \geq 3$, $R_n$ is the **rotation group** for the regular $n$-gon and consists of the rotational symmetries for a regular $n$-gon. As we shall see later, every $R_n$ really is a group under composition of symmetries.

**Problem 2.21.** Consider a puzzle piece like the one in the previous problem, except this time, let's assume that the piece and the hole are an equilateral triangle. Let $D_3$ be the full set of symmetries that allow the triangle to fit back in the hole. In addition to rotations, we will also allow the triangle to be flipped over—called a reflection.

(a) Describe all of the distinct symmetries in $D_3$. How many distinct symmetries are in $D_3$?

(b) Is composition of symmetries a binary operation on $D_3$?

**Problem 2.22.** Repeat the above problem, but do it for a square instead of a triangle. The corresponding set is called $D_4$.

The sets $D_3$ and $D_4$ are examples of dihedral groups. In general, for $n \geq 3$, $D_n$ consists of the symmetries (rotations and reflections) of a regular $n$-gon and is called the **dihedral group of order** $2n$. In this case, the word "order" simply means the number of symmetries in the set. Do you see why $D_n$ consists of $2n$ actions? As expected, we will prove that every $D_n$ really is a group.

**Problem 2.23.** Consider the set $S_3$ consisting of the net actions that permute the positions of three coins (without flipping them over) that are sitting side by side in a line. Assume that you can tell the coins apart.

(a) Write down all distinct net actions in $S_3$ using verbal descriptions. Some of these will be tricky to describe. How many distinct net actions are in $S_3$?

(b) Is composition of net actions a binary operation on $S_3$?

The set $S_3$ is an example of a symmetric group. In general, $S_n$ is the **symmetric group on** $n$ **objects** and consists of the net actions that rearrange the $n$ objects. Such rearrangements are called **permutations**. Later we will prove that each $S_n$ is a group under composition of permutations.

**Problem 2.24.** Explain why composition of spins is not a binary operation on the set of spins in $\text{Spin}_{3\times 3}$.

Some binary operations have additional properties.

**Definition 2.25.** Let $A$ be a nonempty set and let $*$ be a binary operation on $A$.

(a) We say that $*$ is **associative** if and only if $(a*b)*c = a*(b*c)$ for all $a,b,c \in A$.

(b) We say that $*$ is **commutative** if and only if $a*b = b*a$ for all $a,b \in A$.

**Problem 2.26.** Provide an example of each of the following.

(a) A binary operation on a set that is commutative.

(b) A binary operation on a set that is not commutative.

**Problem 2.27.** Provide an example of a set $A$ and a binary operation $*$ on $A$ such that $(a*b)^2 \neq a^2*b^2$ for some $a,b \in A$. Under what conditions will $(a*b)^2 = a^2*b^2$ for all $a,b \in A$? *Note:* The notation $x^2$ is shorthand for $x*x$.

**Problem 2.28.** Define the binary operation $*$ on $\mathbb{R}$ via $a*b = 1+ab$. In this case, $ab$ denotes the multiplication of the real numbers $a$ and $b$. Determine whether $*$ is associative on $\mathbb{R}$.

**Theorem 2.29.** Let $A$ be a nonempty set and let $F$ be the set of functions from $A$ to $A$. Then function composition is an associative binary operation on $F$.

When the set $A$ is finite, we can represent a binary operation on $A$ using a table in which the elements of the set are listed across the top and down the left side (in the same order). The entry in the $i$th row and $j$th column of the table represents the output of combining the element that labels the $i$th row with the element that labels the $j$th column (order matters).

**Example 2.30.** Consider the following table.

| $*$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $b$ | $c$ | $b$ |
| $b$ | $a$ | $c$ | $b$ |
| $c$ | $c$ | $b$ | $a$ |

This table represents a binary operation on the set $A = \{a,b,c\}$. In this case, $a*b = c$ while $b*a = a$. This shows that $*$ is not commutative.

**Problem 2.31.** Consider the following table that displays the binary operation $*$ on the set $\{x,y,z\}$.

| $*$ | $x$ | $y$ | $z$ |
|---|---|---|---|
| $x$ | $x$ | $y$ | $z$ |
| $y$ | $y$ | $x$ | $x$ |
| $z$ | $y$ | $x$ | $x$ |

(a) Determine whether $*$ is commutative.

(b) Determine whether $*$ is associative.

**Problem 2.32.** What property must the table for a binary operation have in order for the operation to be commutative?

## 2.3 Groups

Without further ado, here is our official definition of a group.

**Definition 2.33.** A **group** $(G,*)$ is a set $G$ together with a binary operation $*$ such that the following axioms hold.

(0) The set $G$ is closed under $*$.

(1) The operation $*$ is associative.

(2) There is an element $e \in G$ such that for all $g \in G$, $e*g = g*e = g$. We call $e$ the **identity**.

(3) Corresponding to each $g \in G$, there is an element $g' \in G$ such that $g*g' = g'*g = e$. In this case, $g'$ is called the **inverse** of $g$, which we shall denote as $g^{-1}$.

The **order** of $G$, denoted $|G|$, is the cardinality of the set $G$. If $|G|$ is finite, then we say that $G$ has finite order. Otherwise, we say that $G$ has infinite order.

In the definition of a group, the binary operation $*$ is not required to be commutative. If $*$ is commutative, then we say that $G$ is **abelian**. Commutative groups are called abelian in honor of the Norwegian mathematician Niels Abel (1802–1829). A few additional comments are in order.

- Axiom 2 forces $G$ to be nonempty.
- If $(G,*)$ is a group, then we say that $G$ **is a group under** $*$.
- We refer to $a*b$ as the **product** of $a$ and $b$ even if $*$ is not actually multiplication.
- For simplicity, if $(G,*)$ is a group, we will often refer to $G$ as being the group and suppress any mention of $*$ whatsoever. In particular, we will often abbreviate $a*b$ as $ab$.

**Problem 2.34.** Explain why Axiom 0 is unnecessary.

**Problem 2.35.** Verify that each of the following is a group under composition of actions and determine the order. Which of the groups are abelian?

(a) $\mathrm{Spin}_{3\times 3}$

(b) $R_4$ (see Problem 2.20)

(c) $D_3$ (see Problem 2.21)

(d) $D_4$ (see Problem 2.22)

(e) $S_3$ (see Problem 2.23)

**Problem 2.36.** Determine whether each of the following is a group. If the pair is a group, determine the order, identify the identity, describe the inverses, and determine whether the group is abelian. If the pair is not a group, explain why.

(a) $(\mathbb{Z}, +)$

(b) $(\mathbb{N}, +)$

(c) $(\mathbb{Z}, \cdot)$

(d) $(\mathbb{R}, +)$

(e) $(\mathbb{R}, \cdot)$

(f) $(\mathbb{R} \setminus \{0\}, \cdot)$

(g) $(M_{2\times 2}(\mathbb{R}), +)$

(h) $(M_{2\times 2}(\mathbb{R}), *)$, where $*$ is matrix multiplication.

(i) $(\{a, b, c\}, *)$, where $*$ is the operation determined by the table in Example 5.15.

(j) $(\{x, y, z\}, *)$, where $*$ is the operation determined by the table in Problem 2.31.

Notice that in Axiom 2 of Definition 5.18, we said *the* identity and not *an* identity. Implicitly, this implies that the identity is unique.

**Theorem 2.37.** If $G$ is a group, then there is a unique identity element in $G$. That is, there is only one element $e \in G$ such that $ge = eg = g$ for all $g \in G$.

**Problem 2.38.** Provide an example of a group of order 1. Can you find more than one such group?

Any group of order 1 is called a **trivial group**. It follows immediately from the definition of a group that the element of a trivial group must be the identity.

The following theorem is crucial for proving many theorems about groups.

**Theorem 2.39** (Cancellation Law)**.** Let $G$ be a group and let $g, x, y \in G$. Then $gx = gy$ if and only if $x = y$. Similarly, $xg = yg$ if and only if $x = y$.[‡]

**Problem 2.40.** Show that $(\mathbb{R}, \cdot)$ fails the Cancellation Law confirming the fact that it is not a group.

**Corollary 2.41.** If $G$ is a group, then each $g \in G$ has a unique inverse.

**Theorem 2.42.** If $G$ is a group, then for all $g, h \in G$, the equations $gx = h$ and $yg = h$ have unique solutions for $x$ and $y$ in $G$.

[‡]You only need to prove one of these statements as the proof of the other is similar.

While proving the previous few theorems, hopefully one of the things you realized is that you can multiply both sides of a group equation by the same element but that you have to do it on the same side of each half. That is, since a group may or may not be abelian, if we multiply one side of an equation on the left by a group element, then we must multiply the other side of the equation on the left by the same group element.

Despite the fact that a group may or may not be abelian, if one product is equal to the identity, then reversing the order yields the same result.

**Theorem 2.43.** If $G$ is a group and $g, h \in G$ such that $gh = e$, then $hg = e$.

The upshot of the previous theorem is if we have a "left inverse" then we automatically have a "right inverse" (and vice versa). The next theorem should not be surprising.

**Theorem 2.44.** If $G$ is a group, then $(g^{-1})^{-1} = g$ for all $g \in G$.

The next theorem is analogous to the "socks and shoes theorem" for composition of functions.

**Theorem 2.45.** If $G$ is a group, then $(gh)^{-1} = h^{-1}g^{-1}$ for all $g, h \in G$.

**Definition 2.46.** If $G$ is a group and $g \in G$, then for all $n \in \mathbb{N}$, we define:

(a) $g^n = \underbrace{gg\cdots g}_{n \text{ factors}}$

(b) $g^{-n} = \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{n \text{ factors}}$

(c) $g^0 = e$

Note that if $G$ is a group under $+$, then we can reinterpret Definition 2.46 as:

(a) $ng = \underbrace{g + g + \cdots + g}_{n \text{ summands}}$

(b) $-ng = \underbrace{-g + -g + \cdots + -g}_{n \text{ summands}}$

(c) $0g = 0$

The good news is that the rules of exponents you are familiar with still hold for groups.

**Theorem 2.47.** If $G$ is a group and $g \in G$, then for all $n, m \in \mathbb{Z}$, we have the following:

(a) $g^n * g^m = g^{n+m}$,

(b) $(g^n)^{-1} = g^{-n}$.

**Problem 2.48.** Reinterpret Theorem 2.47 if $G$ is a group under addition.

## 2.4 Generating Sets

In this section, we explore the concept of a generating set for a group.

**Definition 2.49.** Let $G$ be a group and let $S$ be a subset of $G$. A finite product (under the operation of $G$) consisting of elements from $S$ or their inverses is called a **word** in $S$. That is, a word in $S$ is of the form

$$s_{x_1} s_{x_2} \cdots s_{x_n},$$

where each $s_{x_i}$ is either an element of $S$ or the inverse of an element of $S$. Each $s_{x_i}$ is called a **letter** and the set $S$ is called the **alphabet**. By convention, the identity of $G$ can be represented by the **empty word**, which is the word having no letters. The set of elements of $G$ that can be written as words in $S$ is denoted by $\langle S \rangle$ and is called the **group generated by** $S$.

For example, if $a, b$, and $c$ are elements of a group $G$, then $ab$, $c^{-1}acc$, and $ab^{-1}caa^{-1}bc^{-1}$ are words in the set $\{a, b, c\}$. It is important to point out that two different words may be equal to the same element in $G$. We saw this happen when we studied Spinpossible in Section 2.1. For example, see Problems 2.3–2.5.

**Theorem 2.50.** If $G$ is a group under $*$ and $S$ is a subset of $G$, then $\langle S \rangle$ is also a group under $*$.

**Definition 2.51.** If $G$ is a group and $S$ is a subset of $G$ such that $G = \langle S \rangle$, then $S$ is called a **generating set** of $G$. In other words, $S$ is a generating set of $G$ if every element of $G$ can be expressed as a word in $S$. In this case, we say $S$ **generates** $G$. A generating set $S$ for $G$ is a **minimal generating set** if $S \setminus \{x\}$ is no longer a generating set for $G$ for all $x \in S$.

A generating set for a group is analogous to a spanning set for a vector space and a minimal generating set for a group is analogous to a basis for a vector space.

If we know what the elements of $S$ actually are, then we will list them inside the angle brackets without the set braces. For example, if $S = \{a, b, c\}$, then we will write $\langle a, b, c \rangle$ instead of $\langle \{a, b, c\} \rangle$. In the special case when the generating set $S$ consists of a single element, say $g$, we have

$$G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$$

and say that $G$ as a **cyclic group**. As we shall see, $\langle g \rangle$ may be finite or infinite.

**Example 2.52.** In Section 2.1, we discovered that the set of spins is a non-minimal generating set for $\text{Spin}_{3\times3}$ while the set $T = \{s_{11}, s_{12}, s_{23}, s_{36}, s_{56}, s_{45}, s_{47}, s_{78}, s_{89}\}$ is a minimal generating set.

**Problem 2.53.** Consider the rotation group $R_4$ that we introduced in Problem 2.20. Let $r$ be the element of $R_4$ that rotates the square by 90° clockwise.

(a) Describe the action of $r^{-1}$ on the square and express $r^{-1}$ as a word using $r$ only.

(b) Prove that $R_4 = \langle r \rangle$ by writing every element of $R_4$ as a word using $r$ only.

(c) Is $\{r\}$ a minimal generating set for $R_4$?

(d) Is $R_4$ a cyclic group?

**Problem 2.54.** Consider the dihedral group $D_3$ introduced in Problem 2.21. To give us a common starting point, let's assume the triangle and hole are positioned so that one of the tips of the triangle is pointed up. Let $r$ be rotation by 120° in the clockwise direction and let $s$ be the reflection in $D_3$ that fixes the top of the triangle.

(a) Describe the action of $r^{-1}$ on the triangle and express $r^{-1}$ as a word using $r$ only.

(b) Describe the action of $s^{-1}$ on the triangle and express $s^{-1}$ as a word using $s$ only.

(c) Prove that $D_3 = \langle r, s \rangle$ by writing every element of $D_3$ as a word in $r$ or $s$.

(d) Is $\{r, s\}$ a minimal generating set for $D_3$?

(e) Explain why there is no single generating set for $D_3$ consisting of a single element. This proves that $D_3$ is not cyclic.

It is important to point out that the fact that $\{r, s\}$ is a minimal generating set for $D_3$ does not imply that $D_3$ is not a cyclic group. There are examples of cyclic groups that have minimal generating sets consisting of more than one element (see Problem **??**).

**Problem 2.55.** Let's consider the group $D_3$ again. Let $s$ be the same reflection as in Problem 2.54 and let $s'$ be the reflection in $D_3$ that fixes the bottom right corner of the triangle.

(a) Express $r$ as a word in $s$ and $s'$.

(b) Use part (a) together with Problem 2.54 to prove that $\langle s, s' \rangle = D_3$.

**Problem 2.56.** Consider the dihedral group $D_4$ introduced in Problem 2.22. Let $r$ be clockwise rotation by 90° and let $s$ be the reflection over the vertical midline of the square.

(a) Describe the action of $r^{-1}$ on the square and express $r^{-1}$ as a word using $r$ only.

(b) Describe the action of $s^{-1}$ on the square and express $s^{-1}$ as a word using $s$ only.

(c) Prove that $\{r, s\}$ is generating set for $D_4$.

(d) Is $\{r, s\}$ a minimal generating set for $D_4$?

(e) Find a different generating set for $D_4$.

(f) Is $D_4$ a cyclic group?

**Problem 2.57.** Consider the symmetric group $S_3$ that was introduced in Problem 2.23. Let $s_1$ be the action that swaps the positions of the first and second coins and let $s_2$ be the action that swaps the positions of the second and third coins. Prove that $S_3 = \langle s_1, s_2 \rangle$.

**Problem 2.58.** Consider the symmetric group $S_2$ that consists of the permutations of two coins that are sitting side by side.

(a) What is the order of $S_2$?