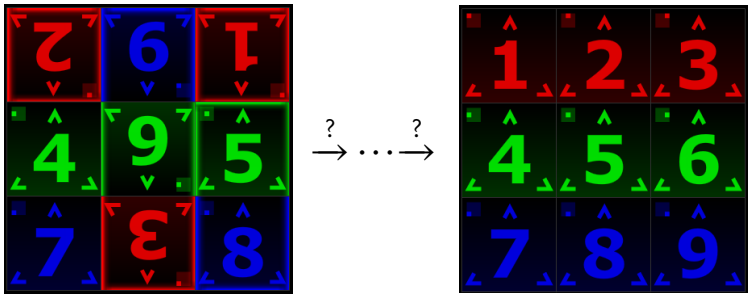
Chapter 2

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™, which used to be available for iOS and Android devices*. The game is played on a 3×3 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 3×3 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} 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.

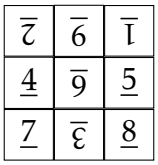
Every word consisting of spins corresponds to a function that takes a scrambled board as input and returns a scrambled board. We say that the words "act on" the scrambled boards. For each word, there is an associated **net action**. For example, the word $s_{12}s_{23}s_{12}$ corresponds to swapping the positions but not orientation of the tiles in positions 1 and 3. You should take the time to verify this for yourself. Notice that the net action does not depend on the current configuration of the board. Sometimes it is difficult to describe what the net action associated to a word is, but there is always some corresponding net action nonetheless. Moreover, each net action has many—infinitely many, in fact—words that determine that net action. For example, it turns out that $s_{12}s_{23}s_{12}$, $s_{23}s_{12}s_{23}$, and $s_{12}s_{23}s_{11}s_{11}s_{12}$ all yield the same net action. In this case, we would write

$$s_{12}s_{23}s_{12} = s_{23}s_{12}s_{23} = s_{12}s_{23}s_{11}s_{11}s_{12}.$$

Notice that equality here is referring to net action and not the words themselves. That is, the words are different, but the result is the same.

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, $s_{12}s_{11}s_{12} = s_{22}$.

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 3×3 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 3×3 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}

[†]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.

(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.

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 real 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. 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 $M_{2\times2}(\mathbb{R})$ be the set of 2×2 matrices with real number entries. Then matrix multiplication is a binary operation on $M_{2\times2}(\mathbb{R})$.

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?

Let's pause for a moment to make sure we understand our use of the word symmetry in this context. A fundamental question in mathematics is "When are two things the same?", where "things" can be whatever mathematical notion we happen to be thinking about at a particular moment. Right now we need to answer, "When do we want to consider two symmetries to be the same?" To be clear, this is a choice, and different choices can lead to different, interesting, and equally valid mathematics. For symmetries, one natural thought is that symmetries are equal when they produce the same net action on the square, meaning that when applied to a square in a particular starting position, they both yield the same ending position. In general, two symmetries are equal if they produce the same net action on the object in question.

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. If A is a nonempty set and F is 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 ith row and jth column of the table represents the output of combining the element that labels the ith row with the element that labels the jth 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 said to be an **inverse** of g.

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.

[‡]The origin of using the letter e for the identity of a group appears to be due to German mathematician Heinrich Weber, who uses "einheit" (German for "unit" or "unity") and e in his *Lehrbuch der Algebra* (1896).

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**[§]. 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.
- In Theorem 2.41, we shall see that each $g \in G$ has a unique inverse. From that point on, we will denote *the* inverse of g by g^{-1}.

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) $(\mathbb{Z},\div)$

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

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

(g) $(\mathbb{Q}\setminus\{0\},\cdot)$

[§]Commutative groups are called abelian in honor of the Norwegian mathematician Niels Abel (1802–1829).

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

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

(j) $([0,1],*)$, where $a*b := \min(a,b)$

(k) $(\{a,b,c\},*)$, where $*$ is the operation determined by the table in Example 2.30.

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

Notice that in Axiom 2 of Definition 2.33, 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.

It is important to note that if we have an equation involving the product of group elements, we can still "do the same thing to both sides" and maintain equality. However, because general groups are not necessarily abelian, we have to be careful that we truly operate in the same way on each side. For example, if we have the equation $g = h$ in some group, then we also have $ag = ah$, where we "multiplied" both sides on the left by the group element a. We could not necessarily conclude that $ag = ha$, unless one pair of the elements happen to commute with each other.

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.

Recall that Axiom (3) of Definition 2.33 states that each element of a group has at least one inverse. The next theorem tells us that each element has exactly one inverse.

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

In light of the previous theorem, the unique inverse of $g \in G$ will be denoted as g^{-1}. In groups, it turns out that inverses are always "two-sided". That is, ff G is a group and $g,h \in G$ such that $gh = e$, then it must be the case that $hg = e$, as well. In this case, $g^{=1} = h$ and $h^{-1} = g$. However, there are mathematical structures where a "left inverse" exists but the "right inverse" does not.

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.

The next theorem should not be surprising.

Theorem 2.43. 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 2.44. If G is a group, then $(gh)^{-1} = h^{-1}g^{-1}$ for all $g, h \in G$.

Definition 2.45. 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) $g^0 = e$

Remark 2.46. If G is a group under $+$, then we can reinterpret Definition 2.45 as:

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

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

(c) $0g = 0$

Notice all that we have done is taken the statements of Definition 2.45, which use multiplicative notation for the group operation, and translated what they say in the case that the group operation uses additive notation.

The good news is that the many of 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) $(g^n)^{-1} = g^{-n}$,

(c) $(g^n)^m = g^{nm}$.

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

Unfortunately, there are some rules of exponents that do not apply for general groups.

Problem 2.49. Show with a specific example that for a group G we may have $(ab)^2 \neq a^2b^2$. What property would guarantee that $(ab)^2 = a^2b^2$ for all $a, b \in G$? Is the converse of your claim true?

2.4 Generating Sets

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

Definition 2.50. 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 from S or the inverse of an element from 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.

It is important to pay close attention to our notation. While S and $\langle S \rangle$ are both sets, the latter set is the set of elements we can build using letters and their inverses from S. It turns out that if S is itself a group, then $S = \langle S \rangle$. Otherwise, S is a proper subset of $\langle S \rangle$.

Example 2.51. Suppose G is a group such that $a, b, c \in G$ and let $S = \{a, b, c\}$. Then ab, $c^{-1}acc$, and $ab^{-1}caa^{-1}bc^{-1}$ are words in $\langle S \rangle$. If any one of these words is not equal to a, b, or c, then $\langle S \rangle$ is strictly larger than S.

It is worth mentioning that we are slightly abusing notation here. For nonempty $S \subset G$, we can form infinitely many words in $\langle S \rangle$, but often there are many words that represent the same group element. We can partition the collection of words in the alphabet S into equivalence classes based on which group element a word represents. Strictly speaking, each group element is an equivalence class of words. When we say two words are equal in the group, what we really mean is that both words are in the same equivalence class.

Theorem 2.52. If G is a group under $*$ and S is a subset of G, then $\langle S \rangle$ is also a group under $*$.

Definition 2.53. 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 is a **cyclic group**. As we shall see, $\langle g \rangle$ may be finite or infinite.

Example 2.54. 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 2.55. 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 2.56. 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 2.71).

Problem 2.57. Let's consider the group D_3 again. Let s be the same reflection as in Problem 2.56 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 2.56 to prove that $\langle s, s' \rangle = D_3$.

Problem 2.58. 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 2.59. 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 2.60. Find a minimal generating set for $(\mathbb{Z}, +)$. Is $\mathbb{Z}$ a cyclic group under addition?

2.5 Group Tables

Recall that we could represent a binary operation on a finite set using a table. Since groups have binary operations at their core, we can represent a finite group (i.e., a group with finitely many elements) using a table, called a **group table**. For example, the group table for D_3 is given below, where we have used $\{r, s\}$ as the generating set (see Problem 2.56).

$*$	e	r	r^2	s	sr	sr^2
e	e	r	r^2	s	sr	sr^2
r	r	r^2	e	sr^2	s	sr
r^2	r^2	e	r	sr	sr^2	s
s	s	sr	sr^2	e	r	r^2
sr	sr	sr^2	s	r^2	e	r
sr^2	sr^2	s	sr	r	r^2	e

As a reminder, our convention is that if x appears in row i and y appears in column j, then row i "times" column j will result in the element determined by xy, where as usual we follow our right to left convention. That is, xy means we apply y first and then x (as in function composition).

Given an arbitrary group G, we should probably say, "a group table for G" and not "the group table for G." The reason for this is that if we chose a different order of the elements (e.g., swap rows 1 and 4—which swaps columns 1 and 4, as well), then the table would look slightly different. Also, if we had chosen a different generating set, then the names of the elements would look different. Regardless, the table still captures the same information about the binary operation. Because every possible table for a given group conveys the same information about the architecture of the group, people may refer to any table for the group as "the" table. Regardless of the ordering of the other elements in the group, it is standard practice to list the identity first. That is, we will always put e in the top row and the leftmost column.

Problem 2.61. For each of the following groups, identify a generating set and then create the group table.

(a) R_4

(b) D_4

(c) S_3

Problem 2.62. Given the table for a group, how can you identify which elements are inverses of each other? Does this tell you anything about which element must appear in every row and column of the group table?

Let's introduce a couple of new groups.

Problem 2.63. Consider the symmetric group S_2 that consists of the net actions that permute the positions of two coins (without flipping them over) that are sitting side by side in a line. Let s be the action that swaps the positions of the two coins.

(a) Verify that $S_2 = \langle s \rangle$. What is the order of S_2?

(b) Create the group table for S_2.

(c) Is S_2 abelian?

Problem 2.64. Consider a rectangle (which may or may not be a square) oriented so that one side is parallel to the ground. Let h be the symmetry that reflects the rectangle over the horizontal midline and let v be the symmetry that reflects the rectangle over the vertical midline. Define $V_4 := \langle v, h \rangle$. This group is called the **Klein group** (or **Vierergruppe**, which is German for "four-group") after the German mathematician Felix Klein (1849–1925).

(a) Verify that $|V_4| = 4$ by describing the symmetries in the group.

(b) Create the group table for V_4.

(c) Is V_4 abelian?

(d) Is V_4 cyclic?

Perhaps you noticed when creating the tables above that each element of the group appeared exactly once in each row and column, respectively. This is true in general for groups.

Theorem 2.65. If $(G, *)$ is a finite group, then each element of G appears exactly once in each row and each column, respectively, in any group table for G.

We can also use tables to define groups. For example, consider the following table on the set $A = \{e, a, b, c\}$.

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

Is this a table for a group? First, we see that the binary operation determined by the table is closed. Second, we see that e is acting as the identity. Since every row and column has the identity element e appearing, we know that every element has an inverse (do you see why that follows?). The only thing left to check is associativity. Imagine for a moment what this entails. It's messy right?! And this is only for a group of order 4.

Thankfully, we can rely on some prior knowledge to help out with associativity. It turns out that if you look closely, the group table for V_4 looks the "same" as the table above. What do we mean by "same" here? The names for elements are different (except for e), but

the product of corresponding elements yields the corresponding result.

To see what I mean, let's color both tables with white, red, blue, and green in such a way that each element corresponds to a unique color. If we choose our colors wisely, it is easy to see that both tables have the same structure.

$\circ$	e	v	h	vh
e	e	v	h	vh
v	v	e	vh	h
h	h	vh	e	v
vh	vh	h	v	e

$\longleftrightarrow$

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

Since we already know that V_4 is a group, we know that the binary operation for V_4 is associative. This discussion verifies that $(A, *)$ is a group.

It is important to point out that if we had not chosen our colors wisely, then perhaps the colorings of the two tables would not agree. Moreover, if we had made the same color choices for elements, but then rearranged columns and rows of one table, the colorings of the two tables would not agree. This doesn't imply anything. The point is whether we *can* get the tables to match.

Problem 2.66. Is it possible to color the group table for R_4 so that it matches the coloring of V_4? Explain your answer.

2.6 Cayley Diagrams

In this section, we will introduce visual way of encoding the abstract structure of the group in terms of a specified generating set. To get started, let's tinker with an example.

Recall that in Problem 2.1, we discovered that there are a total of $2^9 \cdot 9! = 185,794,560$ possible scrambled 3×3 Spinpossible boards. Now, imagine we wanted to write a solution manual that would describe how to solve all these boards. There are many possible ways to construct such a solution manual, but here is one way.

The manual will consist of $185,794,560$ pages such that each page lists a unique scrambling of the 3×3 board. Don't forget that one of these scramblings is the solved board, which we will make page 1. Also, imagine that the book is arranged in such a way that it isn't too difficult to look up a given scrambled board. On each page below the

scrambled board is a table that lists all possible spins. Next to each spin, the table indicates whether doing that particular spin will result in a board that is either closer to being solved or farther away from being solved. In addition, the page number that corresponds to the resulting board is listed next to each spin.

In most cases, there will be many spins that take us closer to the solved board. Given a scrambled board, a solution would consist of following one possible sequence of pages through the book that takes us from the scrambled board to the solved board. There could be many such sequences. If we could construct such a solution manual, we would have an atlas or map for the game Spinpossible.

Note that even if we make a wrong turn (i.e., follow a page that takes us farther away from the solution), we can still get back on track by following page numbers that take us closer to the solved board. In fact, we can always flip back to the page we were on before taking a wrong turn. This page will be listed on our "wrong turn page" since doing the same spin twice has the net effect of doing nothing. If you were to actually do this, the number of pages we would need to visit would be longer than an optimal solution, but we'd get to the solved board nonetheless.

Let's get a little more concrete. Consider the game Spinpossible, except let's simplify it a little. Instead of playing on the 3×3 board, let's play on a 1×2 board consisting of a single row with tiles labeled 1 and 2. The rules of the game are what you would expect; we are restricted to spins involving just the tiles in positions 1 and 2 of the original board. A scrambling of the 1×2 Spinpossible board consists of any rearrangement of the tiles 1 and 2, where either of the tiles can be right-side-up or up-side-down.

Problem 2.67. Let $\text{Spin}_{1\times 2}$ denote the group of net actions that corresponds to compositions of allowable spins on the 1×2 Spinpossible board.

(a) How many scrambled boards are there for the 1×2 Spinpossible game? Write them all down. Don't forget to include the solved board.

(b) What is the order of $\text{Spin}_{1\times 2}$?

(c) Verify that $\text{Spin}_{1\times 2} = \langle s_{11}, s_{22}, s_{12} \rangle$ by writing every element as a word in s_{11}, s_{22}, or s_{12}.

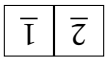
(d) Is $\{s_{11}, s_{22}, s_{12}\}$ a minimal generating set for $\text{Spin}_{1\times 2}$?

Let's try to make a map for $\text{Spin}_{1\times 2}$, but instead of writing a solution manual, we will draw a diagram of the group. The first thing we'll do is draw each of the scramblings that we found in the previous problem. It doesn't matter how we arrange all of these drawings, as long as there is some space between them. Now, for each of our 8 scrambled boards, figure out what happens when we do each of our 3 allowable spins. For each of these spins, we'll draw an arrow from the scrambled board under consideration to the resulting board. Don't worry about whether doing each of these spins is a good idea or not. In this case, each of our scrambled boards will have 3 arrows heading out towards 3 distinct boards. Do you see why?

In order for us to keep straight what each arrow represents, let's color our arrows, so that doing a particular type of spin is always the same color. For example, we could color

the arrows that toggle the tile in the first position as green. Recall that doing the same spin twice has the net effect of doing nothing, so let's just make all of our arrows point in both directions.

To make sure you are following along, consider the following scrambled board.



This board is one of our 8 possible scrambled 1×2 boards. We have three possible spins we can do to this board: toggle position 1, toggle position 2, or spin the whole board. Each of these spins has a corresponding two-way arrow that takes us to three different scrambled boards. Figure 2.1 provides a visual representation of what we just discussed.

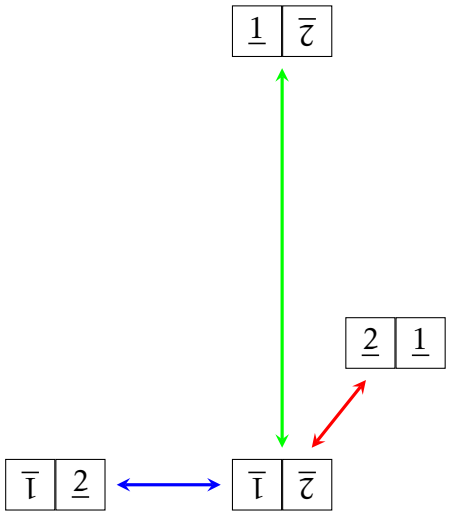


Figure 2.1

Note that I could have drawn the four scrambled boards in Figure 2.1 anywhere I wanted to, but I have a particular layout in mind. Also, notice we have three different colored arrows. In this case, a green arrow corresponds to toggling the tile in position 1 (s_{11}), a blue arrow corresponds to toggling position 2 (s_{22}), and a red arrow corresponds to spinning the whole board (s_{12}).

If we include the rest of the scrambled boards and all possible spins, we obtain Figure 2.2. Note that I've chosen a nice layout for the figure, but it's really the connections between the various boards that are important.

Ultimately, we want a diagram that conveys information about the structure of the group, so instead of labeling the vertices of the diagram for $\text{Spin}_{1\times 2}$ in Figure 2.2 with scrambled boards, we will label the vertices with the elements of the group in a way that respects the configuration of arrows. But in order to do this, we need to make a choice about how to start labeling. A natural choice to make is to label the solved board with the identity e. Then each scrambled board should be labeled by the group element that corresponds to the net action that takes us from the solved board to that scrambled board.

One way to do this is to label each vertex with the word that corresponds to a path of arrows that leads to the vertex from the vertex labeled by the identity e. Don't forget

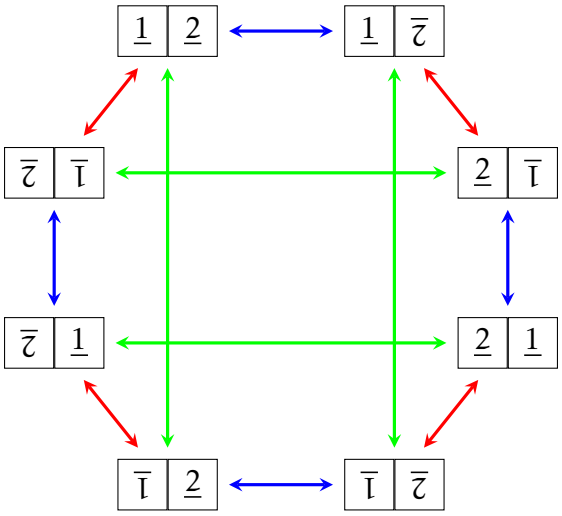
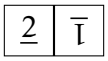


Figure 2.2

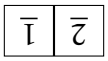
that we apply our composition of actions from right to left. This means that following a sequence of arrows out of the vertex labeled by e will get recorded as a word written right to left. That is, the first arrow out of e corresponds to the rightmost letter in the word.

For example, consider the following scrambled board.



Looking at Figure 2.2, we see that one way to get to this board from the solved board is to follow a blue arrow and then a red arrow. This corresponds to the word $s_{12}s_{22}$. However, it also corresponds to the word $s_{22}s_{12}s_{22}s_{11}$ even though this is not an optimal solution. So, we can label the board in question with either $s_{11}s_{22}$ or $s_{22}s_{12}s_{22}s_{11}$ and there are other choices, as well.

Problem 2.68. Using Figure 2.2, find three distinct words in s_{11}, s_{22}, or s_{12} that correspond to the following scrambled board.



If we continue labeling the vertices of the directed graph in Figure 2.2, then one possible labeling is given in Figure 2.3. Each word tells you how to reach the corresponding scrambled board from the solved board. The directed graph in Figure 2.3 is called the **Cayley diagram** for $\text{Spin}_{1\times 2}$ using $\{s_{11}, s_{22}, s_{12}\}$ as a generating set. It is important to point out that it will not always be the case that the arrows are two-way arrows. This happened to be the case here because each of our generators is its own inverse.

Problem 2.69. Consider the Cayley diagram for $\text{Spin}_{1\times 2}$ in Figure 2.3.

(a) Removing all the red arrows corresponds to forbidding the spin that rotates the full 1×2 board. Can we obtain all of the scrambled boards from the solved board using only blue and green arrows? What does this tell you about $\{s_{11}, s_{22}\}$?

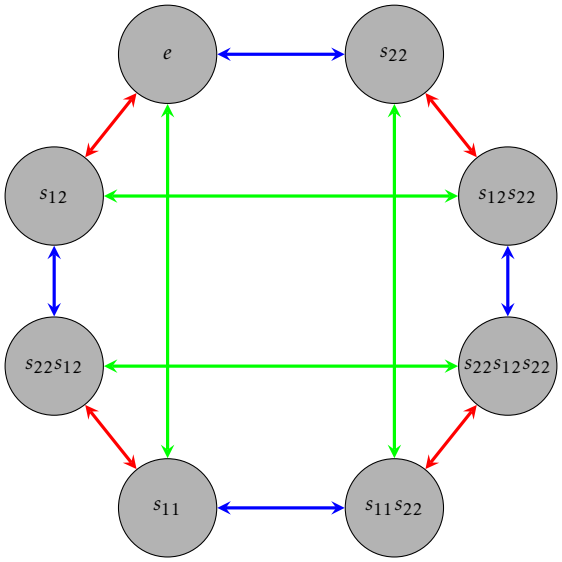


Figure 2.3. Cayley diagram for $\text{Spin}_{1\times 2}$ with generating set $\{s_{11}, s_{22}, s_{12}\}$.

(b) What if we remove the blue arrows? What does this tell you about $\{s_{11}, s_{12}\}$?

(c) What if we remove the green arrows? What does this tell you about $\{s_{22}, s_{12}\}$?

Definition 2.70. Suppose G is a group and S is a generating set of G. The **Cayley diagram**[‖] for G with generating set S is a colored directed graph constructed as follows:

(a) The vertices correspond to elements of G.

(b) Each generator $s \in S$ is assigned a color, say c_s.

(c) For $g \in G$ and $s \in S$, there is a directed edge from g to sg with color c_s.

Note that following the arrow from g to sg with color c_s corresponds to applying the action of s to g. Moreover, following the arrow backwards from sg to g corresponds to applying s^{-1} to sg. If a generator is its own inverse (like the spins in $\text{Spin}_{1\times 2}$), then the arrows corresponding to that generator are two-way arrows.

Before asking you to construct some Cayley diagrams, let's play with another example. In the next problem you will encounter a Cayley diagram where all the edges are one-way arrows.

Problem 2.71. Let R_6 denote the group of rotational symmetries of a regular hexagon and let r be rotation by 60° clockwise. It's not too hard to see that $R_6 = \langle r \rangle$ and $|R_6| = 6$. The Cayley diagram for R_6 with generating set $\{r\}$ is given in Figure 2.4.

(a) Is R_6 cyclic?

(b) Is R_6 abelian?

[‖]Cayley diagrams are named after their inventor Arthur Cayley, a nineteenth century British mathematician.

(c) Write r^{-1} as a word in r.

(d) Can you find a shorter word to describe r^8?

(e) Does r^2 generate the group?

(f) Does r^5 generate the group?

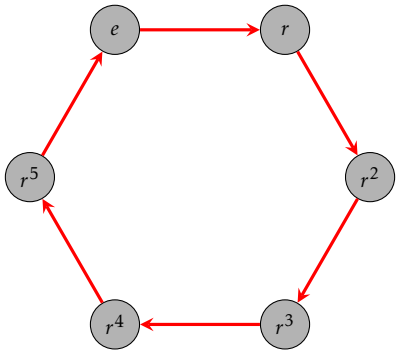


Figure 2.4. Cayley diagram for R_6 with generating set $\{r\}$.

Now, let's build a few Cayley diagrams to further our intuition.

Problem 2.72. Construct a Cayley diagram for each of the following groups using the specified generating set.

(a) S_2 with generating set $\{s\}$ (see Problem 2.63)

(b) R_4 with generating set $\{r\}$ (see Problem 2.20)

(c) V_4 with generating set $\{v, h\}$ (see Problem 2.64)

(d) D_3 with generating set $\{r, s\}$ (see Problem 2.21)

(e) D_3 with generating set $\{s, s'\}$ (see Problem 2.57)

(f) S_3 with generating set $\{s_1, s_2\}$ (see Problem 2.23)

(g) D_4 with generating set $\{r, s\}$ (see Problem 2.22)

Not only are Cayley diagrams visually appealing, but they provide a map for the group in question. That is, they provide a method for navigating the group. Following sequences of arrows tells us how to achieve a net action. However, each Cayley diagram very much depends on the set of generators that are chosen to generate the group. If we change the generating set, we may end up with a very different looking Cayley diagram. For example, compare the Cayley diagrams for D_3 that you constructed in parts (d) and (e) of Problem 2.72.

Before closing out this section, let's tackle a few more problems.

Problem 2.73. Consider the group $(\mathbb{Z}, +)$.

(a) Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{1\}$.

(b) Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{-1\}$. How does this diagram compare to the one in part (a)?

(c) It turns out that $\mathbb{Z} = \langle 2, 3 \rangle$. Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{2, 3\}$.

Problem 2.74. Assume G is a group. Suppose that S and S' are two different sets that generate G. If you draw the Cayley diagram for G using S and then draw the Cayley diagram for G using S', what features of the two graphs are the same and which are potentially different?

Problem 2.75. Consider the diagrams given in Figures 2.5 and 2.6. Explain why neither of these diagrams could possibly be the Cayley diagram for a group.

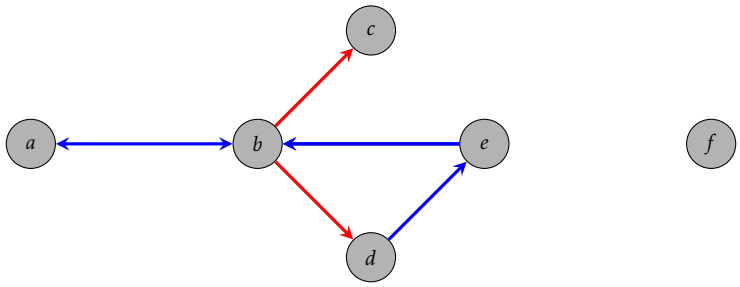


Figure 2.5

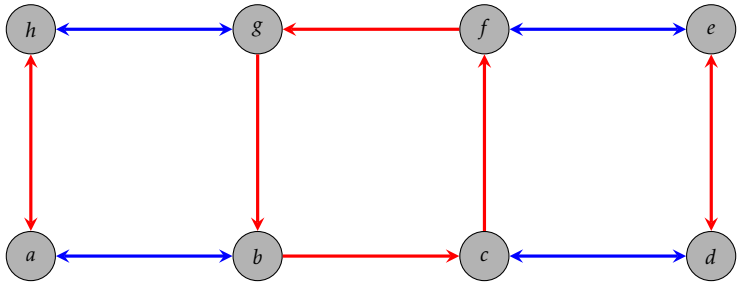


Figure 2.6

While thinking about the previous problem, you likely conjectured the next couple theorems.

Theorem 2.76. If G is a group with generating set S, then for every $g \in G$ and $s \in S$, there is exactly one arrow with color c_s pointing from $s^{-1}g$ to g and exactly one arrow with color c_s pointing from g to sg.

Theorem 2.77. If G is a group with generating set S, then the Cayley diagram for G with generating set S is connected. That is, for every pair of vertices g and h, there is a path of forward or backward arrows connecting g and h.[**]

[**] *Hint:* First consider the case when either g or h is the identity e.

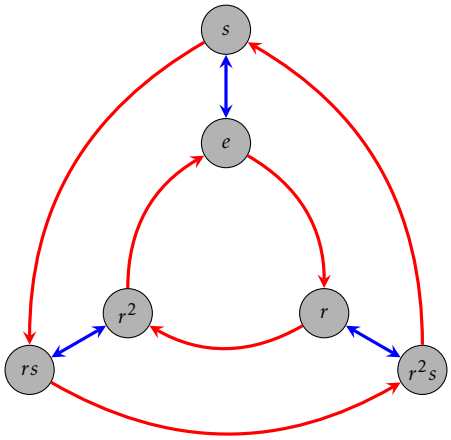


Figure 2.7. Cayley diagram for D_3 with generating set $\{r, s\}$.

Consider the Cayley diagram for D_3 with generating set $\{r, s\}$ that is given in Figure 2.7. Notice that we labeled the lower right corner of the Cayley diagram with the word r^2s. This means that we first followed a blue arrow out of e and then two red arrows. However, we could also get to this vertex by first doing a red arrow out of e followed by a blue arrow. So, we could also have labeled this vertex with the word sr. The upshot is that $r^2s = sr$. These types of group equations are called **relations**.

We discovered this relation by starting at e and then traveling a sequence of arrows to get to the vertex in the lower right corner. However, notice that following a blue and then two red arrows is *always* the same as following a red arrow and then a blue arrow regardless of which vertex we start at. That is, the local relation $r^2s = sr$ starting at e holds globally across the entire Cayley diagram.

Cayley diagrams for groups will always have this uniform symmetry. That is, any local patterns in the diagram appear globally throughout the diagram.

Problem 2.78. Let G be a group with generating set S and consider the corresponding Cayley diagram. Suppose

$$s_{x_1} s_{x_2} \cdots s_{x_n} = s_{y_1} s_{y_2} \cdots s_{y_m}$$

is a relation in G, where each s_{x_i} and s_{y_j} is either an element from S or the inverse of an element from S. Explain what it means for this relation to hold globally across the entire Cayley diagram for G.

You've likely noticed the following theorem while tinkering with examples.

Theorem 2.79. Suppose G is a *finite* group with generating set S and consider the corresponding Cayley diagram. For $s \in S$, if we follow a sequence of (forward) arrows of color c_s out of e, we eventually end up back at e after a finite number of steps.

Problem 2.80. Suppose $\{g_1, \ldots, g_n\}$ is a generating set for a group G.

(a) Explain why $\{g_1^{-1}, \ldots, g_n^{-1}\}$ is also a generating set for G.

(b) How does the Cayley diagram for G with generating set $\{g_1, \ldots, g_n\}$ compare to the Cayley diagram with generating set $\{g_1^{-1}, \ldots, g_n^{-1}\}$?

We close this section with two problems that ask you to think about the structure of Cayley diagrams for cyclic groups and abelian groups.

Problem 2.81. Suppose G is a cyclic group.

(a) If G is finite, what conclusions can you make about Cayley diagrams for G?

(b) If G is infinite, what conclusions can you make about Cayley diagrams for G?

Problem 2.82. Suppose G is an abelian group with generating set S and consider the corresponding Cayley diagram.

(a) If $s, t \in S$, then what relationship must be true about the corresponding arrows?

(b) Is the converse of your claim in part (a) true? That is, if every pair of arrows in the Cayley diagram for G has the property you stated above, will the group be abelian?