An Inquiry-Based Approach to Abstract Algebra

Dana C. Ernst, PhD
Northern Arizona University

Spring 2022

This book is intended to be a task sequence for an undergraduate abstract algebra course that utilizes an inquiry-based learning (IBL) approach. You can find the most up-to-date version of these notes on GitHub:

http://dcernst.github.io/IBL-AbstractAlgebra/

I would be thrilled if you used these notes and improved them. If you make any modifications, you can either make a pull request on GitHub or submit the improvements via email. You are also welcome to fork the source and modify the notes for your purposes as long as you maintain the license below.

Contents

Preface

Mathematics is not about calculations, but ideas. My goal as a teacher is to provide students with the opportunity to grapple with these ideas and to be immersed in the process of mathematical discovery. Repeatedly engaging in this process hones the mind and develops mental maturity marked by clear and rigorous thinking. Like music and art, mathematics provides an opportunity for enrichment, experiencing beauty, elegance, and aesthetic value. The medium of a painter is color and shape, whereas the medium of a mathematician is abstract thought. The creative aspect of mathematics is what captivates me and fuels my motivation to keep learning and exploring.

While the content we teach our students is important, it is not enough. An education must prepare individuals to ask and explore questions in contexts that do not yet exist and to be able to tackle problems they have never encountered. It is important that we put these issues front and center and place an explicit focus on students producing, rather than consuming, knowledge. If we truly want our students to be independent, inquisitive, and persistent, then we need to provide them with the means to acquire these skills. Their viability as a professional in the modern workforce depends on their ability to embrace this mindset.

When I started teaching, I mimicked the experiences I had as a student. Because it was all I knew, I lectured. By standard metrics, this seemed to work out just fine. Glowing student and peer evaluations, as well as reoccurring teaching awards, indicated that I was effectively doing my job. People consistently told me that I was an excellent teacher. However, two observations made me reconsider how well I was really doing. Namely, many of my students seemed to depend on me to be successful, and second, they retained only some of what I had taught them. In the words of Dylan Retsek:

> "Things my students claim that I taught them masterfully, they don't know."

Inspired by a desire to address these concerns, I began transitioning away from direct instruction towards a more student-centered approach. The goals and philosophy behind inquiry-based learning (IBL) resonate deeply with my ideals, which is why I have embraced this paradigm. According to the Academy of Inquiry-Based Learning, IBL is a method of teaching that engages students in sense-making activities. Students are given tasks requiring them to solve problems, conjecture, experiment, explore, create, and communicate—all those wonderful skills and habits of mind that mathematicians engage in regularly. This book has IBL baked into its core.

The primary objectives of this book are to:

- Expand the mathematical content knowledge of the reader,

- Provide an opportunity for the reader to experience the profound beauty of mathematics,
- Allow the reader to exercise creativity in producing and discovering mathematics,
- Enhance the ability of the reader to be a robust and persistent problem solver.

Ultimately, this is really a book about productive struggle and learning how to learn. Mathematics is simply the vehicle.

> Much more important than specific mathematical results are the habits of mind used by the people who create those results. ... Although it is necessary to infuse courses and curricula with modern content, what is even more important is to give students the tools they will need in order to use, understand, and even make mathematics that does not yet exist.
>
> Cuoco, Goldenberg, & Mark in *Habit of Mind: An Organizing Principle for Mathematics Curriculum*

Acknowledgements

This book has been an open-source project since day one. Instructors and students can download the PDF for free and modify the source as they see fit. Several of instructors and students have provided extremely useful feedback, which has improved the book at each iteration. Moreover, due to the open-source nature of the book, I have been able to incorporate content written by others. Below is a list of people (alphabetical by last name) that have contributed content, advice, or feedback.

- Nathan Carter (Bentley University). Nathan's excellent book *Visual Group Theory* has had a huge impact on my approach to teaching abstract algebra.
- Anders Hendrickson (Milliman). Anders is the original author of the content in Appendix A: Elements of Style for Proofs. The current version in Appendix A is a result of modifications made by myself with some suggestions from David Richeson.
- Matthew Macauley (Clemson University). Several Cayley diagrams throughout the book were borrowed from or inspired by Matt.
- Eric Miles (Colorado Mesa University). Eric modified an earlier version of the book. I reincorporated several of his improvements.
- David Richeson (Dickinson College). David is responsible for much of the content in Appendix B: Fancy Mathematical Terms and Appendix C: Definitions in Mathematics.
- Josh Wiscons (CSU Sacramento) and Ben Woodruff (BYU Idaho). In the early stages of development, Josh and Ben were instrumental in the development of this book.

The mathematician does not study pure mathematics because it is useful; he studies it because he delights in it, and he delights in it because it is beautiful.

Henri Poincaré, mathematician & physicist

Chapter 1

Introduction

1.1 What is Abstract Algebra?

Abstract algebra is the subject area of mathematics that studies algebraic structures, such as groups, rings, fields, modules, vector spaces, and algebras. This course is an introduction to abstract algebra. We will spend most of our time studying groups. Group theory is the study of symmetry, and 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. This book covers the basic concepts of group theory, and a special effort will be made to emphasize the intuition behind the concepts and motivate the subject matter. In the final chapter, we will also introduce rings and fields.

Mathematics, rightly viewed, possesses not only truth, but supreme beauty—a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of painting or music, yet sublimely pure, and capable of a stern perfection such as only the greatest art can show. The true spirit of delight, the exaltation, the sense of being more than Man, which is the touchstone of the highest excellence, is to be found in mathematics as surely as poetry.

Bertrand Russell, philosopher & mathematician

1.2 What Should You Expect?

Up to this point, it is possible that your experience of mathematics has been about using formulas and algorithms. You are used to being asked to do things like: "solve for x", "take the derivative of this function", "integrate this function", etc. Accomplishing

tasks like these usually amounts to mimicking examples that you have seen in class or in your textbook. However, this is only one part of mathematics. Mathematicians experiment, make conjectures, write definitions, and prove theorems. While engaging with the material contained in this book, we will learn about doing all of these things, especially writing proofs. Mathematicians are in the business of proving theorems and this is exactly our endeavor. Ultimately, the focus of this book is on producing and discovering mathematics.

Your progress will be fueled by your ability to wrestle with mathematical ideas and to prove theorems. As you work through the book, you will find that you have ideas for proofs, but you are unsure of them. Do not be afraid to tinker and make mistakes. You can always revisit your work as you become more proficient. Do not expect to do most things perfectly on your first—or even second or third—attempt. The material is too rich for a human being to completely understand immediately. Learning a new skill requires dedication and patience during periods of frustration. Moreover, solving genuine problems is difficult and takes time. But it is also rewarding!

> You may encounter many defeats, but you must not be defeated.
>
> Maya Angelou, poet & activist

1.3 An Inquiry-Based Approach

In many mathematics classrooms, "doing mathematics" means following the rules dictated by the teacher, and "knowing mathematics" means remembering and applying them. However, this is not a typical mathematics textbook and is likely a significant departure from your prior experience, where mimicking prefabricated examples led you to success. In order to promote a more active participation in your learning, this book adheres to an educational philosophy called inquiry-based learning (IBL). IBL is a student-centered method of teaching that engages students in sense-making activities and challenges them to create or discover mathematics. In this book, you will be expected to actively engage with the topics at hand and to construct your own understanding. You will be given tasks requiring you to solve problems, conjecture, experiment, explore, create, and communicate. Rather than showing facts or a clear, smooth path to a solution, this book will guide and mentor you through an adventure in mathematical discovery.

This book makes no assumptions about the specifics of how your instructor chooses to implement an IBL approach. Generally speaking, students are told which problems and theorems to grapple with for the next class sessions, and then the majority of class time is devoted to students working in groups on unresolved solutions/proofs or having students present their proposed solutions/proofs to the rest of the class. Students should—as much as possible—be responsible for guiding the acquisition of knowledge and validating the ideas presented. That is, you should not be looking to the instructor as the sole authority. In an IBL course, instructor and students have joint responsibility

for the depth and progress of the course. While effective IBL courses come in a variety of forms, they all possess a few essential ingredients. According to Laursen and Rasmussen (2019), the Four Pillars of IBL are:

- Students engage deeply with coherent and meaningful mathematical tasks.
- Students collaboratively process mathematical ideas.
- Instructors inquire into student thinking.
- Instructors foster equity in their design and facilitation choices.

This book can only address the first pillar while it is the responsibility of your instructor and class to develop a culture that provides an adequate environment for the remaining pillars to take root. If you are studying this material independent of a classroom setting, I encourage you to find a community where you can collaborate and discuss your ideas.

Just like learning to play an instrument or sport, you will have to learn new skills and ideas. Along this journey, you should expect a cycle of victory and defeat, experiencing a full range of emotions. Sometimes you will feel exhilarated, other times you might be seemingly paralyzed by extreme confusion. You will experience struggle and failure before you experience understanding. This is part of the normal learning process. If you are doing things well, you should be confused on a regular basis. Productive struggle and mistakes provide opportunities for growth. As the author of this text, I am here to guide and challenge you, but I cannot do the learning for you, just as a music teacher cannot move your fingers and your heart for you. This is a very exciting time in your mathematical career. You will experience mathematics in a new and profound way. Be patient with yourself and others as you adjust to a new paradigm.

You could view this book as mountaineering guidebook. I have provided a list of mountains to summit, sometimes indicating which trailhead to start at or which trail to follow. There will always be multiple routes to top, some more challenging than others. Some summits you will attain quickly and easily, others might require a multi-day expedition. Oftentimes, your journey will be laced with false summits. Some summits will be obscured by clouds. Sometimes you will have to wait out a storm, perhaps turning around and attempting another route, or even attempting to summit on a different day after the weather has cleared. The strength, fitness, and endurance you gain along the way will allow you to take on more and more challenging, and often beautiful, terrain. Do not forget to take in the view from the top! The joy you feel from overcoming obstacles and reaching each summit under your own will and power has the potential to be life changing. But make no mistake, the journey is vastly more important than the destinations.

> Don't fear failure. Not failure, but low aim, is the crime. In great attempts it is glorious even to fail.
>
> Bruce Lee, martial artist & actor

1.4 Structure of the Textbook

As you read this book, you will be required to digest the material in a meaningful way. It is your responsibility to read and understand new definitions and their related concepts. In addition, you will be asked to complete problems aimed at solidifying your understanding of the material. Most importantly, you will be asked to make conjectures, produce counterexamples, and prove theorems. All of these tasks will almost always be challenging.

The items labeled as **Definition** and **Example** are meant to be read and digested. However, the items labeled as **Problem**, **Theorem**, and **Corollary** require action on your part. Items labeled as **Problem** are sort of a mixed bag. Some Problems are computational in nature and aimed at improving your understanding of a particular concept while others ask you to provide a counterexample for a statement if it is false or to provide a proof if the statement is true. Items with the **Theorem** and **Corollary** designation are mathematical facts and the intention is for you to produce a valid proof of the given statement. The main difference between a theorem and a corollary is that corollaries are typically statements that follow quickly from a previous theorem. In general, you should expect corollaries to have very short proofs. However, that does not mean that you cannot produce a more lengthy yet valid proof of a corollary.

Oftentimes, the problems and theorems are guiding you towards a substantial, more general result. Other times, they are designed to get you to apply ideas in a new way. One thing to always keep in mind is that every task in this book can be done by you, the student. But it may not be on your first try, or even your second.

Discussion of new topics is typically kept at a minimum and there are very few examples in this book. This is intentional. One of the objectives of the items labeled as **Problem** is for you to produce the examples needed to internalize unfamiliar concepts. The overarching goal of this book is to help you develop a deep and meaningful understanding of the processes of producing mathematics by putting you in direct contact with mathematical phenomena.

> Don't just read it; fight it! Ask your own questions, look for your own examples, discover your own proofs. Is the hypothesis necessary? Is the converse true? What happens in the classical special case? What about the degenerate cases? Where does the proof use the hypothesis?
>
> Paul Halmos, mathematician

1.5 Some Minimal Guidance

Below are some guidelines to keep in mind as you get started.

- The statement you are proving should be on the same page as the beginning of your

proof.

- You should indicate where the proof begins by writing "*Proof.*" at the beginning.
- Make it clear to yourself and the reader what your assumptions are at the very beginning of your proof. Typically, these statements will start off "Assume…", "Suppose…", or "Let…". Sometimes there will be some implicit assumptions that we can omit, but at least in the beginning, you should get in the habit of clearly stating your assumptions up front.
- Carefully consider the order in which you write your proof. Each sentence should follow from an earlier sentence in your proof or possibly a result you have already proved.
- Unlike the experience many of you had writing proofs in your high school geometry class, our proofs should be written in complete sentences. You should break sections of a proof into paragraphs and use proper grammar. There are some pedantic conventions for doing this that will be pointed out along the way. Initially, this will be an issue that you may struggle with, but you will get the hang of it.
- There will be many situations where you will want to refer to an earlier definition, problem, theorem, or corollary. In this case, you should reference the statement by number, but it is also helpful to the reader to summarize the statement you are citing.
- There will be times when we will need to do some basic algebraic manipulations. You should feel free to do this whenever the need arises. But you should show sufficient work along the way. In addition, you should organize your calculations so that each step follows from the previous. The order in which we write things matters. You do not need to write down justifications for basic algebraic manipulations (e.g., adding 1 to both sides of an equation, adding and subtracting the same amount on the same side of an equation, adding like terms, factoring, basic simplification, etc.).
- On the other hand, you do need to make explicit justification of the logical steps in a proof. As stated above, you should cite a previous definition, theorem, etc. when necessary.
- Similar to making it clear where your proof begins, you should indicate where it ends. It is common to conclude a proof with the standard "proof box" (□ or ■). This little square at end of a proof is sometimes called a **tombstone** or **Halmos symbol** after Hungarian-born American mathematician Paul Halmos (1916–2006).

It is of utmost importance that you work to understand every proof. Questions—asked to your instructor, your peers, and yourself—are often your best tool for determining whether you understand a proof. Another way to help you process and understand a proof is to try and make observations and connections between different ideas, proof statements and methods, and to compare various approaches.

If you would like additional guidance before you dig in, look over the guidelines in Appendix A: Elements of Style for Proofs. It is suggested that you review this appendix occasionally as you progress through the book as some guidelines may not initially make sense or seem relevant. Be prepared to put in a lot of time and do all the work. Your effort will pay off in intellectual development. Now, go have fun and start exploring mathematics!

> Our greatest glory is not in never falling, but in rising every time we fall.
>
> Confucius, philosopher

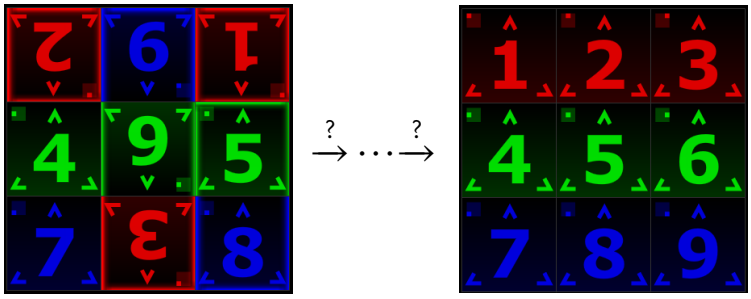
Chapter 2

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.

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.

If you would like to tinker with Spinpossible yourself, check out Jeff Slye's interactive implementation of the game, located here: https://jslyemath.itch.io/spin3x3.

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 $\{s_{ij} \mid i \text{ upper left corner}, j \text{ lower right corner of subrectangle}\}$. Our words will always consist of a finite number of spins.

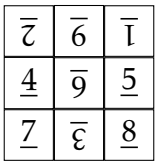
Every word consisting of spins corresponds to a function that takes a scrambled board as input and returns a scrambled board. We say that the words "act on" the scrambled boards. For each word, there is an associated **net action**. For example, the word $s_{12}s_{23}s_{12}$ corresponds to swapping the 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. It is worth mentioning that 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) **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.

2.2 Binary Operations

Before beginning our formal study of groups, we need to 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 $* : A \times A \to A$. 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 $M_{2\times 2}(\mathbb{R})$ be the set of 2×2 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?

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**. Commutative groups are called abelian in honor of the Norwegian mathematician Niels Henrik 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.
- 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) $(\mathbb{Q} \setminus \{0\}, \cdot)$

(h) $(M_{2\times 2}(\mathbb{R}), +)$ *Note:* $M_{2\times 2}(\mathbb{R})$ is the set of 2×2 matrices with real number entries.

(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 $x = y$. *Note:* You only need to prove one of these statements as the proof of the other is similar.

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, if 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 equation $gx = h$ has a unique solution for x in G. Similarly, the equation $xg = h$ has a unique solution. *Note:* You only need to prove one of these statements as the proof for 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

$$s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n},$$

where each $s_i \in S$ and $\varepsilon_i \in \{\pm 1\}$. Each s_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 worth mentioning that we are slightly abusing notation here. For nonempty $S \subseteq G$, 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.

It is also 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.

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 four colors 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 $\text{Spin}_{1\times2}$ 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 $\text{Spin}_{1\times2}$?

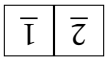
(c) Verify that $\text{Spin}_{1\times2} = \langle s_{11}, s_{22}, s_{12} \rangle$ by writing every element as a word in s_{11}, s_{22}, or s_{12}.

(d) Is $\{s_{11}, s_{22}, s_{12}\}$ a minimal generating set for $\text{Spin}_{1\times2}$?

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.

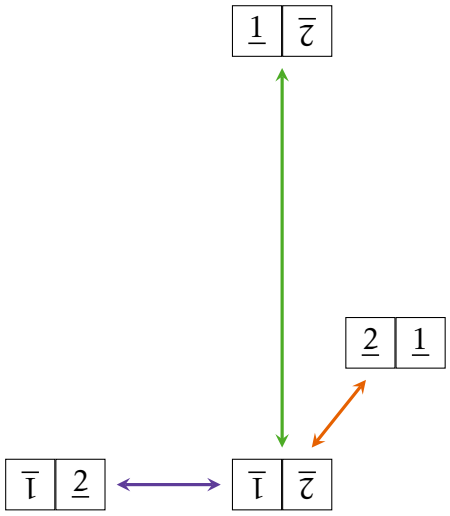


Figure 2.1

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 purple arrow corresponds to toggling position 2 (s_{22}), and a orange 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.

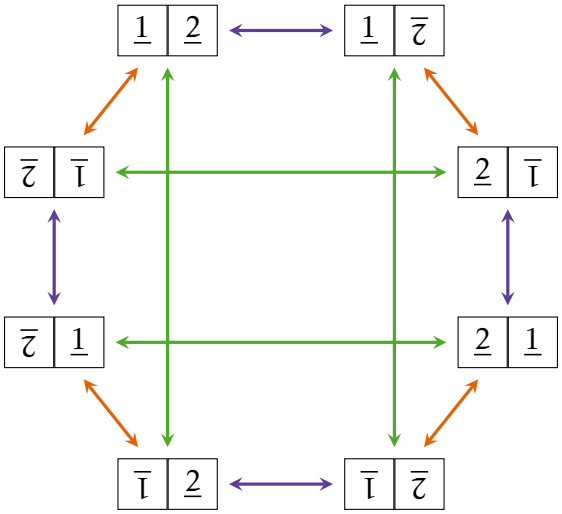
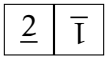


Figure 2.2

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.

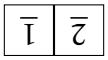
One way to do this is to label each vertex with the word that corresponds to a path of arrows that leads to the vertex from the vertex labeled by the identity e. Don't forget that we apply our composition of actions from right to left. This means that following a sequence of arrows out of the vertex 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 purple arrow and then a orange 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 $s_{12}s_{22}$ 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.

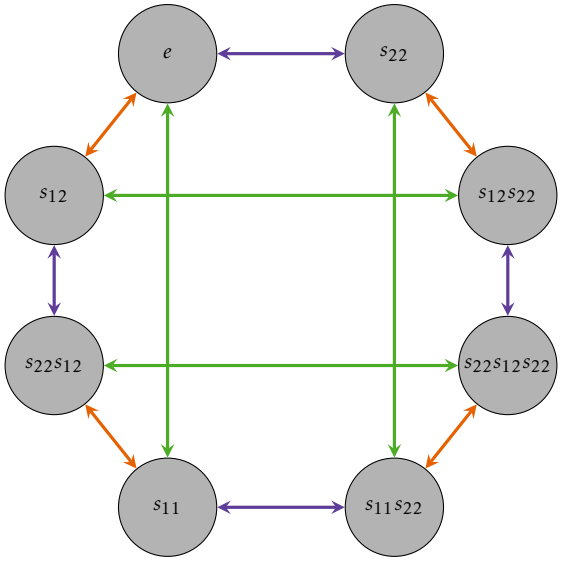


Figure 2.3. Cayley diagram for $\text{Spin}_{1\times 2}$ with generating set $\{s_{11}, s_{22}, s_{12}\}$.

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

(a) Removing all the orange 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 purple and green arrows? What does this tell you about $\{s_{11}, s_{22}\}$?

(b) What if we remove the purple 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.

Cayley diagrams are named after British mathematician Arthur Cayley (1821–1895).

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?

(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?

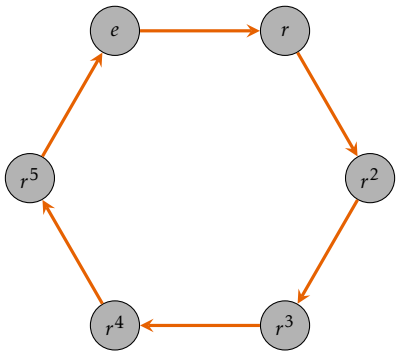


Figure 2.4. Cayley diagram for R_6 with generating set $\{r\}$.

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.

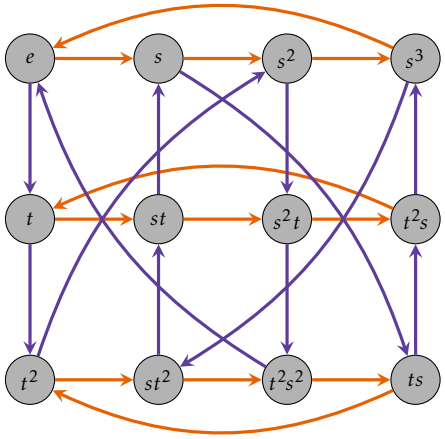
Problem 2.73. Consider the group $(\mathbb{Z}, +)$.

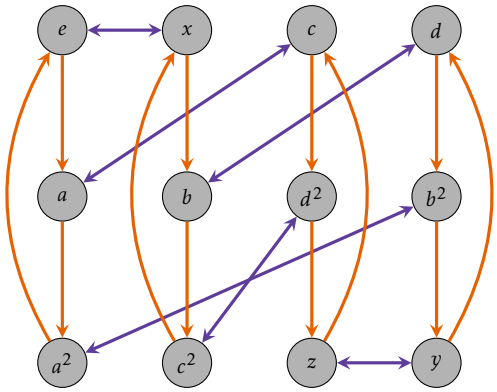
(a) Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{1\}$.

(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. The Cayley diagrams of two groups of order 12 are shown below.





(a) What is the generating set for each group?

(b) Create a group table for each group. For consistency, please order the elements in the first group by

$$e, t, t^2, s, ts, t^2s, s^2, s^2t, s^2t^2, s^3, st^2, st$$

and those in second by

$$e, x, y, z, a, b, c, d, a^2, b^2, c^2, d^2.$$

(c) Squint your eyes. Do you see any patterns in these tables?

(d) Find the inverse of each element.

(e) For each element g, find the smallest positive exponent k such that $g^k = e$.

Problem 2.75. 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 2.76. 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.

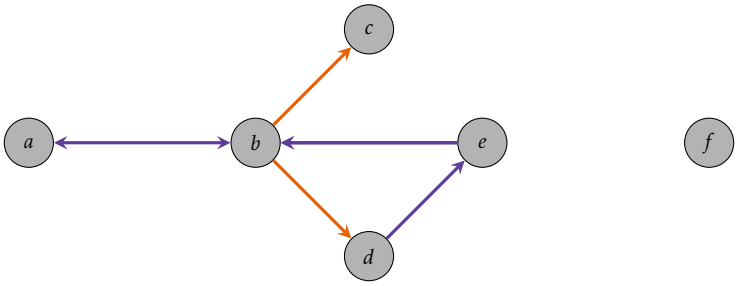


Figure 2.5

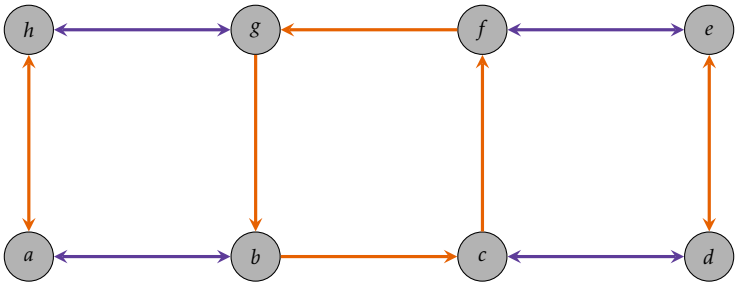


Figure 2.6

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

Theorem 2.77. 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 2.78. 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.

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 purple arrow out of e and then two orange arrows.

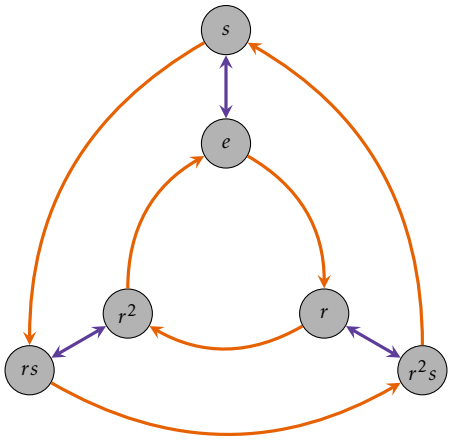


Figure 2.7. Cayley diagram for D_3 with generating set $\{r, s\}$.

However, we could also get to this vertex by first doing a orange arrow out of e followed by a purple 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 purple and then two orange arrows is *always* the same as following a orange arrow and then a purple arrow regardless of which vertex we start at. That is, the local relation $r^2s = sr$ 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 2.79. Let G be a group with generating set S and consider the corresponding Cayley diagram. Suppose

$$s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} = t_1^{\delta_1} t_2^{\delta_2} \cdots t_m^{\delta_m}$$

is a relation in G, where each $s_i, t_j \in S$ and $\epsilon_i, \delta_j \in \{\pm 1\}$. 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 2.80. 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 2.81. 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 2.82. Suppose G is a cyclic group with generator $g \in G$.

(a) If G is finite, what conclusions can you make about the Cayley diagram for G with generating set $\{g\}$?

(b) If G is infinite, what conclusions can you make about the Cayley diagram for G with generating set $\{g\}$?

Problem 2.83. 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?

Chapter 3

Subgroups and Isomorphisms

For the next two sections, it would be useful to have all of the Cayley diagrams we've encountered in one place for reference. So, before continuing, gather up the following Cayley diagrams:

- $\text{Spin}_{1\times 2}$. There are 3 of these. I drew one for you in Section 2.6 and you discovered two more in Problem 2.69.
- S_2. See Problem 2.72(a).
- R_4. See Problem 2.72(b).
- V_4. See Problem 2.72(c).
- D_3. There are two of these. See Problems 2.72(d) and 2.72(e).
- S_3. See Problem 2.72(f).
- D_4. See Problem 2.72(g).

3.1 Subgroups

Problem 3.1. Recall the definition of "subset." What do you think "subgroup" means? Try to come up with a potential definition. Try not to read any further before doing this.

Problem 3.2. Examine your Cayley diagrams for D_4 (with generating set $\{r,s\}$) and R_4 (with generating set $\{r\}$) and make some observations. How are they similar and how are they different? Can you reconcile the similarities and differences by thinking about the actions of each group?

Hopefully, one of the things you noticed in the previous problem is that we can "see" R_4 inside of D_4. You may have used different colors in each case and maybe even labeled the vertices with different words, but the overall structure of R_4 is there nonetheless.

Problem 3.3. If you ignore the labels on the vertices and just pay attention to the configuration of arrows, it appears that there are two copies of the Cayley diagram for R_4 in the Cayley diagram for D_4. Isolate these two copies by ignoring the edges that correspond to the generator s. Now, paying close attention to the words that label the vertices from the original Cayley diagram for D_4, are either of these groups in their own right?

Recall that the identity must be one of the elements included in a group. If this didn't occur to you when doing the previous problem, you might want to go back and rethink your answer. Just like in the previous problem, we can often "see" smaller groups living inside larger groups. These smaller groups are called **subgroups**.

Definition 3.4. Let G be a group and let H be a subset of G. Then H is a **subgroup** of G, written $H \leq G$, provided that H is a group in its own right under the binary operation inherited from G.

The phrase "under the binary operation inherited from G" means that to combine two elements in H, we should treat the elements as if they were in G and perform the binary operation of G.

In light of Problem 3.3, we would write $R_4 \leq D_4$. The second sub-diagram of the Cayley diagram for D_4 (using $\{r, s\}$ as the generating set) that resembles R_4 cannot be a subgroup because it does not contain the identity. However, since it looks a lot like R_4, we call it a "clone" of R_4. We formalize the notion of a clone shortly.

Problem 3.5. Let G be a group and let $H \subseteq G$. If we wanted to determine whether H is a subgroup of G, can we skip checking any of the axioms? Which axioms must we verify?

Let's make the observations of the previous problem a bit more formal.

Theorem 3.6 (Two Step Subgroup Test)**.** Suppose G is a group and H is a nonempty subset of G. Then $H \leq G$ if and only if (i) for all $h \in H$, $h^{-1} \in H$, as well, and (ii) H is closed under the binary operation of G.

Notice that one of the hypotheses of Theorem 3.6 is that H be nonempty. This means that if we want to prove that a certain subset H is a subgroup of a group G, then one of the things we must do is verify that H is in fact nonempty. In light of this, the "Two Step Subgroup Test" should probably be called the "Three Step Subgroup Test".

As Theorems 3.7 and 3.9 will illustrate, there are a couple of subgroups that every group contains.

Theorem 3.7. If G is a group, then $\{e\} \leq G$.

The subgroup $\{e\}$ is referred to as the **trivial subgroup**. All other subgroups are called **nontrivial**.

Problem 3.8. Let G be a group. What does the Cayley diagram for the subgroup $\{e\}$ look like? What are you using as your generating set?

Earlier, we referred to subgroups as being "smaller." However, our definition does not imply that this has to be the case.

Theorem 3.9. If G is a group, then $G \leq G$.

We refer to subgroups that are not equal to the whole group as **proper subgroups**. If H is a proper subgroup, then we may write $H < G$.

Recall Theorem 2.52 that states that if G is a group under $*$ and S is a subset of G, then $\langle S \rangle$ is also a group under $*$. Let's take this a step further.

Theorem 3.10. If G is a group and $S \subseteq G$, then $\langle S \rangle \leq G$. In particular, $\langle S \rangle$ is the smallest subgroup of G containing S.

The subgroup $\langle S \rangle$ is called the **subgroup generated by** S. In the special case when S equals a single element, say $S = \{g\}$, then

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

which is called the (**cyclic**) **subgroup generated by** g. Every subgroup can be written in the "generated by" form. That is, if H is a subgroup of a group G, then there always exists a subset S of G such that $\langle S \rangle = H$. In particular, $\langle H \rangle = H$ for $H \leq G$, and as a special case, we have $\langle G \rangle = G$.

Earlier we mentioned that the Cayley diagram for the subgroup R_4 (using $\{r\}$ as the generating set) of D_4 had a clone in the Cayley diagram for D_4 (using the generating set $\{s, t\}$). Loosely speaking, a clone is a sub-diagram in a Cayley diagram that looks just like the Cayley diagram for a subgroup. More formally, suppose G is a group with generating set S. If $H \leq G$ such that $H = \langle T \rangle$ for some $T \subseteq S$, then H will be visually apparent in the Cayley diagram for G using S as the generating set. In particular, the Cayley diagram for H will appear in the Cayley diagram for G using some subset of the arrow types determined by S. Any collection of vertices C in the Cayley diagram for G whose induced subgraph (i.e., the diagram that results from using the vertices in C and only those arrows connecting vertices in C) is identical to the Cayley diagram for H while ignoring the labels on the vertices is called a **clone** of H. For convenience, we also say that H is a clone of itself. In Section 5.1, we will see that the clones of a subgroup correspond to the "right cosets" of a subgroup.

Example 3.11. Consider the Cayley diagram of the left given in Problem 2.74. Let $H = \langle s \rangle$ (i.e., the cyclic subgroup generated by r). Then $H = \{e, s, s^2, s^3\}$, which we can visualize as the subgraph that is the four-cycle at the top of the Cayley diagram. Then H has three clones, one of which is itself. The other two clones are $\{t, st, s^2t, t^2s\}$ and $\{t^2, st^2, t^2s^2, ts\}$, neither of which are subgroups since they do not contain the identity. Let $K = \langle t \rangle$, so that $K = \{e, t, t^2, s^2, s^2t, t^2s^2\}$. Then K has two clones, namely K is itself and $\{s, ts, t^2s, s^3, st^2, st\}$.

Problem 3.12. Consider $\text{Spin}_{1\times 2}$ with generating set $\{s_{11}, s_{22}, s_{12}\}$.

(a) Find the Cayley diagram for the subgroup $\langle s_{11} \rangle$ inside the Cayley diagram for $\text{Spin}_{1\times 2}$. Identify all of the clones of $\langle s_{11} \rangle$ inside $\text{Spin}_{1\times 2}$.

(b) Find the Cayley diagram for the subgroup $\langle s_{11}, s_{22} \rangle$ inside the Cayley diagram of $\text{Spin}_{1\times 2}$. Identify the clones of $\langle s_{11}, s_{22} \rangle$ inside $\text{Spin}_{1\times 2}$.

One of the benefits of Cayley diagrams is that they are useful for visualizing subgroups. However, recall that if we change our set of generators, we might get a very different looking Cayley diagram. The upshot of this is that we may be able to see a subgroup in one Cayley diagram for a given group, but not be able to see it in the Cayley diagram arising from a different generating set.

Problem 3.13. We currently have two different Cayley diagrams for D_3 (see Problems 2.21 and 2.57).

(a) Can you find the Cayley diagram for the trivial subgroup $\langle e \rangle$ in either Cayley diagram for D_3? Identify all of the clones of $\langle e \rangle$ in both Cayley diagrams for D_3.

(b) Can you find the Cayley diagram for the subgroup $\langle r \rangle = R_3$ in either Cayley diagram for D_3? If possible, identify all of the clones of R_3 in the Cayley diagrams for D_3.

(c) Can you find the Cayley diagrams for $\langle s \rangle$ and $\langle s' \rangle$ in either Cayley diagram for D_3? If possible, identify all of the clones of $\langle s \rangle$ and $\langle s' \rangle$ in the Cayley diagrams for D_3.

Problem 3.14. Consider D_4. Let h be the reflection of the square over the horizontal midline and let v be the reflection over the vertical midline. Which of the following are subgroups of D_4? In each case, justify your answer. If a subset is a subgroup, try to find a minimal generating set. Also, determine whether you can see the subgroups in our Cayley diagram for D_4 with generating set $\{r, s\}$.

(a) $\{e, r^2\}$

(b) $\{e, h\}$

(c) $\{e, h, v\}$

(d) $\{e, h, v, r^2\}$

Perhaps you recognized the set in part (d) of the previous problem as being the Klein four-group V_4. It follows that $V_4 \leq D_4$.

Let's introduce a group we haven't seen yet. Define the **quaternion group** to be the group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ having the Cayley diagram with generating set $\{i, j, -1\}$ given in Figure 3.1. In this case, 1 is the identity of the group.

Notice that I did not mention what the actions actually do. For now, let's not worry about that. The relationship between the arrows and vertices tells us everything we need to know. Also, let's take it for granted that Q_8 actually is a group.

Problem 3.15. Consider the Cayley diagram for Q_8 given in Figure 3.1.

(a) Which arrows correspond to which generators in our Cayley diagram for Q_8?

(b) What is i^2 equal to? That is, what element of $\{1, -1, i, -i, j, -j, k, -k\}$ is i^2 equal to? How about i^3, i^4, and i^5?

(c) What are j^2, j^3, j^4, and j^5 equal to?

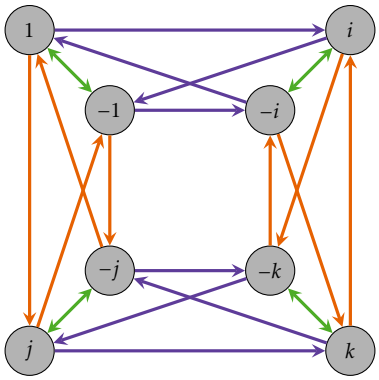


Figure 3.1. Cayley diagram for Q_8 with generating set $\{-1, i, j\}$.

(d) What is $(-1)^2$ equal to?

(e) What is ij equal to? How about ji?

(f) Can you determine what k^2 and ik are equal to?

(g) Can you identify a generating set consisting of only two elements? Can you find more than one?

(h) What subgroups of Q_8 can you see in the Cayley diagram in Figure 3.1?

(i) Find a subgroup of Q_8 that you cannot see in the Cayley diagram.

Problem 3.16. Consider $(\mathbb{R}^3, +)$, where $\mathbb{R}^3$ is the set of all 3-entry row vectors with real number entries (e.g., (a, b, c) where $a, b, c \in \mathbb{R}$) and $+$ is ordinary vector addition. It turns out that $(\mathbb{R}^3, +)$ is an abelian group with identity $(0, 0, 0)$.

(a) Let H be the subset of $\mathbb{R}^3$ consisting of vectors with first coordinate 0. Is H a subgroup of $\mathbb{R}^3$? Prove your answer.

(b) Let K be the subset of $\mathbb{R}^3$ consisting of vectors whose entries sum to 0. Is K a subgroup of $\mathbb{R}^3$? Prove your answer.

(c) Construct a subset of $\mathbb{R}^3$ (different from H and K) that is *not* a subgroup of $\mathbb{R}^3$.

Problem 3.17. Consider the group $(\mathbb{Z}, +)$ (under ordinary addition).

(a) Show that the even integers, written $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$, form a subgroup of $\mathbb{Z}$.

(b) Show that the odd integers are not a subgroup of $\mathbb{Z}$.

(c) Show that all subsets of the form $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ for $n \in \mathbb{Z}$ are subgroups of $\mathbb{Z}$.

(d) Are there any other subgroups besides the ones listed in part (c)? Explain your answer.

(e) For $n \in \mathbb{Z}$, write the subgroup $n\mathbb{Z}$ in the "generated by" notation. That is, find a set S such that $\langle S \rangle = n\mathbb{Z}$. Can you find more than one way to do it?

Problem 3.18. Consider the group of symmetries of a regular octagon. This group is denoted by D_8, where the operation is composition of actions. The group D_8 consists of 16 elements (8 rotations and 8 reflections). Let H be the subset consisting of the following clockwise rotations: 0°, 90°, 180°, and 270°. Determine whether H is a subgroup of D_8 and justify your answer.

Problem 3.19. Find all finite subgroups of $(\mathbb{R} \setminus \{0\}, \cdot)$.

Problem 3.20. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \cdot)$. Explain why $\mathbb{R} \setminus \{0\}$ is not a subgroup of $\mathbb{R}$ despite the fact that $\mathbb{R} \setminus \{0\} \subseteq \mathbb{R}$ and both are groups (under the respective binary operations).

Theorem 3.21. If G is an abelian group such that $H \leq G$, then H is an abelian subgroup.

Problem 3.22. Is the converse of the previous theorem true? If so, prove it. Otherwise, provide a counterexample.

As we've seen, some groups are abelian and some are not. If G is a group, then we define the **center** of G to be

$$Z(G) := \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Notice that if G is abelian, then $Z(G) = G$. However, if G is not abelian, then $Z(G)$ will be a proper subset of G. In some sense, the center of a group is a measure of how close G is to being abelian.

Theorem 3.23. If G is a group, then $Z(G)$ is an abelian subgroup of G.

Problem 3.24. Find the center of each of the following groups.

(a) S_2

(b) V_4

(c) S_3

(d) D_3

(e) D_4

(f) R_4

(g) R_6

(h) $\mathrm{Spin}_{1\times 2}$

(i) Q_8

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

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

3.2 Subgroup Lattices

One of the goals of this section is to gain better understanding of the structure of groups by studying their subgroups.

Suppose we wanted to find all of the subgroups of a finite group G. Theorems 3.7 and 3.9 tell us that $\{e\}$ and G itself are subgroups of G, but there may be others. Theorem 3.6 tells us that if we want to find other subgroups of G, we need to find nonempty subsets of G that are closed and contain all the necessary inverses. So, one method for finding subgroups would be to find all possible nonempty subsets of G and then go about determining which subsets are subgroups by verifying whether a given subset is closed under inverses and closed under the operation of G. This is likely to be fairly time consuming.

Another approach would be to utilize the fact that every subgroup H of G has a generating set. That is, if H is a subgroup of a group G, then there always exists a subset S of G such that $\langle S \rangle = H$. Given a subset S of G, $\langle S \rangle$ is guaranteed to be closed under inverses and the operation of the group G. So, we could determine all of the subgroups of G by generating groups with various subsets S of G. Of course, one drawback is that it might take a bit of effort to determine what $\langle S \rangle$ actually is. Another drawback is that two different subsets S and T may generate the same subgroup.

Let's make this a bit more concrete by exploring an example. Consider the group R_4. What are the subgroups of R_4? Since the order of R_4 is 4, we know that there are $2^4 - 1 = 15$ nonempty subsets of R_4. Some of these are subgroups, but most of them are not. Theorems 3.7 and 3.9 guarantee that $\{e\}$ and R_4 itself are subgroups of R_4. That's 2 out of 15 so far. Are there any others? Let's do an exhaustive search by playing with generating sets. We can certainly be more efficient, but below we list all of the possible subgroups we can generate using subsets of R_4. As you scan the list, you should take a moment to convince yourself that the list is accurate.

$$\langle e \rangle = \{e\}$$
$$\langle r \rangle = \{e, r, r^2, r^3\}$$
$$\langle r^2 \rangle = \{e, r^2\}$$
$$\langle r^3 \rangle = \{e, r^3, r^2, r\}$$
$$\langle e, r \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r^2 \rangle = \{e, r^2\}$$
$$\langle e, r^3 \rangle = \{e, r^3, r^2, r\}$$
$$\langle r, r^2 \rangle = \{e, r, r^2, r^3\}$$
$$\langle r, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r, r^2 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle r, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$
$$\langle e, r, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$$

Let's make a few observations. Scanning the list, we see only three distinct subgroups:

$$\{e\}, \{e, r^2\}, \{e, r, r^2, r^3\}.$$

Out of 15 nonempty subsets of R_4, only 3 subsets are subgroups. Our exhaustive search guarantees that these are the only subgroups of R_4. It is also worth pointing out that

if a subset contains either r or r^3, then that subset generates all of R_4. The reason for this is that $\{r\}$ and $\{r^3\}$ are each minimal generating sets for R_4. More generally, observe that if we increase the size of the generating subset using an element that was already contained in the subgroup generated by the set, then we don't get anything new. For example, consider $\langle r^2 \rangle = \{e, r^2\}$. Since $e \in \langle r^2 \rangle$, we don't get anything new by including e in our generating set. We can state this as a general fact.

Theorem 3.25. Let G be a group and let $g_1, g_2, \ldots, g_n \in G$. If $x \in \langle g_1, g_2, \ldots, g_n \rangle$, then $\langle g_1, g_2, \ldots, g_n \rangle = \langle g_1, g_2, \ldots, g_n, x \rangle$.

In the previous theorem, we are not claiming that $\{g_1, g_2, \ldots, g_n\}$ is a generating set for G—although this may be the case. Instead, are simply making a statement about the subgroup $\langle g_1, g_2, \ldots, g_n \rangle$, whatever it may be.

We can capture the overall relationship between the subgroups of a group G using a **subgroup lattice**. Given a group G, the **lattice of subgroups** of G is the partially ordered set whose elements are the subgroups of G with the partial order relation being set inclusion. It is common to depict the subgroup lattice for a group using a **Hasse diagram**. The Hasse diagram of subgroup lattice is drawn as follows:

(1) Each subgroup H of G is a vertex.

(2) Vertices corresponding to subgroups with smaller order are placed lower in the diagram than vertices corresponding to subgroups with larger order. In particular, the vertex for $\{e\}$ is placed at the bottom of the diagram and the vertex for G is placed at the top.

(3) There is an edge going up from H to K if $H \leq K$ and there is no subgroup L such that $H \leq L \leq K$ with $L \neq H, K$.

Notice that there is an upward path of edges in the Hasse diagram from H to K if and only if $H \leq K$. For convenience we will not make a distinction between the subgroup lattice for a group G and the corresponding Hasse diagram.

The Hasse diagram for the subgroup lattice for R_4 is given in Figure 3.2.

Let's see what we can do with $V_4 = \{e, v, h, vh\}$. Using an exhaustive search, we find that there are five subgroups:

$$\langle e \rangle = \{e\}$$

$$\langle h \rangle = \{e, h\}$$

$$\langle v \rangle = \{e, v\}$$

$$\langle vh \rangle = \{e, vh\}$$

$$\langle v, h \rangle = \langle v, vh \rangle = \langle h, vh \rangle = \{e, v, h, vh\} = V_4$$

For each subgroup above, we've used minimal generating sets to determine the subgroup. The subgroup lattice for V_4 is given in Figure 3.3. Notice that there are no edges among

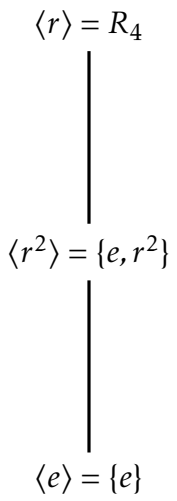


Figure 3.2. Subgroup lattice for R_4.

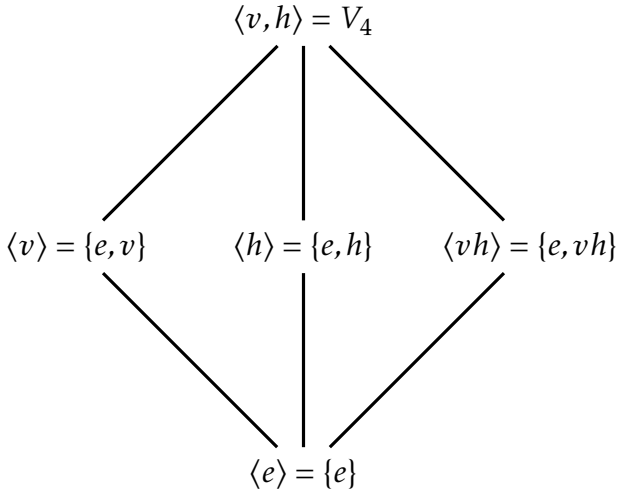


Figure 3.3. Subgroup lattice for V_4.

$\langle v \rangle, \langle h \rangle$, and $\langle vh \rangle$. The reason for this is that none of these groups are subgroups of each other.

The next two theorems provide some further insight into the overall structure of subgroups of a group. Note that a set L is the largest subset contained in both A and B if $L \subseteq A$ and $L \subseteq B$ and whenever $C \subseteq A$ and $C \subseteq B$, we have $C \subseteq L$. Similarly, a set S is the smallest subset containing both A and B if $A \subseteq S$ and $B \subseteq S$ and whenever $A \subseteq C$ and $B \subseteq C$, we have $S \subseteq C$.

Theorem 3.26. If G is a group such that $H, K \leq G$, then $H \cap K \leq G$. Moreover, $H \cap K$ is the largest subgroup contained in both H and K.

It turns out that we cannot simply replace "intersection" with "union" in the previous theorem to obtain the corresponding result involving the smallest subgroup containing two subgroups.

Problem 3.27. Provide an example of a group G and subgroups H and K such that $H \cup K$ is not a subgroup of G.

Theorem 3.28. If G is a group such that $H, K \leq G$, then $\langle H \cup K \rangle \leq G$. Moreover, $\langle H \cup K \rangle \leq G$ is the smallest subgroup containing both H and K.

Theorems 3.26 and 3.28 justify the use of the word "lattice" in "subgroup lattice". In general, a lattice is a partially ordered set in which every two elements have a unique **meet** (also called a **greatest lower bound** or **infimum**) and a unique **join** (also called a **least upper bound** or **supremum**). In the case of a subgroup lattice for a group G, the meet of subgroups H and K is $H \cap K$ and the join is $\langle H \cup K \rangle$. Figure 3.4 illustrates the meet (Theorem 3.26) and join (Theorem 3.28) in the case when H and K are not comparable.

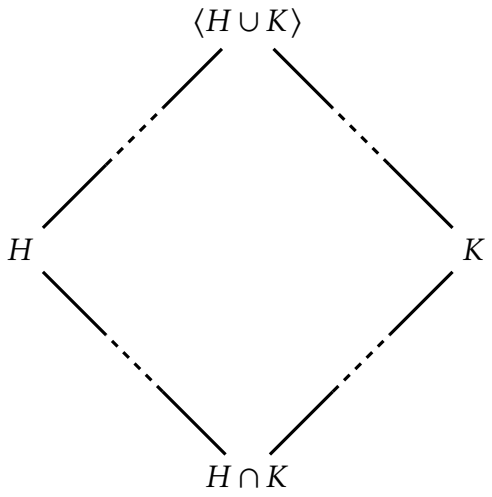


Figure 3.4. Meet and join for subgroups H and K.

In the next few problems, you are asked to create subgroup lattices. As you do this, try to minimize the amount of work it takes to come up with all the subgroups.

Problem 3.29. Find all the subgroups of $R_5 = \{e, r, r^2, r^3, r^4\}$ (where r is clockwise rotation of a regular pentagon by 72°) and then draw the subgroup lattice for R_5.

Problem 3.30. Find all the subgroups of $R_6 = \{e, r, r^2, r^3, r^4, r^5\}$ (where r is clockwise rotation of a regular hexagon by 60°) and then draw the subgroup lattice for R_6.

Problem 3.31. Find all the subgroups of $D_3 = \{e, r, r^2, s, sr, sr^2\}$ (where r and s are the usual symmetries of an equilateral triangle) and then draw the subgroup lattice for D_3.

Problem 3.32. Find all the subgroups of $S_3 = \langle s_1, s_2 \rangle$ (where s_1 is the action that swaps the positions of the first and second coins and s_2 is the action that swaps the second and third coins; see Problem 2.59) and then draw the subgroup lattice for S_3. How does your lattice compare to the one in Problem 3.31? You should look back at parts (e) and (f) of Problem 2.72 and ponder what just happened.

Problem 3.33. Find all the subgroups of $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ (where r and s are the usual symmetries of a square) and then draw the subgroup lattice for D_4.

Problem 3.34. Find all the subgroups of $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ and then draw the subgroup lattice for Q_8.

3.3 Isomorphisms

As we have been exploring various groups, I'm sure you've noticed that some groups seem to look and behave the same. For example, if we choose the same colors for our arrows and ignore the labels on the vertices, the Cayley diagram for D_3 with generating set $\{s, s'\}$ looks the same as the Cayley diagram for S_3 with generating set $\{s_1, s_2\}$. That is, if we pick the appropriate colors and set the Cayley diagram for D_3 (with generating set $\{s, s'\}$) on top of the Cayley diagram for S_3 (with generating set $\{s_1, s_2\}$) such that the identities match up, then the two Cayley diagrams are identical up to relabeling the rest of the vertices. Figure 3.5 should make this clear. This act of matching up the Cayley diagrams establishes a correspondence between the elements of the two groups:

$$\begin{aligned} e &\mapsto e \\ s &\mapsto s_1 \\ s' &\mapsto s_2 \\ ss' &\mapsto s_1 s_2 \\ s's &\mapsto s_2 s_1 \\ ss's &\mapsto s_1 s_2 s_1 \end{aligned}$$

Notice that each correspondence is compatible with the correspondence of the generators, namely: $s \mapsto s_1$ and $s' \mapsto s_2$. Given this correspondence, it should not be surprising that the subgroup lattices for D_3 and S_3 have the same structure.

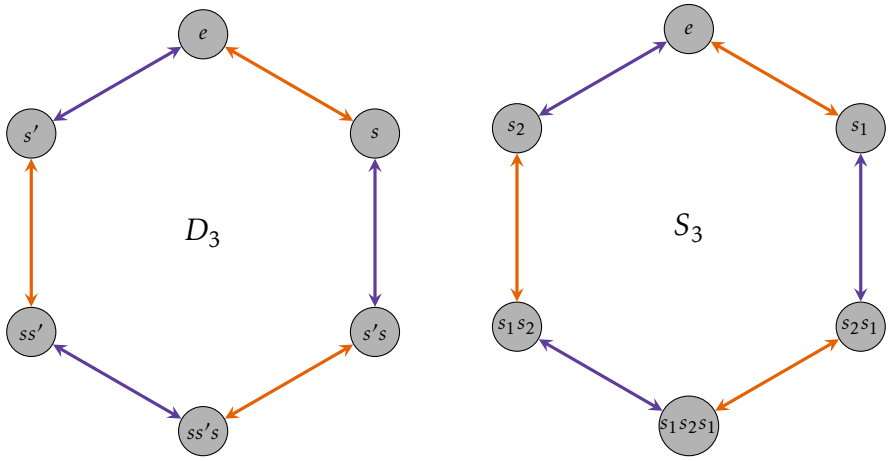


Figure 3.5. Cayley diagrams for D_3 and S_3 with generating sets $\{s, s'\}$ and $\{s_1, s_2\}$, respectively.

The goal of this section is to formalize this phenomenon by introducing the notion of an **isomorphism**. First, let's develop a little more intuition.

If two groups G_1 and G_2 have generating sets T_1 and T_2 such that we can color the edges of the corresponding Cayley diagrams so that the diagrams are identical up to relabeling of the vertices, then we say that there is a **matching** between G_1 and G_2. Above, we showed that D_3 and S_3 have a matching. It's important to emphasize that the existence of a matching between two groups depends on our choice of generating set. If two Cayley diagrams do not look alike, it does not immediately imply that there is not a matching between the groups since it might be the case that choosing different generating sets for the two groups leads to a matching.

Perhaps you've noticed that the Cayley diagram for R_4 with generating set $\{r\}$ looks like the Cayley diagram for the subgroup $\langle j\rangle = \{\pm 1, \pm j\}$ with generating set $\{j\}$ in Q_8. That is, there is a matching between R_4 and $\langle j\rangle$, which we've depicted in Figure 3.6. Similarly, the Cayley diagram for S_2 with generating set $\{s\}$ looks like the Cayley diagram for the subgroup $\langle -1\rangle = \{\pm 1\}$ with generating set $\{-1\}$ in Q_8. The matching between S_2 and $\langle -1\rangle$ is depicted in Figure 3.7. It's fairly easy to see that there is also a matching between S_2 and the subgroup $\langle v\rangle = \{e, v\}$ of V_4. Since there is a matching between S_2 and $\langle -1\rangle$ and a matching between S_2 and $\langle v\rangle$, there is a matching between $\langle -1\rangle$ and $\langle v\rangle$.

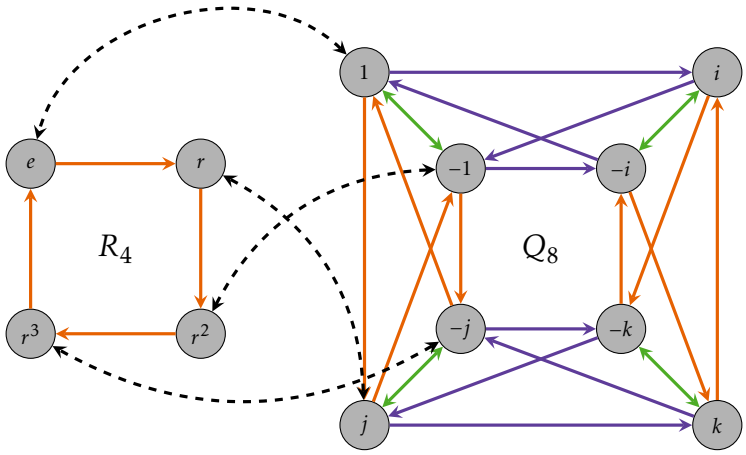


Figure 3.6. A matching between $R_4 = \langle r\rangle$ and $\langle j\rangle \leq Q_8$.

Problem 3.35. We have seen two different Cayley diagrams for D_3, one with generating set $\{s, r\}$ and one with generating set $\{s, s'\}$. As Figure 3.5 illustrates, there is a matching between D_3 and S_3 that relies on the generating sets $\{s, s'\}$ and $\{s_1, s_2\}$, respectively. Find a different matching between D_3 and S_3 that utilizes the generating set $\{r, s\}$ for D_3.

The next theorem follows immediately from the definition of matching.

Theorem 3.36. If there is a matching between G_1 and G_2 using the generating sets T_1 and T_2, respectively, then $|G_1| = |G_2|$ and T_1 and T_2 have the same cardinality.

Unfortunately, the converse of the previous theorem is not true in general. That is, two groups that have the same order may or may not have a matching.

Loosely speaking, if two groups have a matching, then the two groups have the same structure and characteristics. In other words, the two groups essentially do the "same

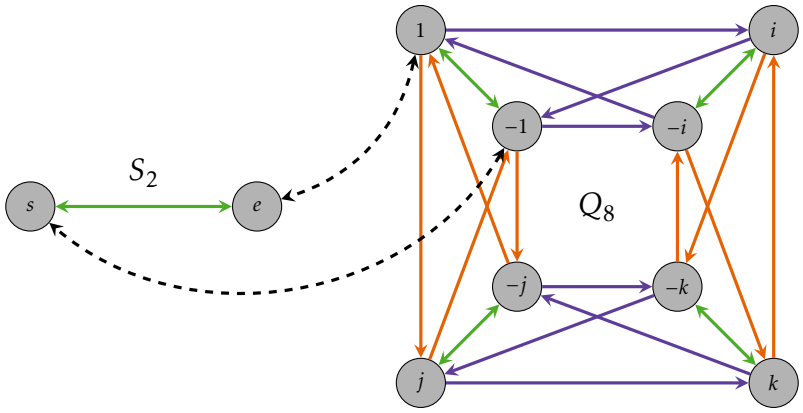


Figure 3.7. A matching between $S_2 = \langle s \rangle$ and $\langle -1 \rangle \leq Q_8$.

kind" of thing. In particular, the corresponding elements in each group have the same characteristics.

On the other hand, if one group has a property that the other does not have, then the two groups cannot have a matching. For example, if one group is abelian and the other is not, then the two groups cannot have a matching. Moreover, for each element g in one group with the property $g^k = e$ for some $k \in \mathbb{Z}$, there must be a corresponding element in the other group with the same property. Otherwise, there cannot be a matching between the two groups.

Problem 3.37. Determine whether there is a matching between D_4 and $\mathrm{Spin}_{1\times 2}$.

Problem 3.38. Determine whether there is a matching between R_4 and V_4.

Problem 3.39. Determine whether there is a matching between D_3 and R_6.

Problem 3.40. Determine whether there is a matching between any pair of the following groups: R_8 (i.e., the group of rotational symmetries of a regular octagon), D_4, Q_8.

Problem 3.41. Consider two light switches on a wall side by side. Consider the group of actions that consists of all possible actions that you can do to the two light switches. For example, one action is toggle the left light switch while leaving the right alone. Let's call this group L_2.

(a) How many distinct actions does L_2 have?

(b) Can you find a minimal generating set for L_2? If so, give these actions names and then write all of the actions of L_2 as words in your generator(s).

(c) Using your generating set from part (b), draw the corresponding Cayley diagram for L_2.

(d) Determine whether there is a matching between L_2 and either of R_4 or V_4.

Problem 3.42. Consider three light switches on a wall side by side. Consider the group of actions that consists of all possible actions that you can do to the three light switches. Let's call this group L_3. It should be easy to see that L_3 has 8 distinct actions.

(a) Can you find a minimal generating set for L_3? If so, give these actions names and then write all of the actions of L_3 as words in your generator(s).

(b) Using your generating set from part (a), draw the corresponding Cayley diagram for L_3.

(c) Is L_3 cyclic? Briefly justify your answer.

(d) Is L_3 abelian? Briefly justify your answer.

(e) Determine whether there is a matching between L_3 and any of R_8, D_4, $\text{Spin}_{1\times 2}$, or Q_8.

At the end of Section 2.5, we tinkered with coloring a group table. Let's revisit this idea. Suppose G is a finite group and consider the group table for G. A **coloring** for the group table is an assignment of a unique color to each element of the group. For example, Figure 3.8 depicts a coloring for the group table of V_4.

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

Figure 3.8. A coloring for the group table of V_4.

We say that two finite groups have an **identical table coloring**, if we can arrange the rows and columns of each table and choose colorings for each table so that the pattern of colors is the same for both tables. Clearly, this is only possible if the two groups have the same order. In Problem 2.66, we showed that R_4 and V_4 never have an identical table coloring.

Problem 3.43. Determine whether V_4 and L_2 have an identical table coloring.

Problem 3.44. Suppose there is a matching between finite groups G_1 and G_2. Explain why G_1 and G_2 must have an identical table coloring.

Problem 3.45. Is the converse of the previous problem true? That is, if G_1 and G_2 are finite groups that have an identical table coloring, will there be a matching between G_1 and G_2?

Problem 3.46. Suppose there is a matching between G_1 and G_2 and suppose T_1 is a generating set for G_1. Explain why there must be a generating set T_2 for G_2 and an appropriate choice of colors such that the Cayley diagrams for G_1 and G_2 using the generating sets T_1 and T_2, respectively, are identical up to relabeling of the vertices.

The last few problems have led us to the following theorem.

Theorem 3.47. If G_1 and G_2 are two finite groups, then there is a matching between G_1 and G_2 if and only if G_1 and G_2 have an identical table coloring.

As you've likely discovered, matchings and identical table coloring (or the lack thereof) are great for developing intuition about when two groups have identical structure, but the process of finding matchings and identical table colorings is cumbersome. Moreover, it turns out to not be a very useful approach for proving theorems. We need a different approach if we want to develop the general theory any further.

If two finite groups G_1 and G_2 have an identical table coloring, then

the product of corresponding elements yields the corresponding result.

This is the essence of what it means for two groups to have the same structure.

Let's try to make this a little more precise. Suppose $(G_1, *)$ and $(G_2, \odot)$ are two finite groups that have an identical table coloring and let $x_1, y_1 \in G_1$. Then these two elements have corresponding elements in the group table for G_2, say x_2 and y_2, respectively. In other words, x_1 and x_2 have the same color while y_1 and y_2 have the same color. Since G_1 is closed under its binary operation $*$, there exists $z_1 \in G_1$ such that $z_1 = x_1 * y_1$. But then there must exist a $z_2 \in G_2$ such that z_2 has the same color as z_1. What must be true of $x_2 \odot y_2$? Since the two tables exhibit the same color pattern, it must be the case that $z_2 = x_2 \odot y_2$. This is what it means for the product of corresponding elements to yield the corresponding result. Figure 3.9 illustrates this phenomenon for group tables.

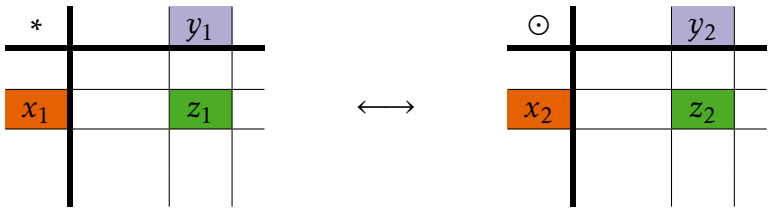


Figure 3.9

We can describe the identical table matching between G_1 and G_2 using a function. Let $\phi : G_1 \to G_2$ be the one-to-one and onto function that maps elements of G_1 to their corresponding elements in G_2. Then $\phi(x_1) = x_2$, $\phi(y_1) = y_2$, and $\phi(z_1) = z_2$. Since $z_2 = x_2 \odot y_2$, we obtain

$$\phi(x_1 * y_1) = \phi(z_1) = z_2 = x_2 \odot y_2 = \phi(x_1) \odot \phi(y_1).$$

In summary, it must be the case that

$$\phi(x_1 * y_1) = \phi(x_1) \odot \phi(y_1).$$

We are now prepared to state a formal definition of what it means for two groups to be isomorphic.

Definition 3.48. Let $(G_1, *)$ and $(G_2, \odot)$ be two groups. Then G_1 is **isomorphic** to G_2, written $G_1 \cong G_2$, if and only if there exists a one-to-one and onto function $\phi : G_1 \to G_2$ such that

$$\phi(x * y) = \phi(x) \odot \phi(y). \tag{3.1}$$

The function ϕ is referred to as an **isomorphism**. Equation 3.1 is often referred to as the **homomorphic property**.

It should be clear from the development that two finite groups are isomorphic if and only if they have an identical table coloring. Moreover, since two finite groups have an identical table coloring if and only if there is a matching between the two groups, it must be the case that two groups are isomorphic if and only if there is a matching between the two groups. The upshot is that we have three different ways to think about what it means for two groups to be isomorphic:

(1) There exists generating sets for the two groups such that the respective Cayley diagrams are identical up to relabeling of the vertices.

(2) There exists a choice of colors and an arrangement of the rows and columns of the group tables such that the two tables exhibit the same pattern of colors.

(3) There exists a bijective function between the two groups that satisfies the homomorphic property.

Problem 3.49. Using the work that you did earlier in this section, determine which of the following groups are isomorphic to each other: S_2, $\langle -1 \rangle$ in Q_8, R_3, R_4, V_4, L_2, $\langle i \rangle$ in Q_8, $\langle sr, sr^3 \rangle$ in D_4, R_5, R_6, D_3, S_3, R_7, R_8, D_4, $\mathrm{Spin}_{1\times 2}$, Q_8, L_3.

Problem 3.50. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$, where $\mathbb{R}^+$ is the set of positive real numbers. It turns out that these two groups are isomorphic, but this would be difficult to discover using our previous techniques because the groups are infinite. Define $\phi : \mathbb{R} \to \mathbb{R}^+$ via $\phi(r) = e^r$ (where e is the natural base, not the identity). Prove that ϕ is an isomorphism.

Problem 3.51. For each of the following pairs of groups, determine whether the given function is an isomorphism from the first group to the second group.

(a) $(\mathbb{Z}, +)$ and $(\mathbb{Z}, +)$, $\phi(n) = n + 1$.

(b) $(\mathbb{Z}, +)$ and $(\mathbb{Z}, +)$, $\phi(n) = -n$.

(c) $(\mathbb{Q}, +)$ and $(\mathbb{Q}, +)$, $\phi(x) = x/2$.

Problem 3.52. Show that the groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are isomorphic.

Perhaps one surprising consequence of the previous problem is that when dealing with infinite groups, a group can have a proper subgroup that it is isomorphic to. Of course, this never happens with finite groups.

Once we know that two groups are isomorphic, there are lots of interesting things we can say. The next theorem tells us that isomorphisms map the identity element of one group to the identity of the second group. This was already clear using Cayley diagrams and groups tables, but you should try to prove the theorem directly using Definition 3.48.

Theorem 3.53. Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$. If e_1 and e_2 are the identity elements of G_1 and G_2, respectively, then $\phi(e_1) = e_2$.

The next theorem tells us that isomorphisms respect inverses.

Theorem 3.54. If $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$, then $\phi(g^{-1}) = [\phi(g)]^{-1}$.

It turns out that "isomorphic" ($\cong$) determines an equivalence relation on the class of all possible groups. The next two theorems justify that $\cong$ is symmetric and transitive.

Theorem 3.55. If $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$, then the function $\phi^{-1} : G_2 \to G_1$ is an isomorphism.

Theorem 3.56. If $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ are isomorphisms from the groups $(G_1, *)$ to $(G_2, \odot)$ and $(G_2, \odot)$ to $(G_3, \star)$, respectively, then the composite function $\psi \circ \phi$ is an isomorphism of G_1 and G_3.

The only thing left to do in order to justify the next theorem is prove that $\cong$ is reflexive.

Theorem 3.57. If $\mathcal{G}$ is any nonempty collection of groups, then the relation $\cong$ is an equivalence relation on $\mathcal{G}$.

Mathematicians love to classify things. In particular, mathematicians want to classify groups. One can think of this pursuit as a taxonomy of groups. In order to simplify the task, one can classify isomorphism classes (i.e., the equivalence classes determined by $\cong$) instead of classifying groups. If two groups are isomorphic, then we say that the groups are **the same up to isomorphism**. If there are k isomorphism classes of order n, then we say that there are k **groups of order** n **up to isomorphism**.

Problem 3.58. Explain why all groups with a single element are isomorphic. Justify your answer using group tables.

In light of the previous problem, we say that there is one group of order one up to isomorphism.

Problem 3.59. Suppose that $(G, *)$ is a group of order 2 such that $G = \{e, a\}$. Complete the following group table for G.

$*$	e	a
e		
a		

Explain why every group of order 2 must be isomorphic to S_2.

The previous problem implies that up to isomorphism, there is only one group of order 2.

Problem 3.60. Suppose $(G, *)$ is a group of order 3 such that $G = \{e, a, b\}$. Complete the following group table for G.

$*$	e	a	b
e			
a			
b			

Explain why every group of order 3 must be isomorphic to R_3.

Problem 3.61. Suppose $(G,*)$ is a group of order 4 such that $G = \{e,a,b,c\}$. Assuming that e is the identity, the first row and first column of the corresponding group table must be completed as follows.

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

The cell with the question mark cannot be filled with an a. So, this entry must be either e, b, or c. However, it should be easy to see that the cases with b and c are symmetric. Thus, there are two cases: (i) the entry with the question mark is filled with e, or (ii) the entry with the question mark is without loss of generality filled with b. Complete the group table in each of these two cases. Are either of the resulting groups isomorphic to R_4 or V_4. What conclusion can you make about groups of order 4?

So far we've seen that there are unique groups up to isomorphism of orders 1, 2, and 3, but that there are two groups up to isomorphism of order 4. A natural question to ask is: how many groups are there of order n?

In a future chapter we will be able to prove that there is only one group up to isomorphism of order 5, namely those groups isomorphic to R_5.

We've seen three groups of order 6, namely R_6, D_3, and S_3. However, $D_3 \cong S_3$ while R_6 is not isomorphic to either of these. So, we can conclude that there are at least two groups up to isomorphism of order 6. But are there others? It turns out that the answer is no, but why?

The group R_7 is the group of rotational symmetries of a regular 7-sided polygon. This group has order 7. Are there other groups of order 7 that are not isomorphic to R_7? It turns out that the answer is no, but why?

We've encountered several groups of order 8, namely D_4, $\mathrm{Spin}_{1\times 2}$, Q_8, R_8, and L_3. Of these, only D_4 and $\mathrm{Spin}_{1\times 2}$ are isomorphic. Thus, there are at least four groups up to isomorphism of order 8. Are these the only isomorphism types? It turns out that there are five groups of order 8 up to isomorphism.

Let's return to proving some general statements about isomorphisms.

Theorem 3.62. Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1,*)$ to the group $(G_2,\odot)$. If G_1 is cyclic, then G_2 is cyclic.

Problem 3.63. Is the converse of Theorem 3.62 true? That is, if $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1,*)$ to the group $(G_2,\odot)$ and G_2 is cyclic, is G_1 necessarily cyclic? If the converse is true, then prove it. If the converse is false, provide a counterexample.

Theorem 3.64. Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$. If G_1 is abelian, then G_2 is abelian.

If $\phi : G_1 \to G_2$ is a function, not necessarily an isomorphism, and $X \subseteq G_1$, then the set

$$\phi(X) := \{y \in G_2 \mid \text{there exists } x \in X \text{ such that } \phi(x) = y\}$$

is called the **image** of X. The next theorem tells us that the image of a subgroup under an isomorphism is also a subgroup.

Theorem 3.65. If $\phi : G_1 \to G_2$ is an isomorphism and $H \leq G_1$, then $\phi(H) \leq G_2$.

Suppose G is a group and let $g \in G$. Define $\phi_g : G \to G$ via $\phi_g(x) = gxg^{-1}$. The map ϕ_g is called **conjugation** by g.

Problem 3.66. Consider the group D_4. Compute the image of each element of D_4 under each of the following conjugation maps.

(a) $\phi_g : D_4 \to D_4$ defined via $\phi_r(x) = rxr^{-1}$.

(b) $\phi_g : D_4 \to D_4$ defined via $\phi_s(x) = sxs^{-1}$.

The next theorem states that conjugation by a fixed group element yields an isomorphism from a group to itself. An isomorphism from a group to itself is called an **automorphism**. Conjugation is an example of an automorphism, but in general, there may be automorphisms that are not equal to conjugation. Note that the identity map is an automorphism of a group to itself that is equal to the map that results from conjugating by the identity.

Theorem 3.67. If G is a group and $g \in G$, then conjugation by g is an isomorphism from G to G.

Now that you've proved the above theorems, it's a good idea to review the key themes. If you were really paying attention, you may have noticed that in a few of the proofs, we did not use the fact that the function was one-to-one and onto despite assuming that the function was an isomorphism.

Problem 3.68. For which of the recent theorems could we remove either the assumption that the function is one-to-one or the assumption that the function is onto?

A function that satisfies the homomorphic property and may or may not be one-to-one or onto is called a **homomorphism** and will be the subject of a future chapter.

Problem 3.69. What claims can be made about the subgroup lattices of two groups that are isomorphic? What claims can be made about the subgroup lattices of two groups that are not isomorphic? What claims can be made about two groups if their subgroup lattices look nothing alike?

Chapter 4

Families of Groups

In this chapter we will explore a few families of groups, some of which we are already familiar with.

4.1 Cyclic Groups

Recall that if G is a group and $g \in G$, then the **cyclic subgroup generated by** g is given by

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

It is important to point out that $\langle g \rangle$ may be finite or infinite. In the finite case, the Cayley diagram with generator g gives us a good indication of where the word "cyclic" comes from (see Problem 4.21). If there exists $g \in G$ such that $G = \langle g \rangle$, then we say that G is a **cyclic group**.

Problem 4.1. List all of the elements in each of the following cyclic subgroups.

(a) $\langle r \rangle$, where $r \in D_3$

(b) $\langle r \rangle$, where $r \in R_4$

(c) $\langle rs \rangle$, where $rs \in D_4$

(d) $\langle r^2 \rangle$, where $r^2 \in R_6$

(e) $\langle i \rangle$, where $i \in Q_8$

(f) $\langle 6 \rangle$, where $6 \in \mathbb{Z}$ and the operation is ordinary addition

Problem 4.2. Consider the group of invertible 2×2 matrices with real number entries under the operation of matrix multiplication. This group is denoted by $\mathrm{GL}_2(\mathbb{R})$. List the elements in the cyclic subgroups generated by each of the following matrices.

(a) $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ (c) $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$

Problem 4.3. Determine whether each of the following groups is cyclic. If the group is cyclic, find at least one generator.

(a) S_2
(b) R_3
(c) R_4
(d) V_4
(e) R_5
(f) R_6
(g) D_3
(h) R_7
(i) R_8
(j) $\mathrm{Spin}_{1\times 2}$
(k) D_4
(l) Q_8

Problem 4.4. Determine whether each of the following groups is cyclic. If the group is cyclic, find at least one generator. If you believe that a group is not cyclic, try to sketch an argument.

(a) $(\mathbb{Z}, +)$
(b) $(\mathbb{R}, +)$
(c) $(\mathbb{R}^+, \cdot)$
(d) $(\{6^n \mid n \in \mathbb{Z}\}, \cdot)$
(e) $\mathrm{GL}_2(\mathbb{R})$ under matrix multiplication
(f) $\{(\cos(\pi/4) + i\sin(\pi/4))^n \mid n \in \mathbb{Z}\}$ under multiplication of complex numbers

Theorem 4.5. If G is a cyclic group, then G is abelian.

Problem 4.6. Provide an example of a finite group that is abelian but not cyclic.

Problem 4.7. Provide an example of an infinite group that is abelian but not cyclic.

Theorem 4.8. If G is a group and $g \in G$, then $\langle g \rangle = \langle g^{-1} \rangle$.

Theorem 4.9. If G is a cyclic group such that G has exactly one element that generates all of G, then the order of G is at most order 2.

Theorem 4.10. If G is a group such that G has no proper nontrivial subgroups, then G is cyclic.

Recall that the order of a group G, denoted $|G|$, is the number of elements in G. We define the **order** of an element g, written $|g|$, to be the order of $\langle g \rangle$. That is, $|g| = |\langle g \rangle|$. It is clear that G is cyclic with generator g if and only if $|G| = |g|$.

Problem 4.11. What is the order of the identity in any group?

Problem 4.12. Find the orders of each of the elements in each of the groups in Problem 4.3.

Problem 4.13. Consider the group $(\mathbb{Z}, +)$. What is the order of 1? Are there any elements in $\mathbb{Z}$ with finite order?

Problem 4.14. Find the order of each of the matrices in Problem 4.2.

The next result follows immediately from Theorem 4.8.

Theorem 4.15. If G is a group and $g \in G$, then $|g| = |g^{-1}|$.

The next result should look familiar and will come in handy a few times in this chapter. We'll take the result for granted and not worry about proving it.

Theorem 4.16 (Division Algorithm)**.** If n is a positive integer and m is any integer, then there exist unique integers q (called the **quotient**) and r (called the **remainder**) such that $m = nq + r$, where $0 \leq r < n$.

For the forward implication in the next theorem, if $\langle g \rangle$ is finite, then there exists distinct positive integers i and j such that $g^i = g^j$. Can you find a useful way to rewrite this equation? For the reverse implication, let $m \in \mathbb{Z}$ and use the Division Algorithm with m and n.

Theorem 4.17. Suppose G is a group and let $g \in G$. The subgroup $\langle g \rangle$ is finite if and only if there exists $n \in \mathbb{N}$ such that $g^n = e$.

Corollary 4.18. If G is a finite group, then for all $g \in G$, there exists $n \in \mathbb{N}$ such that $g^n = e$.

Note that Theorem 4.17 together with the Well-Ordering Principle guarantees the existence of a smallest positive integer n such that $g^n = e$ for every g in a finite group G. In the following theorem, the claim that the set contains n distinct elements is not immediate. You need to argue that there are no repeats in the list. Choose distinct $i, j \in \{0, 1, \ldots, n-1\}$ such that $i \neq j$ and then show that $g^i \neq g^j$. Consider a proof by contradiction and try to contradict the minimality of n.

Theorem 4.19. Suppose G is a group and let $g \in G$ such that $\langle g \rangle$ is a finite group. If n is the smallest positive integer such that $g^n = e$, then $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ and this set contains n distinct elements.

The next result provides an extremely useful interpretation of the order of an element.

Corollary 4.20. If G is a group and $g \in G$ such that $\langle g \rangle$ is a finite group, then the order of g is the smallest positive integer n such that $g^n = e$.

Problem 4.21. Suppose G is a finite cyclic group such that $G = \langle g \rangle$. Using the generating set $\{g\}$, what does the Cayley diagram for G look like?

Problem 4.22. Suppose G is a finite cyclic group of order n with generator g. If we write down the group table for G using $e, g, g^2, \ldots, g^{n-1}$ as the labels for the rows and columns, are there any interesting patterns in the table?

Problem 4.23. Notice that in the definition for $\langle g \rangle$, we allow the exponents on g to be negative. Explain why we only need to use positive exponents when $\langle g \rangle$ is a finite group.

The Division Algorithm should come in handy when proving the next theorem.

Theorem 4.24. Suppose G is a group and let $g \in G$ such that $|g| = n$. Then $g^i = g^j$ if and only if n divides $i - j$.

Corollary 4.25. Suppose G is a group and let $g \in G$ such that $|g| = n$. If $g^k = e$, then n divides k.

Recall that for $n \geq 3$, R_n is the group of rotational symmetries of a regular n-gon, where the operation is composition of actions.

Theorem 4.26. For all $n \geq 3$, R_n is cyclic.

Theorem 4.27. Suppose G is a finite cyclic group of order n. Then G is isomorphic to R_n if $n \geq 3$, S_2 if $n = 2$, and the trivial group if $n = 1$.

Most of the previous results have involved finite cyclic groups. What about infinite cyclic groups?

For the forward implication in the following theorem, try a proof by contradiction and suppose there exists integers i and j such that $g^i = g^j$.

Theorem 4.28. Suppose G is a group and let $g \in G$. The subgroup $\langle g \rangle$ is infinite if and only if each g^k is distinct for all $k \in \mathbb{Z}$.

Theorem 4.29. If G is an infinite cyclic group, then G is isomorphic to $\mathbb{Z}$ (under the operation of addition).

The upshot of Theorems 4.29 and 4.27 is that up to isomorphism, we know exactly what all of the cyclic groups are.

We now turn our attention to two new groups. Recall that two integers are **relatively prime** if the only positive integer that divides both of them is 1. That is, integers n and k are relatively prime if and only if $\gcd(n, k) = 1$.

Definition 4.30. Let $n \in \mathbb{N}$ and define the following sets.

(a) $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$

(b) $U_n := \{k \in \mathbb{Z}_n \mid \gcd(n, k) = 1\}$

Example 4.31. For example, $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ while $U_{12} = \{1, 5, 7, 11\}$ since 1, 5, 7, and 11 are the only elements in $\mathbb{Z}_{12}$ that are relatively prime to 12.

For each set in Definition 4.30, the immediate goal is to determine a binary operation that will yield a group. The key is to use modular arithmetic. Let n be a positive integer. To calculate the sum (respectively, product) of two integers modulo n (we say "mod n" for short), add (respectively, multiply) the two numbers and then find the remainder after dividing the sum (respectively, product) by n. For example, $4 + 9$ is 3 mod 5 since 13 has remainder 3 when divided by 5. Similarly, $4 \cdot 9$ is 1 mod 5 since 36 has remainder 1 when divided by 5. The hope is that these two operations turn $\mathbb{Z}_n$ and U_n into groups.

We write $i \equiv j \pmod{n}$, and say "i is equivalent to j modulo n" or "i is equal to j modulo n", if i and j both have the same remainder when divided by n. It is common to abbreviate "modulo" as "mod". It is also common to write $i \equiv_n j$, or even $i = j$ if the context is perfectly clear.

It is well-known, and not too hard to prove, that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. The corresponding equivalence classes are called congruence classes. The elements of a single congruence class are the integers that all have the same remainder when divided by n. According to the Division Algorithm, there are n congruence classes modulo n, one for each of the remainders $0, 1, \ldots, n-1$. We can think of $\mathbb{Z}_n$ as the set of canonical representatives of these equivalence classes.

Theorem 4.32. Let n be a positive integer and let $i, j \in \mathbb{Z}$. Then $i \equiv j \pmod{n}$ if and only if n divides $i - j$.

The next result follows immediately from Theorems 4.32 and 4.24.

Corollary 4.33. Suppose G is a group and let $g \in G$ such that $|g| = n$. Then $g^i = g^j$ if and only if $i \equiv j \pmod{n}$.

There are two things to prove in the next theorem. First, you need to prove that $\mathbb{Z}_n$ is a group under addition mod n, and then you need to argue that the group is cyclic.

Theorem 4.34. The set $\mathbb{Z}_n$ is a cyclic group under addition mod n.

Like the previous theorem, there are two things to prove for the next theorem. First, prove that U_n is a group under multiplication mod n, and then argue that the group is abelian.

Theorem 4.35. The set U_n is an abelian group under multiplication mod n.

Problem 4.36. Consider $\mathbb{Z}_4$.

(a) Find the group table for $\mathbb{Z}_4$.

(b) Is $\mathbb{Z}_4$ cyclic? If so, list elements of $\mathbb{Z}_4$ that individually generate $\mathbb{Z}_4$. If $\mathbb{Z}_4$ is not cyclic, explain why.

(c) Is $\mathbb{Z}_4$ isomorphic to either of R_4 or V_4? Justify your answer.

(d) Draw the subgroup lattice for $\mathbb{Z}_4$.

The next two problems illustrate that U_n may or may not be cyclic.

Problem 4.37. Consider $U_{10} = \{1, 3, 7, 9\}$.

(a) Find the group table for U_{10}.

(b) Is U_{10} cyclic? If so, list elements of U_{10} that individually generate U_{10}. If U_{10} is not cyclic, explain why.

(c) Is U_{10} isomorphic to either of R_4 or V_4? Justify your answer.

(d) Is U_{10} isomorphic to $\mathbb{Z}_4$? Justify your answer.

(e) Draw the subgroup lattice for U_{10}.

Problem 4.38. Consider $U_{12} = \{1, 5, 7, 11\}$.

(a) Find the group table for U_{12}.

(b) Is U_{12} cyclic? If so, list elements of U_{12} that individually generate U_{12}. If U_{12} is not cyclic, explain why.

(c) Is U_{12} isomorphic to either of R_4 or V_4? Justify your answer.

(d) Draw the subgroup lattice for U_{12}.

The upshot of the next theorem is that for $n \geq 3$, $\mathbb{Z}_n$ is just the set of exponents in the set $R_n = \{e, r, r^2, \ldots, r^{n-1}\}$ (where $e = r^0$).

Theorem 4.39. For $n \geq 3$, $\mathbb{Z}_n \cong R_n$. Moreover, $\mathbb{Z}_2 \cong S_2$ and $\mathbb{Z}_1$ is isomorphic to the trivial group.

The next result can be thought of as a repackaging of Theorems 4.27 and 4.29.

Theorem 4.40. Let G be a cyclic group. If the order of G is infinite, then G is isomorphic to $\mathbb{Z}$. If G has finite order n, then G is isomorphic to $\mathbb{Z}_n$.

Now that we have a complete description of the cyclic groups, let's focus our attention on subgroups of cyclic groups.

Theorem 4.41. Suppose G is a cyclic group. If $H \leq G$, then H is also cyclic.

It turns out that for proper subgroups, the converse of Theorem 4.41 is not true.

Problem 4.42. Provide an example of a group G such that G is not cyclic, but all proper subgroups of G are cyclic.

The next result officially settles Problem 3.17(d) and also provides a complete description of the subgroups of infinite cyclic groups up to isomorphism.

Corollary 4.43. The subgroups of $\mathbb{Z}$ are precisely the groups $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

Let's further explore finite cyclic groups. By Corollary 4.20, the order of g^m is the smallest positive exponent k such that $(g^m)^k = e$. To prove the next theorem, first verify that $k = \frac{n}{\gcd(n,m)}$ has the desired property and then verify that it is the smallest such exponent.

Theorem 4.44. If G is a finite cyclic group with generator g such that $|G| = n$, then for all $m \in \mathbb{Z}$, $|g^m| = \dfrac{n}{\gcd(n, m)}$.

Here is an extensive hint for proving the next theorem. Use Theorem 4.44 for the forward implication. For the reverse implication, first prove that for all $m \in \mathbb{Z}$, $\langle g^m \rangle = \langle g^{\gcd(m,n)} \rangle$ by proving two set containments. To show $\langle g^m \rangle \subseteq \langle g^{\gcd(m,n)} \rangle$, use the fact that there exists an integer q such that $m = q \cdot \gcd(m,n)$. For the reverse containment, you may freely use a fact known as Bezout's Lemma, which states that $\gcd(m,n) = nx + my$ for some integers x and y.

Theorem 4.45. If G is a finite cyclic group with generator g such that $|G| = n$, then $\langle g^m \rangle = \langle g^k \rangle$ if and only if $\gcd(m,n) = \gcd(k,n)$.

Problem 4.46. Suppose G is a cyclic group of order 12 with generator g.

(a) Find the orders of each of the following elements: g^2, g^7, g^8.

(b) Which elements of G individually generate G?

Corollary 4.47. Suppose G is a finite cyclic group with generator g such that $|G| = n$. Then $\langle g \rangle = \langle g^k \rangle$ if and only if n and k are relatively prime. That is, g^k generates G if and only if n and k are relatively prime.

Problem 4.48. Theorem 4.44, Theorem 4.45, and Corollary 4.47 are written using multiplicative notation. Rewrite both of these results using additive notation.

Problem 4.49. Consider $\mathbb{Z}_{18}$.

(a) Find all of the elements of $\mathbb{Z}_{18}$ that individually generate all of $\mathbb{Z}_{18}$.

(b) Draw the subgroup lattice for $\mathbb{Z}_{18}$. For each subgroup, list the elements of the corresponding set. Moreover, circle the elements in each subgroup that individually generate that subgroup. For example, $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$. In this case, we should circle 2, 4, 8, 10, 14, and 16 since each of these elements individually generate $\langle 2 \rangle$ and none of the remaining elements do. I'll leave it to you to figure out why this is true.

Problem 4.50. Repeat the above exercise, but this time use $\mathbb{Z}_{12}$ instead of $\mathbb{Z}_{18}$.

Corollary 4.51. If G is a finite cyclic group such that $|G| = p$, where p is prime, then G has no proper nontrivial subgroups.

Problem 4.52. If there is exactly one group up to isomorphism of order n, then to what group are all the groups of order n isomorphic?

Problem 4.53. Suppose G is a group and $x, y \in G$ such that $|x| = m$ and $|y| = n$. Is it true that $|xy| = mn$? If this is true, provide a proof. If this is not true, then provide a counterexample.

The punchline of the next two theorems is Theorem 4.56. To prove the next theorem, first verify that $(xy)^{mn} = e$ and then suppose $|xy| = k$. What do you immediately know about the relationship between k and mn? Next, consider $(xy)^{kn}$. Argue that m divides kn and then argue that m divides k. Similarly, n divides k. Ultimately, conclude that $mn = k$.

Theorem 4.54. Suppose G is a finite abelian group and let $x, y \in G$ such that $|x| = m$ and $|y| = n$. If $\gcd(m, n) = 1$, then $|xy| = mn$.

Here is a hint for proving the next theorem. Suppose $g \in G$ such that $|g| = n$. Let h be an arbitrary element in G such that $|h| = m$. You need to show that m divides n. For sake of a contradiction, assume otherwise. Then there exists a prime p whose multiplicity as a factor of m exceeds that of n. Let p^a be the highest power of p in m and p^b be the highest power of p in n, so $a > b$. Consider the elements g^{p^a} and h^{m/p^b}.

Theorem 4.55. Suppose G is a finite abelian group. If n is the maximal order among all elements in G, then the order of every element in G divides n.

Recall that every cyclic group is abelian (see Theorem 4.5). However, we know that not every abelian group is cyclic (see Problem 4.6). The next theorem tells us that abelian groups with some additional properties are cyclic.

Here is one method of attack for proving the next theorem. Let n be the maximal order among the elements of G and let $g \in G$ be an element with order n. Prove that $G = \langle g \rangle$.

Theorem 4.56. If G is a finite abelian group with at most one subgroup of any order, then G is cyclic.

Problem 4.57. Is the converse of Theorem 4.56 true for finite groups? That is, if G is a finite cyclic group, does that imply that G contains at most one subgroup of each order? If the answer is yes, then prove it. Otherwise, provide a counterexample.

We conclude this section with a couple interesting counting problems involving the number of generators of certain cyclic groups.

Problem 4.58. Let p and q be distinct primes. Find the number of generators of $\mathbb{Z}_{pq}$.

Problem 4.59. Let p be a prime. Find the number of generators of $\mathbb{Z}_{p^r}$, where r is an integer greater than or equal to 1.

4.2 Dihedral Groups

We can think of finite cyclic groups as groups that describe rotational symmetry. In particular, R_n is the group of rotational symmetries of a regular n-gon. Dihedral groups are those groups that describe both rotational and reflectional symmetry of regular n-gons.

Definition 4.60. For $n \geq 3$, the **dihedral group** D_n is defined to be the group consisting of the symmetry actions of a regular n-gon, where the operation is composition of actions.

For example, as we've seen, D_3 and D_4 are the symmetry groups of equilateral triangles and squares, respectively. The symmetry group of a regular pentagon is denoted by D_5. It is a well-known fact from geometry that the composition of two reflections in the plane is a rotation by twice the angle between the reflecting lines.

Theorem 4.61. The group D_n is a non-abelian group of order $2n$.

Theorem 4.62. Fix $n \geq 3$ and consider D_n. Let r be rotation clockwise by $360°/n$ and let s and s' be any two adjacent reflections of a regular n-gon. Then

(a) $D_n = \langle r, s \rangle = \{\underbrace{e, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}, \underbrace{s, sr, sr^2, \ldots, sr^{n-1}}_{\text{reflections}}\}$ and

(b) $D_n = \langle s, s' \rangle =$ all possible products of s and s'.

The next result is an obvious corollary of Theorem 4.62.

Corollary 4.63. For $n \geq 3$, $R_n \leq D_n$.

The following theorem generalizes many of the relations we have witnessed in the Cayley diagrams for the dihedral groups D_3 and D_4.

Theorem 4.64. Fix $n \geq 3$ and consider D_n. Let r be rotation clockwise by $360°/n$ and let s and s' be any two adjacent reflections of a regular n-gon. Then the following relations hold.

(a) $r^n = s^2 = (s')^2 = e$,

(b) $r^{-k} = r^{n-k}$ (special case: $r^{-1} = r^{n-1}$),

(c) $sr^k = r^{n-k}s$ (special case: $sr = r^{n-1}s$),

(d) $\underbrace{ss's\cdots}_{n \text{ factors}} = \underbrace{s'ss'\cdots}_{n \text{ factors}}$.

Problem 4.65. From Theorem 4.62, we know

$$D_n = \langle r, s \rangle = \{\underbrace{e, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}, \underbrace{s, sr, sr^2, \ldots, sr^{n-1}}_{\text{reflections}}\}.$$

If you were to create the group table for D_n so that the rows and columns of the table were labeled by $e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}$ (in exactly that order), do any patterns arise? Where are the rotations? Where are the reflections?

Problem 4.66. What does the Cayley diagram for D_n look like if we use $\{r, s\}$ as the generating set? What if we use $\{s, s'\}$ as the generating set?

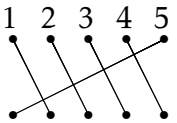
4.3 Symmetric Groups

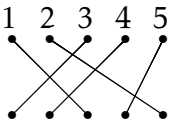
Recall the groups S_2 and S_3 from Problems 2.63 and 2.23. These groups act on two and three coins, respectively, that are in a row by rearranging their positions (but not flipping them over). These groups are examples of symmetric groups. In general, the **symmetric group** on n objects is the set of permutations that rearranges the n objects. The group operation is composition of permutations. Let's be a little more formal.

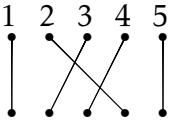
Definition 4.67. A **permutation of a set** A is a function $\sigma : A \to A$ that is both one-to-one and onto.

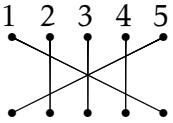
You should take a moment to convince yourself that the formal definition of a permutation agrees with the notion of rearranging the set of objects. The do-nothing action is the identity permutation, i.e., $\sigma(a) = a$ for all $a \in A$. There are many ways to represent a permutation. One visual way is using **permutation diagrams**, which we will introduce via examples.

Consider the following diagrams:

$\alpha =$ 

$\sigma =$ 

$\beta =$ 

$\gamma =$ 

Each of these diagrams represents a permutation on five objects. I've given the permutations the names α, β, σ, and γ. The intention is to read the diagrams from the top down. The numbers labeling the nodes along the top are identifying position. Following an edge from the top row of nodes to the bottom row of nodes tells us what position an object moves to. It is important to remember that the numbers are referring to the position of an object, not the object itself. For example, β is the permutation that sends the object in the second position to the fourth position, the object in the third position to the second position, and the object in the fourth position to the third position. Moreover, the permutation β doesn't do anything to the objects in positions 1 and 5.

Problem 4.68. Describe in words what the permutations σ and γ do.

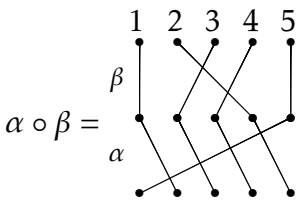
Problem 4.69. Draw the permutation diagram for the do-nothing permutation on 5 objects. This is called the **identity permutation**. What does the identity permutation diagram look like in general for arbitrary n?

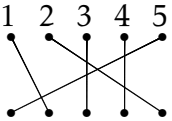
Definition 4.70. The set of all permutations on n objects is denoted by S_n.

Problem 4.71. Draw all the permutation diagrams for the permutations in S_3.

Problem 4.72. How many distinct permutations are there in S_4? How about S_n for any $n \in \mathbb{N}$?

If S_n is going to be a group, we need to know how to compose permutations. This is easy to do using the permutation diagrams. Consider the permutations α and β from earlier. We can represent the composition $\alpha \circ \beta$ via

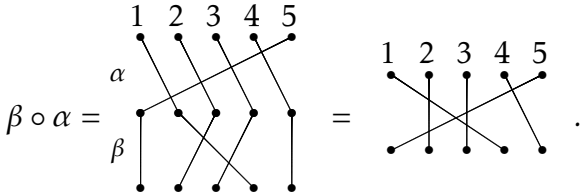
$\alpha \circ \beta =$ 

$=$ 

.

As you can see by looking at the figure, to compose two permutations, you stack the one that goes first in the composition (e.g., β in the example above) on top of the other and just follow the edges from the top through the middle to the bottom. If you think about how function composition works, this is very natural. The resulting permutation is determined by where we begin and where we end in the composition.

We already know that the order of composition matters for functions, and so it should matter for the composition of permutations. To make this crystal clear, let's compose α and β in the opposite order. We see that



The moral of the story is that composition of permutations does not necessarily commute.

Problem 4.73. Consider α, β, σ, and γ from earlier. Can you find a pair of permutations that do commute? Can you identify any features about your diagrams that indicate why they commuted?

Problem 4.74. Fix $n \in \mathbb{N}$. Convince yourself that any $\rho \in S_n$ composed with the identity permutation (in either order) equals ρ.

If S_n is going to be a group, we need to know what the inverse of a permutation is.

Problem 4.75. Given a permutation $\rho \in S_n$, describe a method for constructing ρ^{-1}. Briefly justify that $\rho \circ \rho^{-1}$ will yield the identity permutation.

At this point, we have all the ingredients we need to prove that S_n forms a group under composition of permutations.

Theorem 4.76. The set of permutations on n objects forms a group under the operation of composition. That is, $(S_n, \circ)$ is a group. Moreover, $|S_n| = n!$.

Note that it is standard convention to omit the composition symbol when writing down compositions in S_n. For example, we will simply write $\alpha\beta$ to denote $\alpha \circ \beta$.

Permutation diagrams are fun to play with, but we need a more efficient way of encoding information. There are several compact and efficient notations for describing permutations in S_n. For our purposes, it will be handy for us to describe permutations using **cycle notation**. The **cycle** $(a_1, a_2, \ldots, a_m)$ is the permutation that sends a_i to a_{i+1} for $1 \leq i \leq m-1$ and sends a_m to a_1. In general, for each $\sigma \in S_n$, the numbers 1 through n will be rearranged and grouped into k cycles of the form

$$(a_1, a_2, \ldots, a_{m_1})(a_{m_1+1}, a_{m_1+2}, \ldots, a_{m_2}) \cdots (a_{m_{k-1}+1}, a_{m_{k-1}+2}, \ldots, a_{m_k})$$

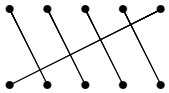
from which the action of σ on any number from 1 to n can easily be determined. In particular, for any $i \in \{1, 2, \ldots, n\}$, locate i in the expression above. Then $\sigma(i)$ is the next number in the corresponding cycle that is cyclicly to the right (i.e., if i is not at the right

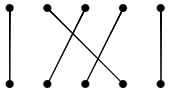
end of a cycle, $\sigma(i)$ is the next number to the right, while if i is at the right end of a cycle, $\sigma(i)$ is the number at the left end of the same cycle. The product of all the cycles is called the **cycle decomposition** of σ.

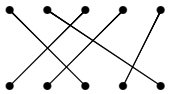
Notice that we can start writing a cycle with any of the numbers appearing in the cycle. What matters is that each number in the cycle is followed by the appropriate number. For example, $(1,3,2) = (3,2,1) = (2,1,3)$. The **length** of a cycle is the number of entries appearing in it. If a cycle has length m, then it is called an m-**cycle**. Two cycles are said to be **disjoint** if they have no entries in common.

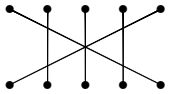
Example 4.77. Consider $\sigma = (1,12,8,10,4)(2,13)(3)(5,11,7)(6,9)$ in S_{13}. This cycle decomposition for σ consists of five pairwise disjoint cycles: a 5-cycle, a 2-cycle, a 1-cycle, a 3-cycle, and another 2-cycle. For convenience, it is common to omit any 1-cycles in the decomposition. So, we may also write $\sigma = (1,12,8,10,4)(2,13)(5,11,7)(6,9)$, keeping in mind that the absence of a number means that the permutation maps that number to itself.

Example 4.78. Consider α, β, σ, and γ in S_5 that we had previously drawn permutation diagrams for. Below I have indicated what each permutation is equal to using cycle notation.

$\alpha =$  $= (1,2,3,4,5)$

$\beta =$  $= (2,4,3)$

$\sigma =$  $= (1,3)(2,5,4)$

$\gamma =$  $= (1,5)$

Example 4.79. The cycle decomposition of the identity permutation in S_n is $(1)(2)\cdots(n)$. It is common to simply write this as (1), again keeping in mind that the the absence of a number means that the permutation maps that number to itself. One disadvantage to this approach is that we lose information about what n is.

Problem 4.80. Suppose $\sigma \in S_9$ is defined by

$$\sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 1, \sigma(4) = 9, \sigma(5) = 8, \sigma(6) = 2, \sigma(7) = 5, \sigma(8) = 7, \sigma(9) = 6.$$

Find the cycle decomposition of σ. What are the lengths of the corresponding cycles?

Problem 4.81. Write down all 6 elements in S_3 using cycle notation.

Problem 4.82. Write down all 24 elements in S_4 using cycle notation.

Suppose $\sigma \in S_n$. Since σ is a bijection, it is clear that it is possible to write σ as a product of disjoint cycles such that each $i \in \{1, 2, \ldots, n\}$ appears exactly once.

Let's see if we can figure out how to multiply elements of S_n using cycle notation. Consider the permutations $\alpha = (1, 3, 2)$ and $\beta = (3, 4)$ in S_4. To compute the composition $\alpha\beta = (1, 3, 2)(3, 4)$, let's explore what happens in each position. Since we are doing function composition, we should work our way from right to left. Since 1 does not appear in the cycle notation for β, we know that $\beta(1) = 1$ (i.e., β maps 1 to 1). Now, we see what $\alpha(1) = 3$. Thus, the composition $\alpha\beta$ maps 1 to 3 (since $\alpha\beta(1) = \alpha(\beta(1)) = \alpha(1) = 3$). Next, we should return to β and see what happens to 3—which is where we ended a moment ago. We see that β maps 3 to 4 and then α maps 4 to 4 (since 4 does not appear in the cycle notation for α). So, $\alpha\beta(3) = 4$. Continuing this way, we see that β maps 4 to 3 and α maps 3 to 2, and so $\alpha\beta$ maps 4 to 2. Lastly, since $\beta(2) = 2$ and $\alpha(2) = 1$, we have $\alpha\beta(2) = 1$. Putting this altogether, we see that $\alpha\beta = (1, 3, 4, 2)$. Now, you should try a few. Things get a little trickier if the composition of two permutations results in a permutation consisting of more than a single cycle.

Problem 4.83. Consider α, β, σ, and γ for which we drew the permutation diagrams. Using cycle notation, compute each of the following.

(a) $\alpha\gamma$

(b) $\gamma\alpha$

(c) $\sigma\alpha$

(d) $\alpha\sigma$

(e) β^2

(f) β^3

(g) β^4

(h) σ^3

(i) σ^6

Problem 4.84. Write down the group table for S_3 using cycle notation.

In Problem 4.82, one of the permutations you should have written down is $(1, 2)(3, 4)$. This is a product of two disjoint 2-cycles. It is worth pointing out that each cycle is a permutation in its own right. That is, $(1, 2)$ and $(3, 4)$ are each permutations. It just so happens that their composition does not "simplify" any further. Moreover, these two disjoint 2-cycles commute since $(1, 2)(3, 4) = (3, 4)(1, 2)$. In fact, this phenomenon is always true.

Theorem 4.85. Suppose α and β are two disjoint cycles. Then $\alpha\beta = \beta\alpha$. That is, products of disjoint cycles commute.

Problem 4.86. Compute the orders of all the elements in S_3. See Problem 4.81.

Problem 4.87. Compute the orders of any twelve of the elements in S_4. See Problem 4.82.

Computing the order of a permutation is fairly easy using cycle notation once we figure out how to do it for a single cycle. In fact, you've probably already guessed at the following theorem.

Theorem 4.88. If $\alpha \in S_n$ such that α consists of a single k-cycle, then $|\alpha| = k$.

Recall that $\text{lcm}(k_1, \ldots, k_m)$ is the **least common multiple** of $\{k_1, \ldots, k_m\}$.

Theorem 4.89. Suppose $\alpha \in S_n$ such that α consists of m disjoint cycles of lengths $k_1, \ldots, k_m$. Then $|\alpha| = \text{lcm}(k_1, \ldots, k_m)$.

Problem 4.90. Is the previous theorem true if we do not require the cycles to be disjoint? Justify your answer.

Problem 4.91. What is the order of $(1,4,7)(2,5)(3,6,8,9)$?

Problem 4.92. Draw the subgroup lattice for S_3.

Problem 4.93. Now, using $(1,2)$ and $(1,2,3)$ as generators, draw the Cayley diagram for S_3. Look familiar?

Problem 4.94. Consider S_3. It turns out that $S_3 = \langle (1,2), (1,3), (2,3) \rangle$.

(a) Using $(1,2)$, $(1,3)$, and $(2,3)$ as generators, draw the Cayley diagram for S_3.

(b) Is $\{(1,2), (1,3), (2,3)\}$ a minimal generating set for S_3? If so, explain why. If not, find a subset of $\{(1,2), (1,3), (2,3)\}$ that is a minimal generating set.

Problem 4.95. Recall that there are $4! = 24$ permutations in S_4.

(a) Pick any 12 permutations from S_4 and verify that you can write them as words in the 2-cycles $(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)$. In most circumstances, your words will not consist of products of disjoint 2-cycles. For example, the permutation $(1,2,3)$ can be decomposed into $(1,2)(2,3)$, which is a word consisting of two 2-cycles that happen to not be disjoint.

(b) Using your same 12 permutations, verify that you can write them as words only in the 2-cycles $(1,2), (2,3), (3,4)$.

By the way, it might take some trial and error to come up with a way to do this. Moreover, there is more than one way to do it.

As the previous exercises hinted at, the 2-cycles play a special role in the symmetric groups. In fact, they have a special name. A **transposition** is a single cycle of length 2. In the special case that the transposition is of the form $(i, i+1)$, we call it an **adjacent transposition**. For example, $(3,7)$ is a (non-adjacent) transposition while $(6,7)$ is an adjacent transposition.

It turns out that the set of transpositions in S_n is a generating set for S_n. In fact, the adjacent transpositions form an even smaller generating set for S_n. To get some intuition, let's play with a few examples.

Problem 4.96. Try to write each of the following permutations as a product of transpositions. You do not necessarily need to use adjacent transpositions.

(a) $(3,1,5)$

(b) $(2,4,6,8)$

(c) $(3,1,5)(2,4,6,8)$

(d) $(1,6)(2,5,3)$

The products you found in the previous exercise are called **transposition representations** of the given permutation.

Problem 4.97. Consider the arbitrary k-cycle $(a_1, a_2, \ldots, a_k)$ from S_n (with $k \leq n$). Find a way to write this permutation as a product of 2-cycles.

Problem 4.98. Consider the arbitrary 2-cycle (a, b) from S_n. Find a way to write this permutation as a product of adjacent 2-cycles.

The previous two problems imply the following theorem.

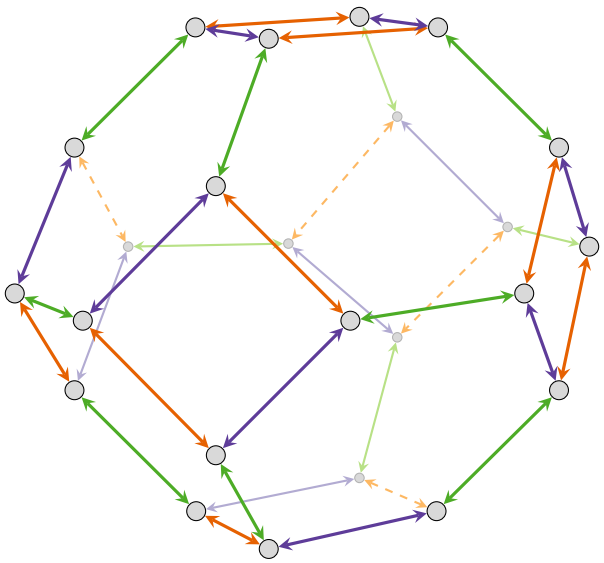
Theorem 4.99. Consider S_n.

(a) Every permutation in S_n can be written as a product of transpositions.

(b) Every permutation in S_n can be written as a product of adjacent transpositions.

Corollary 4.100. The set of transpositions (respectively, the set of adjacent transpositions) from S_n forms a generating set for S_n.

Problem 4.101. The following diagram is an unlabeled version of the Cayley diagram for S_4 using the adjacent transpositions $(1,2)$, $(2,3)$, and $(3,4)$ as generators. Pick a vertex to correspond to the identity, make a suitable choice for which arrows correspond to which generators, and then label the remaining vertices with permutations in S_4. The graph given below is drawn on the a three-dimensional solid called the **permutahedron** (which is a **truncated octahedron**).

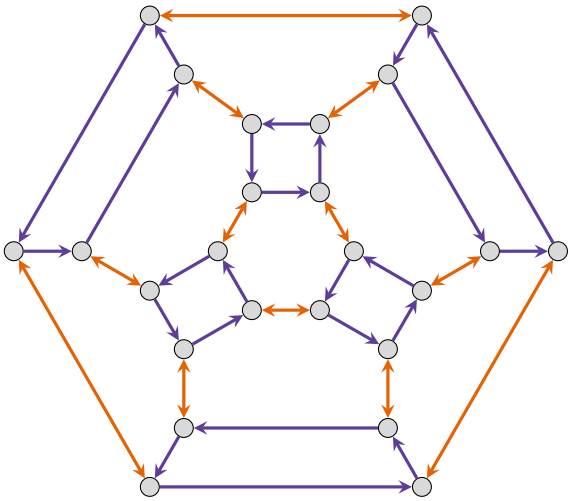


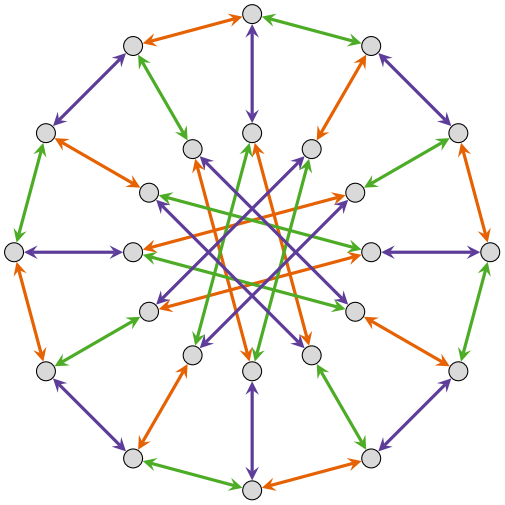
It is important to point out that the transposition representation of a permutation is not unique. That is, there are many words in the transpositions that will equal the same permutation. This is exhibited in the previous problem where there are multiple paths from the vertex corresponding to the identity to another vertex in the Cayley diagram for S_4 using the adjacent transpositions as the generators. However, as we shall see in the next section, given two transposition representations for the same permutation, the number of transpositions will have the same parity (i.e., even versus odd).

Problem 4.102. It turns out that

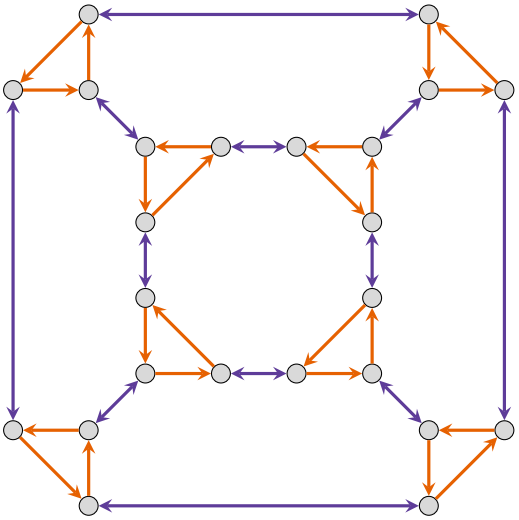
$$S_4 = \langle (1,2),(1,3),(1,4) \rangle = \langle (1,2,3,4),(1,2) \rangle.$$

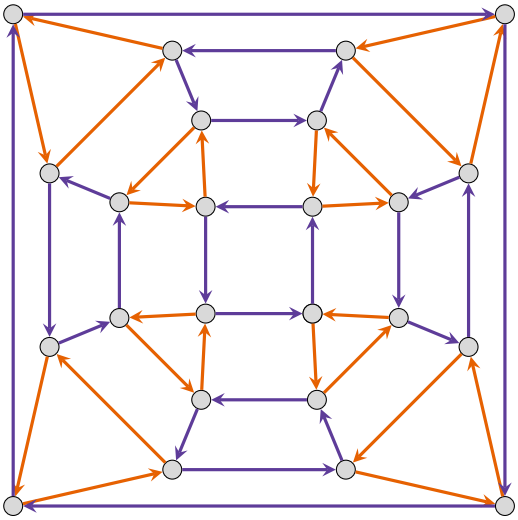
Determine which of the generating sets listed above yield each of the Cayley diagrams given below. Label the vertices in each diagram with permutations (written in cycle notation as a product of disjoint cycles) of S_4. The graph on the right is sometimes called the **Nauru graph**.





Problem 4.103. Two Cayley diagrams for the symmetric group S_4 are given below.





Determine what generating sets will yield these Cayley diagrams. Then label the nodes with permutations in cycle notation, written as a product of disjoint cycles.

Here is an interesting fact that I will let you ponder. The group of rigid motion symmetries for a cube is isomorphic to S_4. Is there a Cayley diagram in one of the last two problems that helps you visualize this fact?

4.4 Permutation Groups and Cayley's Theorem

It turns out that the subgroups of symmetric groups play an important role in group theory.

Definition 4.104. Every subgroup of a symmetric group is called a **permutation group**.

The proof of the following theorem isn't too bad, but we'll take it for granted. After tinkering with a few examples, you should have enough intuition to see why the theorem is true and how a possible proof might go.

Theorem 4.105 (Cayley's Theorem)**.** Every finite group is isomorphic to some permutation group. In particular, if G is a group of order n, then G is isomorphic to a subgroup of S_n.

Cayley's Theorem guarantees that every finite group is isomorphic to a permutation group and it turns out that there is a rather simple algorithm for constructing the corresponding permutation group. I'll briefly explain an example and then let you try a couple.

Consider the Klein four-group $V_4 = \{e, v, h, vh\}$. Recall that V_4 has the following group table.

$*$	e	v	h	vh
e	e	v	h	vh
v	v	e	vh	h
h	h	vh	e	v
vh	vh	h	v	e

If we number the elements e, v, h, and vh as $1, 2, 3$, and 4, respectively, then we obtain the following table.

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Comparing each of the four columns to the leftmost column, we can obtain the corresponding permutations. In particular, we obtain

$$\begin{aligned} e &\leftrightarrow (1) \\ v &\leftrightarrow (1,2)(3,4) \\ h &\leftrightarrow (1,3)(2,4) \\ vh &\leftrightarrow (1,4)(2,3). \end{aligned}$$

Do you see where these permutations came from? The claim is that the set of permutations $\{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ is isomorphic to V_4. In this particular case, it's fairly clear that this is true. However, it takes some work to prove that this process will always result in an isomorphic permutation group. In fact, verifying the algorithm is essentially the proof of Cayley's Theorem.

Since there are potentially many ways to rearrange the rows and columns of a given table, it should be clear that there are potentially many isomorphisms that could result from the algorithm described above.

Here's another way to obtain a permutation group that is isomorphic to a given group. Let's consider V_4 again. Recall that V_4 is a subset of D_4, which is the symmetry group for a square. Alternatively, V_4 is the symmetry group for a non-square rectangle. Label the corners of the rectangle 1, 2, 3, and 4 by starting in the upper left corner and continuing clockwise. Recall that v is the action that reflects the rectangle over the vertical midline. The result of this action is that the corners labeled by 1 and 2 switch places and the corners labeled by 3 and 4 switch places. Thus, v corresponds to the permutation $(1,2)(3,4)$. Similarly, h swaps the corners labeled by 1 and 4 and the corners labeled by 2 and 3, and so h corresponds to the permutation $(1,4)(2,3)$. Notice that this is not the same answer we got earlier and that's okay as there may be many permutation representations for a given group. Lastly, vh rotates the rectangle 180° which sends ends up swapping corners labeled 1 and 3 and swapping corners labeled by 2 and 4. Therefore, vh corresponds to the permutation $(1,3)(2,4)$.

Problem 4.106. Consider D_4.

(a) Using the method outlined above, find a subgroup of S_8 that is isomorphic to D_4.

(b) Label the corners of a square 1–4. Find a subgroup of S_4 that is isomorphic to D_4 by considering the natural action of D_4 on the labels on the corners of the square.

Problem 4.107. Consider $\mathbb{Z}_6$.

(a) Using the method outlined earlier, find a subgroup of S_6 that is isomorphic to $\mathbb{Z}_6$.

(b) Label the corners of a regular hexagon 1–6. Find a subgroup of S_6 that is isomorphic to $\mathbb{Z}_6$ by considering the natural action of $\mathbb{Z}_6$ on the labels on the corners of the hexagon.

4.5 Alternating Groups

In this section, we describe a special class of permutation groups. To get started, let's play with a few exercises.

Problem 4.108. Write down every permutation in S_3 as a product of 2-cycles in the most efficient way you can find (i.e., use the fewest possible transpositions). Now, write every permutation in S_3 as a product of adjacent 2-cycles, but don't worry about whether your decompositions are efficient. Any observations about the number of transpositions you used in each case? Think about even versus odd.

Theorem 4.109. If $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a collection of 2-cycles in S_n such that $\alpha_1\alpha_2\cdots\alpha_k = (1)$, then k must be even.

Proof. Suppose $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a collection of 2-cycles in S_n such that $\alpha_1\alpha_2\cdots\alpha_k = (1)$. We need to show that k is even. We proceed by strong induction. First, it is clear that the statement is not true when $k = 1$, but is true when $k = 2$.

Now, assume that $k > 2$ and if $j \leq k-1$ and we have a product of j 2-cycles that equals the identity, then j is even. Consider $\alpha_1\alpha_2$. The only possibilities are:

(i) $\alpha_1\alpha_2 = (a,b)(a,b)$,

(ii) $\alpha_1\alpha_2 = (a,b)(a,c)$,

(iii) $\alpha_1\alpha_2 = (a,b)(c,d)$,

(iv) $\alpha_1\alpha_2 = (a,b)(b,c)$.

If case (i) happens, then

$$(1) = \alpha_1\alpha_2\cdots\alpha_k = \alpha_3\alpha_4\cdots\alpha_k.$$

Since the expression on the right consists of $k-2$ factors, $k-2$ must be even by induction, which implies that k is even. Now, suppose we are in one of cases (ii), (iii), or (iv). Observe that:

(ii) $(a,b)(a,c) = (b,c)(a,b)$,

(iii) $(a,b)(c,d) = (c,d)(a,b)$,

(iv) $(a,b)(b,c) = (b,c)(a,c)$.

In each case, we were able to move a from the original left 2-cycle to a new right 2-cycle. That is, we were able to rewrite $\alpha_1\alpha_2$ so that a does not appear in the left 2-cycle. Systematically repeat this process for the pairs $\alpha_2\alpha_3$, $\alpha_3\alpha_4, \ldots, \alpha_{k-1}\alpha_k$. If we ever encounter case (i) along the way, then we are done by induction. Otherwise, we are able to rewrite $\alpha_1\alpha_2\cdots\alpha_k$ so that a only appears in the rightmost 2-cycle. But this implies that $\alpha_1\alpha_2\cdots\alpha_k$ does not fix a, which contradicts $\alpha_1\alpha_2\cdots\alpha_k = (1)$. This implies that at some point we must encounter case (i), and hence k is even by induction. □

Theorem 4.110. If $\sigma \in S_n$, then every transposition representation of σ has the same parity.

The previous theorem tells us that the following definition is well-defined.

Definition 4.111. A permutation is **even** (respectively, **odd**) if one of its transposition representations consists of an even (respectively, odd) number of transpositions.

Problem 4.112. Classify all of the permutations in S_3 as even or odd.

Problem 4.113. Classify all of the permutations in S_4 as even or odd.

Problem 4.114. Identify the even permutations in the Cayley diagrams for S_4 given in Problems 4.102 and 4.103. Notice any nice patterns?

Problem 4.115. Determine whether $(1,4,2,3,5)$ is even or odd. How about $(1,4,2,3,5)(7,9)$?

Problem 4.116. Consider the arbitrary k-cycle $(a_1, a_2, \ldots, a_k)$ from S_n (with $k \leq n$). When will this cycle be odd versus even? Briefly justify your answer.

Problem 4.117. Conjecture a statement about when a permutation will be even versus odd. Briefly justify your answer.

And finally, we are ready to introduce the alternating groups.

Definition 4.118. The set of all even permutations in S_n is denoted by A_n and is called the **alternating group**.

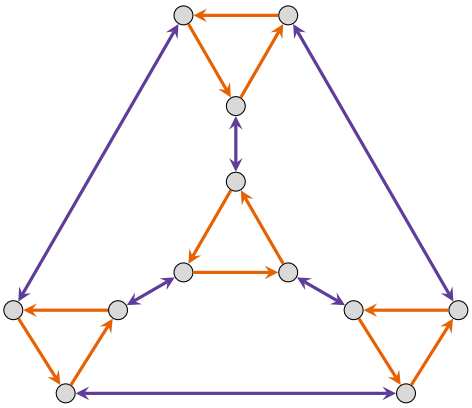
Since we referred to A_n as a group, it darn well better be a group! To show that A_n is a group, argue that A_n is a subgroup of S_n using the Two-Step Subgroup Test (see Theorem 3.6). As expected, for $n > 1$, the order of A_n is exactly half the order of S_n. To show that $|A_n| = n!/2$ for $n > 1$, prove that the number of even permutations in S_n is the same as the number of odd permutations in S_n. Here is one way to accomplish this. Define $f : A_n \to S_n \setminus A_n$ via $f(\sigma) = (1,2)\sigma$. Note that $S_n \setminus A_n$ is the set of odd permutations in S_n. Show that f is a bijection.

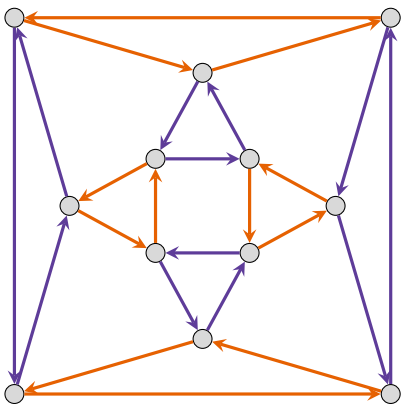
Theorem 4.119. The set A_n forms a group under composition of permutations and has order $n!/2$ when $n > 1$.

Problem 4.120. Find A_3. What group is A_3 isomorphic to?

Problem 4.121. Find A_4 and then draw its subgroup lattice. Is A_4 abelian?

Problem 4.122. Two Cayley diagrams for A_4 are shown below.





Determine what generating sets will yield these Cayley diagrams. Then label the nodes with permutations in cycle notation, written as a product of disjoint cycles.

Problem 4.123. What is the order of A_5? Is A_5 abelian?

Problem 4.124. What orders of elements occur in S_6 and A_6? What about S_7 and A_7?

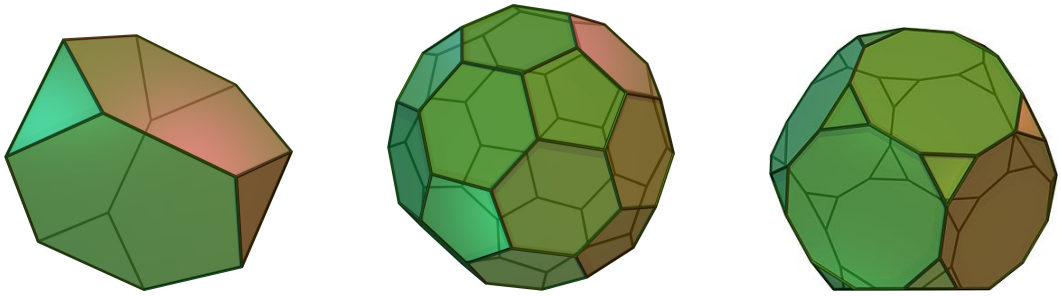
Problem 4.125. Does A_8 contain an element of order 15? If so, find one. If not, explain why no such element exists.

Remark 4.126. Below are a few interesting facts about A_4 and A_5, which we will state without proof.

(a) The group of rigid motion symmetries for a regular tetrahedron is isomorphic to A_4.

(b) You can arrange the Cayley diagram for A_4 with generators $(1,2)(3,4)$ and $(2,3,4)$ (see the left diagram in Problem 4.122) on a truncated tetrahedron, which is depicted in Figure 4.1(a).

(c) You can arrange the Cayley diagram for A_5 with generators $(1,2)(3,4)$ and $(1,2,3,4,5)$ on a truncated icosahedron, which is given in Figure 4.1(b). You can also arrange the Cayley diagram for A_5 with generators $(1,2,3)$ and $(1,5)(2,4)$ on a truncated dodecahedron seen in Figure 4.1(c).



(a) (b) (c)

Figure 4.1. Truncated tetrahedron, truncated icosahedron, and truncated dodecahedron. [Image source: Wikipedia]

Chapter 5

Cosets, Lagrange's Theorem, and Normal Subgroups

5.1 Cosets

Undoubtably, you've noticed numerous times that if G is a group with $H \leq G$ and $g \in G$, then both $|H|$ and $|g|$ divide $|G|$. The theorem that says this is always the case is called Lagrange's theorem and we'll prove it towards the end of this chapter. We begin with a definition.

Definition 5.1. Let G be a group and let $H \leq G$ and $a \in G$. The subsets

$$aH := \{ah \mid h \in H\}$$

and

$$Ha := \{ha \mid h \in H\}$$

are called the **left** and **right cosets of** H **containing** a, respectively.

To gain some insight, let's tinker with an example. Consider the dihedral group $D_3 = \langle r, s \rangle$ and let $H = \langle s \rangle \leq D_3$. To compute the right cosets of H, we need to multiply all of the elements of H on the right by the elements of G. We see that

$$\begin{aligned}
He &= \{ee, se\} = \{e, s\} = H \\
Hr &= \{er, sr\} = \{r, sr\} \\
Hr^2 &= \{er^2, sr^2\} = \{r^2, rs\} \\
Hs &= \{es, ss\} = \{s, e\} = H \\
Hsr &= \{esr, ssr\} = \{sr, r\} \\
Hrs &= \{ers, srs\} = \{rs, ssr^2\} = \{rs, r^2\}.
\end{aligned}$$

Despite the fact that we made six calculations (one for each element in D_3), if we scan the list, we see that there are only 3 distinct cosets, namely

$$\begin{aligned}
H = He = Hs &= \{e, s\} \\
Hr = Hsr &= \{r, sr\} \\
Hr^2 = Hrs &= \{r^2, rs\}.
\end{aligned}$$

We can make a few more observations. First, the resulting cosets formed a partition of D_3. That is, every element of D_3 appears in exactly one coset. Moreover, all the cosets are the same size—two elements in each coset in this case. Lastly, each coset can be named in multiple ways. In particular, the elements of the coset are exactly the elements of D_3 we multiplied H by. For example, $Hr = Hsr$ and the elements of this coset are r and sr. Shortly, we will see that these observations hold, in general.

Here is another significant observation we can make. Consider the Cayley diagram for D_3 with generating set $\{r, s\}$ that is given in Figure 5.1. Given this Cayley diagram, we can visualize the subgroup H and its clones (see Section 3.1 for a reminder of what a clone is). Moreover, H and its clones are exactly the 3 right cosets of H. We'll see that, in general, the *right* cosets of a given subgroup are always the subgroup and its clones (see Problem 5.15).

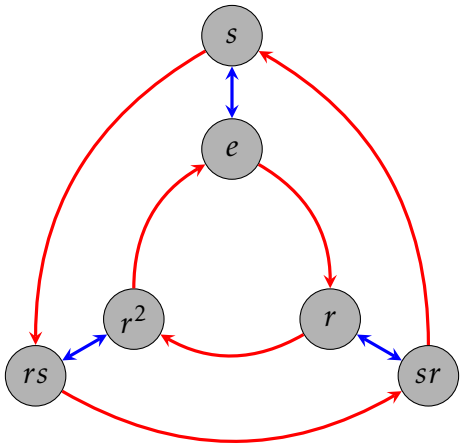


Figure 5.1. Cayley diagram for D_3 with generating set $\{r, s\}$.

Problem 5.2. Consider the group D_3. Find all the left cosets for $H = \langle s \rangle$. Are they the same as the right cosets? Are they the same as the subgroup H and its clones that we can see in the Cayley graph for D_3 with generating set $\{r, s\}$?

As the previous exercise indicates, the collections of left and right cosets may not be the same and when they are not the same, the subgroup and its clones do not coincide with the left cosets.

You might be thinking that somehow right cosets are "better" than left cosets since we were able to visualize them in the Cayley graph. However, this is just a consequence of our convention of composing actions from right to left. If we had adopted a left to right convention, then we would be able to visualize the left cosets in Cayley diagrams.

Computing left and right cosets using a group table is fairly easy. Hopefully, you figured out in Problem 5.2 that the left cosets of $H = \langle s \rangle$ in D_3 are $H = \{e, s\}$, $srH = \{r^2, sr\}$, and $rsH = \{r, rs\}$. Now, consider the following group table for D_3 that has the rows and columns arranged according to the left cosets of H.

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

The left coset srH must appear in the row labeled by sr and in the columns labeled by the elements of $H = \{e, s\}$. We've depicted this below.

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

On the other hand, the right coset Hsr must appear in the column labeled by sr and the rows labeled by the elements of $H = \{e, s\}$:

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

As we can see from the tables, $srH \neq Hsr$ since $\{sr, r^2\} \neq \{sr, r\}$. If we color the entire group table for D_3 according to which *left* coset an element belongs to, we get the following.

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

We would get a similar table (but in this case, not identical) if we colored the elements according to the right cosets.

Let's tackle a few more examples.

Problem 5.3. Consider D_3 and let $K = \langle r \rangle$.

(a) Find all of the left cosets of K and then find all of the right cosets of K in D_3. Any observations?

(b) Write down the group table for D_3, but this time arrange the rows and columns according to the left cosets for K. Color the entire table according to which *left* coset an element belongs to. Can you visualize the observations you made in part (a)?

Problem 5.4. Consider Q_8. Let $H = \langle i \rangle$ and $K = \langle -1 \rangle$.

(a) Find all of the left cosets of H and all of the right cosets of H in Q_8.

(b) Write down the group table for Q_8 so that rows and columns are arranged according to the left cosets for H. Color the entire table according to which *left* coset an element belongs to.

(c) Find all of the left cosets of K and all of the right cosets of K in Q_8.

(d) Write down the group table for Q_8 so that rows and columns are arranged according to the left cosets for K. Color the entire table according to which *left* coset an element belongs to.

Problem 5.5. Consider S_4. Find all of the left cosets and all of the right cosets of A_4 in S_4. Instead of doing brute-force, try to be clever. *Hint:* What happens when you compose two even permutations versus an even permutation and an odd permutation?

Problem 5.6. Consider $\mathbb{Z}_8$. Find all of the left cosets and all of the right cosets of $\langle 4 \rangle$ in $\mathbb{Z}_8$. Why do you know the left and right cosets are the same without actually verifying?

Problem 5.7. Consider $(\mathbb{Z}, +)$. Find all of the left cosets and all of the right cosets of $3\mathbb{Z}$ in $\mathbb{Z}$. Why do you know the left and right cosets are the same without actually verifying?

Theorem 5.8. Let G be a group and let $H \leq G$. If G is abelian, then for all $a \in G$, $aH = Ha$. That is, if G is abelian, then the left cosets of H are the same as the right cosets of H.

Exercises 5.2 and 5.3 illustrate that if a group is non-abelian, then the cosets of a subgroup may or may not coincide. That is, knowing that the group is non-abelian is not enough to determine whether the left and right cosets are different.

In all of the examples we've seen so far, the left and right cosets partitioned G into equal-sized chunks. We need to prove that this is true in general. To prove that the cosets form a partition, we will define an appropriate equivalence relation.

Theorem 5.9. Let G be a group and let $H \leq G$. Define $\sim_L$ and $\sim_R$ via

$$a \sim_L b \text{ if and only if } a^{-1}b \in H$$

and

$$a \sim_R b \text{ if and only if } ab^{-1} \in H.$$

Then both $\sim_L$ and $\sim_R$ are equivalence relations. *Note:* You only need to prove that either $\sim_L$ or $\sim_R$ is an equivalence relation as the proof for the other is similar.

Since $\sim_L$ and $\sim_R$ are equivalence relations, the corresponding equivalence classes form a partition of G. If $a \in G$, then the "left" and "right" equivalence classes containing a are given by

$$[a]_{\sim_L} = \{g \in G \mid a \sim_L g\}$$

and

$$[a]_{\sim_R} = \{g \in G \mid a \sim_R g\}.$$

The next theorem tells us that the equivalence classes determined by $\sim_L$ and $\sim_R$ are indeed the left and right cosets of $H \leq G$, respectively.

Theorem 5.10. If G is a group and $H \leq G$, then $[a]_{\sim_L} = aH$ and $[a]_{\sim_R} = Ha$ for all $a \in G$.

Corollary 5.11. If G is a group and $H \leq G$, then the left (respectively, right) cosets of H form a partition of G.

Next, we argue that all of the cosets have the same size.

Theorem 5.12. Let G be a group, $H \leq G$, and $a \in G$. Define $\phi : H \to aH$ via $\phi(h) = ah$. Then ϕ is one-to-one and onto.

In the next result, $\#(aH)$ denotes the size of aH. Note that everything works out just fine even if H has infinite order.

Corollary 5.13. Let G be a group and let $H \leq G$. Then all of the left and right cosets of H are the same size as H. In other words $\#(aH) = |H| = \#(Ha)$ for all $a \in G$.

The next theorem provides a useful characterization of cosets. Each part can either be proved directly or by appealing to previous results in this section.

Theorem 5.14. Let G be a group and let $H \leq G$.

(a) If $a \in G$, then $a \in aH$ (respectively, Ha).

(b) We have $b \in aH$ (respectively, Ha) if and only if $aH = bH$ (respectively, $Ha = Hb$).

(c) If $a \in H$, then $aH = H = Ha$.

(d) If $a \notin H$, then for all $h \in H$, $ah \notin H$ (respectively, $ha \notin H$).

The upshot of part (b) of Theorem 5.14 is that cosets can have different names. In particular, if b is an element of the left coset aH, then we could have just as easily called the coset by the name bH. In this case, both a and b are called **coset representatives**.

The final result of this section verifies that the clones of a subgroup in a Cayley diagram coincide with the right cosets of the subgroup.

Problem 5.15. Let G be a finite group with generating set S and let H be a proper subgroup of G and suppose we can visualize the subgroup for H in the Cayley diagram for G using S as the generating set.

(a) If $g \in G$, verify that the right coset Hg is a clone of H. *Hint:* Suppose $s \in S$ and $h_1, h_2 \in H$ such that there is an arrow labeled by s that points from h_1 to h_2. Argue that there is an arrow labeled by s pointing from $h_1 g$ to $h_2 g$.

(b) If C is a clone of H, prove that C is a right coset of H.

5.2 Lagrange's Theorem

We're finally ready to state Lagrange's Theorem, which is named after the Italian born mathematician Joseph Louis Lagrange. It turns out that Lagrange did not actually prove the theorem that is named after him. The theorem was actually proved by Carl Friedrich Gauss in 1801.

Theorem 5.16 (Lagrange's Theorem)**.** Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

This simple sounding theorem is extremely powerful. One consequence is that groups and subgroups have a fairly rigid structure. Suppose G is a finite group and let $H \leq G$. Since G is finite, there must be a finite number of distinct left cosets, say $H, a_2H, \ldots, a_nH$. Corollary 5.13 tells us that each of these cosets is the same size. In particular, Lagrange's Theorem implies that for each $i \in \{1, \ldots, n\}$, $|a_iH| = |G|/n$, or equivalently $n = |G|/|a_iH|$. This is depicted in Figure 5.2, where each rectangle represents a coset and we've labeled a single coset representative in each case.

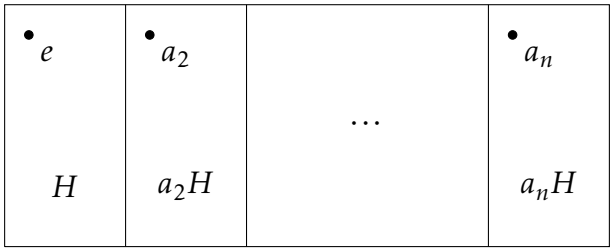


Figure 5.2

One important consequence of Lagrange's Theorem is that it narrows down the possible sizes for subgroups.

Problem 5.17. Suppose G is a group of order 48. What are the possible orders for subgroups of G?

Lagrange's Theorem tells us what the possible orders of a subgroup are, but if k is a divisor of the order of a group, it does not guarantee that there is a subgroup of order k. It's not too hard to show that the converse of Lagrange's Theorem is true for cyclic groups. However, it's not true, in general.

Problem 5.18. Provide an example of a finite group G such that $|G|$ has a divisor k but G does not have a subgroup of order k.

Using Lagrange's Theorem, we can quickly prove both of the following theorems.

Theorem 5.19. Let G be a finite group and let $a \in G$. Then $|a|$ divides $|G|$.

The next exercise shows us that the converse of Theorem 5.19 is not true.

Problem 5.20. Argue that S_4 does not have any elements of order 8.

Theorem 5.21. For every prime p, if G has order p, then $G \cong \mathbb{Z}_p$.

Corollary 5.22. For every prime p, there is a unique group of order p up to isomorphism.

Lagrange's Theorem motivates the following definition.

Definition 5.23. Let G be a group and let $H \leq G$. The **index** of H in G is the number of cosets (left or right) of H in G. Equivalently, if G is finite, then the index of H in G is equal to $|G|/|H|$. We denote the index via $[G : H]$.

Problem 5.24. Let $H = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.

(a) Find $[A_4 : H]$.

(b) Find $[S_4 : H]$.

Problem 5.25. Find $[\mathbb{Z} : 4\mathbb{Z}]$.

5.3 Normal Subgroups

We've seen an example where the left and right cosets of a subgroup were different and a few examples where they coincided. In the latter case, the subgroup has a special name.

Definition 5.26. Let G be a group and let $H \leq G$. If $aH = Ha$ for all $a \in G$, then we say that H is a **normal subgroup**. If H is a normal subgroup of G, then we write $H \trianglelefteq G$.

Problem 5.27. Provide an example of group that has a subgroup that is not normal.

Problem 5.28. Suppose G is a finite group and let $H \leq G$. If $H \trianglelefteq G$ and we arrange the rows and columns of the group table for G according to the left cosets of H and then color the corresponding cosets, what property will the table have? Is the converse true? That is, if the table has the property you discovered, will H be normal in G?

There are a few instances where we can guarantee that a subgroup will be normal.

Theorem 5.29. Suppose G is a group. Then $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$.

Theorem 5.30. If G is an abelian group, then all subgroups of G are normal.

A group does not have to be abelian in order for all the proper subgroups to be normal.

Problem 5.31. Argue that all of the proper subgroups of Q_8 are normal in Q_8.

Theorem 5.32. Suppose G is a group and let $H \leq G$ such that $[G : H] = 2$. Then $H \trianglelefteq G$.

It turns out that normality is not transitive.

Problem 5.33. Consider $\langle s \rangle = \{e, s\}$ and $\langle r^2, sr^2 \rangle = \{e, r^2, sr^2, s\}$. It is clear that

$$\langle s \rangle \leq \langle r^2, sr^2 \rangle \leq D_4.$$

Show that $\langle s \rangle \trianglelefteq \langle r^2, sr^2 \rangle$ and $\langle r^2, sr^2 \rangle \trianglelefteq D_4$, but $\langle s \rangle \not\trianglelefteq D_4$.

The previous problem illustrates that $H \trianglelefteq K \trianglelefteq G$ does not imply $H \trianglelefteq G$.

Definition 5.34. Suppose G is a group and let $H \leq G$. For $g \in G$, we define the **conjugate of H by g** to be the set

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}.$$

Theorem 5.35. Suppose G is a group and let $H \leq G$. Then $H \trianglelefteq G$ if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.

Another way of thinking about normal subgroups is that they are "closed under conjugation." It's not too hard to show that if $gHg^{-1} \subseteq H$ for all $g \in G$, then we actually have $gHg^{-1} = H$ for all $g \in G$. This implies that $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for all $g \in G$. This seemingly stronger version of Theorem 5.35 is sometimes used as the definition of normal subgroup. This discussion motivates the following definition.

Definition 5.36. Let G be a group and let $H \leq G$. The **normalizer of H in G** is defined via

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

Theorem 5.37. If G is a group and $H \leq G$, then $N_G(H)$ is a subgroup of G.

Theorem 5.38. If G is a group and $H \leq G$, then $H \trianglelefteq N_G(H)$. Moreover, $N_G(H)$ is the largest subgroup of G in which H is normal.

It is worth pointing out that the "smallest" $N_G(H)$ can be is H itself—certainly a subgroup is a normal subgroup of itself. Also, the "largest" that $N_G(H)$ can be is G, which happens precisely when H is normal in G.

Problem 5.39. Find $N_{D_4}(V_4)$.

Problem 5.40. Find $N_{D_3}(\langle s \rangle)$.

We conclude this chapter with a few remarks. We've seen examples of groups that have subgroups that are normal and subgroups that are not normal. In an abelian group, all the subgroups are normal. It turns out that there are examples of groups that have no normal subgroups. These groups are called **simple groups**. The smallest simple group is A_5, which has 60 elements and lots of proper nontrivial subgroups, none of which are normal.

The classification of the finite simple groups is a theorem stating that every finite simple group belongs to one of four categories:

1. A cyclic group with prime order;
2. An alternating group of degree at least 5;
3. A simple group of Lie type, including both
   (a) the classical Lie groups, namely the simple groups related to the projective special linear, unitary, symplectic, or orthogonal transformations over a finite field;

(b) the exceptional and twisted groups of Lie type (including the Tits group);

4. The 26 sporadic simple groups.

These groups can be seen as the basic building blocks of all finite groups, in a way reminiscent of the way the prime numbers are the basic building blocks of the natural numbers.

The classification theorem has applications in many branches of mathematics, as questions about the structure of finite groups (and their action on other mathematical objects) can sometimes be reduced to questions about finite simple groups. Thanks to the classification theorem, such questions can sometimes be answered by checking each family of simple groups and each sporadic group. The proof of the theorem consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published mostly between 1955 and 2004.

The classification of the finite simple groups is a modern achievement in abstract algebra and I highly encourage you to go learn more about it. You might be especially interested in learning about one of the sporadic groups called the **Monster Group**.

Chapter 6

Products and Quotients of Groups

6.1 Products of Groups

In this section, we will discuss a method for using existing groups as building blocks to form new groups.

Suppose $(G,*)$ and $(H,\odot)$ are two groups. Recall that the Cartesian product of G and H is defined to be

$$G \times H = \{(g,h) \mid g \in G, h \in H\}$$

Using the binary operations for the groups G and H, we can define a binary operation on the set $G \times H$. Define $\star$ on $G \times H$ via

$$(g_1,h_1) \star (g_2,h_2) = (g_1 * g_2, h_1 \odot h_2).$$

This looks fancier than it is. We're just doing the operation of each group in the appropriate component. It turns out that $(G \times H, \star)$ is a group.

Theorem 6.1. Suppose $(G,*)$ and $(H,\odot)$ are two groups, where e and e' are the identity elements of G and H, respectively. Then $(G \times H, \star)$ is a group, where $\star$ is defined as above. Moreover, (e,e') is the identity of $G \times H$ and the inverse of $(g,h) \in G \times H$ is given by $(g,h)^{-1} = (g^{-1}, h^{-1})$.

We refer to $G \times H$ as the **direct product** of the groups G and H. In this case, each of G and H is called a **factor** of the direct product. We often abbreviate $(g_1,h_1) \star (g_2,h_2) = (g_1 * g_2, h_1 \odot h_2)$ by $(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$. One exception to this is if we are using the operation of addition in each component. For example, consider $\mathbb{Z}_4 \times \mathbb{Z}_2$ under the operation of addition mod 4 in the first component and addition mod 2 in the second component. Then

$$\mathbb{Z}_4 \times \mathbb{Z}_2 = \{(0,0),(1,0),(2,0),(3,0),(0,1),(1,1),(2,1),(3,1)\}.$$

In this case, we will use additive notation in $\mathbb{Z}_4 \times \mathbb{Z}_2$. For example, in $\mathbb{Z}_4 \times \mathbb{Z}_2$ we have

$$(2,1) + (3,1) = (1,0)$$

and

$$(1,0)+(2,1)=(3,1).$$

Moreover, the identity of the group is $(0,0)$. As an example, the inverse of $(1,1)$ is $(3,1)$ since $(1,1)+(3,1)=(0,0)$. There is a very natural generating set for $\mathbb{Z}_4\times\mathbb{Z}_2$, namely, $\{(1,0),(0,1)\}$ since $1\in\mathbb{Z}_4$ and $1\in\mathbb{Z}_2$ generate $\mathbb{Z}_4$ and $\mathbb{Z}_2$, respectively. The corresponding Cayley diagram is given in Figure 6.1.

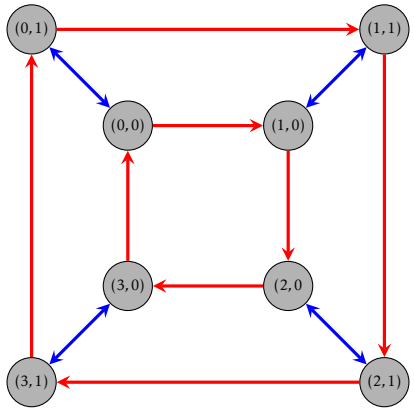


Figure 6.1. Cayley diagram for $\mathbb{Z}_4\times\mathbb{Z}_2$ with generating set $\{(1,0),(0,1)\}$.

Problem 6.2. Consider the group $\mathbb{Z}_4\times\mathbb{Z}_2$. Is this group abelian? Is the group cyclic? Determine whether $\mathbb{Z}_4\times\mathbb{Z}_2$ is isomorphic to any of D_4, Q_8, $\mathbb{Z}_8$, or L_3.

The upshot of the previous problem is that there are at least five groups of order 8 up to isomorphism. It turns out that there are exactly five groups of order 8 up to isomorphism. In particular, every group of order 8 is isomorphic to one of the following groups: $\mathbb{Z}_8$, $\mathbb{Z}_4\times\mathbb{Z}_2$, L_3, D_4, and Q_8. Note that $R_8\cong\mathbb{Z}_8$ and $\mathrm{Spin}_{1\times 2}\cong D_4$. Three of the isomorphism classes correspond to abelian groups while the other two correspond to non-abelian groups. Unfortunately, we will not develop the tools necessary to prove that this classification is complete.

The next two theorems should not be terribly surprising.

Theorem 6.3. If G_1 and G_2 are groups, then $G_1\times G_2\cong G_2\times G_1$.

Theorem 6.4. Suppose G_1 and G_2 are groups with identities e_1 and e_2, respectively. Then $\{e_1\}\times G_2\cong G_2$ and $G_1\times\{e_2\}\cong G_1$.

There's no reason we can't take the direct product of more than two groups. If $A_1,A_2,\ldots,A_n$ is a collection of sets, we define

$$\prod_{i=1}^{n}A_i:=A_1\times A_2\times\cdots\times A_n.$$

Each element of $\prod_{i=1}^{n}A_i$ is of the form $(a_1,a_2,\ldots,a_n)$, where $a_i\in A_i$.

Theorem 6.5. Let $G_1, G_2, \ldots, G_n$ be groups. For $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \prod_{i=1}^{n} G_i$, define

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Then $\prod_{i=1}^{n} G_i$, the **direct product** of $G_1, \ldots, G_n$, is a group under this binary operation.

One way to think about direct products is that we can navigate the product by navigating each factor simultaneously but independently. Computing the order of a group that is a direct product is straightforward.

Theorem 6.6. Let $G_1, G_2, \ldots, G_n$ be finite groups. Then

$$|G_1 \times G_2 \times \cdots \times G_n| = |G_1| \cdot |G_2| \cdots |G_n|.$$

Theorem 6.7. Let $G_1, G_2, \ldots, G_n$ be groups. Then $|G_1 \times G_2 \times \cdots \times G_n|$ is infinite if and only if at least one $|G_i|$ is infinite.

The following theorem should be clear.

Theorem 6.8. Let $G_1, G_2, \ldots, G_n$ be groups. Then $\prod_{i=1}^{n} G_i$ is abelian if and only if each G_i is abelian.

Let's play with a few more examples.

Problem 6.9. Draw the Cayley diagram for $\mathbb{Z}_2 \times \mathbb{Z}_3$ using $\{(1,0), (0,1)\}$ as the generating set. Is $\mathbb{Z}_2 \times \mathbb{Z}_3$ an abelian group? Is it cyclic? What familiar group is $\mathbb{Z}_2 \times \mathbb{Z}_3$ isomorphic to?

Problem 6.10. Consider $\mathbb{Z}_2 \times \mathbb{Z}_2$ under the operation of addition mod 2 in each component. Find a generating set for $\mathbb{Z}_2 \times \mathbb{Z}_2$ and then create a Cayley diagram for this group. What well-known group is $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorphic to?

Consider the similarities and differences between $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Both groups are abelian by Theorem 6.8, but only the former is cyclic. Here's another exercise.

Problem 6.11. Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Find a generating set for $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and then create a Cayley diagram for this group. Is there a group that we have seen before that $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ isomorphic to?

The next theorem tells us how to compute the order of an element in a direct product of groups.

Theorem 6.12. Suppose $G_1, G_2, \ldots, G_n$ are groups and let $(g_1, g_2, \ldots, g_n) \in \prod_{i=1}^{n} G_i$. If $|g_i| = r_i < \infty$, then $|(g_1, g_2, \ldots, g_n)| = \operatorname{lcm}(r_1, r_2, \ldots, r_n)$.

Problem 6.13. Find the order of each of the following elements.

(a) $(6, 5) \in \mathbb{Z}_{12} \times \mathbb{Z}_7$.

(b) $(r, i) \in D_3 \times Q_8$.

(c) $((1,2)(3,4),3) \in S_4 \times \mathbb{Z}_{15}$.

Problem 6.14. Find the largest possible order of elements in each of the following groups.

(a) $\mathbb{Z}_6 \times \mathbb{Z}_8$

(b) $\mathbb{Z}_9 \times \mathbb{Z}_{12}$

(c) $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$

Theorem 6.15. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.

Corollary 6.16. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime.

The previous results can be extended to more than two factors.

Theorem 6.17. The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ if and only if every pair from the collection $\{m_1, m_2, \ldots, m_n\}$ is relatively prime.

Problem 6.18. Determine whether each of the following groups is cyclic.

(a) $\mathbb{Z}_7 \times \mathbb{Z}_8$

(b) $\mathbb{Z}_7 \times \mathbb{Z}_7$

(c) $\mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_8$

(d) $\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_8$

Theorem 6.19. Suppose $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, where each p_i is a distinct prime number. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}.$$

The next theorem tells us that the direct product of subgroups is always a subgroup.

Theorem 6.20. Suppose G_1 and G_2 are groups such that $H_1 \leq G_1$ and $H_2 \leq G_2$. Then $H_1 \times H_2 \leq G_1 \times G_2$.

However, not every subgroup of a direct product has the form above.

Problem 6.21. Find an example that illustrates that not every subgroup of a direct product is the direct product of subgroups of the factors.

Problem 6.22. Can we extend Theorem 6.20 to normal subgroups? That is, if $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$, is it the case that $H_1 \times H_2 \trianglelefteq G_1 \times G_2$? If so, prove it. Otherwise, provide a counterexample.

The next theorem describes precisely the structure of finite abelian groups. We will omit its proof, but allow ourselves to utilize it as needed.

Theorem 6.23 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}} \times \mathbb{Z}^k,$$

where each p_i is a prime number (not necessarily distinct). The product is unique up to rearrangement of the factors.

Note that the number k is called the **Betti number**. A finitely generated abelian group is finite if and only if the Betti number is 0.

Problem 6.24. Find all abelian groups up to isomorphism of order 8. How many different groups up to isomorphism (both abelian and non-abelian) have we seen and what are they?

Problem 6.25. Find all abelian groups up to isomorphism for each of the following orders.

(a) 16

(b) 12

(c) 25

(d) 30

(e) 60

6.2 Quotients of Groups

In the previous section, we discussed a method for constructing "larger" groups from "smaller" groups using a direct product construction. In this section, we will in some sense do the opposite.

Problem 5.28 hinted that if $H \leq G$ and we arrange the group table according to the left cosets of H, then the group table will have checkerboard pattern if and only if H is normal in G (i.e., the left and right cosets of H are the same). For example, see the colored table prior to Problem 5.3 versus the ones you created in Exercises 5.3, 5.4. If we have the checkerboard pattern in the group table that arises from a normal subgroup, then by "gluing together" the colored blocks, we obtain a group table for a smaller group that has the cosets as the elements.

For example, let's consider $K = \langle -1 \rangle \leq Q_8$. Problem 5.4 showed us that K is normal Q_8. The left (and right) cosets of K in Q_8 are

$$K = \{1, -1\}, iK = \{i, -i\}, jK = \{j, -j\}, \text{ and } kK = \{k, -k\}.$$

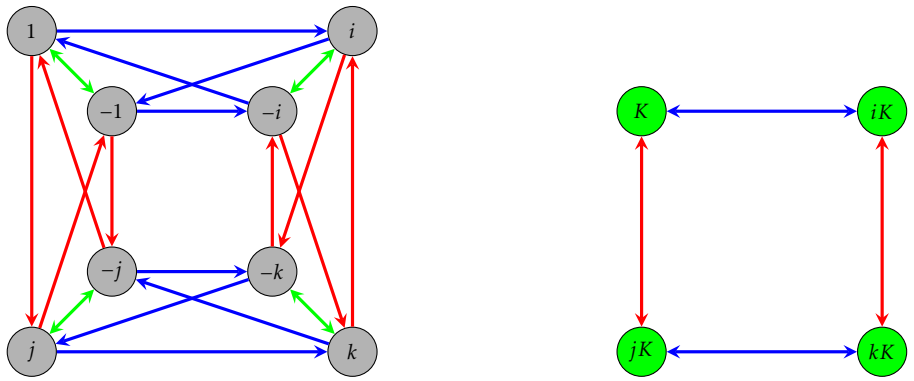
As you found in Problem 5.4, if we arrange the rows and columns of Q_8 according to these cosets, we obtain the following group table.

$*$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

If we consider the 2×2 blocks as elements, it appears that we have a group table for a group with 4 elements. Closer inspection reveals that this looks like the table for V_4. If the table of 2×2 blocks is going to represent a group, we need to understand the binary operation. How do we "multiply" cosets? For example, the table suggests that the coset jK (colored in red) times the coset iK (colored in blue) is equal to kK (colored in purple) despite the fact that $ji = -k \neq k$. Yet, it is true that the product $ji = -k$ is an element in the coset kK. In fact, if we look closely at the table, we see that if we pick any two cosets, the product of any element of the first coset times any element of the second coset will always result in an element in the same coset regardless of which representatives we chose.

In other words, it looks like we can multiply cosets by choosing any representative from each coset and then seeing what coset the product of the representatives lies in. However, it is important to point out that this will only work if we have a checkerboard pattern of cosets, which we have seen evidence of only happening when the corresponding subgroup is normal.

Before continuing, let's continue tinkering with the same example. Consider the Cayley diagram for Q_8 with generators $\{i, j, -1\}$ that is given in Figure 6.2(a).



(a) (b)

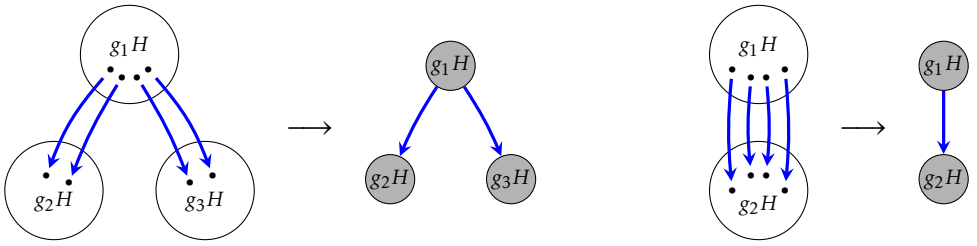
Figure 6.2. The left subfigure shows the Cayley diagram for Q_8 with generating set $\{i, j, -1\}$. The right subfigure shows the collapsed Cayley diagram for Q_8 according to the left cosets of $K = \langle -1 \rangle$.

We can visualize the right cosets of K as the clumps of vertices connected together with the two-way green arrows. In this case, we are also seeing the left cosets since K is

normal in Q_8. If we collapse the cosets onto each other and collapse the corresponding arrows, we obtain the diagram given in Figure 6.2(b). It is clear that this diagram is the Cayley diagram for a group that is isomorphic to V_4. For reasons we will understand shortly, this processing of collapsing a Cayley diagram according to the cosets of a normal subgroup is called the "quotient process."

Problem 6.26. Let's see what happens if we attempt the quotient process for a subgroup that is not normal. Consider $H = \langle s \rangle \leq D_3$. In Problem 5.2, we discovered that the left cosets of H are not the same as the right cosets of H. This implies that H is not normal in D_3. Consider the standard Cayley diagram for D_3 that uses the generators r and s. Draw the diagram that results from attempting the quotient process on D_3 using the subgroup H. Explain why this diagram cannot be the diagram for a group.

The problem that arises in Problem 6.26 is that if the same arrow types (i.e., those representing the same generator) leaving a coset do not point at elements in the same coset, attempting the quotient process will result in a diagram that cannot be a Cayley diagram for a group since we have more than one arrow of the same type leaving a vertex. In Figure 6.3(a), we illustrate what goes wrong if all the arrows for a generator pointing out of a coset do not unanimously point to elements in the same coset. In Figure 6.3(b), all the arrows point to elements in the same coset, and in this case, it appears that everything works out just fine.



(a) (b)

Figure 6.3. In the left subfigure, blue arrows go from elements of the left coset g_1H to elements of *multiple* left cosets, which results in ambiguous blue arrows in the collapsed diagram. This implies that left coset multiplication is not well-defined in this case. In the right subfigure, blue arrows go from elements of the left coset g_1H to elements inside a *unique* left coset, which does not result in any ambiguity.

Problem 6.27. In Problem 5.3, we learned that the subgroup $K = \langle r \rangle$ is normal in D_3 since the left cosets are equal to the right cosets. Note that this follows immediately from Theorem 5.32 since $[D_3 : K] = 2$. Draw the diagram that results from performing the quotient process to D_3 using the subgroup K. Does the resulting diagram represent a group? If so, what group is it isomorphic to?

Now, suppose G is an arbitrary group and let $H \leq G$. Consider the set of left cosets of H. We define

$$(aH)(bH) := (ab)H.$$

The natural question to ask is whether this operation is well-defined. That is, does the result of multiplying two left cosets depend on our choice of representatives? More specifically, suppose $c \in aH$ and $d \in bH$. Then $cH = aH$ and $dH = bH$. According to the operation defined above, $(cH)(dH) = cdH$. It better be the case that $cdH = abH$, otherwise the operation is not well-defined.

Problem 6.28. Let $H = \langle s \rangle \leq D_3$. Find specific examples of $a, b, c, d \in D_3$ such that

$$(aH)(bH) \neq (cH)(dH)$$

even though $aH = cH$ and $bH = dH$.

Theorem 6.29. Let G be a group and let $H \leq G$. Then left coset multiplication (as defined above) is well-defined if and only if $H \trianglelefteq G$.

Theorem 6.30. Let G be a group and let $H \trianglelefteq G$. Then the set of left cosets of H in G forms a group under left coset multiplication.

The group from Theorem 6.30 is denoted by G/H, read "G mod H", and is referred to as the **quotient group** (or **factor group**) of G by H. If G is a finite group, then G/H is exactly the group that arises from "gluing together" the colored blocks in a checkerboard-patterned group table. It's also the group that we get after applying the quotient process to the Cayley diagram. It's important to point out once more that this only works properly if H is a normal subgroup.

Recall that Theorem 5.30 tells us that if G is abelian, then every subgroup is normal. This implies that when G is abelian, G/H is a well-defined group for every subgroup H of G. However, it is not necessary for G to be abelian in order for G/H to be a well-defined group. The quotient group $Q_8/\langle -1 \rangle$ is an example where this happens.

The next theorem tells us how to compute the order of a quotient group.

Theorem 6.31. Let G be a group and let $H \trianglelefteq G$. Then $|G/H| = [G : H]$. In particular, if G is finite, then $|G/H| = |G|/|H|$.

It's important to point out that the order of a quotient group might be finite even if G has infinite order.

Problem 6.32. Consider the group $(\mathbb{Z}, +)$. Since $\mathbb{Z}$ is abelian, every subgroup is normal. For example, $4\mathbb{Z} \trianglelefteq \mathbb{Z}$, which implies that $\mathbb{Z}/4\mathbb{Z}$ is a well-defined quotient group. Moreover, both $\mathbb{Z}$ and $4\mathbb{Z}$ have infinite order. What is $|\mathbb{Z}/4\mathbb{Z}|$ equal to? Can you determine what well-known group $\mathbb{Z}/4\mathbb{Z}$ is isomorphic to?

Suppose G is a group and $H \trianglelefteq G$, so that G/H is a group. Recall that the elements of the group G/H are the left cosets of H, which are of the form aH where $a \in G$. The operation of the group is defined via

$$(aH)(bH) = abH.$$

Moreover, the identity in G/H is $eH = H$ since $(aH)(eH) = aH$. By Corollary 4.20 $|aH| = k$ if and only $(aH)^k = H$ and k is the smallest such positive exponent with this property. But

notice that $(aH)^k = a^kH$. So, in order to compute the order of aH, we need to find the smallest positive exponent k such that $a^kH = H$, but $a^kH = H$ exactly when a^k is in H. The upshot is that to find the order of aH in G/H, we need the smallest positive k such that a^k is in H.

Problem 6.33. Find the order of the given element in the quotient group. You may assume that we are taking the quotient by a normal subgroup.

(a) $s\langle r\rangle \in D_4/\langle r\rangle$

(b) $j\langle -1\rangle \in Q_8/\langle -1\rangle$

(c) $5 + \langle 4\rangle \in \mathbb{Z}_{12}/\langle 4\rangle$

(d) $(2,1) + \langle (1,1)\rangle \in (\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle (1,1)\rangle$

(e) $(1,3) + \langle (0,2)\rangle \in (\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle (0,2)\rangle$

Problem 6.34. For each quotient group below, describe the group. If possible, state what group each is isomorphic to. You may assume that we are taking the quotient by a normal subgroup.

(a) $Q_8/\langle -1\rangle$

(b) $Q_8/\langle i\rangle$

(c) $\mathbb{Z}_4/\langle 2\rangle$

(d) $V_4/\langle h\rangle$

(e) $A_4/\langle (1,2)(3,4), (1,3)(2,4)\rangle$

(f) $(\mathbb{Z}_2 \times \mathbb{Z}_2)/\langle (1,1)\rangle$

(g) $\mathbb{Z}/4\mathbb{Z}$

(h) S_4/A_4

(i) $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2)$

Problem 6.35. Compute the order of every element in the quotient group $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle (0,2)\rangle$. What well-known group is $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle (0,2)\rangle$ isomorphic to?

Theorem 6.36. Let G be a group. Then

(a) $G/\{e\} \cong G$

(b) $G/G \cong \{e\}$

Theorem 6.37. We have the following.

(a) For $n \geq 2$, $S_n/A_n \cong \mathbb{Z}_2$.

(b) For all $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(c) For all $n \in \mathbb{N}$, $\mathbb{R}/n\mathbb{R} \cong \{e\}$.

Theorem 6.38. Let G be a group and let $H \trianglelefteq G$. If G is abelian, then so is G/H.

Problem 6.39. Show that the converse of the previous theorem is not true by providing a specific counterexample.

Problem 6.40. Consider the quotient group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle$.

(a) What is the order of $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle$?

(b) Is the group abelian? Why?

(c) Write down all the elements of $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle$.

(d) Does one of the elements generate the group?

(e) What well-known group is $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle$ isomorphic to?

Theorem 6.41. Let G be a group and let $H \trianglelefteq G$. If G is cyclic, then so is G/H.

Problem 6.42. Show that the converse of the previous theorem is not true by providing a specific counterexample.

Here are few additional exercises. These ones are a bit tougher.

Problem 6.43. For each quotient group below, describe the group. If possible, state what group each is isomorphic to. You may assume that we are taking the quotient by a normal subgroup.

(a) $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,2)\rangle$

(b) $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle$

(c) $\mathbb{Q}/\langle 1\rangle$ (the operation on $\mathbb{Q}$ is addition)

Chapter 7

Homomorphisms and the Isomorphism Theorems

7.1 Homomorphisms

Let G_1 and G_2 be groups. Recall that $\phi : G_1 \to G_2$ is an isomorphism if and only if ϕ

(a) is one-to-one,

(b) is onto, and

(c) satisfies the homomorphic property.

We say that G_1 is isomorphic to G_2 and write $G_1 \cong G_2$ if such a ϕ exists. Loosely speaking, two groups are isomorphic if they have the "same structure." What if we drop the one-to-one and onto requirement?

Definition 7.1. Let $(G_1, *)$ and $(G_2, \odot)$ be groups. A function $\phi : G_1 \to G_2$ is a **homomorphism** if and only if ϕ satisfies the homomorphic property:

$$\phi(x * y) = \phi(x) \odot \phi(y)$$

for all $x, y \in G_1$. At the risk of introducing ambiguity, we will usually omit making explicit reference to the binary operations and write the homomorphic property as

$$\phi(xy) = \phi(x)\phi(y).$$

Group homomorphisms are analogous to linear transformations on vector spaces that one encounters in linear algebra.

Figure 7.1 captures a visual representation of the homomorphic property. We encountered this same representation in Figure 3.9. If $\phi(x) = x'$, $\phi(y) = y'$, and $\phi(z) = z'$ while $z' = x' \odot y'$, then the only way G_2 may respect the structure of G_1 is for

$$\phi(x * y) = \phi(z) = z' = x' \odot y' = \phi(x) \odot \phi(y).$$

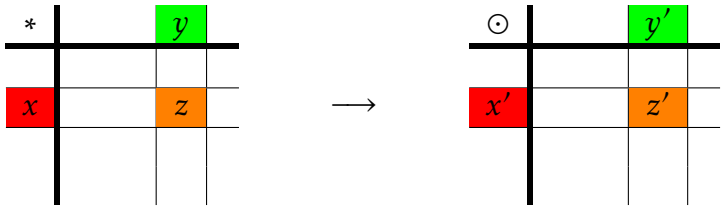


Figure 7.1

Problem 7.2. Define $\phi : \mathbb{Z}_3 \to D_3$ via $\phi(k) = r^k$. Prove that ϕ is a homomorphism and then determine whether ϕ is one-to-one or onto. Also, try to draw a picture of the homomorphism in terms of Cayley diagrams.

Problem 7.3. Let G and H be groups. Prove that the function $\phi : G \times H \to G$ given by $\phi(g,h) = g$ is a homomorphism. This function is an example of a **projection map**.

There is always at least one homomorphism between two groups.

Theorem 7.4. Let G_1 and G_2 be groups. Define $\phi : G_1 \to G_2$ via $\phi(g) = e_2$ (where e_2 is the identity of G_2). Then ϕ is a homomorphism. This function is often referred to as the **trivial homomorphism** or the 0-**map**.

Back in Section 3.3, we encountered several theorems about isomorphisms. However, at the end of that section we remarked that some of those theorems did not require that the function be one-to-one and onto. We collect those results here for convenience.

Theorem 7.5. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism.

(a) If e_1 and e_2 are the identity elements of G_1 and G_2, respectively, then $\phi(e_1) = e_2$.

(b) For all $g \in G_1$, we have $\phi(g^{-1}) = [\phi(g)]^{-1}$.

(c) If $H \leq G_1$, then $\phi(H) \leq G_2$, where

$$\phi(H) := \{y \in G_2 \mid \text{there exists } h \in H \text{ such that } \phi(h) = y\}.$$

Note that $\phi(H)$ is called the **image** of H. A special case is when $H = G_1$. Notice that ϕ is onto exactly when $\phi(G_1) = G_2$.

The following theorem is a consequence of Lagrange's Theorem.

Theorem 7.6. Let G_1 and G_2 be groups such that G_2 is finite and let $H \leq G_1$. If $\phi : G_1 \to G_2$ is a homomorphism, then $|\phi(H)|$ divides $|G_2|$.

The next theorem tells us that under a homomorphism, the order of the image of an element must divide the order of the pre-image of that element.

Theorem 7.7. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. If $g \in G_1$ such that $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.

Every homomorphism has an important subset of the domain associated with it.

Definition 7.8. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. The **kernel** of ϕ is defined via

$$\ker(\phi) := \{g \in G_1 \mid \phi(g) = e_2\}.$$

The kernel of a homomorphism is analogous to the null space of a linear transformation of vector spaces.

Problem 7.9. Identify the kernel and image for the homomorphism given in Problem 7.2.

Problem 7.10. What is the kernel of a trivial homomorphism (see Theorem 7.4).

Theorem 7.11. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Then $\ker(\phi) \trianglelefteq G_1$.

Theorem 7.12. Let G be a group and let $H \trianglelefteq G$. Then the map $\gamma : G \to G/H$ given by $\gamma(g) = gH$ is a homomorphism with $\ker(\gamma) = H$. This map is called the **canonical projection map**.

The upshot of Theorems 7.11 and 7.12 is that kernels of homomorphisms are always normal and every normal subgroup is the kernel of some homomorphism. It turns out that the kernel can tell us whether ϕ is one-to-one.

The next theorem tells us that two elements in the domain of a group homomorphism map to the same element in the codomain if and only if they are in the same coset of the kernel.

Theorem 7.13. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Then $\phi(a) = \phi(b)$ if and only if $a \in b\ker(\phi)$.

One consequence of Theorem 7.13 is that if the kernel of a homomorphism has order k, then the homomorphism is k-to-1. That is, every element in the range has exactly k elements from the domain that map to it. In particular, each of these collections of k elements corresponds to a coset of the kernel.

Problem 7.14. Suppose $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ is a group homomorphism such that $\ker(\phi) = \{0, 5, 10, 15\}$. If $\phi(13) = 8$, determine all elements that ϕ maps to 8.

The next result is a special case of Theorem 7.13.

Theorem 7.15. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Then ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$, where e_1 is the identity in G_1.

Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Given a generating set for G_1, the homomorphism ϕ is uniquely determined by its action on the generating set for G_1. In particular, if you have a word for a group element written in terms of the generators, just apply the homomorphic property to the word to find the image of the corresponding group element.

Problem 7.16. Suppose $\phi : Q_8 \to V_4$ is a group homomorphism satisfying $\phi(i) = h$ and $\phi(j) = v$.

(a) Find $\phi(1)$, $\phi(-1)$, $\phi(k)$, $\phi(-i)$, $\phi(-j)$, and $\phi(-k)$.

(b) Find $\ker(\phi)$.

(c) What well-known group is $Q_8/\ker(\phi)$ isomorphic to?

Problem 7.17. Find a non-trivial homomorphism from $\mathbb{Z}_{10}$ to $\mathbb{Z}_6$.

Problem 7.18. Find all non-trivial homomorphisms from $\mathbb{Z}_3$ to $\mathbb{Z}_6$.

Problem 7.19. Prove that the only homomorphism from D_3 to $\mathbb{Z}_3$ is the trivial homomorphism.

Problem 7.20. Let F be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ and let D be the subset of differentiable functions on $\mathbb{R}$. It turns out that F is a group under addition of functions and D is a subgroup of F (you do not need to prove this). Define $\phi : D \to F$ via $\phi(f) = f'$ (where f' is the derivative of f). Prove that ϕ is a homomorphism. You may recall facts from calculus without proving them. Is ϕ one-to-one? Onto?

7.2 The Isomorphism Theorems

The next theorem is arguably the crowning achievement of the course.

Theorem 7.21 (The First Isomorphism Theorem)**.** Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Then

$$G_1/\ker(\phi) \cong \phi(G_1).$$

If ϕ is onto, then

$$G_1/\ker(\phi) \cong G_2.$$

Problem 7.22. Let $\phi : Q_8 \to V_4$ be the homomorphism described in Problem 7.16. Use the First Isomorphism Theorem to prove that $Q_8/\langle -1 \rangle \cong V_4$.

Problem 7.23. For $n \geq 2$, define $\phi : S_n \to \mathbb{Z}_2$ via

$$\phi(\sigma) = \begin{cases} 0, & \sigma \text{ even} \\ 1, & \sigma \text{ odd.} \end{cases}$$

Use the First Isomorphism Theorem to prove that $S_n/A_n \cong \mathbb{Z}_2$.

Problem 7.24. Use the First Isomorphism Theorem to prove that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$. Attempt to draw a picture of this using Cayley diagrams.

Problem 7.25. Use the First Isomorphism Theorem to prove that $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2) \cong \mathbb{Z}_4$.

The next theorem is a generalization of Theorem 7.7 and follows from the First Isomorphism Theorem together with Lagrange's Theorem.

Theorem 7.26. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. If G_1 is finite, then $|\phi(G_1)|$ divides $|G_1|$.

We finish the chapter by listing a few of the remaining isomorphism theorems.

Theorem 7.27 (The Second Isomorphism Theorem)**.** Let G be a group with $H \leq G$ and $N \trianglelefteq G$. Then

(a) $HN := \{hn \mid h \in H, n \in N\} \leq G$;

(b) $N \trianglelefteq HN$;

(c) $H \cap N \trianglelefteq H$;

(d) $H/(H \cap N) \cong HN/N$.

Theorem 7.28 (The Third Isomorphism Theorem)**.** Let G be a group with $H, K \trianglelefteq G$ and $K \leq H$. Then $H/K \trianglelefteq G/K$ and

$$G/H \cong (G/K)/(H/K).$$

The last isomorphism theorem is sometimes called the *Lattice Isomorphism Theorem*.

Theorem 7.29 (The Fourth Isomorphism Theorem)**.** Let G be a group with $N \trianglelefteq G$. Then there is a bijection from the set of subgroups of G that contain N onto the set of subgroups of G/N. In particular, every subgroup G is of the form H/N for some subgroup H of G containing N (namely, its preimage in G under the canonical projection homomorphism from G to G/N.) This bijection has the following properties: for all $H, K \leq G$ with $N \leq H$ and $N \subseteq K$, we have

(a) $H \leq K$ if and only if $H/N \leq K/N$

(b) If $H \leq K$, then $[K : H] = [K/N : H/N]$

(c) $\langle H, K\rangle/N = \langle H/N, K/N\rangle$

(d) $(H \cap K)/N = H/N \cap K/N$

(e) $H \trianglelefteq G$ if and only if $H/N \trianglelefteq G/N$.

Chapter 8

An Introduction to Rings

8.1 Definitions and Examples

Recall that a group is a set together with a single binary operation, which together satisfy a few modest properties. Loosely speaking, a ring is a set together with two binary operations (called addition and multiplication) that are related via a distributive property.

Definition 8.1. A **ring** R is a set together with two binary operations $+$ and $\cdot$ (called **addition** and **multiplication**, respectively) satisfying the following:

(i) $(R, +)$ is an abelian group.

(ii) $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

(iii) The **distributive property** holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$.

Remark 8.2. We make a couple comments about notation.

(a) We often write ab in place of $a \cdot b$.

(b) The additive inverse of the ring element $a \in R$ is denoted $-a$.

Theorem 8.3. If R is a ring, then for all $a, b \in R$:

(a) $0a = a0 = 0$

(b) $(-a)b = a(-b) = -(ab)$

(c) $(-a)(-b) = ab$

Definition 8.4. A ring R is called **commutative** if multiplication is commutative.

Definition 8.5. A ring R is said to have an **identity** (or called a **ring with 1**) if there is an element $1 \in R$ such that $1a = a1 = a$ for all $a \in R$.

Problem 8.6. Justify that $\mathbb{Z}$ is a commutative ring with 1 under the usual operations of addition and multiplication. Which elements have multiplicative inverses in $\mathbb{Z}$?

Problem 8.7. Justify that $\mathbb{Z}_n$ is a commutative ring with 1 under addition and multiplication mod n.

Problem 8.8. Consider the set $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Which elements have multiplicative inverses in $\mathbb{Z}_{10}$?

Problem 8.9. For each of the following, find a positive integer n such that the ring $\mathbb{Z}_n$ does not have the stated property.

(a) $a^2 = a$ implies $a = 0$ or $a = 1$.

(b) $ab = 0$ implies $a = 0$ or $b = 0$.

(c) $ab = ac$ and $a \neq 0$ imply $b = c$.

Theorem 8.10. If R is a ring with 1, then the multiplicative identity is unique and $-a = (-1)a$.

Problem 8.11. Requiring $(R, +)$ to be a group is fairly natural, but why require $(R, +)$ to be abelian? Suppose R has a 1. Compute $(1 + 1)(a + b)$ in two different ways.

Definition 8.12. A ring R with 1 (with $1 \neq 0$) is called a **division ring** if every nonzero element in R has a multiplicative inverse: if $a \in R \setminus \{0\}$, then there exists $b \in R$ such that $ab = ba = 1$.

Definition 8.13. A commutative division ring is called a **field**.

Definition 8.14. A nonzero element a in a ring R is called a **zero divisor** if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

Problem 8.15. Are there any zero divisors in $\mathbb{Z}_{10}$? If so, find all of them.

Problem 8.16. Are there any zero divisors in $\mathbb{Z}_5$? If so, find all of them.

Problem 8.17. Provide an example of a ring R and elements $a, b \in R$ such that $ax = b$ has more than one solution. How does this compare with groups?

Theorem 8.18 (Cancellation Law)**.** Assume $a, b, c \in R$ such that a is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$.

Definition 8.19. Assume R is a ring with 1 with $1 \neq 0$. An element $u \in R$ is called a **unit** in R if u has a multiplicative inverse (i.e., there exists $v \in R$ such that $uv = vu = 1$). The set of units in R is denoted $U(R)$.

Problem 8.20. Consider the ring $\mathbb{Z}_{20}$.

(a) Find $U(\mathbb{Z}_{20})$.

(b) Find the zero divisors of $\mathbb{Z}_{20}$.

(c) Any observations?

Theorem 8.21. If $U(R) \neq \emptyset$, then $U(R)$ forms a group under multiplication.

Remark 8.22. We make a few observations.

(a) A field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $U(F) = F \setminus \{0\}$.

(b) Zero divisors can never be units.

(c) Fields never have zero divisors.

Definition 8.23. A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

Remark 8.24. The Cancellation Law (Theorem 8.18) holds in integral domains for any three elements.

Theorem 8.25. Any finite integral domain is a field.

Example 8.26. Here are a few examples. Details left as an exercise.

(a) **Zero Ring**: If $R = \{0\}$, we can turn R into a ring in the obvious way. The zero ring is a finite commutative ring with 1. It is the only ring where the additive and multiplicative identities are equal. The zero ring is not a division ring, not a field, and not an integral domain.

(b) **Trivial Ring:** Given any abelian group R, we can turn R into a ring by defining multiplication via $ab = 0$ for all $a, b \in R$. Trivial rings are commutative rings in which every nonzero element is a zero divisor. Hence a trivial ring is not a division ring, not a field, and not a integral domain.

(c) The integers form an integral domain, but $\mathbb{Z}$ is not a division ring, and hence not a field.

(d) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields under the usual operations of addition and multiplication.

(e) The group of units $U(\mathbb{Z}_n)$ is the set of elements in $\mathbb{Z}_n$ that are relatively prime to n. That is, $U(\mathbb{Z}_n) = U_n$. All other nonzero elements are zero divisors. It turns out that $\mathbb{Z}_n$ forms a finite field if and only if n is prime.

(f) The set of even integers $2\mathbb{Z}$ forms a commutative ring under the usual operations of addition and multiplication. However, $2\mathbb{Z}$ does not have a 1, and hence cannot be a division ring nor a field. Moreover, if you look closely at the definition of integral domain, you'll see that $2\mathbb{Z}$ is also not an integral domain since $2\mathbb{Z}$ does not contain a multiplicative identity.

(g) **Polynomial Ring:** Fix a commutative ring R. Let $R[x]$ denote the set of polynomials in the variable x with coefficients in R. Then $R[x]$ is a commutative ring. Moreover, $R[x]$ is a ring with 1 if and only if R is a ring with 1. The units of $R[x]$ are exactly the units of R (if there are any). So, $R[x]$ is never a division ring nor a field. However, if R is an integral domain, then so is $R[x]$.

(h) **Matrix Ring:** Fix a ring R and let n be a positive integer. Let $M_n(R)$ be the set of $n \times n$ matrices with entries from R. Then $M_n(R)$ forms a ring under ordinary matrix addition and multiplication. If R is nontrivial and $n \geq 2$, then $M_n(R)$ always has zero divisors and $M_n(R)$ is not commutative even if R is. If R has a 1, then the matrix with 1's down the diagonal and 0's elsewhere is the multiplicative identity in $M_n(R)$. In this case, the group of units is the set of invertible $n \times n$ matrices, denoted $GL_n(R)$ and called the **general linear group of degree** n **over** R.

(i) **Quadratic Field:** Define $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. It turns out that $\mathbb{Q}(\sqrt{2})$ is a field. In fact, we can replace 2 with any rational number that is not a perfect square in $\mathbb{Q}$.

(j) **Hamilton Quaternions:** Define $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i, j, k \in Q_8\}$ Then $\mathbb{H}$ forms a ring, where addition is definite componentwise in i, j, and k and multiplication is defined by expanding products and the simplifying using the relations of Q_8. It turns out that $\mathbb{H}$ is a non-commutative ring with 1.

Problem 8.27. Find an example of a ring R and an element $a \in R \setminus \{0\}$ such that a is neither a zero divisor nor a unit.

Definition 8.28. A **subring** of a ring R is a subgroup of R under addition that is also closed under multiplication.

Remark 8.29. The property "is a subring" is clearly transitive. To show that a subset S of a ring R is a subring, it suffices to show that $S \neq \emptyset$, S is closed under subtraction, and S is closed under multiplication.

Example 8.30. Here are a few quick examples.

(a) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which in turn is a subring of $\mathbb{C}$.

(b) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(c) The set $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{2})$.

(d) The ring R is a subring of $R[x]$ if we identify R with set of constant functions.

(e) The set of polynomials with zero constant term in $R[x]$ is a subring of $R[x]$.

(f) $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$.

(g) $\mathbb{Z}_n$ is *not* a subring of $\mathbb{Z}$ as the operations are different.

Problem 8.31. Consider the ring $\mathbb{Z}_{10}$ from Problem 8.8. Let $S = \{0, 2, 4, 6, 8\}$.

(a) Argue that S is a subring of $\mathbb{Z}_{10}$.

(b) Is S a ring with 1? If so, find the multiplicative identity. If not, explain why.

(c) Is S a field? Justify your answer.

Problem 8.32. Suppose R is a ring and let $a \in R$. Define $S = \{x \in R \mid ax = 0\}$. Prove that S is a subring of R.

Problem 8.33. Consider the ring $\mathbb{Z}$. It turns out that $2\mathbb{Z}$ and $3\mathbb{Z}$ are subrings (but you don't need to prove this). Determine whether $2\mathbb{Z} \cup 3\mathbb{Z}$ is a subring of $\mathbb{Z}$. Justify your answer.

8.2 Ring Homomorphisms

Definition 8.34. Let R and S be rings. A **ring homomorphism** is a map $\phi : R \to S$ satisfying

(a) $\phi(a+b) = \phi(a) + \phi(b)$

(b) $\phi(ab) = \phi(a)\phi(b)$

for all $a, b \in R$. The **kernel** of ϕ is defined via $\ker(\phi) = \{a \in R \mid \phi(a) = 0\}$. If ϕ is a bijection, then ϕ is called an **isomorphism**, in which case, we say that R and S are **isomorphic rings** and write $R \cong S$.

Example 8.35.

(a) For $n \in \mathbb{Z}$, define $\phi_n : \mathbb{Z} \to \mathbb{Z}$ via $\phi_n(x) = nx$. We see that $\phi_n(x+y) = n(x+y) = nx+ny = \phi_n(x)+\phi_n(y)$. However, $\phi_n(xy) = n(xy)$ while $\phi_n(x)\phi_n(y) = (nx)(ny) = n^2xy$. It follows that ϕ_n is a ring homomorphism exactly when $n \in \{0, 1\}$.

(b) Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ via $\phi(p(x)) = p(0)$ (called **evaluation at 0**). It turns out that ϕ is a ring homomorphism, where $\ker(\phi)$ is the set of polynomials with 0 constant term.

Problem 8.36. For each of the following, determine whether the given function is a ring homomorphism. Justify your answers.

(a) Define $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{12}$ via $\phi(x) = 3x$.

(b) Define $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ via $\phi(x) = 5x$.

(c) Let $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. Define $\phi : \mathbb{C} \to S$ via $\phi(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

(d) Let $T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$. Define $\phi : T \to \mathbb{Z}$ via $\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = a$.

Theorem 8.37. Let $\phi : R \to S$ be a ring homomorphism.

(a) $\phi(R)$ is a subring of S.

(b) $\ker(\phi)$ is a subring of R.

Problem 8.38. Suppose $\phi : R \to S$ is a ring homomorphism such that R is a ring with 1, call it 1_R. Prove that $\phi(1_R)$ is the multiplicative identity in $\phi(R)$ (which is a subring of S). Can you think of an example of a ring homomorphism where S has a multiplicative identity that is not equal to $\phi(1_R)$?

Theorem 8.37(b) states that the kernel of a ring homomorphism is a subring. This is analogous to the kernel of a group homomorphism being a subgroup. However, recall that the kernel of a group homomorphism is also a normal subgroup. Like the situation with groups, we can say something even stronger about the kernel of a ring homomorphism. This will lead us to the notion of an **ideal**.

Theorem 8.39. Let $\phi : R \to S$ be a ring homomorphism. If $a \in \ker(\phi)$ and $r \in R$, then $ar, ra \in \ker(\phi)$. That is, $\ker(\phi)$ is closed under multiplication by elements of R.

8.3 Ideals and Quotient Rings

Recall that in the case of a homomorphism ϕ of groups, the cosets of $\ker(\phi)$ have the structure of a group (that happens to be isomorphic to the image of ϕ by the First Isomorphism Theorem). In this case, $\ker(\phi)$ is the identity of the associated quotient group. Moreover, recall that every kernel is a normal subgroup of the domain and every normal subgroup can be realized as the kernel of some group homomorphism. Can we do the same sort of thing for rings?

Let $\phi : R \to S$ be a ring homomorphism with $\ker(\phi) = I$. Note that ϕ is also a group homomorphism of abelian groups and the cosets of $\ker(\phi)$ are of the form $r + I$. More specifically, if $\phi(r) = a$, then $\phi^{-1}(a) = r + I$.

These cosets naturally have the structure of a ring isomorphic to the image of ϕ:

$$(r + I) + (s + I) = (r + s) + I \tag{8.1}$$

$$(r + I)(s + I) = (rs) + I \tag{8.2}$$

The reason for this is that if $\phi^{-1}(a) = X$ and $\phi^{-1}(b) = Y$, then the inverse image of $a + b$ and ab are $X + Y$ and XY, respectively.

The corresponding ring of cosets is called the **quotient ring** of R by $I = \ker(\phi)$ and is denoted by R/I. The additive structure of the quotient ring R/I is exactly the additive quotient group of the additive abelian group R by the normal subgroup I (all subgroups are normal in abelian groups). When I is the kernel of some ring homomorphism ϕ, the additive abelian quotient group R/I also has a multiplicative structure defined in (2) above, making R/I into a ring.

Can we make R/I into a ring for any subring I?

The answer is "no" in general, just like in the situation with groups. But perhaps this isn't obvious because if I is an arbitrary subring of R, then I is necessarily an additive subgroup of the abelian group R, which implies that I is an additive normal subgroup of the group R. It turns out that the multiplicative structure of R/I may not be well-defined if I is an arbitrary subring.

Let I be an arbitrary *subgroup* of the additive group R. Let $r+I$ and $s+I$ be two arbitrary cosets. In order for multiplication of the cosets to be well-defined, the product of the two cosets must be independent of choice of representatives. Let $r+\alpha$ and $s+\beta$ be arbitrary representatives of $r+I$ and $s+I$, respectively ($\alpha, \beta \in I$), so that $r+I = (r+\alpha)+I$ and $s+I = (s+\beta)+I$. We must have

$$(r+\alpha)(s+\beta)+I = rs+I. \tag{8.3}$$

This needs to be true for all possible choices of $r, s \in R$ and $\alpha, \beta \in I$. In particular, it must be true when $r = s = 0$. In this case, we must have

$$\alpha\beta + I = I. \tag{8.4}$$

But this only happens when $\alpha\beta \in I$. That is, one requirement for multiplication of cosets to be well-defined is that I must be closed under multiplication, making I a *subring*.

Next, if we let $s = 0$ and let r be arbitrary, we see that we must have $r\beta \in I$ for every $r \in R$ and every $\beta \in I$. That is, it must be the case that I is closed under multiplication on the left by elements from R. Similarly, letting $r = 0$, we can conclude that we must have I closed under multiplication on the right by elements from R.

On the other hand, if I is closed under multiplication on the left and on the right by elements from R, then it is clear that relation (4) above is satisfied.

It is easy to verify that if the multiplication of cosets defined in (2) above is well-defined, then this multiplication makes the additive quotient group R/I into a ring (just check the axioms for being a ring).

We have shown that the quotient R/I of the ring R by a subgroup I has a natural ring structure if and only if I is closed under multiplication on the left and right by elements of R (which also forces I to be a subring). Such subrings are called **ideals**.

Definition 8.40. Let R be a ring and let I be a subset of R.

(a) I is a **left ideal** (respectively, **right ideal**) of R if I is a subring and $rI \subseteq I$ (respectively, $Ir \subseteq I$) for all $r \in R$.

(b) I is an **ideal** (or **two-sided ideal**) if I is both a left and a right ideal.

Here's a summary of everything that just happened.

Theorem 8.41. Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I) = (r+s)+I \tag{8.5}$$

$$(r+I)(s+I) = (rs)+I \tag{8.6}$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well-defined, then I is an ideal of R.

Theorem 8.42. If R a commutative ring and I is an ideal of R, then R/I is a commutative ring.

Theorem 8.43. Suppose I and J are ideals of the ring R. Then $I \cap J$ is an ideal of R.

As you might expect, we have some isomorphism theorems.

Theorem 8.44 (First Isomorphism Theorem for Rings)**.** If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R and $R/\ker(\phi) \cong \phi(R)$.

We also have the expected Second, Third, and Fourth Isomorphism Theorems for rings. The next theorem tells us that a subring is an ideal if and only if it is a kernel of a ring homomorphism.

Theorem 8.45. If I is any ideal of R, then the **natural projection** $\pi : R \to R/I$ defined via $\pi(r) = r + I$ is a surjective ring homomorphism with $\ker(\pi) = I$.

For the remainder of this section, assume that R is a ring with identity $1 \neq 0$.

Definition 8.46. Let A be any subset of R. Let (A) denote the smallest ideal of R containing A, called the **ideal generated by** A. If A consists of a single element, say $A = \{a\}$, then $(a) := (\{a\})$ is called a **principal ideal**.

Remark 8.47. The following facts are easily verified.

(a) (A) is the intersection of all ideals containing A.

(b) If R is commutative, then $(a) = aR := \{ar \mid r \in R\}$.

Example 8.48. In $\mathbb{Z}$, $n\mathbb{Z} = (n) = (-n)$. In fact, these are the only ideals in $\mathbb{Z}$ (since these are the only subgroups). So, all the ideals in $\mathbb{Z}$ are principal. If m and n are positive integers, then $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if m divides n. Moreover, we have $(m, n) = (d)$, where d is the greatest common divisor of m and n.

Problem 8.49. Consider the ideal $(2, x)$ in $\mathbb{Z}[x]$. Note that $(2, x) = \{2p(x)+xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$. Argue that $(2, x)$ is not a principal ideal, i.e., there is no single polynomial in $\mathbb{Z}[x]$ that we can use to generate $(2, x)$.

Theorem 8.50. Assume R is a commutative ring with $1 \neq 0$. Let I be an ideal of R. Then $I = R$ if and only if I contains a unit.

Theorem 8.51. Assume R is a commutative ring with $1 \neq 0$. Then R is a field if and only if its only ideals are (0) and R.

Loosely speaking, the previous results say that fields are "like simple groups" (i.e, groups with no non-trivial normal subgroups).

Corollary 8.52. If R is a field, then every nonzero ring homomorphism from R into another ring is an injection.

8.4 Maximal and Prime Ideals

In this section of notes, we will study two important classes of ideals, namely **maximal** and **prime** ideals, and study the relationship between them. Throughout this entire section, we assume that all rings have a multiplicative identity $1 \neq 0$.

Definition 8.53. Assume R is a commutative ring with 1. An ideal M in a ring R is called a **maximal ideal** if $M \neq R$ and the only ideals containing M are M and R.

Example 8.54. Here are a few examples. Checking the details is left as an exercise.

(a) In $\mathbb{Z}$, all the ideals are of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}^+$. The maximal ideals correspond to the ideals $p\mathbb{Z}$, where p is prime.

(b) Consider the integral domain $\mathbb{Z}[x]$. The ideals (x) (i.e., the subring containing polynomials with 0 constant term) and (2) (i.e, the set of polynomials with even coefficients) are not maximal since both are contained in the proper ideal $(2, x)$. However, as we shall see soon, $(2, x)$ is maximal in $\mathbb{Z}[x]$.

(c) The zero ring has no maximal ideals.

(d) Consider the abelian group $\mathbb{Q}$ under addition. We can turn $\mathbb{Q}$ into a trivial ring by defining $ab = 0$ for all $a, b \in \mathbb{Q}$. In this case, the ideals are exactly the additive subgroups of $\mathbb{Q}$. However, $\mathbb{Q}$ has no maximal subgroups, and so $\mathbb{Q}$ has no maximal ideals.

The next result states that rings with an identity $1 \neq 0$ always have maximal ideals. It turns out that we won't need this result going forward, so we'll skip its proof. However, it is worth noting that all known proofs make use of Zorn's Lemma (equivalent to the Axiom of Choice), which is also true for the proofs that a finitely generated group has maximal subgroups or that every vector spaces has a basis.

Theorem 8.55. In a ring with 1, every proper ideal is contained in a maximal ideal.

For commutative rings, there is a very nice characterization about maximal ideals in terms of the structure of their quotient rings.

Theorem 8.56. Assume R is a commutative ring with 1. Then M is a maximal ideal if and only if the quotient ring R/M is a field.

Example 8.57. We can use the previous theorem to verify whether an ideal is maximal.

(a) Recall that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ and that $\mathbb{Z}_n$ is a field if and only if n is prime. We can conclude that $n\mathbb{Z}$ is a maximal ideal precisely when n is prime.

(b) Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ via $\phi(p(x)) = p(0)$. Then ϕ is surjective and $\ker(\phi) = (x)$. By the First Isomorphism Theorem for Rings, we see that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. However, $\mathbb{Z}$ is not a field. Hence (x) is not maximal in $\mathbb{Z}[x]$. Now, define $\psi : \mathbb{Z} \to \mathbb{Z}_2$ via $\psi(x) = x \mod 2$ and consider the composite homomorphism $\psi \circ \phi : \mathbb{Z} \to \mathbb{Z}_2$. It is clear that $\psi \circ \phi$ is onto and the kernel of $\psi \circ \phi$ is given by $\{p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\} = (2, x)$. Again by the First Isomorphism Theorem for Rings, $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field, $(2, x)$ is a maximal ideal.

Definition 8.58. Assume R is a commutative ring with 1. An ideal P is called a **prime ideal** if $P \neq R$ and whenever the product $ab \in P$ for $a, b \in R$, then at least one of a or b is in P.

Example 8.59. In any integral domain, the 0 ideal (0) is a prime ideal. What if the ring is not an integral domain?

Remark 8.60. The notion of a prime ideal is a generalization of "prime" in $\mathbb{Z}$. Suppose $n \in \mathbb{Z}^+ \setminus \{1\}$ such that n divides ab. In this case, n is guaranteed to divide either a or b exactly when n is prime. Now, let $n\mathbb{Z}$ be a proper ideal in $\mathbb{Z}$ with $n > 1$ and suppose $ab \in \mathbb{Z}$ for $a, b \in \mathbb{Z}$. In order for $n\mathbb{Z}$ to be a prime ideal, it must be true that n divides either a or b. However, this is only guaranteed to be true for all $a, b \in \mathbb{Z}$ when p is prime. That is, the nonzero prime ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$, where p is prime. Note that in the case of the integers, the maximal and nonzero prime ideals are the same.

Theorem 8.61. Assume R is a commutative ring with 1. Then P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Corollary 8.62. Assume R is a commutative ring with 1. Every maximal ideal of R is a prime ideal.

Example 8.63. Recall that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, it must be the case that (x) is a prime ideal in $\mathbb{Z}[x]$. However, as we saw in an earlier example, (x) is not maximal in $\mathbb{Z}[x]$ since $\mathbb{Z}$ is not a field. This shows that the converse of the previous corollary is not true.

Appendix A

Elements of Style for Proofs

Years of elementary school math taught us incorrectly that the answer to a math problem is just a single number, "the right answer." It is time to unlearn those lessons; those days are over. From here on out, mathematics is about discovering proofs and writing them clearly and compellingly.

The following rules apply whenever you write a proof. Keep these rules handy so that you may refer to them as you write your proofs.

1. **The burden of communication lies on you, not on your reader.** It is your job to explain your thoughts; it is not your reader's job to guess them from a few hints. You are trying to convince a skeptical reader who doesn't believe you, so you need to argue with airtight logic in crystal clear language; otherwise the reader will continue to doubt. If you didn't write something on the paper, then (a) you didn't communicate it, (b) the reader didn't learn it, and (c) the grader has to assume you didn't know it in the first place.

2. **Tell the reader what you're proving.** The reader doesn't necessarily know or remember what "Theorem 2.13" is. Even a professor grading a stack of papers might lose track from time to time. Therefore, the statement you are proving should be on the same page as the beginning of your proof. For an exam this won't be a problem, of course, but on your homework, recopy the claim you are proving. This has the additional advantage that when you study for exams by reviewing your homework, you won't have to flip back in the notes/textbook to know what you were proving.

3. **Use English words.** Although there will usually be equations or mathematical statements in your proofs, use English sentences to connect them and display their logical relationships. If you look in your notes/textbook, you'll see that each proof consists mostly of English words.

4. **Use complete sentences.** If you wrote a history essay in sentence fragments, the reader would not understand what you meant; likewise in mathematics you must use complete sentences, with verbs, to convey your logical train of thought.

   Some complete sentences can be written purely in mathematical symbols, such as equations (e.g., $a^3 = b^{-1}$), inequalities (e.g., $x < 5$), and other relations (like $5 \mid 10$ or

$7 \in \mathbb{Z}$). These statements usually express a relationship between two mathematical *objects*, like numbers or sets. However, it is considered bad style to begin a sentence with symbols. A common phrase to use to avoid starting a sentence with mathematical symbols is "We see that..."

5. **Show the logical connections among your sentences.** Use phrases like "Therefore" or "because" or "if..., then..." or "if and only if" to connect your sentences.

6. **Know the difference between statements and objects.** A mathematical object is a *thing*, a noun, such as a group, an element, a vector space, a number, an ordered pair, etc. Objects either exist or don't exist. Statements, on the other hand, are mathematical *sentences*: they can be true or false.

   When you see or write a cluster of math symbols, be sure you know whether it's an object (e.g., "$x^2 + 3$") or a statement (e.g., "$x^2 + 3 < 7$"). One way to tell is that every mathematical statement includes a verb, such as $=$, $\leq$, "divides", etc.

7. **The symbol "=" means "equals".** Don't write $A = B$ unless you mean that A actually equals B. This rule seems obvious, but there is a great temptation to be sloppy. In calculus, for example, some people might write $f(x) = x^2 = 2x$ (which is false), when they really mean that "if $f(x) = x^2$, then $f'(x) = 2x$."

8. **Don't interchange $=$ and $\implies$.** The equals sign connects two *objects*, as in "$x^2 = b$"; the symbol "$\implies$" is an abbreviation for "implies" and connects two *statements*, as in "$a + b = a \implies b = 0$." You should avoid using $\implies$ in your formal write-ups.

9. **Avoid logical symbols in your proofs.** Similar to $\implies$, you should avoid using the logical symbols $\forall, \exists, \vee, \wedge$, and $\iff$ in your formal write-ups. These symbols are useful for abbreviating in your scratch work.

10. **Say exactly what you mean.** Just as $=$ is sometimes abused, so too people sometimes write $A \in B$ when they mean $A \subseteq B$, or write $a_{ij} \in A$ when they mean that a_{ij} is an entry in matrix A. Mathematics is a very precise language, and there is a way to say exactly what you mean; find it and use it.

11. **Don't write anything unproven.** Every statement on your paper should be something you *know* to be true. The reader expects your proof to be a series of statements, each proven by the statements that came before it. If you ever need to write something you don't yet know is true, you *must* preface it with words like "assume," "suppose," or "if" (if you are temporarily assuming it), or with words like "we need to show that" or "we claim that" (if it is your goal). Otherwise the reader will think they have missed part of your proof.

12. **Write strings of equalities (or inequalities) in the proper order.** When your reader sees something like
$$A = B \leq C = D,$$
   he/she expects to understand easily why $A = B$, why $B \leq C$, and why $C = D$, and he/she expects the *point* of the entire line to be the more complicated fact that $A \leq$

D. For example, if you were computing the distance d of the point $(12,5)$ from the origin, you could write

$$d = \sqrt{12^2 + 5^2} = 13.$$

In this string of equalities, the first equals sign is true by the Pythagorean theorem, the second is just arithmetic, and the *point* is that the first item equals the last item: $d = 13$.

A common error is to write strings of equations in the wrong order. For example, if you were to write "$\sqrt{12^2 + 5^2} = 13 = d$", your reader would understand the first equals sign, would be baffled as to how we know $d = 13$, and would be utterly perplexed as to why you wanted or needed to go through 13 to prove that $\sqrt{12^2 + 5^2} = d$.

13. **Avoid circularity.** Be sure that no step in your proof makes use of the conclusion!

14. **Don't write the proof backwards.** Beginning students often attempt to write "proofs" like the following, which attempts to prove that $\tan^2(x) = \sec^2(x) - 1$:

$$\begin{aligned}
\tan^2(x) &= \sec^2(x) - 1 \\
\left(\frac{\sin(x)}{\cos(x)}\right)^2 &= \frac{1}{\cos^2(x)} - 1 \\
\frac{\sin^2(x)}{\cos^2(x)} &= \frac{1 - \cos^2(x)}{\cos^2(x)} \\
\sin^2(x) &= 1 - \cos^2(x) \\
\sin^2(x) + \cos^2(x) &= 1 \\
1 &= 1
\end{aligned}$$

Notice what has happened here: the student *started* with the conclusion, and deduced the true statement "$1 = 1$." In other words, he/she has proved "If $\tan^2(x) = \sec^2(x) - 1$, then $1 = 1$," which is true but highly uninteresting.

Now this isn't a bad way of *finding* a proof. Working backwards from your goal often is a good strategy *on your scratch paper*, but when it's time to *write* your proof, you have to start with the hypotheses and work to the conclusion.

Here is an example of a suitable proof for the desired result, where each expression

follows from the one immediately proceeding it:

$$\begin{aligned}
\sec^2(x) - 1 &= \frac{1}{\cos^2(x)} - 1 \\
&= \frac{1 - \cos^2(x)}{\cos^2(x)} \\
&= \frac{\sin^2(x)}{\cos^2(x)} \\
&= \left(\frac{\sin(x)}{\cos(x)}\right)^2 \\
&= (\tan(x))^2 \\
&= \tan^2(x).
\end{aligned}$$

15. **Be concise.** Most students err by writing their proofs too short, so that the reader can't understand their logic. It is nevertheless quite possible to be too wordy, and if you find yourself writing a full-page essay, it's probably because you don't really have a proof, but just an intuition. When you find a way to turn that intuition into a formal proof, it will be much shorter.

16. **Introduce every symbol you use.** If you use the letter "k," the reader should know exactly what k is. Good phrases for introducing symbols include "Let $n \in \mathbb{N}$," "Let k be the least integer such that…," "For every real number a…," and "Suppose that X is a counterexample."

17. **Use appropriate quantifiers (once).** When you introduce a variable $x \in S$, it must be clear to your reader whether you mean "for all $x \in S$" or just "for some $x \in S$." If you just say something like "$y = x^2$ where $x \in S$," the word "where" doesn't indicate whether you mean "for all" or "some".

    Phrases indicating the quantifier "for all" include "Let $x \in S$"; "for all $x \in S$"; "for every $x \in S$"; "for each $x \in S$"; etc. Phrases indicating the quantifier "some" (or "there exists") include "for some $x \in S$"; "there exists an $x \in S$"; "for a suitable choice of $x \in S$"; etc.

    On the other hand, don't introduce a variable more than once! Once you have said "Let $x \in S$," the letter x has its meaning defined. You don't *need* to say "for all $x \in S$" again, and you definitely should *not* say "let $x \in S$" again.

18. **Use a symbol to mean only one thing.** Once you use the letter x once, its meaning is fixed for the duration of your proof. You cannot use x to mean anything else.

19. **Don't "prove by example."** Most problems ask you to prove that something is true "for all"—You *cannot* prove this by giving a single example, or even a hundred. Your answer will need to be a logical argument that holds for *every example there possibly could be*.

On the other hand, if the claim that you are trying to prove involves the existence of a mathematical object with a particular property, then providing a specific example is sufficient.

20. **Write "Let $x = \ldots$," not "Let $\cdots = x$."** When you have an existing expression, say a^2, and you want to give it a new, simpler name like b, you should write "Let $b = a^2$," which means, "Let the new symbol b mean a^2." This convention makes it clear to the reader that b is the brand-new symbol and a^2 is the old expression he/she already understands.

    If you were to write it backwards, saying "Let $a^2 = b$," then your startled reader would ask, "What if $a^2 \neq b$?"

21. **Make your counterexamples concrete and specific.** Proofs need to be entirely general, but counterexamples should be absolutely concrete. When you provide an example or counterexample, make it as specific as possible. For a set, for example, you must name its elements, and for a function you must give its rule. Do not say things like "θ could be one-to-one but not onto"; instead, provide an actual function θ that *is* one-to-one but not onto.

22. **Don't include examples in proofs.** Including an example very rarely adds anything to your proof. If your logic is sound, then it doesn't need an example to back it up. If your logic is bad, a dozen examples won't help it (see rule 19). There are only two valid reasons to include an example in a proof: if it is a *counterexample* disproving something, or if you are performing complicated manipulations in a general setting and the example is just to help the reader understand what you are saying.

23. **Use scratch paper.** Finding your proof will be a long, potentially messy process, full of false starts and dead ends. Do all that on scratch paper until you find a real proof, and only then break out your clean paper to write your final proof carefully.

    Only sentences that actually contribute to your proof should be part of the proof. Do not just perform a "brain dump," throwing everything you know onto the paper before showing the logical steps that prove the conclusion. *That is what scratch paper is for.*

Appendix B

Fancy Mathematical Terms

Here are some important mathematical terms that you will encounter in this course and throughout your mathematical career.

1. **Definition**—a precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true.

2. **Theorem**—a mathematical statement that is proved using rigorous mathematical reasoning. In a mathematical paper, the term theorem is often reserved for the most important results.

3. **Lemma**—a minor result whose sole purpose is to help in proving a theorem. It is a stepping stone on the path to proving a theorem. Very occasionally lemmas can take on a life of their own (Zorn's lemma, Urysohn's lemma, Burnside's lemma, Sperner's lemma).

4. **Corollary**—a result in which the (usually short) proof relies heavily on a given theorem (we often say that "this is a corollary of Theorem A").

5. **Proposition**—a proved and often interesting result, but generally less important than a theorem.

6. **Conjecture**—a statement that is unproved, but is believed to be true (Collatz conjecture, Goldbach conjecture, twin prime conjecture).

7. **Claim**—an assertion that is then proved. It is often used like an informal lemma.

8. **Axiom/Postulate**—a statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proved (Euclid's five postulates, Zermelo-Frankel axioms, Peano axioms).

9. **Identity**—a mathematical expression giving the equality of two (often variable) quantities (trigonometric identities, Euler's identity).

10. **Paradox**—a statement that can be shown, using a given set of axioms and definitions, to be both true and false. Paradoxes are often used to show the inconsistencies in a flawed theory (Russell's paradox). The term paradox is often used informally to describe a surprising or counterintuitive result that follows from a given set of rules (Banach-Tarski paradox, Alabama paradox, Gabriel's horn).

Appendix C

Definitions in Mathematics

It is difficult to overstate the importance of definitions in mathematics. Definitions play a different role in mathematics than they do in everyday life.

Suppose you give your friend a piece of paper containing the definition of the rarely-used word **rodomontade**. According to the Oxford English Dictionary[*] (OED) it is:

> A vainglorious brag or boast; an extravagantly boastful, arrogant, or bombastic speech or piece of writing; an arrogant act.

Give your friend some time to study the definition. Then take away the paper. Ten minutes later ask her to define rodomontade. Most likely she will be able to give a reasonably accurate definition. Maybe she'd say something like, "It is a speech or act or piece of writing created by a pompous or egotistical person who wants to show off how great they are." It is unlikely that she will have quoted the OED word-for-word. In everyday English that is fine—you would probably agree that your friend knows the meaning of the rodomontade. This is because most definitions are *descriptive*. They describe the common usage of a word.

Let us take a mathematical example. The OED[†] gives this definition of *continuous*.

> Characterized by continuity; extending in space without interruption of substance; having no interstices or breaks; having its parts in immediate connection; connected, unbroken.

Likewise, we often hear calculus students speak of a continuous function as one whose graph can be drawn "without picking up the pencil." This definition is descriptive. (As we learned in calculus the picking-up-the-pencil description is not a perfect description of continuous functions.) This is not a mathematical definition.

Mathematical definitions are *prescriptive*. The definition must prescribe the exact and correct meaning of a word. Contrast the OED's descriptive definition of continuous with the the definition of continuous found in a real analysis textbook.

> A function $f : A \to \mathbb{R}$ is **continuous at a point** $c \in A$ if, for all $\varepsilon > 0$, there exists $\delta > 0$ such that whenever $|x-c| < \delta$ (and $x \in A$) it follows that $|f(x)-f(c)| < \varepsilon$. If f

[*] http://www.oed.com/view/Entry/166837
[†] http://www.oed.com/view/Entry/40280

> is continuous at every point in the domain A, then we say that f is **continuous on** A.[‡]

In mathematics there is very little freedom in definitions. Mathematics is a deductive theory; it is impossible to state and prove theorems without clear definitions of the mathematical terms. The definition of a term must completely, accurately, and unambiguously describe the term. Each word is chosen very carefully and the order of the words is critical. In the definition of continuity changing "there exists" to "for all," changing the orders of quantifiers, changing $<$ to $\leq$ or $>$, or changing $\mathbb{R}$ to $\mathbb{Z}$ would completely change the meaning of the definition.

What does this mean for you, the student? Our recommendation is that at this stage you memorize the definitions word-for-word. It is the safest way to guarantee that you have it correct. As you gain confidence and familiarity with the subject you may be ready to modify the wording. You may want to change "for all" to "given any" or you may want to change $|x-c|<\delta$ to $-\delta<x-c<\delta$ or to "the distance between x and c is less than δ."

Of course, memorization is not enough; you must have a conceptual understanding of the term, you must see how the formal definition matches up with your conceptual understanding, and you must know how to work with the definition. It is perhaps with the first of these that descriptive definitions are useful. They are useful for building intuition and for painting the "big picture." Only after days (weeks, months, years?) of experience does one get an intuitive feel for the ε,δ-definition of continuity; most mathematicians have the "picking-up-the-pencil" definitions in their head. This is fine as long as we know that it is imperfect, and that when we prove theorems about continuous functions in mathematics we use the mathematical definition.

We end this discussion with an amusing real-life example in which a descriptive definition was not sufficient. In 2003 the German version of the game show *Who wants to be a millionaire?* contained the following question: "Every rectangle is: (a) a rhombus, (b) a trapezoid, (c) a square, (d) a parallelogram."

The confused contestant decided to skip the question and left with €4000. Afterward the show received letters from irate viewers. Why were the contestant and the viewers upset with this problem? Clearly a rectangle is a parallelogram, so (d) is the answer. But what about (b)? Is a rectangle a trapezoid? We would describe a trapezoid as a quadrilateral with a pair of parallel sides. But this leaves open the question: can a trapezoid have *two* pairs of parallel sides or must there only be *one* pair? The viewers said two pairs is allowed, the producers of the television show said it is not. This is a case in which a clear, precise, mathematical definition is required.

[‡]This definition is taken from page 109 of Stephen Abbott's *Understanding Analysis*, but the definition would be essentially the same in any modern real analysis textbook.