Elementary Abstract Algebra

A First Draft

Emma Norbrothen Wright

August 5, 2016

Welcome

Thank you for considering this text.

Licensing

Please adapt this text to your needs. Dr. Wright asks that if you choose to use the text, please do the following.

1. Email Dr. Wright to inform her of your choice, and she will pass the message on to Dr. Clark. They both will be very pleased to learn that the text has helped others.

2. Encourage your students to donate a few dollars to a charity as a gesture of gratitude, and remind them that they are more fortunate than

most. Listed below are a few of Dr. Wright's favorite charities, and she encourages you to provide more.

- Children's Hospital at Dartmouth: This is New Hampshire's only full-service children's hospital. (Donate.)
- Big Cat Rescue: This organization provides a sanctuary for abused big cats, education to help the future of big cats, and exposure to current laws and bills that affect big cats. (Donate.)

Letter to the Instructor

In the academic year of 2015-2016, I became interested in the O.E.R. movement. Luckily, I found Dr. W. Edwin Clark's "Elementary Abstract Algebra" while searching through O.E.R. repositories. His book provided me the most critical piece: a starting point. Of course, it provided so much more, and you will see influences of the original text throughout this text.

In the spring of 2016, I taught Abstract Algebra while using and modifying Clark's text. Knowing that I would inadvertently leave gaps as I wrote, and having a malleable text, I required my students to contribute to the text. *Pay it forward.* Make the text better, more complete, is what I told my students. Thus, as part of the semester grade, each student had to contribute two of the following.

1. Example
2. Computational exercise and solution
3. Hint about a theoretical exercise

If you use this text, I highly recommend having your students contribute to it. My students reported that contributing to it forced them to reread, to think more deeply, and to think about more types of problems. Many reported that their contributions were about topics they struggled with and used their contributions to solicit more personalized feedback. Student contributions are marked with a Ⓢ symbol. I sincerely hope your students find my students' contributions helpful.

The first exercise in every section is (or will be) an Always/Sometimes/Never exercise, which is one of my favorite types of exercises. To me, they ask, "Is the following statement always true, sometimes true, or never true?" Below is an explanation of these three options.

- Always: This statement is always true, in every situation. No matter what values are substituted into the variables, this statement will be true.
- Sometimes: This statement is sometimes true, and it depends of the values of the variables. I can find at least one case that breaks this statement, and I can find at least one case in which this statement holds.
- Never: This statement is never true in any situation. No matter what values are substituted into the variables, this statement will be false.

This exercise is a quick way to check for understanding. The instructions also have the student justify their claim because sometimes the wording may lead to multiple interpretations. Moreover, you or your students may interpret these instructions differently.

This text is still under construction. I suppose that's part of the point of O.E.R. For example, not all of my students' contributions have been included

yet. Please feel free to use it, contribute to it, modify it, and redistribute it. My next goals for the text are to add more about polynomials and add more linear algebra connections. Feel free to contribute those topics to the text, or take it in an entirely different direction.

I sincerely hope you find this text helpful. Please feel free to use it, and if you do, please let me know. I would love to have a conversation with you about your O.E.R. experience.

Cheers,
Emma

Appreciation

The O.E.R. movement is, in part, about working together within a community to further education. Thus, I have many people to thank for their guidance, suggestions, and patience. In particular, I would like to acknowledge the following people for their help.

- Dr. W. Edwin Clark (University of South Florida), for his original text and insight
- My 2016 Abstract Algebra class (Plymouth State University), for their contributions, openness, and patience
- Christin Wixson (Plymouth State University) and Robin DeRosa (Plymouth State University), for the motivation and guidance in joining the O.E.R. movement
- Stephen Adams (Cabrini University), Nathaniel Schwartz (Washington College), and John Hutchens (Winston-Salem State University), for their feedback

Contents

Chapter 1

Dihedral Groups

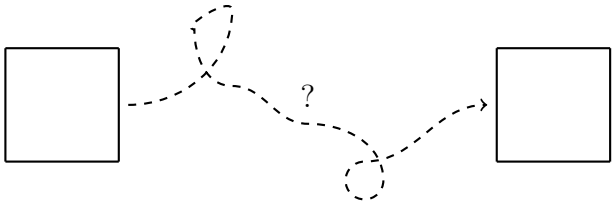
Simple can be harder than complex.
Steve Jobs

Welcome to abstract algebra, perhaps the pinnacle of your undergraduate mathematical career. To begin our transformative journey, we start by asking a simple question.

How can we move a square?

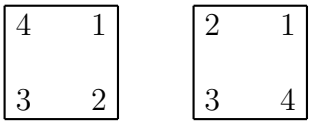
1.1 Introduction to Dihedral Groups

Imagine that you have a square and a trace of that square on the surface before you. You may pick up the square and move it in any way you wish, though ultimately you must put that square down in its trace. You may not rip, stretch, or alter the square. This is a rigid square, meaning that it holds its form.



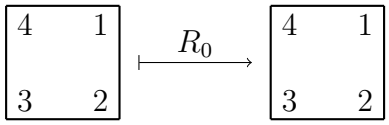
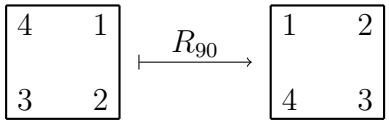
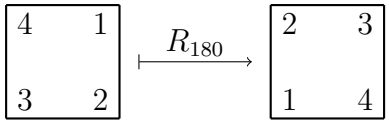
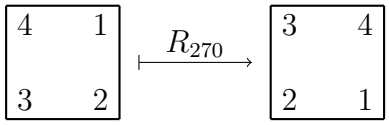
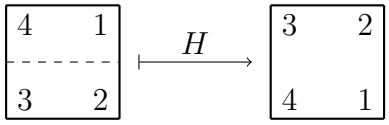
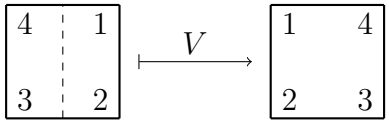
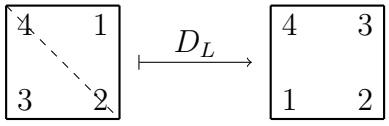
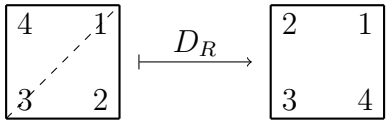
It may seem like there is an infinite number of ways to do this. Ever the diligent mathematician, you know you must simplify. Thus, what are the simplest, yet distinct, ways to pick up a square and put it down in its trace?

Spoiler alert! Imagine numbering the vertices of our square, and let's put the number one in the upper-right corner. There are two orientations of the square: either the numbers can increase as we proceed clockwise, or the numbers can increase as we proceed counterclockwise, as shown below.



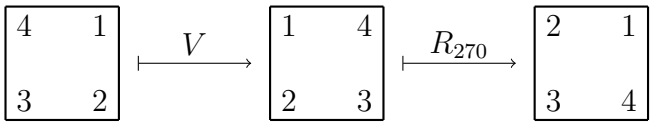
Each corner can be mapped to another corner. In total, each corner can go to one of four corners in one of two orientations. Thus, there must be eight mappings. What are they?

The mappings will involve the number one being in each of the four corners with each orientation. We list them below, along with a name for each different mapping.

Symbol	Description	Mapping
R_0	Rotation of 0° counterclockwise	
R_{90}	Rotation of 90°	
R_{180}	Rotation of 180°	
R_{270}	Rotation of 270°	
H	Reflection about the horizontal axis	
V	Reflection about the vertical axis	
D_L	Reflection about the left diagonal	
D_R	Reflection about the right diagonal	

These must be the eight mappings of the rigid square. What happens if we compose them? Will we get a ninth mapping or a repeat mapping?

Example 1.1.1. Suppose we took our square, $\square$, reflected it about the vertical axis, and then rotated it 270°. What would we get?



We see that, ultimately, we performed the same mapping as D_R, the reflection about the right diagonal. We could write this relation symbolically as

$$R_{270}(V(\square)) = D_R(\square).$$

$\diamond$

Think of each of map as a function acting on the square. Thus, when we perform a series of mappings, we are performing a series of applications of functions, which is function composition.

Notation. Whenever we compose movements of a rigid n-gon, we write them in order from right to left, as we do with function composition. For example, $h(g(f(x)))$ notates that our variable is x, and we will perform function f, function g, and function h, respectively, on x. Recall that we often leave off the x when we want to describe just the function composition. For example, we could write $h \circ g \circ f$, or simply hgf. Similarly, it is common to leave off the shape in function composition of a rigid n-gon. For example, we could write $R_{270} \circ V$, or simply $R_{270}V$.

Just as we composed V and R_{270} in Example 1.1.1, we can compose any two mappings and simplify. The result of all possible compositions of two mappings is charted in the example below. For each row header a and each column header b, the corresponding entry is ab. When working with function composition, this means b is performed first and a is performed second.

Example 1.1.2. Below are all of the possible compositions of two movements of a rigid square. Recall that in Example 1.1.1, we determined that $R_{270}V = D_R$. Similarly, notice that in the R_{270} row and V column, we have the mapping D_R.

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D_L	D_R
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D_L	D_R
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D_R	D_L	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D_R	D_L
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D_L	D_R	V	H
H	H	D_L	V	D_R	R_0	R_{180}	R_{90}	R_{270}
V	V	D_R	H	D_L	R_{180}	R_0	R_{270}	R_{90}
D_L	D_L	V	D_R	H	R_{270}	R_{90}	R_0	R_{180}
D_R	D_R	H	D_L	V	R_{90}	R_{270}	R_{180}	R_0

◇

There are many properties to observe in the table above! We will spend a considerable amount of time analyzing these properties. For now, study the table, observe some properties, and make some conjectures.

Definition 1.1.3. In abstract algebra, an operation table is called a Cayley table.

The table above is the Cayley table of the set of symmetries of a rigid square. As you might have guessed, we could have analyzed the movements of any rigid n-gon, not just a square. We generalize this idea in the definition below.

Definition 1.1.4. For any natural number $n \geq 3$, the dihedral group of order $2n$ is the set of all movements of a rigid n-gon, and is denoted D_n.

In this section, we have created D_4, the set of movements of a rigid square. Notice that we call this the dihedral group of order eight because $|D_4| = 8$.

EXERCISES

Exercise 1.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

- **a.** For $n \geq 3$ in $\mathbb{N}$, D_n has n reflections.
- **b.** For $n \geq 3$ in $\mathbb{N}$, D_n has n rotations.
- **c.** $D_3 \subseteq D_4$
- **d.** $D_n \subseteq D_{n+1}$, for $n \geq 3$ in $\mathbb{N}$
- **e.** $R_0 = R_{360}$
- **f.** A reflection composed with a rotation creates a reflection.

Exercise 1.1.2. Create a Cayley table for D_3.

Exercise 1.1.3. Create a Cayley table for D_5.

Exercise 1.1.4. Create a Cayley table for D_6.

Exercise 1.1.5. Observe the Cayley table of D_4. Make two conjectures about patterns you discover. These conjectures should also hold in D_3, D_5, and D_6.

Exercise 1.1.6. For each of the following equations, find all $x \in D_4$ such that the equation holds. If no such x exists, explain why not.

a. $x^2 = R_0$

b. $x^2 = R_{90}$

c. $x^2 = R_{180}$

d. $x^2 = D_L$

e. $x^3 = R_0$

f. $x^3 = R_{90}$

g. $x^3 = D_L$

Exercise 1.1.7. Let $n \geq 3$ be a natural number and consider D_n for each of the following n. For each element in $x \in D_n$, find the smallest $m \in \mathbb{N}$ such that $x^m = R_0$. Make a chart showcasing your findings.

a. $n = 3$

b. $n = 4$

c. $n = 5$

d. $n = 6$

Make a conjecture that relates m to $|D_n|$.

Chapter 2

Binary Operations

Excellence is achieved by mastery of the fundamentals.
Vince Lombardi

Abstract algebra exposes depth to everything you have taken for granted in mathematics. Everything. Before we can appreciate the magnitude and scope of abstract algebra, we must zoom in and start with its fundamentals. Like any other upper level undergraduate text, we start with something you think you understand and examine it so closely that it will soon become abstract.

2.1 Introduction to Binary Operations

Our first definition is of fundamental importance, though it may seem trivial.

Definition 2.1.1. A binary operation $*$ on a set S is a function from $S \times S$ to S, that is, $* : S \times S \to S$.

Many binary operations are already familiar.

Example 2.1.2. Consider the set $\mathbb{R}$. The operation of addition is a binary operation because any real number added to any real number produces a real number. Similarly, the operation of multiplication is a binary operation because any real number multiplied by any real number produces a real number. $\diamond$

Notice that a binary operation $*$ on a set S is closed on the set S, meaning that $*$ combines two elements in S and produces an element in S.

Notation. Let $(a, b) \in S \times S$. Instead of writing $*((a, b))$ to indicate the image of the element (a, b) under the function $*$, we often write $a * b$.

Example 2.1.3. Addition is a binary operation on the reals, that is, addition combines two real numbers and produces a real number. Thus, we could write $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. For example, when we add 2π to 5π, we could write this as $+((2\pi, 5\pi)) = 7\pi$, because $+$ is a function on $\mathbb{R} \times \mathbb{R}$. In practice, we write $2\pi + 5\pi$ instead of $+((2\pi, 5\pi))$. $\diamond$

Non-Example 2.1.4. Consider the set $\mathbb{N}$. Like in the reals, addition and multiplication are binary operations on $\mathbb{N}$. The operation of subtraction, however, is *not* a binary operation because for $a, b \in \mathbb{N}$, $a-b$ is not necessarily in $\mathbb{N}$. For example, $5 - 105 \notin \mathbb{N}$. $\diamond$

Example 2.1.5. In D_n, function composition is a binary operation. Revisit our Cayley tables for $3 \leq n \leq 6$ and notice that every composition is already an element in D_n. $\diamond$

A set may have several binary operations on it. For example, the operations of addition, subtraction, and multiplication are binary operations on $\mathbb{R}$.

Notation. To indicate which binary operation to use, we may write "$\mathbb{R}$ under addition," which is denoted symbolically as the pair $(\mathbb{R}, +)$. Similarly, we

write $(\mathbb{R}, -)$ and $(\mathbb{R}, \cdot)$ to indicate the set $\mathbb{R}$ with the binary operations of subtraction and multiplication, respectively.

There are many binary operations, and many symbols associated with these binary operations. Some common symbols you may have seen before are

$$+, \cdot, *, \times, \circ, \otimes, \oplus, \vee, \wedge, \cup, \text{ and } \cap .$$

Notation. The symbol $*$ is the generic symbol for a binary operation. Typically, it is used when the exact operation does not matter or is unknown.

Example 2.1.6. Suppose $*$ is a binary operation on $\mathbb{Z}$ such that $3*7 = -2$. In this case, we do not have enough information to determine the behavior of the operation $*$. ◇

It is more common to write $a * b$ instead of $*(a, b)$, and in practice, we abbreviate even more. Just as we use ab instead of $a \cdot b$ or $a \times b$ in high school algebra, we will often use ab instead of $a * b$ for a generic binary operation. Similarly, $a * a$ can be generically written as a^2. *Do not assume that the binary operation is multiplication!* Unless you already know the operation is multiplication, all you may assume is that ab is just the lazy way of writing $a * b$. (If you are a math major and not a bit lazy, you may be the first.)

The following lemma details some implications of the definition of a binary operation.

Lemma 2.1.7. *A binary operation $*$ on a set S satisfies the following conditions.*

1. *Substitution: For all $a_1, b_1, a_2, b_2 \in S$, if $a_1 = a_2$ and $b_1 = b_2$ then $a_1 * b_1 = a_2 * b_2$.*
2. *Right composition: For all $a_1, a_2, b \in S$, if $a_1 = a_2$ then $a_1 * b = a_2 * b$.*

3. *Left composition: For all* $a, b_1, b_2 \in S$*, if* $b_1 = b_2$ *then* $a * b_1 = a * b_2$.

Proof. We prove this lemma in parts. Let $*$ be a binary operation on a set S.

1. Assume $a_1, b_1, a_2, b_2 \in S$ such that $a_1 = a_1$ and $b_1 = b_2$. Therefore, $(a_1, b_1) = (a_2, b_2)$. By the definition of binary operation, $* : S \times S \to S$ is a function. By the definition of function, if $(a_1, b_1) = (a_2, b_2) \in S \times S$, then $*((a_1, b_1)) = *((a_2, b_2))$. Hence, $a_1 * b_1 = a_2 * b_2$.

2. Assume $a_1 = a_2$. By reflexivity of equality, we know that $b = b$ for all $b \in S$. By substitution, $a_1 * b = a_2 * b$, as desired.

3. This proof is similar to the proof of right composition.

□

Notice that the second and third parts Lemma 2.1.7 are about composition. The converse of composition is cancellation, which is noticeably *not* included in this lemma, because it does not always hold. We are not yet ready to study cancellation.

Non-Example 2.1.8. Consider the set $\mathbb{N}$ under the binary operation max. That is, if $a, b \in \mathbb{N}$, then let $a * b = \mathsf{max}(a, b)$. Then $100 * 2 = \mathsf{max}(100, 2) = 100$ and $100 * 70 = \mathsf{max}(100, 70) = 100$. Thus $100 * 2 = 100 * 70$ even though $2 \neq 70$. Ergo, just because $100 * 2 = 100 * 70$, we cannot cancel the 100. ◇

Notice that in Lemma 2.1.7, we distinguish between left and right composition. Order matters! Left and right composition are not necessarily the same. Let $*$ be a binary operation on set S, and consider $a, b \in S$. The order of a and b in the operation is very important. We do not assume that $a * b$ is the same as $b * a$. Although sometimes it may be true that $a * b = b * a$,

it is not part of the definition of binary operation, and nor should you ever assume it.

Definition 2.1.9. Assume that $*$ is a binary operation on the set S. We say that $*$ is commutative if

$$x * y = y * x$$

for all $x, y \in S$. If a binary operation is not commutative, we say it is noncommutative.

Example 2.1.10. Addition and multiplication on $\mathbb{C}$ are commutative. $\diamond$

If the operation on a set is established, we may simply say that the set is commutative, rather than saying the operation on the set is commutative.

It may seem that many binary operations are commutative, thus it is important to have some examples of noncommutative operations.

Example 2.1.11. Subtraction is a binary operation on $\mathbb{R}$. Consider $4.8, \pi \in \mathbb{R}$. Note that $4.8 * \pi \neq \pi * 4.8$ because $4.8 - \pi \neq \pi - 4.8$. Thus, subtraction is noncommutative. $\diamond$

Example 2.1.12. We have already seen that D_4 is not commutative. For example, notice that $R_{270}H = D_L$ and $HR_{270} = D_R$. $\diamond$

Example 2.1.13. Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices with real entries. Matrix multiplication is a binary operation on this set because

1. addition and multiplication of real numbers are binary operations, and
2. a 2×2 matrix multiplied by a 2×2 matrix produces a 2×2 matrix.

Matrix multiplication is noncommutative on $M_2(\mathbb{R})$. For example,

$$\begin{bmatrix} 1 & 7 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 4 & -1 \end{bmatrix} \in M_2(\mathbb{R}).$$

Notice that

$$\begin{bmatrix} 1 & 7 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 4 & -1 \end{bmatrix} = \begin{bmatrix} 9 & 11 \\ -1 & -3 \end{bmatrix},$$
$$\begin{bmatrix} 2 & 1 \\ 4 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 7 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 15 \\ 5 & 27 \end{bmatrix}$$

and

$$\begin{bmatrix} 9 & 11 \\ -1 & -3 \end{bmatrix} \neq \begin{bmatrix} 1 & 15 \\ 5 & 27 \end{bmatrix},$$

thus matrix multiplication is noncommutative on $M_2(\mathbb{R})$. ◇

The first part of Lemma 2.1.7, says that if $a_1 = a_2$ and $b_1 = b_2$, we can substitute a_2 for a_1 and b_2 for b_1 in the expression $a * b$ and obtain the expression $a_2 * b_2$ which is equal to $a_1 * b_1$. One might not think that such a natural statement is necessary. To see the need for it, see Exercise 2.1.9.

Now that we have some basic properties of a binary operation, we give more examples and non-examples. Throughout the examples, consider how the properties detailed in Lemma 2.1.7 hold.

Example 2.1.14. Let $\mathbb{R}[x]$ be the set of polynomials in x with real coefficients, that is,

$$\mathbb{R}[x] = \{a_o + a_1x + a_2x^2 + \cdots + a_nx^n \,|\, a_i \in \mathbb{R},\, n \in \mathbb{N}\}.$$

Then addition and multiplication are binary operations on $\mathbb{R}[x]$. That is, if $f(x), g(x) \in \mathbb{R}[x]$, then $f(x) + g(x), f(x) \cdot g(x) \in \mathbb{R}[x]$. Notice that the

coefficients of the polynomials $f(x) + g(x)$ and $f(x) \cdot g(x)$ are real numbers because addition and multiplication are binary operations on the reals. $\diamond$

Example 2.1.15. Consider $\mathcal{P}(\mathbb{Z})$, the powerset of the integers. The operations of $\cup$ and $\cap$, set union and set intersection, are binary operations on $\mathcal{P}(\mathbb{Z})$. $\diamond$

Non-Example 2.1.16. The operation of division is not a binary operation on the sets $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$. This is because for any element $a \in \mathbb{C}$, $a * 0$ is undefined, hence $a * 0 \notin \mathbb{C}$. $\diamond$

As we will see, the number zero can be pesky when working under the operations of multiplication and division. Thus, we have the following notation.

Notation. For a set of numbers S that includes the element 0, let S^* be the set $S - \{0\}$. For example, $\mathbb{R}^* = \mathbb{R} - \{0\}$.

Example 2.1.17. Consider the operation of division. On $\mathbb{Q}^*$ and $\mathbb{R}^*$, division is a binary operation. Note that division is still not a binary operation on $\mathbb{N}^*$ and $\mathbb{Z}^*$ since, for example, $\frac{1}{2} \notin \mathbb{N}$ and $\frac{1}{2} \notin \mathbb{Z}$. $\diamond$

Abstract algebra is rich with examples. The following definitions will provide examples throughout the text.

Definition 2.1.18. For each integer $n \geq 2$, define the set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\},$$

which is called the set of integers modulo n. For $a, b \in \mathbb{Z}_n$, the operation

$$a + b \bmod n$$

is called addition modulo n, and the operation

$$a \cdot b \bmod n$$

is called multiplication modulo n. For short, these operations are also called modular addition and modular multiplication.

Example 2.1.19. Let $n = 10$. Then $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$. For example, because $8 + 7 \equiv 5 \bmod 10$ in modular arithmetic, in $\mathbb{Z}_{10}$ we write $8 + 7 = 5$. Similarly, because $8 \cdot 7 \equiv 6 \bmod 10$, in $\mathbb{Z}_{10}$ we have $8 \cdot 7 = 6$. $\diamond$

Example 2.1.20. For each $n \geq 2$, addition modulo n and multiplication modulo n are binary operations on the set $\mathbb{Z}_n$. $\diamond$

In Examples 2.1.19 and 2.1.20, it would be more precise to use the notations $a +_n b$ and $a \cdot_n b$ for addition and multiplication in $\mathbb{Z}_n$, but in the interest of keeping the notation simple we omit the subscript n. Of course, this means that in any given situation, we must be very clear about the value of n. Note also that this is really an infinite class of examples, as $n \geq 2$.

Example 2.1.21. Let K denote any one of the following: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$. Let $M_2(K)$ be the set of all 2×2 matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where a, b, c, d are any elements of K. Matrix addition and multiplication

are defined by the following rules:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}$$
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}$$

for all $a, b, c, d, a', b', c', d' \in K$. Note that it is implied to use the forms of addition and multiplication associated with each set K. That is, use "regular" addition and multiplication if $K = \mathbb{Z}$ and modular addition and multiplication if $K = \mathbb{Z}_n$. ◇

Example 2.1.22. Addition of vectors in $\mathbb{R}^n$, $n \in \mathbb{N}$, is a binary operation. More precisely, for

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{R} \text{ for all } 1 \leq i \leq n\}.$$

addition is defined by the rule

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

where $x_i + y_i$ denotes the addition of the real numbers x_i and y_i. ◇

Example 2.1.23. The cross product $\mathbf{u} \times \mathbf{v}$ of vectors $\mathbf{u}$ and $\mathbf{v}$ in $\mathbb{R}^3$ is a binary operation. Recall that given 2×2 matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

the determinant is

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

For vectors $\mathbf{u} = (u_1, u_2, u_3)$ and $\mathbf{v} = (v_1, v_2, v_3)$, $\mathbf{u} \times \mathbf{v}$ is defined by the

formula

$$\mathbf{u} \times \mathbf{v} = \left(\begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}, - \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}, \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} \right).$$

Notice that $\mathbf{u} \times \mathbf{v} \in \mathbb{R}^3$ because multiplication and subtraction are binary operations on the reals. $\diamond$

The following property will become important to us, though not all binary operations have it.

Definition 2.1.24. Assume that $*$ is a binary operation on the set S. We say that $*$ is associative if

$$x * (y * z) = (x * y) * z \quad \text{for all } x, y, z \in S.$$

If a binary operation is not associative, we say it is nonassociative.

If the operation is known, we may simply say that the set is associative, rather than saying the operation on the set is associative.

Example 2.1.25. On the set $\mathbb{R}$, addition and multiplication are associative. For $x, y, z \in \mathbb{R}$, we know that

$$x + (y + z) = (x + y) + z$$

and

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Subtraction is not associative. For example,

$$100 - (99 - 98) \neq (100 - 99) - 98.$$

◇

Non-Example 2.1.26. On $\mathbb{R}^*$, division is not associative. For example,

$$24 \div (6 \div 2) \neq (24 \div 6) \div 2.$$

◇

Notice that the definition of associativity only applies to three elements. In practice, we may need to apply associativity to more than three elements. To do so, we need the theorem below.

Theorem 2.1.27 (The Generalized Associative Law)**.** *Let $*$ be an associative binary operation on a set S. If $a_1, a_2, \ldots, a_n$ is a sequence of $n \geq 3$ elements of S, then the product*

$$a_1 * a_2 * \cdots * a_n$$

is unambiguous; that is, the same element will be obtained regardless of how parentheses are inserted in the product.

As this theorem's statement contains an ellipsis, the proof of this theorem requires induction. The base case, when $n = 3$, is the associative law itself. Some of the cases when $n = 4$ are addressed in Exercise 2.1.12. The remainder of this proof is omitted.

EXERCISES

Exercise 2.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

- **a.** Division is a binary operation on $\mathbb{R}$.
- **b.** Division is a binary operation on $M_2(\mathbb{R})$.

c. The symbol $*$ denotes multiplication.

d. Matrix multiplication is noncommutative.

e. A binary operation is associative.

Exercise 2.1.2. Consider the set $\mathbb{Z}_n$. For each n given below, find -3, -28, $4-16$, and $15-33$ in $\mathbb{Z}_n$.

a. $n = 2$

b. $n = 10$

c. $n = 7$

Exercise 2.1.3. For each of the following, determine if the set is closed under addition modulo n. If it is closed, construct a Cayley table. If it is not closed, give a counterexample.

a. $\{0, 1, 2, 3\}$ when $n = 4$

b. $\{1, 2, 3\}$ when $n = 4$

c. $\{0, 3, 6, 9\}$ when $n = 10$

d. $\{0, 3, 6, 9\}$ when $n = 12$

Exercise 2.1.4. For each of the following, determine if the set is closed under multiplication modulo n. If it is closed, construct a Cayley table. If it is not closed, give a counterexample.

a. $\{1, 2, 3\}$ when $n = 4$

b. $\{1, 2, 3\}$ when $n = 5$

c. $\{1, 3, 5, 7\}$ when $n = 8$

d. $\{0, 2, 4, 6, 8\}$ when $n = 10$

Exercise 2.1.5. Consider the matrices

$$A = \begin{bmatrix} 3 & 7 \\ 8 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 9 & 5 \\ 6 & 2 \end{bmatrix}.$$

a. Find $A + B$, AB, and BA if $A, B \in M_2(\mathbb{Z})$.

b. Find $A + B$, AB, and BA if $A, B \in M_2(\mathbb{Z}_{10})$.

Exercise 2.1.6. Is D_3 commutative? Is D_5 commutative? Is D_6 commutative? Justify your claims.

Exercise 2.1.7. A set S with a binary operation $*$ is not commutative if there exists a pair of elements $a, b \in S$ such that $a * b \neq b * a$. That does not mean $a * b \neq b * a$ for all $a, b, \in S$. That is, there may be some pairs $a, b \in S$ such that $a * b = b * a$. Find all such pairs in D_4. What patterns do you notice?

Exercise 2.1.8. Let $D_2(\mathbb{R})$ be the set of 2×2 diagonal matrices with real entries. Answer each of the following and prove your claims.

a. Is matrix addition commutative?

b. Is matrix multiplication commutative?

Exercise 2.1.9. Here we give an example of a rule that appears to define a binary operation, but does not, because substitution does not hold. Let a, b, c, d be integers with $b \neq 0$ and $d \neq 0$. Then

$$\frac{a}{b} \in \mathbb{Q} \quad \text{and} \quad \frac{c}{d} \in \mathbb{Q}.$$

Define $*$ on $\mathbb{Q}$ by

$$\frac{a}{b} * \frac{c}{d} = \frac{a + c}{b^2 + d^2}.$$

a. Prove that $*$ is a closed on $\mathbb{Q}$.

b. Show by specific example that this rule does not permit substitution.

Exercise 2.1.10. Find a set S with a binary operation $*$ that is not associative. Prove it by giving three specific elements $a, b, c \in S$ such that $a * (b * c) \neq (a * b) * c$.

Exercise 2.1.11. Consider matrix multiplication over $M_2(\mathbb{C})$. Prove that this binary operation is associative.

Exercise 2.1.12. Let $*$ be an associative binary operation on the set S and let $a, b, c, d \in S$. Prove the following statements.

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

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

Exercise 2.1.13. Consider the set $\mathbb{R}[x]$ and the operation of function composition.

a. Is function composition a binary operation? If so, why? If not, give a counterexample.

b. Is function composition associative? If so, why? If not, give a counterexample.

c. Is function composition commutative? If so, why? If not, give a counterexample.

2.2 Some Important Elements

This section consists of definitions that are fancy words for elements you have probably already recognized as being interesting in some way. We mathematicians have a particular proclivity for sophisticated vocabulary... so you should learn them wicked well.

Definition 2.2.1. We say that an element e in S is an identity with respect to $*$ if

$$x * e = x \text{ and } e * x = x \quad \text{for all } x \text{ in } S.$$

Example 2.2.2. In D_4, R_0 is an identity element because for all $x \in D_4$, $R_0 x = x R_0 = x$. ◇

Example 2.2.3. Consider the set $\mathbb{Z}$. Under addition, $0 \in \mathbb{Z}$ is the identity because for ever $x \in \mathbb{Z}$, $x + 0 = 0 + x = x$. Similarly, consider the set $\mathbb{Z}^*$. Under multiplication, $1 \in \mathbb{Z}^*$ is the identity because for every $x \in \mathbb{Z}^*$, $x \cdot 1 = 1 \cdot x = x$. Notice that for multiplication, we must consider $\mathbb{Z}^*$ and not $\mathbb{Z}$. $\diamond$

The previous example may seem obvious, but it demonstrates an important point. An identity depends on both the set and the binary operation. Further, not all binary operations have an identity, though we have to be slightly more creative to find an example.

Non-Example 2.2.4. Consider the set $\mathbb{N}$ under the binary operation min. That is, if $a, b \in \mathbb{N}$, then let $a * b = \mathsf{min}(a, b)$. Then there is no identity. $\diamond$

An identity is necessary in the next definition.

Definition 2.2.5. Assume that $*$ is a binary operation on the set S. Let $e \in S$ be an identity with respect to $*$. Given $x \in S$ we say that an element $y \in S$ is an inverse of x if both

$$x * y = e \text{ and } y * x = e.$$

Example 2.2.6. Consider the set $\mathbb{R}$ under addition. First, note that 0 is the identity in this situation, thus for any $x \in \mathbb{R}$, we are looking for some $y \in \mathbb{R}$ such that $x + y = y + x = 0$. For $7 \in \mathbb{R}$, we see that $-7 \in \mathbb{R}$ is an inverse of 7 because $7 + (-7) = (-7) + 7 = 0$.

Consider the set $\mathbb{R}^*$ under multiplication. First, note that 1 is the identity in this situation, thus for any $x \in \mathbb{R}^*$, we are looking for some $y \in \mathbb{R}^*$ such that $x \cdot y = y \cdot x = 1$. For $7 \in \mathbb{R}^*$, we see that $\frac{1}{7} \in \mathbb{R}^*$ is an inverse of 7 because

$7 \cdot (\frac{1}{7}) = (\frac{1}{7}) \cdot 7 = 1.$ ◇

Notice that in the definition of inverse assumes an identity exists. Whenever we calculate an inverse, we must first determine an identity!

Non-Example 2.2.7. Revisit Example 2.2.4 and let $*$ be the operation min. Consider the element $8 \in \mathbb{N}$. We cannot find an inverse of 8 because, in order to do so, we would need to find some $y \in \mathbb{N}$ such that $8 * y = \min(8, y)$ equals an identity, which does not exist. Therefore, $8 \in \mathbb{N}$ does not have an inverse under the operation min. ◇

Just because a set has an identity does not mean that every element must have an inverse. Consider the following example.

Non-Example 2.2.8. Matrix multiplication is a binary operation the set $M_2(\mathbb{R})$, and an identity element is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

because for any

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}),$$

we have that

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

The matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

does not have an inverse. ◇

In the integers modulo n, finding an inverse element can be tricky. Consider the example below.

Example 2.2.9. Consider $\mathbb{Z}_{12}$ under addition. Recall that

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

First, an identity is 0 because for all $x \in \mathbb{Z}_{12}$, it is true that $x + 0 = 0 + x \equiv x \bmod 12$. To find an inverse of $2 \in \mathbb{Z}_{12}$, we need to find some $y \in \mathbb{Z}_{12}$ such that $2 + y = y + 2 = 0$. Recall that in modular 12 arithmetic

$$\cdots \equiv -24 \equiv -12 \equiv 0 \equiv 12 \equiv 24 \equiv \cdots$$

thus, we are looking for some $y \in \mathbb{Z}_{12}$ such that $2 + y = y + 2$ is equal to -24, or -12, or 0, or 12, or 24, etc.

In the set $\mathbb{Z}$ with no modulus, an inverse of 2 is -2, however, in $-2 \notin \mathbb{Z}_{12}$, thus we must keep searching. For $10 \in \mathbb{Z}_{12}$, we see that $2+10 = 10+2 = 12$. Thus, $10 \in \mathbb{Z}_{12}$ is an inverse of 2. Notice that $-2 \equiv 10$ in modular 12 arithmetic.

Similarly, an inverse of $7 \in \mathbb{Z}_{12}$ is $5 \in \mathbb{Z}_{12}$ because $7 + 5 = 5 + 7 = 12$. ◇

Non-Example 2.2.10. Consider the set $\mathbb{Z}_6$ under multiplication. In this situation, 1 is an identity element. Notice that $0, 2, 4 \in \mathbb{Z}_6$ do not have inverses. ◇

Recall from Section 2.1 that we sometimes get lazy and write our binary operation as multiplication. In Example 2.2.9, using the multiplicative notation, we could write $2^{-1} = 10$ and $7^{-1} = 5$. This may look strange and seem unnecessary, but it can also be very helpful. This leads us to the following notation.

Notation. Given an element with exactly one inverse, the symbol $^{-1}$ denotes

the inverse, and can be useful in symbolic writing. Thus, think of $^{-1}$ as the inverse symbol, and not necessarily as the multiplicative inverse symbol.

In Example 2.2.9, we understand that the binary operation in $\mathbb{Z}_{12}$ is addition. Thus, we know that the symbol $^{-1}$ means inverse under addition. Therefore, $2^{-1} = 10$ in $\mathbb{Z}_{12}$. You may be used to thinking that $2^{-1} = \frac{1}{2}$, but in $\mathbb{Z}_{12}$, this does not make sense because $\frac{1}{2} \notin \mathbb{Z}_{12}$.

Further, notice in Example 2.2.9, that $0 + 0 = 0$. Thus, 0 is its own inverse. This means that we can write $0^{-1} = 0$. If you do indeed write this, it must be clear that the operation is addition!

Definition 2.2.11. We say that an element $a \in S$ is idempotent with respect to $*$ if

$$a * a = a.$$

Example 2.2.12. Consider the set $\mathbb{Z}_{10}^*$ under multiplication modulo 10. Then $1, 5, 6 \in \mathbb{Z}_{10}^*$ are idempotent because

$$\begin{aligned} 1 \cdot 1 &\equiv 1 \bmod 10 \\ 5 \cdot 5 = 25 &\equiv 5 \bmod 10 \\ 6 \cdot 6 = 36 &\equiv 6 \bmod 10 \end{aligned}$$

Notice that $7 \in \mathbb{Z}_{10}^*$ is not idempotent because $7 \cdot 7 \not\equiv 7 \bmod 10$. ◇

The following definition applies strictly when the operation is multiplication, including modular multiplication.

Definition 2.2.13. The S be a set under the binary operation of multiplication. Then $x \in S$ is a unit if x has a multiplicative inverse.

Note that in order to determine if an element is a unit, we first need to determine a multiplicative identity.

Example 2.2.14. Consider $\mathbb{Z}_{10}^*$. Then 1 is a multiplicative identity. For $3 \in \mathbb{Z}_{10}^*$, $3 \cdot 7 = 1$, thus both 3 and 7 are units. The element $4 \in \mathbb{Z}_{10}^*$ is not a unit because there does not exist an $x \in \mathbb{Z}_{10}^*$ such that $4x = 1$. ◇

Non-Example 2.2.15. In $(\mathbb{R}, +)$, 0 is an identity and 2 has inverse -2. Notice that 2 is not a unit because, though it has an inverse, the operation is addition. ◇

When a set has multiple binary operations on it, it is important to distinguish between different types of inverses.

Example 2.2.16. The element $6 \in \mathbb{R}$ has additive inverse -6 and multiplicative inverse $\frac{1}{6}$. ◇

EXERCISES

Exercise 2.2.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

- **a.** If a set has an identity under a binary operation, then every element in the set has an inverse.
- **b.** $3^{-1} = \frac{1}{3}$
- **c.** An identity is an idempotent.
- **d.** An identity is a unit.

e. An inverse of an identity is an identity.

f. An inverse of a unit is a unit.

Exercise 2.2.2. Refer back to Example 2.2.3.

a. We claim $0 \in \mathbb{Z}$ is an identity under addition. Is $0 \in \mathbb{Z}$ an identity under multiplication? Why or why not?

b. We claim $1 \in \mathbb{Z}^*$ is an identity under multiplication. Is $1 \in \mathbb{Z}$ an identity under multiplication? Why or why not?

Exercise 2.2.3. Refer back to Example 2.2.4. For each of the following, determine if there is an identity. If so, what is it? If not, why not? Also, if there is an identity, does the element 8 have an inverse? Why or why not?

a. Consider the set $\mathbb{N}$ under the binary operation max.

b. Consider the set $\mathbb{Z}$ under the binary operation min.

c. Consider the set $\mathbb{Z}$ under the binary operation max.

Exercise 2.2.4. Consider the set $\mathbb{Z}_n$. For each n given below, find 2^{-1} and 7^{-1}. In each case, how many inverses does 2 have? How many inverses does 7 have?

a. $n = 9$

b. $n = 11$

c. $n = 14$

d. $n = 20$

Exercise 2.2.5. Consider the set $\mathbb{Z}_n^*$ under multiplication modulo n. For each n given below, make a Cayley table for $\mathbb{Z}_N^*$. What is an identity? For each element, what are its inverse(s), if any exist?

a. $n = 4$

b. $n = 7$

c. $n = 10$

Exercise 2.2.6. Consider the set $\mathbb{Z}_n^*$ under multiplication modulo n. For each n given below, make a table that lists every element and its inverse(s), if any exist.

a. $n = 5$

b. $n = 8$

c. $n = 15$

Exercise 2.2.7. Make a Cayley table for the set $\{3, 6, 9, 12\}$ under multiplication modulo 15. Is there an identity element? If so, find it, and determine the inverses of each element, if any exist.

Exercise 2.2.8. For each of the following, determine which examples have identities. If there is an identity, determine the elements which *do not* have inverses.

a. $\{1, 2, 3\}$ under multiplication modulo 4

b. $\{1, 3, 5, 7\}$ under multiplication modulo 8

c. $\{0, 2, 4, 6\}$ under multiplication modulo 8

d. $\{1, 3, 5, 7, 9, 11, 13\}$ under multiplication modulo 15

e. $\{1, 7, 9, 11, 13\}$ under multiplication modulo 15

Exercise 2.2.9. Determine which of the examples $(\mathbb{R}, \cdot)$, $(\mathbb{R}, +)$, and $(M_2(\mathbb{R}), \cdot)$ have identities. If there is an identity, determine the elements which *do not* have inverses.

Exercise 2.2.10. Let X be a set. Determine which of the examples $(\mathcal{P}(X), \cup)$ and $(\mathcal{P}(X), \cap)$ have identities. If there is an identity, determine the elements which *do not* have inverses. If there is no identity, explain why not.

Exercise 2.2.11. Find all idempotents in $\mathbb{Z}_{12}^*$. Find all idempotents in $\mathbb{Z}_{20}^*$.

Exercise 2.2.12. Let $e \in S$ be an identity under the operation $*$. Prove that e is an idempotent.

Exercise 2.2.13. For each of the following $n \in \mathbb{N}$, find all of the units in $\mathbb{Z}_n^*$. Then, conjecture which elements in $\mathbb{Z}_n*$ will be units and which will not be units.

a. $n = 6$

b. $n = 7$

c. $n = 8$

d. $n = 9$

e. $n = 12$

Exercise 2.2.14. Let $e \in S$ be an identity under multiplication. Prove that e is a unit.

Chapter 3

Groups

We cannot solve our problems with the same thinking we used when we created them.
Albert Einstein

At this point, you may be wondering how the dihedral groups relate to binary operations and why any of this is considered "abstract." The dihedral groups are examples of a type of algebraic structure, a structure called a *group*. In this chapter, we generalize the dihedral groups to include many of the examples we saw in Chapter 2.

3.1 Introduction to Groups

Below we define a group, which is a major building block of abstract algebra.

Definition 3.1.1. A group G is a set with a binary operation such that the following properties are satisfied.

1. Associativity: For all $x, y, z \in G$, $x * (y * z) = (x * y) * z$.
2. Identity: There exists $e \in G$ such that $e * x = x * e = x$ for all x in G.
3. Inverses: For every element $x \in G$, there exists $y \in G$ such that $x * y = y * x = e$.

We have already seen many examples of groups in the previous chapters. Some examples are reiterated below.

Example 3.1.2. The dihedral groups D_n are indeed groups. We will focus on D_4. We know that

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D_L, D_R\}$$

and function composition is a binary operation on this set. Now, we must verify the three properties.

1. Associativity: Though it is cumbersome, we could check every possible triple $x, y, z \in D_4$ to see that $x * (y * z) = (x * y) * z$.
2. Identity: The element $R_0 \in D_4$ is an identity element.
3. Inverses: Every element does indeed have an inverse. We see that R_0, R_{180}, H, V, D_L, and D_R are self-inverses. The elements R_{90} and R_{270} are inverses of each other.

To verify the claims about associativity and inverses, refer back to the Cayley table of D_4 in Chapter 1. ◇

Before we more rigorously analyze how to prove a set with a binary operation is a group, we give more examples of groups, and leave many of these proofs

to the reader.

Example 3.1.3. The set $\mathbb{Z}$ under addition is a group with identity $0 \in \mathbb{Z}$. The inverse of $x \in \mathbb{Z}$ is $-x \in \mathbb{Z}$ because $x + (-x) = 0$. $\diamond$

Example 3.1.4. The set $\mathbb{R}^*$ under multiplication is a group with identity $1 \in \mathbb{R}^*$. The inverse of $x \in \mathbb{R}^*$ is $\frac{1}{x} \in \mathbb{R}^*$ because $x \cdot \frac{1}{x} = 1$. Notice that it is essential that $x \in \mathbb{R}^*$ because $\frac{1}{x}$ does not exist when $x = 0$. $\diamond$

Non-Example 3.1.5. The set $\mathbb{Z}$ under multiplication is not a group. Notice that there is no identity in $\mathbb{Z}$. Initially, we may guess that $1 \in \mathbb{Z}$ could be an identity, though it is not, because for $0 \in \mathbb{Z}$, $0 \cdot 1 = 1 \cdot 0 \neq 1$.

The set $\mathbb{Z}^*$ under multiplication is not a group. Notice that $1 \in \mathbb{Z}^*$ is an identity, but it is not true that every element has an inverse. The elements $1, -1 \in \mathbb{Z}^*$ have inverses, but no other elements have inverses. For example, $37 \in \mathbb{Z}^*$ does not have an inverse. $\diamond$

Non-Example 3.1.6. The set $\mathbb{N}$ is not a group under addition. Notice that it does not have an identity, because $0 \notin \mathbb{N}$. Further, it does not have inverses, because for $x \in \mathbb{N}$, $-x \notin \mathbb{N}$. $\diamond$

Note that a group has both a set and a binary operation on the set. For this reason, we have the alternate notation given below.

Notation. A group G may be expressed as the pair $(G, *)$, where G is the set and $*$ is the binary operation on the set.

Often, the binary operation on the set is inherent, thus the notation of simply G is sufficient. If the operation is unknown, unusual, or must be emphasized, the notation $(G, *)$ might be better.

Example 3.1.7. The set $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ is a group under multiplication modulo 7. Its identity is 1. Notice that 2 and 4 are inverses because

$2 \cdot 4 \equiv 1 \bmod 7$. Similarly, 3 and 5 are inverses because $3 \cdot 5 \equiv 1 \bmod 7$. The elements 1 and 6 are self-inverses because $1 \cdot 1 \equiv 1 \bmod 7$ and $6 \cdot 6 \equiv 1 \bmod 7$. ◇

Non-Example 3.1.8. The set $\mathbb{Z}_8^* = \{1, 2, 3, 4, 5, 6, 7\}$ is not a group under multiplication modulo 8. This set has identity 1, but not all elements have inverses. For example, there is no element $x \in \mathbb{Z}_8^*$ such that $2x = 1$ because $2 \cdot 1 = 2 \cdot 5 = 2$, $2 \cdot 2 = 2 \cdot 6 = 4$, and $2 \cdot 3 = 2 \cdot 7 = 6$. ◇

Example 3.1.7 and Non-Example 3.1.8 show us that not every $\mathbb{Z}_n^*$ is a group under multiplication modulo n. To remedy this, we begin with the definitions below.

Definition 3.1.9. Integers a and b are relatively prime if their greatest common divisor is 1, that is, $\gcd(a, b) = 1$.

Example 3.1.10. The integers 4 and 9 are relatively prime because $\gcd(4, 9) = 1$. Notice that 4 and 9 are relatively prime in relation to each other, even though neither is a prime itself. ◇

Non-Example 3.1.11. The integers 4 and 14 are not relatively prime because $\gcd(4, 14) = 2$. ◇

Notice that the term relatively prime describes how two integers relate to each other, as opposed to the term prime, which describes one integer by itself. The relatively prime relationship is useful in the following definition.

Definition 3.1.12. Let $n \geq 2$ be a natural number. Define $U(n)$ to be the set of all natural numbers that are less than n and relatively prime to n, that

is,

$$U(n) = \{x \in \mathbb{N} \,|\, 1 \leq x < n,\, \gcd(x, n) = 1\}$$

under the operation of multiplication modulo n. This group is called the group of units modulo n.

Example 3.1.13. Consider $U(8) = \{x \in \mathbb{N} \,|\, 1 \leq x < 8,\, \gcd(x, 8) = 1\}$. We see that

$$U(8) = \{1, 3, 5, 7\}$$

and indeed this is a group, as justified below.

0. Multiplication modulo 8 is a binary operation on this set because for the product of any two numbers in $U(8)$ will also be in $U(8)$.

1. The binary operation is associative because all multiplication modulo n is associative.

2. The element $1 \in U(8)$ is a multiplicative identity.

3. Every element has an inverse, in fact, every element is its own inverse.

Thus, we see that $U(8)$ is indeed a group. ◇

Example 3.1.14. Ⓢ Consider $U(22) = \{x \in \mathbb{N} | 1 \leq x < 22, \gcd(x, 22) = 1\}$.

a) *Construct a Cayley table for* $U(22)$. Below is a Cayley table for $U(22)$.

$U(22)$	1	3	5	7	9	13	15	17	19	21
1	1	3	5	7	9	13	15	17	19	21
3	3	9	15	21	5	17	1	7	13	19
5	5	15	3	13	1	21	9	19	7	17
7	7	21	13	5	19	3	17	9	1	15
9	9	5	1	19	15	7	3	21	17	13
13	13	17	21	3	7	15	19	1	5	9
15	15	1	9	17	3	19	5	13	21	7
17	17	7	19	9	21	1	13	3	15	5
19	19	13	7	1	17	5	19	15	9	3
21	21	19	17	15	13	9	7	5	3	1

b) *Find the inverse of each element of* $U(22)$. Using the Cayley table, we find inverses by seeing where two numbers are multiplied using multiplication mod 22 to make 1, which is the identity of $U(22)$. Below is a list of the inverse of each element of $U(22)$.

$$
\begin{aligned}
1^{-1} &= 1,\\
3^{-1} &= 15,\\
5^{-1} &= 9,\\
7^{-1} &= 19,\\
9^{-1} &= 5,\\
13^{-1} &= 17,\\
15^{-1} &= 3,\\
17^{-1} &= 13,\\
19^{-1} &= 7,\\
21^{-1} &= 21.
\end{aligned}
$$

c) *Prove $U(22)$ is a group.* We see that multiplication modulo 22 is a binary operation on this set. Notice from the Cayley table for $U(22)$, we see that for every $x, y \in U(22), xy \in U(22)$. Therefore, $U(22)$ has closure. We know that any multiplication modulo n is associative. Therefore, $U(22)$ multiplication modulo 22 is associative. Notice $1 \in U(22)$ and is the multiplicative identity. We see that inverses exist in $U(n)$. Hence, $U(22)$ is a group.

$\diamond$

Note that even though the name of $U(n)$ includes the word group, we still must prove $U(n)$ is a group. We need a few more tools for this proof, thus it comes later in the chapter. Below is our first example of how to prove a set with an operation is a group, and it is an important one. We will reference this result many times.

Theorem 3.1.15. *The set $\mathbb{C}$ is a group under addition.*

Proof. We already know addition is a binary operation on $\mathbb{C}$. Thus, to prove that $\mathbb{C}$ is a group under addition, we must prove that the binary operation is associative, the set has an identity, and each element has an inverse.

1. Let $x = a_x + b_x i, y = a_y + b_y i, z = a_z + b_z i \in \mathbb{C}$. Then, because addition is a binary operation on the reals,

$$\begin{aligned} x + (y + z) &= a_x + b_x i + (a_y + b_y i + a_z + b_z i) \\ &= a_x + b_x i + [(a_y + a_z) + (b_y + b_z)i] \\ &= (a_x + a_y + a_z) + (b_x + b_y + b_z)i \\ &= (a_x + a_y) + (b_x + b_y)i + a_z + b_z i \\ &= (x + y) + z. \end{aligned}$$

Thus, addition is associative over the complex numbers.

2. We see that $0 \in \mathbb{C}$ because $0 = 0 + 0i$. For any $a + bi \in \mathbb{C}$,

$$(a + bi) + 0 = 0 + (a + bi) = a + bi.$$

Similarly, $0 + (a + bi) = a + bi$. Thus, we have an identity element.

3. Recall that $0 \in \mathbb{C}$ is an identity and consider $a + bi \in \mathbb{C}$. By the definition of $\mathbb{C}$, $a, b \in \mathbb{R}$. Further $-a, -b \in \mathbb{R}$, thus $(-a) + (-b)i \in \mathbb{C}$. Then

$$(a + bi) + [(-a) + (-b)i] = [a + (-a)] + [b + (-b)]i = 0 + 0i = 0.$$

Similarly, $[(-a) + (-b)i] + (a + bi) = 0$. Thus, each complex number has an additive inverse.

Thus, $\mathbb{C}$ under addition is a group. □

Compare the different proof styles of Example 3.1.2 and Theorem 3.1.15. In Example 3.1.2, we prove D_4 is a group by verifying the properties on the individual elements. In Theorem 3.1.15, we prove $\mathbb{C}$ is a group not by studying individual elements, but instead by verifying the properties using the generic form of complex numbers. When asked to prove a small, finite set is a group, consider verifying the properties on the individual elements. When asked to prove either an infinite set or set given in set-builder notation, consider using the generic form of the elements in the set.

Theorem 3.1.15 will be very useful in the future because $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R} \subseteq \mathbb{C}$. For similar reasons, the next results are also useful, and the proofs are left to the reader.

Theorem 3.1.16. *The set $\mathbb{C}^*$ under multiplication is a group.*

Theorem 3.1.17. *The set $\mathbb{Z}_n$ is a group under addition modulo n.*

The following notation gives us infinitely more examples of groups.

Notation. Let $n \in \mathbb{N}$. Then the set $n\mathbb{Z}$ is defined to be

$$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$$

which is the set of multiples of n.

Theorem 3.1.18. *Given $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a group under addition.*

The proof of this is left as a homework exercise.

EXERCISES

Exercise 3.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

- **a.** A group has closure.
- **b.** The empty set is a group.
- **c.** Given an element g in group G, g^{-1} is also in G.
- **d.** Group G has an idemptotent.
- **e.** For $n \geq 2$, $\mathbb{Z}_n^*$ is a group.
- **f.** For $n \geq 2$, $1 \in U(n)$.
- **g.** For $n \geq 2$, $2 \in U(n)$.
- **h.** For $n \geq 2$, the elements in $U(n)$ are units.

Exercise 3.1.2. For each of the following, give a reason why the set and operation do not form a group.

- **a.** $\mathbb{Z}$ under subtraction

b. The odd integers under addition

c. The odd integers under multiplication

d. The even integers under multiplication

e. $\mathbb{Q}$ under multiplication

Exercise 3.1.3. Construct a Cayley table for $U(10)$. Find the inverse(s) of each element.

Exercise 3.1.4. Construct a Cayley table for $U(12)$. Find the inverse(s) of each element.

Exercise 3.1.5. Prove that $\{1, -1, i, -i\}$ is a group under multiplication.

Exercise 3.1.6. Prove that $3\mathbb{Z} = \{3x \mid x \in \mathbb{Z}\}$ is a group under addition.

Exercise 3.1.7. For each of the following n, determine if $\mathbb{Z}_n^*$ is a group. If it is a group, state the identity and each element's inverse(s). If it is not a group, explain why not.

a. $n = 2$

b. $n = 3$

c. $n = 4$

d. $n = 5$

e. $n = 6$

Make a conjecture about what restrictions need to be put on $n \in \mathbb{N}$ to make $\mathbb{Z}_n^*$ a group.

Exercise 3.1.8. Prove Theorem 3.1.16.

Exercise 3.1.9. Prove Theorem 3.1.17.

3.2 Basic Properties of Groups

Now that we have established what a group is and some examples of groups, we study some properties common to all groups. Thus, we adopt a generic notation. From now on, unless otherwise stated, G will denote a group, the identity of G will be denoted by e, and the inverse of $a \in G$ will be denoted by a^{-1}. Notice that this assumes a multiplicative notation for the binary operation.

In the previous chapters, you may have noticed the language *an identity* or *an inverse*. Yet, if you did your homework, you also noticed that there was never more than one identity and each element had at most one inverse. We prove these observations below. Also notice that we begin to drop the generic $*$ notation for the binary operation.

Theorem 3.2.1. *In a group G, the identity is unique.*

Proof. First, we are given that G is a group. By the definition of group, G has an identity, which we will call e.

Second, assume $e' \in G$ is also an identity. By definition of identity, we know that for all $g \in G$,

$$eg = ge = g \tag{3.1}$$

and

$$e'g = ge' = g. \tag{3.2}$$

These equalities are true for every $g \in G$, thus consider when $g = e'$. From Equation 3.1, we see that $ee' = e'e = e'$. Similarly, when $g = e$, we see from

Equation 3.2 that $e'e = ee' = e$. By transitivity of equality,

$$e' = ee' = e.$$

Thus, there is no second identity. In conclusion, the identity of G is unique. □

For this reason, we will refer to *the* identity of a group, not *an* identity of a group.

To prove that inverses are unique, we need the following lemma. If this lemma seems trivial, revisit Non-Example 2.1.8.

Lemma 3.2.2 (Cancellation Laws)**.** *In a group G, left and right cancellation laws hold. That is, for $a, b, c \in G$,*

1. *if $ab = ac$, then $b = c$, and*
2. *if $ba = ca$, then $b = c$.*

Proof. Let a, b, and c be elements in group G such that $ab = ac$. By the definition of a group, we know that a has an inverse, say a^{-1}. Composing a^{-1} on the left, we get

$$a^{-1}(ab) = a^{-1}(ac). \tag{3.3}$$

By the definition of a group, we know the operation is associative, thus we can rewrite Equation 3.3 as

$$(a^{-1}a)b = (a^{-1}a)c. \tag{3.4}$$

By the definition of inverse, we know that $a^{-1}a = e$, where e is the identity

of G, thus Equation 3.4 becomes

$$eb = ec. \tag{3.5}$$

Finally, by the definition of the identity, we see that $b = c$.

The proof is similar for right cancellation and is therefore left to the reader in Exercise 3.2.2. □

Notice that in the proof of Lemma 3.2.2, we used every piece of the definition of a group. We use associativity to create Equation 3.4, we used the existence and the definition of the identity in Equation 3.5 and the final result, and we used the existence of inverses in Equation 3.3. Cancellation allows us to get the following result, whose proof is left to the reader in Exercise 3.2.3.

Another interesting note about this proof is the level of detail. For example, once we know $a^{-1}(ab) = a^{-1}(ac)$, we do not immediately conclude $b = c$. Instead, we use the properties of groups to explain every step in between. In this chapter, your proofs should go into a similar level of detail.

Theorem 3.2.3. *In a group, inverses are unique. That is, for element $g \in G$, there is exactly one element $h \in G$ such that $gh = hg = e$, where $e \in G$ is the identity.*

Thus, we may now refer to *the* inverse of a given element, not *an* inverse of the given element. Also, when writing the inverse of element a generically, we will often write a^{-1}. If the operation is known to be addition, for example, we know the inverse of a is the element $-a$. Remember, never assume the operation is multiplication just because the notation simply looks like multiplicative notation.

Recall the Generalized Associative Law. Now that we know inverses are unique, we can define the notation a^n for $n \in \mathbb{Z}$.

Notation. Let G be a group with identity e. Let a be any element of G. For $n \in \mathbb{N}$, we define integral powers a^n as follows:

$$\begin{aligned} a^0 &= e \\ a^1 &= a \\ a^n &= a \cdots a \qquad (n \text{ copies of } a) \\ a^{-n} &= (a^{-1})^{|n|}. \end{aligned}$$

This notation helps us establish the following theorem.

Theorem 3.2.4 (Laws of Exponents for Groups)**.** *Let G be a group with identity e. Then for all $a \in G$ and for all $n, m \in \mathbb{Z}$ we have*

1. $a^n * a^m = a^{n+m}$
2. $(a^n)^m = a^{nm}$.

Below is another important property of groups. This shows us how the binary operation and inverses relate.

Theorem 3.2.5 (Socks and Shoes Property)**.** *Let a and b be elements of group G. Then*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Proof. We know that for element $ab \in G$, by the definition of inverse, $(ab)^{-1}(ab) = e$. Multiplying both sides by b^{-1} on the right, we get

$$\begin{aligned} [(ab)^{-1}(ab)]b^{-1} &= (ab)^{-1}[(ab)b^{-1}] \\ &= (ab)^{-1}[a(bb^{-1})] \\ &= (ab)^{-1}[a(e)] \\ &= (ab)^{-1}a \end{aligned}$$

by associativity and the definitions of the identity and inverses. Thus, $(ab)^{-1}a = b^{-1}$. Multiplying both sides on the right by a^{-1}, we get

$$\begin{aligned}[(ab)^{-1}a]a^{-1} &= (ab)^{-1}[aa^{-1}] \\ &= (ab)^{-1}[e] \\ &= (ab)^{-1}\end{aligned}$$

by associativity and the definitions of the identity and inverses. Ergo, $(ab)^{-1} = b^{-1}a^{-1}$, as desired. □

In the above proof, notice that we are careful to "multiply on the right." Unless we know the elements commute, we must specify on which side we multiply. Also, notice that by "multiply," we really mean "perform the operation."

Many of the groups we have seen thus far have the following property.

Definition 3.2.6. A group G is said to be Abelian if $x * y = y * x$ for all $x, y \in G$. A group is said to be non-Abelian if it is not Abelian.

Notice that the definition of Abelian and the definition of commutative are almost identical. In practice, if a group is commutative, we call it Abelian. If another type of structure is commutative, we call it commutative.

Example 3.2.7. The groups $\mathbb{C}$ under addition, $\mathbb{C}^*$ under multiplication, $\mathbb{Z}_7$ under addition, and $\mathbb{Z}_7^*$ under multiplication are all Abelian because all of their elements commute. ◇

Non-Example 3.2.8. The group D_4 is non-Abelian because not all of its elements commute. For example, $HD_L = R_{90}$ whereas $D_L H = R_{270}$. ◇

The definitions below give us some useful examples of more non-Abelian groups.

Definition 3.2.9. Let K be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ for p a prime. Then the general linear group of 2×2 matrices is the set of 2×2 matrices with entries in K and nonzero determinant under matrix multiplication, that is,

$$\mathsf{GL}_2(K) = \{A \in M_2(K) \mid \det(A) \neq 0\}.$$

Similarly, the special linear group of 2×2 matrices is the set of 2×2 matrices with entries in K and a determinant of one under matrix multiplication, that is,

$$\mathsf{SL}_2(K) = \{A \in M_2(K) \mid \det(A) = 1\}.$$

Notation. Another common notation for sets of 2×2 matrices with entries in K, instead of $M_2(K)$, is $M(2, K)$. Similarly, the general linear group may be represented as $\mathsf{GL}(2, K)$ and the special linear group may be represented as $\mathsf{SL}(2, K)$.

Theorem 3.2.10. *The general linear group of* 2×2 *matrices is a group for any* K *that is* $\mathbb{Q}$*,* $\mathbb{R}$*,* $\mathbb{C}$*, or* $\mathbb{Z}_p$ *for* p *a prime.*

The proof of this theorem is left as an exercise.

Example 3.2.11. The general linear group is a non-Abelian group. The identity of $\mathsf{GL}(2, K)$ is the identity matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Consider element

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathsf{GL}(2, K).$$

By definition of $\mathsf{GL}(2, K)$, we know that $det(A) = ad - bc \neq 0$. The inverse of element A is the element

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in \mathsf{GL}(2, K).$$

Notice that it is critical that $ad - bc \neq 0$ because we need $ad - bc$ to have a multiplicative inverse.

Not all 2×2 matrices commute, thus $\mathsf{GL}(2, K)$ is non-Abelian. For example, taking $K = \mathbb{C}$, we see that

$$\begin{bmatrix} -1 & 2 \\ 3 & 7 \end{bmatrix} \cdot \begin{bmatrix} \pi & e \\ 0 & i \end{bmatrix} = \begin{bmatrix} -\pi & 2i - e \\ 3\pi & 7i + 3e \end{bmatrix}$$

and

$$\begin{bmatrix} \pi & e \\ 0 & i \end{bmatrix} \cdot \begin{bmatrix} -1 & 2 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} 3e - \pi & 7e + 2\pi \\ 3i & 7i \end{bmatrix}.$$

$\diamond$

Note that in the inverse element, we specifically write $(ad - bc)^{-1}$ instead of $\frac{1}{ad-bc}$ to emphasize the multiplicative inverse of element $ad - bc \in K$.

Theorem 3.2.12. *The special linear group of 2×2 matrices is a group for any K that is $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ for p a prime.*

Some of the homework exercises in the previous chapters asked you to determine, given some group element g, how many copies of g were necessary under the binary operation before creating the identity. Now we begin to

develop the machinery to analyze the patterns you may have noticed.

Definition 3.2.13. Let G be a group. The order of G is the cardinality of the set G, denoted $|G|$.

Example 3.2.14. As we saw in Chapter 1, $|D_3| = 6$, $|D_4| = 8$, $|D_5| = 10$, and $|D_6| = 12$. For natural numbers $n > 2$, $|D_n| = 2n$ because there will be n rotations and n reflections. $\diamond$

Example 3.2.15. Groups can also have infinite order. For example, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$ have infinite order. $\diamond$

Example 3.2.16. For natural numbers $n \geq 2$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, thus $|\mathbb{Z}_n| = n$. $\diamond$

Definition 3.2.17. Let G be a group and consider $g \in G$. We define the order of the element g to be the smallest $n \in N$ such that $g^n = e$, and we denote this as $|g| = n$. If no such n exists, then g has infinite order.

Notice that this definition relies on the existence of the identity in the group. Thus, to determine the order of a given element, we must first determine the identity of the group.

Example 3.2.18. In $\mathbb{Z}_6$, the operation is addition modulo 6, thus the identity is 0. We have the following orders of elements.

- In $\mathbb{Z}_6$, $|0| = 1$ because one copy of 0 is needed to add to 0.
- In $\mathbb{Z}_6$, $|1| = 6$ because $1 + 1 + 1 + 1 + 1 + 1 = 0$ and no fewer copies of

1 will add to 0.

- In $\mathbb{Z}_6$, $|2| = 3$ because $2 + 2 + 2 = 0$ and no fewer copies of 2 will add to 0.
- In $\mathbb{Z}_6$, $|3| = 2$ because $3 + 3 = 0$ and no fewer copies of 3 will add to 0.
- In $\mathbb{Z}_6$, $|4| = 3$ because $4 + 4 + 4 = 0$ and no fewer copies of 4 will add to 0.
- In $\mathbb{Z}_6$, $|5| = 6$ because $5 + 5 + 5 + 5 + 5 + 5 = 0$ and no fewer copies of 5 will add to 0.

$\diamond$

Example 3.2.19. In $\mathbb{Z}$, the operation is addition, thus the identity is 0. Every element other than 0 itself has infinite order. For example, $3 \in \mathbb{Z}$ has infinite order because 3 added to itself will never sum to 0, no matter how many copies of 3 we add together. That is, $3 + 3 + 3 + \cdots + 3 \neq 0$. $\diamond$

The following example demonstrates an important point about the definition of the order of a group element.

Non-Example 3.2.20. In D_4, $|R_{180}| = 2$. Notice that $(R_{180})^4 = R_0$, but that does not necessarily mean that R_{180} has order four. The order of element is the *smallest* number of copies needed to create the identity, if any such number exists. $\diamond$

Lastly, we are now ready to prove that $U(n)$ is indeed a group. To prove that its elements have inverses, we will use Bézout's Lemma and the Division Algorithm, given below. The proofs of these theorems can be found in an introductory book about Number Theory.

Lemma 3.2.21 (Bézout's Lemma)**.** *Let $a, b \in \mathbb{Z}^*$ and $d = \gcd(a, b)$. Then there exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = d.$$

Example 3.2.22. Take $a = 6$ and $b = 15$. Then $d = \gcd(6, 15) = 3$. Bézout's Lemma states that we can find two integers x and y such that $6x + 15y = 3$. We see that when $x = 3$ and $y = -1$, $6(3) + 15(-1) = 3$, as desired. Similarly, the pair $x = -2$ and $y = 1$ also satisfies $6x + 15y = 3$. $\diamond$

Example 3.2.23. Take $a = 14$ and $b = 32$, thus $d = \gcd(14, 32) = 2$. We want to find $x, y \in \mathbb{Z}$ such that $14x + 32y = 2$. We see that when $x = 7$ and $y = -3$, $14(7) + 32(-3) = 2$. Similarly, the pair $x = -9$ and $y = 4$ also satisfies $14x + 32y = 2$. $\diamond$

Before we prove that $U(n)$ is a group, we also need the following theorem.

Theorem 3.2.24 (Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ such that $b \neq 0$. Then there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $1 \leq r < b$.*

Example 3.2.25. Let $a = 139$ and $b = 8$. By the Division Algorithm, there exist $q, r \in \mathbb{Z}$ such that $139 = 8q + r$ and $1 \leq r < 8$. We see that $q = 17$ and $r = 3$, $139 = 8(17) + 3$, as desired. $\diamond$

When using the Division Algorithm, it may be helpful to think of r as the remainder of a when divided by b.

Recall that $U(n) = \{x \in \mathbb{N} \,|\, 1 \leq x < n, \gcd(x, n) = 1\}$. As promised, the proof is slightly more complicated than the proof of Theorem 3.1.15. Typically, to prove a set with an operation is a group, we first verify that the operation is binary, and then we prove the three properties of a group: associativity, identity, and inverses. The proof that $U(n)$ is a group does not directly follow this path because proving that the operation is binary is

nontrivial. Even though multiplication modulo n is a binary operation on $\mathbb{Z}_n$, we can not assume it is a binary operation on $U(n)$. This is because $U(n)$ is a proper subset of $\mathbb{Z}_n$, thus we must verify that the operation is indeed closed on the smaller set, that is, we must verify that two elements in $U(n)$, when multiplied together, create an element in $U(n)$ and not $\mathbb{Z}^* - U(n)$.

Example 3.2.26. Let $n = 8$, then $U(8) = \{1, 3, 5, 7\}$. To show that $U(8)$ is closed, we need to know that for every combination of $a, b \in U(8)$, ab is an odd number less than $n = 8$. Create the Cayley table of $U(8)$ to verify that this is indeed true. $\diamond$

Example 3.2.27. Let $n = 10$ and consider $9, 13 \in \mathbb{Z}$. Notice that $\gcd(9, 10) = \gcd(13, 10) = 1$. Further, $\gcd(9 \cdot 13, 10) = \gcd(3^2 \cdot 13, 10) = 1$. $\diamond$

Below is a lemma that generalizes Example 3.2.27. This will help us prove the closure of $U(n)$.

Lemma 3.2.28. *Suppose* $a, b, n \in \mathbb{N}$ *such that* $\gcd(a, n) = \gcd(b, n) = 1$. *Then* $\gcd(ab, n) = 1$.

Proof. Let $a, b, n \in \mathbb{N}$ such that $\gcd(a, n) = \gcd(b, n) = 1$. Suppose that $\gcd(ab, n) = d \in \mathbb{N}$. Thus, d divides both n and ab. By assumption, $1 \in \mathbb{N}$ is the largest natural number that divides both a and n, thus d must divide b. Similarly, $1 \in \mathbb{N}$ is the largest natural number that divides both b and n, thus $d = 1$. $\square$

Theorem 3.2.29. *For every natural number* $n \geq 2$, $U(n)$ *is a group.*

Proof. To prove that $U(n)$ is a group, we will first verify that the set of units under multiplication modulo n is associative, has an identity, and has inverses.

1. Multiplication modulo n is associative because multiplication over the integers is associative.

2. The natural number 1 will always be an element of $U(n)$ because for any natural $n \geq 2$, $\gcd(1, n) = 1$. Moreover, 1 is the identity because for any $a \in U(n)$, $1 \cdot a = a \cdot 1 = a$.

3. Let $a \in U(n)$, thus $\gcd(a, n) = 1$. We want to find some element b such that $ab \equiv 1 \bmod n$ and $1 \leq b < n$. By Bézout's Lemma, there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$, or $ax = 1 - ny$. In modular n arithmetic, this means that

$$ax \equiv 1 \bmod n. \tag{3.6}$$

   Thus, if $1 \leq x < n$, then x is the inverse of a.

   If it is not already true that $1 \leq x < n$, then by the Division Algorithm, we can find $q, r \in \mathbb{Z}$ such that $x = qn + r$ and $1 \leq r < n$. Thus $x \equiv qn + r \equiv r \bmod n$. Further, $ax \equiv a(qn + r) \equiv ar \equiv 1$ by Equation 3.6. Thus, r is the inverse of a.

Last, we will show that the set of units multiplication modulo n is closed. Take $a, b \in U(n)$. By definition, $\gcd(a, n) = \gcd(b, n) = 1$ and $1 \leq a, b < n$. By Lemma 3.2.28, $\gcd(ab, n) = 1$. If it is not already true that $1 \leq ab < n$, then, using the same argument as above, the Division Algorithm guarantees we can reduce ab to some r such that $ab \equiv r \bmod n$.

□

EXERCISES

Exercise 3.2.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let G be a group with identity e and elements a, b, c.

a. Left cancellation and right cancellation are equivalent properties.

b. If $ab = e$ and $ac = e$, then $b = c$.

c. If $a^8 = e$, then $|a| = 8$.

d. $ab = ba$

e. $(ab)^{-1} = a^{-1}b^{-1}$

f. For $n \in \mathbb{N}$, $(ab)^n = a^n b^n$.

g. Group G has an element of finite order.

h. Group G has an element of infinite order.

i. If set A is a proper subset of set B, and B has binary operation $*$, then $*$ is also binary on A.

Exercise 3.2.2. Prove that right cancellation holds.

Exercise 3.2.3. Prove Theorem 3.2.3.

Exercise 3.2.4. Prove that the inverse of an inverse is the original element. That is, if $h \in G$ is the inverse of $g \in G$, prove that g is the inverse of h.

Exercise 3.2.5. Prove Theorem 3.2.10.

Exercise 3.2.6. Prove Theorem 3.2.12.

Exercise 3.2.7. Let G be a group and $a \in G$. For $n \in \mathbb{N}$, show that $a^{-n} = (a^n)^{-1}$.

Exercise 3.2.8. Write the Socks-and-Shoes Property in additive notation.

Exercise 3.2.9. Refer back to the Socks-and-Shoes Property.

a. In your own words, how does the property relate to "socks and shoes?"

b. Give a specific example of a group G and two specific elements $a, b \in G$ in the group such that $(a * b)^{-1} \neq a^{-1} * b^{-1}$.

c. Prove that G is Abelian if and only if $(a * b)^{-1} = a^{-1} * b^{-1}$.

Exercise 3.2.10. Consider the Socks-and-Shoes Property and the Generalized Associative Law. Let $n \geq 3$ be a natural number and $a_1, a_2, \ldots, a_n$ are elements of a group G.

a. Show that $(a_1 * a_2 * a_3)^{-1} = a_3^{-1} * a_2^{-1} * a_1^{-1}$.

b. Show that $(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a_2^{-1} * a_1^{-1}$. *(Hint: Use induction.)*

Exercise 3.2.11. Let G be a group and $a, b \in G$.

a. Give an example of a group and two elements such that $(ab)^2 \neq a^2b^2$.

b. Prove that if $ab = ba$, then $(ab)^n = a^n b^n$. *(Hint: Use induction.)*

c. Why is the above assumption that $ab = ba$ weaker than commutativity? That is, what is the difference between assuming $ab = ba$ and assuming G is commutative?

Exercise 3.2.12. For $n \in \mathbb{N}$, prove that $n\mathbb{Z}$ is an Abelian group.

Exercise 3.2.13. Consider the group $\mathsf{GL}_2(\mathbb{Z}_7)$.

a. Find $A, B \in \mathsf{GL}(2, \mathbb{Z}_7)$ such that $AB \neq BA$.

b. Find the inverse of $\begin{bmatrix} 1 & 6 \\ 5 & 3 \end{bmatrix} \in \mathsf{GL}_2(\mathbb{Z}_7)$.

c. Find the inverse of $\begin{bmatrix} 2 & 5 \\ 3 & 6 \end{bmatrix} \in \mathsf{GL}_2(\mathbb{Z}_7)$.

d. Give a nonzero example of $C \in M_2(\mathbb{Z}_7)$ that does not have an inverse.

Exercise 3.2.14. Translate Definition 3.2.17 into additive notation.

Exercise 3.2.15. Find the order of each of the following groups. In each group, determine how many elements have finite order.

a. $\mathbb{Z}_{10}$

b. $U(10)$

c. $10\mathbb{Z}$

Exercise 3.2.16. Find an example of an element $a \in \mathbb{Z}_{12}$ such that $a^6 = e$ but $|a| \neq 6$.

Exercise 3.2.17. Suppose G is a group and $a \in G$ such that $a^{12} = e$. What are all the possibilities of $|a|$? Justify your answer.

Exercise 3.2.18. For each of the following groups, find the order of the group and the order of each element. How do the orders of the elements relate to the order of the group?

a. D_5

b. Z_8

c. $U(20)$

Exercise 3.2.19. Find all the elements in the group $\mathsf{GL}_2(\mathbb{Z}_2)$, and find their orders.

Exercise 3.2.20. Find a group of order one and prove your set is indeed a group.

Exercise 3.2.21. Let $g \in G$. Prove that $|g| = 1$ if and only if g is the identity.

Exercise 3.2.22. In a group G, prove that an element and its inverse have the same order.

3.3 Subgroups

Now that we have some familiarity with groups, we begin to develop some useful tools that will help us prove some of the patterns we have begun to observe.

Definition 3.3.1. Let G be a group. A subgroup of G is a subset $H \subseteq G$ which is also a group under the same operation as G. This relationship is denoted as $H \leq G$.

This means that H is closed under the operation of G, has associativity, has the same identity as G, and has inverses. Notice that by referring to H as a *sub*group, we must establish the *parent* group G.

Example 3.3.2. In Theorem 3.1.15, we proved that $\mathbb{C}$ is a group under addition. As $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ and all of these sets are themselves groups under addition, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all subgroups of $\mathbb{C}$. In fact, $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{C}$. $\diamond$

Example 3.3.3. The group $4\mathbb{Z}$ is a subgroup of $2\mathbb{Z}$. By Theorem 3.1.18, both $4\mathbb{Z}$ and $2\mathbb{Z}$ are groups under the operation of addition. The multiples of four form a subset of the multiples of two, thus $4\mathbb{Z} \subset 2\mathbb{Z}$. Thus, $4\mathbb{Z} \leq 2\mathbb{Z}$. $\diamond$

Definition 3.3.4. Given a group G with identity e, the group $\{e\}$ is the trivial subgroup of G. A subgroup H of G is called nontrivial if $\{e\} < H \leq G$; further, it is a proper subgroup of G if $\{e\} < H < G$.

Throughout the text, we will use the notation $H \leq G$ to imply that H is a subgroup of group G. When we wish to refer to the sets H and G, and not the algebraic structure implied by the word "group," we may write $H \subseteq G$ for emphasis.

The definition of subgroup has two important pieces to it: the set must be a subset of a group and the operation must be the same. These distinctions are illustrated in the non-example below.

Non-Example 3.3.5. Consider $\mathbb{Z}_5$ and $\mathbb{Z}$. While it is true that $\{0, 1, 2, 3, 4\} \subseteq \mathbb{Z}$, $\mathbb{Z}_5 \not\leq \mathbb{Z}$ because the two groups have different operations. The group $\mathbb{Z}_5$ has the operation of addition modulo 5 and $\mathbb{Z}$ has the operation of addition. Thus, $\mathbb{Z}_5$ is *not* a subgroup of $\mathbb{Z}$. $\diamond$

Non-Example 3.3.6. Consider $U(5)$ and $\mathbb{Z}_5$. It is true that $\{1, 2, 3, 4\} \subseteq \{0, 1, 2, 3, 4\}$, though $U(5) \not\leq \mathbb{Z}_5$ because the two groups have different operations. The operation of $U(5)$ is multiplication modulo 5, whereas the operation of $\mathbb{Z}_5$ is addition modulo 5. $\diamond$

Non-Example 3.3.7. The group D_4 is not a subgroup of D_5. Although function composition is the operation of both groups, neither set is a subset of the other. $\diamond$

Example 3.3.8. Consider the group D_8, which is the group of rigid movements of a regular octagon. The rotations in this group will be increments of $45°$. The reflections in this group will be along the lines of symmetry, which occur in increments of $45°$. As function composition is the operation of all dihedral groups, $D_4 \leq D_8$. $\diamond$

It is often easier to prove a set H is a subgroup of a known group than to prove H is a group by itself. As you may have noticed, proving that a group satisfies closure and associativity can be cumbersome. The One-Step Subgroup Test and Two-Step Subgroup Test are tools that allow us to bypass the definition of a group and prove a set H is a subgroup, and hence a group, of a parent group G. As we will see, proofs using the subgroup tests can be much shorter.

Theorem 3.3.9 (Two-Step Subgroup Test)**.** *Let G be a group and let $H \subseteq G$ be nonempty. Assume G and H are under the same operation. For $a, b \in H$, if*

1. *$ab \in H$, and*

2. $a^{-1} \in H$

then H is a subgroup of G.

Proof. To prove that H is a subgroup of G, we must show that it is a group, thus we must show that the operation is closed and associative, there is an identity, and every element has an inverse.

1. We are given that for all $a, b \in H$, $ab \in H$, thus H is closed.
2. We are given that G is a group under its operation, thus the operation is associative.
3. We are given that for all $a, b \in H$, $ab, a^{-1} \in H$. Taking $b = a^{-1}$, we see that $aa^{-1} = e \in H$.
4. We are given that for all $a \in H$, $a^{-1} \in H$.

Thus, the subset H is a group under the operation of G, making H a subgroup of G. □

The Two-Step Subgroup Test shows that, in order to prove H is a subgroup of G, it is sufficient to prove that H is closed and contains inverses, hence the name Two-Step. There is a hidden zeroth step in the Two-Step Subgroup Test: the test assumes H is nonempty. Thus, in order to apply the Two-Step Subgroup Test, we must always first prove that the subset H has an element in it. This is usually done by example. As every group must have an identity, it is often easiest to prove that the identity of the parent group is indeed in the subset. We give an example of this below.

Recall that if a set is given in set-builder notation, it is often prudent to prove it is a group using the defining qualities of the set. This is also demonstrated

in the example below. Lastly, notice that the Two-Step Subgroup Test assumes multiplicative notation. The groups in the example below have the binary operation of addition, thus the Two-Step Subgroup Test is translated into additive notation.

Example 3.3.10. In Example 3.3.3, we prove that the group $4\mathbb{Z}$ is a subgroup of $2\mathbb{Z}$. For emphasis, we will now use the Two-Step Subgroup Test to achieve this same result.

Let $4z \in 4\mathbb{Z}$. Then $4z = 2(2z) \in 2\mathbb{Z}$. Thus $4\mathbb{Z} \subset 2\mathbb{Z}$. We know that $2\mathbb{Z}$ is a group with identity 0. Further, $0 \in 4\mathbb{Z}$ because $0 = 4 \cdot 0$ where $0 \in \mathbb{Z}$. Thus, $4\mathbb{Z}$ is nonempty and we may apply the Two-Step Subgroup Test. Take $4x, 4y \in 4\mathbb{Z}$. Then $4x+4y = 4(x+y)$ by distributivity, and because $x+y \in \mathbb{Z}$, $4(x+y) \in 4\mathbb{Z}$. Thus, $4\mathbb{Z}$ is closed. Further, $-4x = 4(-x) \in 4\mathbb{Z}$ because $-x \in \mathbb{Z}$, and $4x + (-4x) = 0$. Thus, elements in $4\mathbb{Z}$ have inverses. By the Two-Step Subgroup Test, $4\mathbb{Z}$ is a subgroup of $2\mathbb{Z}$. $\diamond$

The One-Step Subgroup Test also shows that it is sufficient to prove that H is closed and contains inverses; it just does this in one step instead of two. Like the Two-Step Subgroup Test, the One-Step Subgroup Test also assumes the subset H is nonempty. To prove it, we use our new favorite tool, the Two-Step Subgroup Test.

Theorem 3.3.11 (One-Step Subgroup Test)**.** *Let G be a group and let $H \subseteq G$ be nonempty. Assume G and H are under the same binary operation. For $a, b \in H$, if*

1. $ab^{-1} \in H$

then H is a subgroup of G.

Proof. By assumption, H is nonempty, thus we may take some $x \in H$. We

are also given that for all $a, b \in H$, $ab^{-1} \in H$, thus taking $a = b = x$, we see that $xx^{-1} = e \in H$. Now we proceed using the Two-Step Subgroup Test.

1. Taking $a = a$ and $b = e$, we see that $ab^{-1} = a \in H$. Now we have that $a, e \in H$, thus by the given, $ea^{-1} = a^{-1} \in H$.

2. Now that we have shown that H contains inverses, we may assume that for all $a, b \in H$, we have $ab^{-1}, a^{-1}, b^{-1} \in H$. Thus, $a(b^{-1})^{-1} = ab \in H$.

Therefore, by the Two-Step Subgroup Test, H is a subgroup of G. □

Below is an example of how to use the One-Step Subgroup Test.

Example 3.3.12. In Examples 3.3.3 and 3.3.10, we showed that $4\mathbb{Z}$ is a subgroup of $2\mathbb{Z}$. Once again, we prove this result, only this time we do so using the One-Step Subgroup Test.

We know that $4\mathbb{Z}$ is a subset of $2\mathbb{Z}$ and the group $2\mathbb{Z}$ has identity 0. Moreover, $0 \in 4\mathbb{Z}$ because $0 = 4 \cdot 0$ and $0 \in \mathbb{Z}$. Thus, $4\mathbb{Z}$ is nonempty and we may apply the One-Step Subgroup Test. Take $4x, 4y \in 4\mathbb{Z}$. By definition of $4\mathbb{Z}$, $x, y \in \mathbb{Z}$, thus $-y \in \mathbb{Z}$. Then $4x - 4y = 4(x - y)$ by distributivity, and because $x - y \in \mathbb{Z}$, $4(x - y) \in 4\mathbb{Z}$. By the One-Step Subgroup Test, $4\mathbb{Z} \leq 2\mathbb{Z}$. ◇

Let G be a group and H a set. As Examples 3.3.10 and 3.3.12 demonstrate, sometimes it is necessary to also address that H is indeed a subset of G before employing the Two-Step or One-Step Subgroup Test. This depends on the definition of H.

- If H is *not* defined to consist of elements of G, then we *do* need to address that $H \subseteq G$. For example, when $G = 2\mathbb{Z}$ and

$$H = 4\mathbb{Z} = \{4z \mid z \in \mathbb{Z}\},$$

it is not necessarily evident from the definition of H that every element of H will also be in G.

- If H *is* defined to consist of elements of G, then we do *not* need to address that $H \subseteq G$. For example, if

$$H = \{g \in G \mid g \text{ has whatever property}\},$$

then all elements of H come from G by the definition of H.

The theorem below will be a useful one, and its proof is another example of the One-Step Subgroup Test.

Theorem 3.3.13. *Let $n \geq 3$ be a natural number. The set of all rotations in D_n is a subgroup of D_n.*

Proof. We know that R_0 is a rotation in every D_n, thus the set of all rotations is nonempty and we may now apply the One-Step Subgroup Test. Consider two arbitrary rotations $R_a, R_b \in D_n$. Each rotation will be some multiple of $360/n$ degrees. Thus,

$$a = a'\left(\frac{360}{n}\right) \text{ and } b = b'\left(\frac{360}{n}\right)$$

for some $a', b' \in \{0, 1, \ldots n-1\}$. Then $R_a(R_b)^{-1}$ is a rotation by $-b$ degrees followed by a rotation of a degrees. This simplifies into a rotation by

$$\begin{aligned} -b + a &= -b'\left(\frac{360}{n}\right) + a'\left(\frac{360}{n}\right) \\ &= (-b' + a')\left(\frac{360}{n}\right) \end{aligned}$$

degrees. Notice that because $\{0, 1, \ldots n-1\} = \mathbb{Z}_n$ is a group, $-b' + a \in \{0, 1, \ldots n\}$. Thus, $R_a(R_b)^{-1}$ is also a rotation in D_n. □

Now that we have these tools, proving a set under an operation is a group is less cumbersome, as long as we have a parent group.

We give one last example below. Notice that the operation is addition, thus when we employ the One-Step Subgroup Test, we use the additive notation.

Theorem 3.3.14. *The integers are a group under addition.*

Proof. In Theorem 3.1.15, we proved that $\mathbb{C}$ is a group. Thus, to show that $\mathbb{Z}$ is a group, we will show that $\mathbb{Z}$ is a subgroup of $\mathbb{C}$. We proceed using the One-Step Subgroup Test. Let $a, b \in \mathbb{Z}$. Then $a - b \in \mathbb{Z}$, thus $\mathbb{Z}$ is a subgroup of $\mathbb{C}$. □

That is one cute proof.

EXERCISES

Exercise 3.3.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a. $\mathbb{Q} \leq \mathbb{C}$

b. For $n \in \mathbb{N}$, $D_n \leq D_{n+1}$.

c. For $n \in \mathbb{N}$, $D_n \leq D_{n+2}$.

d. For $n \in \mathbb{N}$, $D_n \leq D_{2n}$.

e. For $n \in \mathbb{N}$, $\mathbb{Z}_n \leq \mathbb{Z}_{n+1}$.

f. For $n \in \mathbb{N}$, $\mathbb{Z}_n \leq \mathbb{Z}_{2n}$.

g. For G a group, $G \leq G$.

h. A group G has at least two subgroups.

i. The intersection of two subgroups is a subgroup.

j. The union of two subgroups is a subgroup.

Exercise 3.3.2. Determine which of the following subsets of $\mathbb{Z}_{12}$ are subgroups of $\mathbb{Z}_{12}$. If the set is not a group, explain why not.

a. $A = \{0, 3, 6, 9\}$

b. $B = \{0, 6\}$

c. $C = \{1, 3, 5, 7, 9, 11\}$

Exercise 3.3.3. For each of the following, G is a group and S is a subset of G. If S is a subgroup of G, prove it. If S is not a subgroup, explain why not.

a. $G = U(16)$, $S = U(8)$

b. $G = D_5$, $S = \{x \in D_5 \mid x \text{ is a reflection}\}$

c. $G = D_4$, $S = \{R_0, R_{180}\}$

d. G, $S = \varnothing$

Exercise 3.3.4. Let G be a group with identity e.

a. Prove that $\{e\}$ is a subgroup of G.

b. Prove that G is a subgroup of G.

Exercise 3.3.5. Refer back to Theorems 3.3.9 and 3.3.11.

a. Translate the Two-Step Subgroup Test into additive notation.

b. Translate the One-Step Subgroup Test into additive notation.

Exercise 3.3.6. Prove that $12\mathbb{Z}$ is a subgroup of $3\mathbb{Z}$.

Exercise 3.3.7. Let G be a group. Suppose H is a subgroup of G and K is a subgroup of H. Prove that K is a subgroup of G.

Exercise 3.3.8. Let G be a group and let H and K be subgroups of G. For each of the following statements, if the statement is true, prove it, and if the statement is false, find a counterexample.

a. $H \cup K \leq G$

b. $H \cap K \leq G$

Exercise 3.3.9. Let G be an Abelian group with identity e and fix $n \in \mathbb{N}$. Prove that

$$H = \{g \in G \mid g^n = e\}$$

is a subgroup of G.

Exercise 3.3.10. Let G be an Abelian group and fix $n \in \mathbb{N}$. Define the set G^n as

$$G^n = \{g^n \mid g \in G\}$$

a. Pick you favorite Abelian group and your favorite small $n \in \mathbb{N}$ to create an example G^n. Create the Cayley table for your example.

b. Prove that G^n is a subgroup.

c. Does this result hold when G is non-Abelian? Why or why not?

3.4 Permutation Groups

In the next section, we will study subgroups common to all groups. To understand some of their important subtleties, we will be better served by analyzing subgroups of non-Abelian groups. In this section, we introduce a very important type of non-Abelian group, the group of permutations. Before we define the group of permutations, we revisit permutations and some related definitions.

Definition 3.4.1. Let f be a function on a set D. Then f is one-to-one, or injective, if for every $a, b \in D$,

$$f(a) = f(b) \text{ implies } a = b.$$

A function that is not injective is called non-injective.

A function is one-to-one if for every output, there is exactly one input. In the definition above, we start with one output represented two different ways as $f(a)$ and $f(b)$. In this notation, it appears as if there are two inputs, a and b. A one-to-one function guarantees us that the two inputs are actually equal, that is, $a = b$, and thus there is actually just one input.

We have seen plenty of examples of injective and non-injective functions in calculus.

Example 3.4.2. Take $f(x) = x$ in $\mathbb{R}[x]$. Then $f(x)$ is one-to-one because, for $a, b \in \mathbb{R}$, if $f(a) = f(b)$, then by the definition of $f(x)$, $a = b$. Thus, we conclude that if we start with one output, that output came from one input. $\diamond$

Example 3.4.3. Take $f(x) = x^3 - 2$ in $\mathbb{R}[x]$. Then $f(x)$ is one-to-one because, for $a, b \in \mathbb{R}$, if $f(a) = f(b)$, then by the definition of $f(x)$,

$$\begin{aligned} a^3 - 2 &= b^3 - 2 \\ a^3 &= b^3 \\ a &= b. \end{aligned}$$

Thus, we see that one output, $f(a) = f(b)$, came from one input $a = b$. $\diamond$

Non-Example 3.4.4. Take $f(x) = x^2$ in $\mathbb{R}[x]$. Then $f(x)$ is *not* one-to-one. For example, if $f(a) = f(b) = 4$, then $a = 2$ and $b = -2$ could *both* produce this output. Thus, we see that two different inputs created one output. $\diamond$

Non-Example 3.4.4 gives an example of a *two*-to-one function instead of a one-to-one function. We will study functions like these more in Section 4.1.

Below is an example of a one-to-one function on a finite set.

Example 3.4.5. Define $\sigma : \mathbb{Z}_5 \to \mathbb{Z}_5$ as $\sigma(0) = 4$, $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 0$, and $\sigma(4) = 1$. We can see that σ is one-to-one because every output is created by only one input. $\diamond$

The next definition measures the "niceness" of functions in a different way. One-to-one means that every output came from exactly one input. This next definition means that everything in the codomain is indeed an output of the function, that is, that the codomain and the range are equal.

Definition 3.4.6. Let f be a function from set D to set C. Then f is onto, or surjective, if

$$\forall\, c \in C,\ \exists\, a \in D \text{ such that } f(a) = c.$$

A function that is not surjective is called non-surjective.

A function is onto if everything in the codomain gets mapped to by at least one element in the domain.

Example 3.4.7. Define $f : \mathbb{R} \to \mathbb{R}$ as $f(x) = x + 1$ and take $c \in \mathbb{R}$ to be an element of the codomain $\mathbb{R}$. To show that $f(x)$ is onto, we need to find an element a in the domain $\mathbb{R}$ that maps to c. That is, we need to solve $f(a) = c$ for a. Notice that

$$\begin{aligned} f(a) &= c \\ a + 1 &= c \\ a &= c - 1. \end{aligned}$$

Thus, take the element $a = c - 1$ in the domain $\mathbb{R}$. We see that

$$f(a) = f(c-1) = (c-1) + 1 = c.$$

Hence, c, our generic element in the codomain, gets mapped to by the element $c - 1$ in the domain. Therefore $f(x)$ is onto. $\diamond$

Example 3.4.8. The function $f(x) = x^2$ is *not* onto if we define $f(x)$ to map from $\mathbb{R}$ to $\mathbb{R}$. This is because none of the negative reals are in the range of $f(x)$.

The function $f(x) = x^2$ *is* onto if we define $f(x)$ to map from $\mathbb{R}$ to $[0, \infty)$. $\diamond$

The function in Example 3.4.5 is also onto. Functions that are both one-to-one and onto have a special name.

Definition 3.4.9. A function that is both injective and surjective is called bijective.

Example 3.4.10. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function.

- The function $f(x) = 2x$ is injective but not surjective. It is injective because for every even integer, there is a unique input. It is non-surjective because not all of $\mathbb{Z}$ is mapped to by f, specifically, f does not produce any odd integers.

- The function
$$f(x) = \begin{cases} x - 1 & x \in \mathbb{N} \\ x & x \in \mathbb{Z} - \mathbb{N} \end{cases}$$
is surjective but not injective. It is non-injective because $f(x) = 0$

when $x = 1$ and when $x = 0$. It is surjective because every integer will be produced.

- The function $f(x) = x + 5$ is both injective and surjective. It is injective because every integer gets produced uniquely from the integer five integers before it.
- The function $f(x) = |x|$ is neither injective nor surjective. It is non-injective because every positive integer can be produced from either itself or its negative. It is non-surjective because no negative integers are produced.

$\diamond$

Now that we have an understanding of injectivity, surjectivity, and bijectivity, we are ready to begin to study an important class of groups.

Definition 3.4.11. A permutation of a set D is a function from D to D that is both one-to-one and onto. A permutation group of a set D is a set of permutations of D that is a group under function composition.

While this definition allows for the set D to be finite or infinite, we will mainly focus on permutations of finite sets. The function in Example 3.4.5 is a permutation of $\mathbb{Z}_5$ because it is a bijection that acts on $\mathbb{Z}_5$. It is common to label permutations with lowercase Greek letters.

A permutation group is a group of permutations. There are two main groups that we will study in this section. As we mentioned earlier, once we study subgroups more in Section 3.5, we will see more constructions of groups of permutations.

Definition 3.4.12. Take a natural number $n \geq 2$ and let $D = \{1, 2, 3, \ldots, n\}$. The set of all permutations of D is the symmetric group of degree n and is denoted S_n.

Of course, we must prove S_n is a group. We are not proving it is a subgroup of something else, thus our proof technique will be to show that the definition of S_n satisfies the definition of a group.

Theorem 3.4.13. *The symmetric group S_n, where $n \geq 2$ is a natural number, is a group.*

Proof. The set of permutations is closed because any composition of permutations of n items will result in a permutation of those n times. It is associative because function composition is associative. The identity, e, is the permutation that sends each number to itself. Thus, $e \in S_n$ for all $n \geq 2$. If $\sigma \in S_n$, then σ^{-1} is also a permutation of n objects, and hence $\sigma^{-1} \in S_n$. □

Example 3.4.14. Let $n = 6$, $D = \{1, 2, 3, 4, 5, 6\}$, and define $\sigma : D \to D$ as $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 5$, $\sigma(4) = 4$, $\sigma(5) = 6$, and $\sigma(6) = 3$. Then $\sigma \in S_6$. ◇

As you can see in Example 3.4.14, it can be a bit cumbersome to define the exact mapping of a permutation. We will study two different notations for permutations of finite order. The first notation is matrix notation, and though it is initially more intuitive, we will see the other notation is more fluid.

Notation. We can represent permutations using *matrix notation*. The per-

mutation $\sigma \in S_n$ has form

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}.$$

In this matrix, the top row contains all of the n natural numbers that will be permuted. The second row contains the image of each number.

Example 3.4.15. The permutation in Example 3.4.14 can be represented in matrix notation as

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}.$$

$\diamond$

Example 3.4.16. Let's consider S_3. Functions in S_3 permute the symbols 1, 2, and 3. Thus there are 3! functions in total. These functions are listed in matrix notation below:

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}.$$

$\diamond$

Example 3.4.17. Ⓢ Consider S_4, the set of permutation of four objects. Traditionally we work with the objects as numbers, but they do not necessarily have to be numbers. Let these four objects be ♡, ♢, ♠, ♣. Observe the identity element in S_4 in matrix notation is

$$\begin{bmatrix} ♡ & ♢ & ♠ & ♣ \\ ♡ & ♢ & ♠ & ♣ \end{bmatrix}.$$

Since we have four objects, we know that there are $4! = 24$ different cycles we can generate in S_4.

Consider the permutation which maps $\heartsuit \mapsto \spadesuit$, $\diamondsuit \mapsto \spadesuit$, $\spadesuit \mapsto \diamondsuit$, and $\spadesuit \mapsto \heartsuit$. This permutation is written in matrix notation as

$$\begin{bmatrix} \heartsuit & \diamondsuit & \spadesuit & \clubsuit \\ \spadesuit & \clubsuit & \diamondsuit & \heartsuit \end{bmatrix}.$$

$\diamondsuit$

The symmetric groups and the dihedral groups are closely related, though they are not the same. Consider the numbering of the vertices of the regular n-gon. Before any movements act on the n-gon, the vertices are presented in numerical order. After a movement acts on the n-gon, the vertices may be relabeled, though the numbers $1, 2, \ldots, n$ still appear on the n-gon. Thus, an element in D_n permutes the numbers $1, 2, \ldots, n$.

Example 3.4.18. Consider the groups S_5 and D_5. The element $F_{SE} \in D_5$ can be represented as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{bmatrix}.$$

Let $\beta \in S_5$ be the permutation

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}.$$

We see that β represents $R_{144} \in D_5$. Now let $\gamma \in S_5$ be the permutation

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{bmatrix}.$$

We see that though γ is indeed a permutation of the numbers 1 through 5, it does not represent any elements in D_5. This is because it is impossible to switch the vertices labeled 1 and 2 while holding the vertices labeled 3, 4, and 5 fixed (without ripping our precious pentagon). $\diamondsuit$

In Example 3.4.16, you may have noticed how redundant it was to list the first row in the permutations because the first row for all three was always [1 2 3]. Similarly, in Example, 3.4.18, the first row in the permutations α, β, and γ was [1 2 3 4 5], because as $\alpha, \beta, \gamma \in S_5$. The next notation for permutations avoids this redundancy. We introduce this notation with an example, and then formalize it.

Example 3.4.19. Consider the permutations $\alpha, \beta, \gamma \in S_5$ as in Example 3.4.18. We see that in α

$$1 \mapsto 3 \mapsto 1$$
$$2 \mapsto 2$$
$$4 \mapsto 5 \mapsto 4.$$

In this sense, α represents the permutation of these three cycles. We can thus represent α in terms of its cycles as

$$\alpha = (13)(45),$$

and notice that we've left off the cycle (2) because 2 maps to itself. Similarly, in terms of their cycles, we see that in β,

$$1 \mapsto 3 \mapsto 5 \mapsto 2 \mapsto 4 \mapsto 1.$$

Thus, $\beta = (13524)$. In γ,

$$1 \mapsto 2 \mapsto 1$$
$$3 \mapsto 3$$
$$4 \mapsto 4$$
$$5 \mapsto 4,$$

thus $\gamma = (12)$. $\diamond$

In Example 3.4.19, β has the cycle

$$1 \mapsto 3 \mapsto 5 \mapsto 2 \mapsto 4 \mapsto 1.$$

Of course, this is a cycle, and it repeats indefinitely. We could continue to write the cycle as

$$1 \mapsto 3 \mapsto 5 \mapsto 2 \mapsto 4 \mapsto 1 \mapsto 3 \mapsto 5 \mapsto 2 \mapsto 4 \mapsto \cdots .$$

This is a bit redundant. To be as succinct as possible, we want to list every number in the cycle in the order in which it appears, and no more. Thus, we represent β as (13524). The last number in this cycle is 4, which is a clue that 4 is the end of the first unique cycle. Thus, in order to start the cycle again, 4 must go back to the first number in the cycle, which in this case is 1.

Below we formalize this notation. Given that we are mathematicians, this will be the preferred notation as it is more succinct, though it is perfectly fine to use matrix notation as you familiarize yourself with permutations.

Notation. We can represent permutations using *cycle notation*. Each cycle is written in parentheses, and the permutation is written as a string of cycles. When writing a permutation in cycle notation, there are a few customs to notice.

1. When the cycle repeats, rather than rewriting the first number in listed in the cycle, we just close the cycle.

2. Cycles of just one number are not written.

3. We begin each new cycle with the smallest number that has not yet

been included in a cycle. That is why, for example, in Example 3.4.19, α has the cycle (13) written first and the cycle (45) written second.

4. If $n \geq 10$, it is acceptable to use commas to punctuate the cycles.

Below is some vocabulary to help us describe cycles.

Definition 3.4.20. Given a permutation $\sigma \in S_n$, an m-cycle is a cycle of length m. Two cycles are disjoint if they share no common symbols.

Example 3.4.21. In Example 3.4.19, α has two 2-cycles, β is one 5-cycle, and γ is one 2-cycle. $\diamond$

Permutations are functions and the group operation in S_n is function composition. Below are some examples of how to compose permutations. Remember, function composition is read *right to left*.

Example 3.4.22. Let $\alpha, \beta \in S_7$ be

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 7 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 2 & 1 & 4 & 7 & 3 \end{bmatrix}.$$

Then to determine $\alpha\beta$, we see that

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 2 & 1 & 4 & 7 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 7 & 6 \end{bmatrix},$$

which creates the maps listed below.

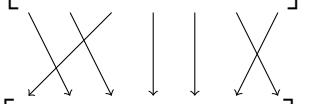
$$\begin{array}{ccccc} \text{Original} & & \beta & & \alpha \\ \downarrow & & \downarrow & & \downarrow \\ 1 & \mapsto & 6 & \mapsto & 7 \\ 2 & \mapsto & 5 & \mapsto & 5 \\ 3 & \mapsto & 2 & \mapsto & 3 \\ 4 & \mapsto & 1 & \mapsto & 2 \\ 5 & \mapsto & 4 & \mapsto & 4 \\ 6 & \mapsto & 7 & \mapsto & 6 \\ 7 & \mapsto & 3 & \mapsto & 1 \end{array}$$

Ergo, $\alpha\beta$ is the permutation

$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 3 & 2 & 4 & 6 & 1 \end{bmatrix}.$$

Similarly, to determine $\beta\alpha$, we see that

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 7 & 6 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 2 & 1 & 4 & 7 & 3 \end{bmatrix},$$

thus $\beta\alpha$ is the permutation

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 6 & 1 & 4 & 3 & 7 \end{bmatrix}.$$

$\diamond$

Again, matrix notation is cumbersome and redundant. Below we rework the compositions in Example 3.4.22 using cycle notation.

Example 3.4.23. Consider α and β in Example 3.4.22. In cycle notation, we see that

$$\alpha = (123)(67) \text{ and } \beta = (1673254).$$

The composition $\alpha\beta$ is

$$\alpha\beta = (123)(67)(1673254).$$

For ease of the example, let's label the cycles $\sigma_3 = (123)$, $\sigma_2 = (67)$, and $\sigma_1 = (1673254)$, though this labeling is nontraditional. Remember that we read function composition right to left, thus we start reading on the right and scan left. We will determine how each cycle affects each number.

Adhering to convention, we first focus on how $\alpha\beta$ permutes the symbol 1. In σ_1, we see that $1 \mapsto 6$. Thus, as we continue reading right to left, we now must determine where 6 is sent. In σ_2, we see that $6 \mapsto 7$. As we continue, we now must determine where 7 gets sent. In σ_3, 7 does not appear, meaning that 7 is fixed. Thus, in total, $1 \mapsto 6 \mapsto 7$, meaning that 1 ultimately mapped to 7. This means we begin the cycle notation of $\alpha\beta$ with the symbols (17.

In cycle notation, the symbol that follows in the cycle (17 is the symbol to which 7 maps. Thus, we now repeat this process, only this time, we focus on how $\alpha\beta$ permutes the symbol 7. In σ_1, we see that $7 \mapsto 3$. Thus, as we continue reading right to left, we now must determine where 3 is sent. In σ_2, we see that 3 does not appear, meaning that 3 is fixed. In σ_3, we see that $3 \mapsto 1$. Thus, in total, $7 \mapsto 3 \mapsto 1$, meaning that 7 ultimately mapped to 1. As we began our cycle (17 with 1, we now may close the cycle. Thus, the first cycle in $\alpha\beta$ is (17). Of course, we are not necessarily finished; we must determine how $\alpha\beta$ affects the remaining numbers.

Next, we find the smallest number not in any of the previous cycles, in this case 2, and follow it through $\alpha\beta$. We see that $2 \mapsto 5$ in σ_1, and because 5 does not appear in σ_2 or σ_3, we know that $5 \mapsto 5$ ultimately. Thus, our next cycle in $\alpha\beta$ begins with (25. We now follow 5 through its mapping in $\alpha\beta$: $5 \mapsto 4 \mapsto 4 \mapsto 4$. Next, we follow 4: $4 \mapsto 1 \mapsto 2$, which is the first symbol in our cycle. Thus, we can complete this cycle as (254).

The next smallest number not in any of the previous cycles is 3. In $\alpha\beta$, $3 \mapsto 2 \mapsto 2 \mapsto 3$. Thus, 3 maps to itself, and, as customary, we omit this 1-cycle. Last, we follow 6: $6 \mapsto 7 \mapsto 6 \mapsto 6$, thus we omit 6 when writing $\alpha\beta$.

Therefore, $\alpha\beta = (17)(254)$. Similarly, $\beta\alpha = (154)(36)$. ◇

Example 3.4.24. Ⓢ Consider S_4, the set of permutation of four objects. Traditionally we work with the objects as numbers, but they do not necessarily have to be numbers. Let these four objects be ♡, ♢, ♠, ♣. Consider the permutations

$$\alpha = \begin{bmatrix} ♡ & ♢ & ♠ & ♣ \\ ♢ & ♣ & ♡ & ♠ \end{bmatrix} \text{ and } \beta = \begin{bmatrix} ♡ & ♢ & ♠ & ♣ \\ ♠ & ♢ & ♡ & ♣ \end{bmatrix}.$$

In cycle notation these elements are written $\alpha = (♡♢♣♠)$ and $\beta = (♡♠)$.

The compositions of these elements gives us the following permutations.

$$\alpha\beta = (♡♢♣♠)(♡♠) = (♡)(♢♣♠) = (♢♣♠)$$
$$\beta\alpha = (♡♠)(♡♢♣♠) = (♡♢♣)(♠) = (♡♢♣)$$

◇

One of the benefits of cycle notation is that it makes the following result easier to visualize.

Lemma 3.4.25. *Let $n \geq 2$ be a natural number, let $m \leq n$ be a natural number, and let $\sigma \in S_n$ be a disjoint m-cycle. Then $|\sigma| = m$.*

Example 3.4.26. Let $\alpha, \beta \in S_6$ be $\alpha = (12345)$ and $\beta = (123456)$. To determine the order of a permutation, we need to determine how many times the permutation must be composed with itself in order to create the identity permutation $e = (1)(2)(3)(4)(5)(6) \in S_6$. We perform these computations below:

$$\begin{aligned}
\alpha &= (12345) \\
\alpha^2 &= (12345)(12345) = (13524) \\
\alpha^3 &= \alpha^2\alpha = (13524)(12345) = (14253) \\
\alpha^4 &= \alpha^3\alpha = (14253)(12345) = (15432) \\
\alpha^5 &= \alpha^4\alpha = (15432)(12345) = e
\end{aligned}$$

and

$$\begin{aligned}
\beta &= (123456) \\
\beta^2 &= (123456)(123456) = (135)(246) \\
\beta^3 &= \beta^2\beta = (135)(246)(123456) \\
\beta^4 &= \beta^3\beta = (45)(123)(45) = (123) \\
\beta^5 &= \beta^4\beta = (123)(123)(45) = (132)(45) \\
\beta^6 &= \beta^5\beta = (132)(45)(123)(45) = e.
\end{aligned}$$

$\diamond$

The notation used in the next example will be helpful in the proof of the following theorem.

Example 3.4.27. Consider the permutation $\sigma = (176)(24) \in S_7$. Notice that σ sends 1 to 7. Thus, to emphasize the σ is a function that acts on the

set $\{1, 2, \ldots, 7\}$, we can write $\sigma(1) = 7$. To determine $\sigma^2(1)$, notice that

$$\sigma^2(1) = \sigma(\sigma(1)) = \sigma(7) = 6.$$

$\diamond$

Now that we have some basic familiarity with permutations, we study some properties of permutations. It is common to refer to a permutation as a "product" of cycles, though we know the operation is function composition.

Theorem 3.4.28. *Every permutation of a finite set can be written as a product of disjoint cycles.*

Proof. Take natural number $n \geq 2$. Let σ be a permutation on the set $D = \{1, 2, \ldots, n\}$. We will first build the cycle in σ containing $1 \in D$. Let $a_1 = 1$ be the first number in the first cycle of σ, and continue to making the following assignments

$$a_2 = \sigma(1)$$
$$a_3 = \sigma(a_2) = \sigma^2(1)$$

until $1 = \sigma^i(1)$ for some $i \leq n$. Note that a power of σ *will* eventually map 1 back to 1 because permutations are bijective functions and we are operating on finite set D. Thus, we have built the cycle

$$\sigma = (1, a_2, a_3, \ldots, a_i).$$

Let $A = \{1, a_2, a_3, \ldots, a_i\} \subseteq D$. If $D - A \neq \varnothing$, let $B = D - A$. Take the smallest natural $b_1 \in B$, and begin the process of building the cycle containing b_1.

We can continue this process of building cycles until we have included every

element of D in some cycle. Further, we know every element will be included in some cycles and we know this process will terminate because σ is a bijective function on a finite set. □

The following definition will be helpful in the proof of the following theorem.

Definition 3.4.29. Let S_1 and S_2 be sets. If $S_1 \cap S_2 = \varnothing$, then the union of S_1 and S_2 is called a disjoint union, denoted $S_1 \sqcup S_2$.

Theorem 3.4.30. *Disjoint cycles commute.*

Proof. Take natural number $n \geq 2$. Let α and β be disjoint cycles on the set $D = \{1, 2, \ldots, n\}$. We are given that α and β are disjoint, thus we can write

$$\begin{aligned} D = \{1, 2, \ldots, n\} &= A \sqcup B \sqcup C \\ &= \{a_1, \ldots, a_i, b_1, \ldots, b_j, c_1, \ldots, c_k\}, \end{aligned}$$

where $A = \{a_1, \ldots, a_i\}$ is the set of numbers appearing in α, $B = \{b_1, \ldots, b_j\}$ is the set of numbers appearing in β, and $C = \{c_1, \ldots, c_k\}$ is the set of numbers appearing in neither α nor β.

We must show that $\alpha\beta(d) = \beta\alpha(d)$ for every $d \in D$. We proceed by cases. First let $d \in A$ and assume d is the ℓ^{th} number in α. Then

$$\alpha\beta(d) = \alpha\beta(a_\ell) = \alpha(a_\ell) = a_{\ell+1}$$

because β leaves a_ℓ fixed. Further,

$$\beta\alpha(d) = \beta\alpha(a_\ell) = \beta(a_{\ell+1}) = a_{\ell+1}$$

because β leaves $a_{\ell+1}$ fixed. Hence, $\alpha\beta(d) = \beta\alpha(d)$ for every $d \in A$. Without loss of generality, $\alpha\beta(d) = \beta\alpha(d)$ for every $d \in B$.

Now let $d \in C$. Then $\alpha\beta(d) = \alpha(d) = d$ because both α and β leave d fixed. Similarly, $\beta\alpha(d) = \beta(d) = d$. Therefore, $\alpha\beta(d) = \beta\alpha(d)$ for every $d \in D$. □

Now that we know we can write permutations as products of disjoint cycles, consider the following example.

Example 3.4.31. Let $\alpha, \beta \in S_6$ be $\alpha = (123)(456)$ and $\beta = (123)(45)$. Notice that $|(123)| = 3$, $|(456)| = 3$, and $|(45)| = 2$. Further,

$$\begin{aligned}
\alpha &= (123)(456) \\
\alpha^2 &= (123)(456)(123)(456) = (132)(465) \\
\alpha^3 &= \alpha^2\alpha = (132)(465)(123)(456) = e
\end{aligned}$$

and

$$\begin{aligned}
\beta &= (123)(45) \\
\beta^2 &= (123)(45)(123)(45) = (132) \\
\beta^3 &= \beta^2\beta = (132)(123)(45) = (45) \\
\beta^4 &= \beta^3\beta = (45)(123)(45) = (123) \\
\beta^5 &= \beta^4\beta = (123)(123)(45) = (132)(45) \\
\beta^6 &= \beta^5\beta = (132)(45)(123)(45) = e.
\end{aligned}$$

◇

We generalize this example in the theorem below. In order to prove the theorem below, we first give a lemma, which is a generalization of Exercise 3.2.17. Note that the lemma is about any group element a, and therefore applies to more than just permutations.

Lemma 3.4.32. *Let G be a group with identity e, and take $a \in G$ of order m. Suppose $a^n = e$ for some $n \in \mathbb{N}$. Then m divides n.*

Proof. By the Division Algorithm, $n = qm + r$ for some $q \in Z$ and r such that $0 \leq r < m$. By way of contradiction, suppose $m \nmid n$. Thus, $0 < r < m$. We are given that $a^n = e$, thus

$$a^n = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r = e^q a^r = a^r = e.$$

This is a contradiction, because m is the the order of a yet $r < m$. Therefore, m divides n. □

This leads us to a very useful result.

Theorem 3.4.33. *The order of a permutation is the least common multiple of the lengths of its disjoint cycles.*

Proof. Let $\sigma \in S_n$ for $n \geq 2$ in $\mathbb{N}$. By Theorem 3.4.28, we can write σ as a product of disjoint cycles. By Theorem 3.4.25, each cycle has order equal to its length. Let $|\sigma| = m$. We proceed by induction on the number of disjoint cycles in σ.

For the base case, assume σ is one cycle. Then $|\sigma| = m$.

For a more illuminating base case, assume σ is a product of two disjoint cycles, say $\sigma = \alpha_1\alpha_2$. Let $\ell = \mathsf{lcm}(|\alpha_1|, |\alpha_2|)$, and note that we want to show $m = \ell$. Then, by Theorem 3.4.30 and Exercise 3.2.11,

$$\sigma^\ell = (\alpha_1\alpha_2)^\ell = \alpha_1^\ell \alpha_2^\ell.$$

Thus, by Lemma 3.4.32, $|\sigma| = m$ divides ℓ. By a similar argument, $\sigma^m = (\alpha_1\alpha_2)^m = \alpha_1^m\alpha_2^m = e$, thus $\alpha_1^m = \alpha_2^{-m}$. We are given that α_1 and α_2 are

disjoint, thus $\alpha_1^m = \alpha_2^{-m} = e$. Similarly, $\alpha_2^m = \alpha_1^{-m} = e$. Therefore, by Lemma 3.4.32, both $|\alpha_1|$ and $|\alpha_2|$ divide m. Further, $\ell = \mathsf{lcm}(|\alpha_1|, |\alpha_2|)$ must also divide m. We see that $m|\ell$ and $\ell|m$, thus $m = \ell$.

The rest of the proof is left as an Exercise. □

Surprise! There is yet another useful way to express permutations. We seldom use it in computations, as it is cumbersome. What is most useful about this notation is the fact that it exists. Below, we begin to introduce this new notation.

Definition 3.4.34. A transposition is a 2-cycle.

Example 3.4.35. The permutation (123456) can also be written as a product of transpositions. In particular, we see

$$(123456) = (16)(15)(14)(13)(12).$$

◇

Theorem 3.4.36. *Every permutation can be written as a product of transpositions.*

The proof is left to the reader, and the summary below may be helpful.

Notation. Every permutation can be written as a product of transpositions. For permutation $\sigma = (s_1, s_2, s_3, \ldots, s_{m-1}, s_m)$, we can write

$$\sigma = (s_1 s_m)(s_1 s_{m-1}) \cdots (s_1 s_3)(s_1 s_2).$$

While it may seem unwieldy to write a permutation as a product of trans-

positions, there is a major advantage: transpositions provide yet another means of "measuring" permutations. Previously, we measured a permutation by its order. Now, we can also measure a permutation by the number of its transpositions. Consider the examples below.

Example 3.4.37. The following permutations in S_5 have been written as a product of transpositions. There are many ways to express a single permutation as a product of transpositions, as demonstrated below. Notice that the transpositions are not written in numerically ascending order for the sake of demonstrating different expressions of the same permutation.

$$\begin{aligned}
(12) &= (12) \\
(123) &= (13)(12) \\
&= (312) = (32)(31) \\
&= (231) = (21)(23) \\
(1234) &= (14)(13)(12) \\
&= (4123) = (43)(42)(41) \\
&= (3412) = (32)(31)(34) \\
&= (2341) = (21)(24)(23) \\
(12345) &= (15)(14)(13)(12) \\
&= (51234) = (54)(53)(52)(51) \\
&= (45123) = (43)(42)(41)(45) \\
&= (34512) = (32)(31)(35)(34) \\
&= (23451) = (21)(25)(24)(23)
\end{aligned}$$

Notice that the 3-cycle can be written as three different products of two transpositions. Similarly, the 4-cycle can be written as four different products of three transpositions. ◇

Example 3.4.38. The identity permutation can be written as a product

of transpositions in many different ways. In S_2,

$$e = (12)(12).$$

In S_3,

$$e = (12)(12) = (13)(13) = (23)(23).$$

In S_4

$$\begin{aligned} e &= (12)(12) = (13)(13) = (14)(14) = (23)(23) = (24)(24) = (34)(34) \\ &= (12)(34)(12)(34) = (13)(24)(13)(24) = (14)(23)(14)(23) \end{aligned}$$

and there are many more ways to express e. ◇

This example is generalized below.

Lemma 3.4.39. *When written as a product of transpositions, the identity is always a product of an even number of transpositions.*

Proof. Let $e = \tau_1\tau_2\cdots\tau_m$, where each τ is a transposition. Notice that $m \neq 1$, because a single transposition can not be the identity. If $m = 2$, then we are done. We proceed by induction on m. Assume that e can be rewritten as a product of m transpositions for every even $m < k$ for some k.

Suppose $m = k$ and hence $e = \tau_1\tau_2\cdots\tau_k$. The transposition $\tau_k = (ab)$ for some $a, b \in N$ such that $a \neq b$. Now consider the product of transpositions $\tau_{k-1}\tau_k$, the two transpositions furthest right. These two transpositions have

one of the following forms, where $a, b, c, d \in \mathbb{N}$ are all distinct:

$$\begin{aligned} &(ab)(ab) = e \\ &(ac)(ab) = (abc) = (bca) = (ab)(bc) \\ &(bc)(ab) = (acb) = (cba) = (ac)(cb) \\ &(cd)(ab) = (ab)(cd). \end{aligned} \tag{3.7}$$

If Equation 3.7 is true, then we may reduce e to $e = \tau_1\tau_2\cdots\tau_{k-2}$. If this is true, then $k-2$, and hence k is even, thus we are done.

If any of the other three cases is true, we may rewrite the form of $\tau_{k-1}\tau_k$ on the left as the form on the right. This allows us to rewrite $\tau_{k-1}\tau_k$ so that a is the transposition that is second from the right.

Now consider the product of transpositions $\tau_{k-2}\tau_{k-1}$, and apply the same rewriting process. Once again, either Equation 3.7 is true, or we can shift a one transposition left. Repeating this process as needed, we will eventually shift a far enough left to obtain Equation 3.7, because the product of these transpositions is the identity. Thus, we have rewritten e as the product of $k-2$ transpositions. By hypothesis, $k-2$ is even, and hence k is even, thus we are done. □

Examples 3.4.37 and 3.4.38 are generalized below.

Theorem 3.4.40. *If a permutation can be expressed as a product of an odd number of transpositions, then every transposition decomposition of the permutation contains an odd number of transpositions. Similarly, if a permutation can be expressed as a product of an even number of transpositions, then every transposition decomposition of the permutation contains an even number of transpositions.*

Proof. Take $\sigma \in S_n$ and rewrite it as two different transposition decomposi-

tions:

$$\alpha_1\alpha_2\cdots\alpha_i = \beta_1\beta_2\cdots\beta_j.$$

Then

$$\begin{aligned} e &= \alpha_1\alpha_2\cdots\alpha_i(\beta_1)^{-1}(\beta_2)^{-1}\cdots(\beta_j)^{-1} \\ &= \alpha_1\alpha_2\cdots\alpha_i\beta_1\beta_2\cdots\beta_j \end{aligned}$$

because a transposition is its own inverse. By Lemma 3.4.39, $i + j$ is even. Thus, i and j are either both even or both odd. □

This leads to the following descriptors of permutations.

Definition 3.4.41. A permutation is odd if it can be decomposed into an odd number of transpositions. A permutation is even if it can be decomposed into an even number of transpositions.

Example 3.4.42. In each of the following cycles, notice the relationship between number of distinct numbers and the number of transpositions.

- The permutation (12) is odd. It has two distinct numbers in its cycle, but it has one transposition.
- The permutation (123) = (13)(12) is even. It has three distinct numbers in its cycle, but it has two transpositions.
- The permutation (1234) = (14)(13)(12) is odd.
- The permutation (12345) = (15)(14)(13)(12) is even.

◇

This leads us to a rich bank of examples of subgroups.

Definition 3.4.43. The set of even permutations of n objects, denoted A_n, is the alternating group of degree n.

Theorem 3.4.44. *For natural number $n \geq 2$, A_n is a subgroup of S_n.*

Example 3.4.45. We will determine A_3. We know

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

The identity is even, thus $e \in A_3$. The cycles (12), (13), and (23) are single transpositions, thus, $(12), (13), (23) \notin A_3$. The 3-cycles (123) and (132) can each be decomposed into two transpositions, thus $(123), (132) \in A_3$. In conclusion,

$$A_3 = \{e, (123), (132)\}.$$

$\diamond$

The proof of Theorem 3.4.44 and the proof of the theorem below are left to the reader.

Theorem 3.4.46. *For natural number $n \geq 2$, $|S_n| = n!$ and $|A_n| = n!/2$.*

EXERCISES

Exercise 3.4.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let σ be a permutation in S_n.

a. $(12) \in S_n$

b. $(13) \in S_n$

c. If $|\sigma| = 5$, then σ is a 5-cycle.

d. If $|\sigma| = 6$, then σ is a 6-cycle.

e. If $|\sigma| = 5$, then $\sigma \in A_n$.

f. If $|\sigma| = 6$, then $\sigma \in A_n$.

g. The set of odd permutations in S_n is a subgroup of S_n.

Exercise 3.4.2. Review definitions 3.4.1 and 3.4.6. For each of the following, choose $m, n \in \mathbb{Z}$ to create a function $f : \mathbb{Z}_m \to \mathbb{Z}_n$, and specify how the function the f maps the elements in $\mathbb{Z}_m$, to satisfy the given condition.

a. f is one-to-one but not onto,

b. f is onto but not one-to-one,

c. f is both one-to-one and onto,

d. f is neither one-to-one nor onto.

Exercise 3.4.3. Consider D_3 and S_3.

a. Represent each element of D_3 as a permutation written in matrix notation.

b. Represent each element of D_3 as a permutation written in cycle notation.

c. Which elements of S_3 do not represent any elements in D_3?

Exercise 3.4.4. Consider D_4 and S_4.

a. Represent each element of D_4 as a permutation written in matrix notation.

b. Represent each element of D_4 as a permutation written in cycle notation.

c. Which elements of S_4 do not represent any elements in D_4?

Exercise 3.4.5. Let $\alpha, \beta, \gamma \in S_8$ be given as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 5 & 1 & 8 & 7 & 2 & 3 \end{bmatrix},$$
$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 6 & 7 & 8 & 5 \end{bmatrix},$$
$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 8 & 1 & 7 & 3 & 4 & 6 \end{bmatrix}.$$

a. Write $\alpha, \beta, \gamma \in S_8$ in cycle notation.

b. Find $\alpha\beta$, $\beta\alpha$, $\alpha\gamma$, $\gamma\beta$, and γ^2.

c. Find the orders of $\alpha, \beta, \gamma \in S_8$.

d. Find $\alpha^{-1}, \beta^{-1}, \gamma^{-1} \in S_8$

Exercise 3.4.6. Show that a function on a finite set is one-to-one if and only if it is onto.

Exercise 3.4.7. Write $(193)(2734)(15)(38) \in S_9$ in matrix notation.

Exercise 3.4.8. Find the order of each of the following permutations

a. (62715)

b. (62)(715)

c. (62)(715)(125)

Exercise 3.4.9. Prove Lemma 3.4.25.

Exercise 3.4.10. For each of the following, find the inverse of the permutation. For each inverse, begin the cycle with the number 1. What pattern do you notice?

a. (123)

b. (1234)

c. (12345)

d. (123456)

Exercise 3.4.11. Finish the proof of Theorem 3.4.33.

Exercise 3.4.12. Find all the possible orders of elements in S_7. *(Hint: Do not find all elements in S_7.)*

Exercise 3.4.13. Suppose $\sigma = (1624)(15263)$. Find σ^{100}.

Exercise 3.4.14. Take $\sigma = (1, 2, 3, 4, 5)(6, 7)(8, 9, 10) \in S_{10}$ and suppose σ^k is a 5-cycle. What can you conclude about k?

Exercise 3.4.15. Let $H = \{\alpha \in S_5 \,|\, \alpha(1) = 1 \text{ and } \alpha(5) = 5\}$. Prove that H is a subgroup of S_5. Find $|H|$.

Exercise 3.4.16. Show that in S_4, the equation $x^2 = (1234)$ has no solutions and the equation $x^3 = (1234)$ has a solution.

Exercise 3.4.17. For each of the following permutations in S_5, find two different ways to express the permutation as a product of transpositions.

a. (13542)

b. (142)(35)

c. (2453)

Exercise 3.4.18. Prove Theorem 3.4.36.

Exercise 3.4.19. What is the maximum order of an element in A_{10}? Justify your answer. *(Hint: Do not find all elements in A_{10}.)*

Exercise 3.4.20. Find all of the permutations in S_4 that commute with (12)(34). Does this subset form a subgroup?

Exercise 3.4.21. Given $\sigma \in S_n$, prove that σ and σ^{-1} have the same parity.

Exercise 3.4.22. Let α and β be transpositions. What are the possibilities for $|\alpha\beta|$? Justify your answer.

Exercise 3.4.23. Suppose $\sigma \in S_n$ and $\sigma^4 = (1234567)$.

a. Find σ if $n = 7$.

b. Find σ if $n = 9$.

Exercise 3.4.24. Prove Theorem 3.4.44.

Exercise 3.4.25. Prove Theorem 3.4.46.

Exercise 3.4.26. Prove that S_n is non-Abelian for all $n \geq 3$. Prove that A_n is non-Abelian for all $n \geq 4$.

3.5 Some Important Subgroups

After studying examples of groups, we studied properties common to all groups. In order to apply our our ideas to all groups, we adopted the generic group notation. Similarily, now that we have studied subgroups, we turn to subgroups common to all groups, and we do so using the generic group notation.

As we have noticed in previous homework problems, even in non-Abelian groups, there can be elements that commute with all elements. For example, if e is the identity of group G and $g \in G$, $eg = ge$, thus we see that the identity is an element that commutes with all elements in its group. We take this idea further in the definition below.

Definition 3.5.1. Let G be a group. The center of group G, denoted $Z(G)$, is the subgroup of all elements that commute with all elements, that is,

$$Z(G) = \{g \in G \mid gx = xg \ \forall \, x \in G\}.$$

Example 3.5.2. The center of D_4 is the subgroup of all elements that commute with all of the elements in D_4. Consulting the Cayley table of D_4, we see that

$$Z(D_4) = \{R_0, R_{180}\}.$$

$\diamond$

Example 3.5.3. Let G be an Abelian group, thus every element commutes with every element. In this case, $Z(G) = G$. $\diamond$

Below, we prove that the center is a subgroup. For variety, we employ the Two-Step Subgroup Test. Recall that to prove a subset is a subgroup, we may prove the subset meets the subgroup definition or use either of the subgroup tests.

Theorem 3.5.4. *The center of group G is a subgroup of G.*

Proof. Let G be a group and e its identity. By the definition of $Z(G)$, $Z(G)$ is a subset of G. By definition of the identity, e is in $Z(G)$, thus $Z(G)$ is nonempty. We may now apply the Two-Step Subgroup Test. Consider $a, b \in Z(G)$.

1. By the definition of $Z(G)$, $ax = xa$ and $bx = xb$ for all $x \in G$. Then, using these properties and associativity, we see that

   $$(ab)x = a(bx) = a(xb) = (ax)b = x(ab)$$

   for all $x \in G$. Thus, $ab \in Z(G)$.

2. By the definition of $Z(G)$, $ax = xa$. By the definition of a group, we

know that a^{-1} exists. Multiplying on the left by a^{-1}, we see that

$$\begin{aligned} a^{-1}(ax) &= a^{-1}(xa) \\ x &= a^{-1}(xa) \end{aligned}$$

by associativity and the definitions of inverse and identity. Multiplying on the right by a^{-1}, we see that

$$\begin{aligned} x &= a^{-1}(xa) \\ xa^{-1} &= a^{-1}(xa)a^{-1} \\ &= a^{-1}x. \end{aligned}$$

This is true for all $x \in G$, thus $a^{-1} \in Z(G)$.

Therefore, by the Two-Step Subgroup Test, $Z(G)$ is a subgroup of G. □

The center of a group is every element that commutes with every element. Compare this to the definition below.

Definition 3.5.5. Let G be a group and take $a \in G$. The centralizer of a in G, denoted $C_G(a)$, is the set of elements in G that commute with a. That is,

$$C_G(a) = \{x \in G \mid ax = xa\}.$$

Notice that we need two pieces of information in order to define the centralizer. First, we need a parent group, G. Second, we need the element, $a \in G$, whose ability to commute we shall analyze. If the parent group is clear, you guessed it, we get lazy and just write $C(a)$.

Example 3.5.6. Consider D_4. The centralizers of each element are listed below.

$$\begin{aligned} C(R_0) &= D_4 = C(R_{180}) \\ C(R_{90}) &= \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270}) \\ C(H) &= \{R_0, R_{180}, H, V\} = C(V) \\ C(D) &= \{R_0, R_{180}, D, D'\} = C(D') \end{aligned}$$

$\diamond$

Theorem 3.5.7. *Let G be a group and take $a \in G$. Then $C_G(a)$ is a subgroup of G.*

The proof of Theorem 3.5.7 is left to the reader as an exercise.

Theorem 3.5.8. *Let H be a subgroup of group G. Then the centralizer of H*

$$C_G(H) = \{g \in G \,|\, gh = hg \,\forall\, h \in H\}$$

is a subgroup of G.

Again, the proof is left to the reader because it is yet another fantastic opportunity to practice using the subgroup tests. Below is an example of the centralizer of a subgroup.

Example 3.5.9. Consider the subgroup $H = \{e, (13)\}$ of the groups S_3, S_4, and S_5. Below we find the centralizers of H in each of these parent groups.

When $G = S_3$,

$$\begin{aligned} C_G(H) &= \{g \in S_3 \,|\, gh = hg \,\forall\, h \in H\} \\ &= \{e, (13)\}. \end{aligned}$$

When $G = S_4$,

$$\begin{aligned} C_G(H) &= \{g \in S_4 \,|\, gh = hg \,\forall\, h \in H\} \\ &= \{e, (13), (24), (13)(24)\}. \end{aligned}$$

When $G = S_5$,

$$\begin{aligned} C_G(H) &= \{g \in S_5 \,|\, gh = hg \,\forall\, h \in H\} \\ &= \{e, (13), (24), (25), (45), (245), (254), (13)(24), (13)(25), (13)(45)\}. \end{aligned}$$

$\diamond$

Definition 3.5.10. Let G be a group and H a subgroup of G. Take $x \in G$. Then

$$xHx^{-1} = \{xhx^{-1} \,|\, h \in H\}$$

is called the conjugate of H by x in G.

Example 3.5.11. Let $G = S_3$ and $H = \{e, (12)\}$. Take $(123) \in G$. Then

$$\begin{aligned} (123)H(123)^{-1} &= \{(123)e(123)^{-1}, (123)(12)(123)^{-1}\} \\ &= \{(123)e(132), (123)(12)(132)\} \\ &= \{e, (23)\} \end{aligned}$$

is also a subgroup of G. $\diamond$

Theorem 3.5.12. *Let G be a group and H a subgroup of G. Then for every $x \in G$, xHx^{-1} is a subgroup of G.*

Proof. Let $x \in G$. We are given that H is a subgroup, thus $e \in H$. Further,

$xex^{-1} = e \in xHx^{-1}$, thus xHx^{-1} is nonempty. We proceed using the One-Step Subgroup Test. The elements $a, b \in xHx^{-1}$ have form $a = xcx^{-1}$ and $b = xdx^{-1}$ for some $c, d \in H$. Then, using the Socks and Shoes property, we see that

$$\begin{aligned} ab^{-1} &= xcx^{-1}(xdx^{-1})^{-1} \\ &= xcx^{-1}(x^{-1})^{-1}(d)^{-1}(x)^{-1} \\ &= xcx^{-1}xd^{-1}x^{-1} \\ &= xcd^{-1}x^{-1}. \end{aligned}$$

Further, because H is a subgroup, $cd^{-1} \in H$. Therefore, $ab^{-1} \in xHx^{-1}$, and xHx^{-1} is a subgroup of G. □

As we saw in Example 3.5.11, a conjugate of a subgroup is not always equal to the original subgroup. Many nice properties arise when a conjugate and its original subgroup are equal, as we will see in Chapter 5. For now, we study a subgroup arising from this property; the proof that it is indeed a subgroup is left to the reader.

Definition 3.5.13. Let H be a subgroup of group G. Then the normalizer of H in G is the set

$$N(H) = \{x \in G \,|\, xHx^{-1} = H\}$$

Example 3.5.14. Let $G = S_5$ and $H = \{e, (123), (132)\}$. Then

$$\begin{aligned} N(H) &= \{\sigma \in G \,|\, \sigma H \sigma^{-1} = H\} \\ &= \{\sigma \in G \,|\, \sigma e \sigma^{-1} \in H,\, \sigma(123)\sigma^{-1} \in H,\, \sigma(132)\sigma^{-1} \in H\} \\ &= \{e, (123), (132), (45), (123)(45), (132)(45)\}. \end{aligned}$$

◇

Theorem 3.5.15. *Let H be subgroup of group G. Then $N(H)$ is a subgroup of G.*

Example 3.5.16. Ⓢ Let $G = D_3$ and $H = \{R_0, R_{120}, R_{240}\}$. We will first itemize the conjugates for each element in $H < D_3$. Then we will determine the normalizer of the subgroup H. The following table gives the conjugates in H for each $x \in G$.

$x \in G$	xR_0x^{-1}	$xR_{120}x^{-1}$	$xR_{240}x^{-1}$	xHx^{-1}
R_0	R_0	R_{120}	R_{240}	$\{R_0, R_{120}, R_{240}\} = H$
R_{120}	R_0	R_{120}	R_{240}	$\{R_0, R_{120}, R_{240}\} = H$
R_{240}	R_0	R_{120}	R_{240}	$\{R_0, R_{120}, R_{240}\} = H$
V	R_0	R_{240}	R_{120}	$\{R_0, R_{120}, R_{240}\} = H$
L	R_0	R_{240}	R_{120}	$\{R_0, R_{120}, R_{240}\} = H$
R	R_0	R_{240}	R_{120}	$\{R_0, R_{120}, R_{240}\} = H$

Since we have $xHx^{-1} = H$ for all $x \in G$, we have that $N(H) = G$. ◇

Recall from Section 3.4 that permutations are functions that act on the elements $D_n = \{1, 2, \ldots, n\}$. Whenever we have a group of functions acting on objects, like permutations acting on numbers, or movements acting on shapes, we can create subgroups based on how the functions behave.

Definition 3.5.17. Let G be a group of permutations on the set D. Take $d \in D$. Then the stabilizer of d in G is

$$\mathsf{stab}_G(d) = \{\sigma \in G \,|\, \sigma(d) = d\},$$

which is the set of all permutations that leave d fixed.

Example 3.5.18. Ⓢ Find $\mathsf{stab}_G(3)$ where $G = S_4$. By definition, $\mathsf{stab}_G(3)$ has all the elements in S_4 where $3 \mapsto 3$. We can see that

$$\mathsf{stab}_G(3) = \{e, (12), (14), (24), (124), (142)\}.$$

Due to laziness we usually do not write cycles of order 1 like (3), which is why the digit 3 does not appear in the any of the permutations of $\mathsf{stab}_G(3)$. $\diamond$

In the above definition, notice that our only restriction on G is that it is a permutation group, and not any particular permutation group.

Theorem 3.5.19. *Let G be a group of permutations on the set D and take $d \in D$. Then $\mathsf{stab}_G(d)$ is a subgroup of G.*

The proof is left to the reader as an exercise.

EXERCISES

Exercise 3.5.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let G be a group and $H \leq G$.

- **a.** A group has an Abelian subgroup.
- **b.** $Z(G) \neq \varnothing$
- **c.** For $a \in G$, $C(a) \neq \varnothing$.
- **d.** For $a \in G$, $C(a) = C(a^{-1})$.
- **e.** For $a \in G$, $C(a)$ is Abelian.
- **f.** For $a \in G$, $Z(G) \subseteq C(a)$.
- **g.** For $x \in G$, $xHx^{-1} = H$.

Exercise 3.5.2. Find $Z(S_4)$. Find $Z(A_4)$.

Exercise 3.5.3. Find $Z(D_n)$ for $n = 3, 4, 5, 6$.

Exercise 3.5.4. Let H be a subgroup of group G. Define $HZ(G)$ as

$$HZ(G) = \{hz \,|\, h \in H,\, z \in Z(G)\}.$$

a. Pick your favorite non-Abelian group and your favorite nontrivial subgroup of it. Create an example of $HZ(G)$.

b. Prove $HZ(G)$ is a subgroup of G.

c. Is it necessary for H to be a subgroup of G in order for $HZ(G)$ to be a subgroup? Why or why not?

Exercise 3.5.5. Find all of the centralizers in S_4.

Exercise 3.5.6. Ⓢ Find $N(SL_2(\mathbb{Z}_2))$ where $G = GL_2(\mathbb{Z}_2))$.

Exercise 3.5.7. Consider the permutation $\sigma = (12)(34)(56)$. For each of the following G, find $C_G(\sigma)$.

a. $G = S_6$

b. $G = S_7$

Exercise 3.5.8. Prove Theorem 3.5.7.

Exercise 3.5.9. Let G be a group and $a, b \in G$. Prove that if $b \in C_G(a)$, then $a \in C_G(b)$.

Exercise 3.5.10. Let G be a group. Prove that $Z(G)$ is a subgroup of $C_G(a)$ for all $a \in G$.

Exercise 3.5.11. Let G be a group. Prove that

$$Z(G) = \bigcap_{a \in G} C_G(a).$$

Exercise 3.5.12. Prove Theorem 3.5.8.

Exercise 3.5.13. Let $G = S_n$ and $H = \{e, (12), (34), (12)(34)\}$.

a. Find $N(H)$ if $n = 4$.

b. Find $N(H)$ if $n = 6$.

c. Find $N(H)$ if $n = 7$.

Exercise 3.5.14. Prove Theorem 3.5.15.

Exercise 3.5.15. Ⓢ Let G be a group and H be a subgroup of G with $H \subseteq Z(G)$. Prove that $N(H) = G$.

Exercise 3.5.16. Let $G = S_4$. Find $\mathsf{stab}_G(i)$ for each $i = 1, 2, 3, 4$.

Exercise 3.5.17. Let $G = A_5$. Find $\mathsf{stab}_G(i)$ for each $i = 1, 2, 3, 4, 5$.

Exercise 3.5.18. Prove Theorem 3.5.19.

3.6 Cyclic Groups and Subgroups

Definition 3.6.1. Let a be an element of the group G. Define

$$\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}.$$

We call $\langle a \rangle$ the cyclic subgroup of G generated by a.

In a sense, the subgroup generated by element $a \in G$ is the set of everything a creates with itself, and we will prove it is indeed a subgroup of G.

Example 3.6.2. Consider $2 \in \mathbb{R}^*$. The group operation is multiplication,

thus

$$\begin{aligned}\langle 2\rangle &= \{2^i \mid i \in \mathbb{Z}\} \\ &= \{\ldots, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, \ldots\} \\ &= \left\{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \ldots\right\}\end{aligned}$$

is a subgroup of $\mathbb{R}$. Notice that $1 \in \mathbb{R}^*$, and for $2^n \in \mathbb{R}^*$, we will find $2^{-n} \in \mathbb{R}^*$. ◇

Example 3.6.3. Consider $2 \in \mathbb{Z}_{12}$. The group operation is addition, thus

$$\langle 2\rangle = \{2, 4, 6, 8, 10, 0\}.$$

Notice that these are all the elements of $\langle 2\rangle$. For example, if we wanted to find 2^{17}, we would sum 17 copies of 2, which creates $2^{17} = 34 = 10$. Thus, though the definition of $\langle 2\rangle$ includes infinite powers of 2, because we are in a finite group, the elements created begin to repeat. ◇

Example 3.6.4. Let G be a group and e its identity. Then $\langle e\rangle = \{e\}$. ◇

Below we prove that a cyclic subgroup is indeed a subgroup, and we go one step further.

Theorem 3.6.5. *For each $a \in G$, $\langle a\rangle$ is a subgroup of G. Furthermore, $\langle a\rangle$ is the smallest subgroup of G that contains a.*

Proof. First, we see that $a \in \langle a\rangle$, thus $\langle a\rangle$ is nonempty and we may apply the One-Step Subgroup Test. Let $x, y \in \langle a\rangle$. Then, by the definition of $\langle a\rangle$, these elements have the form $x = a^m$ and $y = a^n$ for some $m, n \in \mathbb{Z}$. Furthermore,

$$xy^{-1} = a^m(a^n)^{-1} = a^m a^{-n} = a^{m-n}.$$

By the definition of $\langle a \rangle$, $a^{m-n} \in \langle a \rangle$ because $m - n \in \mathbb{Z}$. Therefore, by the One-Step Subgroup Test, $\langle a \rangle \leq G$.

Suppose H is another subgroup of G that contains a. By the definition of subgroup, H is closed, thus $a^n \in H$ for all $n \in \mathbb{Z}$. Thus, $\langle a \rangle \subseteq H$, which implies that $\langle a \rangle$ is the smallest subgroup of G that contains a. □

Example 3.6.6. Ⓢ Consider $\langle 2 \rangle$. We will find $|\langle 2 \rangle|$ for $U(3), U(7), U(9), U(21)$, and $U(63)$. Note for unit groups, 1 is the identity under multiplication.

- We calculate the powers of 2 in $U(3)$, obtaining the following.

$$2^2 = 4 \bmod 3 = 1$$

  Hence, $\langle 2 \rangle = \{1, 2\} \leq U(3)$.

- The powers of 2 in $U(7)$ follow.

$$2^2 = 4 \bmod 7 = 4$$
$$2^3 = 8 \bmod 7 = 1$$

  Hence, $\langle 2 \rangle = \{1, 2, 4\} \leq U(7)$.

- The powers of 2 in $U(9)$ follow,

$$2^2 = 4 \bmod 9 = 4$$
$$2^3 = 8 \bmod 9 = 8$$
$$2^4 = 16 \bmod 9 = 7$$
$$2^5 = 32 \bmod 9 = 5$$
$$2^6 = 64 \bmod 9 = 1$$

  Hence, $\langle 2 \rangle = \{1, 2, 4, 5, 7, 8\} \leq U(9)$.

- The powers of 2 in $U(21)$ follow.

$$2^2 = 4 \bmod 21 = 4$$
$$2^3 = 8 \bmod 21 = 8$$
$$2^4 = 16 \bmod 21 = 16$$
$$2^5 = 32 \bmod 21 = 11$$
$$2^6 = 64 \bmod 21 = 1$$

  Hence, $\langle 2 \rangle = \{1, 2, 4, 8, 11, 16\} \leq U(21)$.

- The powers of 2 in $U(63)$ follow.

$$2^2 = 4 \bmod 63 = 4$$
$$2^3 = 8 \bmod 63 = 8$$
$$2^4 = 16 \bmod 63 = 16$$
$$2^5 = 32 \bmod 63 = 32$$
$$2^6 = 64 \bmod 63 = 1$$

  Hence, $\langle 2 \rangle = \{1, 2, 4, 8, 16, 32\} \leq U(7)$.

$\diamond$

Groups themselves can be cyclic.

Definition 3.6.7. A group G is cyclic if there exists $a \in G$ such that $G = \langle a \rangle$, and the element a is called a generator of G.

We have already seen many example of cyclic groups, both finite and infinite.

Example 3.6.8. The group $\mathbb{Z}_8$ is cyclic and has generators 1, 3, 5, and 7. Notice

$$\begin{aligned}\langle 1\rangle &= \{1,2,3,4,5,6,7,0\}\\ \langle 3\rangle &= \{3,6,1,4,7,2,5,0\}\\ \langle 5\rangle &= \{5,2,7,4,1,6,3,0\}\\ \langle 7\rangle &= \{7,6,5,4,3,2,1,0\}.\end{aligned}$$

Of course, order doesn't matter in a set, thus $\langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \mathbb{Z}_8$. ◇

Example 3.6.9. The group $U(10) = \{1,3,7,9\}$ is cyclic with generators 3 and 7. ◇

Non-Example 3.6.10. The group $U(8) = \{1,3,5,7\}$ is not cyclic. Notice that no element generates all of $U(10)$.

$$\begin{aligned}\langle 1\rangle &= \{1\}\\ \langle 3\rangle &= \{3,1\}\\ \langle 5\rangle &= \{5,1\}\\ \langle 7\rangle &= \{7,1\}\end{aligned}$$

◇

Example 3.6.11. The group of the integers under addition is cyclic. The elements 1 and -1 generate the integers, that is,

$$\mathbb{Z} = \langle 1\rangle = \langle -1\rangle = \{\ldots,-2,-1,0,1,2,\ldots\}.$$

◇

Non-Example 3.6.12. The group of the real numbers under addition is not cyclic. There is no $a \in \mathbb{R}$ that, when added to itself as many as infinitely

times, will create every real number. ◇

In a cyclic group, there may be some elements that do not generate the entire group. For example, as long as the group is nontrivial, the identity will not generate the entire group. Notice that in a non-cyclic group, none of the elements generate the entire group.

Cyclic groups are so named because, in a sense, they are cycles of elements. The lemma below gives us a tool to measure when two seemingly different elements are really the same element in a cycle.

Lemma 3.6.13. *Let G be a group with identity e, take $a \in G$, and let $i, j \in \mathbb{N}$.*

- *If $|a|$ is infinite, then $a^i = a^j$ if and only if $i = j$.*
- *If $|a| = n$, then $a^i = a^j$ if and only if $i \equiv j \bmod n$. Further, $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.*

Proof. First, assume $|a|$ is infinite. Then the only power of a that generates the identity is zero, that is, $a^0 = e$. If $a^i = a^j$, then $a^{i-j} = e$. Thus, $i - j = 0$ and $i = j$.

Second, assume $|a| = n$ for some $n \in \mathbb{N}$. Let $a^k \in \langle a \rangle$ for some $k \in \mathbb{Z}$. By the Division Algorithm, we know that $k = qn + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < n$. Thus,

$$a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = ea^r = a^r.$$

Therefore, for every $k \in \mathbb{Z}$

$$a^k \in \{a^r \,|\, 0 \leq r < n\} = \{a^0, a^1, a^2, \ldots, a^{n-1}\} = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Suppose $a^i = a^j$ for some $i, j \in \mathbb{N}$. Then $a^{i-j} = e = a^0$. By the Division Algorithm, we know that $i-j = qn+r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < n$. Hence, $e = a^{i-j} = a^r$. We assumed $|a| = n$, and the Division Algorithm gave us $0 \leq r < n$, thus $r = 0$. Therefore, $i - j = qn$, or $i \equiv j \bmod n$. □

Previously, you may have found it strange that we used the term "order" in two different ways.

1. The order of an element is the number of copies needed to create the identity,
2. The order of a group is the number of elements in the group.

The corollary below provides the link between the two meanings.

Corollary 3.6.14. *For any group element a, $|a| = |\langle a \rangle|$.*

Corollary 3.6.15. *Suppose a group has identity e and let a be an element with order n. If $a^k = e$, then n divides k.*

We have already seen many examples of these corollaries, though we did not study them in this light. Below is another example.

Example 3.6.16. Consider the element $(12345) \in S_5$. We know that $|(12345)| = 5$. Thus, if we also know that $(12345)^k = e$, we may conclude that k is a multiple of 5. ◇

There are many examples we could create to demonstrate properties of cyclic groups. As we began to see in Example 3.6.8, for $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a cyclic group. Similarly, as we saw in Example 3.6.11, $\mathbb{Z}$ is a cyclic group. Thus, we will often demonstrate properties of cyclic groups with $\mathbb{Z}_n$ and $\mathbb{Z}$, because, if nothing else, these groups are fairly familiar already.

There are many, many patterns to observe about cyclic groups. Read the example below, and conjecture about when two distinct group elements create the same cyclic group.

Example 3.6.17. Consider the group $\mathbb{Z}_{12}$. We know that 1 is a generator. Are there any other generators?

The element 1 generates every element in $\mathbb{Z}_{12}$. Thus, we can view every element as a power of 1. For example, $2 = 1^2$ because $2 = 1 + 1$. Similarly, $3 = 1^3$, $4 = 1^4$, and so on. Let's observe what each element generates.

$$\begin{aligned}
\langle 1^0 \rangle &= \langle 0 \rangle = \{0\} \\
\langle 1^1 \rangle &= \langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0\} = \mathbb{Z}_{12} \\
\langle 1^2 \rangle &= \langle 2 \rangle = \{2, 4, 6, 8, 10, 0\} \\
\langle 1^3 \rangle &= \langle 3 \rangle = \{3, 6, 9, 0\} \\
\langle 1^4 \rangle &= \langle 4 \rangle = \{4, 8, 0\} \\
\langle 1^5 \rangle &= \langle 5 \rangle = \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\} = \mathbb{Z}_{12} \\
\langle 1^6 \rangle &= \langle 6 \rangle = \{6, 0\} \\
\langle 1^7 \rangle &= \langle 7 \rangle = \{7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5, 0\} = \mathbb{Z}_{12} \\
\langle 1^8 \rangle &= \langle 8 \rangle = \{8, 4, 0\} = \langle 4 \rangle \\
\langle 1^9 \rangle &= \langle 9 \rangle = \{9, 6, 3, 0\} = \langle 3 \rangle \\
\langle 1^{10} \rangle &= \langle 10 \rangle = \{10, 8, 6, 4, 2, 0\} = \langle 2 \rangle \\
\langle 1^{11} \rangle &= \langle 11 \rangle = \{11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1, 0\} = \mathbb{Z}_{12}
\end{aligned}$$

We see that

$$\langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle$$
$$\langle 2\rangle = \langle 10\rangle$$
$$\langle 3\rangle = \langle 9\rangle$$
$$\langle 4\rangle = \langle 8\rangle$$

How do 1, 5, 7, and 11 relate to 12? How do 2 and 10 relate to 12? How do 3 and 9 relate to 12? How do 4 and 8 relate to 12? The answers to these questions can help us predict when two elements create the same cyclic subgroups, and, in the case of cyclic groups, which elements are generators. ◇

The previous example is generalized in the theorem below.

Theorem 3.6.18. *Let a be an element of order n and let $k \in \mathbb{N}$. Then*

$$\langle a^k\rangle = \langle a^{\gcd(n,k)}\rangle$$

and

$$|a^k| = \frac{n}{\gcd(n,k)}.$$

Proof. To make the calculations less cumbersome, it is common to call a greatest common divisor d. Thus, let $d = \gcd(n,k)$. Thus, d is a divisor of k, hence $\langle a^k\rangle \subseteq \langle a^d\rangle$. By Bézout's Lemma, there exist $x, y \in \mathbb{Z}$ such that $d = nx + ky$. Therefore,

$$a^d = a^{nx+ky} = (a^n)^x(a^k)^y = (a^k)^y \in \langle a^k\rangle$$

by the definition of $\langle a^k\rangle$. By closure, $\langle a^d\rangle \subseteq \langle a^k\rangle$. Ergo, $\langle a^d\rangle = \langle a^k\rangle$.

Now let d be any divisor of n. We are given that $|a| = n$, thus $(a^d)^{n/d} = e$,

which shows that $|a^d|$ divides n/d. If $i \in \mathbb{N}$ is less than n/d, then $i \cdot d < i \cdot n/d$ and because

$$(a^d)^{n/d} = a^n = e,$$

we know that $(a^d)^i \neq e$. Therefore, no such i exists, meaning that $|a^d|$ can not be smaller than n/d. Therefore, $|a^d| = n/d$. When $d = \gcd(n, k)$,

$$|a^k| = |\langle a^k \rangle| = |\langle a^{\gcd(n,k)} \rangle| = \frac{n}{\gcd(n, k)}.$$

□

This theorem tells us when two cyclic subgroups are equal. Thus, when considering $\langle a^k \rangle$, we can instead consider $\langle a^{\gcd(n,k)} \rangle$. This may yield a much more convenient calculation, as $\gcd(n, k) \leq k$.

Example 3.6.19. To find $\langle 27 \rangle$ in $\mathbb{Z}_{48}$, we could start adding copies of 27 to itself, but only the rare math student thinks that sounds like fun. Instead, we use Theorem 3.6.18 to reduce our workload.

We know that 1 generates $\mathbb{Z}_{48}$ and $|1| = 48$. Thus, 27 is generated by 1. We see that $27 = 1^{27}$, so $\langle 27 \rangle = \langle 1^{27} \rangle$. By Theorem 3.6.18, $\langle 1^{27} \rangle = \langle 1^{\gcd(|1|,27)} \rangle$ and notice that

$$\gcd(|1|, 27) = \gcd(48, 27) = 3.$$

Therefore,

$$\begin{aligned} \langle 27 \rangle &= \langle 1^{27} \rangle \\ &= \langle 1^{\gcd(48,27)} \rangle = \langle 1^3 \rangle = \langle 3 \rangle \\ &= \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 0\}. \end{aligned}$$

We could use Theorem 3.6.18 once again to also conclude that

$$|27| = |1^{27}| = \frac{|1|}{\gcd(|1|, 27)} = \frac{48}{\gcd(48, 27)} = \frac{48}{3} = 16.$$

Of course, notice that $|\langle 27 \rangle| = 16$. ◇

Theorem 3.6.18 provides a powerful tool when working with cyclic groups.

Corollary 3.6.20. *In a finite cyclic group, the order of an element divides the order of the group.*

The following corollaries help us determine when two cyclic groups are equal.

Corollary 3.6.21. *Let a be an element of order n. Let $i, j \in \mathbb{N}$. The following are equivalent.*

1. $\langle a^i \rangle = \langle a^j \rangle$
2. $\gcd(n, i) = \gcd(n, j)$
3. $|a^i| = |a^j|$

Proof. To show that these statements are equivalent, we will show that (1) implies (2), (2) implies (3), and (3) implies (1).

For the first implication we must show, assume $\langle a^i \rangle = \langle a^j \rangle$. By Corollary 3.6.14, $|a^i| = |\langle a^i \rangle| = |\langle a^j \rangle| = |a^j|$. By Theorem 3.6.18,

$$|a^i| = \frac{n}{\gcd(n, i)} = \frac{n}{\gcd(n, j)} = |a^j|.$$

Therefore, $\gcd(n, i) = \gcd(n, j)$.

For the second implication we must show, assume $\gcd(n,i) = \gcd(n,j)$. By Theorem 3.6.18,

$$|a^i| = \frac{n}{\gcd(n,i)} \text{ and } |a^j| = \frac{n}{\gcd(n,j)}.$$

We are assuming $\gcd(n,i) = \gcd(n,j)$, thus $|a^i| = |a^j|$.

For the third implication we must show, assume $|a^i| = |a^j|$. By Theorem 3.6.18,

$$|a^i| = \frac{n}{\gcd(n,i)} = |a^j| = \frac{n}{\gcd(n,j)},$$

hence $\gcd(n,i) = \gcd(n,j)$. Using Theorem 3.6.18 again, we see that

$$\langle a^i \rangle = \langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle = \langle a^j \rangle.$$

□

Corollary 3.6.22. *Let a be an element of order n and take $i \in \mathbb{N}$. Then $\langle a \rangle = \langle a^i \rangle$ if and only if $\gcd(n,i) = 1$.*

A special case of Corollary 3.6.22 is when a is a generator of a group, that is $G = \langle a \rangle$. In this case, $|G| = n$. Corollary 3.6.22 tells us that $\langle a \rangle = G = \langle a^i \rangle$ if and only if $\gcd(n,i)$. Thus, to find other generators of G, we need to find elements a^i whose orders are relatively prime to the order of the group.

Example 3.6.23. Consider the group $U(18) = \{1,5,7,11,13,17\}$ which is cyclic because it can be generated by 5. Notice that $|U(18)| = |5| = 6$. By Corollary 3.6.22, for any $i \in \mathbb{N}$ such that $\gcd(6,i) = 1$, 5^i will also generate $U(18)$. In this case, $5^5 = 11$ is also a generator. ◇

By now, you have probably passed your calculus courses, and know that the various Fundamental Theorems of Calculus were, surprisingly, important. Similarly, when you encounter a "Fundamental Theorem" in algebra, you

know it will be important.

Theorem 3.6.24 (Fundamental Theorem of Cyclic Groups)**.** *Every subgroup of a cyclic group is cyclic. Further, if the group has order n, then*

1. *the order of each subgroup divides n, and*
2. *for each positive divisor k of n, there exists exactly one subgroup of order k, the subgroup $\langle a^{n/k} \rangle$.*

Proof. Let H be a subgroup of G, and assume G is generated by a. If $H = \{e\}$, where e is the identity of G, then H is cyclic. Now assume there exists another element of G in H, say $a^j \neq e \in H$. By the definition of cyclic, either j is positive or $-j$ is positive, and by closure, $a^{-j} \in H$. Thus, we may assume H has at least one element that is a positive power of a. Let $a^i \in H$ be the element with the smallest positive power of a in H. By closure, $\langle a^i \rangle \subset H$. We wish to show $\langle a^i \rangle = H$.

Let $b \in H$; we wish to show b is generated by a^i. We are given that $H \leq G$, thus b is generated by a. Assume $b = a^\ell$ for some $\ell \in \mathbb{Z}$. By the Division Algorithm, there exist $q, r \in \mathbb{Z}$ such that $\ell = qi + r$ and $0 \leq r < i$. Hence,

$$a^\ell = a^{qi+r} = a^{qi}a^r$$
$$a^r = a^\ell a^{-qi}.$$

By closure, $a^{-qi} \in H$. Further, $b = a^\ell \in H$. Thus, by closure, $a^r \in H$. Recall that $0 \leq r < i$ and i is the smallest positive power of a in H, thus $r = 0$. Therefore, $b = a^\ell = a^{qi} \in \langle a^i \rangle$. Ergo, $H \subseteq \langle a^i \rangle$ and $H = \langle a^i \rangle$.

Next, we will show that, when the order of the group is finite, the order of the subgroup divides the order of the group. Suppose $|G| = n$ and let H be any subgroup of G. By the previous work, we know that $H = \langle a^i \rangle$ for some

$i \in \mathbb{N}$. Applying the above work to the special case when $b = e = a^n$, we see that

$$b = e = a^n = a^{qi} = (a^i)^q.$$

Recall that i is the smallest positive power of a in H. Thus, $|H| = q$, which divides n.

Last, we will show that, for k a divisor of n, $\langle a^{n/k} \rangle$ is the unique subgroup of order k. By Theorem 3.6.18,

$$|a^{n/k}| = \frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k.$$

To show that $\langle a^{n/k} \rangle$ is the unique subgroup of order k, let H be a subgroup of G of order k. We wish to show $H = \langle a^{n/k} \rangle$. By the above work, we know that $H = \langle a^i \rangle$ and i is a divisor of n. Notice that $i = \gcd(n, i)$. By construction and the previous corollaries,

$$k = |H| = |\langle a^i \rangle| = |\langle a^{\gcd(n,i)} \rangle| = \frac{n}{\gcd(n, i)} = \frac{n}{i}.$$

Thus, $i = n/k$ and therefore $H = \langle a^i \rangle = \langle a^{n/k} \rangle$. □

Notice that Theorem 3.6.24 tells us exactly how many subgroups of a cyclic group there are, that they are all cyclic, and how to generate them. This is the first tool we have developed that allows us to categorize all subgroups of a given group, which is kind of a big deal.

Example 3.6.25. We can use Theorem 3.6.24 to find all of the subgroups of $\mathbb{Z}_{24}$. We know that $\mathbb{Z}_{24}$ is generated by 1 and $|\mathbb{Z}_{24}| = 24$. Thus for each positive divisor k of 24, we can find the subgroup of order k, namely, $\langle 1^{24/k} \rangle$. Below is a table of all divisors, the subgroups $\langle 1^{24/k} \rangle$, and their orders.

Divisor	Subgroup	Order
1	$\langle 1^{24} \rangle = \langle 0 \rangle = \{0\}$	1
2	$\langle 1^{24/2} \rangle = \langle 12 \rangle = \{0, 12\}$	2
3	$\langle 1^{24/3} \rangle = \langle 8 \rangle = \{0, 8, 16\}$	3
4	$\langle 1^{24/4} \rangle = \langle 6 \rangle = \{0, 6, 12, 18\}$	4
6	$\langle 1^{24/6} \rangle = \langle 4 \rangle = \{0, 4, 8, 12, 16, 20\}$	6
8	$\langle 1^{24/8} \rangle = \langle 3 \rangle = \{0, 3, 6, 912, 15, 18, 21\}$	8
12	$\langle 1^{24/12} \rangle = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$	12
24	$\langle 1^{24/24} \rangle = \langle 1 \rangle = \mathbb{Z}_{24}$	24

◇

As Theorem 3.6.18, its corollaries, and Theorem 3.6.24 indicate, when a cyclic group has finite order, the divisors of the order play a big role in subgroup computations. This may lead you to wondering how many elements can create the various subgroups.

Definition 3.6.26. Given a natural $n > 1$, the Euler Phi Function, denoted $\phi(n)$, is the number of natural numbers relatively prime to n. When $n = 1$, $\phi(1) = 1$.

Example 3.6.27. Consider $U(12) = \{1, 5, 7, 11\}$. We know that this group consists of the natural numbers that are relatively prime to 12 and less than 12. Thus, by the definition of $U(12)$ and $\phi(12)$, $|U(12)| = \phi(12)$. In fact, for all natural numbers $n > 2$, $|U(n)| = \phi(n)$. ◇

The Euler Phi Function is a very useful function, both in abstract algebra and in number theory (and life, of course). Below is a table of the first few values of the Euler Phi Function.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

The theorem below gives a classification of the value of the Euler Phi Function in certain cases. These cases are not comprehensive, but common enough that you may find these formulas useful. The proofs of these formulas can be found in an introductory book on number theory.

Theorem 3.6.28. *Let $n > 2$ be a natural number and $\phi(n)$ the Euler Phi Function.*

1. *If $n = p^k$ where p is prime, then $\phi(p^k) = p^k - p^{k-1}$.*
2. *If $n = rs$ where $r, s \in \mathbb{N}$ and $\gcd(r, s) = 1$, then $\phi(rs) = \phi(r)\phi(s)$.*

Example 3.6.29. Consider $n = 80$. We know that 80 is not a power of a prime, thus in order to compute $\phi(80)$, we need to find two relatively prime factors of 80. Thus,

$$\begin{aligned}\phi(80) &= \phi(5 \cdot 16) = \phi(5)\phi(16) \\ &= \phi(5^1)\phi(2^4) = (5^1 - 5^0)(2^4 - 2^3) = (4)(8) = 32.\end{aligned}$$

◇

The theorem below gives a formula for computing $\phi(n)$ for any natural number $n > 2$.

Theorem 3.6.30. *Let $n > 2$ be a natural number and $\phi(n)$ the Euler Phi Function. Let $p_1, p_2, \ldots, p_k \in \mathbb{N}$ be the distinct primes that divide n. Then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Example 3.6.31. Let's consider $\phi(80)$ again, only this time we will compute it using the formula in Theorem 3.6.30. Notice that 2 and 5 are the distinct primes that divide 80. Thus,

$$\phi(80) = 80\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 80\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 32.$$

$\diamond$

While you surely enjoyed that brief foray into number theory, you may be wondering how the Euler Phi Function relates to cyclic groups. This is addressed below.

Theorem 3.6.32. *Let G be a cyclic group of order n and d a divisor of n. Then the number of elements of order d in G is $\phi(d)$.*

Proof. Let G be a cyclic group of order n, and let d be a divisor of n. By the Fundamental Theorem of Cyclic Groups, G has exactly one subgroup of order d, say $\langle b\rangle$ for some $b \in G$. By Corollary 3.6.21, every other element of order d also generates $\langle b\rangle$. Let $c \in G$ be another element of order d. Then $\langle b\rangle = \langle c\rangle$. Moreover, we can write b as a power of c and vice versa.

Suppose $c = b^i$ for some $i \in \mathbb{Z}$. By Corollay 3.6.21, $\langle b\rangle = \langle b^i\rangle$ if and only if $\gcd(|b|, i) = \gcd(d, i) = 1$, that is, d and i are relatively prime. The number of elements of the form b^i that meet this quality is exactly $\phi(d)$. $\square$

Example 3.6.33. We saw in Example 3.6.25 that $\mathbb{Z}_{24}$ will have eight cyclic subgroups, one for each divisor of 24. Notice that 6 and 18 generate the same subgroup, and though $12 \in \langle 6\rangle = \langle 18\rangle$, 12 does not generate this subgroup. This is because $|6| = |18|$ in $\mathbb{Z}_{24}$, and $|12| \neq |6|$ in $\mathbb{Z}_{24}$.

We could use Theorem 3.6.32 to predict this result. Notice that 6 is a divisor of 24 and $|6| = 4$. Thus, to apply the theorem, let $d = |6| = 4$ and $n = 24$.

Then the number of elements in $\mathbb{Z}_{24}$ of order 4 is $\phi(4) = 2$. This tells us that 6 and one other element have order 4. By Corollary 3.6.21, we know this other element will create a the same cyclic subgroup as 6. $\diamond$

Example 3.6.34. Consider $\mathbb{Z}_{50}$. Certainly $\langle 5 \rangle$ is a subgroup of $\mathbb{Z}_{50}$. We know by Corollary 3.6.14 that $|5| = |\langle 5 \rangle|$, and in this case, $|5| = |\langle 5 \rangle| = 10$. By the Fundamental Theorem of Cyclic Groups, we know that $\langle 5 \rangle$ is the *unique* cyclic subgroup of order 10. What else generates this subgroup? How many elements are we even searching for? The Euler Phi Function helps us answer this question.

We are searching for elements of the same order as 5 because those elements will create $\langle 5 \rangle$. Thus, using Theorem 3.6.32, let $d = |5| = 10$ and $n = 50$. Then the number of elements in $\mathbb{Z}_{50}$ of order 10 is $\phi(10) = 4$. This tells us that 5 and three other elements have order 10.

Now we know we are searching for three more elements in $\mathbb{Z}_{50}$ that have order 10. By Corollary 3.6.21, each will be some i such that $\gcd(50, 5) = \gcd(50, i)$. Thus, we need numbers whose greatest common divisor with 50 is 5. We see that those numbers are 15, 35, and 45. Hence

$$\langle 5 \rangle = \langle 15 \rangle = \langle 35 \rangle = \langle 45 \rangle.$$

$\diamond$

Notice that the corollary below applies to finite groups, not just finite cyclic groups. This is a big step!

Corollary 3.6.35. *In a finite group, the number of elements of order d is a multiple of $\phi(d)$.*

Proof. Let G be a finite group, $d \in \mathbb{N}$, and m the number of elements of order d. If there are no elements of order d, that is, if $m = 0$, then m is a

multiple of d.

Now assume that $m \geq 1$, that is, at least one element in G has order d. Let $a \in G$ is an element of order d. Note that d dividies $|\langle a \rangle| = |a| = d$. Applying Theorem 3.6.32 to the group $\langle a \rangle$, we see that $\langle a \rangle$ will have $\phi(d)$ elements of order d in it, including a.

We proceed by induction on the number of distinct cyclic subgroups in G of order d. The case of 1 distinct cyclic subgroup of order d we just discussed. Now, for another base case, assume $b \notin \langle a \rangle$ is another element of G of order d. By a similar argument, $\langle b \rangle$ has $\phi(d)$ elements of order d, including b.

Moreover, $\langle a \rangle$ and $\langle b \rangle$ have no common elements of order d. To see this, assume by contradiction that $c \in \langle a \rangle \cap \langle b \rangle$ is an element of order d. Then $\langle c \rangle \subseteq \langle a \rangle$, and because $|a| = |c| = d$, $\langle a \rangle = \langle c \rangle$. By a similar argument, $\langle b \rangle = \langle c \rangle$. Thus, $\langle a \rangle = \langle b \rangle$ and $b \in \langle a \rangle$, which contradicts our choice of b.

Therefore, $\langle a \rangle$ and $\langle b \rangle$ contribute a total of $2\phi(d)$ elements of order d. □

The completion of the proof by induction is left to the reader as an exercise.

Example 3.6.36. Consider the finite and noncyclic group S_7. Below are a few examples of how Corollary 3.6.35 applies.

- A permutation in the form of a 5-cycle composed with a 2-cycle will have order 10, and that is the only way to create an element of order 10 in S_7. The number of elements of order 10 is a multiple of $\phi(10) = 4$.
- A permutation in the form of a 4-cycle composed with a 3-cycle will have order 12, and that is the only way to create an element of order 12 in S_7. The number of elements of order 12 is a multiple of $\phi(12) = 4$.

◇

EXERCISES

Exercise 3.6.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a. A cyclic group has at least two generators.

b. A cyclic group is Abelian.

c. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is cyclic.

d. For $n \in \mathbb{N}$, $U(n)$ is cyclic.

e. For $n \in \mathbb{N}$, $n\mathbb{Z}$ is cyclic.

f. A subgroup of a cyclic group is cyclic.

g. A cyclic group has at least one finite cyclic subgroup.

h. In $\mathbb{Z}$, for $n \in \mathbb{N}$, $\langle n \rangle \subseteq \langle 2n \rangle$.

i. For group element a, $\langle a^2 \rangle \subseteq \langle a^4 \rangle$.

Exercise 3.6.2. For each group listed below, find every cyclic subgroup.

a. $\mathbb{Z}_8$

b. $\mathbb{Z}_5^*$

c. $U(20)$

d. S_4

Exercise 3.6.3. Prove Corollary 3.6.14.

Exercise 3.6.4. Prove Corollary 3.6.15.

Exercise 3.6.5. Consider the group $\mathbb{Z}_{60}$. Find the following subgroups and their orders.

a. $\langle 5 \rangle$

b. $\langle 35 \rangle$

c. $\langle 48 \rangle$

d. $\langle 57 \rangle$

Exercise 3.6.6. Consider the group D_n for $n \geq 2$. Find the following subgroups and their orders.

a. $\langle R_{135} \rangle$ when $n = 8$

b. $\langle R_{270} \rangle$ when $n = 8$

c. $\langle R_{252} \rangle$ when $n = 10$

d. $\langle R_{288} \rangle$ when $n = 10$

Exercise 3.6.7. Suppose $G = \langle a \rangle$. Find all of the generators of G for each of the following cases.

a. $|a| = 4$

b. $|a| = 10$

c. $|a| = 20$

Exercise 3.6.8. Ⓢ Consider the group $\mathbb{Z}_{90}$. Find $\langle 54 \rangle$ and $|\langle 54 \rangle|$.

Exercise 3.6.9. Let $G = \langle a \rangle$ be a group and $|a| = 20$. For each of the following, first, find the order of the element, and then find all of the other elements of that order.

a. a^2

b. a^8

c. a^{15}

Exercise 3.6.10. Ⓢ Using Theorem 3.6.30, which defines the Euler Phi Function as

$$\phi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)...\Big(1 - \frac{1}{p_k}\Big),$$

find $\phi(210)$.

Exercise 3.6.11. Let a be an element of a group. Prove that $\langle a \rangle = \langle a^{-1} \rangle$.

Exercise 3.6.12. Prove Corollary 3.6.20.

Exercise 3.6.13. Prove Corollary 3.6.22.

Exercise 3.6.14. Consider $\mathbb{Z}_{60}$. Find all generators of the subgroup $\langle 42 \rangle \cap \langle 18 \rangle$.

Exercise 3.6.15. **a.** Find all subgroups of $\mathbb{Z}_{30}$.

b. Find all subgroups of $G = \langle a \rangle$ where $|a| = 30$.

Exercise 3.6.16. Let G be a cyclic group with exactly three subgroups: $\{e\}$, G, and H where $|H| = 5$. Find $|G|$.

Exercise 3.6.17. Let G be a group with element a. Prove that $\langle a \rangle$ is a subgroup of $C_G(a)$.

Exercise 3.6.18. Consider the set $\{8, 16, 24, 32\}$ under multiplication modulo 40. Create a Cayley table for this set to justify that it is indeed a group. What is the identity? Is it cyclic? If so, find its generators. If not, explain why not.

Exercise 3.6.19. Find all elements of order 12 in $\mathbb{Z}_{120,000}$. Justify that your list is complete.

Exercise 3.6.20. For each of the following n, give an example of a cyclic group G with exactly n subgroups, including $\{e\}$ and G.

a. $n = 3$

b. $n = 4$

c. $n = 5$

Exercise 3.6.21. Consider the group $\mathbb{Z}_{300}$ and its cyclic subgroups. Find the largest chain

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_n \rangle$$

in $\mathbb{Z}_{300}$, that is, find the highest number of nested cyclic subgroups in $\mathbb{Z}_{300}$. Justify why the n you found is maximal.

Exercise 3.6.22. Let a and b be elements of group G such that $|a|$ and $|b|$ are relatively prime. Prove that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Exercise 3.6.23. Compute $\phi(n)$ for each of the following n.

a. $n = 27$

b. $n = 125$

c. $n = 40$

d. $n = 120$

e. $n = 2^3 \cdot 3 \cdot 5^2 \cdot 7$

Exercise 3.6.24. Let p be an odd prime and $k \in \mathbb{N}$. Prove that $|U(p^k)| = |U(2p^k)|$.

Exercise 3.6.25. Consider $\mathbb{Z}_{250}$. First, find all of the orders of the subgroups. Then, for each order d, find the following.

a. The number of elements that will generate the subgroup of order d

b. The subgroup of order d

Exercise 3.6.26. Let H be a group of order three and G a group of order four.

a. Prove that H is cyclic.

b. Prove that G can not have a subgroup of order three.

Exercise 3.6.27. Complete the proof of Corollary 3.6.35.

Exercise 3.6.28. Ⓢ Let $a \in U(n)$ and $m \in \mathbb{N}$ with $1 \leq m \leq n$.

a. Show that if $|\langle a \rangle| = m$, then $n \mid (a^m - 1)$.

b. Show that if $n \mid a^m - 1$ and $n > a^k$ for all k that divide m, then $|\langle a \rangle| = m$.

Chapter 4

Functions on Groups

One can state, without exaggeration, that
the observation of and the search for similarities and differences
are the basis of all human knowledge.
Alfred Nobel

By now we have seen many examples of many different types of groups. Some groups are quite different from each other. Hopefully, you noticed that some groups are quite similar, though you may not have the precise vocabulary to describe what "similar" even means. In this chapter, we study functions that map from one group to another. By understanding these functions, we will better understand the groups themselves. These functions will also provide some structure that will allow us to determine when two groups are "similar."

4.1 Homomorphisms

How do we create functions between groups? Can we create any function at all? Before we begin to study "nice" mappings, let's study some poorly behaved mappings.

Non-Example 4.1.1. Let $f : \mathbb{Z}_4 \to \mathbb{Z}_4$ be defined as $f(x) = x + 1$ for all $x \in \mathbb{Z}_4$. First, we consider $f(2 + 3)$, in which the group operation is done *before* applying the function to the group elements. Second, we consider $f(2) + f(3)$, in which the group operation is done *after* applying the function to the group elements.

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

Notice that $f(2 + 3) \neq f(2) + f(3)$. ◇

Non-Example 4.1.2. Let $f : D_3 \to S_3$ be defined as

$$f(R_0) = (123)$$
$$f(R_{120}) = (132)$$
$$f(R_{240}) = (12)$$
$$f(V) = (13)$$
$$f(L) = (23)$$
$$f(R) = e.$$

Again, we will compose two elements two different ways: before applying the function and after applying the function. For the sake of emphasis, we write

$*$ as each group's operation. Consider $R_{120}, V \in D_3$.

$$f(R_{120} * V) = f(R) = e$$
$$f(R_{120}) * f(V) = (132) * (13) = (12)$$

Once again, we see that $f(R_{120} * V) \neq f(R_{120}) * f(V)$. $\diamond$

Non-Example 4.1.3. Let $f : S_3 \to \mathbb{Z}_6$ be defined as

$$f(\,e\,) = 0$$
$$f(\,(12)\,) = 1$$
$$f(\,(13)\,) = 2$$
$$f(\,(23)\,) = 3$$
$$f(\,(123)\,) = 4$$
$$f(\,(132)\,) = 5$$

Again, we will compose two elements two different ways: before applying the function and after applying the function. Notice that these two groups have different operations. Thus, when we compose two elements before the applying the function, we are composing elements of S_3 under function composition. When we compose two elements after applying the function, we are composing elements of $\mathbb{Z}_6$ under addition modulo 6.

$$f(\,(132) * (123)\,) = f(e) = 0$$
$$f(\,(132)\,) * f(\,(123)\,) = 5 * 4 = 3$$

Once again, we see that $f(\,(132) * (123)\,) \neq f(\,(132)\,) * f(\,(123)\,)$. $\diamond$

Below is the definition of the type of function that does not allow for this

type of misbehavior.

Definition 4.1.4. A homomorphism ϕ is a mapping from a group G to a group G' that preserves the group operation, that is,

$$\phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in G$ and for all $\phi(x), \phi(y) \in G'$.

Non-Examples 4.1.1, 4.1.2, and 4.1.3 are examples of mappings that are *not* homomorphisms because they do not preserve the group operation. Below is an example of a homomorphism, with many more following the next definition. There are many, many properties to observe. As you work through these examples, perhaps make a conjecture about the patterns you see.

Example 4.1.5. The function $g : \mathbb{Z}_4 \to \mathbb{Z}_4$ defined by $f(x) = x$ for all $x \in \mathbb{Z}_4$ is a homomorphism. ◇

Non-Example 4.1.6. Ⓢ Let $\phi : M_2(K) \to M_2(P)$, where $K = \mathbb{Z}$ and $P = \mathbb{Z}$, be defined as $\phi(x) = x \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. Notice that the group operation is matrix multiplication. We will compose two arbitrary elements of $M_2(K)$ before applying the function ϕ. Then we will compose those two elements after applying the function, thus we will compose elements of $M_2(P)$. This will let us know if ϕ is a homomorphism.

Let $a, b, c, d, h, k, m, n \in \mathbb{Z}$. Then,

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} h & k \\ m & n \end{bmatrix}\right) = \phi\left(\begin{bmatrix} ah+bm & ak+bn \\ ch+dm & ck+dn \end{bmatrix}\right)$$
$$= \begin{bmatrix} ah+bm & 2(ah+bm)+(ak+bn) \\ ch+dm & 2(ch+dm)+(ck+dn) \end{bmatrix}.$$

Further,

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\phi\left(\begin{bmatrix} h & k \\ m & n \end{bmatrix}\right) = \begin{bmatrix} a & 2a+b \\ c & 2c+d \end{bmatrix} \cdot \begin{bmatrix} h & 2h+k \\ m & 2m+n \end{bmatrix}$$
$$= \begin{bmatrix} ah+m(2a+b) & a(2h+k)+(2a+b)(2m+n) \\ ch+m(2c+d) & c(2h+k)+(2c+d)(2m+n) \end{bmatrix}.$$

Thus, $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} h & k \\ m & n \end{bmatrix}\right) \neq \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\phi\left(\begin{bmatrix} h & k \\ m & n \end{bmatrix}\right)$.

Therefore, ϕ is not a homomorphism. ◇

One of the reasons why f in Non-Example 4.1.1 was not a homomorphism was because the identity did not get to the identity. In Example 4.1.5, the identity gets sent to itself. In fact, the set of elements that get sent to the identity plays an important role in analyzing homomorphisms.

Definition 4.1.7. Let $\phi : G \to G'$ be a homomorphism from group G to group G' with identity e'. The kernel of ϕ is the set of all elements that get sent to the identity, that is,

$$\ker(\phi) = \{g \in G \mid \phi(g) = e'\}.$$

Example 4.1.8. The map $\phi : \mathbb{R}^* \to \mathbb{R}^*$ given by $\phi(x) = |x|$ is a homomorphism. Note that the operation on $\mathbb{R}^*$ is multiplication. To prove ϕ is a homomorphism, we need to show that for $x, y \in \mathbb{R}^*$, $\phi(xy) = \phi(x)\phi(y)$. Notice,

$$\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y),$$

thus the operation is preserved.

The identity of $\mathbb{R}^*$ is 1. The kernel of ϕ is

$$\begin{aligned}\ker(\phi) &= \{x \in \mathbb{R}^* \,|\, \phi(x) = 1\} \\ &= \{x \in \mathbb{R}^* \,|\, |x| = 1\} \\ &= \{1, -1\}.\end{aligned}$$

$\diamond$

Example 4.1.9. The map $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_4$ defined by $\phi(x) = x \bmod 4$ is a homomorphism. Note that the operation on $\mathbb{Z}_{20}$ is addition modulo 20; the operation on $\mathbb{Z}_4$ is addition modulo 4. To prove ϕ is a homomorphism, we see that for $x, y \in \mathbb{Z}_{20}$,

$$\phi(x + y) = (x + y) \bmod 4 = (x \bmod 4) + (y \bmod 4) = \phi(x) + \phi(y).$$

The identity of $\mathbb{Z}_4$ is 0. The kernel of ϕ is

$$\begin{aligned}\ker(\phi) &= \{x \in \mathbb{Z}_{20} \,|\, \phi(x) = 0\} \\ &= \{x \in \mathbb{Z}_{20} \,|\, x \bmod 4 = 0\} \\ &= \{0, 4, 8, 12, 16\}.\end{aligned}$$

$\diamond$

Example 4.1.10. The map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{20}$ defined by $\phi(x) = 5x$ is a homomorphism. Note that the operation on $\mathbb{Z}_4$ is addition modulo 4; the

operation on $\mathbb{Z}_{20}$ is addition modulo 20. To prove ϕ is a homomorphism, we see that for $x, y \in \mathbb{Z}_4$,

$$\phi(x+y) = 5(x+y) = 5x + 5y = \phi(x) + \phi(y).$$

The identity of $\mathbb{Z}_{20}$ is 0. The kernel of ϕ is

$$\begin{aligned} \ker(\phi) &= \{x \in \mathbb{Z}_4 \,|\, \phi(x) = 0\} \\ &= \{x \in \mathbb{Z}_4 \,|\, 5x = 0\} \\ &= \{0\}. \end{aligned}$$

$\diamond$

Example 4.1.11. The map $\phi : \mathbb{R} \to \mathbb{R}^2$ defined by $\phi(x) = (x, 0)$ is a homomorphism. Note that the operation on $\mathbb{R}$ is addition; the operation on $\mathbb{R}^2$ is coordinate addition. To prove ϕ is a homomorphism, we see that for $x, y \in \mathbb{R}$,

$$\phi(x+y) = (x+y, 0) = (x, o) + (y, 0) = \phi(x) + \phi(y).$$

The identity of $\mathbb{R}^2$ is $(0, 0)$. The kernel of ϕ is

$$\begin{aligned} \ker(\phi) &= \{x \in \mathbb{R} \,|\, \phi(x) = (0,0)\} \\ &= \{x \in \mathbb{R} \,|\, (x,0) = (0,0)\} \\ &= \{0\}. \end{aligned}$$

$\diamond$

Example 4.1.12. Consider $\mathbb{R}[x]$ under addition, not function composition. The map $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ defined by $\phi(f(x)) = f'(x)$ is a homomorphism.

To prove ϕ is a homomorphism, we see that for $f(x), g(x) \in \mathbb{R}[x]$,

$$\phi(f(x) + g(x)) = (f(x) + g(x))' = f'(x) + g'(x) = \phi(f(x)) + \phi(g(x)).$$

The identity of $\mathbb{R}[x]$ under addition is 0. The kernel of ϕ is

$$\begin{aligned} \ker(\phi) &= \{f(x) \in \mathbb{R}[x] \mid \phi(f(x)) = 0\} \\ &= \{f(x) \in \mathbb{R}[x] \mid f'(x) = 0\} \\ &= \{f(x) = c \mid c \in \mathbb{R}\}, \end{aligned}$$

which is the set of all constant functions. ◇

Example 4.1.13. The map $\phi : S_7 \to S_7$ defined by $\phi(x) = e$ is a homomorphism. Note that the operation on S_7 is function composition. To prove ϕ is a homomorphism, we see that for $\alpha, \beta \in S_7$,

$$\phi(\alpha \circ \beta) = e = e \circ e = \phi(\alpha) \circ \phi(\beta).$$

The identity of S_7 is e. The kernel of ϕ is

$$\ker(\phi) = \{\sigma \in S_7 \mid \phi(\sigma) = e\} = S_7$$

because, by the definition of ϕ, every permutation gets mapped to the identity. ◇

As always, *order matters*. A homomophism ϕ preserves the group operation, that is, for group elements x and y,

$$\phi(xy) = \phi(x)\phi(y).$$

Do not assume $\phi(x)\phi(y) = \phi(y)\phi(x)$. Order matters.

Notice that the kernels in Examples 4.1.5 through 4.1.13 were indeed subgroups. Further, in Non-Examples 4.1.1 and 4.1.2, notice that the elements that get mapped to the identity do not form a subgroup.

Below are some properties of elements under homomorphisms.

Theorem 4.1.14. *Let $\phi : G \to G'$ be a homomorphism, and let $g \in G$. Let $e \in G$ be the identity of G; let $e' \in G'$ be the identity of G'.*

1. *The identity maps to the identity, that is, $\phi(e) = e'$.*
2. *For $n \in \mathbb{Z}$, $\phi(g^n) = [\phi(g)]^n$.*
3. *If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.*

Proof. For the first part, notice that $e = ee$. Applying ϕ to both sides, we see that

$$\phi(e) = \phi(ee) = \phi(e)\phi(e) \tag{4.1}$$

because ϕ is a homomorphism and thus operation preserving. Also note that by the definition of the identity $e' \in G'$,

$$\phi(e) = e'\phi(e). \tag{4.2}$$

Hence, by Equations 4.1 and 4.2, we see that

$$\phi(e)\phi(e) = e'\phi(e).$$

By cancelling $\phi(e)$ on right, we see that $\phi(e) = e'$.

The second part may be proved for $n \in \mathbb{N}$ by induction. When $n = 0$, we have the claim $\phi(e) = e'$, which we just proved to be true. Now consider when n is a negative integer. Thus, $-n$ is a positive integer, and we may

assume the result holds for $-n$. Using this assumption and the first part of this theorem, we see that

$$\begin{aligned} e' &= \phi(e) \\ &= \phi(g^n g^{-n}) \\ &= \phi(g^n)\phi(g^{-n}) \qquad (4.3) \\ &= \phi(g^n)[\phi(g)]^{-n} \qquad (4.4) \end{aligned}$$

Note that we get line 4.3 because a homomorphism preserves the group operation. Next, line 4.4 is true by assumption because $-n$ is positive. Multiplying both sides by $[\phi(g)]^n$, we get that

$$[\phi(g)]^n = \phi(g^n)$$

for negative integers n. Thus, $\phi(g^n) = [\phi(g)]^n$ for all integers n.

For the third part of the theorem, assume $|g| = n$ for some $n \in \mathbb{N}$, thus $g^n = e$. By the first two results, we see that

$$\begin{aligned} e &= g^n \\ \phi(e) &= \phi(g^n) \\ e' &= [\phi(g)]^n. \end{aligned}$$

Thus, $|\phi(g)|$ divides $n = |g|$. □

Below are two examples to demonstrate these properties.

Example 4.1.15. Let $\phi : \mathbb{Z}_5 \to \mathbb{Z}_{10}$ be given by $\phi(x) = 2x$. Then ϕ is a homomorphism because for $x, y \in \mathbb{Z}_5$,

$$\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y).$$

We create some examples to observe the properties in Theorem 4.1.14 below. Note that the group operations are addition.

1. For $0 \in \mathbb{Z}_5$, $\phi(0) = 0 \in \mathbb{Z}_{10}$.

2. Take $2 \in \mathbb{Z}_5$. When $n = 2$, we see that

$$\begin{aligned} \phi(2^2) = \phi(2+2) = \phi(4) = 8 \\ [\phi(2)]^2 = 4^2 = 4+4 = 8, \end{aligned}$$

   thus $\phi(2^2) = [\phi(2)]^2$. When $n = 3$, we see that

$$\begin{aligned} \phi(2^3) = \phi(2+2+2) = \phi(1) = 2 \\ [\phi(2)]^3 = 4^3 = 4+4+4 = 2, \end{aligned}$$

   thus $\phi(2^3) = [\phi(2)]^3$.

3. Take $2 \in \mathbb{Z}_5$, then $|2| = 5$. Notice that $|\phi(2)| = |4| = 5$ divides $|2|$.

$\diamond$

Example 4.1.16. Let $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_3$ be given by $\phi(x) = x \bmod 3$. Then ϕ is a homomorphism because for $x, y \in \mathbb{Z}_{30}$,

$$\phi(x+y) = (x+y) \bmod 3 = x \bmod 3 + y \bmod 3 = \phi(x) + \phi(y).$$

We create some examples to observe the properties in Theorem 4.1.14 below. Note that the group operations are addition.

1. For $0 \in \mathbb{Z}_{30}$, $\phi(0) = 0 \in \mathbb{Z}_3$.

2. Take $17 \in \mathbb{Z}_{30}$. When $n = 2$, we see that

$$\phi(17^2) = \phi(17 + 17) = \phi(4) = 1$$
$$[\phi(17)]^2 = 2^2 = 2 + 2 = 1,$$

thus $\phi(17^2) = [\phi(17)]^2$. When $n = 3$, we see that

$$\phi(17^3) = \phi(17 + 17 + 17) = \phi(21) = 0$$
$$[\phi(17)]^3 = 2^3 = 2 + 2 + 2 = 0,$$

thus $\phi(17^3) = [\phi(17)]^3$.

3. Take $17 \in \mathbb{Z}_{30}$, then $|17| = 30$. Notice that $|\phi(17)| = |2| = 3$ divides 30. Take $28 \in \mathbb{Z}_{30}$, then $|28| = 15$. Notice that $|\phi(28)| = |1| = 3$ divides 15.

$\diamond$

Note that in Examples 4.1.5 through 4.1.13, the identity of the first group is in the kernel of the homomorphism, that is, the identity of the first group is always sent to the identity of the second group. This leads us to the following theorem, the proof of which is an exercise.

Theorem 4.1.17. *Let $\phi : G \to G'$ be a homomorphism. Then* $\ker(\phi)$ *is a subgroup of G.*

Look back at the previous examples of homomorphisms to see some examples of the kernel being a subgroup.

The following theorem describes how subgroups behave under homomorphisms.

Theorem 4.1.18. *Let $\phi : G \to G'$ be a homomorphism, and let H be a subgroup of G.*

1. *The set* $\phi(H) = \{\phi(h) \,|\, h \in H\}$ *is a subgroup of* G'.

2. *If* H *is cyclic, then* $\phi(H)$ *is cyclic.*

3. *If* H *is Abelian, then* $\phi(H)$ *is Abelian.*

4. *If* H' *is a subgroup of* G', *then* $\phi^{-1}(H') = \{h \in G \,|\, \phi(h) \in H'\}$ *is a subgroup of* G.

The proofs of these claims are left to the reader as exercises. Below are some examples demonstrating these claims.

Example 4.1.19. Consider the group D_3 and its subgroup $H = \langle R_{120} \rangle = \{R_0, R_{120}, R_{240}\}$. Let $\phi : D_3 \to S_3$ be defined as

$$\begin{aligned} \phi(R_0) &= e \\ \phi(V) &= (23) \\ \phi(L) &= (12) \\ \phi(R) &= (13) \\ \phi(R_{120}) &= (132) \\ \phi(R_{240}) &= (123). \end{aligned}$$

Examples of the properties of Theorem 4.1.18 are given below.

1. The image of H under the homomorphism ϕ is

$$\begin{aligned} \phi(H) &= \{\phi(h) \,|\, h \in H\} \\ &= \{\phi(R_0), \phi(R_{120}, \phi(R_{240}\} \\ &= \{e, (132), (123)\}, \end{aligned}$$

   which is a subgroup of S_3.

2. The subgroup H is cyclic because it is generated by R_{120} and R_{240}. The subgroup $\phi(H)$ is cyclic because it is generated by (123) and (132).

3. Cyclic groups are Abelian, thus both H and $\phi(H)$ are Abelian.

4. Consider the subgroup $K' = \{e, (12)\}$ in S_3. Its inverse image is the set

$$\begin{aligned}\phi^{-1}(K') &= \{k \in G \,|\, \phi(k) \in K'\} \\ &= \{k \in G \,|\, \phi(k) = e \text{ or } \phi(k) = (12)\} \\ &= \{R_0, L\},\end{aligned}$$

which is a subgroup of D_3.

◇

EXERCISES

Exercise 4.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let $\phi : G \to G'$ be a homomorphism from group G to group G'.

a. $|\phi(g)| = |g|$

b. $\phi(G) = G'$

c. A homomorphism is injective.

d. A homomorphism is surjective.

e. A homomorphism is bijective.

f. For $m, n \in \mathbb{N}$, there is a homomorphism from $\mathbb{Z}_m$ to $\mathbb{Z}_n$.

g. For $m, n \in \mathbb{N}$, there is a surjective homomorphism from $\mathbb{Z}_m$ to $\mathbb{Z}_n$.

Exercise 4.1.2. Revisit Examples 4.1.5 through 4.1.13. Which homomorphisms are one-to-one and onto? Which are only one-to-one? Which are only onto? Which are neither one-to-one nor onto?

Exercise 4.1.3. Suppose $\phi : \mathbb{R} \to \mathbb{R}^2$ and $\psi : \mathbb{R}^2 \to \mathbb{R}$. For each of the following, determine if the map is a homomorphism. If so, prove that the map is a homomorphism and find its kernel. If not, give a reason why not.

a. $\phi(x) = (0, x)$
b. $\phi(x) = (x, 1)$
c. $\phi(x) = (x, x)$
d. $\psi((x, y)) = x$
e. $\psi((x, y)) = x + y$
f. $\psi((x, y)) = \lfloor x + y \rfloor$

Exercise 4.1.4. Consider $\mathbb{R}[x]$ under function composition. Define the map $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ as $\phi(f(x)) = f'(x)$. Is ϕ a homomorphism? If so, prove that the map is a homomorphism and find its kernel. If not, give a reason why not.

Exercise 4.1.5. Let $n \geq 2$ be a natural number. For each of the following, prove that ϕ is a homomorphism and find $\ker(\phi)$.

a. The map $\phi : \mathbb{Z}_{7n} \to \mathbb{Z}_n$, defined by $\phi(x) = x \bmod n$.
b. The map $\phi : \mathbb{Z}_n \to \mathbb{Z}_{7n}$, defined by $\phi(x) = 7x$.
c. The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$, defined by $\phi(x) = x \bmod n$.

Exercise 4.1.6. Ⓢ The map $\phi : \mathbb{Z}_{18} \to \mathbb{Z}_{378}$ defined by $\phi(x) = 21x$ is a homomorphism. When $x = 15 \in \mathbb{Z}_{18}$, show that $[\phi(x)]^n = \phi(x^n)$ for $n = 3$ and $n = 20$.

Exercise 4.1.7. Let G be a permutation group. For each $\sigma \in G$, define

$$\mathsf{sgn}(\sigma) = \begin{cases} +1 & \sigma \text{ is even} \\ -1 & \sigma \text{ is odd.} \end{cases}$$

Prove that sgn is a homomorphism from G to the group $\{1, -1\}$ under multiplication. Find its kernel.

Exercise 4.1.8. Let G, H, and K be groups. Suppose $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms. Is $\psi\phi : G \to K$ a homomorphism? If so, prove it and find its kernel. If not, find a counterexample.

Exercise 4.1.9. Revisit Theorem 4.1.14. Prove that for $n \in \mathbb{N}$, $\phi(g^n) = [\phi(g)]^n$.

Exercise 4.1.10. Prove Theorem 4.1.17.

Exercise 4.1.11. Revisit Theorem 4.1.18. Let $\phi : G \to G'$ be a homomorphism, and let H be a subgroup of G. Prove that $\phi(H)$ is a subgroup of G'.

Exercise 4.1.12. How many homomorphisms are there from $\mathbb{Z}_{45}$ to $\mathbb{Z}_{18}$? How many of these homomorphisms are onto?

Exercise 4.1.13. Revisit Theorem 4.1.18. Prove that the set $\phi(H) = \{\phi(h) \,|\, h \in H\}$ is a subgroup of G'.

Exercise 4.1.14. Revisit Theorem 4.1.18. Prove that if H is cyclic, then $\phi(H)$ is cyclic.

Exercise 4.1.15. Revisit Theorem 4.1.18. Prove that if H is Abelian, then $\phi(H)$ is Abelian.

Exercise 4.1.16. Revisit Theorem 4.1.18. Prove that if H' is a subgroup of G', then $\phi^{-1}(H') = \{h \in G \,|\, \phi(h) \in H'\}$ is a subgroup of G.

4.2 Isomorphisms

As we saw, a homomorphism can embed a smaller group *into* a larger group, as, for example, $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{20}$ does. Conversely, a homomorphism can

collapse a larger group *onto* a smaller group, as, for example, $\psi : \mathbb{Z}_{20} \to \mathbb{Z}_4$ does. Of course, a homomorphism can go between equally sized groups. Now we study a special type of a homomorphism, one that requires equally sized groups.

Definition 4.2.1. An isomorphism ϕ from a group G to a group G' is a bijective homomorphism.

We have already seen some examples of isomorphisms; nonetheless, we give a few more.

Example 4.2.2. The map $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = -x$ is an isomorphism, as we prove below. To show a function is an isomorphism, we must show it is operation preserving, one-to-one, and onto.

1. Operation preserving: For $x, y \in \mathbb{Z}$, we see that

$$\phi(x + y) = -(x + y) = -x - y = \phi(x) + \phi(y).$$

2. One-to-one: Assume $\phi(x) = \phi(y)$. By the definition of ϕ, this means that $-x = -y$. By cancellation, $x = y$.

3. Onto: Take $y \in \phi(\mathbb{Z})$, thus y is also an integer. We want to find some $x \in \mathbb{Z}$ such that $\phi(x) = y$. This means that we want to find some $x \in \mathbb{Z}$ such that $-x = y$, thus $x = -y$. Hence, for y in the image of ϕ, we can find $-y \in \mathbb{Z}$ such that $\phi(-y) = -(-y) = y$.

$\diamond$

Example 4.2.3. Define $\phi : \mathbb{Z}_4 \to U(10)$ by

$$0 \mapsto 1$$
$$1 \mapsto 3$$
$$2 \mapsto 9$$
$$3 \mapsto 7.$$

Then ϕ is an isomorphism. Compare the Cayley tables of $\mathbb{Z}_4$ and $U(10)$, as shown below. Notice that because 9 is mapped to by 2, we list 9 in the same row and column headers as 2 in the Cayley table of $\mathbb{Z}_4$.

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$U(10)$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

◇

Example 4.2.4. The map $\psi : U(10) \to \mathbb{Z}_4$ given by

$$1 \mapsto 0$$
$$3 \mapsto 1$$
$$7 \mapsto 3$$
$$9 \mapsto 2.$$

is also an isomorphism. ◇

Examples 4.2.3 and 4.2.4 lead us to the lemma and definition below.

Lemma 4.2.5. *If $\phi : G \to G'$ is an isomorphism from group G to group G', then $\phi^{-1} : G' \to G$ is also an isomorphism.*

Proof. Let $\phi : G \to G'$ is an isomorphism from group G to group G'. To prove that $\phi^{-1} : G' \to G$ is an isomorphism, we need to prove that ϕ^{-1} is operation preserving, one-to-one, and onto.

1. Operation preserving: For $x', y' \in G'$,

$$\phi^{-1}(x') = x \text{ and } \phi^{-1}(y') = y \tag{4.5}$$

for some $x, y \in G$. Then $\phi^{-1}(x')\phi^{-1}(y') = xy$. Applying ϕ to both sides, we see that

$$\phi(\phi^{-1}(x')\phi^{-1}(y')) = \phi(xy) = \phi(x)\phi(y)$$

because ϕ is an isomorphism and thus preserves the operation. By Equations 4.5,

$$\phi(x)\phi(y) = x'y'$$

and thus $\phi(\phi^{-1}(x')\phi^{-1}(y')) = x'y'$. Applying ϕ^{-1} to both sides, we see that

$$\begin{aligned} \phi^{-1}(\phi(\phi^{-1}(x')\phi^{-1}(y'))) &= \phi^{-1}(x'y') \\ \phi^{-1}(x')\phi^{-1}(y') &= \phi^{-1}(x'y') \end{aligned}$$

which shows that ϕ^{-1} is operation preserving.

2. One-to-one: With $\phi^{-1} : G' \to G$, we want to show that if $\phi^{-1}(x') = \phi^{-1}(y') \in G$, then $x' = y' \in G'$. By way of contradiction, assume $\phi^{-1}(x') = \phi^{-1}(y')$. Applying ϕ to both sides, we get $\phi(\phi^{-1}(x')) = \phi(\phi^{-1}(y'))$ and thus $x' = y'$.

3. Onto: Suppose $x \in G$. We want to find an element of G' that ϕ^{-1} maps to x. By construction, $\phi(x) \in G'$, thus $\phi^{-1}(\phi(x)) = x$. Therefore, ϕ^{-1} is onto.

□

Thus, if there exists an isomorphism from group G to group G', there also exists an isomorphism from G' to G. In this sense, we can think of there existing an isomorphism between groups G and G'.

Definition 4.2.6. If there exists an isomorphism between groups G and G', then we say G and G' are isomorphic and we write $G \approx G'$.

Thus, in Example 4.2.2, $\mathbb{Z} \approx \mathbb{Z}$, and in Example 4.2.3, $\mathbb{Z}_4 \approx U(10)$. Example 4.2.2 is just one example of the lemma below, whose proof is left as an exercise.

Lemma 4.2.7. *Let G be a group. Then $G \approx G$.*

We take Example 4.2.3 further below.

Example 4.2.8. Refer back to Example 4.2.3. Below are the Cayley tables of $\mathbb{Z}_4$ and $U(10)$.

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$U(10)$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

We can see from the Cayley tables that $\mathbb{Z}_4 \approx U(10)$. Now consider group $G = \{\bigcirc, \divideontimes, \odot, \sun\}$ under operation $*$ with the Cayley table below.

G	○	✳	☺	☼
○	○	✳	☺	☼
✳	✳	☺	☼	○
☺	☺	☼	○	✳
☼	☼	○	✳	☺

We can see from all three Cayley tables that $\mathbb{Z}_4 \approx U(10) \approx G$. ◇

This leads us to the lemma below, whose proof is left as an exercise.

Lemma 4.2.9. *Let G, H, and K be groups such that $G \approx H$ and $H \approx K$. Then $G \approx K$.*

Notice that Lemma 4.2.7 states that the relation "is isomorphic to" is reflexive. Lemma 4.2.5 states that "is isomorphic to" is symmetric. Lastly, Lemma 4.2.9 shows that "is isomorphic to" is a transitive relation. These lemmas prove the very, extremely, super duper useful theorem below.

Theorem 4.2.10. *The relation "is isomorphic to" is an equivalence relation.*

For this reason, for groups G and G', we can also notate $G \approx G'$ as $G \equiv G'$.

Theorem 4.2.10 means that isomorphic groups are equivalent groups. Let's take a moment to reflect on the depth of this relationship. Consider the following example. In modulo 37 arithmetic, $521 \equiv 3 \bmod 37$. Thus, if you were required to evaluate 521^3, you could instead evaluate 3^3. This is because, in modulo 37 arithmetic, 521 and 3 are *equivalent*. This type of "reduction calculation" is also possible between groups because isomorphic groups are equivalent. If you need to work within some group G, but find G to be too cumbersome, you can instead work with a group G' that is isomorphic to G. In a sense, isomorphisms give us a way to move relatively freely between groups.

We demonstrate these ideas with the example below. Note that to prove two groups are isomorphic, we must find an isomorphism between them.

Example 4.2.11. Consider the set

$$C = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

We will prove that $\mathbb{C}^* \approx C^*$ under multiplication. To do this, we must first find a function between $\mathbb{C}^*$ and C^*, and then show our function is indeed an isomorphism. On a hunch, we let $\phi : \mathbb{C}^* \to C^*$ be given by

$$\phi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

First, we show that ϕ is an isomorphism.

1. Operation preserving: Let $a + bi, c + di \in \mathbb{C}^*$. Then

$$\begin{aligned} \phi((a + bi) \cdot (c + di)) &= \phi((ac - bd) + (ad + bc)i) \\ &= \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix} \\ \phi(a + bi) \cdot \phi(c + di) &= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ &= \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix}. \end{aligned}$$

2. One-to-one: Suppose $\phi(a + bi) = \phi(c + di)$ for some $a + bi, c + di \in \mathbb{C}^*$. Then

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}.$$

   Thus, $a = c$ and $b = d$, which implies that $a + bi = c + di$.

3. Onto: Let
$$A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in C^*.$$
We see $\phi(a + bi) = A$.

Therefore, $\mathbb{C}^* \approx C^*$, meaning that these two groups are equivalent. Notice how we use this relationship to reduce the difficulty of our calculations.

- Typically, matrices do not commute under multiplication, which can make matrix calculations hard. The group $\mathbb{C}^*$ is Abelian, which tells us that C^* must also be Abelian. This will make our calculations in C^* easier.

- Suppose we needed to calculate
$$\left(\begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 6 & 2 \\ -2 & 6 \end{bmatrix} \right)^2.$$
Instead of multiplying these matrices, we know that under ϕ,
$$\begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix} \approx 4 + 3i \text{ and } \begin{bmatrix} 6 & 2 \\ -2 & 6 \end{bmatrix} \approx 6 - 2i,$$
thus we can instead perform the calculation below:
$$\begin{aligned} ((4 + 3i)(2 - 6i))^2 &= (4 + 3i)^2(6 - 2i)^2 \\ &= (7 + 24i)(32 - 24i) \\ &= 7 \cdot 32 - 7 \cdot 24i + 32 \cdot 24i - 24^2 i^2 \\ &= 800 - 600i. \end{aligned}$$

This tells us that

$$\left(\begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 6 & 2 \\ -2 & 6 \end{bmatrix}\right)^2 = \begin{bmatrix} 800 & -600 \\ 600 & 800 \end{bmatrix}$$

and we never performed any matrix multiplication.

- We know that $\mathbb{C}^*$ is not cyclic, that is, there is no complex number that generates all of the nonzero complex numbers. Therefore, we also know that there is no matrix that will generate all of C^*.

$\diamond$

The idea that isomorphisms can be used to show group equivalence can help us discover some rather counter-intuitive results. Consider the example below.

Example 4.2.12. Let $\eta : \mathbb{Z} \to 2\mathbb{Z}$ be given by $\eta(x) = 2x$. Then η is an isomorphism, as we show below.

1. Operation preserving: Take $x, y \in \mathbb{Z}$. Then

$$\eta(x + y) = 2(x + y) = 2x + 2y = \eta(x) + \eta(y).$$

2. One-to-one: Assume $\eta(x) = \eta(y)$ for some $x, y \in \mathbb{Z}$. Then $2x = 2y$, thus $x = y$.

3. Onto: The element $2x \in 2\mathbb{Z}$ is mapped to by $x \in \mathbb{Z}$ because $\eta(x) = 2x$.

Thus, $\mathbb{Z} \approx 2\mathbb{Z}$. In a sense, this means that the set of integers and the set of even integers are equivalent. One might find this counterintuitive, because it may seem as if $2\mathbb{Z}$ should be half the size of $\mathbb{Z}$. $\diamond$

Like with homomorphisms, we will study how isomorphisms act on group elements. As we see from the theorem below, these properties are much "nicer" than the properties of homomorphisms. A few of these properties we began to see in Example 4.2.11. Also, notice that any statement given as an implication is actually a biconditional, because inverse isomorphisms are also isomorphisms.

Theorem 4.2.13. *Suppose $\phi : G \to G'$ is an isomorphism from group G to group G', and let $g, h \in G$. Let $e \in G$ be the identity of G; let $e' \in G'$ be the identity of G'.*

1. *The identity maps to the identity, that is, $\phi(e) = e'$.*
2. *For $n \in \mathbb{Z}$, $\phi(g^n) = [\phi(g)]^n$.*
3. *Order is preserved, that is, $|g| = |\phi(g)|$.*
4. *If g is a generator of G, then $\phi(g)$ is a generator of G'.*
5. *If $gh = hg$, then $\phi(g)\phi(h) = \phi(h)\phi(g)$.*
6. *For $k \in \mathbb{Z}$ and variable x, the equations $x^k = g$ and $x^k = \phi(g)$ have the same number of solutions.*
7. *If G is finite, then G and G' have the same number of elements of each order.*

Proof. The proof of the first two properties is the same as the proof of these properties in Theorem 4.1.14.

For the third part of this theorem, we first assume $|g|$ is infinite, and by way of contradiction, we assume $|\phi(g)| = n$ is finite. Then $e' = \phi(g)^n = \phi(g^n)$ because ϕ preserves the operation. Further, if $\phi(g^n) = e'$, then $g^n = e$ by the first property. This implies that $|g| \leq n$, which is a contradiction.

Now assume that $|g| = m$ and $|\phi(g)| = n$ for some $m, n \in \mathbb{N}$. By the argument above, $|g| = m \leq n$. By similar logic, $e = g^m$, thus $e' = \phi(e) = \phi(g^m) = [\phi(g)]^m$. Thus, $|\phi(g)| = n \leq m$. Therefore, $|g| = |\phi(g)|$.

For the fourth part of this theorem, assume g is a generator of G, thus $G = \langle g \rangle$. By closure $\langle \phi(g) \rangle \subseteq G'$. Further, because ϕ is onto, for any element $h' \in G$, there exists $h \in G$ such that $\phi(h) = h'$. By our assumption, we know that $h = g^k$ for some $k \in \mathbb{Z}$, thus $h' = \phi(g^k) = [\phi(h)]^k$ because ϕ preserves the operation. Thus, we have shown that a random element in G' can be generated by $\phi(g)$. Ergo, $G = \langle \phi(g) \rangle$.

We assume $gh = hg$ to begin our proof of the fifth property. By operation preservation, $\phi(gh) = \phi(g)\phi(h)$ and $\phi(hg) = \phi(h)\phi(g)$. Thus, $\phi(g)\phi(h) = \phi(h)\phi(g)$.

For the sixth property, assume $x^k = g$. Then $\phi(x^k) = \phi(x)^k = \phi(g)$, and because x, and hence $\phi(x)$, is a random variable, we may write $\phi(x)^k = \phi(g)$ as $x^k = \phi(g)$. Assume a is a solution to $x^k = g$. Then, because ϕ is one-to-one, $\phi(a)$ is a solution to $x^k = \phi(g)$. This means that there are at least as many solutions to $x^k = \phi(g)$ as there are to $x^k = g$. Assume b' is a solution to $x^k = \phi(g)$, thus $(b')^k = \phi(g)$. Then, because ϕ is onto, there is a $b \in G$ such that $\phi(b) = b'$. By substitution, $\phi(g) = (b')^k = [\phi(b)]^k = \phi(b^k)$ and thus $g = b^k$. This shows that for every solution to $x^k = \phi(g)$, we have a solution to $x^k = g$. Ergo, the two equations have the same number of solutions.

The seventh property is left as an exercise. □

We will use these properties in two main ways.

1. When two groups are isomorphic, we may study the properties of one group to better understand the other.

2. We will use these properties in proofs that two groups are not isomor-

phic.

Property 6, in particular, can be useful in showing that two groups are not isomorphic.

Example 4.2.14. Consider the equation $x^2 = -1$. In $\mathbb{R}^*$, there are no solutions to this equation. In $\mathbb{C}^*$, there are two solutions to this equation. Thus, by Property 6 of Theorem 4.2.13, $\mathbb{R}^* \not\approx \mathbb{C}^*$. $\diamond$

By the definition of isomorphic, if two groups G and G' are *not* isomorphic, that means that *there does not exist* an isomorphism between G and G'. Note that this is a much stronger statement than simply saying that some function $f : G \to G'$ is not an isomorphism. To prove G and G' are not isomorphic, we must prove that it is impossible to construct an isomorphism between them. The strategy to prove that no such isomorphism exists is to assume, by way of contradiction, that an isomorphism does exist. Then use that assumption to contradict a known property of isomorphisms.

Non-Example 4.2.15. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2 + 1$. Then f is not an isomorphism. The identity does not map to the identity, as $f(0) = 1 \neq 0$. Further, f is not onto, as the image contains only positive integers, that is, $f(\mathbb{Z}) \subseteq \mathbb{N}$.

If we were attempting to show that $\mathbb{Z} \approx \mathbb{Z}$, this f *does not* prove that $\mathbb{Z} \not\approx \mathbb{Z}$. We know this idea to be absurd, as well have already shown $\mathbb{Z} \approx \mathbb{Z}$ and, moreover, a group is isomorphic to itself. Thus, if we were attempting to show $\mathbb{Z} \approx \mathbb{Z}$, all we have shown is that f is not an isomorphism, and that we must keep searching for an isomorphism. $\diamond$

Now that we know some properties of how isomorphisms act on elements, we study how isomorphisms act on groups. Again, notice that any statement given as an implication is actually a biconditional, because inverse isomor-

phisms are also isomorphisms.

Theorem 4.2.16. *Suppose $\phi : G \to G'$ is an isomorphism from group G to group G'.*

1. *If G is Abelian, then G' is Abelian.*
2. *If G is cyclic, then G' is cyclic.*
3. *If H is a subgroup of G, then $\phi(H)$ is a subgroup of G'.*
4. *The center maps to the center, that is, $\phi(Z(G)) = Z(G')$.*

The proofs of these properties are left as exercises.

As we know from Lemma 4.2.7, a group is isomorphic to itself. In Example 4.2.2, we saw that $\phi(x) = -x$ is an isomorphism on $\mathbb{Z}$. Further, $\psi(x) = x$ is also an isomorphism on $\mathbb{Z}$. Thus, we can already see that there may be several isomorphisms from a group to itself. This leads us to the definition and theorem below.

Definition 4.2.17. An isomorphism from a group to itself is an automorphism.

Theorem 4.2.18. *The set of automorphisms of a group, denoted $\mathsf{Aut}(G)$, is a group.*

How meta. We just defined a group based on isomorphisms acting on some other group.

Example 4.2.19. We will determine $\mathsf{Aut}(\mathbb{Z}_{12})$. We know $\mathbb{Z}_{12}$ is cyclic, thus it has a generator. By property 3 of Theorem 4.2.13, we know that isomorphisms preserve order, thus we must map generators to generators.

By Corollary 3.6.22, we know that the generators of $\mathbb{Z}_{12}$ are exactly the numbers in $U(12)$, thus $\mathbb{Z}_{12}$ has generators 1, 5, 7, and 11. Therefore, our isomoprhism should map the generator 1 to 1, 5, 7, or 11. Now we analyze each of these possibilities.

Let ϕ_i be the function with mapping $\phi_i(1) = i$. The mapping ϕ_1 is the identity mapping $\phi(x) = x$. This is an isomorphism. The mapping ϕ_5 is the mapping $\phi_5(x) = 5x$. It is operation preserving because

$$\phi_5(x + y) = 5(x + y) = 5x + 5y = \phi_5(x) + \phi_5(y).$$

Suppose $\phi_5(x) = \phi_5(y)$ for some $x, y \in \mathbb{Z}_{12}$. Then $5x = 5y$, and because $5^{-1} = 5$ in $\mathbb{Z}_{12}$, by multiplying on the left by 5, we see that $x = y$. Thus, ϕ_5 is one-to-one. Lastly, consider $x \in \mathbb{Z}_{12}$. Again, because $5^{-1} = 5$ and $5x \bmod 12 \in \mathbb{Z}_{12}$, we see that $\phi_5(5x) = 5 \cdot 5x = x$. Thus, ϕ_5 is onto. In conclusion, $\phi_5 \in \mathsf{Aut}(\mathbb{Z}_{12})$. Without loss of generality, $\phi_7, \phi_{11} \in \mathsf{Aut}(\mathbb{Z}_{12})$. $\diamond$

This example may lead you to the conclusion below, whose proof is left as an exercise.

Theorem 4.2.20. *For every $n \in \mathbb{N}$ such $n \geq 2$, $\mathsf{Aut}(\mathbb{Z}_n) \approx U(n)$.*

How meta. We just said a group of isomorphisms is isomorphic to another group. Mind. Blown.

EXERCISES

Exercise 4.2.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let $\phi : G \to G'$ be an isomorphism from group G to group G'.

a. $\phi(Z(G)) = Z(G')$

b. $|G| = |G'|$

c. $|\ker(\phi)| = 1$

Exercise 4.2.2. Consider the dihedral groups and the symmetric groups. For each of the following, determine if the two groups given are isomorphic. If so, prove it. If not, explain why not.

a. D_3 and S_3.

b. D_4 and S_4.

c. D_{12} and S_4.

Exercise 4.2.3. Consider the following groups of units.

a. Show that $U(8)$ and $U(10)$ are not isomorphic.

b. Show that $U(8)$ and $U(12)$ are isomorphic.

c. To which of these group(s) is $U(5)$ isomorphic? Justify your response.

Exercise 4.2.4. Let $H = \{\alpha \in S_4 \,|\, \alpha(1) = 1\}$ and $K = \{\alpha \in S_4 \,|\, \alpha(2) = 2\}$.

a. Find an isomorphism between H and K. Justify your isomorphism by creating symmetric Cayley tables for H and K.

b. To which familiar group are H and K isomorphic?

Exercise 4.2.5. Prove Lemma 4.2.7, that is, for any group G, $G \approx G$.

Exercise 4.2.6. Prove Lemma 4.2.9, that is, if G, H, and K be groups such that $G \approx H$ and $H \approx K$, then $G \approx K$.

Exercise 4.2.7. Revisit Example 4.2.11. Prove that $\mathbb{C} \approx C$.

Exercise 4.2.8. Let $\mathbb{R}^+$ be the group of positive real numbers under multiplication.

a. Prove that $\phi : \mathbb{R}^+ \to \mathbb{R}$ defined by $\phi(x) = \ln(x)$ is an isomorphism.

b. Prove that $\psi : \mathbb{R} \to \mathbb{R}^+$ defined by $\psi(x) = e^x$ is an isomorphism.

c. This shows that $\mathbb{R}^+ \equiv \mathbb{R}$. In a sentence or two, why is this a somewhat counter-intuitive result?

(Hint: Lemma 4.2.5 should cut your work in half.)

Exercise 4.2.9. Revisit Example 4.2.12. Prove that $\mathbb{Z}$ has infinitely many subgroups to which it is isomorphic.

Exercise 4.2.10. Let $\phi : G \to G'$ be an isomorphism, and assume G is finite. Prove that G and G' have the same number of elements of each order.

Exercise 4.2.11. Suppose $\phi : G \to G'$ is an isomorphism from group G to group G'. Prove the following.

a. If H is a subgroup of G, then $\phi(H)$ is a subgroup of G'.

b. If H' is a subgroup of G', then $\phi^{-1}(H')$ is a subgroup of G.

(Hint: Lemma 4.2.5 should cut your work in half.)

Exercise 4.2.12. Suppose $\phi : G \to G'$ is an isomorphism from group G to group G'. Prove the following.

a. If G is Abelian, then G' is Abelian.

b. If G is cyclic, then G' is cyclic.

Exercise 4.2.13. Suppose $\phi : G \to G'$ is an isomorphism from group G to group G'. Prove that $\phi(Z(G)) = Z(G')$.

Exercise 4.2.14. Prove that $\mathbb{Z} \not\approx \mathbb{Q}$.

Exercise 4.2.15. Let G be a group. Prove that $\phi(x) = x^{-1}$ is an automorphism if and only if G is Abelian.

Exercise 4.2.16. Find $\mathsf{Aut}(\mathbb{Z})$. Justify your answer.

Exercise 4.2.17. Find two groups G and H such that $G \not\approx H$ and $\mathsf{Aut}(G) \approx \mathsf{Aut}(H)$.

Exercise 4.2.18. Let ϕ be an automorphism of group G. Prove that

$$H = \{g \in G \mid \phi(g) = g\}$$

is a subgroup of G.

Exercise 4.2.19. Suppose ϕ is an automorphism of $\mathbb{Z}_{24}$ such that $\phi(6) = 6$. Find all the possibilities of $\phi(x)$. Justify your answer.

Exercise 4.2.20. Prove Theorem 4.2.18.

Exercise 4.2.21. Prove Theorem 4.2.20.

Chapter 5

Lagrange's Theorem

Lagrange, in one of the later years of his life,
imagined that he had overcome the difficulty [*of the parallel axiom*]*.*
He went so far as to write a paper, which he took with him to the Institute,
and began to read it. But in the first paragraph
something struck him that he had not observed.
He muttered, "Il faut que j'y songe encore," and put the paper in his pocket.
[*I must think about it again.*]
Augustus De Morgan

Lagrange's Theorem is, perhaps, the most important theorem in group theory. To say it is a fundamental theorem would be an understatement. Like some of the most beautiful pieces of mathematics, it is a seemingly simple theorem, one you can appreciate immediately. Of course, it is not so simple, because it has taken us several chapters to be ready to understand its proof. We are not quite ready, as we need a few more definitions.

5.1 Cosets

Cosets provide powerful tools in group theory. Before we define them, we give an example of cosets, which should help us parse the definitions that follow.

Example 5.1.1. Consider the group S_3 and its subgroup $H = \{e, (23)\}$. We multiply H by each element in S_3, one at a time, that is, for all $\sigma \in S_3$, we determine $\sigma H = \{\sigma h \,|\, h \in H\}$.

$$\begin{aligned} eH &= \{ee, e(23)\} = \{e, (23)\} \\ (12)H &= \{(12)e, (12)(23)\} = \{(12), (123)\} \\ (13)H &= \{(13)e, (13)(23)\} = \{(13), (132)\} \\ (23)H &= \{(23)e, (23)(23)\} = \{(23), e\} \\ (123)H &= \{(123)e, (123)(23)\} = \{(123), (12)\} \\ (132)H &= \{(132)e, (132)(23)\} = \{(132), (13)\} \end{aligned}$$

Notice that $H = eH = (23)H$ because e and (23) are the elements of H. Thus, when we compute eH and $(23)H$, we get H back. Also notice that $(12)H = (123)H$ and, moreover, $(123) \in (12)H$ and $(12)H$. Similarly, $(13)H = (132)H$, $(132) \in (13)H$, and $(13) \in (132)H$. Notice that every element of S_3 is in exactly on of these sets, that is, these sets partition S_3. Further, notice that each set is the same size.

Of course, S_3 is non-Abelian, thus multiplying on the left is potentially different than multiplying on the right. Below we perform similar computations,

only this time, for all $\sigma \in S_3$, we determine $H\sigma = \{h\sigma \mid h \in H\}$.

$$\begin{aligned} He &= \{ee, (23)e\} = \{e, (23)\} \\ H(12) &= \{e(12), (23)(12)\} = \{(12), (132)\} \\ H(13) &= \{e(13), (23)(13)\} = \{(13), (123)\} \\ H(23) &= \{e(23), (23)(23)\} = \{(23), e\} \\ H(123) &= \{e(123), (23)(123)\} = \{(123), (13)\} \\ H(132) &= \{e(132), (23)(132)\} = \{(132), (12)\} \end{aligned}$$

Again, we see that multiplying by the elements of H recreates H, that is, $H = He = H(23)$. Again, we have some repeat sets: $H(12) = H(132)$ and $H(13) = H(123)$. Again, these sets partition S_3 and all have the same size.

There are some important differences between σH and $H\sigma$, though. For example, notice that when we multiply H on the left by (12), we get $(12)H = (123)H$, and when we multiply H on the right by (12), we get $H(12) = H(132)$. Thus, we see that σH is not always equal to $H\sigma$. For which elements $\sigma \in S_3$ is it true that $\sigma H = H\sigma$? $\diamond$

The example above demonstrates both left and right cosets. The definitions of these objects, and related definitions, are given below.

Definition 5.1.2. Let G be a group and H a subgroup of G. For $a \in G$, the set

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

is a left coset in G, in particular, it is the left coset in G containing a. Similarly, for $a \in G$, the set

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

is a right coset in G, in particular, it is the right coset in G containing a. In

both situations, the element a is called the coset representative because it is the element used to create the coset.

As we saw in Example 5.1.1, left and right cosets are not always equal. Below is another example of cosets in a non-Abelian group.

Example 5.1.3. Consider the group D_4 and its subgroup $K = \{R_0, V\}$. Below are the left cosets of K in D_4.

$$\begin{aligned} R_0K &= \{R_0R_0, R_0V\} = VK \\ R_{90}K &= \{R_{90}R_0, R_{90}V\} = D_LK \\ R_{180}K &= \{R_{180}R_0, R_{180}V\} = HK \\ R_{270}K &= \{R_{270}R_0, R_{270}V\} = D_RK \end{aligned}$$

Once again, notice that for coset representatives not in K itself, the left cosets do not equal the right cosets, shown below.

$$\begin{aligned} KR_0 &= \{R_0R_0, VR_0\} = KV \\ KR_{90} &= \{R_0R_{90}, VR_{90}\} = KD_R \\ KR_{180} &= \{R_0R_{180}, VR_{180}\} = KH \\ KR_{270} &= \{R_0R_{270}, VR_{270}\} = KD_R \end{aligned}$$

$\diamond$

When a group is Abelian, the left cosets are equal to the right cosets. Below are some examples of cosets in Abelian groups.

Example 5.1.4. Consider the group $\mathbb{Z}$ and its subgroup $5\mathbb{Z}$. Below are the cosets of $5\mathbb{Z}$ in $\mathbb{Z}$, and note that the cosets are written in additive notation

because the operation on $\mathbb{Z}$ is addition.

$$0 + 5\mathbb{Z} = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, \ldots\} = 5\mathbb{Z} + 0 = 5\mathbb{Z}$$
$$1 + 5\mathbb{Z} = \{\ldots, -19, -14, -9, -4, 1, 6, 11, 16, \ldots\} = 5\mathbb{Z} + 1$$
$$2 + 5\mathbb{Z} = \{\ldots, -18, -13, -8, -3, 2, 7, 12, 17, \ldots\} = 5\mathbb{Z} + 2$$
$$3 + 5\mathbb{Z} = \{\ldots, -17, -12, -7, -2, 3, 8, 13, 18, \ldots\} = 5\mathbb{Z} + 3$$
$$4 + 5\mathbb{Z} = \{\ldots, -16, -11, -6, -1, 4, 9, 14, 19, \ldots\} = 5\mathbb{Z} + 4$$

Notice that coset representatives are not unique. For example, the following are just different representations of the coset $1 + 5\mathbb{Z}$.

$$-9 + 5\mathbb{Z} = \{\ldots, -24, -19, -14, -9, -4,1, 6, 11, \ldots\}$$
$$-4 + 5\mathbb{Z} = \{\ldots, -19, -14, -9, -4,1, 6, 11, 16, \ldots\}$$
$$1 + 5\mathbb{Z} = \{\ldots, -19, -14, -9, -4,1, 6, 11, 16, \ldots\}$$
$$6 + 5\mathbb{Z} = \{\ldots, -14, -9, -4,1, 6, 11, 16, 21, \ldots\}$$
$$11 + 5\mathbb{Z} = \{\ldots, -9, -4,1, 6, 11, 16, 21, 26 \ldots\}$$

$\diamond$

As the above example illustrates, there are many ways to represents a single coset. Further, even in an infinite group, there may be a finite number of cosets. This leads us to the definition below.

Definition 5.1.5. Let G be a group and H a subgroup of G. The number of left (or right) cosets of H in G is the index of H in G, denoted $|G : H|$.

In Example 5.1.1, $|G : H| = 5$. In Example 5.1.4, $|G : H| = 5$.

Cosets form many patterns, as you may have begun to observe. Below are some properties of cosets that describe those patterns. Theorem 5.1.6 is written about left cosets, and analogous results hold for right cosets.

Theorem 5.1.6. *Let G be a group, H a subgroup of G, and $a, b \in G$.*

1. *The coset representative is in the coset, that is, $a \in aH$.*
2. *The coset $aH = H$ if and only if $a \in H$.*
3. *Associativity holds, that is, $(ab)H = a(bH)$.*
4. *The coset $aH = bH$ if and only if $a \in bH$.*
5. *Cosets partition the group, that is, every element is in a coset and either $aH = bH$ or $aH \cap bH = \varnothing$.*
6. *The coset $aH = bH$ if and only if $a^{-1}b \in H$.*
7. *The coset aH is a subgroup if and only if $a \in H$.*
8. *All cosets have equal cardinality, that is, $|aH| = |bH|$.*

Proof. Let G be a group, H a subgroup of G, and $a, b \in G$.

1. By definition of a subgroup $e \in H$ and therefore $ae = a \in aH$.
2. First, assume $aH = H$. By the first property, $a \in aH$, thus $a \in H$. Next, assume $a \in H$. By closure, $ah \in H$ for all $h \in H$, thus $aH \subseteq H$. To show $H \subseteq aH$, notice that for all $h \in H$, $a^{-1}h \in H$. Thus

$$h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$$

because $a^{-1}h \in H$. Therefore, $H \subseteq aH$, and ergo $aH = H$.

3. By the definition of a group, $(ab)h = a(bh)$ for all $a, b, h \in G$.

4. First, assume $aH = bH$. By the first property, $a \in aH$, thus $a \in bH$. Next, assume $a \in bH$. Then $a = bh$ for some $h \in H$. Thus, $aH = bhH$. By the second property, because $h \in H$, $bhH = bH$. By transitivity of equality, $aH = bH$.

5. By the first property, $a \in aH$, thus every element is in a coset. By the fourth property, $c \in aH \cap bH$ if and only if $cH = aH$ and $cH = bH$. Thus, $aH \cap bH$ is nonempty if and only if $aH = bH$.

6. By the fourth property, $aH = bH$ if and only if $a \in bH$. Further, $a \in bH$ if and only if $a = bh$ for some $h \in H$, that is, $e = a^{-1}bh$. We know $e = a^{-1}bh \in H$, and by the second property, this is true if and only if $H = a^{-1}bhH = a^{-1}bH$ because $h \in H$.

7. First, assume aH is a subgroup. Thus, $e \in aH$. By the fifth property, because $e \in H \cap aH$, $H = aH$. By the second property, $a \in H$. The argument reverses.

8. Consider the mapping $aH \to bH$ given by $ah \mapsto bh$ for all $ah \in aH$. This is a one-to-one mapping because if $bh_1 = bh_2$, by cancellation, $h_1 = h_2$ and hence $ah_1 = ah_2$. Therefore, because the mapping is one-to-one, $|aH| = |bH|$.

□

As Theorem 5.1.6 shows, if we compute aH for every $a \in G$, where H is a subgroup of group G, we will have redundancies. Thus, it is not practical to find all cosets by exhausting all representatives. Below is an example of a more practical approach to computing cosets.

Example 5.1.7. Consider the group $U(20)$ and its subgroup $H = \{1, 11\}$. We know by property (1) of Theorem 5.1.6 that $H = 11H$ is a coset. By property (5), these are the only representations of this coset and, further, we can find another coset by choosing a representative not in H. By choosing representative 3, we see that $3H = \{3, 13\}$. We continue to find cosets by choosing representatives not already in a coset. Thus, we get the following cosets.

$$\begin{aligned} H = 11H &= \{1, 11\} \\ 3H = 13H &= \{3, 13\} \\ 7H = 17H &= \{7, 17\} \\ 9H = 19H &= \{9, 19\} \end{aligned}$$

◇

Example 5.1.8. Ⓢ Let's study a group with symbols to see how coset properties hold, because numbers are really just symbols. Consider the group $J = \{\heartsuit, \☺, \☽, \bigstar, \☎, \clubsuit\}$. Below is the Cayley Table for group J, so that we can determine what the identity is and understand what different compositions will yield.

J	♡	☺	☽	★	☎	♣
♡	♡	☺	☽	★	☎	♣
☺	☺	☽	♡	♣	★	☎
☽	☽	♡	☺	☎	♣	★
★	★	☎	♣	♡	☺	☽
☎	☎	♣	★	☽	♡	☺
♣	♣	★	☎	☺	☽	♡

By observing the Cayley Table, we see that ♡ is the identity. In group J, let

$W = \{\heartsuit, \bigstar\}$, which is a subgroup. The right and left cosets of W are listed below.

$$\heartsuit W = \{\heartsuit\heartsuit, \heartsuit\bigstar\} = \{\heartsuit, \bigstar\} \qquad W\heartsuit = \{\heartsuit\heartsuit, \bigstar\heartsuit\} = \{\heartsuit, \bigstar\}$$
$$\☺ W = \{\☺\heartsuit, \☺\bigstar\} = \{\☺, \☎\} \qquad W\☺ = \{\heartsuit\☺, \bigstar\☺\} = \{\☺, \clubsuit\}$$
$$\jmath W = \{\,\jmath\heartsuit,\ \jmath\bigstar\} = \{\,\jmath, \clubsuit\} \qquad W\,\jmath = \{\heartsuit\,\jmath, \bigstar\,\jmath\} = \{\,\jmath, \☎\}$$

Notice that using the subgroup W, we created three unique left and right cosets. In this example we are able to see that $\heartsuit W = W\heartsuit$, and only coset representatives from W generate equal left and right cosets. Notice that $\☺ W \neq W\☺$ and $\jmath W \neq W\,\jmath$. This is because J is not a commutative group. Thus we can see from the example that not all left and right cosets will necessarily be equal to one another. ◇

Cosets may seem random at first, but they provide a lot of structure. In a sense, cosets allow us to partition a group into sets based on some desirable quality. Consider the following example.

Example 5.1.9. Consider the group $\mathsf{GL}(2,\mathbb{R})$ and its subgroup $\mathsf{SL}(2,\mathbb{R})$. Recall that the operation on these groups is multiplication. Then the cosets of $\mathsf{SL}(2,\mathbb{R})$ in $\mathsf{GL}(2,\mathbb{R})$ have form $c\mathsf{SL}(2,\mathbb{R})$ for $c \in \mathbb{R}^*$. Notice that the set $c\mathsf{SL}(2,\mathbb{R})$ is the set of all matrices of determinant c. Thus, in this way, cosets give us a way to categorize all matrices based on their determinants. ◇

In particular, because the kernel of a homomorphism is a subgroup, cosets help us understand more about homomorphisms.

Theorem 5.1.10. *Let $\phi : G \to G'$ be a homomorphism from group G to group G'.*

1. *For $a, b \in G$, $\phi(a) = \phi(b)$ if and only if $a\ker(\phi) = b\ker(\phi)$.*

2. *For $a \in G$, if $\phi(a) = a'$, then $\phi^{-1}(a') = a\ker(\phi)$.*

Proof. Let $\phi : G \to G'$ be a homomorphism from group G to group G' and $a, b \in G$. For the first property, assume $\phi(a) = \phi(b)$. Then

$$e = (\phi(a))^{-1}\phi(b) = \phi(a^{-1})\phi(b) = \phi(a^{-1}b)$$

because ϕ is a homomorphism. By property (6) of Theorem 5.1.6, $a\ker(\phi) = b\ker(\phi)$. This argument reverses.

For the second property, assume $\phi(a) = a'$ for some $a' \in G$. Then

$$\phi^{-1}(a') = \{g \in G \mid \phi(g) = a'\}.$$

To show set equality, first assume $g \in \phi^{-1}(a')$, thus $\phi(g) = a'$. Thus, $\phi(a) = \phi(g)$, and by the previous property, $a\ker(\phi) = g\ker(\phi)$. By property (4) of Theorem 5.1.6, $g \in a\ker(\phi)$. Hence $\phi^{-1}(a') \subseteq a\ker(\phi)$. For the reverse set inclusion, assume $k \in \ker(\phi)$. Then

$$\phi(ak) = \phi(a)\phi(k) = \phi(a) = a'.$$

Therefore, $ak \in \phi^{-1}(a')$, and note that by the definition of coset, $ak \in a\ker(\phi)$. Hence, $a\ker(\phi) \subseteq \phi^{-1}(a')$, and ergo $a\ker(\phi) = \phi^{-1}(a')$. □

Property (1) of Theorem 5.1.10 gives us a way to find which elements map to the same place without determining to where those elements actually map. Property (2) give us a way to determine all the elements that map to a given $a' \in G'$ once we know one element in G that maps to a'. Below is an example of how to use these properties in computations.

Example 5.1.11. The mapping $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_4$ given by $\phi(x) = x \bmod 4$ is

a homomorphism. Then

$$\ker(\phi) = \{x \in \mathbb{Z}_{20} \mid x = 0 \bmod 4\} = \{0, 4, 8, 12, 16\} = \langle 4 \rangle.$$

The operation on $\mathbb{Z}_{20}$ is addition, thus we will write the cosets additively. Consider the element $a = 17 \in \mathbb{Z}_{20}$.

1. Which elements map to the element $\phi(17) \in \mathbb{Z}_4$? For $b \in \mathbb{Z}_{20}$, we know $\phi(17) = \phi(b)$ if and only if $17 + \ker(\phi) = b + \ker(\phi)$. By property (4) of Theorem 5.1.6, this is true if and only if $b \in 17 + \ker(\phi)$. By computation, we see that

   $$17 + \ker(\phi) = \{17, 1, 5, 9, 13\}.$$

   Thus, we may conclude that 1, 5, 9, and 13 also map to $\phi(17)$. Note that we never had to determine to which element 17 actually maps.

2. Which elements map to $3 \in \mathbb{Z}_4$? Certainly, $3 \in \mathbb{Z}_{20}$ maps to $3 \in \mathbb{Z}_4$. Then the set of all elements that map to $3 \in \mathbb{Z}_4$ is

   $$\phi^{-1}(3) = 3 + \ker(\phi) = \{3, 7, 11, 15, 19\}.$$

   Thus, we determined all elements that map to 3 by only knowing $3 \mapsto 3$.

◇

Example 5.1.12. Ⓢ Let the map of $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ be a homomorphism defined by $\phi(22) = 29$ with $\ker(\phi) = \langle 5 \rangle$. By applying Theorem 5.2, we know elements that also map to 29 are $2, 7, 12, 17$, and 27. ◇

Though cosets are not mentioned in the theorem below, we use cosets to prove it.

Theorem 5.1.13. *Let $\phi : G \to G'$ be a homomorphism, and let H be a subgroup of G.*

1. *If $|\ker(\phi)| = n$, then ϕ is an n-to-one mapping.*
2. *If $|H| = n$, then $|\phi(H)|$ divides n.*
3. *If ϕ is onto and $\ker(\phi)$ is the subgroup of the identity, then ϕ is an isomorphism.*

Proof. Let $\phi : G \to G'$ be a homomorphism, and let H be a subgroup of G.

1. Assume $|\ker(\phi)| = n$. By property (8) in Theorem 5.1.6, all cosets have the same size, thus all cosets have size $|\ker(\phi)| = n$. By property (2) in Theorem 5.1.10, when $\phi(a) = a'$, $\phi^{-1}(a') = a\ker(\phi)$. Thus, $|\phi^{-1}(a')| = n$ for all $a' \in G'$, which means ϕ is an n-to-one mapping.
2. Let ϕ_H be the restriction of ϕ that acts only on H, that is, $\phi_H : H \to \phi(H)$. Then ϕ_H is a homomorphism, and moreover, it is onto $\phi(H)$. Suppose $|\ker(\phi_H)| = m$. By the previous result, ϕ_H is an m-to-one mapping. Thus $|\phi_H|m = |H|$, and therefore $|\phi_H|$ divides $|H| = n$.
3. If $\ker(\phi)$ is the subgroup of the identity, then by the first property, ϕ is one-to-one. If ϕ is also onto, then ϕ is an isomorphism by definition.

□

We continue with the homomorphism established in Example 5.1.11 to demonstrate the properties in Theorem 5.1.13.

Example 5.1.14. Let $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_4$ be the homomorphism from Example 5.1.11. We know that $|\ker(\phi)| = 5$, thus ϕ is a five-to-one mapping. This

means that for each element in $g \in \mathbb{Z}_4$, five elements from $\mathbb{Z}_{20}$ map to that element g.

Let $H = \langle 2 \rangle \in \mathbb{Z}_{20}$, then $|H| = 10$. By computation, we see that $\phi(H) = \{0, 2, 4, 6, 8\} = \langle 2 \rangle \leq \mathbb{Z}_4$. Thus, $|\phi(H)|$ divides $|H|$. $\diamond$

EXERCISES

Exercise 5.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let G be a group and H a subgroup of G.

a. For $a \in G$, $aH = Ha$.

Exercise 5.1.2. Let $H = \{e, (13), (24), (13)(24)\}$.

a. Find the left cosets of H in S_4.

b. Find the right cosets of H in S_4.

Exercise 5.1.3. Let $H = \langle 6 \rangle \leq \mathbb{Z}$.

a. Find the left cosets of H in $\mathbb{Z}$.

b. Are the cosets $23 + H$ and $35 + H$ equal? Why?

c. Are the cosets $14 + H$ and $42 + H$ equal? Why?

d. Are the cosets $-17 + H$ and $11 + H$ equal? Why?

Exercise 5.1.4. For $n \in \mathbb{N}$, let $H = \langle n \rangle \leq \mathbb{Z}$. How many left cosets of H are there in $\mathbb{Z}$?

Exercise 5.1.5. Find all the left cosets of $H = \{1, 11\}$ in $U(30)$.

Exercise 5.1.6. Suppose $a \in G$ and $|a| = 30$. For each of the following subgroups, find all of the left cosets of the subgroup in $\langle a \rangle$.

a. $\langle a^6 \rangle$

b. $\langle a^{16} \rangle$

c. $\langle a^{25} \rangle$

d. $\langle a^{27} \rangle$

Exercise 5.1.7. Let G be an Abelian group, $a \in G$, and H a subgroup of G. Prove that $aH = Ha$.

Exercise 5.1.8. Prove that "is in the same coset as" is an equivalence relation.

Exercise 5.1.9. Let $H = \{a + bi \in \mathbb{C}^* \mid a^2 + b^2 = 1\}$ be a subset of $\mathbb{C}^*$.

a. Prove H is a subgroup of $\mathbb{C}^*$.

b. If you graph H on the complex plane, what will be the shape of the graph?

c. Give a geometric description of the coset $(4 + 3i)H$.

d. Find another coset representative of $(4 + 3i)H$.

Exercise 5.1.10. Suppose $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{50}$ is a homomorphism such that $\phi(37) = 45$ and $\ker(\phi) = \langle 10 \rangle$. Determine all the elements that also map to 45.

Exercise 5.1.11. Let $\phi : \mathbb{Z}^2 \to \mathbb{Z}$ be given by $\phi((x, y)) = x - y$.

a. Prove that ϕ is a homomorphism.

b. Find $\ker(\phi)$.

c. Describe the set $\phi^{-1}(1)$.

d. Describe the coset $(2, 5) + \ker(\phi)$.

e. Find another coset representative of $(2, 5) + \ker(\phi)$.

Exercise 5.1.12. Let H and K be subgroups of group G. Let $g \in G$. Prove that $g(H \cap K) = gH \cap gK$.

5.2 Lagrange's Theorem

In your algebraic heart of hearts, you may already realize Lagrange's Theorem. Indeed, we have already seen its restriction to cyclic groups. Note that Lagrange's Theorem applies to *all* finite groups, and is therefore a very strong theorem.

Theorem 5.2.1 (Lagrange's Theorem)**.** *Let G be a finite group and H a subgroup of G. Then $|H|$ divides $|G|$, and moreover, $|G : H| = |G|/|H|$.*

Proof. Let G be a finite group and H a subgroup of G. We know that G is finite, thus there are a finite number of cosets of H. Assume there are k distinct cosets of H in G. Let a_i for $1 \leq i \leq k$ be coset representatives of the k distinct cosets of H in G. By property 5 of Theorem 5.1.6, these cosets partition G, thus

$$G = a_1H \cup \cdots \cup a_kH.$$

Further, these cosets are disjoint, thus

$$|G| = |a_1H| + \cdots + |a_kH|.$$

By property 8 of Theorem 5.1.6, these cosets all have the same cardinality, thus

$$|G| = \sum_{i=1}^{k} |a_iH| = k|H|.$$

Therefore, $|H|$ divides $|G|$. Further, k, index of H in G, is $|G|/|H|$. □

We have already seen many examples of Lagrange's Theorem. Take a moment to look back to your favorite subgroups of finite groups to determine some examples of Lagrange's Theorem.

Example 5.2.2. Let G be a group of order $3^2 \cdot 5 \cdot 7$ and let H be a subgroup of G. Then H has order 1, 3, 3^2, $3 \cdot 5$, $3^2 \cdot 5$, $3 \cdot 7$, $3^2 \cdot 7$, $3 \cdot 5 \cdot 7$, or $3^2 \cdot 5 \cdot 7$. $\diamond$

Lagrange's Theorem has some immediate corollaries, the proofs of which are left as exercises.

Corollary 5.2.3. *In a finite group, the order of the element divides the order of the group.*

Example 5.2.4. Ⓢ We will prove that a group of order 16 must have an element of order 2.

Suppose we have a group G and $|G| = 16$, and consider some $a \in G$. By Corollary 5.1, $|a|$ must divide $|G|$. Thus, $|a| = 1, 2, 4, 8$, or 16. Thus, we proceed with the following 5 cases.

- Case 1: If $|a| = 1$, then a is the identity e of G and $\langle e \rangle = \{e\}$. Thus, we can not construct an element of order two using only this a, though there 15 other elements to consider.
- Case 2: If $|a| = 16$, then

  $$\langle a \rangle = \{e, a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, a^{15}\}$$

  and $|\langle a \rangle| = 16$. Notice that $|a^8| = 2$.
- Case 3: If $|a| = 8$, then $\langle a \rangle = \{e, a^1, a^2, a^3, a^4, a^5, a^6, a^7\}$ and $|\langle a \rangle| = 8$. Notice $|a^4| = 2$.
- Case 4: If $|a| = 4$, then $\langle a \rangle = \{e, a^1, a^2, a^3\}$ and $|\langle a \rangle| = 4$. Notice $|a^2| = 2$.
- Case 5: If $|a| = 2$, then we are done.

Thus, for each possibility of $|a| \neq 1$, we have shown that there is an element with order 2. In conclusion, a group of order 16 must have an element of order 2. $\diamond$

Corollary 5.2.5. *A group of prime order is cyclic.*

Corollary 5.2.6. *Let G be a group with identity e. Then for every $a \in G$, $a^{|G|} = e$.*

Another corollary of Lagrange's Theorem is Fermat's Little Theorem, a theorem you may have proved in your Number Theory class.

Corollary 5.2.7 (Fermat's Little Theorem)**.** *For every $a \in \mathbb{Z}$ and every prime p, $a^p \equiv a \bmod p$.*

Proof. Let $a \in \mathbb{Z}$. By the Division Algorithm, $a = pm + r$ for some $m, r \in \mathbb{Z}$ such that $0 \leq r < p$. Thus, $a \equiv pm + r \equiv r \bmod p$. Therefore we will prove that $r^p \equiv r \bmod p$.

If $r = 0$, then $0^p \equiv 0 \bmod p$ and the result holds. Now assume $r \neq 0$. Therefore, r is relatively prime to p, that is, $r \in U(p)$. By the definition of the Euler Phi Function and Theorem 3.6.28, $|U(p)| = \phi(p) = p - 1$. Note that the identity of $U(p)$ is 1. By Corollary 5.2.6,

$$r^{|U(p)|} = r^{p-1} = 1$$

in $U(p)$, thus $r^{p-1} \equiv r \bmod p$ in $\mathbb{Z}$. Multiplying both sides by r, we see that $r^p \equiv r \bmod p$. $\square$

Lagrange's Theorem provides a list of possible orders of subgroups. It does not guarantee that a subgroup exists for each order! Consider the non-example below.

Non-Example 5.2.8. Consider A_4, which has order 12. In particuar, A_4 has one element of order 1, three elements of order 2, and eight elements of order 3. By Lagrange's Theorem, every subgroup of A_5 will have order 1, 2, 3, 4, 6, or 12. Below we show that A_4 has no subgroup of order 6.

By way of contradiction, assume H is a subgroup of order 6, thus H can not contain all eight elements of order 3. Let $a \in A_4 - H$ be an element of order 3. By Lagrange's Theorem, the index of H in A_4 is 2, that is, there are two left cosets of H in A_4. We consider the element a^2 and proceed by cases.

1. If $a^2 \in H$, then by closure, $(a^2)^2 \in H$. Recall that $|a| = 3$. Thus, $a^4 = a \in H$, which is a contradiction.
2. If $a^2 \in aH$, then $a^2 = ah$ for some $h \in H$. By cancellation, $a = h \in H$, which is a contradiction.

Therefore, no subgroup of order 6 can exist. ◇

EXERCISES

Exercise 5.2.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let G be a group and H a subgroup of G.

a. Assume $|G|$ is divisible by $d \in \mathbb{N}$. Then G has a subgroup of order d.

Exercise 5.2.2. Refer back to Fermat's Little Theorem and compute each of the following.

a. $3^{15} \bmod 7$

b. $8^{24} \bmod 11$

c. $4^{64} \bmod 31$

Exercise 5.2.3. Let G be a group and H and K subgroups of orders 8 and 15, respectively. Find $|H \cap K|$.

Exercise 5.2.4. Let G be a group and H and K subgroups of orders m and n, respectively, where m and n are relatively prime. Find $|H \cap K|$ and prove your conjecture.

Exercise 5.2.5. Prove Corollary 5.2.3.

Exercise 5.2.6. Prove Corollary 5.2.5.

Exercise 5.2.7. Prove Corollary 5.2.6.

Exercise 5.2.8. Prove that $|U(n)|$ is even for every $n > 2$.

Exercise 5.2.9. Prove that a group of order 8 must have an element of order 2.

Exercise 5.2.10. Let p be a prime. Prove that a group of order p^3 must have an element of order p.

Exercise 5.2.11. Ⓢ Let G be a group. Show that $N(G) = G$.

Exercise 5.2.12. Let G be a group such that $|G| = pq$ for distinct primes p and q. Let $a, b \in G$ be elements such that $|a| = p$ and $|b| = q$. Prove that the only subgroup of G that contains both a and b is G itself.

Exercise 5.2.13. Let G be a group such that $|G| = pq$ for distinct primes p and q. Prove that every proper subgroup of G is cyclic.

Exercise 5.2.14. Let H be a subgroup of S_4 containing both (34) and (123). Prove that $H = S_4$.

Chapter 6

Constructing Groups

Innovation is taking two things that already exist
and putting them together in a new way.
Tom Freston

In Section 3.3, we first studied subgroups, or groups within a larger group. Now we begin the study of using existing groups to build new groups. First, we will put groups together to create a larger group, a sort of "group multiplication." Second, we will reduce a group to cosets to create a smaller group, a sort of "group division."

6.1 External Direct Products

In Exercise 4.2.2, we saw that $D_4 \not\approx S_4$ and $D_{12} \not\approx S_4$. This may have left you wondering if the groups D_4, D_{12}, and S_4 were isomorphic to anything other than themselves. Recall that we could show these groups were not isomorphic by studying the orders of their elements. Once again, the orders

of the elements and the patterns of their behavior will help us, this time, to find isomorphisms. We begin by learning how piece together groups to make larger groups.

Definition 6.1.1. Let $n \in \mathbb{N}$. An n-tuple is an ordered list of n items.

In calculus, you studied n-tuples frequently, for a 2-tuple is simply an ordered pair and a 3-tuple is an ordered triple. Thus, an n-tuple is just a generalization of these ideas.

Example 6.1.2. Consider the space

$$\mathbb{R}^7 = \{(r_1, r_2, r_3, r_4, r_5, r_6, r_7) \mid r_i \in \mathbb{R}, 1 \leq i \leq 7\}.$$

Then the element $(\sqrt{2}, 0, -1.5, \pi, -\pi, e, 12) \in \mathbb{R}^7$ is a 7-tuple. $\diamond$

Now we consider groups whose elements are n-tuples.

Definition 6.1.3. Let G_1, G_2, ..., G_n be groups for $n \in \mathbb{N}$. The external direct product of these groups is the set of all n-tuples such that the i^{th} component is an element of G_i, that is,

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i, 1 \leq i \leq n\}.$$

Note that the collection G_1, G_2, ..., G_n is a finite collection of groups.

Theorem 6.1.4. *Given groups G_1, G_2, ..., G_n be groups for $n \in \mathbb{N}$, the external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is a group under the component-*

wise operation.

The proof that the external direct product is indeed a group is left as an exercise. Below is an example of an external direct product and how our previous concepts apply to this new idea.

Example 6.1.5. Consider the group $\mathbb{Z}_4 \oplus U(4)$. We see that this group is the set

$$\begin{aligned}\mathbb{Z}_4 \oplus U(4) = \{&(0,1),(1,1),(2,1),(3,1),\\ &(0,3),(1,3),(2,3),(3,3)\}\end{aligned}$$

whose operation is addition modulo 4 in the first component and multiplication modulo 4 in the second component. Below are some examples of previous topics now applied to this external direct product.

- Operation: Consider the elements $(2,3)$ and $(3,3)$. Then

  $$(2,3) * (3,3) = (2+3, 3\cdot 3) = (1,1)$$

  because the first component contains elements of $\mathbb{Z}_4$ and the second component contains elements of $U(4)$.

- Identity: As the operation is performed component-wise, the identity is found according to the components. The identity of the first component is 0 and the identity of the second component is 1. Thus, $(0,1)$ is the identity of $\mathbb{Z}_4 \oplus U(4)$.

- Inverses: Consider the element $(3,3) \in \mathbb{Z}_4 \oplus U(4)$. To find its inverse, we must find the inverse of the elements in each of the components. Thus,

  $$(3,3)^{-1} = (3^{-1}, 3^{-1}) = (1,3).$$

To check, we see that

$$(3,3) * (3,3)^{-1} = (3,3) * (1,3) = (3+1, 3\cdot 3) = (0,1),$$

and $(0,1)$ is indeed the identity.

- Order: Consider the element $(1,3) \in \mathbb{Z}_4 \oplus U(4)$. In Z_4, $|1| = 4$. In $U(4)$, $|3| = 2$. Thus, $|(1,3)| = \mathsf{lcm}(4,2) = 4$. Just to check, consider the example below.

- Cyclic subgroup: The subgroup $\langle (1,3) \rangle$ is shown below.

$$\begin{aligned} \langle (1,3) \rangle &= \{(1,3)^i \mid i \in \mathbb{Z}\} \\ &= \{(1^i, 3^i) \mid i \in \mathbb{Z}\} \\ &= \{(1,3), (2,1), (3,3), (0,1)\} \end{aligned}$$

  As predicted, $|(1,3)| = |\langle (1,3) \rangle| = 4$.

- Cosets: Once again, consider the subgroup $\langle (1,3) \rangle$, which has order four. The group $\mathbb{Z}_4 \oplus U(4)$ has order eight, thus, by Lagrange's Theorem, $|\mathbb{Z}_4 \oplus U(4) : \langle (1,3) \rangle| = 8/4 = 2$. To find the second coset of $\langle (1,3) \rangle$, we take an element not in this subgroup, say $(2,3)$. Then

$$\begin{aligned} (2,3)\langle (1,3) \rangle &= \{(2,3) * (1,3), (2,3) * (2,1), (2,3) * (3,3), (2,3) * (0,1)\} \\ &= \{(2+1, 3\cdot 3), (2+2, 3\cdot 1), (2+3, 3\cdot 3), (2+0, 3\cdot 1)\} \\ &= \{(3,1), (0,3), (1,1), (2,3)\}. \end{aligned}$$

  Thus, we see that $\mathbb{Z}_4 \oplus U(4) = \langle (1,3) \rangle \sqcup (2,3)\langle (1,3) \rangle$.

$\diamond$

The following are some theorems that summarize some of the patterns you

might have predicted while reading through Example 6.1.5.

Theorem 6.1.6. *Consider an element of external direct product of a finite number of groups.*

- *If all components of the element have finite order, then the order of the element is the least common multiple of the orders of the components.*
- *If a component of the element has infinite order, then the order of the element is infinite.*

Proof. For $n \in \mathbb{N}$, let $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ be an external direct product of groups G_i, $1 \leq i \leq n$. For each i, let $e_i \in G_i$ be the identity. Consider the element $g = (g_1, g_2, \ldots, g_n)$. We proceed by cases.

Let $j = |g|$ and $k = \mathsf{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$. By construction, k is a multiple of $|g_i|$ for each i, and because the operation is component-wise,

$$g^k = (g_1, g_2, \ldots, g_n)^k = (g_1^k, g_2^k, \ldots, g_n^k) = (e_1, e_2, \ldots, e_n).$$

Thus, $|g| = j \leq k$. By construction, j is the order of g, thus,

$$g^j = (g_1, g_2, \ldots, g_n)^j = (g_1^j, g_2^j, \ldots, g_n^j) = (e_1, e_2, \ldots, e_n).$$

Thus, j must be a multiple of the order of g_i for each i. Therefore, $j \geq k$. Ergo, $j = k$.

Now assume one of the components of g has infinite order, without loss of generality, call this component g_1. By definition of infinite order, there does not exist a natural number ℓ such that $g_1^\ell = e_1$. Therefore, there does not exist a natural number ℓ such that

$$g^\ell = (g_1, g_2, \ldots, g_n)^\ell = (g_1^\ell, g_2^\ell, \ldots, g_n^\ell) = (e_1, e_2, \ldots, e_n).$$

Ergo, $|g|$ is infinite. □

In Example 6.1.5, we saw an example of a cyclic subgroup within an external direct product. The following theorem goes in the opposite direction, that is, it provides a tool for determining when an external direct product is itself a cyclic group.

Theorem 6.1.7. *Given finite cyclic groups G_1, G_2, ..., G_n, for $n \in \mathbb{N}$, the external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime for all $i \neq j$.*

Proof. For each group G_i, let $|G_i| = m_i$ and let e_i be the identity of G_i. We proceed by induction on n. When $n = 1$, it follows that G is cyclic if and only if the external direct product G is cyclic.

When $n = 2$, we consider $G_1 \oplus G_2$. First, assume $G_1 \oplus G_2$ is cyclic and let (g_1, g_2) be a generator. Suppose $\gcd(m_1, m_2) = d$. The group $G_1 \oplus G_2$ has order $m_1 m_2$, thus $|(g_1, g_2)| = m_1 m_2$. Notice that d divides $m_1 m_2$ by definition. By Corollary 5.2.6 of Lagrange's Theorem,

$$\begin{aligned}(g_1, g_2)^{m_1 m_2/d} &= (g_1^{m_1 m_2/d}, g_2^{m_1 m_2/d}) \\ &= ((g_1^{m_1})^{m_2/d}, (g_2^{m_2})^{m_1/d}) \\ &= (e_1^{m_2/d}, e_2^{m_1/d}) \\ &= (e_1, e_2).\end{aligned}$$

Therefore, $|(g_1, g_2)| \leq m_1 m_2/d$, yet $|(g_1, g_2)| = m_1 m_2$, thus it must be that $d = 1$. Therefore, $|G_1|$ and $|G_2|$ are relatively prime.

Second, assume $|G_1| = m_1$ and $|G_2| = m_2$ are relatively prime. Let $g_1 \in G_1$ and $g_2 \in G_2$ be generators. By Theorem 6.1.6, $|(g_1, g_2)| = \mathsf{lcm}(m_1, m_2) = m_1 m_2$ because m_1 and m_2 are relatively prime. Then $|g_1, g_2| = m_1 m_2 = |G_1 \oplus G_2|$, thus $G_1 \oplus G_2$ is cyclic. □

The remaining proof is left as an exercise.

Example 6.1.8. The group $U(10) \oplus \mathbb{Z}_8$ is not cyclic because

$$\gcd(|U(10)|, |\mathbb{Z}_8|) \neq 1.$$

We see that $|U(10)| = 4$, $|\mathbb{Z}_8| = 8$, and $|U(10) \oplus \mathbb{Z}_8| = 32$. An element in $U(10)$ has order one, two, or four. An element in $\mathbb{Z}_8$ has order one, two, four, or eight. Thus, it is impossible to choose $a \in U(10)$ and $b \in \mathbb{Z}_8$ such that $|(a, b)| = \mathsf{lcm}(|a|, |b|) > 8$. ◇

Example 6.1.9. The group $U(10) \oplus \mathbb{Z}_{10}$ is not cyclic because

$$\gcd(|U(10)|, |Z_{10}|) \neq 1.$$

We see that $|U(10)| = 4$, $|\mathbb{Z}_{10}| = 10$, and $|U(10) \oplus \mathbb{Z}_8| = 40$. An element in $U(10)$ has order one, two, or four. An element in $\mathbb{Z}_{10}$ has order one, two, five, or ten. Thus, it is impossible to choose $a \in U(10)$ and $b \in \mathbb{Z}_{10}$ such that $|(a, b)| = \mathsf{lcm}(|a|, |b|) > 20$. ◇

The following corollary applies Theorem 6.1.7 to the groups of integers under modular arithmetic. Its proof is left as an exercise.

Corollary 6.1.10. *Let $k = m_1 m_2 \cdots m_n$ for natural numbers $m_1, m_2, \ldots, m_n$. Then*

$$\mathbb{Z}_k \approx \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$$

if and only if m_i and m_j are relatively prime for all $i \neq j$.

Example 6.1.11. The groups $\mathbb{Z}_{14}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_7$ are isomorphic because $|\mathbb{Z}_2|$ and $|\mathbb{Z}_7|$ are relatively prime. ◇

Example 6.1.12. The prime decomposition of 105 is $105 = 3 \cdot 5 \cdot 7$. Thus, we know $\mathbb{Z}_{105} \approx \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$. Further, by Corollary 6.1.10, these groups are

also isomorphic the following groups.

$$\begin{aligned}\mathbb{Z}_{105} &\approx \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \\ &\approx \mathbb{Z}_{15} \oplus \mathbb{Z}_7 \\ &\approx \mathbb{Z}_{21} \oplus \mathbb{Z}_5 \\ &\approx \mathbb{Z}_{35} \oplus \mathbb{Z}_3\end{aligned}$$

◇

The contrapositive of Corollary 6.1.10 is particularly useful. Consider the example below.

Example 6.1.13. All of the following groups have order sixteen, though only one of them is cyclic. By Corollary 6.1.10, none of these groups are isomorphic.

- $\mathbb{Z}_{16}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_8$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_4$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

◇

Consider the following example about some groups of units.

Example 6.1.14. Consider $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$. We know that 20 has prime decomposition $20 = 2^2 \cdot 5$, thus we also consider $U(4) =$

$\{1, 3\}$ and $U(5) = \{1, 2, 3, 4\}$. Below is a table of each element in $U(20)$, and the equivalence of that element in $U(4)$ and $U(5)$.

$x \in U(20)$	$x \bmod 4$	$x \bmod 5$
1	1	1
3	3	3
7	3	2
9	1	4
11	3	1
13	1	3
17	1	2
19	3	4

There are many patterns to notice. Every element in $U(20)$ reduces to an element in $U(4)$ and $U(5)$. Further, the eight elements in $U(20)$ reduce into four copies of $U(4)$ and two copies of $U(5)$. $\diamond$

This example is generalized in the theorem below.

Theorem 6.1.15. *Let $k = m_1 m_2 \cdots m_n$ for natural numbers $m_1, m_2, \ldots, m_n$. If m_i and m_j are relatively prime for all $i \neq j$, then*

$$U(k) \approx U(m_1) \oplus U(m_2) \oplus \cdots \oplus U(m_n).$$

Proof. We proceed by induction on n. When $n = 1$, it follows that $U(m_1) \approx U(m_1)$. Now, consider when $n = 2$. To prove that $U(m_1 m_2)$ and $U(m_1) \oplus U(m_2)$, we need to find an isomorphism linking the two groups. Let $x \in U(m_1 m_2)$ and consider the function $\phi : U(m_1 m_2) \to U(m_1) \oplus U(m_2)$ given by

$$\phi(x) = (x \bmod m_1, x \bmod m_2).$$

The proof that this function is indeed an isomorphism is left as an exercise. □

The remaining proof by induction is also left as an exercise.

EXERCISES

Exercise 6.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a. For cyclic groups G and G', $G \oplus G'$ is cyclic.

Exercise 6.1.2. Prove Theorem 6.1.4.

Exercise 6.1.3. Find all of the subgroups of order two in $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Exercise 6.1.4. Ⓢ Find two distinct subgroups of order twenty in $\mathbb{Z}_{50} \oplus \mathbb{Z}_{60}$.

Exercise 6.1.5. Find two distinct subgroups of order twelve in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{40}$.

Exercise 6.1.6. Let G and G' be groups with identities $e \in G$ and $e' \in G'$. Prove that $G \approx G \oplus \{e'\}$.

Exercise 6.1.7. Suppose G, G', H, and H' are groups such that $G \approx G'$ and $H \approx H'$. Prove that $G \oplus H \approx G' \oplus H'$.

Exercise 6.1.8. Determine if the following groups are cyclic.

a. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

b. $\mathbb{Z}_2 \oplus \mathbb{Z}_3$

c. $S_3 \oplus \mathbb{Z}_3$

d. $U(10) \oplus U(12)$

Exercise 6.1.9. For groups G and G', conjecture when $G \oplus G'$ is Abelian. Prove your conjecture.

Exercise 6.1.10. Are the groups D_3 and $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ isomorphic? Prove your conjecture.

Exercise 6.1.11. Is $\mathbb{Z} \oplus \mathbb{Z}$ cyclic? Prove your conjecture.

Exercise 6.1.12. Consider the group $\mathbb{Z}_{15} \oplus \mathbb{Z}_{25}$.

a. What are all of the orders of its elements?

b. Is $\mathbb{Z}_{15} \oplus \mathbb{Z}_{25}$ cyclic? Why or why not?

Exercise 6.1.13. Consider the group $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$.

a. Determine the number of elements of order 3 in $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$.

b. Determine the number of cyclic subgroups of order 3 in $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$.

Exercise 6.1.14. Consider the group $\mathbb{Z}_{20} \oplus \mathbb{Z}_{50}$.

a. Determine the number of elements of order 10 in $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$.

b. Determine the number of cyclic subgroups of order 10 in $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$.

Exercise 6.1.15. Are the groups $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ isomorphic? Prove your conjecture.

Exercise 6.1.16. Complete the proof of Theorem 6.1.7.

Exercise 6.1.17. Prove Corollary 6.1.10.

Exercise 6.1.18. For each of the following, use Corollary 6.1.10 to find all of the isomorphic decompositions of $\mathbb{Z}_n$.

a. $n = 30$

b. $n = 60$

c. $n = 120$

Exercise 6.1.19. Classify all cyclic groups of order 12. For each distinct group, find its generators.

Exercise 6.1.20. Prove that the function $\phi : U(m_1 m_2) \to U(m_1) \oplus U(m_2)$ given by

$$\phi(x) = (x \bmod m_1, x \bmod m_2).$$

in the proof of Theorem 6.1.15 is an isomorphism.

Exercise 6.1.21. Prove that $U(55) \approx U(75)$. *(Hint: Do not find an isomorphism.)*

Exercise 6.1.22. Let G and H be groups. Prove that $G \oplus H \approx H \oplus G$.

Exercise 6.1.23. Finish the proof of Theorem 6.1.15.

6.2 Normal Subgroups

As we saw in Section 5.1, given a coset representative, the left coset is not necessarily equal to the right coset. There are certain subgroups, though, that do produce left and right cosets that are equal. We now study this phenomenon, as these subgroups will play an important role in developing new groups groups and understanding isomorphisms.

Definition 6.2.1. Let G be a group. A subgroup H is normal if $aH = Ha$ for all $a \in G$. The normal subgroup relationship is denoted $H \lhd G$.

Example 6.2.2. Every subgroup in an Abelian group is normal. For every coset representative $a \in G$ and every h in subgroup H, $ah = ha$, thus $aH = Ha$. ◇

Example 6.2.3. Given a group G, its center, $Z(G)$, is a normal subgroup. For every coset representative $a \in G$ and every $z \in Z(G)$, $az = za$ because

$Z(G)$ is the subgroup of all elements in G that commute with all elements in G. ◇

Example 6.2.4. Let $G = S_4$ and $H = \{e, (12)(34), (13)(24), (14)(23)\}$. The index of H in G is $|G : H|/|H| = 24/4 = 6$, thus we expect to find six cosets of H in G. Through calculation, we that

$$\begin{aligned} H &= \{e, (12)(34), (13)(24), (14)(23)\} \\ (12)H &= \{(12), (34), (1324), (1423)\} \\ (13)H &= \{(13), (1234), (24), (1432)\} \\ (14)H &= \{(14), (1243), (1342), (23)\} \\ (23)H &= \{(23), (1342), (1243), (14)\} \\ (24)H &= \{(24), (1432), (13), (1234)\} \end{aligned}$$

Through calculation, we that

$$\begin{aligned} H &= \{e, (12)(34), (13)(24), (14)(23)\} \\ H(12) &= \{(12), (34), (1423), (1324)\} \\ H(13) &= \{(13), (1432), (24), (1234)\} \\ H(14) &= \{(14), (1342), (1243), (23)\} \\ H(23) &= \{(23), (1243), (1342), (14)\} \\ H(24) &= \{(24), (1234), (13), (1432)\} \end{aligned}$$

Thus, for every $a \in S_4$, $aH = Ha$, which means that H is a normal subgroup of S_4. ◇

The definition of normal only requires that a coset representative creates the

same left coset as right coset. The definition does not require that the coset representative creates the same coset elements in the same order. That is, for coset representative a and subgroup H, the definition requires $aH = Ha$, but it does not require that $ah = ha$ for all $h \in H$. Consider the example below.

Example 6.2.5. In Example 6.2.4, we found that S_4 has normal subgroup $H = \{e, (12)(34), (13)(24), (14)(23)\}$. Consider the coset representative $a = (12)$ and the cosets it generates, shown below.

$$\begin{aligned}(12)H &= \{(12)e, (12)(12)(34), (12)(13)(24), (12)(14)(23)\} \\ &= \{(12), (34), (1324), (1423)\} \\ H(12) &= \{e(12), (12)(34)(12), (13)(24)(12), (14)(23)(12)\} \\ &= \{(12), (34), (1423), (1324)\}\end{aligned}$$

Consider $h = (13)(24) \in H$. In $(12)H$, $ah = (12)(13)(24) = (1324)$. In $H(12)$, $ha = (13)(24)(12) = (1423)$. Thus, we see that $ah \neq ha$ for some $h \in H$. Nonetheless, $H \lhd S_4$, because $aH = Ha$ for all coset representatives $a \in S_4$. ◇

Non-Example 6.2.6. Let $G = S_4$ and $K = \{e, (12), (34), (12)(34)\}$. Through calculation, we that

$$\begin{aligned}(13)K &= \{(13), (123), (134), (1234)\} \\ K(13) &= \{(13), (132), (143), (1432)\}\end{aligned}$$

Thus, we have found an $a \in S_4$ such that $aK \neq Ka$, therefore, K is not a normal subgroup of S_4. ◇

The theorem below gives an equivalent definition of a normal subgroup.

Theorem 6.2.7. *Let G be a group and H a subgroup of G. Then H is*

normal in G if and only if $aHa^{-1} \subseteq H$ for all $a \in G$.

Proof. Let G be a group and H a subgroup of G. First, assume H is normal in G. Thus, for every $h \in H$, there exists an $h' \in H$ such that $ah = h'a$. Hence, $aha^{-1} = h' \in H$ for all $h \in H$. Therefore, $aHa^{-1} \subseteq H$.

Second, assume $aHa^{-1} \subseteq H$ for all $a \in G$. Then, for every $h \in H$, there exists an $h' \in H$ such that $aha^{-1} = h'$. Hence, $ah = h'a \in Ha$, thus $aH \subseteq Ha$. Similarly, when $aha^{-1} = h'$, $ha^{-1} = a^{-1}h' \in a^{-1}H$, thus $Ha^{-1} \subseteq a^{-1}H$. This true for all $a \in G$, including a^{-1}. Therefore, $aH = Ha$, which means that H is normal in G. □

Below, we reconsider Non-Example 6.2.6 to better understand how to use Theorem 6.2.7.

Example 6.2.8. Let $G = S_4$ and $K = \{e, (12), (34), (12)(34)\}$, as in Non-Example 6.2.6. For coset representative (13), we see that

$$\begin{aligned}(13)K(13)^{-1} &= (13)K(13) \\ &= \{(13)e(13), (13)(12)(13), (13)(34)(13), (13)(12)(34)(13)\} \\ &= \{e, (23), (14), (14)(23)\}\end{aligned}$$

which is not a subset of K. Therefore, K is not a normal subgroup of S_4. ◇

Theorem 6.2.7 gives us an alternative way to test if a subgroup is normal. Like with many of our previous concepts, we will test our knowledge in two types of subgroup calculations: 1) the subgroup is given explicitly and 2) the subgroup is given in set-builder notation. In practice, we find the following.

- When working with a subgroup given in set-builder notation, Theorem 6.2.7 will be useful to determine whether or not a subgroup is normal.

This is because Theorem 6.2.7 only requires one calculation.

- When working with a subgroup given explicitly, this theorem is particularly useful for showing a subgroup is not normal. This is because Theorem 6.2.7 requires only one calculation to conclude that a subgroup is not normal. Comparatively, when using the definition, we must perform two calculations to determine that the subgroup was not normal, as in Non-Example 6.2.6.
- When working with a subgroup given explicitly, Theorem 6.2.7 is might not be as useful as the definition of normal. This is because, using the definition, for group G and subgroup H, we only must perform $2|G : H|$ calculations to determine that the subgroup is normal. When using Theorem 6.2.7, we may have to perform $|G|$ calculations.

Below is an example of how to use the definition to prove that a subgroup is normal.

Theorem 6.2.9. *The intersection of two normal subgroups is normal.*

Proof. Let G be a group with normal subgroups M and N. Take $a \in M \cap N$. By Exercise 5.1.12,

$$a(M \cap N) = aM \cap aN.$$

By the definition of normal, $aM \cap aN = Ma \cap Na$, and by Exercise 5.1.12 again, $Ma \cap Na = (M \cap N)a$. Hence, $M \cap N$ is normal in G. □

Below is an example of how to use Theorem 6.2.7 to prove that a subgroup given in set-builder notation is normal.

Theorem 6.2.10. *Let ϕ be a homomorphism from group G to group G'.*

1. *If N' is a normal subgroup of G', then $\phi^{-1}(N')$ is a normal subgroup of G.*

2. *The kernel of ϕ is a normal subgroup of G.*

Proof. Let ϕ be a homomorphism from group G to group G' and assume N' is a normal subgroup of G'. We know that

$$\phi^{-1}(N') = \{n \in G \,|\, \phi(n) \in \phi(N')\}.$$

Take $a \in G$. Then

$$a\phi^{-1}(N')a^{-1} = \{ana^{-1} \,|\, \phi(n) \in \phi(N')\}.$$

By the definition of homomorphism,

$$\phi(ana^{-1}) = \phi(a)\phi(n)\phi(a^{-1}) = \phi(a)\phi(n)\phi(a)^{-1}.$$

Recall that $\phi(n) \in N'$. By Theorem 6.2.7, $g'N'(g')^{-1} \subseteq N'$ for all $g' \in G'$. Taking, $g' = \phi(a) \in G'$, we see that $\phi(a)\phi(n)\phi(a)^{-1} \in N'$. Hence, $ana^{-1} \in \phi^{-1}(N')$. Thus, $a\phi^{-1}(N')a^{-1} \subseteq \phi^{-1}(N')$, and by Theorem 6.2.7, $\phi^{-1}(N')$ is normal in G.

The subgroup $\{e'\}$, where $e' \in G'$ is the identity, is normal in G'. By the first property,

$$\phi^{-1}(\{e'\}) = \{n \in G \,|\, \phi(n) = e'\} = \ker(\phi)$$

is normal in G. □

The following definition relates to normal subgroups.

Definition 6.2.11. A group is simple if its only normal subgroups are the trivial subgroup and the group itself.

Example 6.2.12. The group $\mathbb{Z}_5$ is simple because it has no proper subgroups, let alone proper normal subgroups. The group $\mathbb{Z}_6$ is not simple because $H = \{0, 2, 4\}$ is a proper subgroup of $\mathbb{Z}_6$, and $\mathbb{Z}_6$ is Abelian. $\diamond$

Further study of simple groups requires more advanced abstract algebra, material that might be covered in a second or third semester.

EXERCISES

Exercise 6.2.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let G be a group and H a subgroup of G.

a. A group G has nontrivial normal subgroups.

Exercise 6.2.2. Revisit Examples 5.1.1 through 5.1.9. Determine which examples are about normal subgroups and which examples are about subgroups that are not normal.

Exercise 6.2.3. Let G be a group with subgroup H. Prove that if each left coset of H is equal to some right coset of H, then H is normal in G.

Exercise 6.2.4. Let $n > 2$ be a natural number. Prove that $A_n \lhd S_n$.

Exercise 6.2.5. Is A_3 simple? Is A_4 simple?

Exercise 6.2.6. Prove that a subgroup of index two is normal.

Exercise 6.2.7. For natural number $n \geq 3$, let H be the subgroup of rotations in D_n. Prove that H is normal in D_n. Conclude that D_n is not simple.

Exercise 6.2.8. Let M be a normal subgroup of N, and let N be a normal subgroup of G. Is M normal in G? Prove your conjecture.

Exercise 6.2.9. Consider $G = S_n$ for natural number $n \geq 2$, and let i be a natural such that $1 \leq i \leq n$. Is $\mathsf{stab}_G(i) \lhd G$? Prove your conjecture.

Exercise 6.2.10. Let G be a group with subgroup H. Prove that $H \lhd N(H)$.

6.3 Quotient Groups

Now we begin the study of groups created by "dividing groups," or quotient groups.

Definition 6.3.1. Let G be a group and N a normal subgroup of G. The set of cosets of N in G,

$$G/N = \{aN \mid a \in G\},$$

is a group under the operation $(aN) * (bN) = (ab)N$ for all $a, b \in G$. This group is called the quotient group of G by N.

Before we prove that the quotient group is indeed a group, we study some examples.

Example 6.3.2. The subgroup $4\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$ because $\mathbb{Z}$ is Abelian. Note that the operation in $\mathbb{Z}$ is addition, thus we write the cosets additively. The quotient group of $\mathbb{Z}$ by $4\mathbb{Z}$ is

$$\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}.$$

The operation of addition modulo 4 is performed on the coset representatives.

The Cayley tables of $\mathbb{Z}/4\mathbb{Z}$ is shown below.

$\mathbb{Z}/4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

Look familiar? ◇

Example 6.3.3. The group $U(20)$ has normal subgroup $\langle 11\rangle$. Below is the quotient groups they create.

$$U(20)/\langle 11\rangle = \{\langle 11\rangle, 3\langle 11\rangle, 7\langle 11\rangle, 9\langle 11\rangle\}$$

To which group is $U(20)/\langle 11\rangle$ isomorphic? ◇

The example below begins to illustrate a difficulty when using cosets in computations.

Example 6.3.4. Consider the quotient group in Example 6.3.2. Each coset is infinite, hence there are an infinite number of coset representatives for each coset, thus, we could instead represent the quotient group as

$$\mathbb{Z}/4\mathbb{Z} = \{-12+4\mathbb{Z}, 17+4\mathbb{Z}, 30+4\mathbb{Z}, 11+4\mathbb{Z}\}.$$

Continuing to choose less-than-helpful coset representatives, we could display the Cayley table of $\mathbb{Z}/4\mathbb{Z}$ as shown below.

$\mathbb{Z}/4\mathbb{Z}$	$-12+\mathbb{Z}$	$17+4\mathbb{Z}$	$30+4\mathbb{Z}$	$11+4\mathbb{Z}$
$-12+\mathbb{Z}$	$60+4\mathbb{Z}$	$61+4\mathbb{Z}$	$62+4\mathbb{Z}$	$63+4\mathbb{Z}$
$17+4\mathbb{Z}$	$-19+4\mathbb{Z}$	$-18+4\mathbb{Z}$	$-17+4\mathbb{Z}$	$-16+4\mathbb{Z}$
$30+4\mathbb{Z}$	$202+4\mathbb{Z}$	$203+4\mathbb{Z}$	$204+4\mathbb{Z}$	$205+4\mathbb{Z}$
$11+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

It may not be initially intuitive that $(-12+4\mathbb{Z})+(17+4\mathbb{Z})=61+4\mathbb{Z}$ and that this coset is indeed the same coset as $(17+4\mathbb{Z})+(-12+4\mathbb{Z})=-19+4\mathbb{Z}$. Judging from the Cayley table alone, it does not appear that the group $\mathbb{Z}/4\mathbb{Z}$ is Abelian. Moreover, judging from the Cayley table alone, it does not appear that $\mathbb{Z}/4\mathbb{Z}$ is a group at all. ◇

The potential difficulty with coset computations arises because there are multiple ways to represent a single coset. Recall that a binary operation on a set S is a function from $S\times S$ to S. This leads us the following definition.

Definition 6.3.5. An assignment is well-defined if, for each input, it yields the same output, regardless of the representation of the input.

A function is well-defined, thus you have seen many examples of well-defined assignments before. Therefore, we begin with some non-examples.

Non-Example 6.3.6. Consider the sets $A=\{0,1,2,3,4\}$, $B=\{3,4,5,6\}$, and $C=\{0,1,2,3,4,5,6\}$. For $c\in C$, the assignment

$$f(c)=\begin{cases}0 & c\in A\\ 1 & c\in B\end{cases}$$

is not well-defined. Consider $c=3$. When considering $3\in A$, it may seem as

though $f(3) = 0$. When considering $3 \in B$, it may seem as though $f(3) = 1$. Thus, the assignment f is not well-defined. $\diamond$

Non-Example 6.3.7. Consider the quotient group $\mathbb{Z}/4\mathbb{Z}$. The assignment $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}_{12}$ given by $f(x + 4\mathbb{Z}) = 2x$ is not well-defined. The element $2 + 4\mathbb{Z}$ in $\mathbb{Z}/4\mathbb{Z}$ can also be represented as $6 + 4\mathbb{Z}$. The assignment f acts on this coset in the following ways.

$$f(2 + 4\mathbb{Z}) = 2 \cdot 2 = 4 \in \mathbb{Z}_{12}$$
$$f(6 + 4\mathbb{Z}) = 2 \cdot 6 = 0 \in \mathbb{Z}_{12}$$

Therefore, even though $2 + 4\mathbb{Z} = 6 + 4\mathbb{Z}$, $f(2 + 4\mathbb{Z}) \neq f(6 + 4\mathbb{Z})$. Therefore, the assignment f is not well-defined. $\diamond$

As we began to see in Non-Examples 6.3.6 and 6.3.7, an assignment is not well-defined if it assigns one input to more than one output. Recall the following types of assignments, and let $n > 1$ be a natural number.

- A homomorphism can be n-to-one.
- An isomorphism is one-to-one.
- A not well-defined assignment is one-to-n for at least one input.

In practice, when working with elements that have multiple representations, like cosets, we must verify that any assignment we create is well-defined. To do this, assume two distinct representations of the input and prove that the two forms of the output are equal. Below, we give an example of how this proof technique fails in when the assignment is not well-defined.

Non-Example 6.3.8. Revist the assignment f in Non-Example 6.3.7. Consider the element $x+4\mathbb{Z}$ and its alternative representation $y+4\mathbb{Z}$ where $x \neq y$.

Then $f(x + 4\mathbb{Z}) = 2x$ and $f(y + 4\mathbb{Z}) = 2y$. By assumption, $x \neq y$, thus $2x$ does not necessarily equal $2y$. $\diamond$

The proof of the lemma below includes an example of how to prove an assignment is well-defined.

Lemma 6.3.9. *Let G be a group and N a normal subgroup of G. For all $a, b \in G$, the operation $(aN) * (bN) = (ab)N$ is well-defined.*

Proof. Let G be a group and N a normal subgroup of G. If N is the trivial subgroup, then $(aN) * (bN) = (ab)N$ holds because $a * b = ab$.

Now assume $|N| > 1$. Take elements $a, a', b, b' \in G$ such that $aN = a'N$ and $bN = b'N$, yet $a \neq a'$ and $b \neq b'$. As a subgroup, the identity e is in N, thus $ae = a = a'n_1$ and $be = e = b'n_2$ for some $n_1, n_2 \in N$. Taking the element ab as a coset representative, we see that

$$(ab)N = (a'n_1)(b'n_2)N = a'(n_1b')n_2N = a'(n_1b')N$$

because $n_2 \in N$. Note that $n_1b \in Nb = bN$ because N is normal. Therefore, $n_1b' = b'n_3$ for some $n_3 \in N$, which allows us to continue rewriting the coset as

$$a'(n_1b')N = a'(b'n_3)N = (a'b')N.$$

In conclusion, the cosets $(ab)N$ and $(a'b')N$ are equal, which proves that the operation is well-defined. $\square$

Lemma 6.3.9 provides the tool we need to prove that the quotient group is indeed a group.

Theorem 6.3.10. *Let G be a group and N a normal subgroup of G. The quotient group G/N is a group under the operation $(aN) * (bN) = (ab)N$ for all $a, b \in G$.*

Proof. Let G be a group, N a normal subgroup of G, and $a, b \in G$ where is the identity. In Lemma 6.3.9, we verified that the operation is well-defined. By the construction of the operation, $(aN) * (bN) = (ab)N$, and abN is a coset of N in G, thus the operation is closed.

Consider cosets $aN, bN, cN \in G/N$. Then

$$\begin{aligned}(aN * bN) * cN &= (abN) * cN \\ &= (ab)cN \\ &= a(bc)N \\ &= aN * (bcN) \\ &= aN * (bN * cN)\end{aligned}$$

because G is associative.

By definition of a group, G has an identity, say e. Then, for all $a \in G$, $(aN) * (eN) = (ae)N = aN$, and similarly, $(eN) * (aN) = aN$. Therefore, $eN = N$ is the identity of G/N. By definition of a group, for all $a \in G$, $a^{-1} \in G$. Then, $(aN) * (a^{-1}N) = (aa^{-1})N = N$, thus $a^{-1}N = (aN)^{-1}$. □

Given a normal subgroup N in group G, we now know that G/N is a group. This means that, for coset representative $a \in G$, aN plays two roles:

1. The set aN is a coset, thus $|aN|$ represents the number of elements in the coset aN.

2. The set aN is a group element, thus $|aN|$ represents the order of the element aN in the quotient group G/N.

We will use both writing and mathematical context to determine how to interpret $|aN|$. Consider the examples below.

Example 6.3.11. The subgroup $\langle 4\rangle$ is normal in the group $\mathbb{Z}_{24}$. We know that $|\langle 4\rangle| = 6$ and $|\mathbb{Z}_{24}/\langle 4\rangle| = 4$. Consider the coset $3 + \langle 4\rangle$. The notation $|3 + \langle 4\rangle|$ has the following interpretations.

1. As a coset, $3 + \langle 4\rangle = \{3, 7, 11, 15, 19, 23\}$, thus $|3 + \langle 4\rangle| = 6$.
2. As an element in the quotient group $\mathbb{Z}_{24}/\langle 4\rangle$, we see that

$$\langle 3 + \langle 4\rangle\rangle = \{3 + \langle 4\rangle, 2 + \langle 4\rangle, 1 + \langle 4\rangle, \langle 4\rangle\},$$

   thus $|3 + \langle 4\rangle| = 4$.

◇

Example 6.3.12. The subgroup $\langle 4\rangle$ is normal in the group $\mathbb{Z}$. We know that $|\langle 4\rangle|$ is infinite and $|\mathbb{Z}/\langle 4\rangle| = 4$. Consider the coset $3+\langle 4\rangle$. The notation $|3 + \langle 4\rangle|$ has the following interpretations.

1. As a coset, $3+\langle 4\rangle = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$, thus $|3+\langle 4\rangle|$ is infinite.
2. As an element in the quotient group $\mathbb{Z}/\langle 4\rangle$, we see that

$$\langle 3 + \langle 4\rangle\rangle = \{3 + \langle 4\rangle, 2 + \langle 4\rangle, 1 + \langle 4\rangle, \langle 4\rangle\},$$

   thus $|3 + \langle 4\rangle| = 4$.

Thus, the interpretation of $|3 + \langle 4\rangle|$ can yield both a finite order and an infinite order. ◇

As we will see, quotient groups yield many powerful results. Below are a few.

Theorem 6.3.13. *Let G be a group with center $Z(G)$. If $G/Z(G)$ is cyclic, then G is Abelian.*

Proof. Let G be a group and assume $G/Z(G)$ is cyclic. Thus, there exists some element $aZ(G) \in G/Z(G)$ such that $G/Z(G) = \langle aZ(G)\rangle$. Taking $g \in G$ to be a coset representative, there exists some $i \in \mathbb{Z}$ such that $gZ(G) = (aZ(G))^i = a^iZ(G)$. Hence, $g = a^iz$ for some $z \in Z(G)$. By the definition of center, z commutes with all elements, ergo

$$ga = a^iza = a^iaz = aa^iz = ag,$$

therefore $g \in C(a)$. By assumption, $g \in G$ is arbitrary, thus $G \subseteq C(a)$. This implies that $a \in Z(G)$, which implies that $aZ(G) = Z(G)$.

Recall that $aZ(G)$ is the generator of $G/Z(G)$ and $Z(G)$ is the identity element of $G/Z(G)$. Thus, $|G/Z(G)| = 1$. This implies that $G = Z(G)$. Therefore, G is Abelian. □

In the next example, we use the contrapositive of Theorem 6.3.13.

Example 6.3.14. We know that D_4 is non-Abelian, thus by Theorem 6.3.13, $D_4/Z(D_4)$ is not cyclic. We verify this by calculating all of the cosets of $Z(D_4)$ below.

$$\begin{aligned} Z(D_4) &= \{R_0, R_{180}\} \\ R_{90}Z(D_4) &= \{r_{90}, R_{270}\} \\ HZ(D_4) &= \{H, V\} \\ D_LZ(D_4) &= \{D_L, D_R\} \end{aligned}$$

Notice that $|D_4/Z(D_4)| = 4$ and each non-identity element in $D_4/Z(D_4)$ has order two. Therefore, no element in $D_4/Z(D_4)$ is a generator.

Also notice that $D_4/Z(D_4)$ categorizes the movements of D_4. This is another example of how the partitions cosets form highlight some structure of the original group. ◇

The proof of the theorem below provides a good example of how quotient groups can be helpful in calculations and proofs.

Theorem 6.3.15 (Cauchy's Theorem for Abelian Groups)**.** *Let G be an Abelian group of order n, and let p be a prime divisor of n. Then G has an element of order p.*

Proof. Let G be a finite Abelian group. If $|G| = 2$, then its nonidentity element has order two. If $|G| = 3$, then by Exercise 3.6.26, G is cyclic, and its nonidentity elements have order three. We proceed by induction. Assume $|G| = n$, p is a prime that divides n, and each group of order less than n has an element of order p.

Let $g \neq e \in G$. Then $|g| > 1$ and $|g|$ has a prime factor. Suppose $|g| = mq$ for $m, q \in \mathbb{N}$ and q is prime. Then $|g^m| = q$. Thus, we may conclude that G has an element of prime order.

Let $a \in G$ be an element of prime order. If $|a| = p$, then a is an element in G of order p. Assume $|a| \neq p$, say $|a| = r$ where r is prime. We know that G is Abelian, thus all of its subgroups are normal. Therefore, $G/\langle a\rangle$ is an Abelian group. Moreover, p divides $|G|$, and because $|\langle a\rangle| = r \neq p$, p must also divides $|G/\langle a\rangle|$. By the inductive hypothesis, $G/\langle a\rangle$ has an element of order p, say $b\langle a\rangle$ for $b \in G$.

If $|b\langle a\rangle| = p$, then $(b\langle a\rangle)^p = b^p\langle a\rangle = e\langle a\rangle = \langle a\rangle$. This implies that $b^p \in \langle a\rangle$. If $b^p = e \in \langle a\rangle$, then $b \in G$ is an element of order p.

Suppose $b^p \neq e \in \langle a\rangle$. Recall that $|\langle a\rangle| = r$ where r is prime. Thus, $|b^p| = r$. Therefore, b^r has order p. □

EXERCISES

Exercise 6.3.1. For each of the following, determine if the statement is

always true, sometimes true, or never true. In a sentence or two, justify your response. Let G be a group and H a subgroup of G.

a. The set G/H is a group.

b. The set G/G is a group.

Exercise 6.3.2. For each of the following quotient groups, make a Cayley table and then determine to which familiar group the group is isomorphic. (You do not need to prove the two groups are isomorphic.)

a. $\mathbb{Z}/6\mathbb{Z}$

b. $D_3/\langle(123)\rangle$

c. $U(40)/\langle 27\rangle$

Exercise 6.3.3. Let $f : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}_{50}$ be given by $f(x + 10\mathbb{Z}) = x$. Is this assignment well-defined? If so, prove it. If not, find a counterexample.

Exercise 6.3.4. In the definition of a quotient group, why is the condition that the subgroup is normal necessary? If the subgroup is not normal, what happens?

Exercise 6.3.5. The groups $\langle 5\rangle$ and $\langle 20\rangle$ are subgroups of $\mathbb{Z}$. Prove that $\langle 5\rangle/\langle 20\rangle \approx \mathbb{Z}_4$.

Exercise 6.3.6. Let $H = \{e, (13)(24)\} \leq A_4$.

a. Prove that H is not normal.

b. Prove that the set of cosets of H in A_4 is not a group.

Exercise 6.3.7. Let G be a group with normal subgroup N. For each of the following, compute the order of the element $g \in G/N$.

a. $9 + \langle 12\rangle$ in $\mathbb{Z}/\langle 12\rangle$

b. $19\langle 5\rangle$ in $U(28)/\langle 5\rangle$

c. $(12)\langle(123)\rangle$ in $S_4/\langle 123\rangle$

d. $11 + \langle 42\rangle$ in $\mathbb{Z}_{60}/\langle 42\rangle$

e. $(1,1)\langle(3,3)\rangle$ in $\mathbb{Z}_6 \oplus U(8)/\langle(3,3)\rangle$

Exercise 6.3.8. For group G with normal subgroup N, prove the following about G/N.

a. If G is Abelian, then G/N is Abelian.

b. If G is cyclic, then G/N is cyclic.

Exercise 6.3.9. Let G be a group with normal subgroups M and N. If $M \approx N$, must G/M be isomorphic to G/N? Prove your conjecture.

Exercise 6.3.10. Let $G = U(16)$, $M = \langle 15\rangle$, and $N = \langle 9\rangle$. Are M and N isomorphic? Are G/M and G/N isomorphic?

Exercise 6.3.11. Let p and q be distinct prime numbers. Prove that an Abelian group of order pq is cyclic.

Exercise 6.3.12. The groups below are isomorphic to either $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Determine to which group each quotient group is isomorphic and justify your claim.

a. $\mathbb{Z}_4 \oplus \mathbb{Z}_{12}/\langle(2,10)\rangle$

b. $U(32)/\langle 31\rangle$

6.4 The Isomorphism Theorems

A common theme you may have noticed throughout your mathematics education is that after learning how to use a definition, we often create new ways to show a definition holds without having to individually prove each piece of the definition. In this section, we will study some theorems that allow us ways to conclude two groups are isomorphic without having to construct an isomorphism between them.

Example 6.4.1. Revisit Example 4.1.9. The map $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_4$ defined by $\phi(x) = x \bmod 4$ is a homomorphism with kernel

$$\ker(\phi) = \{0, 4, 8, 12, 16\} = \langle 4 \rangle \leq \mathbb{Z}_{20}.$$

We see that the quotient group $\mathbb{Z}_{20}/\ker(\phi)$ is

$$\mathbb{Z}_{20}/\ker(\phi) = \{\langle 4 \rangle, 1 + \langle 4 \rangle, 2 + \langle 4 \rangle, 3 + \langle 4 \rangle\}.$$

We will see that $\mathbb{Z}_{20}/\ker(\phi) \approx \phi(\mathbb{Z}_{20}) \approx \mathbb{Z}_4$. ◇

Example 6.4.2. The map $\phi : \mathbb{Z}_{40} \to \mathbb{Z}_{10}$ defined by $\phi(x) = 2x \bmod 10$ is a homomorphism with kernel

$$\ker(\phi) = \{0, 5, 10, 15, 20, 25, 30, 35\} = \langle 5 \rangle \leq \mathbb{Z}_{40}.$$

We see that the quotient group $\mathbb{Z}_{40}/\ker(\phi)$ is

$$\mathbb{Z}_{40}/\ker(\phi) = \{\langle 5 \rangle, 1 + \langle 5 \rangle, 2 + \langle 5 \rangle, 3 + \langle 5 \rangle, 4 + \langle 5 \rangle\}.$$

Notice that ϕ only maps elements of $\mathbb{Z}_{40}$ to the evens in $\mathbb{Z}_{10}$, that is

$$\phi(\mathbb{Z}_{40}) = \{0, 2, 4, 6, 8\} = \langle 2 \rangle \leq \mathbb{Z}_{10}.$$

We will see that $\mathbb{Z}_{40}/\ker(\phi) \approx \phi(\mathbb{Z}_{40}) \approx \mathbb{Z}_5$. ◇

In Theorem 6.2.10, we saw that the kernel of a homomorphism is a normal subgroup. In Section 6.3, we studied how quotient groups can be isomorphic to other, non-quotient, groups. Now, we put these two ideas together and see that when the quotient group is constructed with using a kernel, a very specific group to which the quotient group is isomomorphic is the image. This idea is summarized and formalized below.

Theorem 6.4.3 (The First Isomorphism Theorem)**.** *Let G and G' be groups and $\phi : G \to G'$ a homomophism. Then $G/\ker(\phi) \approx \phi(G)$ is an isomorphism.*

Proof. Let $\psi : G/\ker(\phi) \to \phi(G)$ be defined by $\psi(g\ker(\phi)) = \phi(g)$ for $g \in G$. First we will show that ψ is well-defined, and then we will show that it is an isomorphism.

0. Well-defined: Consider $g\ker(\phi), h\ker(\phi) \in G/\ker(\phi)$ such that $g\ker(\phi) = h\ker(\phi)$ and $g \neq h \in G$. By property 1 of Theorem 5.1.10, $g\ker(\phi) = h\ker(\phi)$ if and only if $\phi(g) = \phi(h)$. Notice that

$$\phi(g) = \psi(g\ker(\phi)) = \psi(h\ker(\phi)) = \phi(h)$$

by definition of ψ. Therefore, ψ maps distinct representations of the same coset to the same element in $\phi(G)$, hence ψ is well-defined.

1. Operation-preserving: Take $g\ker(\phi), h\ker(\phi) \in G/\ker(\phi)$. Then

$$\psi(g\ker(\phi) * h\ker(\phi)) = \psi(g * h\ker(\phi))$$

by the definition of the operation on the quotient group. Further,

$$\psi(g * h\ker(\phi)) = \phi(g * h)$$

by the definition of ψ. Recall that ϕ is a homomorphism and therefore preserves the operation, yielding

$$\phi(g * h) = \phi(g) * \phi(h).$$

Once again, by the definition of ψ, we see that

$$\phi(g) * \phi(h) = \psi(g\ker(\phi)) * \psi(h\ker(\phi)).$$

All together, we find that

$$\psi(g\ker(\phi) * h\ker(\phi)) = \psi(g\ker(\phi)) * \psi(h\ker(\phi)),$$

meaning that ψ preserves the operation.

2. One-to-one: Assume $\phi(g) = \phi(h) \in \phi(G)$. By property 1 of Theorem 5.1.10, this is true if and only if $g\ker(\phi) = h\ker(\phi)$.

3. Onto: Consider the element $\phi(g) \in \phi(G)$. Then $g\ker(\phi) \in G/\ker(\phi)$ is the element such that $\psi(g\ker(\phi)) = \phi(g)$.

Therefore, $G/\ker(\phi) \approx \phi(G)$.

□

Recall that a homomorphism is n-to-one, where $n \in \mathbb{N}$, and its kernel has size n. The First Isomorphism Theorem has us place two restrictions on the homomorphism.

1. In a sense, by using the kernel to construct the quotient group, we are "canceling" all of the redundancies, making the resulting function one-to-one.

2. By considering only the image of the homomorphism, and not necessarily the full codomain, the function, we are considering is an onto homomorphism.

The result is that the homomorphism under these restrictions is both one-to-one and onto. Thus, the homomorphism under these restrictions is an isomorphism. The example below illustrates this idea.

Example 6.4.4. Consider the homomophism $\phi : \mathbb{Z}_{18} \to \mathbb{Z}_6$ given by $\phi(x) = 2x \bmod 6$. It has kernel $\ker(\phi) = \langle 3 \rangle \leq \mathbb{Z}_{18}$ and thus is a six-to-one mapping.

The quotient group

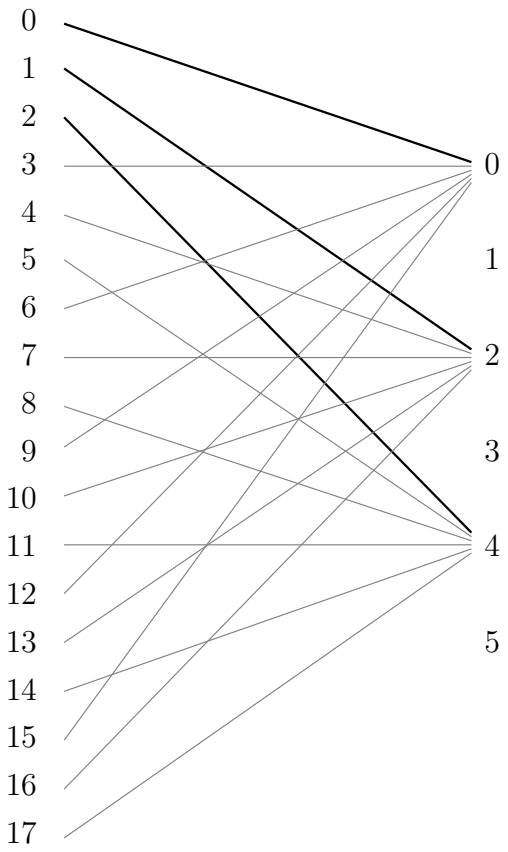
$$\mathbb{Z}_{18}/\ker(\phi) = \{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$$

has order three. In a sense, when we "divide" a group of order eighteen by a group of order six, we create a group of order three. Thus, the domain of our six-to-one mapping becomes restricted to the first three elements, reducing our six-to-one mapping down to a one-to-one mapping.

Let $\phi|_{\{0,1,2\}}$ denote the mapping ϕ restricted to the set $\{0, 1, 2\}$.

Below is an illustration of the mapping of ϕ. The darker lines represent the mapping of $\phi|_{\{0,1,2\}}$. They emanate from the three coset representatives, showing that the mapping applied to the reduction $\mathbb{Z}_{18}/\ker(\phi)$ is indeed one-to-one.

Notice that neither ϕ nor $\phi|_{\{0,1,2\}}$ is onto. Thus, in order to make these functions onto, we must consider these functions as mapping to image $\phi(\mathbb{Z}_{18})$ instead of the codomain $\mathbb{Z}_6$.



◇

Below is an example of how to use the First Isomorphism Theorem.

Example 6.4.5. We will prove that $\mathsf{GL}(2,\mathbb{R})/\mathsf{SL}(2,\mathbb{R}) \approx \mathbb{R}^*$. Previously, we would have done this by fulfilling the definition of isomorphism. To do that, we could have had to calculate the cosets, find a function, and then show that the function is well-defined, one-to-one, onto, and preserves the operation. Instead, we'll use the First Isomorphism Theorem. We'll find a homomorphism that maps from $\mathsf{GL}(2,\mathbb{R})$ to $\mathbb{R}^*$ with kernel $\mathsf{SL}(2,\mathbb{R})$.

The identity of $\mathbb{R}^*$ is $1 \in \mathbb{R}^*$, thus we need to find a function that maps $\mathsf{SL}(2,\mathbb{R})$ to $1 \in \mathbb{R}^*$. Noting that all elements in $\mathsf{SL}(2,\mathbb{R})$ have determinant one, we choose the function $\phi : \mathsf{GL}(2,\mathbb{R}) \to \mathbb{R}^*$ defined by $\phi(A) = \det(A)$ for all $A \in \mathsf{GL}(2,\mathbb{R})$. Therefore, $\ker(\phi) = \mathsf{SL}(2,\mathbb{R})$. Notice that all elements in $\mathsf{GL}(2,\mathbb{R})$ have nonzero determinant, and, moreover, all other real values are determinants of matrices in $\mathsf{GL}(2,\mathbb{R})$. Therefore, $\phi(\mathsf{GL}(2,\mathbb{R})) = \mathbb{R}^*$. By the First Isomorphism Theorem, $\mathsf{GL}(2,\mathbb{R})/\mathsf{SL}(2,\mathbb{R}) \approx \mathbb{R}^*$.

Additionally, this tells us that we can treat the cosets in $\mathsf{GL}(2,\mathbb{R})/\mathsf{SL}(2,\mathbb{R})$ as nonzero real numbers, and we did not have to perform any coset computations. ◇

The First Isomorphism Theorem offers more insight into the behavior of both homomorphisms and isomorphisms. The proofs of the corollaries below are left as exercises.

Corollary 6.4.6. *Let G and G' be finite groups. If $\phi : G \to G'$ is a homomorphism, then $|\phi(G)|$ divides $|G|$ and $|G'|$.*

Corollary 6.4.7. *For natural number $n \geq 2$, $\mathbb{Z}/\langle n \rangle \approx \mathbb{Z}_n$.*

In the Theorem 6.2.10, we see that the kernel of a homomorphism is a normal subgroup. Below is the converse of this property.

Theorem 6.4.8. *Every normal subgroup of a group G is a kernel of a homomorphism of G.*

Proof. Let G be a group and N a normal subgroup of G. Define $\phi : G \to G/N$ as $\phi(x) = xN$ for $x \in G$. The identity of G/N is the coset N. By the

definition of ϕ and property 2 of Theorem 5.1.6,

$$\begin{aligned}\ker(\phi) &= \{g \in G \,|\, \phi(g) \in N\} \\ &= \{g \in G \,|\, gN \in N\} \\ &= \{g \in G \,|\, g \in N\} \\ &= N.\end{aligned}$$

Therefore, N is the kernel of the homomorphism ϕ. □

Of course, when creating delightful quotient groups, we can continue to get more complicated. Below is an example of how to compute a nested quotient group.

Example 6.4.9. In $\mathbb{Z}$, $12\mathbb{Z}$ and $3\mathbb{Z}$ are normal subgroups and $12\mathbb{Z}$ is a subgroup of $3\mathbb{Z}$. We will calculate the nested quotient group $(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z})$. First, we see

$$\mathbb{Z}/12\mathbb{Z} = \{12\mathbb{Z}, 1 + 12\mathbb{Z}, 2 + 12\mathbb{Z}, \ldots, 11 + 12\mathbb{Z}\}.$$

By calculation, we see that

$$3\mathbb{Z}/12\mathbb{Z} = \{12\mathbb{Z}, 3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}\}.$$

Therefore, by definition, the cosets in $(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z})$ are

$$\begin{aligned}(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) &= \{g + 3\mathbb{Z}/12\mathbb{Z} \mid g \in \mathbb{Z}/12\mathbb{Z}\} \\ &= \{(12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, (1 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\ &\quad (2 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, (3 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\ &\quad (4 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, (5 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\ &\quad (6 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, (7 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\ &\quad (8 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, (9 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\ &\quad (10 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, (11 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}\}\end{aligned}$$

Recall that $3\mathbb{Z}/12\mathbb{Z} = \{12\mathbb{Z}, 3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}\}$. Below we show each of these cosets explicilty.

$$\begin{aligned}(12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{12\mathbb{Z}, 3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}\} \\ (1 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{1 + 12\mathbb{Z}, 4 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 10 + 12\mathbb{Z}\} \\ (2 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{2 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 8 + 12\mathbb{Z}, 11 + 12\mathbb{Z}\} \\ (3 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}, 12 + 12\mathbb{Z}\} \\ (4 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{4 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 10 + 12\mathbb{Z}, 13 + 12\mathbb{Z}\} \\ (5 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{5 + 12\mathbb{Z}, 8 + 12\mathbb{Z}, 11 + 12\mathbb{Z}, 14 + 12\mathbb{Z}\} \\ (6 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}, 12 + 12\mathbb{Z}, 15 + 12\mathbb{Z}\} \\ (7 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{7 + 12\mathbb{Z}, 10 + 12\mathbb{Z}, 13 + 12\mathbb{Z}, 16 + 12\mathbb{Z}\} \\ (8 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{8 + 12\mathbb{Z}, 11 + 12\mathbb{Z}, 14 + 12\mathbb{Z}, 17 + 12\mathbb{Z}\} \\ (9 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{9 + 12\mathbb{Z}, 12 + 12\mathbb{Z}, 15 + 12\mathbb{Z}, 18 + 12\mathbb{Z}\} \\ (10 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{10 + 12\mathbb{Z}, 13 + 12\mathbb{Z}, 16 + 12\mathbb{Z}, 19 + 12\mathbb{Z}\} \\ (11 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{11 + 12\mathbb{Z}, 14 + 12\mathbb{Z}, 17 + 12\mathbb{Z}, 20 + 12\mathbb{Z}\}\end{aligned}$$

Recall that when considering cosets of $12\mathbb{Z}$, we can reduce our representatives

modulo 12. Therefore, our cosets are actually the following.

$$
\begin{aligned}
(12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{12\mathbb{Z}, 3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}\} \\
(1 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{1 + 12\mathbb{Z}, 4 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 10 + 12\mathbb{Z}\} \\
(2 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{2 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 8 + 12\mathbb{Z}, 11 + 12\mathbb{Z}\} \\
(3 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}, 12\mathbb{Z}\} \\
(4 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{4 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 10 + 12\mathbb{Z}, 1 + 12\mathbb{Z}\} \\
(5 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{5 + 12\mathbb{Z}, 8 + 12\mathbb{Z}, 11 + 12\mathbb{Z}, 2 + 12\mathbb{Z}\} \\
(6 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{6 + 12\mathbb{Z}, 9 + 12\mathbb{Z}, 12\mathbb{Z}, 3 + 12\mathbb{Z}\} \\
(7 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{7 + 12\mathbb{Z}, 10 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, 4 + 12\mathbb{Z}\} \\
(8 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{8 + 12\mathbb{Z}, 11 + 12\mathbb{Z}, 2 + 12\mathbb{Z}, 5 + 12\mathbb{Z}\} \\
(9 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{9 + 12\mathbb{Z}, 12\mathbb{Z}, 3 + 12\mathbb{Z}, 6 + 12\mathbb{Z}\} \\
(10 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{10 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, 4 + 12\mathbb{Z}, 7 + 12\mathbb{Z}\} \\
(11 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= \{11 + 12\mathbb{Z}, 2 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 8 + 12\mathbb{Z}\}
\end{aligned}
$$

We have some redundant cosets listed. Notice that we have the following

partitions:

$$\begin{aligned}
(12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= (3 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} \\
&= (6 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} \\
&= (9 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\
(1 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= (4 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} \\
&= (7 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} \\
&= (10 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\
(2 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} &= (5 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} \\
&= (8 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z} \\
&= (11 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}.
\end{aligned}$$

In conclusion, we see that

$$\begin{aligned}
(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) = \{&(12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\
&(1 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}, \\
&(2 + 12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}\}.
\end{aligned}$$

Notice that $(12\mathbb{Z}) + 3\mathbb{Z}/12\mathbb{Z}$ is the identity element of this quotient group. Thus, the cosets in $(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z})$ have representatives 0, 1, and 2. To simplify notation, we write this quotient group and its elements as

$$(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) = \{3\mathbb{Z}/12\mathbb{Z}, 1 + 3\mathbb{Z}/12\mathbb{Z}, 2 + 3\mathbb{Z}/12\mathbb{Z}\}.$$

We could continue the example by showing that $(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) \approx \mathbb{Z}_3$. ◇

Did that seem like a lot of work? Do nested quotient groups seem like fun?

Below is a theorem to help us simplify nested quotient groups.

Theorem 6.4.10 (Third Isomorphism Theorem)**.** *Let G be a group with normal subgroups M and N such that $N \leq M$. Then*

$$(G/N) \,/\, (M/N) \approx G/M.$$

The proof of this theorem is left as an exercise. Below is an example of the power of the Third Isomorphism Theorem.

Example 6.4.11. Revisit Example 6.4.9. Now, we'll apply the Third Isomorphism Theorem, with $G = \mathbb{Z}$, $M = 3\mathbb{Z}$, and $N = 12\mathbb{Z}$. We see that

$$(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) \approx \mathbb{Z}/3\mathbb{Z}.$$

By Corollary 6.4.7, $\mathbb{Z}_3 \approx \mathbb{Z}/3\mathbb{Z}$. Thus,

$$(\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) \approx \mathbb{Z}_3$$

as conjectured in Example 6.4.9. ◇

EXERCISES

Exercise 6.4.1. Use the First Isomorphism Theorem to prove that for any group G with identity e, $G/\{e\} \approx G$.

Exercise 6.4.2. Use the First Isomorphism Theorem to prove that for any groups G and G' with identities e and e', respecitively, $G \oplus G'/G \oplus \{e'\} \approx G'$.

Exercise 6.4.3. Recall that $\mathbb{R}^+$ is the group of positive real numbers under multiplication. Use the First Isomorphism Theorem to prove that

$$\mathbb{R}^*/\{1, -1\} \approx \mathbb{R}^+.$$

Exercise 6.4.4. Prove Corollary 6.4.6.

Exercise 6.4.5. Prove Corollary 6.4.7.

Exercise 6.4.6. Use the First Isomorphism Theorem to prove that for distinct primes p and q, $\mathbb{Z}_{pq} \approx \mathbb{Z}_p \oplus \mathbb{Z}_q$.

Exercise 6.4.7. Consider the groups $\mathbb{Z} \oplus \mathbb{Z}/\langle(2,5)\rangle$ and $\mathbb{Z}$.

a. Use the First Isomorphism Theorem to prove that $\mathbb{Z} \oplus \mathbb{Z}/\langle(2,5)\rangle \approx \mathbb{Z}$.

b. Graph the kernel on the $\mathbb{Z} \oplus \mathbb{Z}$ plane.

c. Describe the cosets in $\mathbb{Z} \oplus \mathbb{Z}/\langle(2,5)\rangle$ graphically.

d. Justify why $\mathbb{Z} \oplus \mathbb{Z}/\langle(2,5)\rangle \approx \mathbb{Z}$ by referencing your graph.

Exercise 6.4.8. Let G be a finite group with normal subgroup N. Prove that the order of the group element $gN \in G/N$ divides the order of the group element $g \in G$.

Exercise 6.4.9. Ⓢ Use the Third Isomorphism Theorem to determine the elements in $(\mathbb{Z}/30\mathbb{Z})/(6\mathbb{Z}/30\mathbb{Z})$.

Exercise 6.4.10. Use the Third Isomorphism Theorem to determine the elements in $(\mathbb{Z}/20\mathbb{Z})/(5\mathbb{Z}/20\mathbb{Z})$.

Exercise 6.4.11. Use the First Isomorphism Theorem to prove the Third Isomorphism Theorem. Let $\phi : G/N \to G/M$ be defined by $\phi(gN) = gM$.

Chapter 7

Rings

Quotes
Person

Good stuff.

7.1 Introduction to Rings

Definition 7.1.1. Ⓢ Let R be a ring. The order of R is the cardinality of the set R, denoted $|R|$.

Theorem 7.1.2. *Let R be a ring and let $a, b, c \in R$. Then*

1. $a0 = 0a = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. Ⓢ $-(-a) = a$

4. Ⓢ $-(-ab) = ab$
5. $(-a)(-b) = ab$,
6. $a(b-c) = ab - ac$, *and*
7. $(a-b)c = ac - bc$.

Moreover, if R has unity 1, then

6. $(-1)a = -a$ *and*
7. $(-1)(-1) = 1$.

Proof. Let R be a ring and let $a, b, c \in R$.

1. By the definition of additive identity, we know that $0 + a0 = a0$ and $0 + 0 = 0$. Substituting for 0, we see that $a0 = a(0 + 0)$. Recall that R is a group under addition, thus we may assume additive distributivity. Therefore, $a(0 + 0) = a0 + a0$. By transitivity of equality, we see that

$$0 + a0 = a(0 + 0) = a0 + a0.$$

   We may assume additive cancellation because R is a group under addition, thus we may cancel $a0$ on both sides of the equation above, yielding

$$0 = a0.$$

   A similar argument shows that $0a = 0$.

2. When $b \in R$, we know that $-b \in R$ because R is a group under addition. By distributivity, $a(-b) + ab = a(-b + b)$. By definition of additive inverse, $(-b) + b = 0$. Thus,

$$a(-b) + ab = a(-b + b) = a0 = 0.$$

Additing $-(ab)$ to both sides, we see that $a(-b) = -(ab)$, as desired. A similar argument shows that $(-a)b = -(ab)$

3. Ⓢ We know that $a + (-a) = 0$ by our definition of additive inverse. Consider that the negation of $(-a)$ will be $-(-a)$. By definition of the inverse, we can then assume $(-a) + (-(-a)) = 0$. Taking our two equations that are both equal to zero, we can substitute for zero to find that

$$a + (-a) = (-a) + (-(-a)).$$

A ring is commutative under addition, thus we may rearrange the first equation such that

$$(-a) + a = (-a) + (-(-a)).$$

We may assume additive cancellation here because R is a group under addition, thus we may cancel $(-a)$ on the left of both sides of the equation above yielding

$$a = (-(-a)).$$

Thus we get that $-(-a) = a$ as desired.

4. Ⓢ We can use a similar argument to show that $-(-ab) = ab$.

□

Example 7.1.3. Ⓢ The group $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is also a ring. Observe the Cayley table of its elements under addition:

$(\mathbb{Z}_2 \oplus \mathbb{Z}_3, +)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$
$(0,2)$	$(0,2)$	$(1,2)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,2)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$

We find that the operation is closed, as well as commutative. We also have the additive identity $(0,0)$. Notice that each element has an inverse, since the element $(0,0)$ appears once in each column and row. Anytime the composition of two elements creates $(0,0)$, the elements are inverses of one another.

Observe the Cayley table under multiplication of the nonzero elements of $\mathbb{Z}_2 \oplus \mathbb{Z}_3$:

$((\mathbb{Z}_2 \oplus \mathbb{Z}_3)^*, \cdot)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,0)$	$(0,0)$	$(1,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,1)$	$(0,2)$	$(0,2)$
$(1,1)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(0,2)$	$(0,0)$	$(0,2)$	$(0,2)$	$(0,1)$	$(0,1)$
$(1,2)$	$(1,0)$	$(0,2)$	$(1,2)$	$(0,1)$	$(1,1)$

We observe that the operation multiplication is closed with unity $(1,1)$. Thus, $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is a ring. $\diamond$

Recall that in groups, the generic notation for the operation is multiplication, does not necessarily imply that, in a specific group, the operation must be multiplication. Similarly, in rings, the generic notations for the operations are addition and multiplication, though a specific ring does not necessarily have those operations. In many of the examples we will study, the operations will be some variant of addition and multiplication, like addition and

multiplication modulo a natural number, or matrix addition and multiplication. Below is an example of a ring whose two operations are distinctly *not* addition and multiplication. To understand the example, we first have a definition.

Definition 7.1.4. Let A and B be sets. The symmetric difference between A and B, denoted $A\Delta B$, is the set of elements that are in A or B but not both, as shown below.

$$A\Delta B = (A - B) \cup (B - A).$$

Example 7.1.5. Let X be a set. Then $\mathcal{P}(X)$, the power set of X, is a ring under the operations Δ and $\cap$. $\diamond$

EXERCISES

Exercise 7.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a. A ring is commutative.

b. For $n \in \mathbb{N}$, D_n is a ring.

c. Ring operations are addition and multiplication.

Exercise 7.1.2. Consider the ring $R = \{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10. Does R have a unity? If so, what is it?

Exercise 7.1.3. Find an $n \in \mathbb{N}$ such that the ring $\mathbb{Z}_n$ does not have the following properties. For each of the following properties, give an example to show that the property does not hold in $\mathbb{Z}_n$. Let $a, b, c \in \mathbb{Z}_n$.

a. If $a^2 = a$, then $a = 0$ or $a = 1$.

b. If $ab = 0$, then $a = 0$ or $b = 0$.

c. If $ab = ac$ and $a \neq 0$, then $b = c$.

Exercise 7.1.4. Complete the proof of Theorem 7.1.2. Justify each step; do not simply present strings of equalities.

Exercise 7.1.5. Give an example of elements a and b in a ring R such that the equation $ax = b$ has multiple solutions. Include at least two distinct solutions in your explanation.

Exercise 7.1.6. Let A and B be sets. Show that an equivalent definition of $A\Delta B$ is

$$A\Delta B = (A \cup B) - (A \cap B).$$

7.2 Subrings

Non-Example 7.2.1. Ⓢ We justify that $\mathbb{N}$ is not a subring of $\mathbb{Z}$ below.

Let $a, b \in \mathbb{N}$ such that $a = 5$ and $b = 7$. Recall that for $\mathbb{N}$ to be a subring of $\mathbb{Z}$, $a - b \in \mathbb{N}$. Notice that $5 - 7 = -2 \notin \mathbb{N}$. This shows that $\mathbb{N}$ does not have closure over subtraction. Therefore, $\mathbb{N}$ is not a subring of $\mathbb{Z}$, as desired. $\diamond$

Theorem 7.2.2 (Subring Test)**.** *Let R be a ring and let $S \subseteq R$ be nonempty. For $a, b \in S$, if*

1. *$a - b \in S$, and*
2. *$ab \in S$*

then S is a subring of R.

Proof. Let R be a ring and let $S \subseteq R$ be nonempty. Assume S is closed under subtraction and multiplication, that is, for all $a, b \in S$, $a - b, ab \in S$.

To show that S is a subgroup of R under addition, we will use the One-Step Subgroup Test. Recall that the additive version of the One-Step Subgroup Test claims that if the subset is closed over subtraction, then the subset is a subgroup. Therefore, S is a subgroup of R under addition. Further, by the definition of a ring, R is an Abelian group under addition. As S is a subset of R, S is also Abelian.

By assumption, S is closed under multiplication, therefore multiplication is a binary operation on S. By the definition of a ring, associativity and distributivity hold in R. As S is a subset of R, associativity and distributivity also hold in S.

Therefore, S is a ring, and as it is a subset of R with the same operations, S is a subring of R. □

Example 7.2.3. Ⓢ The set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. Note that $0 = 0 + 0i \in \mathbb{Z}[i]$, and that $\mathbb{Z}[i] \subset \mathbb{C}$. Now let $x, y \in \mathbb{Z}[i]$. Then $x = a+bi$ and $y = c+di$ for $a, b, c, d \in \mathbb{Z}$. Note that $x-y = a+bi-(c+di) = (a-c)+(b-d)i$, where $(a-c), (b-d) \in \mathbb{Z}$, by closure of integer addition. Further, $xy = (a+bi)(c+di) = ac+adi+bci-bd = (ac-bd)+(ad+bc)i$ where $(ac-bd), (ad+bc) \in \mathbb{Z}$ under closure of integer addition and multiplication. Thus, $\mathbb{Z}[i]$ passes the Subring Test. ◇

Non-Example 7.2.4. Ⓢ Let $\mathbb{I}$ be the imaginary numbers with integer coefficients. The set $\mathbb{Z} \cup \mathbb{I}$ is not a subring of $\mathbb{C}$. Let $a \in \mathbb{Z}$ and $b \in \mathbb{I}$, $a, b \neq 0$. Then $a - b = a - ci$ for some $c \in \mathbb{Z}$, $c \neq 0$. Thus, $a - b \notin \mathbb{Z}$ and $a - b \notin \mathbb{I}$. Hence, S fails the subring test. ◇

Below is an example of how to use the Subring Test in a proof.

Theorem 7.2.5. *For $n \in \mathbb{N}$, the subset $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.*

Proof. Let $n \in \mathbb{N}$ and consider the set $n\mathbb{Z}$. In Exercise 4.2.9, we proved that

$n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Therefore, for all $x, y \in n\mathbb{Z}$, $x - y \in n\mathbb{Z}$, because a group is closed and contains inverses.

Consider elements $x, y \in n\mathbb{Z}$. Then $x = nx'$ and $y = ny'$ for some $x', y' \in n\mathbb{Z}$. Moreover,

$$xy = (nx')(ny') = n(x'ny')$$

is an element of $n\mathbb{Z}$. Therefore, by the Subring Test, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. □

Definition 7.2.6. The set of Gaussian integers, denoted, $\mathbb{Z}[i]$, is the set

$$\mathbb{Z}[i] = \{a + bi \,|\, a, b \in Z\}.$$

EXERCISES

Exercise 7.2.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a.

Exercise 7.2.2. Ⓢ For each of the following sets, S, determine if S is a subring of $\mathbb{C}$ and justify your answer. Let $\mathbb{I}$ be the imaginary numbers with integer coefficients.

a. $S = \{a + bi \mid a, b \in \mathbb{Z}, a = b\}$.

b. $S = \{a + bi \mid a, b \in \mathbb{Z}, a = -b\}$.

c. $S = \{a + bi \mid a, b \in \mathbb{Z}, a = \pm b\} \cup \mathbb{Z} \cup \mathbb{I}$.

Exercise 7.2.3. Find an example of a subset S of a ring R that is a subgroup of R under addition but not a subring. Prove that S is a subgroup. Give an example to prove that S is not a subring.

Exercise 7.2.4. Ⓢ We know that the ring $3\mathbb{Z}$ does not have unity. Find a subset of $3\mathbb{Z}$ under a modulo of your choosing that does have unity. Use a Cayley table under multiplication to prove your subset has unity.

Exercise 7.2.5. Prove that the Gaussian integers form a subring of $\mathbb{C}$.

Exercise 7.2.6. Let R be a ring with element a. Show that $S = \{r \in R \,|\, ar = 0\}$ is a subring of R.

Exercise 7.2.7. Let $U(\mathbb{Z}[i])$ denote the units of the Gaussian integers, $\mathbb{Z}[i]$.

a. Find $U(\mathbb{Z}[i])$ and prove that the set you found is correct and complete.

b. Is $U(\mathbb{Z}[i])$ a subring of $\mathbb{Z}[i]$? If so, prove it. If not, explain why not.

7.3 Integral Domains

Definition 7.3.1. Let R be a commutative ring. A zero-divisor is an element $a \in R$ such that there exists a nonzero $b \in R$ such that $ab = 0$.

Example 7.3.2. Ⓢ Here we see that external direct products can also have zero-divisors. Consider the external direct product $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. We know $(1,0) \cdot (0,1) = (0,0)$, yet $(1,0) \neq (0,0)$ and $(0,1) \neq (0,0)$, thus $(1,0)$ and $(0,1)$ are zero-divisors. Similarly, $(0,2) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is also a zero-divisor. ◇

Example 7.3.3. Consider the commutative ring $\mathbb{Z}_{10}$. We know $2 \cdot 5 = 0$, yet $2 \neq 0$ and $5 \neq 0$, thus 2 and 5 are zero-divisors. Similarly, $4, 6, 8 \in \mathbb{Z}_{10}$ are also zero-divisors. ◇

Definition 7.3.4. An integral domain is a commutative ring with unity and without zero-divisors.

Theorem 7.3.5. *Let D be an integral domain and $a, b, c \in D$. If $ab = ac$ and $a \neq 0$, then $b = c$.*

EXERCISES

Exercise 7.3.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a. A ring of infinite order has a zero-divisor.

Exercise 7.3.2. Ⓢ Let $R = \mathbb{Z}_{35}$. Which elements of R, if any, are zero-divisors?

Exercise 7.3.3. Revisit Theorem 7.3.5.

a. Prove Theorem 7.3.5.

b. Prove that a commutative ring with multiplication cancellation is an integral domain.

Exercise 7.3.4. **a.** Find the set of zero-divisors in $\mathbb{Z}_{20}$. Compare this to the set $U(20)$.

b. Show that every element $r \in \mathbb{Z}_{20}^*$ is either a unit or a zero-divisor.

Exercise 7.3.5. Find an example of an element in a ring that is neither a unit nor a zero-divisor.

Exercise 7.3.6. Give an example of a commutative ring that does not have any zero-divisors, yet is not an integral domain.

Exercise 7.3.7. Ⓢ Let $R = \mathcal{P}(\{1, 2, 3\})$ under the operations $\cap$ and Δ.

a. What is the additive identity?

b. What is the additive inverse of $\{1, 2\}$?

c. Let $a \in \mathcal{P}(\{1, 2, 3\})$. What is the additive inverse of a?

d. Determine if R is an integral domain and justify your answer.

e. Does R have unity, and if so, what is it?

f. Which elements have multiplicative inverses? Justify your answer.

7.4 Ideals

This is the ring-equivalent of a normal subgroup.

Definition 7.4.1. Let R be a ring. A subring I of R is an ideal if for every $r \in R$ and every $a \in I$, $ra, ar \in I$.

A subring I is an ideal if, for every $r \in R$, $rI = \{ra \,|\, a \in I\}$ and $Ir = \{ar \,|\, a \in I\}$ are both subsets of I. In a sense, I "absorbs" elements from r because its elements can be composed with elements in $R - I$ and that composition will always land in I.

Theorem 7.4.2. *Let R be a ring with element r and let I be a nonempty subset of R with elements a and b. Then I is an ideal of R if*

1. $a - b \in I$, *and*
2. $ra, ar \in I$.

Definition 7.4.3. Let R be a commutative ring with unity. For $a \in R$, the set

$$\langle a \rangle = \{ra \,|\, r \in R\}$$

is the principal ideal generated by a.

Example 7.4.4. In the ring $\mathbb{Z}$, the principal ideal generated by 2 is

$$\langle 2 \rangle = \{2r \,|\, r \in \mathbb{Z}\} = 2\mathbb{Z}.$$

In the ring $\mathbb{Z}[x]$, the principal ideal generated by 2 is

$$\langle 2 \rangle = \{2r \,|\, r \in \mathbb{Z}[x]\},$$

which is the set of integer polynomials with even coefficients and even constants. ◇

Non-Example 7.4.5. The ring $2\mathbb{Z}$ is commutative but does not have unity, thus we can not use ring elements to generate principal ideals. Suppose, for a moment, that we wanted to use $2 \in 2\mathbb{Z}$ as a generator. Then we would create the set of all elements in $2\mathbb{Z}$ multiplied by 2, which would create the set of all multiples of 4. This means that 2 would not actually be in the ideal it "generated." Weird, right? Thus, when we generate principal ideals, we do so in commutative rings with unity. ◇

Definition 7.4.6. Let R be a commutative ring with unity and let $a, b \in R$. Then the ideal generated by a and b is

$$\langle a, b \rangle = \{r_1 a + r_2 b \,|\, r_1, r_2 \in R\},$$

which is the linear combination of elements a and b.

Of course, the definition of $\langle a, b \rangle$ could be extended to any finite number of generators. Below is an example with two generators.

Example 7.4.7. Consider the ring $\mathbb{Z}[x]$. The ideal generated by $2, x \in \mathbb{Z}[x]$ is

$$\langle 2, x \rangle = \{2r_1(x) + xr_2(x) \,|\, r_1(x), r_2(x) \in \mathbb{Z}[x]\}.$$

Notice that $2r_1(x)$ will generate all polynomials with even coefficients and even constants. Also notice that $xr_2(x)$ will generate all polynomials with

a constant term of zero. Thus, when we take linear combinations of even polynomials and polynomials without a constant term, we will create

$$\langle 2, x\rangle = \{a_n^x n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \,|\, n \in \mathbb{N}, a_0 \text{ is even}\},$$

the set of polynomials with even constant term. For example, consider the polynomials $r_1(x) = 3x^2+5, r_2(x) = 7x-1 \in \mathbb{Z}[x]$. These polynomials create the element

$$2r_1(x) + xr_2(x) = 2 \cdot (3x^2 + 5) + x \cdot (7x - 1) = 13x^2 - x + 10 \in \langle 2, x\rangle.$$

Notice that this polynomial has odd coefficients and its constant term is even. ◇

Definition 7.4.8. Let R be a commutative ring with elements a and b. Let I be a proper ideal of R. Then I is a prime ideal if $ab \in I$ implies that $a \in I$ or $b \in I$.

Non-Example 7.4.9. The ring $\mathbb{Z}$ is commutative and has unity, thus we can consider the principal ideals generated by its elements. Consider the ideal $\langle 12\rangle$. Notice that $12 = 3 \times 4$, where $3, 4 \in \mathbb{Z} - \langle 12\rangle$. Thus, 12 is an element of the ideal even though none of its factors (in this decomposition) is in the ideal. Therefore, $\langle 12\rangle$ is not a prime ideal. ◇

Example 7.4.10. The ideal $\langle 7\rangle$ is a prime ideal of the ring $\mathbb{Z}$. Any $x \in \langle 7\rangle$ has form $x = 7y$ for $y \in \mathbb{Z}$. The factor 7 can not be decomposed further because it is prime. Thus, because every decomposition of every element in $\langle 7\rangle$ will include a 7, which is an element of $\langle 7\rangle$, the ideal $\langle 7\rangle$ is prime. ◇

Definition 7.4.11. Let R be a commutative ring and let I be a proper ideal of R. Let J be an ideal of R. Then I is a maximal ideal if $I \subseteq J \subseteq R$ implies that either $J = I$ or $J = R$.

In a sense, a proper ideal is maximal if the only ideal that contains it is the ring itself.

Non-Example 7.4.12. Consider the ideal $\langle 12 \rangle$ in ring $\mathbb{Z}$. The ideals $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, and $\langle 6 \rangle$ are all proper ideals that contain $\langle 12 \rangle$. Thus, $\langle 12 \rangle$ is not a maximal ideal. $\diamond$

Example 7.4.13. The ring $\mathbb{Z}_{10}$ is commutative and has unity, thus we can consider the principal ideals generated by its elements. Consider the ideal $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$. This ideal is maximal.

To see that $\langle 2 \rangle$ is maximal, by way of contradiction, assume that it is not. Then there must be some proper ideal, say J such that $\langle 2 \rangle \subset J \subset \mathbb{Z}_{10}$. This means that J must contain at least one element in $\mathbb{Z}_{10} - \langle 2 \rangle$, without loss of generality, suppose J contains $3 \in \mathbb{Z}_{10} - \langle 2 \rangle$. Thus we know that

$$0, 2, 4, 6, 8, \text{ and } 3$$

are all elements of J. Now, in order for J to be a maximal ideal, it must be a subring. As we just introduced a new element into our subset, we turn back to the definition of subring to determine if the inclusion of 3 forces us to include any other elements of $\mathbb{Z}_{10} - \langle 2 \rangle$ in J.

A subring is a subgroup under addition, thus J must be closed under addition. We know that two evens added together will produce an even number, thus

we focus on the element $3 \in J$. Below, we add 3 to the elements of J:

$$\begin{aligned} 3+0 &= 3, \\ 3+2 &= 5, \\ 3+4 &= 7, \\ 3+6 &= 9, \\ 3+8 &= 1, \\ 3+3 &= 6. \end{aligned}$$

Thus, by the additive closure property of rings, J needs to include the elements $1, 5, 7, 9 \in \mathbb{Z}_{10}$. This means that J now includes the elements

$$0, 2, 3, 4, 6, 8, 1, 3, 5, 7, \text{ and } 9.$$

Thus, $J = \mathbb{Z}_{10}$. This is a contradiction! We assumed that $\langle 2 \rangle$ was not maximal, meaning that we could find a proper ideal containing $\langle 2 \rangle$. We could not find such a proper ideal, thus it must be that $\langle 2 \rangle$ is maximal after all. $\diamond$

Example 7.4.14. The ideal $\langle 2 \rangle$ in $\mathbb{Z}$ is a maximal ideal. Similarly, the ideal $\langle 3 \rangle$ in $\mathbb{Z}$ is a maximal ideal. $\diamond$

Example 7.4.15. The ideal $\langle 2 \rangle$ in $\mathbb{Z}_{12}$ is a maximal ideal. Similarly, the ideal $\langle 3 \rangle$ in $\mathbb{Z}_{12}$ is a maximal ideal. Notice that these ideals have different orders, and both are maximal. $\diamond$

Below is an example of an ideal is that is maximal but not prime.

Example 7.4.16. Consider the ring $R = \{0, 2, 4, 6\}$ under arithmetic modulo 8. This is a commutative ring without unity, thus we can not create principal ideals, though we can consider prime and maximal ideals. Notice

that $I = \{0, 4\}$ is an ideal because it is a subring and

$$\begin{aligned} rI &= \{ra \,|\, r \in R,\, a \in I\} \\ &= \{0 \cdot 0, 2 \cdot 0, 4 \cdot 0, 6 \cdot 0, 0 \cdot 4, 2 \cdot 4, 4 \cdot 4, 6 \cdot 4\} \\ &= I. \end{aligned}$$

Is I prime? No. Notice that $4 \in I$ and $4 = 2 \cdot 2$, where $2 \notin I$. Thus, because $4 \in I$ can be decomposed into factors not in I, I is not a prime ideal.

Is I maximal? Yes. Suppose, by way of contradiction, J is some proper ideal such that $I \subset J \subset R$. Then J must contain either 2 or 6, but not both. If J contains 2, then by additive closure, J must contain $2 + 4 = 6$. If J contains 6, then by additive closure, J must contain $4 + 6 = 2$. Thus, J can not exist, and therefore, I is maximal. ◇

Below is an example of an ideal is that is prime but not maximal.

Example 7.4.17. Consider the ring $\mathbb{Z}[x]$. Below are two examples of prime ideals, neither of which is maximal.

- The ideal $\langle 2 \rangle$ is prime.
- The ideal $\langle x \rangle = \{rx \,|\, r \in \mathbb{Z}[x]\}$ is prime.

Both $\langle 2 \rangle$ and $\langle x \rangle$ are contained in $\langle 2, x \rangle$, the ideal of polynomials with even constant term, thus neither $\langle 2 \rangle$ nor $\langle x \rangle$ is maximal. ◇

EXERCISES

Exercise 7.4.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a. An ideal is a subring.

b. In a ring, the maximal ideals have the same cardinality.

Exercise 7.4.2. Ⓢ Show that $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Exercise 7.4.3. Consider the subset $S = \{a + bi \,|\, a, b \in \mathbb{Z},\, b \in 2\mathbb{Z}\} \subseteq \mathbb{Z}[i]$. Prove that S is a subring of $\mathbb{Z}[i]$ but not an ideal of $\mathbb{Z}[i]$.

Exercise 7.4.4. Let R be a commutative ring with unity. Prove that $\langle a \rangle$ is an ideal for every $a \in R$.

Exercise 7.4.5. Let A and B be ideals of ring R. Prove that

$$A + B = \{a + b \,|\, a \in A, b \in B\}$$

is an ideal of R.

Exercise 7.4.6. Our definition of ideal is technically the definition of a *two-sided* ideal.

a. Create the definitions for a left ideal and a right ideal.

b. Show that the subset

$$D = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} : b, d \in \mathbb{R} \right\}$$

is a left ideal of the ring $M_2(\mathbb{R})$.

c. Show that the subset

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : b, d \in \mathbb{R} \right\}$$

is a right ideal of the ring $M_2(\mathbb{R})$.

Exercise 7.4.7. Let R be a ring and I an ideal of R.

a. Prove that if $1 \in I$, then $I = R$.

b. Prove that if $u \in I$ is a unit, then $I = R$.

Exercise 7.4.8. Find all of the maximal ideals in each of the following. Justify why these ideals are maximal.

a. $\mathbb{Z}_8$

b. $\mathbb{Z}_{15}$

c. $\mathbb{Z}_{20}$

d. $\mathbb{Z}_n$, $n \in \mathbb{N}$ and $n \geq 2$

Exercise 7.4.9. Let $n \in \mathbb{N}$.

a. Prove that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

b. Prove that $n\mathbb{Z}$ is a prime ideal if and only if n is prime.

Exercise 7.4.10. Consider the ring $R = \{0, 2, 4, 6, 8, 10\}$ under modulo 12 arithmetic. Find an ideal in R that is maximal but not prime. Prove your set meets these qualifications.

7.5 Fields

As we have seen, multiplication can behave rather unexpectedly in rings. Below is a definition of a type of ring in which multiplication behaves quite nicely.

Definition 7.5.1. A field is a commutative ring with unity in which every nonzero element is a unit.

Thus, a field is a ring in which every nonzero element has a multiplicative inverse.

Non-Example 7.5.2. The ring $\mathbb{Z}$ is not a field because, for example, $7 \in \mathbb{Z}$ does not have a multiplicative inverse. $\diamond$

Example 7.5.3. The rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all are fields because every nonzero element has a multiplicative inverse. $\diamond$

Example 7.5.4. Ⓢ Take the ring $3\mathbb{Z}$. Notice $3\mathbb{Z}$ is a group under addition but $3\mathbb{Z}^*$ is not a group under multiplication, because, for

$$3\mathbb{Z} = \{..., -6, -3, 0, 3, 6, 9, 12, 15, ...\},$$

there are no inverses for elements in the set. Therefore, $3\mathbb{Z}$ is not a field. $\diamond$

Non-Example 7.5.5. The ring $\mathbb{Z}_{12}$ is not a field because, for example, $4 \in \mathbb{Z}_{12}$ does not have a multiplicative inverse. $\diamond$

Example 7.5.6. The ring $\mathbb{Z}_7$ is a field. Below is the Cayley table of $\mathbb{Z}_7^*$ under multiplication. Notice that every element has an inverse.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

We see that $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, and $6^{-1} = 6$. $\diamond$

Definition 7.5.7. Ⓢ Let F be a ring. The order of F is the cardinality of the set F, denoted $|F|$.

A field is always an integral domain, though the converse is not necessarily true. Below is a theorem about a case when the converse is true.

Theorem 7.5.8. *A finite integral domain is a field.*

Proof. Let D be a finite integral domain, thus D is commutative and has unity. The unity is its own inverse, thus take some element $d \neq 0 \in D$ that is not the unity. Consider the set of elements d generates multiplicatively:

$$\{d, d^2, d^3, \ldots\}.$$

By Lemma 3.6.13, because D is finite, $d^i = d^j$ for some $i, j \in \mathbb{N}$. Without loss of generality, we may assume $i > j$, say $i = j + k$ for some $k \in \mathbb{N}$. Then $d^i = d^{j+k} = d^j d^k$. By transivity of equality,

$$d^j d^k = d^j.$$

Recall that D is an integral domain, thus by Theorem 7.3.5, we may cancel d^j from both sides of the equation, yielding $d^k = 1$. This implies that

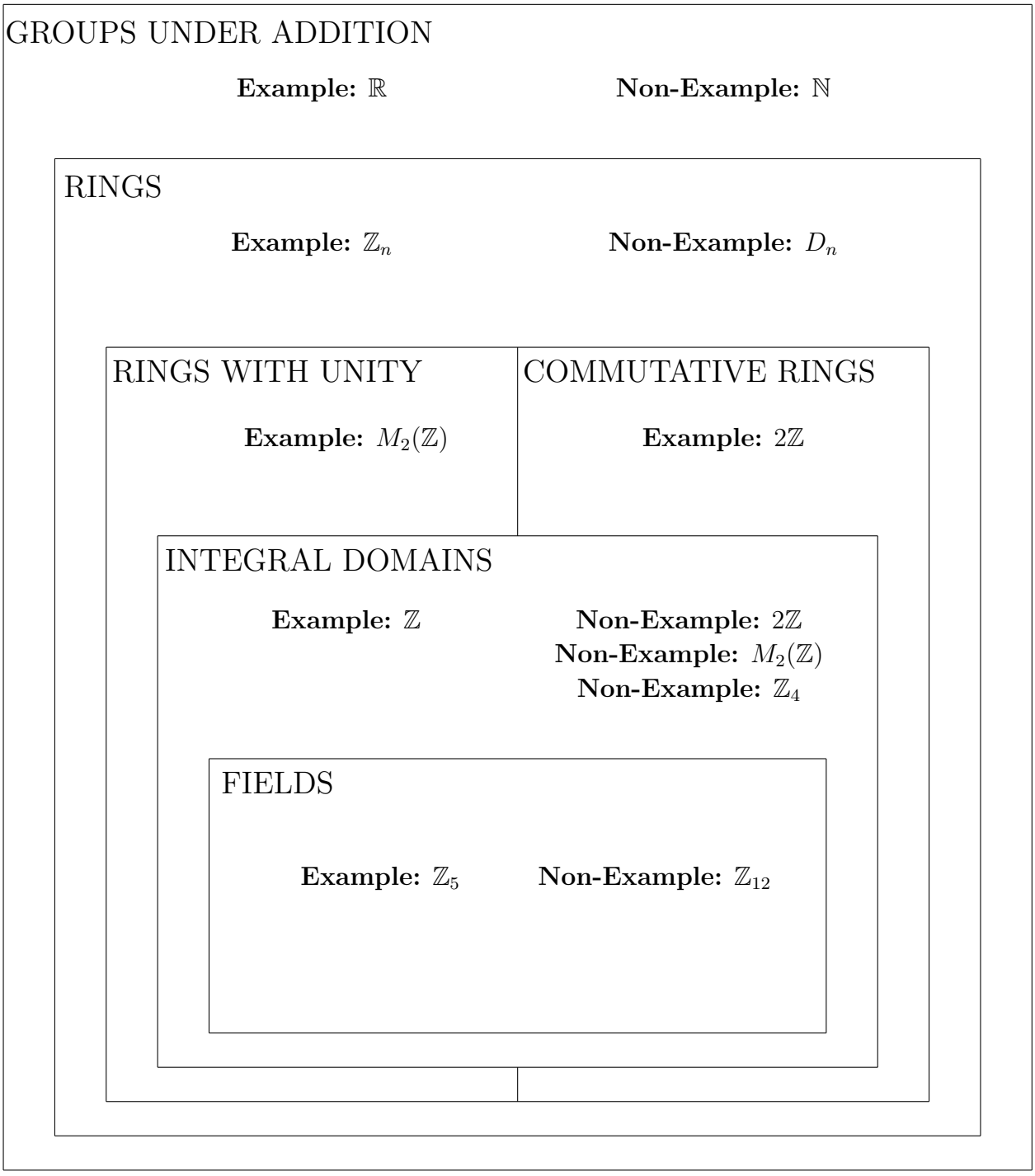
$$d^k = d^{k-1} d = 1,$$

showing that d^{k-1} is the multiplicative inverse of d. We chose $d \in D$ arbitrarily, thus every nonzero element in D has a multiplicative inverse. Therefore, D is a field. □

The proof of the following is left as an exercise.

Corollary 7.5.9. *Let p be a prime. Then $\mathbb{Z}_p$ is a field.*

Example 7.5.10. Ⓢ The diagram below shows the nested "niceness" of groups, rings, and fields.


GROUPS UNDER ADDITION
Example: $\mathbb{R}$
Non-Example: $\mathbb{N}$
RINGS
Example: $\mathbb{Z}_n$
Non-Example: D_n
RINGS WITH UNITY
Example: $M_2(\mathbb{Z})$
COMMUTATIVE RINGS
Example: $2\mathbb{Z}$
INTEGRAL DOMAINS
Example: $\mathbb{Z}$
Non-Example: $2\mathbb{Z}$
Non-Example: $M_2(\mathbb{Z})$
Non-Example: $\mathbb{Z}_4$
FIELDS
Example: $\mathbb{Z}_5$
Non-Example: $\mathbb{Z}_{12}$

◇

As with groups and rings, fields have subsets that are also fields, and once again, we have a two-step test for such a subset.

Theorem 7.5.11. *Let F be a field and K a subset of F with at least two elements. Then K is a subfield of F if for every $a, b \in K$ and $b \neq 0$,*

1. *$a - b \in K$, and*
2. *$ab^{-1} \in K$.*

Example 7.5.12. Ⓢ This is an example of determining that $\mathbb{Q}$ is a subfield of $\mathbb{C}$. We can prove this by using Theorem 7.5.11. First we can see that $\mathbb{Q}$ has at least 2 elements because it has 0 and 1. Now let $a, b \in \mathbb{Q}$. Thus we can let

$$a = \frac{x}{y} \text{ and } b = \frac{w}{z}$$

where $w, x \in \mathbb{Z}$ and $y, z \in \mathbb{Z}^*$. So we can see that $a - b = \frac{x}{y} - \frac{w}{z} = \frac{xz - wy}{yz}$. Now because the integers are closed under addition and multiplication, $xz - wy \in \mathbb{Z}$ and $yz \in \mathbb{Z}^*$ because $\mathbb{Z}$ has no zero-divisors, and thus we know that $a - b \in \mathbb{Q}$. We can also see that the inverse of b under multiplication will be $\frac{z}{w}$ when $b \neq 0$. Thus

$$ab^{-1} = \frac{x}{y} \cdot \frac{z}{w} = \frac{xz}{wy}.$$

Again because the integers are closed under multiplication we know that $ab^{-1} \in \mathbb{Q}$. Therefore by Theorem 7.5.11 we know that $\mathbb{Q}$ will be a subfield of $\mathbb{C}$. ◇

EXERCISES

Exercise 7.5.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response.

a. If F is a field and $x \in F$, then x is a unit.

b. For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a field.

Exercise 7.5.2. Give an example of an integral domain that is not a field and contains $\mathbb{C}$.

Exercise 7.5.3. Consider the ring $R = \{0, 2, 4, 6, 8\}$ under modulo 10 arithmetic. Make a Cayley table for R under addition. Make a Cayley table for R^* under multiplication. Is R a field?

Exercise 7.5.4. For $n \in \mathbb{N}$, what is the difference between $\mathbb{Z}_n[i]^*$ and $\mathbb{Z}_n^*[i]$?

Exercise 7.5.5. For each of the following $n \in \mathbb{N}$, is $\mathbb{Z}_n[i]$ a field? If so, create the Cayley table for $\mathbb{Z}_2[i]^*$. If not, explain why not.

a. $n = 2$

b. $n = 3$

Exercise 7.5.6. Prove Corollary 7.5.9.

Exercise 7.5.7. Ⓢ Let K, H and G be rings. Prove if K is a subfield of H and H is a subfield of G, then K is a subfield of G.

Exercise 7.5.8. **a.** Give an example of a field F with subfield K.

b. Prove the Subfield Test. *(Hint: Use the One-Step Subgroup Test twice.)*

7.6 Characteristic of a Ring

Recall that in a group G under addition, the order of an element $g \in G$ is the smallest $n \in \mathbb{N}$ such that n copies of g yields the additive identity, that is, $ng = 0$. Similarly, in a group G under multiplication, the order of an element $g \in G$ is the smallest $n \in \mathbb{N}$ such that n copies of g yields the multiplicative

identity, that is, $g^n = 1$. In either case, if no such $n \in \mathbb{N}$ exists, the order of g is infinite. The definition below is a bit a like order, only now that we are studying rings, we mix multiplication with the additive identity.

Definition 7.6.1. Let R be a ring. If there exists an $n \in \mathbb{N}$ such that $nx = 0$ for all $x \in R$, then the smallest such n is the characteristic of R. If no such $n \in \mathbb{N}$ exists, then R has characteristic 0. In both cases, the characteristic of ring R is denoted $\mathsf{char}(R)$.

Example 7.6.2. The characteristic of $\mathbb{Z}_3$ is 3. The table below shows the values of nx for all $x \in \mathbb{Z}_3$, beginning with $n = 0$.

n	0	1	2
1	0	1	2
2	0	2	1
3	0	0	0

Notice that $n = 3$ is the smallest positive integer such that $nx = 0$ for all $x \in \mathbb{Z}_3$. Thus, $\mathsf{char}(R) = 3$. ◇

Example 7.6.3. The characteristic of $\mathbb{Z}_4$ is 4. The table below shows the values of nx for all $x \in \mathbb{Z}_4$, beginning with $n = 0$.

n	0	1	2	3
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1
4	0	0	0	0

Notice that $n = 2$ is the smallest positive integer such that $nx = 0$ for all $x \in \mathbb{Z}_4$. Thus, $\mathsf{char}(R) = 4$. ◇

Example 7.6.4. Let $R = \{0, 5, 10, 15, 20, 25\}$ under modulo 30 arithmetic. The table below shows the values of nx for all $x \in R$, beginning with $n = 0$.

n	0	5	10	15	20	25
1	0	5	10	15	20	25
2	0	10	20	0	10	20
3	0	15	0	15	0	15
4	0	20	10	0	20	10
5	0	25	20	15	10	5
6	0	0	0	0	0	0

Notice that $n = 6$ is the smallest positive integer such that $nx = 0$ for all $x \in R$. Thus, $\mathsf{char}(R) = 6$. ◇

Example 7.6.5. Consider the ring $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. The table below shows the values of $n(x, y)$ for all $(x, y) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$, beginning with $n = 0$.

n	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
1	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
2	$(0,0)$	$(0,2)$	$(0,1)$	$(0,0)$	$(0,2)$	$(0,1)$
3	$(0,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$	$(1,0)$
4	$(0,0)$	$(0,1)$	$(0,2)$	$(0,0)$	$(0,1)$	$(0,2)$
5	$(0,0)$	$(0,2)$	$(0,1)$	$(1,0)$	$(1,2)$	$(1,1)$
6	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$

Thus, $\mathsf{char}(\mathbb{Z}_2 \oplus \mathbb{Z}_3) = 6$. ◇

Example 7.6.6. The characteristic of $\mathbb{Z}_5[i]$ is 5. Let $x = a + bi \in \mathbb{Z}_5[i]$, thus $a, b \in \mathbb{Z}_5$. Then

$$5x = 5(a + bi) = 5a + 5bi = 0 + 0i = 0,$$

hence $\mathsf{char}(\mathbb{Z}_5[i]) \leq 5$. To show that $\mathsf{char}(\mathbb{Z}_5[i])$ is equal to 5, we must show that 5 the smallest $n \in \mathbb{N}$ such that $nx = 0$ for all $x \in \mathbb{Z}_5[i]$. Recall that $1 \in \mathbb{Z}_5$ has order 5 under addition. Thus, for $1 \in \mathbb{Z}_5[i]$, $n \cdot 1 = 0$ for $n = 5$, and $n = 5$ is the smallest such number. Therefore, $\mathsf{char}(\mathbb{Z}_5[i]) = 5$, even though $|\mathbb{Z}_5[i]| = 25$. $\diamond$

This example hints at that theorem below. Its proof is left as an exercise.

Theorem 7.6.7. *Let R be a ring with unity 1. If the order of 1 under addition is infinite, then $\mathsf{char}(R) = 0$. If the order of 1 under addition is n, then $\mathsf{char}(R) = n$.*

Recall that integral domains are a specific, "nicer" type of ring. Thus, we can strengthen Theorem 7.6.7 if we assume the ring is an integral domain.

Theorem 7.6.8. *Let D be an integral domain. Then $\mathsf{char}(D)$ is either 0 or prime.*

Proof. Let D be an integral domain. Thus, D has unity 1. If the order of 1 under addition is infinite, then by Theorem 7.6.7, $\mathsf{char}(D) = 0$.

Assume the order of 1 under addition is n, where $n \in \mathbb{N}$. By the definition of order under addition, $n \cdot 1 = 0$. Further, suppose n can be factored as $n = jk$, where $j, k \in \mathbb{N}$. Then

$$0 = n \cdot 1 = (jk) \cdot 1 = (j \cdot 1)(k \cdot 1).$$

Thus, we have two factors, $(j \cdot 1)$ and $(k \cdot 1)$, whose product is 0. As D is an integral domain, which as no zero divisors, either $(j \cdot 1)$ or $(k \cdot 1)$ must be 0.

Without loss of generality, suppose $(j \cdot 1) = 0$. Recall that n is the smallest natural number such that $n \cdot 1 = 0$, thus $n \leq j$. Also recall that j is a factor

of n, hence $j \leq n$. Therefore, $j = n$. Hence, the only way to decompose n into positive factors is $n = n \cdot 1$, which means that n is prime.

Hence, the order of 1 under addition is prime. By Theorem 7.6.7, $\mathsf{char}(D)$ is also prime. □

EXERCISES

Exercise 7.6.1. Prove Theorem 7.6.7.

Exercise 7.6.2. Let F be a field of order 3^n, for $n \in \mathbb{N}$. Prove that $\mathsf{char}(F) = 3$.

Exercise 7.6.3. Let R be a ring with elements x and y. Suppose $\mathsf{char}(R) = n$, where $n \in \mathbb{N}$. Consider the expression $(x + y)^n$.

a. When $n = 2$, show that

$$(x + y)^2 = x^2 + y^2.$$

b. When $n = 3$, show that

$$(x + y)^3 = x^3 + y^3.$$

c. Let $n = 4$. Find an example of $x, y \in R$ such that $(x + y)^4 \neq x^4 + y^4$.

d. Conjecture about the expansion of $(x + y)^p$ for general prime p.

Exercise 7.6.4. Ⓢ Consider the ring $\mathbb{Z}_p \oplus \mathbb{Z}_q$ such that $p, q \in \mathbb{N}$ and p and q are relatively prime. What is the characteristic of the ring?

Exercise 7.6.5. Ⓢ **a.** What is the characteristic of $\mathbb{Z}_{15} \oplus \mathbb{Z}_{20}$?

b. Prove that $\mathsf{char}(\mathbb{Z}_m \oplus \mathbb{Z}_n) = \mathsf{lcm}(m, n)$ where $m, n \geq 2$.

c. Conjecture about the value of $\mathsf{char}(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n})$ where $n \in \mathbb{N}$ and $m_i \geq 2$.

7.7 Quotient Rings

Like with groups, given a ring, we can create a quotient ring. Recall that a quotient group is a group of cosets. Similarly, a quotient ring is a ring of cosets. Cosets in rings are defined very similarly to cosets in groups.

Recall that, given a group G, H being a subgroup of G is not sufficient for G/H to be a quotient group because the operation is not necessarily well-defined. In order for G/H to be a quotient group, H must be a normal subgroup of G. Similarly, given a ring R, S being a subring is not sufficient for R/S to be a quotient ring. In order for R/S to be a quotient ring, S must be an ideal of R, as the definitions below state, and as well will prove after a few examples.

Definition 7.7.1. Let R be a ring and I an ideal of R. For $r \in R$, the set

$$r + I = \{r + a \,|\, a \in I\}$$

is the ring coset in R containing r.

Notice that, unlike in group theory, we do not differentiate between a left coset and a right coset because rings are commutative under addition.

Definition 7.7.2. Let R be a ring and I an ideal of R. The set of cosets of I in R,

$$R/I = \{r + I \,|\, r \in R\}$$

is a ring under the operations of coset representative addition and coset representative multiplication. This ring is called the quotient ring.

Before we prove that the quotient ring is indeed a ring, we give some examples.

Example 7.7.3. Consider the ideal $6\mathbb{Z}$ in the ring $\mathbb{Z}$. Then $\mathbb{Z}/6\mathbb{Z}$ is a quotient ring. To see an example of addition and multiplication of elements in $\mathbb{Z}/6\mathbb{Z}$, consider the elements $3 + 6\mathbb{Z}$ and $4 + 6\mathbb{Z}$ in $\mathbb{Z}/6\mathbb{Z}$. Below is an example of addition:

$$(3 + 6\mathbb{Z}) + (4 + 6\mathbb{Z}) = (3 + 4) + 6\mathbb{Z} = 7 + 6\mathbb{Z} = 1 + 6\mathbb{Z}.$$

Below is an example of multiplication:

$$(3 + 6\mathbb{Z}) \cdot (4 + 6\mathbb{Z}) = (3 \cdot 4) + 6\mathbb{Z} = 12 + 6\mathbb{Z} = 6\mathbb{Z}.$$

As we might expect, the coset represented by the additive identity, $0 + 6\mathbb{Z} = 6\mathbb{Z}$, is the additive identity in the quotient ring. Similarly, the coset represented by the unity, $1 + 6\mathbb{Z}$, is the unity in the quotient ring. ◇

Recall that to show that a quotient group is a group, we first showed that the operation of coset addition is well-defined. Similarly, we now show that the operation of coset multiplication is well-defined.

Lemma 7.7.4. *Let R be a ring and S a subring of R. Then coset multiplication is well-defined if and only if S is an ideal of R.*

Proof. Let R be a ring and suppose S is a subring of R. Let $u, u', v, v' \in R$ be coset representatives such that $u + S = u' + S$ and $v + S = v' + S$ and $u \neq u'$ and $v \neq v'$. Then $u = u' + s_1$ and $v = v' + s_2$ for elements $s_1, s_2 \in S$. Hence,

$$uv = (u' + s_1)(v' + s_2) = u'v' + u's_1 + v's_2 + s_1s_2$$

by distributivity. By closure, we know $s_1s_2 \in S$ because S is a subring. The elements $u's_1$ and $v's_2$ will be in S for all $u', v' \in R$ and for all $s_1, s_2 \in S$ if

and only if S is an ideal, by the definition of ideal. Thus,

$$(u+S)(v+S) = uv + S = u'v' + S = (u'+S)(v'+S)$$

if and only if S is an ideal of R. □

As the definition states, a quotient ring is indeed a ring, and the proof is left as an exercise.

Theorem 7.7.5. *Let R be a ring and I an ideal of R. The quotient ring R/I is a ring under the operations of coset representative addition and multiplication.*

Below is an example of a quotient ring without unity.

Example 7.7.6. The ring $2\mathbb{Z}$ does not have unity. In $2\mathbb{Z}$, $8\mathbb{Z}$ is an ideal, and thus we may consider the quotient ring $2\mathbb{Z}/8\mathbb{Z}$. Below is the Cayley tables of $2\mathbb{Z}/8\mathbb{Z}$ under addition.

$+$	$8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$
$8\mathbb{Z}$	$8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$
$2+8\mathbb{Z}$	$2+\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$	$8\mathbb{Z}$
$4+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$	$8\mathbb{Z}$	$2+8\mathbb{Z}$
$6+8\mathbb{Z}$	$6+8\mathbb{Z}$	$8\mathbb{Z}$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$

Below is the Cayley table of $2\mathbb{Z}/8\mathbb{Z}$ under multiplication. Notice that there is no unity.

$\cdot$	$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$6+8\mathbb{Z}$
$2+8\mathbb{Z}$	$4+8\mathbb{Z}$	$8\mathbb{Z}$	$4+8\mathbb{Z}$
$4+8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$
$6+8\mathbb{Z}$	$4+8\mathbb{Z}$	$8\mathbb{Z}$	$4+8\mathbb{Z}$

◇

The example below may seem similar to Example 7.7.6. Look for a surprising difference as you read it.

Example 7.7.7. The ring $2\mathbb{Z}$ does not have unity. In $2\mathbb{Z}$, $6\mathbb{Z}$ is an ideal, and thus we may consider the quotient ring $2\mathbb{Z}/6\mathbb{Z}$. Below are the Cayley tables of $2\mathbb{Z}/6\mathbb{Z}$ under addition and multiplication.

$+$	$6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$
$6\mathbb{Z}$	$6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$
$2+6\mathbb{Z}$	$2+\mathbb{Z}$	$4+6\mathbb{Z}$	$8\mathbb{Z}$
$4+6\mathbb{Z}$	$4+6\mathbb{Z}$	$6\mathbb{Z}$	$2+6\mathbb{Z}$

$\cdot$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$
$2+6\mathbb{Z}$	$4+6\mathbb{Z}$	$2+6\mathbb{Z}$
$4+6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$

Thus, we see that $2+6\mathbb{Z}$ is the unity of $2\mathbb{Z}/6\mathbb{Z}$. This may seem strange, because the quotient ring has unity even though the original ring $2\mathbb{Z}$ does not. ◇

Below is a particularly fun example of a quotient ring.

Example 7.7.8. The Gaussian integers form a commutative ring with unity 1, thus we may consider principal ideals in $\mathbb{Z}[i]$. Consider the principal ideal $\langle 3-i\rangle$. What are the cosets in the quotient ring $\mathbb{Z}[i]/\langle 3-i\rangle$? Certainly, they have form $a+bi+\langle 3-i\rangle$, where $a+bi\in\mathbb{Z}[i]$. What are the distinct cosets in $\mathbb{Z}[i]/\langle 3-i\rangle$? Is there a finite number of them?

We know $0+\langle 3-1\rangle$ is a coset. Further, both 0 and $3-i$ can represent the coset $0+\langle 3-1\rangle = 3-i+\langle 3-1\rangle$. Thus, 0 and $3-i$ are equivalent, because "is in the same coset as" is an equivalence relation. Therefore, in $\mathbb{Z}[i]/\langle 3-i\rangle$, $0=3-i$, which then implies that $3=i$. How does this help us determine the distinct cosets in $\mathbb{Z}[i]/\langle 3-i\rangle$?

Consider, for example, the coset $8+7i+\langle 3-i\rangle$. The relation $3=i$ implies

that $7i = 21$. Thus, $8 + 7i + \langle 3 - i \rangle = 8 + 21 + \langle 3 - i \rangle = 29 + \langle 3 - i \rangle$.

We can make another reduction on our coset representatives. If $3 = i$, then $3^2 = i^2$. Thus, $9 = -1$, which implies that $10 = 0$. Hence, we may reduce our coset representatives even further. For example,

$$\begin{aligned} 8 + 7i + \langle 3 - i \rangle &= 29 + \langle 3 - i \rangle \\ &= 10 + 10 + 9 + \langle 3 - i \rangle \\ &= 9 + \langle 3 - i \rangle. \end{aligned}$$

Thus far, we have taken a coset of the form of $a + bi + \langle 3 - i \rangle$, where $a, b \in \mathbb{Z}$, and reduced it to a coset of the form $c + \langle 3 - i \rangle$, where $c \in \mathbb{Z}$. We then showed that we could reduce the representative c using modulo 10 arithmetic. Therefore, we know the cosets

$$\langle 3 - i \rangle, 1 + \langle 3 - i \rangle, 2 + \langle 3 - i \rangle, \ldots, 9 + \langle 3 - i \rangle$$

are in $\mathbb{Z}[i]/\langle 3 - i \rangle$. Can we reduce this set any more?

To answer this question, we will show that the coset $1 + \langle 3 - i \rangle$, as an element in the quotient group $\mathbb{Z}[i]/\langle 3 - i \rangle$, has additive order 10. Notice that

$$10(1 + \langle 3 - i \rangle) = 10(1) + \langle 3 - i \rangle = 0 + \langle 3 - i \rangle = \langle 3 - i \rangle,$$

thus the order of $1 + \langle 3 - i \rangle$ divides 10. We proceed by cases.

- If the order of $1 + \langle 3 - i \rangle$ is 1, then $1 + \langle 3 - i \rangle = 0 + \langle 3 - i \rangle$, thus $1 \in \langle 3 - i \rangle$. As $\langle 3 - i \rangle$ is an ideal, this means that

  $$1 = (3 - i)(a + bi)$$

  for some $a + bi \in \mathbb{Z}[i]$. Then $1 = (3a + b) + (-a + b)i$. Solving the linear

system $1 = 3a + b$ and $0 = -a + b$ yields $a = \frac{3}{10}$ and $b = \frac{1}{10}$. This is a contradiction, because $a + bi\mathbb{Z}[i]$. Ergo, the order of $1 + \langle 3 - i \rangle$ is not 1.

- If the order of $1 + \langle 3 - i \rangle$ is 5, then

$$5(1 + \langle 3 - i \rangle) = 5 + \langle 3 - i \rangle = 0 + \langle 3 - i \rangle.$$

Similarly, this means that

$$5 = (3 - i)(a + bi)$$

for some $a + bi \in \mathbb{Z}[i]$. Solving the induced linear system, we find that $a = \frac{3}{2}$ and $b = \frac{1}{2}$, which is a contradiction. Ergo, the order of $1 + \langle 3 - i \rangle$ is not 5.

Therefore, the additive order of $1 + \langle 3 - i \rangle$, as an element of $\mathbb{Z}[i]/\langle 3 - i \rangle$ is 10. This shows that

$$\mathbb{Z}[i]/\langle 3 - i \rangle = \{a + \langle 3 - i \rangle \mid a \in \{0, 1, 2, \ldots, 9\}\}.$$

$\diamond$

Recall that there are more specific and "nice" types of rings and ideals. As the ideal is more well-behaved, the resulting quotient ring is more well-behaved, as the theorems below state.

Theorem 7.7.9. *Let R be a commutative ring with unity and let I be an ideal of R. Then R/I is an integral domain if and only if I is a prime ideal.*

Theorem 7.7.10. *Let R be a commutative ring with unity and let I be an ideal of R. Then R/I is a field if and only if I is a maximal ideal.*

EXERCISES

Exercise 7.7.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let R be a ring, S a subring of R, and I an ideal of R.

a. The set R/S is a ring.

b. The set R/I is a field.

Exercise 7.7.2. Revisit Examples 7.7.6 and 7.7.7. Find another example of a ring R with ideals I and H such that R and R/I do not have unity and R/H does have unity. Prove your claims by including the Cayley tables of R/I and R/H under multiplication. What is the unity of R/H?

Exercise 7.7.3. Prove Theorem 7.7.5.

Exercise 7.7.4. For each of the following ideals I, find all distinct cosets in $\mathbb{Z}[i]/I$. Justify your claims.

a. $I = \langle 2 - i \rangle$

b. $I = \langle 1 - 2i \rangle$

Exercise 7.7.5. Find the multiplicative inverse of each of the following cosets in the quotient ring $\mathbb{Z}_5[x]/\langle x^2 + x + 2 \rangle$. For each coset a, prove that the inverse you find, a^{-1}, is indeed the inverse by showing that $aa^{-1} = 1$.

a. $x + 4 + \langle x^2 + x + 2 \rangle$

b. $4x + 3 + \langle x^2 + x + 2 \rangle$

Exercise 7.7.6. Consider the ring $\mathbb{Z}_3[x]$ and its ideal $I = \langle x^2 + x + 1 \rangle$. Show that $\mathbb{Z}_3[x]/\langle x^2 + x + 1 \rangle$ is not a field.

7.8 Ring Homomorphisms

Definition 7.8.1. A ring homomorphism ϕ is a mapping from a ring R to a ring R' that preserves both ring operations, that is,

$$\phi(x+y) = \phi(x) + \phi(y)$$

and

$$\phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in R$.

Example 7.8.2. For natural number $n \geq 2$, the mapping $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(x) = x \bmod n$ is a ring homomophism. $\diamond$

Example 7.8.3. Consider the rings $\mathbb{Z}_{12}$ and $\mathbb{Z}_{30}$. To find a ring homomorphism $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$, we first find a group homomorphism between these groups, that is, we first focus on addition.

We know that $\phi(x) = cx$, for some $c \in \mathbb{Z}_{30}$, and, more specifically, $\phi(1) = c$. By Theorem 4.1.14, $|c|$ divides $|1| = 12$. By Corollary 5.2.3, $|c|$ divides $|\mathbb{Z}_{30}| = 30$. Thus, $|c|$ can equal 1, 2, 3, or 6. We proceed by cases.

- If $|c| = 1$, then $c = 0$. Thus, $\phi(x) = 0$.
- If $|c| = 2$, then $c = 15$. Thus, $\phi(x) = 15x$.
- If $|c| = 3$, then $c = 10$ or $c = 20$. Thus, $\phi(x) = 10x$ or $\phi(x) = 20x$.
- If $|c| = 6$, then $c = 5$ or $c = 25$. Thus, $\phi(x) = 5x$ or $\phi(x) = 25x$.

Next, we focus on multiplication. Recall that $\phi(1) = c$. A ring homomorphism preserves multiplication, thus because $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$, we

know that $c = c \cdot c$ must be true as well. By calculation, we see that

$$\begin{aligned} 0 &= 0 \cdot 0 \bmod 30 \\ 5 &\neq 5 \cdot 5 \bmod 30 \\ 10 &= 10 \cdot 10 \bmod 30 \\ 15 &= 15 \cdot 15 \bmod 30 \\ 20 &\neq 20 \cdot 20 \bmod 30 \\ 25 &= 25 \cdot 25 \bmod 30. \end{aligned}$$

Thus, there are four ring homomorphisms $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$, namely, $\phi(x) = 0$, $\phi(x) = 10x$, $\phi(x) = 15x$, and $\phi(x) = 25x$. ◇

Below is a theorem detailing these properties.

Theorem 7.8.4. *Let $\phi : R \to R'$ be a ring homomorphism from ring R to ring R', and let $r \in R$. Let S be a subring of R and let I' be an ideal of R'.*

1. *For any $n \in \mathbb{N}$, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = [\phi(r)]^n$.*
2. *The set $\phi(S)$ is a subring of R'.*
3. *If S is an ideal and ϕ is onto, then $\phi(S)$ is an ideal.*
4. *If R is commutative, then $\phi(R)$ is commutative.*
5. *If R has unity, R' is not the trivial ring, and ϕ is onto, then $\phi(1)$ is the unity of R'.*
6. *The map ϕ is an isomorphism if and only if ϕ is onto and $\ker(\phi) = \{0\}$.*
7. *If ϕ is an isomorphism, then ϕ^{-1} is an isomorphism.*

Example 7.8.5. Revisit Example 7.8.3. None of the homomorphisms were onto, and none mapped the unity of $\mathbb{Z}_{12}$ to the unity of $\mathbb{Z}_{30}$. ◇

Non-Example 7.8.6. Groups $\mathbb{Z}$ and $2\mathbb{Z}$ are isomorphic. In particular, $\phi : \mathbb{Z} \to 2\mathbb{Z}$ given by $\phi(x) = 2x$ and $\phi(x) = -2x$ are isomorphisms between these groups. As rings, there does not exist a ring ismorphism between these groups! Notice that these rings do not have the same structure, in particular, one of these rings has unity and one does not. $\diamond$

Theorem 7.8.7. *Let $\phi : R \to R'$ be a ring homomorphism from ring R to ring R'. Then* $\ker(\phi)$ *is an ideal of R.*

Theorem 7.8.8 (First Isomorphism Theorem for Rings)**.** *Let $\phi : R \to R'$ be a ring homomorphism from ring R to ring R'. Then $R/\ker(\phi) \approx \phi(R)$.*

Theorem 7.8.9. *Let R be a ring with unity* 1*. Then the mapping $\phi : \mathbb{Z} \to R$ given by $\phi(x) = x$ is a ring homomorphism.*

EXERCISES

Exercise 7.8.1. Determine if each of the following is a ring homomorphism.

a. $\phi : \mathbb{Z}_5 \to \mathbb{Z}_{10}$ given by $\phi(x) = 5x$

b. $\phi : \mathbb{Z}_5 \to \mathbb{Z}_{20}$ given by $\phi(x) = 4x$

Exercise 7.8.2. For each of the following pairs, determine if the rings are ring-isomorphic.

a. $2\mathbb{Z}$ and $3\mathbb{Z}$

b. $2\mathbb{Z}$ and $4\mathbb{Z}$

Exercise 7.8.3. Prove that $\phi : \mathbb{C} \to \mathbb{C}$ given by $\phi(a + bi) = a - bi$ is a ring automorphism.

Exercise 7.8.4. Prove Theorem 7.8.7.

Exercise 7.8.5. Prove Theorem 7.8.8.

Exercise 7.8.6. Prove that $\mathbb{Z}[x]/\langle x\rangle \approx \mathbb{Z}$. Use this result to determine if $\langle x\rangle$ is prime or maximal in $\mathbb{Z}[x]$.

Exercise 7.8.7. Prove that $\mathbb{Z}_3[i]/ \approx \mathbb{Z}_3[x]/\langle x^2+1\rangle$.

Chapter 8

Polynomials

Quote
Person

W

8.1 Polynomial Rings

Definition 8.1.1. Let R be a commutative ring. For variable x, the set of polynomials with coefficients in R,

$$\begin{aligned} R[x] &= \left\{ \sum_{i=0}^{n} a_i x^i \,\middle|\, a_i \in R \forall\, i \leq n \in \mathbb{N} \right\} \\ &= \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \,|\, a_i \in R \forall\, i \leq n \in \mathbb{N}\}, \end{aligned}$$

is the ring of polynomials over R.

Two polynomials are equal if their monomials are equal.

Notice that $R[x]$ is a ring whose elements are polynomials with coefficients in ring R. We do not explicitly state the domain and codomain of these polynomials, nor do we necessarily care. We are interested in these polynomials as elements, and not necessarily as functions. For $f(x), g(x) \in R[x]$, think of $f(x)$ and $g(x)$ as elements in the polynomial ring; do not think of them simply by the maps they induce. To see the difference, consider the example below.

Example 8.1.2. Consider the ring $\mathbb{Z}_5[x]$. The elements $f(x) = x$, $g(x) = x^5$, $h(x) = x + 1$, and $j(x) = x^5 + 1$ are all distinct elements because each has a unique combination of monomials. The table below shows how these polynomials map the elements of $\mathbb{Z}_5$ to $\mathbb{Z}_5$.

$f(x)$	$g(x)$	$h(x)$	$j(x)$
$0 \mapsto 0$	$0 \mapsto 0$	$0 \mapsto 1$	$0 \mapsto 1$
$1 \mapsto 1$	$1 \mapsto 1$	$1 \mapsto 2$	$1 \mapsto 2$
$2 \mapsto 2$	$0 \mapsto 32 = 2$	$2 \mapsto 3$	$2 \mapsto 33 = 3$
$3 \mapsto 3$	$3 \mapsto 243 = 3$	$3 \mapsto 4$	$3 \mapsto 244 = 4$
$4 \mapsto 4$	$4 \mapsto 1024 = 4$	$4 \mapsto 0$	$4 \mapsto 1025 = 0$

As maps, $f(x)$ and $g(x)$ have the same behavior, but they are not the same element in $\mathbb{Z}_5[x]$. The elements $f(x)$ and $g(x)$ are distinct in $\mathbb{Z}_5[x]$, even though the maps they induce are the same. Similarly, $h(x)$ and $j(x)$ are distinct elements in $\mathbb{Z}_5[x]$, even though the maps they induce on $\mathbb{Z}_5$ are the same. $\diamond$

To add polynomials, we add the coefficients of the monomials of the same degree. To multiply polynomials, we use the distributivity property of rings. This is exactly how you once learned to add and multiply real polynomials.

Addition and multiplication of polynomials in rings under modular arithmetic, however, may seem a bit surprising. Consider the example below.

Example 8.1.3. Consider the elements $f(x) = 3x^2 + 2x + 4$ and $g(x) = 4x + 1$ in $\mathbb{Z}_5[x]$. By definition, the coefficients of the monomials in $f(x)$ and $g(x)$ are elements in $\mathbb{Z}_5$, which means that these coefficients are under modulo 5 arithmetic. Thus,

$$\begin{aligned} f(x) + g(x) &= (3x^2 + 2x + 4) + (4x + 1) \\ &= (3 + 0)x^2 + (2 + 4)x + (4 + 1) \\ &= 3x^2 + x. \end{aligned} \tag{8.1}$$

Notice that in Equation 8.1, $2 + 4 = 1$ in $\mathbb{Z}_5$, thus $(2 + 4)x = x$. Similarly, $4 + 1 = 0$ in $\mathbb{Z}_5$.

Below we find the product $f(x) \cdot g(x)$.

$$\begin{aligned} f(x) \cdot g(x) &= (3x^2 + 2x + 4) \cdot (4x + 1) \\ &= 3x^2 \cdot 4x + 2x \cdot 4x + 4 \cdot 4x + 3x^2 \cdot 1 + 2x \cdot 1 + 4 \cdot 1 \\ &= (3 \cdot 4)x^3 + (2 \cdot 4)x^2 + (4 \cdot 4)x + (3 \cdot 1)x^2 + (2 \cdot 1)x + (4 \cdot 1) \\ &= 2x^3 + 3x^2 + x + 3x^2 + 2x + 4 \\ &= (2x^3) + (3x^2 + 3x^2) + (x + 2x) + (4) \\ &= 2x^3 + x^2 + 3x + 4 \end{aligned}$$

◇

The definition of a polynomial ring claims that the set is indeed a ring, though it is worth verifying this claim. The proof of the theorem below is left as an exercise.

Theorem 8.1.4. *Let R be a commutative ring. Then $R[x]$ is a ring.*

Polynomial rings can misbehave, especially if the ring of coefficients is not an integral domain or field. Consider the examples below.

Example 8.1.5. Consider the ring $\mathbb{Z}_{12}[x]$, and notice that $\mathbb{Z}_{12}$ is not an integral domain because it has zero-divisors. Consider the elements $8x, 3x^2 \in \mathbb{Z}_{12}$. Traditionally, you may think that a degree one polynomial multiplied by a degree two polynomial will yield a degree three polynomial, but that is not necessarily true. Under multiplication, $8x \cdot 3x^2 = 24x^3 = 0$ because $24 = 0 \in \mathbb{Z}_{12}$. Thus, a degree one polynomial multiplied by a degree two polynomial yielded a constant. $\diamond$

Example 8.1.6. Consider the polynomial $f(x) = x^3 + 2x \in \mathbb{Z}_{12}$, and notice that $\mathbb{Z}_{12}$ is not an integral domain. Traditionally, you may think that $f(x)$ has three roots, or at most three roots, because it is a degree three polynomial, but that is not necessarily true. Through calculation, we find that $f(x)$ induces the map listed below.

$$\begin{aligned}
f(0) &= 0 \\
f(1) &= 3 \\
f(2) &= 12 = 0 \\
f(3) &= 33 = 9 \\
f(4) &= 72 = 0 \\
f(5) &= 135 = 3 \\
f(6) &= 228 = 0 \\
f(7) &= 357 = 9 \\
f(8) &= 528 = 0 \\
f(9) &= 747 = 3 \\
f(10) &= 1020 = 0 \\
f(11) &= 1353 = 9
\end{aligned}$$

Ergo, we see that $f(x)$ is a degree three polynomial with six roots. $\diamond$

The proof of the theorem below is left as an exercise, though the following examples may shed some light on the proof.

Theorem 8.1.7. *If D is an integral domain, then $D[x]$ is an integral domain.*

Example 8.1.8. Recall that $\mathbb{Z}$ is an integral domain because it is commutative, has unity 1, and has no zero divisors. Then $\mathbb{Z}[x]$ is an integral domain. $\diamond$

Non-Example 8.1.9. The ring $\mathbb{Z}_6$ is not an integral domain because $2, 3 \in \mathbb{Z}_6$ are zero divisors. Similarly, $\mathbb{Z}_6[x]$ is not an integral domain. The elements 2 and 3 are zero-divisors in $\mathbb{Z}_6[x]$. Similarly, $2x$ and $3x^2$ are zero-divisors.

Interestingly, the element $2x + 3$ is not a zero-divisor. If it was, then

$$(2x + 3)(ax + b) = 0$$

for some $a, b \in \mathbb{Z}_6$ where a and b are not both $0 \in \mathbb{Z}_6$. Notice

$$(2x + 3)(ax + b) = 2ax^2 + (2b + 3a)x + 3b = 0$$

induces a system of three equations:

$$2a = 0 \tag{8.2}$$

$$2b + 3a = 0 \tag{8.3}$$

$$3b = 0. \tag{8.4}$$

Equation 8.2 implies that $a = 3$ or $a = 0$. Equation 8.4 implies that $b = 2$ or $b = 0$. Recall that a and b are not both 0. This leaves us with three cases.

1. Assume $a = 3$ and $b = 2$. Then $2b + 3a = 4 + 9 = 1$, which contradicts Equation 8.3.

2. Assume $a = 3$ and $b = 0$. Then $2b + 3a = 9 = 3$, which contradicts Equation 8.3.

3. Assume $a = 0$ and $b = 2$. Then $2b+3a = 4$, which contradicts Equation 8.3.

Therefore, we see that no such a and b exist. Hence, the element $2x+3 \in \mathbb{Z}_6[x]$ is not a zero-divisor. $\diamond$

EXERCISES

Exercise 8.1.1. For each of the following, determine if the statement is always true, sometimes true, or never true. In a sentence or two, justify your response. Let R be a ring and $f(x) \in R[x]$ be a polynomial of degree d.

a. Two polynomials that induce the same map are equal polynomials.

b. Polynomial $f(x)$ has d roots.

c. Polynomial $f(x)$ has at most d roots.

d. If $g(x) \in R[x]$ has degree n, then $\deg f(x) \cdot g(x) = d + n$.

Exercise 8.1.2. Find two distinct elements in $\mathbb{Z}_3[x]$ that induce the same mapping on $\mathbb{Z}_3$.

Exercise 8.1.3. Consider the rings $\mathbb{Z}_2$ and $\mathbb{Z}_2[x]$.

a. Find all possible maps from $\mathbb{Z}_2$ to $\mathbb{Z}_2$.

b. Find all polynomials up through degree 2 in $\mathbb{Z}_2[x]$. Which of these induce the same maps on $\mathbb{Z}_2$?

c. For $n \in \mathbb{N}$, how many polynomials of degree n are in $\mathbb{Z}_2[x]$?

Exercise 8.1.4. For each of the following pairs, find $f(x) + g(x)$ and $f(x) \cdot g(x)$.

a. $f(x) = 3x + 5, g(x) = 6x + 2 \in \mathbb{Z}_7[x]$

b. $f(x) = 2x + 3, g(x) = x^2 + 2x \in \mathbb{Z}_4[x]$

c. $f(x) = 2x^2 + 2x + 1, g(x) = x^2 + 2 \in \mathbb{Z}_3[x]$

Exercise 8.1.5. For each of the following, find all of the roots of $f(x)$.

a. $f(x) = 3x^2 + 4x + 1 \in \mathbb{Z}_8[x]$ in $\mathbb{Z}_8$.

b. $f(x) = x^3 + 3x^2 + 2x \in \mathbb{Z}_{10}$ in $\mathbb{Z}_{10}$

Exercise 8.1.6. Prove Theorem 8.1.4.

Exercise 8.1.7. Prove Theorem 8.1.7.

Exercise 8.1.8. Determine if the following elements are zero-divisors in $\mathbb{Z}_8[x]$. Justify your claims.

a. $6x$

b. $4x^2 + 2$

c. $2x^3 + 4x + 6$

Exercise 8.1.9. Determine if the following elements are zero-divisors in $\mathbb{Z}_{10}[x]$. Justify your claims.

a. $5x$

b. $8x^2 + 2$

c. $5x^3 + 4x$

Exercise 8.1.10. Let R be a ring and $f(x), g(x) \in R[x]$.

a. Show, by example, that it is possible for $\deg(f(x) \cdot g(x)) < \deg(f(x)) + \deg(g(x))$.

b. Prove that when R is an integral domain, $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$.

8.2 Division Algorithm

Recall that Theorem 3.2.24, the Division Algorithm, is about integers. Below, we adapt this theorem to be about polynomials. The purpose of either Division Algorithm is to write something larger in terms of how many copies of something smaller it contains plus the resulting remainder.

If the proof seems notationally cumbersome, follow along with the example that follows.

Theorem 8.2.1 (Division Algorithm for Polynomials)**.** *Let F be a field. Let $a(x), b(x) \in F[x]$ such that $b(x) \neq 0$. Then there exist $q(x), r(x) \in F[x]$ such that $a(x) = b(x) \cdot q(x) + r(x)$ and $0 \leq \deg(r(x)) < \deg(b(x))$.*

Proof. To begin, out of $a(x)$ and $b(x)$, we assume at least one function has degree greater than zero. Otherwise, $a(x)$ and $b(x)$ are simply constants in F.

If $\deg(a(x)) = 0$, then we are assuming $\deg(b(x)) > 0$. In this case, $q(x) = 0$ and $r(x) = b(x)$ because $a(x)$ has smaller degree than $b(x)$. Similarly, if $\deg(a(x)) < \deg(b(x))$, $q(x) = 0$ and $r(x) = b(x)$.

Now we may assume $\deg(a(x)) \geq \deg(b(x))$. Let $n = \deg(a(x))$ and $m = \deg(b(x))$, thus we are assuming $n \geq m$. Further, let $a(x)$ and $b(x)$ be represented by the following:

$$a(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$b(x) = \sum_{i=0}^{m} b_i x^i = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0.$$

Using polynomial long division, we divide $a(x)$ by $b(x)$. The monomial we need to multiply $b(x)$ by to create the leading monomial of $a(x)$ is $\frac{a_n}{b_n} x^{n-m}$.

For the next step in polynomial long division, we compute

$$a(x) - \left(\frac{a_n}{b_n}x^{n-m}\right) b(x),$$

which we will call $\alpha_1(x)$. Hence, $\deg(\alpha_1(x)) = 0$ or $\deg(\alpha_1(x)) < \deg(a(x))$, and, as we have already shown, $\alpha_1(x) = b(x)\cdot q_1(x)+r_1(x)$ for some $q_1(x), r_1(x) \in F[x]$. Thus

$$\begin{aligned} a(x) &= \left(\frac{a_n}{b_n}x^{n-m}\right) b(x) + \alpha_1(x) \\ &= \left(\frac{a_n}{b_n}x^{n-m}\right) b(x) + b(x)\cdot q_1(x) + r_1(x) \\ &= b(x)\cdot\left(\frac{a_n}{b_n}x^{n-m} + q_1(x)\right) + r_1(x). \end{aligned}$$

Thus, we have found $q(x) = \frac{a_n}{b_n}x^{n-m} + q_1(x)$ and $r(x) = r_1(x)$. □

Example 8.2.2. Suppose $b(x) = 2x^2 + 3 \in \mathbb{R}[x]$. For each of the following $a(x) \in \mathbb{R}[x]$, we wish to determine the polynomials $q(x), r(x) \in \mathbb{R}[x]$ such that $a(x) = b(x)\cdot q(x) + r(x)$. We roughly follow the presentation of cases in the proof of Theorem 8.2.1.

- Let's consider a case when $a(x)$ is a constant. If $a(x) = 5$, then

  $$a(x) = 5 = 0\cdot(2x^2 + 3) + 5.$$

  In this case, $q(x) = 0$ and $r(x) = 5 = a(x)$.

- Let's consider a different case when $\deg(a(x))) < \deg(b(x))$. If $a(x) = x + 5$, then

  $$a(x) = x + 5 = 0\cdot(2x^2 + 3) + (x + 5).$$

  Once again, $q(x) = 0$ and $r(x) = x + 5 = a(x)$.

- Let's consider a case when $\deg(a(x)) = \deg(b(x))$. Suppose $a(x) = 3x^2 - x - 1$. We perform polynomial long division below.

$$\begin{array}{r|l} & \frac{3}{2} \\ \hline 2x^2+3 & 3x^2 - x - 1 \\ & -3x^2 \quad\quad -\frac{9}{2} \\ \hline & -x - \frac{11}{2} \end{array}$$

Thus, we see that

$$a(x) = 3x^2 - x - 1 = \left(\frac{3}{2}\right)\left(2x^2+3\right) + \left(-x - \frac{11}{2}\right),$$

meaning that $q(x) = \frac{3}{2}$ and $r(x) = -x - \frac{11}{2}$. Notice that $\deg(r(x)) < \deg(b(x))$.

- Let's consider a case when $\deg(a(x)) > \deg(b(x))$. Suppose $a(x) = x^3 + 4x^2 - x - 1$. We perform polynomial long division below.

$$\begin{array}{r|l} & \frac{1}{2}x + 2 \\ \hline 2x^2+3 & x^3 + 4x^2 - x - 1 \\ & -x^3 \quad\quad -\frac{3}{2}x \\ \hline & 4x^2 - \frac{5}{2}x - 1 \\ & -4x^2 \quad\quad -6 \\ \hline & -\frac{5}{2}x - 7 \end{array}$$

Thus, we see that

$$a(x) = x^3 + 4x^2 - x - 1 = \left(\frac{1}{2}x + 2\right)\left(2x^2+3\right) + \left(-\frac{5}{2}x - 7\right),$$

meaning that $q(x) = \frac{1}{2}x + 2$ and $r(x) = -\frac{5}{2}x - 7$. Notice that $\deg(r(x)) < \deg(b(x))$.

◇

The proof of the following corollary is left as an exercise.

Corollary 8.2.3. *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder of $f(x)$ divided by the polynomial $x - a$.*

Example 8.2.4. Consider $f(x) = x^2 - 3x + 5 \in \mathbb{R}[x]$ and take $a = 4$. Below, we divide $f(x)$ by $x - 4$ using polynomial long division.

$$\begin{array}{r|l} & x + 1 \\ \hline x - 4 & x^2 - 3x + 5 \\ & \underline{-x^2 + 4x} \\ & x + 5 \\ & \underline{-x + 4} \\ & 9 \end{array}$$

Thus, the remainder is 9. Notice that $f(4) = 9$. ◇

The proof of the following corollary is left as an exercise.

Corollary 8.2.5. *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $x - a$ is a factor of $f(x)$ if and only if a is a root of $f(x)$.*

Theorem 8.2.6. *Let F be a field and $f(x) \in F[x]$ a polynomial of degree n. Then f has at most n roots, counting multiplicity.*

Proof. We proceed by induction on the degree of $f(x)$. For the first base case, if $\deg(f(x)) = 0$, then $f(x)$ has no roots, as it is a constant, and the result holds. For the second base case, if $\deg(f(x)) = 1$, then $f(x) = a_1x + a_0$ for $a_1, a_0 \in F$, and $-a_0/a_1$ is the only root of $f(x)$. Again, the result holds.

For the inductive hypothesis, assume that the result holds for all polynomials in $F[x]$ of degree $n - 1$ or less. Further, assume $\deg(f(x)) = n$. If $f(x)$ has

no roots, then the result holds. Assume $f(x)$ has root a of multiplicity k. By the Division Algorithm and Corollary 8.2.5, we may write $f(x)$ as

$$f(x) = (x-a)^k \cdot q(x). \tag{8.5}$$

Notice that

$$\deg(f(x)) = \deg((x-a)^k \cdot q(x)) = k + \deg(q(x)),$$

thus $1 \leq k \leq n$.

If a is the only root of $f(x)$, the result holds. Assume $b \neq a$ is a root of $f(x)$. Hence $f(b) = 0$. Substituting $x = b$ into Equation 8.5, we see that

$$0 = f(b) = (b-a)^k \cdot q(b).$$

By assumption, $b - a \neq 0$, and because F is a field, it must be that $q(b) = 0$. Therefore, b is also a root of the polynomial $q(x)$. Recall that $1 \leq k \leq n$, which means that $\deg(q(x)) < n$. By the inductive hypothesis, $q(x)$ has at most $\deg(q(x)) = n - k$ roots. Ergo, $f(x)$ has at most $k + (n-k)$ roots. □

Example 8.2.7. Let $f(x) = x^4 - 1$. As a polynomial in $\mathbb{R}[x]$, $f(x)$ has two roots, namely 1 and -1. As a polynomial in $\mathbb{C}[x]$, $f(x)$ has four roots, namely 1, -1, i, and $-i$. Notice that $\mathbb{R}$ and $\mathbb{C}$ are fields. ◇

Non-Example 8.2.8. In Exercise 8.1.5, $3x^2 + 4x + 1$ has more than two roots. This can happen in polynomial rings when the coefficients are elements of a ring that is not a field. ◇

EXERCISES

Exercise 8.2.1. Prove Corollary 8.2.3.

Exercise 8.2.2. Prove Corollary 8.2.5.

Exercise 8.2.3. Let $f(x) \in \mathbb{R}[x]$. For $a \in \mathbb{R}$, suppose that $f(a) = 0$ and $f'(a) \neq 0$, where $f'(x)$ is the derivative of $f(x)$ with respect to x. Prove that the multiplicity of the root a is one.

8.3 Irreducible Polynomials

Definition 8.3.1. Let D be an integral domain and $f(x) \in D[x]$ be a polynomial that is neither the zero polynomial nor a unit. Then the polynomial $f(x)$ is irreducible over D if for every decomposition $f(x) = g(x) \cdot h(x)$, $g(x), h(x) \in D[x]$, either $g(x)$ or $h(x)$ is a unit in $D[x]$. A polynomial that is nonzero, not a unit, and not irreducible is reducible over D.

Example 8.3.2. Let $f(x) = 3x^2 + 12$.

- As a polynomial in $\mathbb{Z}[x]$,

  $$f(x) = 3x^2 + 12 = 3(x^2 + 4)$$

  is the only decomposition of $f(x)$ into factors that are also in $\mathbb{Z}[x]$. Neither 3 nor $x^2 + 4$ is a unit in $\mathbb{Z}[x]$, thus $f(x)$ is reducible over $\mathbb{Z}$.

- As a polynomial in $\mathbb{R}[x]$,

  $$f(x) = 3x^2 + 12 = 3(x^2 + 4)$$

  is the only decomposition of $f(x)$ into factors that are also in $\mathbb{R}[x]$. The polynomial 3 is a unit in $\mathbb{R}[x]$, thus $f(x)$ is irreducible over $\mathbb{R}$.

- As a polynomial in $\mathbb{C}[x]$,

$$f(x) = 3x^2 + 12 = 3(x^2 + 4) \tag{8.6}$$
$$= [3(x - 2i)](x + 2i) \tag{8.7}$$
$$= (x - 2i)[3(x + 2i)] \tag{8.8}$$

  are the only decompositions of $f(x)$ into factors that are also in $\mathbb{C}[x]$. In Equation 8.6, the polynomial 3 is a unit in $\mathbb{C}[x]$. In Equations 8.7 and 8.8, none of the factors are units in $\mathbb{C}[x]$. Therefore, because not all decompositions include a factor that is a unit, the polynomial $f(x) = 3x^2 + 12$ is reducible over $\mathbb{C}$.

$\diamond$

Theorem 8.3.3. *Let F be a field and $f(x) \in F[x]$ be a polynomial of degree two or three. Then $f(x)$ is irreducible over F if and only if $f(x)$ has a zero in F.*

Example 8.3.4. Consider $f(x) = x^2 + 2$.

- As a polynomial in $\mathbb{Z}_3[x]$, $f(1) = 0$ and $f(2) = 0$. Thus, $f(x)$ is reducible in $\mathbb{Z}_3$.
- Below is a chart displaying the mapping of the elements in $\mathbb{Z}_5[x]$.

$$f(0) = 2$$
$$f(1) = 3$$
$$f(2) = 1$$
$$f(3) = 1$$
$$f(4) = 3.$$

  Thus, $f(x)$ has no roots in $\mathbb{Z}_5[x]$, therefore it is irreducible over $\mathbb{Z}_5$.

◇

EXERCISES

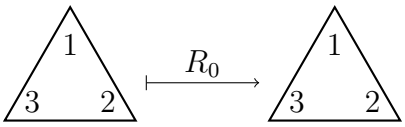
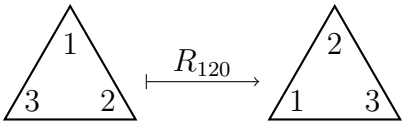
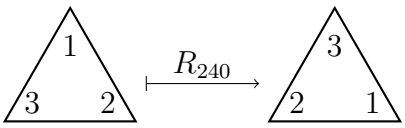
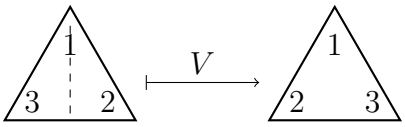
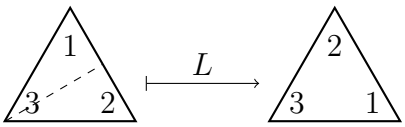
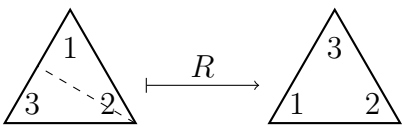
Exercise 8.3.1. Consider the polynomial $f(x) = x^2 + 1$. Determine $f(x)$ is irreducible over the following fields and justify your claim.

a. $\mathbb{Z}_3$

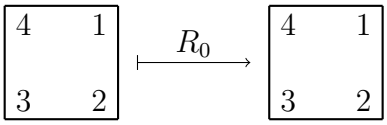
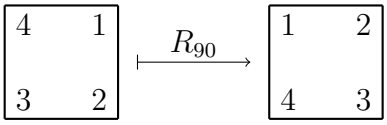
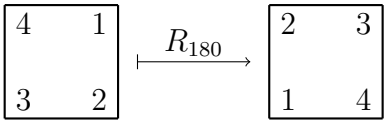
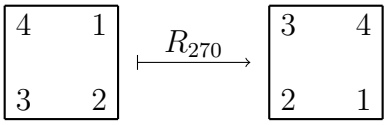
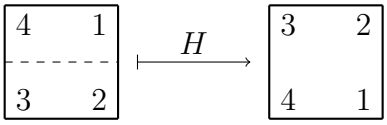
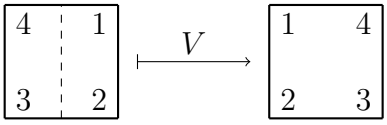
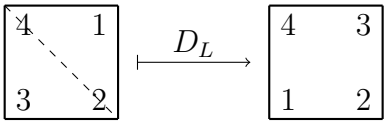
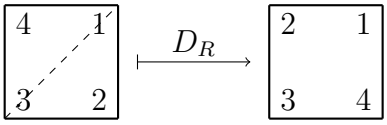
b. $\mathbb{Z}_5$

Appendix A

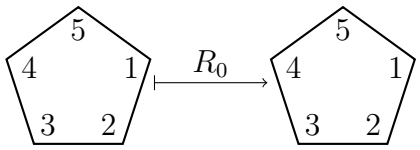
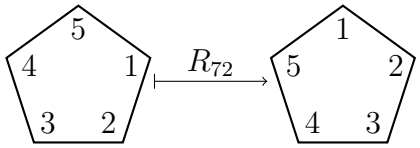
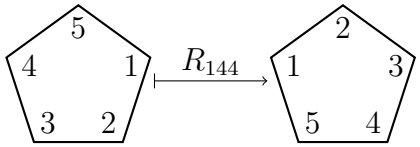
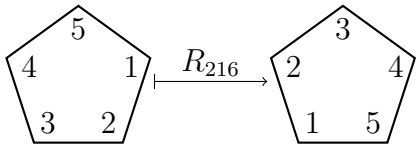
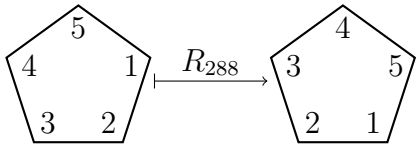
Cayley Tables of Some Dihedral Groups

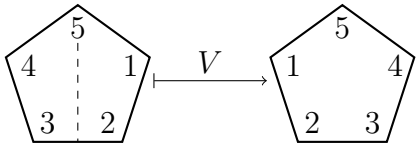
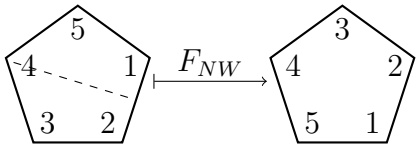
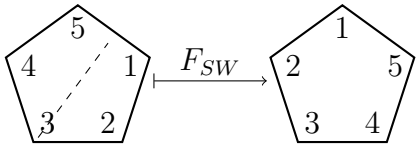
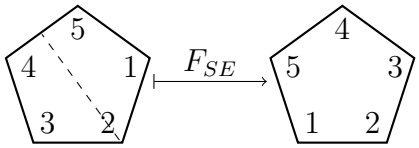
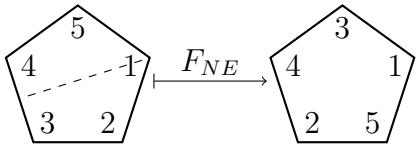
Symbol	Description	Mapping
R_0	Rotation of 0° counterclockwise	
R_{120}	Rotation of 120°	
R_{240}	Rotation of 240°	
V	Reflection about the vertical axis	
L	Reflection about the axis from the left vertex	
R	Reflection about the axis from the right vertex	

D_3	R_0	R_{120}	R_{240}	V	L	R
R_0	R_0	R_{120}	R_{240}	V	L	R
R_{120}	R_{120}	R_{240}	R_0	R	V	L
R_{240}	R_{240}	R_0	R_{120}	L	R	V
V	V	L	R	R_0	R_{120}	R_{240}
L	L	R	V	R_{240}	R_0	R_{120}
R	R	V	L	R_{120}	R_{240}	R_0

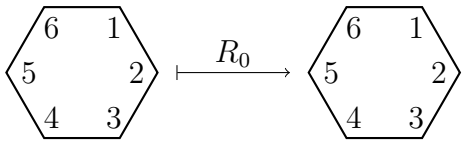
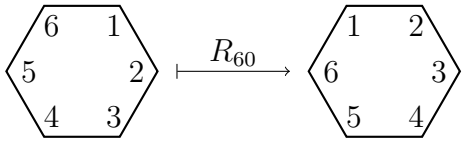
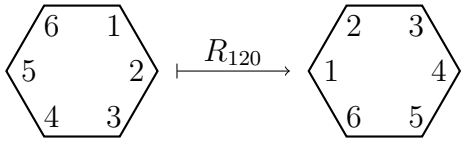
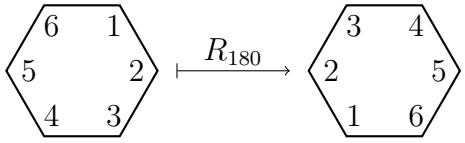
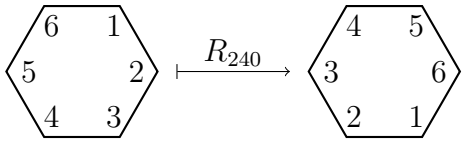
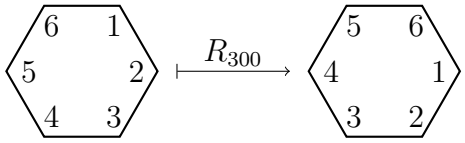
Symbol	Description	Mapping
R_0	Rotation of 0° counterclockwise	
R_{90}	Rotation of 90°	
R_{180}	Rotation of 180°	
R_{270}	Rotation of 270°	
H	Reflection about the horizontal axis	
V	Reflection about the vertical axis	
D_L	Reflection about the left diagonal	
D_R	Reflection about the right diagonal	

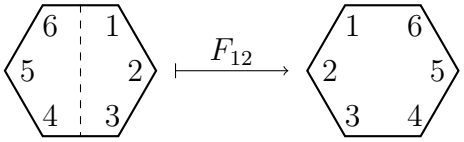
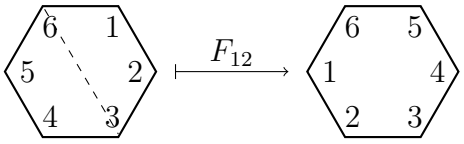
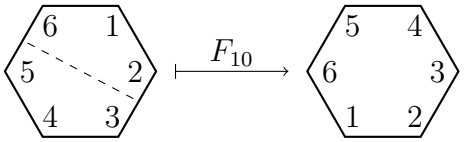
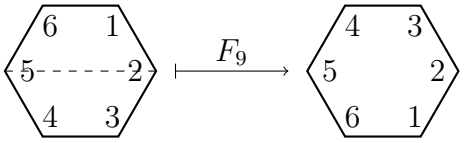
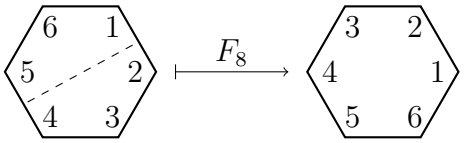
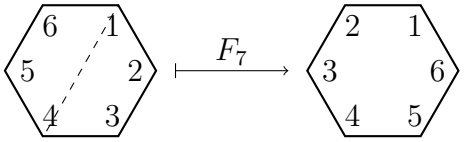
D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D_L	D_R
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D_L	D_R
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D_R	D_L	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D_R	D_L
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D_L	D_R	V	H
H	H	D_L	V	D_R	R_0	R_{180}	R_{90}	R_{270}
V	V	D_R	H	D_L	R_{180}	R_0	R_{270}	R_{90}
D_L	D_L	V	D_R	H	R_{270}	R_{90}	R_0	R_{180}
D_R	D_R	H	D_L	V	R_{90}	R_{270}	R_{180}	R_0

Symbol	Description	Mapping
R_0	Rotation of 0° counterclockwise	
R_{72}	Rotation of 72°	
R_{144}	Rotation of 144°	
R_{216}	Rotation of 216°	
R_{288}	Rotation of 288°	

Symbol	Description	Mapping
V	Reflection about the vertical axis	
F_{NW}	Reflection about the axis from the northwest vertex	
F_{SW}	Reflection about the axis from the southwest vertex	
F_{SE}	Reflection about the axis from the southeast vertex	
F_{NE}	Reflection about the axis from the northeast vertex	

D_5	R_0	R_{72}	R_{144}	R_{216}	R_{288}	V	F_{NW}	F_{SW}	F_{SE}	F_{NE}
R_0	R_0	R_{72}	R_{144}	R_{216}	R_{288}	V	F_{NW}	F_{SW}	F_{SE}	F_{NE}
R_{72}	R_{72}	R_{144}	R_{216}	R_{288}	R_0	F_{SE}	F_{NE}	V	F_{NW}	F_{SW}
R_{144}	R_{144}	R_{216}	R_{288}	R_0	R_{72}	F_{NW}	F_{SW}	F_{SE}	F_{NE}	V
R_{216}	R_{216}	R_{288}	R_0	R_{72}	R_{144}	F_{NE}	V	F_{NW}	F_{SW}	F_{SE}
R_{288}	R_{288}	R_0	R_{72}	R_{144}	R_{216}	F_{SW}	F_{SE}	F_{NE}	V	F_{NW}
V	V	F_{SW}	F_{NE}	F_{NW}	F_{SE}	R_0	R_{144}	R_{288}	R_{72}	R_{216}
F_{NW}	F_{NW}	F_{SE}	V	F_{SW}	F_{NE}	R_{216}	R_0	R_{144}	R_{288}	R_{72}
F_{SW}	F_{SW}	F_{NE}	F_{NW}	F_{SE}	V	R_{72}	R_{216}	R_0	R_{144}	R_{288}
F_{SE}	F_{SE}	V	F_{SW}	F_{NE}	F_{NW}	R_{288}	R_{72}	R_{216}	R_0	R_{144}
F_{NE}	F_{NE}	F_{NW}	F_{SE}	V	F_{SW}	R_{144}	R_{288}	R_{72}	R_{216}	R_0

Symbol	Description	Mapping
R_0	Rotation of 0° counterclockwise	
R_{60}	Rotation of 60°	
R_{120}	Rotation of 120°	
R_{180}	Rotation of 180°	
R_{240}	Rotation of 240°	
R_{300}	Rotation of 300°	

Symbol	Description	Mapping
F_{12}	Reflection about the 12 o'clock axis	
F_{11}	Reflection about the 11 o'clock axis	
F_{10}	Reflection about the 10 o'clock axis	
F_9	Reflection about the 9 o'clock axis	
F_8	Reflection about the 8 o'clock axis	
F_7	Reflection about the 7 o'clock axis	

D_6	R_0	R_{60}	R_{120}	R_{180}	R_{240}	R_{300}	F_{12}	F_{11}	F_{10}	F_9	F_8	F_7
R_0	R_0	R_{60}	R_{120}	R_{180}	R_{240}	R_{300}	F_{12}	F_{11}	F_{10}	F_9	F_8	F_7
R_{60}	R_{60}	R_{120}	R_{180}	R_{240}	R_{300}	R_0	F_{11}	F_{10}	F_9	F_8	F_7	F_{12}
R_{120}	R_{120}	R_{180}	R_{240}	R_{300}	R_0	R_{60}	F_{10}	F_9	F_8	F_7	F_{12}	F_{11}
R_{180}	R_{180}	R_{240}	R_{300}	R_0	R_{60}	R_{120}	F_9	F_8	F_7	F_{12}	F_{11}	F_{10}
R_{240}	R_{240}	R_{300}	R_0	R_{60}	R_{120}	R_{180}	F_8	F_7	F_{12}	F_{11}	F_{10}	F_9
R_{300}	R_{300}	R_0	R_{60}	R_{120}	R_{180}	R_{240}	F_7	F_{12}	F_{11}	F_{10}	F_9	F_8
F_{12}	F_{12}	F_7	F_8	F_9	F_{10}	F_{11}	R_0	R_{300}	R_{240}	R_{180}	R_{120}	R_{60}
F_{11}	F_{11}	F_{12}	F_7	F_8	F_9	F_{10}	R_{60}	R_0	R_{300}	R_{240}	R_{180}	R_{120}
F_{10}	F_{10}	F_{11}	F_{12}	F_7	F_8	F_9	R_{120}	R_{60}	R_0	R_{300}	R_{240}	R_{180}
F_9	F_9	F_{10}	F_{11}	F_{12}	F_7	F_8	R_{180}	R_{120}	R_{60}	R_0	R_{300}	R_{240}
F_8	F_8	F_9	F_{10}	F_{11}	F_{12}	F_7	R_{240}	R_{180}	R_{120}	R_{60}	R_0	R_{300}
F_7	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	R_{300}	R_{240}	R_{180}	R_{120}	R_{60}	R_0

Appendix B

Hints and Solutions

All hints and solutions are contributed by students. Be grateful for those who come before you.

CHAPTER 3

A Solution to Exercise 3.5.6. Ⓢ First, we consider that $GL_2(\mathbb{Z}_2)$ is given by the set of 2×2 matrices, A, with entries in $\mathbb{Z}_2$ for which $\det(A) \neq 0$, and that $SL_2(\mathbb{Z}_2)$ is given by the set of 2×2 matrices, B, with elements in $\mathbb{Z}_2$ for which $\det(B) = 1$. Since $1 \in \mathbb{Z}_2$ is the only non-zero number in $\mathbb{Z}_2$, it follows that $SL_2(\mathbb{Z}_2) = GL_2(\mathbb{Z}_2)$. Let $G = GL_2(\mathbb{Z}_2) = H = SL_2(\mathbb{Z}_2)$. Since $N(H)$ is given by the set of all $g \in G$ for which the conjugate of g in H is equal to H, and in our case, $H = G$, we are looking for $g \in GL_2(\mathbb{Z}_2)$ for which $gGg^{-1} = G$. Since this involves a large number (36) of matrix operations, we

will name each $g \in GL_2(\mathbb{Z}_2)$ as follows, noting that e is our identity:

$$a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, c = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$
$$d = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, f = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Note that in $GL_2(\mathbb{Z}_2)$, we have $a = a^{-1}$, $b = d^{-1}$, $c = c^{-1}$, $d = b^{-1}$, $e = e^{-1}$, and $f = f^{-1}$. Now using these assignments to evaluate our conjugates, we produce the following table for each $h \in SL_2(\mathbb{Z}_2) = GL_2(\mathbb{Z}_2)$.

ghg^{-1}	$h = a$	$h = b$	$h = c$	$h = d$	$h = e$	$h = f$	gHg^{-1}
aha	a	d	f	b	e	c	$GL_2(\mathbb{Z}_2)$
bhd	f	b	a	d	e	c	$GL_2(\mathbb{Z}_2)$
chc	f	d	c	b	e	a	$GL_2(\mathbb{Z}_2)$
dhb	c	b	f	d	e	a	$GL_2(\mathbb{Z}_2)$
ehe	a	b	c	d	e	f	$GL_2(\mathbb{Z}_2)$
fhf	c	d	a	b	e	f	$GL_2(\mathbb{Z}_2)$

Hence, for all $g \in GL_2(\mathbb{Z}_2)$, we have $gHg^{-1} = gGg^{-1} = H = G$, and it follows that $N(H) = H = G$. ◇

A Solution to Exercise 3.5.15. Ⓢ By the definition of group center, given $z \in Z(G)$, we are assured that $zx = xz$ for all $x \in G$. Furthermore, since $H \subseteq Z(G)$, we have $h \in Z(G)$ for all $h \in H$, and thus $hx = xh$ for every $h \in H$ and $x \in G$. It then follows that for every $h \in H$, given $x \in G$, we have $xhx^{-1} = xx^{-1}h = h$. Thus $xHx^{-1} = H$ for all $x \in G$, and we see that $N(H) = G$ by definition. □

A Solution to Exercise 3.6.8. Ⓢ Notice that 1 is a generator of $\mathbb{Z}_{60}$. Therefore

$$\begin{aligned}\langle 54\rangle &= \langle 1^{54}\rangle \\ &= \langle 1^{\gcd(90,54)}\rangle \\ &= \langle 1^{18}\rangle \\ &= \langle 18\rangle \\ &= \{18, 36, 54, 72, 0\}.\end{aligned}$$

Also notice, using Theorem 3.32,

$$\begin{aligned}|\langle 54\rangle| &= |1^{54}| \\ &= \frac{|1|}{\gcd(|1|, 54)} \\ &= \frac{90}{\gcd(90, 54)} \\ &= \frac{90}{18} \\ &= 5.\end{aligned}$$

◇

A Solution to Exercise 4.1.6. Ⓢ Notice, $210 = 2 \cdot 3 \cdot 5 \cdot 7$. Thus,

$$\begin{aligned}\phi(210) &= 210\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big)\Big(1 - \frac{1}{5}\Big)\Big(1 - \frac{1}{7}\Big) \\ &= 210\Big(\frac{1}{2}\Big)\Big(\frac{2}{3}\Big)\Big(\frac{4}{5}\Big)\Big(\frac{6}{7}\Big) \\ &= 210\Big(\frac{48}{210}\Big) \\ &= 48.\end{aligned}$$

Therefore, $\phi(210) = 48$. ◇

A Hint about Exercise 3.6.22. Ⓢ Use Theorem 3.6.18. Be sure to follow biconditional proof techniques.

A Solution to Exercise 3.6.28. Ⓢ a. Suppose $|\langle a \rangle| = m$. By Corollary 3.1, $|a| = m$, and it follows that $a^m = 1 \in U(n)$. Furthermore, this implies that $a^m \equiv 1 \bmod n$ and hence $n \mid a^m - 1$.

b. Suppose $n \mid a^m - 1$. Then it follows that $a^m \equiv 1 \bmod n$, hence $a^m = 1 \in U(n)$. Furthermore, $|a|$ divides m, and thus $m = j|a|$ for some $j \in \mathbb{N}$. Now suppose that $n > a^k$ for all k that divide m. It follows that $a^k \bmod n = a^k \neq 1$ for all k that divide m. Since $|a|$ divides m, we have $a^{|a|} \bmod n = a^{|a|} \neq 1$. But $a^{|a|} = 1$ by definition, and thus if $n \mid a^m - 1$ and $n > a^k$ for all k that divide m, then $|a| = m$.

□

CHAPTER 4

A Solution to Exercise 4.1.6. Ⓢ Recall that the operation in $\mathbb{Z}_{18}$ is addition modulo 18 and the operation in $\mathbb{Z}_{378}$ is addition modulo 378.

- Suppose $n = 3$. Then,

$$\phi(15^3) = \phi(15 + 15 + 15) = \phi(9) = 189 \bmod 378$$

and

$$[\phi(15)]^3 = (315)^3 = 945 = 189 \bmod 378.$$

Thus, $\phi(15^3) = [\phi(15)]^3$.

- Suppose $n = 20$. Then,

$$\phi(15^{20}) = \phi(300) = \phi(12) = 252 \bmod 378$$

and

$$[\phi(15)]^{20} = (315)^{20} = 6300 = 252 \bmod 378.$$

Thus, $\phi(15^{20}) = [\phi(15)]^{20}$.

◇

A Hint about Exercise 4.1.10. Ⓢ Use the properties of the identity such as $ee = e$.

A Hint about Exercise 4.1.12. Ⓢ Recall property 3 of Theorem 4.1.14. Let $g \in G$. Once you've narrowed down the possibilities for $|g|$, proceed with cases.

CHAPTER 5

A Solution to Exercise 5.2.11. Ⓢ Let G be a group. By Lagrange's Theorem, note that $|G : G| = |G|/|G| = 1$. Further, note that $eG = G$ where e is the identity in G. Since $|G : G| = 1$, then by Theorem 5.1 part 8, it follows that $gG = G$ for all $g \in G$. Now take $g, h \in G$. Note that for each g we have $hg^{-1} = j$ for some $j \in G$, by group closure. Thus, for each $g \in G$, we have $gj = ghg^{-1}$. Hence, each representative coset of G in G is equivalent to the set of conjugates of the representative element in G. Since each coset in G yields G, it then follows that $gGg^{-1} = G$ for all $g \in G$, and thus $N(G) = G$. □

CHAPTER 6

A Solution to Exercise 6.1.4. Ⓢ Notice in $\mathbb{Z}_{50}$, $|10| = 5$. Similarly in $\mathbb{Z}_{60}$, $|15| = 4$. Therefore, $|(10, 15)| = \mathsf{lcm}(5, 4) = 20$. Thus, the subgroup $\langle(10, 15)\rangle \subset \mathbb{Z}_{50} \oplus \mathbb{Z}_{60}$ and has order 20. Notice in $\mathbb{Z}_{50}$, $|0| = 1$. Similarly in $\mathbb{Z}_{60}$, $|3| = 20$. Therefore, $|(0, 20)| = \mathsf{lcm}(1, 20) = 20$. Thus, the subgroup $\langle(0, 20)\rangle \subset \mathbb{Z}_{50} \oplus \mathbb{Z}_{60}$ and has order 20. These subgroups are distinct because for $0, 10 \in \mathbb{Z}_{50}$ and $15, 20 \in \mathbb{Z}_{60}$, $|10| \neq |0|$ and $|15| \neq |20|$. In conclusion, our two subgroups of order 20 in $\mathbb{Z}_{50} \oplus \mathbb{Z}_{60}$ are $\langle(10, 15)\rangle$ and $\langle(0, 20)\rangle$. ◇

A Hint about Exercise 6.3.11. Ⓢ Use Cauchy's Theorem for Abelian Groups. This will be a direct proof.

A Solution to Exercise 6.4.9. Ⓢ By the Third Isomorphism Theorem, we get that $(\mathbb{Z}/30\mathbb{Z})/(6\mathbb{Z}/30\mathbb{Z}) \approx \mathbb{Z}/6\mathbb{Z}$. Then, by Corollary 6.3, we get that $\mathbb{Z}/6\mathbb{Z} \approx \mathbb{Z}_6$. We know that $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and

$$(\mathbb{Z}/30\mathbb{Z})/(6\mathbb{Z}/30\mathbb{Z}) = \{a + 6\mathbb{Z}/30\mathbb{Z} | a \in \mathbb{Z}_6\}.$$

Thus, we get that

$$\begin{aligned}(\mathbb{Z}/30\mathbb{Z})/(6\mathbb{Z}/30\mathbb{Z}) =& \{6\mathbb{Z}/30\mathbb{Z}, 1 + 6\mathbb{Z}/30\mathbb{Z}, 2 + 6\mathbb{Z}/30\mathbb{Z}, \\ & 3 + 6\mathbb{Z}/30\mathbb{Z}, 4 + 6\mathbb{Z}/30\mathbb{Z}, 5 + 6\mathbb{Z}/30\mathbb{Z}\}.\end{aligned}$$

◇

A Hint about Exercise 6.4.11. Ⓢ If the identity of G/M is $M = mM$ for $m \in M$, then what is $\ker(\phi)$?

CHAPTER 7

A Hint about Exercise 7.1.4. Ⓢ Be sure to reference the definition of a ring frequently.

A Solution to Exercise 7.3.7. Ⓢ Let $a \in R = \mathcal{P}(\{1,2,3\})$.

a. The empty set is the additive identity because $\varnothing \Delta a = a$.

b. We can see that the additive inverse of $\{1,2\}$ is itself because there is nothing in $\{1,2\}$ and not in $\{1,2\}$.

c. The additive inverse of a is itself because $a \Delta a = \varnothing$.

d. We can see that R is not an integral domain because the only non-zero element that is not a zero-divisor is the element $\{1,2,3\}$. We can see that $\{1\} \cap \{2,3\} = \varnothing$, $\{3\} \cap \{1,2\} = \varnothing$, and $\{2\} \cap \{1,3\} = \varnothing$.

e. The ring does have unity and it is the element $\{1,2,3\}$.

f. The only element that has a multiplicative inverse is the $\{1,2,3\}$.

$\diamond$

A Solution to Exercise 7.2.2. Ⓢ a. We find that $S = \{a+bi \mid a, b \in \mathbb{Z}, a = b\}$ is not a subring of $\mathbb{C}$. Let $a + ai, c + ci \in S$. Then $a + ai = a(1 + i)$ and $c + ci = c(1 + i)$. Thus, $(a + ai)(c + ci) = ac(1 + i)^2 = 2aci \in \mathbb{Z}[i]$. Consider that $2aci \notin S$ for all cases where both $a \neq 0$ and $c \neq 0$. Thus, S fails the subring test.

b. We find that $S = \{a + bi \mid a, b \in \mathbb{Z}, a = -b\}$ also fails the subring test. Let $a - ai, c - ci \in S$. Then $a - ai = a(1 - i)$ and $c - ci = c(1 - i)$.

Thus, $(a-ai)(c-ci) = ac(1-i)^2 = -2aci \in \mathbb{Z}[i]$. Similarly to part a), $-2aci \notin S$ for all cases where both $a \neq 0$ and $c \neq 0$. Thus, S fails the subring test.

c. Finally, $S = \{a + bi \mid a, b \in \mathbb{Z}, a = \pm b\} \cup \mathbb{Z} \cup \mathbb{I}$ fails the subring test as well. Although the set is closed under multiplication, it is now not closed under addition. Note that there exists $a \in \mathbb{Z} \subset S$ and $b = ci \in \mathbb{I} \subset S$ where $c \in \mathbb{Z}, a \neq c$. In this case, $a - b \notin S$.

◇

A Solution to Exercise 7.2.4. Ⓢ Answers may vary. Notice one solution to this problem is the ring $R = \{0, 3, 6, 9\}$ which is a subset of $3\mathbb{Z}$, and consider it under modulo 12 arithmetic. Observe the Cayley table of the nonzero elements under multiplication

R^*	3	6	9
3	9	6	3
6	6	0	6
9	3	6	9

This shows that the unity here is 9. ◇

A Solution to Exercise 7.3.2. Ⓢ A zero-divisor is a nonzero element $a \in R$ such that there exists a nonzero $b \in R$ such that $ab = 0$. In $\mathbb{Z}_{35}$, $ab = 0$ if $ab = 35k$, for $k \in \mathbb{Z}$, because we are in modulo 35 arithmetic. Therefore, the multiples of 5 or 7 are zero-divisors and the set of zero-divisors in R is $\{5, 7, 10, 14, 15, 20, 21, 25, 28, 30\}$. ◇

A Hint about Exercise 7.3.3. Ⓢ Consider Theorem 7.1.2.

A Hint about Exercise 7.3.6. Ⓢ Recall the definitions of a commutative ring and an integral domain. Then, find what makes them different.

A Solution to Exercise 7.4.2. Ⓢ For $2\mathbb{Z}$ to be an ideal of $\mathbb{Z}$, then $a - b \in 2\mathbb{Z}$ and $ra, ar \in 2\mathbb{Z}$ for $a, b \in 2\mathbb{Z}$ and $r\mathbb{Z}$. Since $a, b \in 2\mathbb{Z}$, we can say $a = 2m$ and $b = 2n$ for $m, n \in \mathbb{Z}$. So we can say $a - b = 2m - 2n = 2(m - n)$. Since $m - n \in \mathbb{Z}$, $2(m - n) \in 2\mathbb{Z}$. So $a - b \in 2\mathbb{Z}$. We can also say that $ra = r(2m)$. Since rings are commutative, $r(2m) = (2m)r$. Since rings are associative, $(2m)r = 2(mr)$. Since $mr \in \mathbb{Z}$, $2(mr) \in 2\mathbb{Z}$. So $ra \in 2\mathbb{Z}$. We can say that $ar = (2m)r$. Since rings are associative, $(2m)r = 2(mr)$. Since $mr \in \mathbb{Z}$, $2(mr) \in 2\mathbb{Z}$. So $ar \in 2\mathbb{Z}$. In summation, $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. $\diamond$

A Hint about Exercise 7.4.9. Ⓢ When proving the direction, "If $n\mathbb{Z}$ is a prime ideal, then n is prime," use proof by contradicition.

A Hint about Exercise 7.5.6. Ⓢ What is $\gcd(a, p)$ for all $a \in \mathbb{Z}_p^*$?

A Solution to Exercise 7.5.7. Ⓢ Let H, K and G be fields so that K is a subfield of H and H is a subfield of G. Notice that since K is a subfield of H, K is a subgroup of H. Similarly, since H is a subfield of G then H is a subgroup of G. Therefore by Exercise 3.3.7, K is a subgroup of G. Therefore, for K to be a subfield of G we need to show for $a, b \in K$, $a - b \in K$ and $ab^{-1} \in K$.

1. Non-empty:
   Notice that since K is a subfield of H, we know K has at least two elements. Thus K is non-empty.

2. $a - b \in K$:
   Notice that since K is a subfield of H, we know that for $a, b \in K$, $a - b \in K$.

3. $ab^{-1} \in K$:
   Notice that since K is a subfield of H, we know that for $a, b \in K$, $ab^{-1} \in K$.

Hence, K is a subfield of G. □

A Hint about Exercise 7.6.2. Ⓢ Be sure to reference LaGrange's Theorem.

A Hint about Exercise 7.6.3. Ⓢ Consider the coefficients of the binomial expansion.

A Solution to Exercise 7.6.4. Ⓢ Notice that the ring is made up of elements $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, increasing to $(p-1, q-1)$. Since p and q are relatively prime, we know the only factor they share is 1. Also, since p and q are prime themselves, the values 1 through $p-1$ are relatively prime to q, and the values 1 through $q-1$ are relatively prime to p. Thus the only way to generate a zero element is to multiply the coordinate by a multiple of both p and q. This is the least common multiple of p and q, which is pq. Thus the characteristic of the ring is pq. ◇

A Solution to Exercise 7.6.5. Ⓢ a. Notice that the highest order of an element is 15 in $\mathbb{Z}_{15}$ and the highest order of an element is 20 in $\mathbb{Z}_{20}$. Thus $\mathsf{char}(\mathbb{Z}_{15} \oplus \mathbb{Z}_{20}) = \mathsf{lcm}(15, 20) = 60$.

b. Let $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$. Then from the corollary 5.1 we know that

the order of a under addition will divide $|\mathbb{Z}_m| = m$ and the order of b under addition will divide $|\mathbb{Z}_n| = n$. Thus $ak = m$ and $bc = n$ where $c, k \in \mathbb{N}$. By definition $\mathsf{lcm}(m, n)$ is a multiple of both m and n. So we can see that $(a, b)\mathsf{lcm}(m, n) = (0, 0)$ because $am = 0$ and $bn = 0$.

Now suppose that a natural $d < \mathsf{lcm}(m, n)$ exists such that $(a, b)d = (0, 0)$ for all $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$. Thus d has to be a multiple of the orders under addition of a and b. Now the least common multiple is the smallest number that is a multiple of both m and n which we know exist as orders in $\mathbb{Z}_n$ and $\mathbb{Z}_m$. Thus $d = \mathsf{lcm}(m, n)$. Therefore $\mathsf{char}(\mathbb{Z}_m \oplus \mathbb{Z}_n) = \mathsf{lcm}(m, n)$ where $m, n \geq 2$. $\diamond$

c. We can see that $\mathsf{char}(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}) = \mathsf{lcm}(m_1, m_2, \cdots, m_n)$ where $n \in \mathbb{N}$ and $m_i \geq 2$.

$\diamond$

A Hint about Exercise 7.8.6. Ⓢ Show there is a ring homomorphism ϕ from $\mathbb{Z}[x]$ to $\mathbb{Z}$. Consider Theorem 7.7.9.

CHAPTER 8

A Hint about Exercise 8.2.1. Ⓢ Use the Division Algorithm and evaluate when $x = a$.

Bibliography

[Art91] M. Artin, *Algebra*, Prentice-Hall, 1991.

[Cla01] W. Edwin Clark, *Elementary abstract algebra*, Creative Commons, 2001.

[Gal13] Joseph A. Gallian, *Contemporary abstract algebra*, Brooks/Cole, 2013.

[MJ01] Neal H. McCoy and Gerald J. Janusz, *Introduction to abstract algebra*, Harcourt Academic Press, 2001.

[Sil13] Joseph H. Silverman, *A friendly introduction to number theory*, Pearson, 2013.

Index