Introduction to Group Theory

An Activity-Based Approach

Joseph Fox

Contents

Chapter 1

Symmetry Groups

This book provides an introduction to the subject of abstract algebra via a look at one particular type of algebraic structure: a group. A natural way to become acquainted with groups is through specific examples known as *symmetry groups*.

1.1 Symmetries of Plane Shapes

A **symmetry** of a geometric shape in a plane is one of three types of transformations of the shape:

1. a rotation of the shape about some point which leaves the shape looking exactly as it originally did,

2. a reflection of the shape over some line which leaves the shape looking exactly as it originally did, or

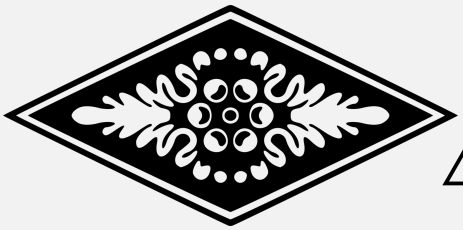
3. a translation (i.e., movement) of the shape along a line which leaves the shape looking exactly as it originally did.

The entire set of symmetries of a plane shape is called the **symmetry group** of the shape. Every plane shape has a symmetry group, even shapes which don't look very "symmetrical".

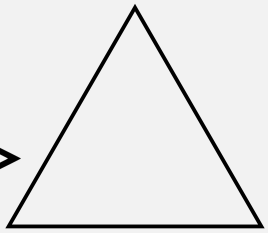
Activity 1.1.1. Think about what it would mean to "describe" the symmetry group of a shape, and then do so for each of the following shapes.

Shape 1

Shape 2

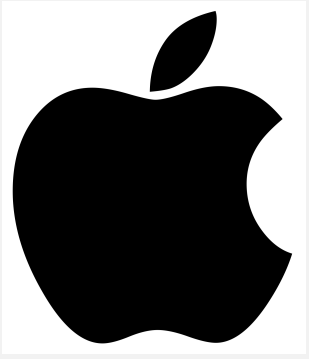


Shape 3



Shape 4

Shape 5



Shape 6

Activity 1.1.2.

- The symmetry group of a regular polygon with n sides (where $n \geq 3$) is called the **dihedral group of degree** n and is denoted by D_n.
- The symmetry group consisting only of the *rotations* of a regular polygon with n sides is called the **cyclic group of degree** n and is denoted by C_n.

1. How many elements are in the dihedral group D_n?
2. How many elements are in the cyclic group C_n?
3. Which of the symmetry groups from Activity 1.1.1 are dihedral? Which are cyclic? Which are neither?

Activity 1.1.3. None of the examples from Activity 1.1.1 have any translational symmetries. Try to come up with an example of a shape whose symmetry group contains a translation.

1.2 Symmetry Composition

What if we perform two symmetry transformations on a shape in a row? Two symmetries performed in a row like this is called a **symmetry composition**.

Example 1.2.1. The symmetry group of a square is D_4. It has four rotations, which we will denote:

R_0 for the counterclockwise rotation through $0°$,

R_{90} for the counterclockwise rotation through $90°$,

R_{180} for the counterclockwise rotation through $180°$, and

R_{270} for the counterclockwise rotation through $270°$.

It also has four reflection symmetries, which we will denote:

H for the reflection across the horizontal symmetry axis through the center of the square,

V for the reflection across the vertical symmetry axis through the center of the square,

D for the reflection across the diagonal symmetry axis through the upper left and lower right corners, and

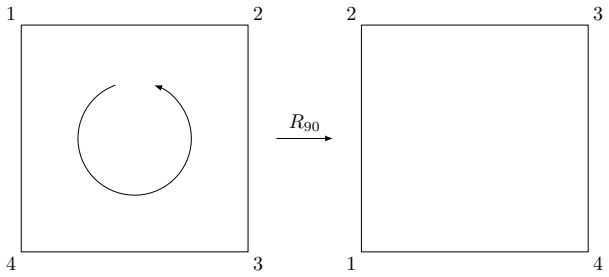
D' for the reflection across the diagonal symmetry axis through the upper right and lower left corners. (Remember that D' is a reflection across the upward sloping diagonal, just as the "prime" symbol $'$ slopes upward.)

Suppose we want to investigate the symmetry composition obtained by first performing R_{90}, then D. We will denote this composition as

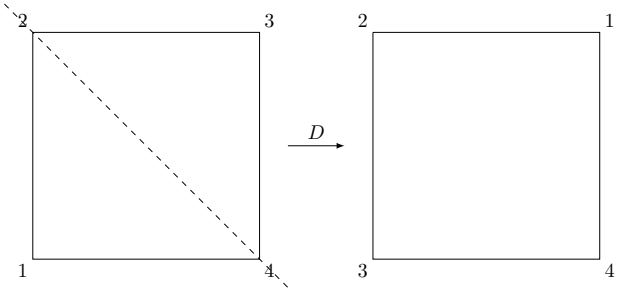
$$D \cdot R_{90}.$$

Why wouldn't we write it as $R_{90} \cdot D$ since we're doing R_{90} first? The reason is that symmetry composition is really just function composition, like starting with two functions $f(x)$ and $g(x)$ and forming their composition $f(g(x))$. You know that the function g acts on x first producing the result $g(x)$, and then f acts on that result. The order in which the functions act is the reverse of the order in which they're written. The same is therefore true for symmetry compositions.

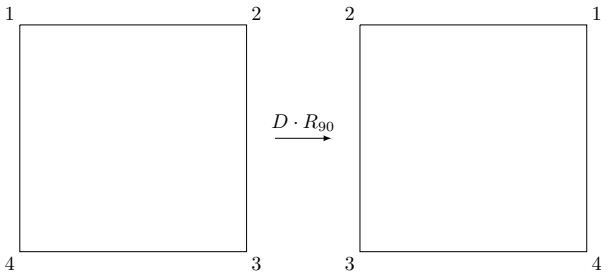
Now let's compose D with R_{90}. It will help to label the vertices of the square to keep track of what the symmetries are doing. First we perform R_{90}:



Now start with the output of R_{90} and perform D on it:



The symmetry composition $D \cdot R_{90}$ can thus be pictured as:



Notice that composing D with R_{90} has the same effect as V. Therefore $D \cdot R_{90} = V$.

Notice that what we're really doing with symmetry composition in this example is starting with two elements of D_4 (D and R_{90}) and combining them via some sort of abstract "multiplication" to produce another element of D_4 (namely, V). Symmetry composition is therefore an example of a **binary operation**.

If we wanted to further investigate this binary operation, we could perform all 64 possible compositions and record the results in a table, just like you do with multiplication tables in elementary school. In this context, we call these multiplication tables **Cayley tables** after Arthur Cayley (1821-1895), an important figure in the development of abstract algebra.

The Cayley table for D_4 is below. Notice that we're putting $D \cdot R_{90}$ in the row labelled by D and the column labelled by R_{90}. We'll stick with that as our convention: *The product $S_1 \cdot S_2$ of two symmetries is placed in the Cayley table in the S_1 row and the S_2 column.*

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Table 1.1: Cayley table for D_4

Activity 1.2.2. Construct the Cayley tables for each of the symmetry groups in Activity 1.1.1

Activity 1.2.3.

1. We say that a set is **closed** with respect to a binary operation provided that performing the operation on elements of the set does not produce any elements outside of the set.

   Look at the Cayley tables we've produced so far. Would you say that symmetry groups are closed with respect to symmetry composition?

2. Observe the way that R_0 interacts with the other elements in your symmetry groups. What plays the same role as R_0 when multiplying real numbers? What plays the same role as R_0 when adding real numbers? Why is it appropriate to call R_0 the "identity element" of a symmetry group?

3. Think about the real numbers $\frac{2}{3}$ and $\frac{3}{2}$. What property do they have with respect to each other? In D_4, does R_{90} have a "partner" like this? Why would it make sense to call this partner an "inverse"?

4. Look at all of your Cayley tables so far. Does every element always seem to have an inverse? State the inverses of each of the 8 elements in D_4.

5. Look up the term **Latin square**. Verify that each of your Cayley tables is a Latin square.

6. What does it mean to say that real number multiplication is *commutative*? For which of the groups from Activity 1.1.1 is symmetry composition commutative? Is it commutative in D_4?

The activity above focuses our interest not on geometric shapes and transformations (which is what we first seemed concerned with) but on questions involving arithmetic and algebra. For example:

- Symmetry composition should make you think of number multiplication.
- The element R_0 should make you think of a version of the number 1.
- Inverses of symmetries should make you think of reciprocals of numbers.

The study of algebra and arithmetic in sets equipped with binary operations is what abstract algebra is about. In the next chapter, we will use our sym-

metry group examples from this chapter to define the notion of a *group* purely abstractly, not referring to symmetries or numbers or anything concrete.

1.3 Writing Proofs: "For every ..." Statements

Often, you'll have to prove that a certain property holds *for all* elements in a set. For example, suppose you have to prove that the sum of any two even numbers is even. You cannot just show that this holds for a few (or even a lot) of examples because those examples can't cover every single instance. Then what are you supposed to do? There are infinitely many pairs of even numbers, so even if you wanted to, you couldn't check that they all have an even sum.

The proper technique with any "for every" or "for each" or "for all" proof is to fix an *arbitrary* element (or elements) from the set and prove the statement for those. An arbitrary element is one which is in no way specific – it's general enough to be a stand-in for any element in the set. So by proving the statement using arbitrary elements, you will be simultaneously proving it for all specific elements.

For the above example then, we'd have to start with two arbitrary even numbers. What makes a number even? The answer, of course, is that it's divisible by 2. Alternatively, you can say that a number x is even if it can be written as $2n$ for some integer n. The other arbitrary even number can be specified similarly: if the other even number is called y, then $y = 2m$ for some integer m. (Do you see why we had to use a letter other than n when we defined y as an even number?)

The proof would now look like this:

Proof. Let x and y be even numbers. Then $x = 2n$ for some integer n and $y = 2m$ for some integer m. To prove that $x + y$ is even, we have to prove that $x + y$ equals 2 times some integer. Well,

$$\begin{aligned} x + y &= 2n + 2m \\ &= 2(n + m). \end{aligned}$$

Since n and m are both integers, so is $n + m$. Thus, $x + y$ is equal to 2 times an integer and is therefore even. □

A few observations about this proof:

- It has a narrative structure. The reader is led through the argument with complete sentences and proper English, not just a bunch of math symbols (although it's still okay to use symbols).
- Any time a variable is introduced, there's a comment about what it represents. For example, we're explicitly told that n and m are integers, even though it's clear from the context.

- There are sentences that tell the reader what has to happen to make the desired conclusion. (See the "To prove that $x + y$ is even ..." sentence.)
- There's a concluding sentence that confirms that the desired statement has been proved, bringing closure to the argument.

Keep these ideas in mind as you work on Exercise 11 below.

1.4 Exercises

1. True or False:
   (a) Some plane shapes have no symmetries.
   (b) For two symmetries S_1 and S_2 in some symmetry group, it is possible that $S_1 \cdot S_2 \neq S_2 \cdot S_1$.
   (c) Abstract algebra is mainly about geometric shapes and transformations.
   (d) The symmetry groups C_{10} and D_{10} both have 20 elements.
2. Write down the elements of the dihedral group D_5.
3. Write down the letters of the English alphabet whose symmetry groups consist only of R_0.
4. Consider an infinitely long strip of equally spaced H's:

   $$\cdots \text{ H } \text{ H } \text{ H } \text{ H } \text{ H } \cdots$$

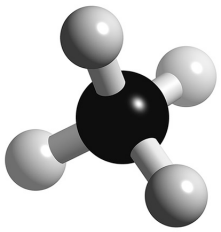
   Describe the symmetry group of this strip of H's.
5. Repeat the previous exercise for an infinitely long strip of R's:

   $$\cdots \text{ R } \text{ R } \text{ R } \text{ R } \text{ R } \cdots$$

6. Draw a shape whose symmetry group is D_8 (other than a regular octagon).
7. Draw a shape whose symmetry group is C_8.
8. Draw a shape which has translational symmetry along two different lines.
9. Find an image of a well-known logo and describe its symmetry group. Choose a logo whose symmetry group contains more than just R_0.
10. (a) Describe the symmetry group of a circle.
    (b) Describe the symmetry group of an entire infinite plane. (This is known as the *Euclidean group*.)

11. **Prove** that symmetry composition in a cyclic symmetry group is commutative.

12. Three-dimensional shapes have symmetry groups as well. Describe the symmetries of the methane molecule CH_4 pictured below.



13. Give another example of non-commutative multiplication from your experience.

14. What does it mean for a binary operation to be *associative*? Do you think symmetry composition is associative? If so, explain (without proof) why. If not, give a counterexample.

15. (a) Explain why the composition of any number of rotations is still a rotation.

    (b) Explain why the composition of an even number of reflections is a rotation and an odd number of reflections is a reflection.

    (c) Suppose r_1, r_2, and r_3 are rotations in some symmetry group and f_1 and f_2 are reflections. What kind of symmetry is $r_2 f_2 f_1 r_2 r_1 f_1 r_3$? (Is it a rotation or reflection?)

    (d) Associate the number 1 with a rotation and -1 with a reflection. Describe the analogy between multiplying these two numbers and composing symmetries in a symmetry group.

16. (a) Show that every element of D_4 can be obtained by multiplying copies of R_{90} and D in some order. (For example, $D' = D \cdot R_{90} \cdot R_{90}$. Show the other seven elements of D_4 can also be obtained using some combination of D and R_{90}.)

    (b) Because every element of D_4 can be obtained as a product of D and R_{90}, we call these two elements **generators** of D_4. Find a pair of two other generators of D_4 and verify that every element of D_4 can be written as a product of (possibly multiple copies) of them.

    (c) Could a pair of two reflections generate D_4? How about a pair of two rotations? Explain your answers.

    (d) Could a single element generate D_4? Explain.

17. (a) Write down the 8 rotations in the cyclic symmetry group C_8.

    (b) Show that it is possible to generate C_8 (in the sense of the previous problem) by a single element. Say what this element is, and show how the elements of C_8 are obtained from it.

    (c) Actually, there are four different elements of C_8 that serve as generators. Find all four. (You already have one from part (b).)

    (d) Make a guess about how to tell whether an element of a cyclic group C_n is a generator of C_n without actually exhibiting how every element of the group is obtained from the generator. (You might have to work through a few other examples similar to part (c). Maybe try part (c) with C_4, C_5, and C_6.)

Chapter 2

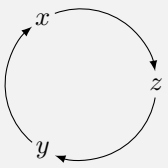
Abstract Groups

2.1 The Group Axioms

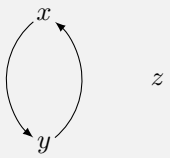
Many of the essential features of the symmetry groups we saw in the last chapter are applicable in other situations as well. The realization in the 19th century that several different areas of mathematics, such as geometry, algebra, and number theory, were actually employing many of the same ideas and techniques we just saw with symmetry groups led to a need to study the underlying similarities that problems in these fields shared and to define a more general notion of a group. The next activity introduces another natural way in which objects like symmetry groups show up.

Activity 2.1.1. In this activity, we'll look at a slightly more general version of symmetry transformations. It will help to keep in mind that *a symmetry of a shape is a permutation (aka, rearrangement) of the shape's points that leaves the shape looking unchanged.*

1. Suppose we have three symbols x, y, and z, each occupying some specific location. Consider the permutation of these symbols which sends x to z's location, z to y's location, and y to x's. We could denote this permutation like this:



Activity 2.1.1. (continued)
We have another permutation that interchanges x and y and leaves z alone:



Find all possible permutations of these three symbols.

2. Apply each of the permutations from the previous problem to the variables of the polynomial $f(x, y, z) = (x-y)(y-z)(x-z)$. Which of them leave $f(x, y, z)$ unchanged? We can think of this set of preserving permutations as the symmetry group of f.

3. Repeat the previous problem for the polynomial $g(x, y, z) = xyz - 2xy - 2xz - 2yz$. What is the symmetry group of g?

This activity shows that the geometric notion of symmetry can be abstracted to a totally different setting. This motivates us to extract the essential defining properties of symmetry groups so that we can study them abstractly. These essential defining properties are called **axioms**.

Using axioms to define algebraic structures became very popular in the 19th and 20th centuries, and it's what abstract algebra is all about. Deciding upon an axiom system is a process that evolves slowly and naturally over several years, but here is the now decided upon axiomatic definition of a group.

Definition 2.1.2. A **group** is a set (which we'll denote for now by G) on which there is defined a binary operation (which we'll denote for now by $*$) which satisfies the following axioms:

1. G is **closed** with respect to $*$. This means that for any two elements x and y in G, the element $x * y$ is also in G.

2. The operation $*$ is **associative**. This means that for any three elements x, y, and z in G, $(x * y) * z = x * (y * z)$.

3. G contains an **identity element** with respect to $*$. This means G contains an element e with the property that $g * e = g$ and $e * g = g$ for all $g \in G$.

4. Every element in G contains an **inverse** in G with respect to $*$. This means that for any element x in G, there is some element y in G such that $x * y = e$ and $y * x = e$.

Notice that a desirable axiom seems to be missing: the commutativity of $*$. It turns out that groups are *not* required to have commutative operations. This

leaves open the door to include the dihedral groups and certain sets of matrices (with matrix multiplication as the operation) as groups.

Activity 2.1.3.

1. Verify that the symmetry groups from Chapter 1 actually are groups. That is, verify that they satisfy the four group axioms.
2. Construct the Cayley tables for the symmetry groups of the polynomials from Activity 2.1.1. Then verify that these polynomial symmetry groups are actually groups.
3. Axioms 3 and 4 might seem to be stated redundantly. Is it really necessary in Axiom 3 to say both $g * e = g$ *and* $e * g = g$? And in Axiom 4, do we really have to state both $x * y = e$ *and* $y * x = e$?

Sometimes, group operations *are* commutative, though. When a group operation is commutative, we say the group is **Abelian**. These are named after Niels Abel (1802-1829), who famously used an early version of the notion of a group to prove that there is no solution formula expressible only in terms of radicals and the four basic arithmetic operations for degree 5 (or higher) polynomial equations.

Activity 2.1.4.

1. Look back at the symmetry groups we've seen so far. Which ones are Abelian?
2. In light of Exercise 11 from Chapter 1, what can you say about all cyclic groups?

2.2 First Properties of Groups

Now that we've seen a few examples of groups (symmetry groups of shapes and polynomials), we might start to notice some properties they all seem for share. Each of them as one and only one identity element. In each of them, any given element has one and only one inverse. The Cayley table of each of them in a Latin square.

It's natural to ask whether these properties always hold for any group we come across, and the way to determine this is to see whether they follow logically from the group axioms alone. If they do, then we know that any set with a binary operation that satisfies the axioms will automatically have these properties.

This is why abstraction is powerful. Proving a theorem about groups ab-

stractly will automatically prove it for every single example of a group. Let's prove the properties noted above, paying special attention to how these proofs use the group axioms.

Theorem 2.2.1. *Every group has one and only one identity element.*

This might seem obvious, and it's certainly true for the symmetry groups we've seen: only R_0 acts as the identity. But there's nothing in the definition of a group that states that this *has* to be true, so it technically requires proof. Notice that in the proof below, we're resorting to the more streamlined notation of gh for the product of g and h rather than the clunky $g * h$.

Proof. Let G be a group. By the identity axiom, G has at least one identity element. Let's call it e_1. But what if G were to have a second identity element different from e_1? Is this a possibility?

Suppose, for the sake of argument, that G *does* have a second identity element. Let's call it e_2. So $e_1 \neq e_2$. By the identity axiom, since e_1 is an identity, $e_1 e_2 = e_2$. Similarly, since e_2 is an identity, $e_1 e_2 = e_1$. Notice that the left sides of these equations are the same. This means that the right sides must also be the same, and thus we have to conclude that $e_1 = e_2$.

So the assumption that G has two different identity elements, e_1 and e_2, is forcing us to conclude two contradictory statements: (1) $e_1 \neq e_2$ and (2) $e_1 = e_2$. A major precept of logical argumentation is that any assumption that would imply a contradiction must itself be false. Therefore, we can say that it *cannot* be the case that G has two different identities, and the only thing left to conclude is that G has one and only one identity. □

This is an example of a "proof by contradiction". We'll learn more about these in Section 2.5.2.

Since this theorem proves that any group has a unique identity, we're allowed to give it a special name. For an abstract group, we'll usually denote the identity by the letter e.

The above proof only referenced the third group axiom. The next theorem is slightly more complex.

Theorem 2.2.2 (Cancellation Law)**.** *Suppose G is a group and x, y, and z are elements of G. If $xy = xz$, then $y = z$. Also, if $yx = zx$, then $y = z$. In other words, you can cancel from the left or from the right in groups.*

Activity 2.2.3. Prove the Cancellation Law.

Theorem 2.2.4. *Every element in a group has one and only one inverse.*

Activity 2.2.5. Prove this theorem using the proof-by-contradiction style of the proof of Theorem 2.2.1. Hint: You're now also allowed to use either of the above two theorems if needed.

The conventional notation for the unique inverse of a group element x is x^{-1}.

The next theorem will have a very practical use, as we'll see. Recall that a **Latin square** is a rectangular array of objects in which no single row or column contains the same object more than once.

Theorem 2.2.6. *The Cayley table of any group is a Latin square.*

Activity 2.2.7. Prove this theorem. You can use a proof by contradiction yet again. Here's a hint: Suppose, to the contrary, that the same element shows up in two different locations in a single row of a Cayley table. Let's suppose the row corresponds to an element x and the repeated element shows up in two different columns, one corresponding to an element y and one corresponding to a different element z. The element in row x and column y is xy, and the one in row x and column z is xz. Thus, we're supposing that (1) $y \neq z$ and (2) $xy = xz$. Show that these two statements lead to a contradiction. You may use only the group axioms and the two theorems above if necessary. When you're done, don't forget to prove a similar statement about repeated elements in a single column.

Before we start to think that proof by contradiction is the only way to prove theorems, we should note that it worked particularly well on the theorems in this section that stated that something *cannot* happen: there *cannot* be more than one identity in a group, elements *cannot* have more than one inverse, rows and columns of Cayley tables *cannot* have repeated elements. Proofs by contradiction are good ways to prove that something cannot happen. Notice that we did not use a proof by contradiction to prove the Cancellation Law.

2.3 Groups of Small Order

The **order** of a group refers to the number of elements it contains. The order of a group G is denoted by $|G|$.

Activity 2.3.1. List the symmetry groups from Chapter 1 and polynomial symmetry groups from Chapter 2 whose order is 3. Look carefully at their Cayley tables. What do you notice?

Activity 2.3.2. Let G be an abstract group of order 3. Let's call the elements e, a, and b. The element denoted e will represent the identity of G, which we know exists by the identity axiom and which we know is unique by Theorem 2.2.1. (So in particular, a and b cannot also be an identity of G.) Can you construct the entire Cayley table for G, even though you don't know what the elements are or what the binary operation is? Try to do so. (Hint: Remember that Cayley tables must be Latin squares.)

Because of the Latin square property of Cayley tables, there is only one way we can fill this out. Here's another instance of the power of abstraction:

> *There is essentially only ONE group of order 3. The only differences among such groups are superficial, like the names of the elements and the symbol we use for the operation.*

When the elements of one group can be renamed as the elements of the other in such a way that their Cayley tables become identical, we say that the groups are *isomorphic*. Activity 2.3.2 says that any two groups of order 3 are isomorphic to each other.

A major project, which we'll discuss in Chapter 10, in 20th century mathematics was to classify all possible groups of finite order. We have at this point completely classified groups of order 3. What about groups of other orders?

Activity 2.3.3. Let's move on to groups of order 2. Let $G = \{e, a\}$ be such a group, where e is the unique identity element. Construct the Cayley table of G.

Activity 2.3.4. To summarize:

1. Up to isomorphism, how many groups of order 3 are there?
2. Up to isomorphism, how many groups of order 2 are there?
3. Up to isomorphism, how many groups of order 1 are there? (Make a Cayley table to find out.)
4. Up to isomorphism, how many groups of order 0 are there? (This is a trick question.)

In Exercise 5, you'll investigate how many groups of order 4 there are. (This is where it finally gets interesting!)

2.4 Exponent Laws

For any element g in a group G, the element gg is also in G. The closure axiom for groups ensures this. We'll denote this element gg by g^2.

Activity 2.4.1. If g^2 is interpreted as gg, then we should interpret g^3 as ggg. But since the operation in a group is *binary*, we can only form products of *two* elements at a time. How do we make sense of the "triple product" ggg then? For any positive integer n, state a way to make sense of g^n as the n-fold product

$$\overbrace{gg\cdots g}^{n \text{ copies}}.$$

What if n is negative? We already know how to interpret g^{-1}; it's the unique inverse of g in G. Since $g^{-1} \in G$, we can multiply it by itself to get an element still in G (closure again): $g^{-1}g^{-1}$. We'll abbreviate this as g^{-2}. In general, g^{-n} for a positive integer n is the product of n copies of g^{-1}.

What about g^0? You can probably already guess that we'll define g^0 to be e, and we'll see why this makes sense very soon.

So the definition of exponentiation in a group is as follows. The number n is a positive integer.

- $g^n = \overbrace{gg\cdots g}^{n \text{ copies of } g}$
- $g^{-n} = (g^{-1})^n$
- $g^0 = e$

With these definitions, we can state the following exponent laws. Below, m and n represent arbitrary integers (positive, negative, or 0), and g and h represent arbitrary group elements.

- $g^m g^n = g^{m+n}$
- $(g^m)^n = g^{mn}$
- $(gh)^{-1} = h^{-1}g^{-1}$

Activity 2.4.2.

1. Justify the first two of these laws.
2. Some of the familiar exponent laws from real number algebra are missing. Which ones?
3. The third law above is often called the "Socks-Shoes Property". Why might that be?

The first property explains why it makes sense to define g^0 to be e. By definition, $gg^{-1} = e$. But the first property says that $gg^{-1} = g^1 g^{-1} = g^{1+(-1)} = g^0$. Therefore, $g^0 = e$.

The Socks-Shoes Property is very important and well worth proving here.

Proof of the Socks-Shoes Property. This is a little easier to think about if we restate the property in words: We have to prove that the inverse of gh is $h^{-1}g^{-1}$. By the definition of inverses, the way to show that two group elements are inverses of each other is to multiply them and show that the product is the identity. The product of gh and $h^{-1}g^{-1}$ is:

$$(gh)(h^{-1}g^{-1}). \tag{2.1}$$

By the associative property, Expression (2.1) can be written as:

$$g(hh^{-1})g^{-1}. \tag{2.2}$$

We need to show that Expression (2.2) equals e.

Activity 2.4.3. Finish the proof from here.

□

One conspicuously absent exponent law above is the familiar $(gh)^n = g^n h^n$. You'll investigate when this actually does hold in Exercise 12a. For now, though, thanks to the Cancellation Law, we can prove that when this law holds for $n = 2$, then our group must have a nice property.

Activity 2.4.4. Let G be a group. Prove that if $(gh)^2 = g^2h^2$ for any two elements g and h in G, then G must be Abelian.

Sometimes in groups, it makes more sense and feels more natural to denote the group operation symbol by a + sign. When this is the case, everything we've proven so far about groups still holds, we just have to adjust the notation.

When using additive notation, it just wouldn't look right to us to denote the "product" $g+g$ by g^2, so we revert to our usual notation for repeated addition: $g+g$ is denoted $2g$. We'll borrow other additive notation from our experience as well. Instead of denoting the inverse of g by g^{-1}, we'll call it $-g$. Instead of calling the identity e, we'll call it 0. Thus in additive notation, the "exponent" definitions become:

- $ng = \overbrace{g+g+\cdots+g}^{n \text{ copies of } g}$
- $(-n)g = n(-g)$
- $0g = 0$

Activity 2.4.5. Rewrite the three exponent laws right before Activity 2.4.2 in additive notation.

2.5 Writing Proofs: Contrapositive, Contradiction, and Induction

2.5.1 Proof by Contrapositive

Suppose we want to prove a mathematical statement: If a hypothesis H is true, then a conclusion C is true. To do so, we could try to see how assuming that H is true allows us to deduce the truth of C. This technique is called a *direct proof*, and it was used in the proof in Section 1.3.

Direct proofs are not always the best way to proceed, though. Another tactic is to show that if C is not true, then H can't be true. This statement – "If C is not true, then H is not true" – is called the **contrapositive** of "If H is true, then C is true." The contrapositive negates and reverses the hypothesis and conclusion.

For example, suppose you have to prove:

> If two numbers x and y are not equal, then x^3 and y^3 are not equal. (2.3)

To prove this by contrapositive, we begin by assuming the negation of the conclusion: $x^3 = y^3$. Taking cube roots of both sides allows us to deduce that $x = y$, which is the negation of the hypothesis. We've thus established that the contrapositive of Statement (2.3) is true, and we can therefore conclude that Statement (2.3) itself must be true.

The reason proof by contrapositive works so well on Statement (2.3) is that its hypothesis and conclusion are *negative statements*; you're trying to prove

that if something does *not* happen, then something else does *not* happen. This can be hard to do directly. But the contrapositive allows you to instead *begin* with a *positive* statement – $x^3 = y^3$ – and *end* with a positive statement – $x = y$. That's much easier to do. In summary, proofs by contrapositive work best when the hypothesis and conclusion are both negative statements.

Note that proofs by contrapositive feel similar to proofs by contradiction. The main difference is that while proofs by contradiction also begin by assuming the negation of the conclusion, they end by deducing that a known false statement it true, whereas proofs by contrapositive end by deducing the negation of the hypothesis.

2.5.2 Proof by Contradiction

A proof by contradiction is similar to a proof by contrapositive. In each case, you begin by assuming the negation of the conclusion. But whereas a proof by contrapositive aims to conclude the negation of the hypothesis, a proof by contradiction aims to conclude the negation of some other known true statement. The logical effect of this is to say that if the conclusion I'm trying to reach is not true, then something I know to be true is false. Well, since that can't be, the conclusion I'm trying to reach must actually be true. Proofs by contradiction were used to prove the three theorems in Section 2.2.

This is an argumentation technique that is used all the time outside of mathematics and was popularized by Plato. It's sometimes called *reductio ad absurdum* (reduction to an absurdity). A famous example of it is the philosopher John Stuart Mill's argument for the non-existence of God. (I'm not advocating the truth of Mill's position, just using it as an example of a proof by contradiction.) Mill argued by supposing, to the contrary, that the being referred to as God exists. If that's so, then according to universally agreed upon theology, this being would be all-knowing, all-powerful, and all-loving. Thus, this being would know about evil, would be powerful enough to stop it, and would love the victims of evil enough to want to stop it. So if God exists, there would be no evil in the world. But surely there is evil in the world. Therefore, assuming that God exists allows us to deduce a statement that contradicts a known truth, and we must thus conclude that God does not exist. (By the way, do you agree with Mill's argument? If not, try to pinpoint a flaw.)

This example nicely illustrates the proof by contradiction technique: Assume the conclusion is false, and deduce a false statement from that assumption. Here's a mathematical example:

Theorem. *Suppose n is the product of two prime numbers p and q, and suppose $p < \sqrt{n}$. Then $q \geq \sqrt{n}$.*

Proof. Suppose, to the contrary, that $q < \sqrt{n}$. If that were true, then we would have that $p < \sqrt{n}$ and $q < \sqrt{n}$. This would imply that $pq < (\sqrt{n})(\sqrt{n})$. Since

$(\sqrt{n})(\sqrt{n}) = n$, it would therefore have to be that $pq < n$. However, we are given that $pq = n$, and we would thus be forced to conclude that $n < n$, which is obviously false. Therefore, it can't possibly be that $q < \sqrt{n}$, and we can safely conclude that $q \geq \sqrt{n}$. □

2.5.3 Mathematical Induction

Have you ever noticed that if you add up the first n odd numbers, you get n^2? How could we prove this? It's not enough to just check this for lots of values of n and assume that the pattern always holds.

Suppose we've checked that the pattern holds for $n = 50$:

$$1 + 3 + 5 + \cdots + 99 = 2500 = 50^2. \tag{2.4}$$

Now we want to check that it holds for $n = 51$. Well, it would be a huge waste of time to start over from 1 and add up through the 51st odd number (which is 101). Instead, we should just add 101 to both sides of Equation (2.4):

$$(1 + 3 + 5 + \cdots + 99) + 101 = 2601,$$

and we can check that 2601 is indeed 51^2.

Does this always work? In other words, if we've verified that adding up the first k odd numbers gives a sum of k^2 for some k, will it be true that adding the $(k + 1)$st odd number to the total will give a sum of $(k + 1)^2$? Let's check.

So we're supposing that we know:

$$1 + 3 + \cdots + k\text{th odd number} = k^2. \tag{2.5}$$

But the kth odd number is $2k - 1$, so Equation (2.5) becomes:

$$1 + 3 + \cdots + (2k - 1) = k^2. \tag{2.6}$$

Now add the $(k+1)$st odd number, which is $2(k+1)-1$ to both sides of Equation (2.6):

$$(1 + 3 + \cdots + (2k - 1)) + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1). \tag{2.7}$$

Simplifying the right side of Equation (2.7), we get:

$$\begin{aligned} k^2 + (2(k + 1) - 1) &= k^2 + 2k + 1 \\ &= (k + 1)^2. \end{aligned}$$

We've just shown that *if* the pattern holds for the first k odd numbers, then it will automatically hold for the first $k + 1$ odd numbers. So for example, if we wanted to verify the pattern for the first 17 odd numbers, it would be sufficient to verify it for the first 16 odd numbers. But by the same reasoning, if we

wanted to verify it for the first 16 odd numbers, it would suffice to verify it for the first 15 odd numbers. And again, if we wanted to verify it for the first 15 odd numbers, it would suffice to verify it for the first 14 odd numbers. What we're seeing is that the burden of proof is being pushed back to smaller and smaller values of n until finally we arrive at having to verify the pattern for $n = 1$. At that point, we're verifying something trivial: the sum of the first 1 odd numbers equals 1^2.

So we know two things: (1) the case for $n = 1$ is definitely true, and (2) for some arbitrary k, if the case for $n = k$ is true, then the case for $n = k + 1$ is automatically true. These two statements together allow us to say that the pattern thus holds for any n, and we have therefore proved that the sum of the first n odd numbers is n^2 for any n.

This technique is called **mathematical induction**, and it is applicable any time we need to prove a series of statements indexed by the positive integers. It consists of two parts: (1) proving the statement is true for $n = 1$ – this is called the *base case*, and (2) proving that if the statement holds for $n = k$, then it must hold for $n = k+1$ – this is called the *induction step*. The induction step is where most of the work comes in; the base case is usually very easy to prove. When proving the induction step, we start by assuming for the moment that the statement is true for $n = k$, where k is some arbitrary positive integer. This temporary assumption is called the *induction hypothesis*. Using the induction hypothesis, we then show that the statement must be true for $n = k + 1$.

Here's a cleaned-up version of our proof from above. This can serve as a model for how induction proofs should be worded and laid out.

Theorem. *The sum of the first n odd integers is n^2.*

Proof. We will proceed by mathematical induction on n. When $n = 1$, our sum contains only the number 1 as a summand. Therefore, the sum is 1, which is equal to 1^2. Thus, the base case is true.

Now suppose that the sum of the first k odd integers is k^2 for some positive integer k. That is, suppose

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2. \tag{2.8}$$

To show that this induction hypothesis implies that the theorem holds for $n = k + 1$, we will add the $(k + 1)$st odd number, which is $2(k + 1) - 1$ to both sides of Equation (2.8):

$$(1 + 3 + 5 + \cdots + (2k - 1)) + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1). \tag{2.9}$$

The right side of Equation (2.9) is:

$$\begin{aligned} k^2 + (2(k + 1) - 1) &= k^2 + 2k + 1 \\ &= (k + 1)^2, \end{aligned}$$

so we thus have that the induction hypothesis for $n = k$ implies that the theorem holds for $n = k + 1$. This completes the induction step.

Therefore, by mathematical induction, we have that the theorem holds for all positive integers n. □

Here's an example of induction in the context of groups:

Theorem. *Let a and b be group elements. Then $(aba^{-1})^n = ab^n a^{-1}$ for all positive integers n.*

Proof. We will proceed by mathematical induction on n. To prove the base case, we have to verify that

$$(aba^{-1})^1 = ab^1 a^{-1}. \tag{2.10}$$

Any group element raised to the power of 1 equals that group element, so the left side of Equation (2.10) equals aba^{-1}. By that same fact, the right side of Equation (2.10) equals aba^{-1}. Since the left and right sides of Equation (2.10) are thus equal, Equation (2.10) holds, and we have therefore proved the base case.

Now suppose that for some positive integer k, $(aba^{-1})^k = ab^k a^{-1}$. This is our induction hypothesis, and we will show that it implies:

$$(aba^{-1})^{k+1} = ab^{k+1} a^{-1}. \tag{2.11}$$

The left side of Equation (2.11) is

$$(aba^{-1})^{k+1} = (aba^{-1})^k (aba^{-1})^1. \tag{2.12}$$

By the induction hypothesis, $(aba^{-1})^k = ab^k a^{-1}$. Therefore Equation (2.12) becomes:

$$\begin{aligned}(aba^{-1})^{k+1} &= ab^k a^{-1}(aba^{-1})^1 \\ &= ab^k (a^{-1}a)ba^{-1} \\ &= ab^k eba^{-1} \\ &= ab^k ba^{-1} \\ &= ab^{k+1} a^{-1},\end{aligned}$$

and we have thus verified that the induction hypothesis for $n = k$ implies that the theorem holds for $n = k + 1$. This completes the induction step.

Therefore, by mathematical induction, $(aba^{-1})^n = ab^n a^{-1}$ for all positive integers n. □

A couple of observations about these proofs:

- They begin by stating that we'll be using mathematical induction, and they end with a concluding statement about what we've just accomplished. These are good practices.
- It's made explicitly clear where the induction hypothesis is being used.
- When we proved the base case, even though it was very easy, we didn't just say something like, "The theorem is obviously true for $n = 1$, therefore the base case is true." If a statement that you need to prove is obvious, you should fully justify it anyway, even if it only takes one or two lines to do so.
- In the second proof, we had to verify Equation (2.10) for the base case. Here is a common mistake when verifying that an equation holds:

  "To prove Equation (2.10), we start with $(aba^{-1})^1 = ab^1a^{-1}$. This equation simplifies to $aba^{-1} = aba^{-1}$, which is clearly true since anything equals itself. Therefore, $(aba^{-1})^1 = ab^1a^{-1}$."

  The spirit of this is correct – you're showing that both sides simplify to the same thing. However, this setup is *using* the equation you're trying to prove as a starting point and deducing a true statement from it. This means you're already assuming the truth of what you're trying to prove, and that's a logical error. Instead, you should work independently with the left and right sides of the equation you need to prove, showing that they simplify to the same thing *without* jumping the gun and equating them. The same tactic was used above to verify Equation (2.11).

2.6 Exercises

1. Determine whether each set below is closed under the given operation.
   (a) set: the positive integers; operation: subtraction
   (b) set: the nonzero integers; operation: division
   (c) set: $n \times n$ matrices; operation: matrix multiplication
   (d) set: the odd integers; operation: addition
   (e) set: the odd integers; operation: multiplication
2. Determine whether the following operations are (i) associative and (ii) commutative.
   (a) multiplication of real numbers
   (b) division of real numbers
   (c) $n \times n$ matrix multiplication
   (d) subtraction of integers

(e) composition of symmetries

3. Let S be the set $\{a, b, c\}$. Let $P(S)$ be the power set of S, that is, the set of all subsets of S. Is $P(S)$ a group with respect to the "union" operation? If so, show that all four group axioms are satisfied. If not, state which ones fail.

4. Show that for $n \geq 3$, D_n is not Abelian. (Hint: Show that a reflection and the smallest possible (nonzero) rotation do not commute with each other.)

5. (a) Up to isomorphism, how many groups of order 4 are there? (Hint: Investigate how many ways you can possibly fill out a 4×4 Cayley table.)
   (b) By looking at the two possible Cayley tables from part (a), explain why every group of order 4 must be Abelian.

6. **Prove** that $(a^{-1})^{-1} = a$.

7. The Cancellation Law says that left cancellation and right cancellation are allowed in equations in groups. What about *cross cancellation*? That is, for group elements x, y, and z, if $xy = zx$, must it be true that $y = z$? Answer by doing the following:
   (a) Show by example that cross cancellation does *not* hold in D_4.
   (b) Explain why cross cancellation *does* hold if the group is Abelian.

8. Let a and b be group elements. Suppose $a^2 = b^2$. Must it be true that $a = b$? If so, **prove** it. If not, give a counterexample.

9. (a) Show by example that it is possible for a group element (other than the identity) to be its own inverse.
   (b) **Prove** that if G is a group with the property that *every* element is its own inverse, then G must be Abelian.

10. Translate the following multiplicative expressions into their additive versions.
    (a) a^2b^3
    (b) $a^{-2}(b^{-1}c)^2$
    (c) $(ab^2)^{-3}c^2 = e$

11. (a) **Prove** that $(aba^{-1})^0 = ab^0a^{-1}$
    (b) Suppose n is a positive integer. **Prove** that $(aba^{-1})^{-n} = ab^{-n}a^{-1}$. (Hint: Induction isn't necessary.)

12. (a) **Prove** that for an *Abelian* group G with elements a and b, $(ab)^n = a^nb^n$ for any integer n. (Hint: Break this into three separate cases: $n > 0$, $n = 0$, and $n < 0$.)
    (b) Find two elements a and b of D_4 such that $(ab)^2 \neq a^2b^2$.

Chapter 3

Examples of Groups

Activity 3.0.1.

1. Let a be a non-negative integer. The remainder obtained upon dividing a by a positive integer n is denoted $a \bmod n$, which stands for "a modulo n". Find the values of 8 mod 3, 30 mod 5, 100 mod 6, and 2 mod 10.

2. Let $\mathbb{Z}_3$ be the set $\{0, 1, 2\}$. Define a binary operation on $\mathbb{Z}_3$ as follows: for any two elements a and b in $\mathbb{Z}_3$, let $a + b$ be the value of $(a + b) \bmod 3$. This operation is referred to as *addition modulo 3*. For example, $2 + 2 = 1$. Construct the Cayley table for $\mathbb{Z}_3$.

3. Verify that $\mathbb{Z}_3$ is a group with respect to addition modulo 3. Then explain why $\mathbb{Z}_3$ is isomorphic to C_3 as well as the symmetry group of $f(x, y, z) = (x - y)(y - z)(x - z)$ from Activity 2.1.1.

The above activity shows that groups which arise naturally as symmetry groups can sometimes (but maybe not always) be described more easily by imagining them as groups of numbers. This is a very common practice in group theory, and it motivates many of the examples of groups we'll see in this chapter. The example of identifying symmetry groups with number groups from Activity 3.0.1 easily generalizes:

Activity 3.0.2. Let $\mathbb{Z}_n$ be the set $\{0, 1, 2, \ldots, n\}$, where $n \geq 2$. Define a binary operation on $\mathbb{Z}_n$ as follows: for any two elements a and b in $\mathbb{Z}_n$, let $a + b$ be the value of $(a + b) \bmod n$.

1. Verify that $\mathbb{Z}_5$ is a group with respect to addition modulo 5.
2. Construct the Cayley table for the number group $\mathbb{Z}_5$ as well as for the symmetry group C_5.
3. Explain why $\mathbb{Z}_5$ and C_5 are isomorphic groups. This shows that the symmetry group C_5 can be represented by a group of numbers. Why is that a good thing?
4. Explain why, for any positive integer n, $\mathbb{Z}_n$ is a group with respect to addition modulo n. How do you think you could prove that C_n is isomorphic to $\mathbb{Z}_n$?

3.1 Number Systems as Groups

Recall that the **order** of a group G is the number of elements it contains and is denoted by $|G|$. If $|G| < \infty$, we say G is a **finite group**; otherwise, we say G is an **infinite group**. As we'll see, many of the number systems you're very familiar with are actually infinite groups.

3.1.1 The Real Numbers

A **real number** is any number expressible in decimal notation. The set of real numbers, which is denoted by $\mathbb{R}$, is equipped with the four obvious binary operations: addition, subtraction, multiplication, and division (as long as division by 0 is avoided).

Activity 3.1.1. Do any of these operations make $\mathbb{R}$ into a group? In other words, does the set $\mathbb{R}$ together with any of these operations satisfy all of the groups axioms?

You should have found that $\mathbb{R}$ is *not* a group with respect to multiplication, and the only reason for this is that one of its elements, 0, has no multiplicative inverse.

So $\mathbb{R}$ with respect to multiplication is *not* a group, and it's all 0's fault! . Let's get rid of 0 and try again:

Activity 3.1.2. Let $\mathbb{R}^*$ be the set of *nonzero* real numbers. Show that $\mathbb{R}^*$ a group with respect to multiplication.

The process by which we salvaged a multiplicative group structure for the real numbers by throwing out the non-invertible element 0 will be copied several times below, so it's worth saying what's happening *abstractly*. That way, the abstract principle can be applied in the specific examples below without having to repeat our work each time.

Theorem 3.1.3. *Let S be a set on which there is defined an associative binary operation $*$. Suppose S contains an identity element e with respect to $*$. Let S^* be the set consisting of the elements of S which have inverses with respect to $*$ in S. Then S^* is a group with respect to $*$.*

Activity 3.1.4. Prove Theorem 3.1.3.

3.1.2 The Rational Numbers

A **rational number** is any real number expressible as a ratio of integers. The set of rational numbers is denoted by $\mathbb{Q}$. It is very straightforward to show that $\mathbb{Q}$ is a group with respect to addition.

Activity 3.1.5. Use Theorem 3.1.3 to show that $\mathbb{Q}*$, the set of nonzero rational numbers is a group with respect to multiplication.

3.1.3 The Integers

The set of integers is denoted $\mathbb{Z}$. (In case you're wondering, the letter "Z" is used because the German word for "numbers" is *zahlen*.) Checking that $\mathbb{Z}$ is a group with respect to addition is easy.

Activity 3.1.6. In Chapter 1, Exercise 5, you described the symmetry group of an infinitely long strip of R's:

$$\cdots \text{ R } \text{ R } \text{ R } \text{ R } \text{ R } \cdots$$

Explain why this symmetry group is isomorphic to $\mathbb{Z}$.

Now what about multiplication? First, note that multiplication in $\mathbb{Z}$ is associative, and $\mathbb{Z}$ contains a multiplicative identity, 1. This means the hypotheses

of Theorem 3.1.3 are satisfied and that $\mathbb{Z}^*$ is a group with respect to multiplication.

Activity 3.1.7.

1. What are the elements in $\mathbb{Z}^*$?
2. What is the order of $\mathbb{Z}^*$?
3. To which group we've seen must $\mathbb{Z}^*$ be isomorphic?

3.1.4 The Complex Numbers

If we let i denote the non-real number $\sqrt{-1}$, then for real numbers a and b, a **complex number** is a number of the form $a + bi$. The sum of two complex numbers $a + bi$ and $c + di$ is defined to be $(a + c) + (b + d)i$, and the product $(a + bi)(c + di)$ is defined to be $(ac - bd) + (ad + bc)i$.

Though we won't often refer to these groups, it's at least worth stating for completeness' sake that the set of complex numbers, denoted $\mathbb{C}$, is a group with respect to complex number addition and that the set of nonzero complex numbers, $\mathbb{C}^*$, is a group with respect to complex number multiplication.

3.2 Matrix Groups

So far, we've seen that groups which arise as symmetries of things (shapes, polynomials, etc) can sometimes be identified with isomorphic, but more familiar groups of numbers. It turns out that another very fruitful approach to understanding groups is to identify them with groups of *matrices*. This approach to understanding groups spawned an entire subfield of abstract algebra beginning in the 19th century called **representation theory**. Representation theory has been at the forefront of abstract algebra research ever since (and happens to be the main research interest of the author).

With representation theory as our motivation, we will introduce some examples of groups of matrices in this chapter.

3.2.1 Linear Algebra Review

We'll need a few basic linear algebra facts throughout this chapter and beyond. These are very briefly summarized below, without any proof or exposition. This is more of a reference section.

Activity 3.2.1. Remind yourself how matrix addition and multiplication are defined by verifying the following:

$$\begin{bmatrix} 3 & -2 & 7 \\ 8 & 0 & -10 \end{bmatrix} + \begin{bmatrix} 5 & 6 & -2 \\ 8 & 9 & -6 \end{bmatrix} = \begin{bmatrix} 8 & 4 & 5 \\ 16 & 9 & -16 \end{bmatrix}$$

and

$$\begin{bmatrix} 6 & 1 & 5 \\ -3 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & -2 & 1 & -1 \\ 4 & 2 & 3 & 0 \\ 7 & 0 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 51 & -10 & 14 & 4 \\ -2 & 8 & 0 & 3 \end{bmatrix}.$$

Activity 3.2.2. Is matrix addition commutative? Is matrix multiplication commutative?

Recall that the identity matrix I is the matrix with 1's on the main diagonal and 0's elsewhere. The identity matrix must therefore be a square matrix – that is, it must have the same number of rows as columns.

A matrix A has an inverse if there is a matrix A^{-1} such that $AA^{-1} = I$ and $A^{-1}A = I$. When A^{-1} exists, we say that A is **invertible** or **nonsingular**. Notice that invertible matrices are necessarily square. (Do you see why?)

We will rarely have the need to actually compute the inverse of an invertible matrix. Rather, it is often sufficient to be able to just determine whether a matrix *has* an inverse. Either of the following two criteria can be used to determine whether a matrix is invertible without actually trying to compute the inverse.

- A matrix is invertible if and only if its row echelon form has at least one nonzero entry in each row.
- A matrix is invertible if and only if its determinant is nonzero.

Determinants play a big role when working with matrix groups. We won't often have to compute determinants, but it will be helpful to know their following theoretical properties:

- $\det(AB) = \det(A)\det(B)$
- $\det(I) = 1$
- $\det(A^{-1}) = \frac{1}{\det(A)}$

At the very least, though, we should be able to handle determinants and inverses of 2×2 matrices computationally:

$$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc,$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}.$$

Conceptually, the centrality of matrices in linear algebra is due to the fact that every linear transformation from one vector space to another can be represented by a matrix. Thus, we can think of matrices as functions, and by defining matrix multiplication in the seemingly strange way that we do, it turns out that we can represent the composition of two linear transformations as the product of their matrix representations. So matrix multiplication is really just function composition.

3.2.2 The General Linear Group

Let $M_{m\times n}(\mathbb{R})$ be the set of all $m \times n$ matrices with real number entries. It's straightforward to check that $M_{m\times n}(\mathbb{R})$ is a group with respect to matrix addition, although this example isn't very useful.

Because matrix multiplication corresponds to function composition, and because function composition is a much more natural way for functions to interact with each other than function addition, we'll focus mostly on sets of matrices that are groups with respect to matrix multiplication.

Activity 3.2.3. In this activity, we'll use Theorem 3.1.3 to pare $M_{m\times n}(\mathbb{R})$ down to a multiplicative group.

1. If we're going to try to get a set of matrices that is a group with respect to matrix multiplication, then all of the matrices in that set have to have the same dimensions and be *square*. Why?
2. Now that we know our matrices must be square in this context, we'll use the same letter for the number of rows and columns. Does $M_{n\times n}(\mathbb{R})$ contain any elements that have no inverses with respect to matrix multiplication?
3. Now referring to Theorem 3.1.3, we'll need matrix multiplication in $M_{n\times n}(\mathbb{R})$ to be associative. Is it? (Hint: Matrix multiplication is really just function composition.)
4. Theorem 3.1.3 also requires $M_{n\times n}(\mathbb{R})$ to have an identity element. What is it?
5. What can we now conclude?

We won't use the clunky notation $(M_{n\times n}(\mathbb{R}))^*$ to denote the multiplicative group of invertible $n \times n$ matrices. Instead, we refer to it as the **general linear group** and denote it by $GL_n(\mathbb{R})$.

A few words about terminology and notation: Recall that matrices are representations of linear transformations between vector spaces, and hence the word "linear" in the name of the group $GL_n(\mathbb{R})$. The "general" part comes from the fact that $GL_n(\mathbb{R})$ contains all of the other multiplicative matrix groups, in a sense that we will soon understand. Finally, it may seem unnecessary to include the $\mathbb{R}$ in the notation, and indeed, we will only consider matrices with real number entries. However, in practice, matrices with entries that come from other number systems are very important. For example, the groups $GL_n(\mathbb{C})$ and $GL_n(\mathbb{Z}_p)$ (where p is a prime number) are very widely used.

3.2.3 The Special Linear Group

We'll mention here just a few of the many other examples of matrix groups. First, consider the matrices in $GL_n(R)$ whose determinant equals 1. We call this set the **special linear group** and denote it $SL_n(\mathbb{R})$.

Activity 3.2.4. Verify that $SL_n(\mathbb{R})$ is a group with respect to matrix multiplication.

Activity 3.2.5. Give three examples of elements of $SL_2(\mathbb{R})$.

3.3 The Integers Modulo n

In Activity 3.0.2, we introduced $\mathbb{Z}_n$, which consists of the integers $0, 1, 2, \ldots, n-1$ and which is a group with respect to addition modulo n. Further, though we haven't officially proved this yet, we hinted that $\mathbb{Z}_n$ is isomorphic to the cyclic symmetry group C_n.

Activity 3.3.1. Construct the Cayley table for $\mathbb{Z}_4$ with respect to addition modulo 4.

Multiplication modulo n in $\mathbb{Z}_n$ is defined the same way as addition modulo n: for two elements a and b in $\mathbb{Z}_n$, ab is the value of ab mod n.

Activity 3.3.2. Construct the Cayley table for $\mathbb{Z}_4$ with respect to multiplication modulo 4. Why isn't $\mathbb{Z}_4$ a group with respect to multiplication modulo 4?

We've been in this situation before: we have a set which is a group with respect to an addition operation but not a multiplication operation. Our usual process has been to invoke Theorem 3.1.3.

Activity 3.3.3. Theorem 3.1.3 requires two things: (1) that multiplication modulo n is associative and (2) that $\mathbb{Z}_n$ contains an identity element with respect to multiplication modulo n. Verify that both of these are true. What can you conclude?

We now know that we can salvage a multiplicative group structure on $\mathbb{Z}_n$ by paring down just to the elements of $\mathbb{Z}_n$ which have multiplicative inverses. Instead of calling this group $(\mathbb{Z}_n)^*$, however, the conventional name for it is $U(n)$. (The "U" stands for "units"; invertible elements in abstract algebra are often called units.) To be able to understand $U(n)$, though, we need an easily checked criterion to determine exactly what these invertible elements of $\mathbb{Z}_n$ are.

Activity 3.3.4. Find the elements of $\mathbb{Z}_n$ that have multiplicative inverses for $n = 2$, $n = 3$, $n = 4$, $n = 5$, and $n = 6$, $n = 7$, $n = 8$, and $n = 9$. Do your results suggest a criterion for invertibility in $\mathbb{Z}_n$?

The above activity seems to indicate that the invertible elements of $\mathbb{Z}_n$ are those which share no common divisors (other than 1) with n. When two numbers have this property, we say they are **relatively prime**.

Suppose a is an element of $\mathbb{Z}_n$ which is *not* relatively prime to n. By definition, this means that a and n share a common divisor which is greater than 1. Call it d.

Why can't a have a multiplicative inverse in $\mathbb{Z}_n$? Well, suppose for the moment that it did. Let's call this hypothetical inverse b. Then in $\mathbb{Z}_n$, $ab = 1$. Remember, though, that this is multiplication modulo n. So to say $ab = 1$ really means that ab, when divided by n, leaves a remainder of 1. In other words, ab is 1 more than a multiple of n. The following activity shows that this is impossible.

Activity 3.3.5. Suppose a and n are both divisible by a number d, and that $d > 1$. Suppose also that $ab = qn + 1$ for some integer q. Explain why this leads to a contradiction.

The conclusion of the above activity is that a does not have an inverse in $\mathbb{Z}_n$. Thus, if an element of $\mathbb{Z}_n$ is invertible, then it must be relatively prime to n.

What about the converse? If an element in $\mathbb{Z}_n$ is invertible, must it be relatively prime to n? The answer is yes, although it's a little harder to see why. The following activity will lead you through a proof.

Activity 3.3.6.

1. Let a be an element in $\mathbb{Z}_n$. Suppose you were to multiply a by each element of $\mathbb{Z}_n$ modulo n. Is there any possibility that you could get the same product more than once? Try this for $a = 6$ and $n = 8$. Then try it for $a = 5$ and $n = 8$.
2. Suppose now that a and n are relatively prime. In this special case, is it possible to get a repeated product when multiplying a by the elements of $\mathbb{Z}_n$ modulo n? Suppose for the moment, we take the hypothesis that it *is* possible. This would mean that for two different elements x and y of $\mathbb{Z}_n$, $ax \bmod n = ay \bmod n$. Show that this would imply that n is a divisor of $ax - ay$.
3. Continuing with the hypothesis of the previous problem, show that if n is a divisor of $ax - ay$, then n must actually be a divisor of $x - y$. (Use the fact that a and n are relatively prime.)
4. If n is a divisor of $x - y$, explain why x and y cannot both be elements of $\mathbb{Z}_n$.
5. The previous problem creates a contradiction, since x and y were assumed to both be in $\mathbb{Z}_n$. We therefore have to reject the hypothesis of the second problem that it's possible to get the same product more than once when multiplying a by the elements of $\mathbb{Z}_n$ modulo n. Therefore, when we multiply a by the elements of $\mathbb{Z}_n$ modulo n, we get a different product each time. Explain why this means that the product of a and some element of $\mathbb{Z}_n$ modulo n must be 1.
6. Explain why the previous problem allows us to conclude that if a is relatively prime to n, then a has an inverse in $\mathbb{Z}_n$.

The outcome of the above activity is our desired criterion for invertibility in $\mathbb{Z}_n$:

Theorem 3.3.7. *An element a in $\mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.*

We thus finally have a full description of $U(n)$: as a set, it consists of the elements of $\mathbb{Z}_n$ which are relatively prime to n, and it is a group with respect to multiplication modulo n.

Activity 3.3.8. Construct the Cayley table for $U(10)$.

3.4 Summary of Examples of Groups So Far

The table below contains a summary of the examples of groups we've seen so far. We'll update this list in Chapter 5, where we'll add two new families of groups.

set	**operation**	**Abelian?**	**order**
D_n $(n \geq 3)$	symmetry composition	no	$2n$
$\mathbb{R}$	addition	yes	infinite
$\mathbb{R}^*$	multiplication	yes	infinite
$\mathbb{Q}$	addition	yes	infinite
$\mathbb{Q}^*$	multiplication	yes	infinite
$\mathbb{Z}$	addition	yes	infinite
$\mathbb{C}$	addition	yes	infinite
$\mathbb{C}^*$	multiplication	yes	infinite
$GL_n(\mathbb{R})$ $(n \geq 2)$	matrix multiplication	no	infinite
$SL_n(\mathbb{R})$ $(n \geq 2)$	matrix multiplication	no	infinite
$\mathbb{Z}_n$ $(n \geq 2)$	addition mod n	yes	n
$U(n)$ $(n \geq 2)$	multiplication mod n	yes	$< n$

Table 3.1: Examples of groups so far

3.5 Writing Proofs: "If and only if" Statements and One-to-One Correspondences

3.5.1 "If and only if" Statements

Suppose I were to say, "I go to church if and only if it's Sunday." This is actually two separate statements: (1) "I go to church if it's Sunday." and (2) "I go to church only if it's Sunday." Let's examine what these statements mean.

Using statement (1) only, what can we conclude if we know it's Sunday? Answer: That I will go to church. Still using only statement (1), what can we conclude if we know I will go to church that day? Answer: *nothing*. Statement (1) is only conclusive about my church-going if we know it's Sunday. As far as that statement is concerned, maybe I go to church every day, so if we know I'm going to church on some given day, statement (1) does not allow us to conclude anything about what day of the week it is.

Now consider only statement (2), and suppose we know that I am going

to church. Then we can conclude that it must be Sunday since statement (2) says I go to church *only* on Sunday. Suppose we know that it's Sunday. Can we conclude anything? Well, statement (2) says that I only go to church on Sunday, but it doesn't say I go *every* Sunday. So if we know it's Sunday, statement (2) allows us to conclude *nothing*.

So statement (1) says: If we assume it's Sunday, then we can conclude I will go to church. Statement (2) is the **converse** of statement (1). It interchanges the hypothesis and conclusion: If we assume I will go to church, then we can conclude it's Sunday.

In general, if we have a statement of the form "P if and only if Q", then we really have two statements: (1) "If P, then Q." and the converse (2) "If Q, then P." That means that when we prove an "if and only if" statement, we actually have two if-then statements to prove. For example:

Theorem. *A group G is Abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.*

Proof. We will begin by assuming that G is an Abelian group, and we will prove that $(ab)^2 = a^2b^2$ for all $a, b \in G$. By the definition of exponentiation,

$$(ab)^2 = abab. \tag{3.1}$$

Since we're assuming G is Abelian, we can rewrite the right side of Equation (3.1) as $aabb$, which is a^2b^2 by definition. Thus,

$$(ab)^2 = a^2b^2.$$

Conversely, we will now assume that $(ab)^2 = a^2b^2$ for all $a, b \in G$, and we will prove that G is an Abelian group. This means that we have to fix two arbitrary elements a and b in G and prove that $ab = ba$.

Since $(ab)^2 = abab$ and $a^2b^2 = aabb$, we have

$$abab = aabb. \tag{3.2}$$

Applying the Cancellation Law on the left, we have

$$bab = abb,$$

and applying the Cancellation Law on the right, we have

$$ba = ab.$$

This is the same as saying $ab = ba$, and we can conclude that G is therefore Abelian. □

Notice that for each half of the proof, we clearly stated the hypothesis and conclusion. This is especially important in an "if and only if" proof since they interchange places halfway through.

"If and only if" statements are very powerful in mathematics. They establish a *logical equivalence* of two statements that might otherwise seem to be saying very different things. We've seen a few examples already in this chapter. For instance:

- A matrix is invertible if and only if its determinant is not 0.
- A number in $\mathbb{Z}_n$ is invertible if and only if it's relatively prime to n.

Invertibility can sometimes be hard to check directly, but these two "if and only if" statements establish easily checked – but totally equivalent – criteria for determining invertibility indirectly.

3.5.2 One-to-One Correspondences

We will often have an occasion in which we need to show that two sets are the same size as each other. The standard way to do this is to establish a *one-to-one correspondence* between them. A one-to-one correspondence is a function from one of the sets to the other that has two special properties.

First, some notation. When we define a function, we give it a name. (f, θ, ϕ, ψ, etc, are all common names, but any name will do.) Then we specify the set that the inputs are coming from and the set that the outputs are going to. So suppose we name our function f, and suppose the inputs are coming from a set X and the outputs are going to a set Y. We denote this all at once by saying:

$$f : X \to Y.$$

Then we *define* the rule for the function by saying what the function does to an arbitrary input. Suppose we want a function named f that takes the square root of natural numbers. We can define such a function as follows:

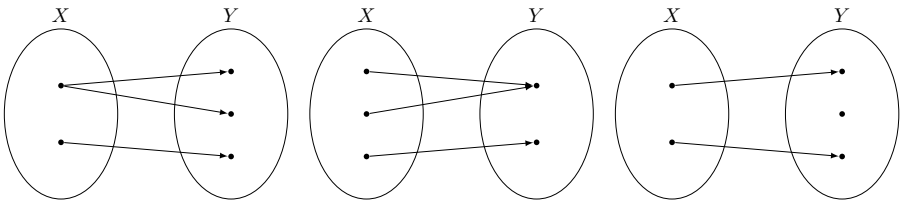
$$\text{Define a function } f : \mathbb{N} \to \mathbb{R} \text{ by } f(n) = \sqrt{n}.$$

One-to-One

The first property of a one-to-one correspondence is that no two input elements are sent to the same output element. (Note that, by definition, *any* function has the property that no single input is sent to more than one output.) This leads to the following definition.

Definition 3.5.1. A function $f : X \to Y$ is **one-to-one** provided that for x_1 and x_2 in X, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

One-to-one functions are often called **injections**. The definition says that an injection sends different inputs to different outputs; no two inputs are sent to the same output.



not a function | function, but not 1-to-1 | 1-to-1 function

Note also that the definition indicates that to prove that a function is one-to-one, we assume a hypothesis ($x_1 \neq x_2$) and deduce a conclusion ($f(x_1) \neq f(x_2)$). Since this hypothesis and conclusion are both negative statements, it's much easier to work with the definition if we convert it to its contrapositive. This is a valid move since every if-then statement is logically equivalent to its contrapositive.

Definition 3.5.2 (Contrapositive of Definition 3.5.1)**.** A function $f : X \to Y$ is **one-to-one** provided that for x_1 and x_2 in X, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Example 3.5.3. Let's prove that the function $f : \mathbb{R} \setminus \{1\} \to \mathbb{R}$ defined by $f(x) = \frac{x+2}{x-1}$ is one-to-one. (Notice that the set of inputs, $\mathbb{R} \setminus \{1\}$, does not include 1 since f is not defined at 1.)

We'll use Definition 3.5.2. Let x_1 and x_2 be elements of $\mathbb{R} \setminus \{1\}$. Suppose that $f(x_1) = f(x_2)$. We will prove that $x_1 = x_2$.

Using the definition of f, we have that if $f(x_1) = f(x_2)$, then

$$\frac{x_1 + 2}{x_1 - 1} = \frac{x_2 + 2}{x_2 - 1}.$$

Cross-multiplying, we get

$$(x_1 + 2)(x_2 - 1) = (x_2 + 2)(x_1 - 1).$$

Expanding both sides gives

$$x_1x_2 - x_1 + 2x_2 - 2 = x_1x_2 + 2x_1 - x_2 - 2.$$

Collecting like terms and simplifying leads to

$$x_1 = x_2$$

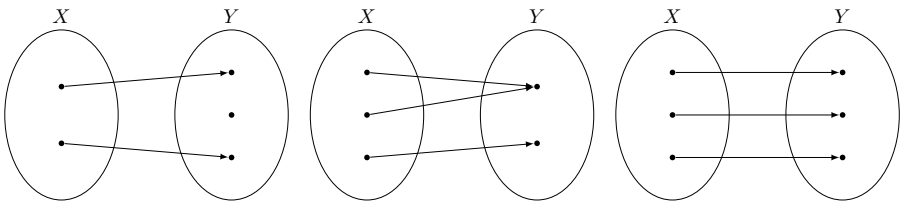
as desired. Therefore, f is one-to-one.

Notice that the hypothesis that $f(x_1) = f(x_2)$ leads to an equation: $\frac{x_1+2}{x_1-1} = \frac{x_2+2}{x_2-1}$. Using this equation as a starting point, we perform algebraic manipulations to reduce it to $x_1 = x_2$. This is typical of a one-to-one proof.

Onto

The second property of a one-to-one correspondence is that every element of the output set has an element in the input set that gets sent to it. More precisely:

Definition 3.5.4. A function $f : X \to Y$ is **onto** provided that for every element y in Y, there is an element x in X such that $f(x) = y$.



not onto onto, but not 1-to-1 1-to-1 and onto

Onto functions are often called **surjections**. Proving that a function is a surjection requires a "fix/find/show" proof. We begin by fixing an arbitrary output element, y. This element is considered a constant throughout the rest of the proof; it's the output element we're "aiming for". Then we somehow find a corresponding input element x that we're proposing as the input element that our function sends to our fixed target output y. Finally we show that this x does the job for y by verifying that $f(x) = y$.

Example 3.5.5. Let $\mathbb{R}^+$ denote the set of positive real numbers. Let's prove that the function $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^{2x-1}$ is onto.

First, we fix an element $y \in \mathbb{R}^+$. Now we must find an associated element $x \in X$ that f sends to y. It's up to you how you go about finding such an x. When proving a function is onto, you don't have to show the work you used to get your x – you just have to propose one and then show it works. In that spirit, let's propose that $x = \frac{1+\ln(y)}{2}$. (We'll see where this came from soon.)

Now we have to show that this x works by showing that $f(x) = y$. We have

$$\begin{aligned} f(x) &= f\left(\frac{1+\ln(y)}{2}\right) \\ &= e^{2[(1+\ln(y))/2]-1} \\ &= e^{\ln(y)} \\ &= y. \end{aligned}$$

Therefore, for an arbitrary $y \in \mathbb{R}^+$, we have found an $x \in \mathbb{R}$ such that $f(x) = y$, which means that f is onto.

So how did we come up with $x = \frac{1+\ln(y)}{2}$? Well, we needed an x such that

$f(x) = y$. In other words, we needed an x that satisfies

$$e^{2x-1} = y.$$

You can check that solving this equation for x gives our $x = \frac{1+\ln(y)}{2}$.

Notice that we left this equation-solving out of the proof. You'll usually need to solve some kind of equation like this when proving a function is onto, but it should be done as scratch work.

With our new vocabulary, we can provide an official definition of a one-to-one correspondence.

Definition 3.5.6. A function $f : X \to Y$ is a **one-to-one correspondence** (also known as a **bijection**) provided that f is both one-to-one and onto.

For a finite set S, we will let $|S|$ denote the number of elements in S.

Theorem 3.5.7. *Suppose X and Y are finite sets. If there exists a one-to-one correspondence $f : X \to Y$, then $|X| = |Y|$.*

Proof. Let S be the subset of Y consisting of all elements of the form $f(x)$ for $x \in X$. In other words, S is the set of all of the outputs of f.

Since f is one-to-one, no two inputs in X can be sent to the same output in S. Thus, $|X| = |S|$. Since f is onto, every element of Y is an output of f, and so S and Y are the same set. Thus $|S| = |Y|$. Therefore $|X| = |Y|$. □

3.6 Exercises

1. Let $\mathbb{R}^+$ denote the set of positive real numbers. (The real number 0 is not considered positive.)
   (a) Determine whether $\mathbb{R}^+$ is a group with respect to addition.
   (b) Determine whether $\mathbb{R}^+$ is a group with respect to multiplication.
2. Let $\mathbb{I}$ represent the set of **irrational numbers**, i.e., the set of real numbers which cannot be written as a ratio of integers. Give two reasons why $\mathbb{I}$ is not a group with respect to multiplication.
3. Let g be an element in $GL_n(\mathbb{R})$ and let h be an element in $SL_n(\mathbb{R})$. Explain why ghg^{-1} is an element of $SL_n(\mathbb{R})$.
4. (a) Why is it that for any natural number n, $n - 1 \in U(n)$?
   (b) Show that for any natural number n, $n-1$ is its own inverse in $U(n)$.
5. (a) Construct the Cayley tables for $\mathbb{Z}_4$ and $U(8)$. Using them, explain why these two groups are *not* isomorphic.

(b) Compare the Cayley table for $U(8)$ to the Cayley table for the symmetry group of Shape 5 from Activity 1.1.1 which you worked out in Activity 1.2.2. Is this symmetry group isomorphic to $U(8)$?

6. When referring to $GL_n(\mathbb{R})$ and $SL_n(\mathbb{R})$, we often restrict to the cases when $n \geq 2$. Why? (Think about what familiar groups $GL_1(\mathbb{R})$ and $SL_1(\mathbb{R})$ are isomorphic to.)

7. Find the inverse of each element in the indicated group.

   (a) 6 in $\mathbb{Z}_{25}$

   (b) 6 in $U(25)$

   (c) $\begin{bmatrix} 4 & -2 \\ 1 & 2 \end{bmatrix}$ in $GL_2(\mathbb{R})$

   (d) $\frac{2}{3}$ in $\mathbb{R}$

   (e) $\frac{2}{3}$ in $\mathbb{R}^*$

8. Give an example of a group of order 113. Give two examples of groups of order 200.

9. If p is a prime number, what is the order of $U(p)$?

10. Describe the analogy between raising the rotation R_{30} to higher and higher powers in C_{12} and taking higher and higher multiples of the number 1 in $\mathbb{Z}_{12}$.

11. Table 3.1 only states that the order of the group $U(n)$ is less than n. We won't derive an exact formula, but we can get a little more specific. Find the orders of several of the $U(n)$ groups for various values of n and make a conjecture (without proof) about the order of the $U(n)$.

12. Table 3.1 seems to be missing a few of the groups we've discussed, namely C_n and $\mathbb{Z}^*$. Why do you think that is?

13. **Prove** that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.

14. Is the function f in Example 3.5.3 onto? If so, **prove** it. If not, find an element $y \in \mathbb{R}$ such that there is no $x \in \mathbb{R} \setminus \{1\}$ such that $f(x) = y$.

15. Is the function f in Example 3.5.5 one-to-one? If so, **prove** it. If not, find two different elements x_1 and x_2 in $\mathbb{R}$ such that $f(x_1) = f(x_2)$.

Chapter 4

Subgroups

By the mid-19th century, the subject of geometry had evolved from the two- and three-dimensional geometry of the Ancient Greeks to a more abstract and varied collection of geometries that didn't adhere to the traditional rules and dimensional constraints. This collection of new geometries became known as *non-Euclidean geometry*. In 1872, the German mathematician Felix Klein (1849-1925) attempted to unite the rapidly branching study of geometry by developing a general and uniform technique to compare various geometries. His technique involved groups.

Klein stated that to every geometry is associated a group of geometric transformations. The transformations leave certain geometric properties, called *invariants*, unchanged. For example, the group associated to Euclidean geometry is the Euclidean group from Exercise 10b in Chapter 1. The elements of the Euclidean group – rotations, reflections, and translations – preserve Euclidean invariants such as distance, angle, area, etc, when applied to shapes in the plane.

Another type of geometry known as *affine geometry* is basically what remains of Euclidean geometry when one ignores geometric properties that involve distance and angle (parallelism, for example). Thus, the set of invariants of affine geometry is a subset of that of Euclidean geometry. This means that every transformation of the Euclidean group is automatically a transformation of the affine group, and therefore the Euclidean group is entirely contained in the affine group (see Figure 4.1).

The idea of a group contained in a larger group leads us immediately to the notion of a subgroup.

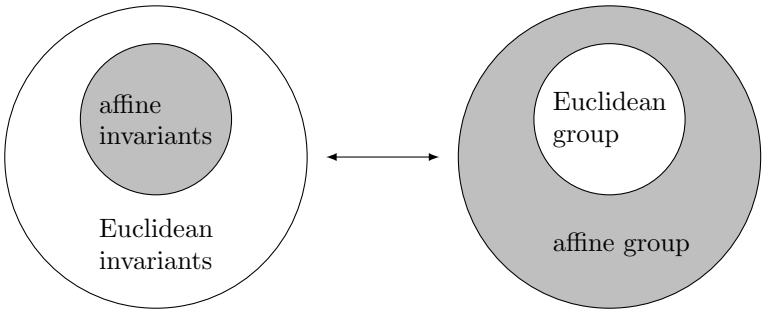


Figure 4.1: A comparison of Euclidean and affine geometry via their groups

4.1 Definition and Examples

A **subgroup** H of a group G is a subset of G which is a group with respect to the same operation of G. When H is a subset of G, we denote this by $H \subseteq G$. When H is a subgroup of G, we denote this by $H \leq G$.

Activity 4.1.1. In Activity 2.1.3, you verified that the sets of permutations from Activity 2.1.1 are groups. Explain why the symmetry group of f is a subgroup of the symmetry group of g.

Activity 4.1.2. Checking that a given subset is actually a subgroup is really just a matter of running through the group axioms, although there's one we can skip. Which one?

So when checking that H is a subgroup of a group G, we need only to perform the following steps. These constitute the **Subgroup Test**. A set H is a subgroup of a group G if and only if:

1. H is a subset of G
2. H is closed under the group operation in G
3. H contains the identity element of G
4. Every element of H contains an inverse in H

Activity 4.1.3. Which of the number system groups from Section 3.1 are subgroups of other number system groups?

Activity 4.1.4. Show that $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Activity 4.1.5. Is $U(n)$ a subgroup of $\mathbb{Z}_n$?

Activity 4.1.6. Find a subgroup of $\mathbb{Z}_{20}$.

Activity 4.1.7. Every group of order greater than 1 has at least two subgroups. What are they?

4.2 Cyclic Subgroups

A very common way to construct subgroups is to form *cyclic subgroups*. Here's how it works:

Let G be a group, and let a be an element of G. Let $\langle a \rangle$ represent the set of all powers of a. Then

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots\}.$$

Theorem 4.2.1. *The set $\langle a \rangle$ is a subgroup of G. It's called the* **cyclic subgroup** *of G generated by a.*

Activity 4.2.2. Prove Theorem 4.2.1.

Activity 4.2.3. Write out the elements in the following cyclic subgroups of the indicated groups.

1. $\langle 2 \rangle$ in $\mathbb{Z}$
2. $\langle R_{90} \rangle$ in D_8
3. $\langle \frac{1}{2} \rangle$ in $\mathbb{Q}^*$
4. $\left\langle \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle$ in $GL_2(\mathbb{R})$
5. $\langle 2 \rangle$ in $\mathbb{Z}_{12}$
6. $\langle 3 \rangle$ in $U(10)$

Notice in problem 6 of the activity above that 3 generates the entire group $U(10)$. Groups G with this property – namely, that there is an element a in G such that $G = \langle a \rangle$ – are called **cyclic groups** (to re-use the term for C_n). The element a such that $G = \langle a \rangle$ is called a **generator** of G. Cyclic groups will be studied in detail in Chapter 7.

4.3 Orders of Elements

We know that the order of a group refers to the number of elements it contains and is denoted by $|G|$. We will also use the term in reference to a single element. Let G be a group and let a be an element of G. The **order** of the element a (denoted $|a|$) is the order of the cyclic subgroup $\langle a \rangle$ of G that it generates.

Activity 4.3.1. For each part of Activity 4.2.3 from the last section, state the order of the generating element.

As we can see from these examples, an alternative but equivalent definition of the order of a group element a is a natural number n with the following two properties:

- $a^n = e$
- If m is a natural number such that $a^m = e$, then $n \leq m$.

Taken together, these two conditions state that $|a|$ is the *smallest* natural number n such that $a^n = e$. If there is no natural number n such that $a^n = e$, then we say that the order of a is infinite and write $|a| = \infty$.

Activity 4.3.2. Find the orders of the elements in $U(20)$.

The orders of elements will play an important role in Chapter 6 when we examine the notion of isomorphisms of groups more closely.

It's important to remember that saying $a^n = e$ is *not* the same as saying $|a| = n$. This is because $|a|$ is the *smallest* natural number n such that $a^n = e$. However, if we know $a^n = e$, then even though n might not be the order of a, n is still closely related to the order of a, as the following theorem shows:

Theorem 4.3.3. *Let G be a group, and let a be an element of G. If $a^n = e$, then $|a|$ divides n.*

Proof. At first glance, this seems to be saying that n divides itself, which is obvious. However, saying that $a^n = e$ is *not* the same as saying $|a| = n$. Remember that for n to be the order, it must be the *smallest* natural number such that $a^n = e$.

Suppose, then, that $a^n = e$ and that $|a| = m$. We have to show that n is a multiple of m. Suppose we divide n by m, getting a quotient q and a remainder r. Then $n = qm + r$, or equivalently, $r = n - qm$. Since r is a remainder obtained upon division by m, we know that $0 \leq r < m$. If we can show $r = 0$, then we'd have $n = qm$, which would mean that m divides n as desired. So our goal is to show that $r = 0$.

If we raise a to the power of r, we have $a^r = a^{n-mq} = a^n a^{-mq}$. We know that $a^n = e$. Also, $a^{-mq} = (a^m)^{-q}$ by an exponent law, and of course $a^m = e$ since $|a| = m$. Thus $(a^m)^{-q} = e^{-q} = e$. Therefore $a^r = ee = e$.

We know that $0 \leq r < m$, so r can't be a natural number, for otherwise that would violate the condition that m is supposed to be the smallest natural number such that $a^m = e$. The only possibility left is for r to be 0. Since this must be the case, we have that m divides n. □

Activity 4.3.4. Suppose a is an element in some group such that $a^{20} = e$. What are the possible orders of a?

4.4 Lagrange's Theorem

4.4.1 Statement of the Theorem and Corollaries

One of the earliest and most useful theorems of group theory is Lagrange's Theorem, named after Joseph-Louis Lagrange (1736-1813). It states a relationship between the orders of *finite* groups and the orders of their subgroups. You may have noticed this relationship already:

Theorem 4.4.1 (Lagrange's Theorem)**.** *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.*

This is our first "deep" theorem so far, meaning that it is far from obvious and that its proof is not easy. Its proof is well worth working through since it will require that we develop the idea of a *coset*, which will be central in Chapters 9 and 10. But first we will get some practice using Lagrange's Theorem.

Before we do, though, there are two facts to keep in mind:

- Lagrange's Theorem only applies to *finite groups*. A given infinite group can potentially have subgroups of any order, both finite and infinite. (In Exercise 17, we'll see an example of an infinite group which has subgroups of every finite order as well as subgroups of infinite order.)

- The converse of Lagrange's Theorem is not always true. It may be that some number k divides $|G|$, even though G has no subgroup of order k. (We'll have to wait until Chapter 5 to see such an example.) We'll see in Chapter 8, however, that the converse of Lagrange's Theorem *does* always hold when G is Abelian.

Activity 4.4.2. List the *possible* orders of the subgroups of the following groups:

1. D_{15}
2. $\mathbb{Z}_{24}$
3. $U(30)$
4. $\left\langle \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle$

There are many corollaries to Lagrange's Theorem, two of which we'll cover in this chapter.

Corollary 4.4.3. *Let G be a finite group and let a be an element of G. Then the order of the element a divides the order of G.*

Activity 4.4.4. Prove Corollary 4.4.3.

Activity 4.4.5. Corollary 4.4.3 makes it easier to find orders of group elements. To see how, find the order of the element 3 in $U(14)$ by raising 3 to successively higher powers. At some point in this process, Lagrange's Theorem will allow you to quit early.

Corollary 4.4.6. *Suppose the order of a group G is prime. Then G is cyclic.*

Activity 4.4.7. Prove Corollary 4.4.6.

4.4.2 Cosets and the Proof of the Theorem

To prove Lagrange's Theorem, we first need some setup. Let G be a finite group and let H be a subgroup of G. For an element $a \in G$, we define the **left coset** of H in G represented by a to be the set $\{ah : h \in H\}$. We will denote this left coset by aH. In other words, aH is the set that results by multiplying every element of H on the left by a.

Activity 4.4.8. Let $G = D_4$, and K be the subgroup $\{R_0, V\}$. (We're using K to denote the subgroup rather than H because H already refers to one of the elements of D_4.) Form the left coset of K in G represented by R_{90}. Then find the other left cosets of K in D_4.

When our group G uses additive notation, we form left cosets the same way, only with addition rather than multiplication. The notation for the left coset of H represented by a becomes $a + H$ rather than aH.

Activity 4.4.9. Find the left cosets of $\langle 3 \rangle$ in $\mathbb{Z}_{24}$ represented by 0, 1, 2, 3, 4, and 5.

In Chapter 9, we will revisit cosets and also introduce the notion of a *right* coset. For now, though, we will only develop the theory of cosets enough to prove Lagrange's Theorem, and we will drop the adjective "left" for the time being.

Activity 4.4.10. You may have noticed that the cosets of a subgroup H are always the same size as the subgroup itself. You also may have noticed that every element of the group G is in exactly one coset. Explain why this would imply that $|G|$ is a multiple of the order of $|H|$, i.e., Lagrange's Theorem. (Suppose $|H| = 6$ and that there are 3 cosets. What must $|G|$ be?)

Our path is now clear: We have to prove that (1) any coset of a given subgroup is the same size as the subgroup, (2) every element of the group lies in a coset, and (3) no element of the group can be in two different cosets. We will establish these results through a series of *lemmas*. A lemma is a theorem that, though it may be of interest in its own right, is only stated and proved in order to help prove a bigger theorem.

Lemma 4.4.11. *Let G be a finite group and let H be a subgroup of G. Then for any element a in G, aH and H have the same number of elements.*

Proof. As stated in Section 3.5.2, the way to prove that aH and H have the same number of elements is to establish a one-to-one correspondence from aH to H.

The first step is to define a function $f : aH \to H$. To do so, we have to specify the output in H to which f sends an arbitrary input in aH. An arbitrary input in aH is an element of the form ah, where h is in H. Given the element ah, the obvious element in H to which f could send ah is just h itself. Thus, we will define our candidate for a one-to-one correspondence f by $f(ah) = h$.

We now have to show that f is one-to-one and onto. We'll follow the examples in Section 3.5.2. To prove that f is one-to-one, suppose $f(ah_1) = f(ah_2)$ for elements h_1 and h_2 in H. We have to show that $ah_1 = ah_2$. Since $f(ah_1) = h_1$ and $f(ah_2) = h_2$, we can conclude that $h_1 = h_2$, and thus $ah_1 = ah_2$. Therefore f is one-to-one.

To prove f is onto, fix an arbitrary element h in H. We have to find an element in aH which f sends to h. By the definition of f, we know that

$f(ah) = h$, and therefore f is onto.

Since f is one-to-one and onto, f is a one-to-one correspondence. Therefore by Theorem 3.5.7, aH and H have the same number of elements. □

Lemma 4.4.12. *Let G be a group, and let H be a subgroup of G. Then every element of G is in a coset of H in G.*

Proof. Let a be an arbitrary element of G. Since H is a subgroup, it contains the identity e of G. Therefore, the coset aH contains the element $ae = a$. Our element a is thus in the coset aH. □

Lemma 4.4.13. *Let G be a group, and let H be a subgroup of G. Then no element of G can be in two different cosets of H in G.*

Proof. Because the conclusion of this theorem is stating that something cannot happen, a proof by contradiction is appropriate. So we will suppose, to the contrary, that there is an element x in G which is in two different cosets of H in G, aH and bH. For aH and bH to be different, at least one of them must contain an element that the other does not. Without loss of generality, let's assume that aH contains an element y that is not in bH.

Since $x \in aH$, $x = ah_1$ for some $h_1 \in H$, and since $x \in bH$, $x = bh_2$ for some $h_2 \in H$. We also know that since $y \in aH$, $y = ah_3$ for some $h_3 \in H$.

Solving the equation $x = ah_1$ for a, we get $a = xh_1^{-1}$. Replacing x with bh_2 gives $a = (bh_2)h_1^{-1}$. Since $y = ah_3$, we get $y = ((bh_2)h_1^{-1})h_3$. Using the associative property, we can rewrite this as $y = b(h_2h_1^{-1}h_3)$. Since H is a subgroup, it's closed under multiplication, so we have $h_2h_1^{-1}h_3 \in H$. Therefore, y can be written as the product of b and an element of H, which means $y \in bH$. But y was specifically chosen to be an element that is *not* in bH. This is a contradiction, which means we have to reject as false the hypothesis that there is an element of G that is in two different cosets of H. □

This series of lemmas taken together says that the cosets of H in a finite group G *partition* G into parts of the same size. (To partition a set means to split it into disjoint subsets in such a way that every element of the set is in one and only one subset.) Having said that, we're finally ready for the proof of Lagrange's Theorem:

Proof of Lagrange's Theorem. Suppose $|G| = n$ and $|H| = k$. Though this hasn't been said yet, it's clear that H is a coset of itself; it's the coset of H in G represented by e. By Lemma 4.4.11, all of the cosets of H in G therefore have exactly k elements. Suppose there are t cosets of H in G. By Lemma 4.4.13, since no two distinct cosets can share any elements, then the total number of elements in all t of these cosets must be tk. But by Lemma 4.4.12, every element of G is in one coset, so the set of tk elements in all the cosets put

together actually constitutes the entire group G. Thus $n = tk$, which implies that k (the order of H) divides n (the order of G). □

4.5 Writing Proofs: Subset and Set Equality Proofs

By definition, two sets are equal provided that the elements of one are the same as the elements of the other; neither set has any elements that the other does not. Thus, to *prove* that two sets X and Y are equal, we have to do two things: (1) show that every element of X is guaranteed to be in Y and (2) show that every element of Y is guaranteed to be in X. In other words, we have to show that $X \subseteq Y$ and $Y \subseteq X$. Once we establish this, we can say that $X = Y$.

Theorem. *Let G be a group and let H be a subgroup of G. Let a be an element of G. If b is an element of G such that $b \in aH$, then $aH = bH$.*

Proof. We will first prove that $aH \subseteq bH$. Fix an arbitrary element ah of aH. Our goal is to prove that $ah \in bH$. Since we're given that $b \in aH$, we can say that $b = ah_1$ for some $h_1 \in H$. Solving this equation for a gives $bh_1^{-1} = a$. Now multiply both sides of this equation on the right by h to obtain $b(h_1^{-1}h) = ah$. Since H is closed and h_1^{-1} and h are elements of H, $h_1^{-1}h \in H$, and thus $ah \in bH$. We have proved that $aH \subseteq bH$.

We will now prove that $bH \subseteq aH$. Fix an arbitrary element bh of bH. Again, since $b \in aH$, we have that $b = ah_1$ for some $h_1 \in H$. Multiplying both sides of this equation on the right by h gives $bh = a(h_1h)$. Since H is closed and h_1 and h are both elements of H, $h_1h \in H$. Thus $bh \in aH$. We have now proved that $bH \subseteq aH$.

Since $aH \subseteq bH$ and $bH \subseteq aH$, we can conclude that $aH = bH$. □

4.6 Exercises

1. Let F be the subset of reflectional symmetries in D_n. Is F a subgroup of D_n? Explain.
2. Is $\mathbb{Q}^*$ a subgroup of $\mathbb{Q}$? Explain.
3. Suppose H and K are both subgroups of a group G. **Prove** that the intersection $H \cap K$ of H and K is a subgroup of G.
4. Show by example that the union of two subgroups of a group need not be a subgroup.
5. For a natural number n, let $n\mathbb{Z}$ be the subset of $\mathbb{Z}$ consisting of the integer multiples of n. Show that for any such n, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

6. Show that the subset of matrices of the form

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix},$$

where a and b are both nonzero real numbers, is a subgroup of $GL_2(\mathbb{R})$.

7. Show that C_n is a cyclic subgroup of D_n. (This explains why the name *cyclic* is appropriate for C_n.)

8. Find the order of each element in $U(30)$. Is $U(30)$ a cyclic group?

9. (a) **Prove** that a subgroup of an Abelian group is Abelian.
   (b) Could a non-Abelian group have an Abelian subgroup? If so, give an example. If not, **prove** it.

10. Could any group element other than the identity have order 1? Explain.

11. **Prove** that any cyclic group must be Abelian.

12. Suppose G is a group of order 20. Explain why G cannot have an element a (other than the identity) such that $a^{27} = e$. (Hint: What are the possible orders of a?)

13. Suppose G is a non-cyclic group of order 25. Explain why G must have an element of order 5.

14. Suppose G is a group of order pq, where p and q are prime numbers. Explain why every subgroup of G (other than G itself) must be cyclic.

15. List the elements of finite order in each of $\mathbb{R}$, $\mathbb{R}^*$, and $\mathbb{Z}$.

16. **Prove** that for any group element a, $\langle a \rangle = \langle a^{-1} \rangle$.

17. Let G be the symmetry group of a circle. Show that G has elements of every possible finite order as well as elements of infinite order.

Chapter 5

The Symmetric and Alternating Groups

As we well know, any quadratic equation $ax^2 + bx + c = 0$ can be solved using the Quadratic Formula. This formula is an expression in terms of a, b, and c involving the four basic arithmetic functions as well as a square root. There are also versions of the Quadratic Formula that work for 3rd and 4th degree polynomial equations, although they're very complicated.

By the late 1700s, an open question was whether there is a "Quintic Formula", that is, a formula that would give the solutions of a general 5th degree polynomial equation in terms of its coefficients involving only the four arithmetic functions and roots. In 1830, an 18-year-old mathematician named Évariste Galois (1811-32) proposed a system for determining whether a solution formula for a polynomial equation exists. It involves investigating algebraic structures that are left invariant by certain permutations of the polynomials' roots. In so doing, he developed many of the basic results of group theory. (He was even the first to use the word "group" in this context.) By the way, Galois' system can be used to prove that there is no version of the Quadratic Formula for polynomial equations of degree 5 or higher.

The point of this historical excursion is that the earliest examples of groups were groups of permutations. We've seen such groups before (see Activity 2.1.1). In this chapter, we'll work out some of the basic facts about permutation groups.

5.1 Permutations

A **permutation** of a set X is a one-to-one correspondence from X to itself. Informally, we can think of a permutation of a set as a "rearrangement" of the elements in the set in each others' spots. For example, when we shuffle a deck of

cards, we permute the cards in the deck. The shuffle is a permutation of the set of cards. When we perform a symmetry transformation on a shape, we permute the points that make up the shape. The transformation is a permutation of the points in the shape. We should think of permutations as *functions* from a set to itself.

Activity 5.1.1. Let X be any set. Let S_X denote the set of all permutations of X. (Again, think of S_X as the set of all possible ways to rearrange the elements of X in each others' places.)

There is a binary operation on S_X: Let α and β be elements of S_X. This means that α and β are both functions from X to itself. The binary operation $\alpha \cdot \beta$ is just the *composition* if α and β. So we interpret $\alpha \cdot \beta$ as the function which first applies β to X and then applies α to the result of β. This is just like symmetry composition from Chapter 1.

Verify that S_X is a group with respect to composition.

At this point, we would be ready to fully explore these permutation groups. Are they Abelian? Are they cyclic? What are their subgroups? How do we find the orders of the elements? What notation should we use? Are they ever isomorphic to other familiar groups?

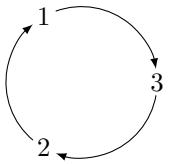
We'll answer these questions in the rest of this chapter, but only in the special case that the set X being permuted is $\{1, 2, \ldots, n\}$, where n is a natural number. The resulting permutation groups and a special class of their subgroups will be the last specific examples of groups we'll introduce.

5.2 The Symmetric Group

The permutation group of the set $\{1, 2, \ldots, n\}$ is called the **symmetric group of degree** n and is denoted by S_n. Our first order of business will be to develop a good way to denote the elements of S_n.

5.2.1 Cycle Notation and the Order of S_n

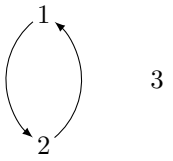
Let's describe all of the elements in S_3. This would be the group of all permutations of the set $\{1, 2, 3\}$. Suppose we have the permutation which sends 1 to 3, 2 to 1, and 3 to 2. We could copy the picture we drew in Activity 2.1.1:



The obvious disadvantage of this notation is that it would be cumbersome to draw every time. Instead, we can capture the information in this picture using **cycle notation**. We just pick a starting point and list the elements we encounter as we follow the arrows. The permutation above will thus be denoted (1 3 2), with the understanding that the last element in the parentheses cycles back to the first one.

Activity 5.2.1. Given that you can start a permutation's cycle notation with any element, state the two other possible ways to denote the above permutation in cycle notation.

It's possible for a permutation to leave some elements of the set where they are. For example, another element of S_3 might interchange 1 and 2 and leave 3 alone. Pictorially, we'd have:



We express this in cycle notation by just omitting the 3: (1 2) (or (2 1)). When *all* of the elements are left alone, we express this permutation in cycle notation as (1).

Activity 5.2.2. How many permutations of the set $\{1, 2, 3\}$ are there? Write them all down in cycle notation.

Sometimes a permutation will contain disjoint cycles. For example, in S_4, we'd have a permutation that interchanges 1 and 4 and interchanges 2 and 3. We would express this in cycle notation as (1 4)(2 3).

Activity 5.2.3. How many elements are there in S_4? Write them all down.

The above activity is a special case of a general fact about the symmetric groups:

Theorem 5.2.4. *The order of the group S_n is $n!$.*

5.2.2 Composition

To further explore the group theoretic properties of S_n, let's take a closer look at its binary operation: composition.

Example 5.2.5. We'll consider, for example, the product $(1\,3\,2)(1\,3)$ in S_3. Remembering that permutations are functions and the binary operation in S_n is function composition, we should see this product $(1\,3\,2)(1\,3)$ as two functions being composed. As such, we first apply the function on the right, $(1\,3)$ and then apply $(1\,3\,2)$ to the result.

We'll start by tracking where $(1\,3\,2)(1\,3)$ sends 1. As a function, $(1\,3)$ sends 1 to 3. The 1 is the input of this function, and the 3 is the output. Now we take this output of 3 and use it as input for the next function in line: $(1\,3\,2)$ (just like your familiar function composition from high school). The function $(1\,3\,2)$ sends this 3 to 2. Therefore, the product $(1\,3\,2)(1\,3)$ sends 1 to 2 (with a stop along the way at 3). So far then, our product is looking like:

$$(1\,2$$

Now we have to see where $(1\,3\,2)(1\,3)$ sends the 2 we left off with. The rightmost permutation $(1\,3)$ has no 2 in it, meaning that it sends 2 to itself. So the input of 2 to $(1\,3)$ results in an output of 2, and this 2 now gets passed along as input to $(1\,3\,2)$, which sends it to 1. So the product $(1\,3\,2)(1\,3)$ sends 2 to 1. We can now update our product as:

$$(1\,2)$$

The only place left that our product can send 3 is itself, but we should make sure: $(1\,3)$ sends 3 to 1, and $(1\,3\,2)$ sends 1 to 3, so the product $(1\,3\,2)(1\,3)$ sends 3 to 3. Thus, we have that $(1\,3\,2)(1\,3) = (1\,2)(3)$, or by our convention,

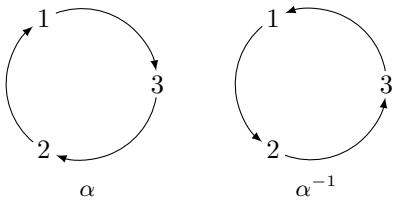
$$(1\,3\,2)(1\,3) = (1\,2).$$

Activity 5.2.6. Construct the Cayley table for S_3.

You can plainly see from this table that S_3 is not Abelian. You'll verify that in general, S_n is not Abelian for any $n \geq 3$ in Exercise 3.

5.2.3 Inverses

Recall from Activity 5.1.1 that the inverse of a permutation would just be the permutation that sends everything back where it came from; it would reverse the arrows:



Translating these pictures into cycle notation, we see that $\alpha = (1\,3\,2)$ and $\alpha^{-1} = (2\,3\,1)$. The order of the numbers is reversed.

Activity 5.2.7. Find the inverses of the following permutations:

1. any cycle with two elements (these are often called **2-cycles** or **transpositions**)
2. $(3\,4\,2\,6\,1\,5)$ in S_6
3. $(4\,1\,7\,9)(2\,8\,3)$ in S_9 (Hint: You will need the Socks-Shoes Property for this one!)

5.2.4 Element Order

The last bit of information we'll need for now about the symmetric groups is a method for computing the orders of permutations. We'll start easy with permutations that can be expressed as single cycles.

Example 5.2.8. Consider $\sigma = (3\,4\,1\,2)$ in S_4. Let's find its order by raising σ to successively higher powers (starting with 2 since only the identity element can have order 1) until we get the identity element.

$\sigma^2 = (3\,4\,1\,2)(3\,4\,1\,2) = (3\,1)(4\,2) \neq (1)$, so $|\sigma| \neq 2$.

$\sigma^3 = \sigma^2\sigma = [(3\,1)(4\,2)][(3\,4\,1\,2)] = (3\,2\,1\,4) \neq (1)$, so $|\sigma| \neq 3$.

$\sigma^4 = \sigma^3\sigma = (3\,2\,1\,4)(3\,4\,1\,2) = (1)$, so $|\sigma| = 4$.

This should not seem surprising, since each successive power of σ just sends each element one more spot to the right in the cycle. Since the cycle length is 4, the smallest power of σ that brings all of the elements back where they started is 4.

In general, the order of an n-cycle is always just n. Now what if the permutation is a product of more than one cycle?

Example 5.2.9. Let's find the order of $\sigma = (1\,4\,5\,10)(2\,3\,9\,6\,8\,7)$ in S_{10}.

$\sigma^2 = [(1\,5)(4\,10)][(2\,9\,8)(3\,6\,7)] \neq (1)$, so $|\sigma| \neq 2$.

$\sigma^3 = [(1\,10\,5\,4)][(2\,6)(3\,8)(9\,7)] \neq (1)$, so $|\sigma| \neq 3$.

$\sigma^4 = [(1)][(2\,8\,9)(3\,7\,6)] \neq (1)$, so $|\sigma| \neq 4$.

Notice, however, that the 4-cycle in σ has been brought back to the identity. This is expected since it's a 4-cycle and we've just raised it to the power of 4. The 6-cycle has not yet been brought back to the identity, though. We know this won't happen until we get to a power of 6. Let's skip ahead to this:

$\sigma^6 = [(1\,5)(4\,10)][(1)] \neq (1)$, so $|\sigma| \neq 6$.

What will it take for the 4-cycle and the 6-cycle to both be brought back to the identity *at the same time*? The power would have to be a common multiple of both 4 and 6. For this power to be given the title of the *order* of σ, it would have to be the *smallest* such common multiple, namely 12. So $|\sigma| = 12$.

This situation generalizes easily to give us:

Theorem 5.2.10. *The order of a permutation in S_n is the least common multiple of the permutation's cycle lengths when it's written as a product of disjoint cycles.*

Activity 5.2.11. Find the order of $(1\,6\,2)(6\,8\,1\,5\,2)$ in S_8. Be careful, the answer is *not* 15.

5.3 The Alternating Group

As stated in Activity 5.2.7, a cycle of length 2 is called a **2-cycle** or **transposition**; it "transposes" the two elements in the cycle.

Activity 5.3.1. Show that the permutation $(5\,6\,1\,2\,4\,3)$ can be written as the following product of transpositions:

$$(5\,3)(5\,4)(5\,2)(5\,1)(5\,6).$$

Activity 5.3.2. Use the pattern observed in the previous activity to propose a way to write any given cycle as a product of transpositions. Then use this method to decompose the following permutations into transpositions:

1. $(3\,4\,1\,7\,2)$
2. $(1\,2)(6\,3\,5\,4)$

When a permutation can be carried out by an odd number of transpositions, we say that the permutation is **odd**. Otherwise we say that the permutation is **even**.

Activity 5.3.3. State whether the permutations in the previous two activities are even or odd. Would an 8-cycle be even or odd? How about a 15-cycle? How about the product of an 11-cycle and a 26-cycle?

Let A_n denote the set of all even permutations in S_n.

Activity 5.3.4. Show that A_n is a subgroup of S_n by applying the Subgroup Test.

The group A_n is called the **alternating group of degree** n.

Activity 5.3.5. Historically, the names for the symmetric and alternating groups come from symmetric and alternating polynomials. A **symmetric polynomial** is one with the property that every transposition of two of its variables leaves the polynomial unchanged. An **alternating polynomial** is one with the property that any transposition of two of its variables multiplies the entire polynomial by -1.

1. Show that the polynomial f from Activity 2.1.1 is an alternating polynomial and that its symmetry group is A_3.
2. Show that the polynomial g from Activity 2.1.1 is a symmetric polynomial and that its symmetry group is S_3.

The order of A_n is given by the following theorem.

Theorem 5.3.6. *The order of A_n is $\frac{1}{2}n!$.*

Proof. Recall that the order of S_n is $n!$. This theorem is thus claiming that exactly half of the permutations of $\{1, 2, \ldots, n\}$ are even (and necessarily, the other half are odd). In other words, the number of even permutations of the set $\{1, 2, \ldots, n\}$ is the same as the number of odd permutations. To establish that this claim is true, we will employ the standard method of establishing a one-to-one correspondence between A_n and the set of odd permutations. Let's call the set of odd permutations B_n for now.

So our job is to define a function $f : A_n \to B_n$ which is one-to-one and onto. The function f would take each even permutation as an input and send it to an odd permutation as an output. First note that the product of an even permutation σ and the transposition $(1\,n)$ must be an odd permutation since $\sigma(1\,n)$ would be the product of an odd number of transpositions. We will thus define our function $f : A_n \to B_n$ by $f(\sigma) = \sigma \cdot (1\,n)$.

To show that f is one-to-one, suppose for two elements σ_1 and σ_2 in A_n that $f(\sigma_1) = f(\sigma_2)$. This would mean that $\sigma_1 \cdot (1\,n) = \sigma_2 \cdot (1\,n)$. Applying the Cancellation Law, this equation reduces to $\sigma_1 = \sigma_2$, and this implies that f is one-to-one.

To show that f is onto, fix an arbitrary odd permutation τ in B_n. We will propose an even permutation σ in A_n such that $f(\sigma) = \tau$. Let's propose that we try $\sigma = \tau \cdot (1\,n)$. Clearly, σ is even since τ is odd. Also,

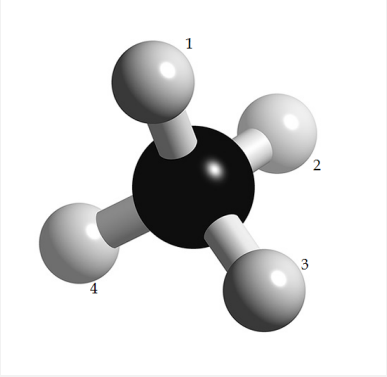
$$\begin{aligned} f(\sigma) &= f(\tau \cdot (1\,n)) \\ &= (\tau \cdot (1\,n))(1\,n) \\ &= \tau \cdot ((1\,n)(1\,n)) \\ &= \tau. \end{aligned}$$

We can therefore conclude that f is onto in addition to being one-to-one and is hence a one-to-one correspondence. □

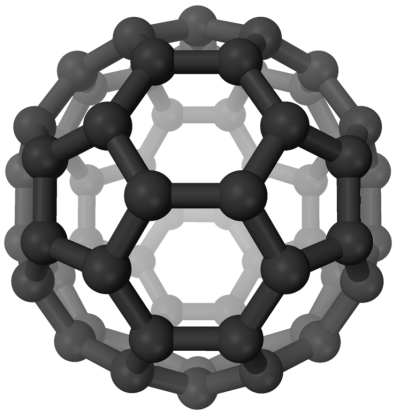
Activity 5.3.7. How many elements does A_4 have? Write them all down.

When you first encounter them, the alternating groups seem like kind of a "niche" group. We have to work pretty hard to define them, and the motivation to even define them in the first place seems to be missing. However, as we'll see below, they show up very naturally as symmetry groups. They also form a class of so-called *simple* groups, which we'll define in Chapter 10. Simple groups are in a sense "building block" groups from which all other groups can be built, kind of like atoms in chemistry or prime numbers in number theory.

Activity 5.3.8. Show that the rotation group of the methane molecule (first encountered in Exercise 12 in Chapter 1) is A_4. Try to express the rotations as permutations of the hydrogen atoms labeled 1, 2, 3, and 4.



Though we won't do so here, one can show that an alternating group describes the rotational symmetries of another famous molecule, buckminsterfullerine. This molecule consists of 60 carbon atoms and can be visualized as below. Because of its sphere-like shape, it's often called the "Buckyball". Its



namesake is the American architect Buckminster Fuller (1895-1983) who popularized geodesic domes. Its group of rotational symmetries turns out to be A_5. The Buckyball probably looks like a soccer ball to you, and indeed, a soccer ball also has A_5 as its rotational symmetry group.

Another role that one of the alternating groups, A_4, plays is the promised counterexample to the converse of Lagrange's Theorem. It can be shown, using methods we won't cover, that even though $|A_4| = 12$, A_4 has no subgroup of order 6, despite the fact that 6 divides 12.

5.4 Updated Summary of Examples of Groups

The table below contains a summary of the examples of groups we will cover, updated from the one in Chapter 3. While this list is far from complete, it's sufficient for an introduction to group theory.

set	**operation**	**Abelian?**	**order**
D_n $(n \geq 3)$	symmetry composition	no	$2n$
$\mathbb{R}$	addition	yes	infinite
$\mathbb{R}^*$	multiplication	yes	infinite
$\mathbb{Q}$	addition	yes	infinite
$\mathbb{Q}^*$	multiplication	yes	infinite
$\mathbb{Z}$	addition	yes	infinite
$\mathbb{C}$	addition	yes	infinite
$\mathbb{C}^*$	multiplication	yes	infinite
$GL_n(\mathbb{R})$ $(n \geq 2)$	matrix multiplication	no	infinite
$SL_n(\mathbb{R})$ $(n \geq 2)$	matrix multiplication	no	infinite
$\mathbb{Z}_n$ $(n \geq 2)$	addition mod n	yes	n
$U(n)$ $(n \geq 2)$	multiplication mod n	yes	$< n$, even
S_n $(n \geq 3)$	permutation composition	no	$n!$
A_n $(n \geq 4)$	permutation composition	no	$\frac{1}{2}n!$

Table 5.1: Examples of groups

5.5 Exercises

1. Let σ be the permutation $(4\,7\,2)(8\,4\,1)(5\,4\,3)$ in S_8.
   (a) How do you interpret the fact that the number 6 doesn't show up in σ?
   (b) Write σ as a product of disjoint cycles.
   (c) Find the inverse of σ.
   (d) Find the order of σ.
   (e) Is $\sigma \in A_8$? Explain.
2. What familiar group is S_2 isomorphic to? (Because of this, when we refer to the symmetric groups, we restrict attention to S_n with $n \geq 3$.)
3. Show that the n-cycle $(1\,2\,\cdots\,n)$ and the 2-cycle $(1\,2)$ do not commute in S_n for $n \geq 3$, and conclude that S_n is not Abelian for $n \geq 3$.

4. Let H be the subset of S_n consisting of the permutations of $\{1\,2\,\ldots n\}$ which fix the number n. **Prove** that H is a subgroup of S_n and state its order.

5. What are the possible orders of the subgroups of S_4? Find a subgroup of each possible order. (Recall that Lagrange's Theorem makes no guarantee that subgroups of each possible order actually exist, but it just so happens that they do in this case.)

6. Give two reasons why the subset of odd permutations in S_n is not a subgroup of S_n.

7. Let $\sigma = (1\,4\,5)(1\,2\,3)$. Write σ^{99} as a product of disjoint cycles.

8. What familiar group is A_3 isomorphic to? For this reason, when considering the alternating groups, we restrict to $n \geq 4$. (Hint: What's the order of A_3?)

9. Let α and β be elements of S_n. Explain why $\alpha^{-1}\beta^{-1}\alpha\beta$ is in A_n.

10. According to Lagrange's Theorem, what are the possible orders of the elements of A_6?

11. What is the symmetry group of the polynomial

$$f(x, y, z) = x^2y^2z^2 + xyz^2 + xy^2z + x^2yz?$$

How about

$$g(w, x, y, z) = (w - x)^3(w - y)^3(w - z)^3(x - y)^3(x - z)^3(y - z)^3?$$

12. Consider D_4 as a subgroup of S_4 by thinking of the elements of D_4 as permutations of the vertices of a square. Which elements of D_4 are even and which are odd?

13. A *perfect shuffle* of a deck of 52 playing cards is performed as follows. First, split the deck into two piles of 26 cards each. Place one pile on the left and the other on the right. Second, shuffle the cards together into a new stack of 52 by picking up the first card in the left pile, then the first card in the right, then the second card in the left, then the second card in the right, etc, until all 52 cards are picked up.

    Without actually performing any shuffles, how many consecutive perfect shuffles will it take to return the deck to its original arrangement? (Hint: A perfect shuffle is just a permutation of the 52 cards. Try to write this permutation in cycle notation.)

Chapter 6

Isomorphisms of Groups

6.1 Definition and Examples

In Chapter 2, we informally defined what it means for two groups to be *isomorphic*: there is a way to rename the elements of one group as the elements of another in such a way that the two groups' Cayley tables become identical. This definition is convenient when the two groups' orders are small but not when the groups are big, infinite, or defined abstractly. We thus need a way to establish that two groups are isomorphic without having to look at their Cayley tables.

For example, in Activity 3.0.2, we were left wondering how you could prove that C_n is isomorphic to $\mathbb{Z}_n$ for some general, unspecified positive integer n. The first thing we'd have to do is to rename the elements of C_n as elements of D_n. In other words, we would have to state a rule which says how to take an element of C_n and associate it to an element of $\mathbb{Z}_n$. What we're really talking about, then, is defining a function $f : C_n \to \mathbb{Z}_n$. The function is the rule that describes how the renaming will work.

Activity 6.1.1.

1. Write down the elements of C_4 as well as the elements of $\mathbb{Z}_4$.
2. Propose a way to associate each element of C_4 to exactly one element of $\mathbb{Z}_4$. (There are lots of ways to do this.)
3. Your answer to the previous problem actually defines a function (let's call it f) from C_4 to $\mathbb{Z}_4$. Rewrite your associations from Problem 2 using function notation.

Activity 6.1.1. (continued)

4. Propose a way to associate the elements of C_n to elements of $\mathbb{Z}_n$ by defining a function $f : C_n \to \mathbb{Z}_n$. (You'll have to give a *formula* for your function.)

Activity 6.1.2. Verify that your functions from Problems 3 and 4 from the previous activity are one-to-one and onto.

The above two activities show that the process of renaming the elements of one group as the elements of the other is exactly the same as the process of defining a one-to-one correspondence from one group to the other.

Recall, though, that for the groups to be considered isomorphic to each other, the renaming (aka, one-to-one correspondence) must be such that the groups' Cayley tables become identical.

Activity 6.1.3.

1. Suppose we were to define a one-to-one correspondence $f : C_3 \to \mathbb{Z}_3$ by $f(R_0) = 2$, $f(R_{120}) = 0$, and $f(R_{240}) = 1$. Rewrite the Cayley table for C_3 according to f; that is, make the Cayley table for C_3, then replace all of the R_0's by 2, all of the R_{120}'s by 0, and all of the R_{240}'s by 1. Is the result identical to the Cayley table for $\mathbb{Z}_3$?

2. The previous problem does *not* mean that C_3 and $\mathbb{Z}_3$ are not isomorphic. It just means that the function f doesn't rename the elements of C_3 in a way that makes the Cayley tables identical. Maybe a different function would. Repeat Problem 1 by defining $f : C_3 \to \mathbb{Z}_3$ by $f(R_0) = 0$, $f(R_{120}) = 1$, and $f(R_{240}) = 2$.

3. Does your function f from Problem 3 in Activity 6.1.1 make the Cayley table for C_4 identical to the one for $\mathbb{Z}_4$? If not, redefine your f so that they *will* be identical.

It still remains to determine how to show that a one-to-one correspondence will make the Cayley table of one group identical to that of another's without actually constructing the Cayley table.

Suppose we have two groups, G and H, which we suspect are isomorphic. Suppose also that we've defined a function $\phi : G \to H$ which we've shown is one-to-one and onto. Now let's look at what would have to happen in the Cayley tables of G and H in order for ϕ to turn the Cayley table for G into that for H. Suppose a and b are elements of G. They get renamed as the elements $\phi(a)$

and $\phi(b)$ of H. The Cayley tables look like this so far:

	$\cdots$	b	$\cdots$
$\vdots$			
a		ab	
$\vdots$			

Table 6.1: Cayley Table for G

	$\cdots$	$\phi(b)$	$\cdots$
$\vdots$			
$\phi(a)$		$\phi(a)\phi(b)$	
$\vdots$			

Table 6.2: Cayley Table for H

In order for these Cayley tables to be the same, the element ab in row a, column b of the Cayley table for G must get renamed as the element in row $\phi(a)$, column $\phi(b)$ in the Cayley table for H. The element ab gets renamed as $\phi(ab)$, so this must coincide with the element $\phi(a)\phi(b)$ that's already in row $\phi(a)$, column $\phi(b)$ in the Cayley table for H. In other words, we must have

$$\phi(ab) = \phi(a)\phi(b)$$

for any elements $a, b \in G$. This finally brings us to the official definition of an isomorphism:

Definition 6.1.4. An **isomorphism** of groups G and H is a function $\phi : G \to H$ such that

1. ϕ is one-to-one,
2. ϕ is onto, and
3. $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

When an isomorphism of G and H exists, we say G is **isomorphic** to H, and we denote this by $G \cong H$.

Note that the isomorphism is the function that renames the elements of G as elements of H in such a way that the Cayley tables are identical. The function f in Problem 1 of Activity 6.1.3 is not an isomorphism, but the altered version of f in Problem 2 of that same activity is an isomorphism.

The word "isomorphism" hints at the right way to think about isomorphic groups. "Iso" means "same" and "morph" means "shape". Two isomorphic groups are groups that are the "same shape". We should think of isomorphic groups as groups that are essentially the same, with only superficial differences.

If a function from one group to another satisfies the third property – $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$ – but is not necessarily one-to-one or onto, then we call it a **homomorphism**. ("Homo" means "similar", which is a weaker condition than "same".)

Activity 6.1.5. Prove that $C_n \cong \mathbb{Z}_n$ by defining a function $f : C_n \to \mathbb{Z}_n$ and verifying that it's one-to-one, onto, and a homomorphism.

Being able to prove that an unfamiliar or seemingly complicated group is isomorphic to a familiar or seemingly simple one is one of the most powerful moves in abstract algebra. Here's an example.

Example 6.1.6. Let G be the subgroup of $GL_3(\mathbb{R})$ consisting of matrices of the form

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

where a can be any real number. (It's not obvious that G is a subgroup, but you'll verify this in Exercise 1.) We'll prove that G is isomorphic to $\mathbb{R}$, the additive group of real numbers.

The first step in proving that two groups are isomorphic is to propose a function from one group to the other that will hopefully turn out to satisfy the three isomorphism properties. This is often the hardest part of an isomorphism proof, but in this case, there's an obvious way to do it.

We'll define our function $\phi : G \to \mathbb{R}$ by

$$\phi\left(\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = a.$$

We first prove that ϕ is one-to-one. Suppose

$$\phi\left(\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = \phi\left(\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right).$$

Then by the definition of ϕ, $a = b$. This means that

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and therefore ϕ is one-to-one.

We'll now prove that ϕ is onto. Fix an arbitrary element $a \in \mathbb{R}$. We need to find a matrix in G that ϕ sends to a. By the definition of ϕ, the matrix

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

will work since

$$\phi\left(\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = a.$$

Thus, ϕ is onto.

Finally, we have to prove that ϕ is a homomorphism. This means showing that

$$\phi\left(\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = \phi\left(\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) + \phi\left(\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right).$$

Notice that on the left side of the equation, the operation is matrix multiplication since that's the operation in G, while the operation on the right is addition since that's the operation in $\mathbb{R}$. Remember that to prove that an equation holds, we work with the two sides independently, showing that they're equal to each other.

The left side is

$$\phi\left(\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right).$$

Multiplying the two matrices in parentheses gives

$$\phi\left(\begin{bmatrix} 1 & 0 & a+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right).$$

Now by the definition of ϕ, this equals $a + b$.

The right side is

$$\phi\left(\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) + \phi\left(\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right),$$

which by the definition of ϕ is also $a+b$. The left and right sides are equal, and we thus have that ϕ is a homomorphism.

We can now conclude that ϕ is an isomorphism, which means $G \cong \mathbb{R}$.

An **automorphism** is an isomorphism from a group to itself. ("Auto" means "self".) One can think of an automorphism of a group G as a symmetry of G – it's a way to rearrange the elements of G without actually changing the group structure of G.

Activity 6.1.7. Prove that the function $f : \mathbb{Q}^* \to \mathbb{Q}^*$ defined by $f(\frac{a}{b}) = \frac{b}{a}$ is an automorphism of $\mathbb{Q}^*$.

6.2 Isomorphism Properties

In abstract algebra, isomorphic groups are often thought of as being the "same" as each other. Strictly speaking, this isn't true. For example, C_n and $\mathbb{Z}_n$, though isomorphic, are different groups. But being isomorphic ensures that they share the same group-theoretic properties. For example, they have the same order, they're both Abelian, and the orders of their elements are the same. Their differences, such as the names of the elements and the way the binary operation is defined, are superficial. In this section, we'll prove that isomorphic groups share properties such as the ones mentioned above.

Theorem 6.2.1. *Suppose G and H are isomorphic groups. Then $|G| = |H|$.*

Activity 6.2.2.

1. Explain why this is true when G and H are finite. (See Section 3.5.2.)
2. Explain why this is true when at least one of G or H is infinite. (Try it as a proof by contradiction: What if G were infinite but H were finite? Could there possibly be an isomorphism from G to H?)

The theorem above confirms something we already believe: groups of different orders cannot be isomorphic.

Theorem 6.2.3. *Suppose G and H are isomorphic groups. Then G is Abelian if and only if H is Abelian.*

Proof. You'll prove this in Exercise 8. □

Activity 6.2.4. The groups D_4 and $\mathbb{Z}_8$ both have order 8. Are they isomorphic?

So far we've seen that isomorphic groups must have the same order as each other and must either both be Abelian or both be non-Abelian. But these properties alone are not enough to distinguish non-isomorphic groups from each other:

Activity 6.2.5. In Exercise 5 in Chapter 2, you showed that there are two groups of order 4, both of which are Abelian, that are not isomorphic to each other. Look again at the two possible 4×4 Cayley tables and use them to explain why these groups are not isomorphic.

The above activity illustrates a good way to distinguish non-isomorphic groups from each other: Find the orders of the elements of each group, and if the lists of orders (including repeated orders) aren't identical, then the groups are not isomorphic. We'll prove this now by first working through three lead-up lemmas. Notice that each of these lemmas is stated under the hypothesis that the function is only an *onto homomorphism*. The reason is that the proofs only require the onto and operation-preserving property, not the one-to-one property. However, since every isomorphism is an onto homomorphism, anything that can be proved about onto homomorphisms automatically applies to isomorphisms as well.

Lemma 6.2.6. *Suppose G and H are groups and $\phi : G \to H$ is a homomorphism which is onto. Suppose e_G is the identity element in G and e_H is the identity element in H. Then $\phi(e_G) = e_H$.*

Proof. We have to prove that $\phi(e_G)$ is the identity element of H. This means we have to show that for an arbitrary element $h \in H$, $\phi(e_G)h = h$ and $h\phi(e_G) = h$.

Fix an arbitrary element $h \in H$. Since $\phi : G \to H$ is onto, there is an element $g \in G$ such that $\phi(g) = h$. Thus,

$$\phi(e_G)h = \phi(e_G)\phi(g). \tag{6.1}$$

Since ϕ is a homomorphism, the right side of Equation (6.1) equals $\phi(e_G g)$, and since e_G is the identity of G, $e_G g = g$. This means we can rewrite Equation (6.1) as

$$\phi(e_G)h = \phi(g). \tag{6.2}$$

But g was chosen from G so that $\phi(g) = h$, so Equation (6.2) becomes

$$\phi(e_G)h = h.$$

(The proof that $h\phi(e_G) = h$ is nearly identical and is not included here.)

Since $\phi(e_G)h = h$ and $h\phi(e_G) = h$, we can conclude that $\phi(e_G) = e_H$. □

A consequence of this result is:

Lemma 6.2.7. *Suppose G and H are groups and $\phi : G \to H$ is a homomorphism which is onto. Then for any $g \in G$, $\phi(g^{-1}) = [\phi(g)]^{-1}$.*

Proof. We have to show that the inverse of $\phi(g)$ (as an element of H) is $\phi(g^{-1})$. To do so, we will prove that $\phi(g)\phi(g^{-1})$ and $\phi(g^{-1})\phi(g)$ both equal the identity e_H in H.

Since ϕ is a homomorphism, we have that

$$\begin{aligned}\phi(g)\phi(g^{-1}) &= \phi(gg^{-1}) \\ &= \phi(e_G),\end{aligned}$$

where e_G is the identity in G. By the previous lemma, we know that $\phi(e_G) = e_H$. We therefore have that $\phi(g)\phi(g^{-1}) = e_H$. (The proof that $\phi(g^{-1})\phi(g) = e_H$ is nearly identical and is skipped here.)

We can therefore conclude that $\phi(g)$ and $\phi(g^{-1})$ are inverses of each other in H. In other words, $\phi(g^{-1}) = [\phi(g)]^{-1}$. □

Lemma 6.2.8. *Suppose G and H are groups and $\phi : G \to H$ is a homomorphism which is onto. Then for any integer n and any element $g \in G$, $\phi(g^n) = [\phi(g)]^n$.*

Proof. This is a tailor-made induction proof and is the goal of Exercise 9. □

We now come to one of the most important and useful properties of isomorphisms. Notice that this theorem is stated for *isomorphisms*, not just onto homomorphisms, which means the proof will make use of the one-to-one property.

Theorem 6.2.9. *Suppose G and H are groups and $\phi : G \to H$ is an isomorphism. For any element $g \in G$, $|g| = |\phi(g)|$.*

Proof. We will consider two separate cases: Case 1 will be that $|g|$ is finite, and Case 2 will be that $|g|$ is infinite.

Case 1: We will fix an arbitrary element $g \in G$ and assume that $|g|$ is finite. Let's say $|g| = n$. This means that n is the smallest natural number such that $g^n = e_G$. We have to show that n is also the smallest natural number such that $[\phi(g)]^n = e_H$.

We know by Lemma 6.2.8 that $[\phi(g)]^n = \phi(g^n)$. Since n is the order of g, $g^n = e_G$. Thus, $[\phi(g)]^n = \phi(e_G) = e_H$ by Lemma 6.2.6. However, to conclude that n is the order of $\phi(g)$, we also have to show that n is the *smallest* natural number such that $[\phi(g)]^n = e_H$.

Toward that end, suppose that m is another natural number such that $[\phi(g)]^m = e_H$. We will prove that $m \geq n$.

By Lemma 6.2.8 again, we have $\phi(g^m) = e_H$. We know by Lemma 6.2.6 that $\phi(e_G) = e_H$, and since we're told that ϕ is an isomorphism, we also know that ϕ is one-to-one. This means that if we have both $\phi(g^m) = e_H$ and $\phi(e_G) = e_H$, then it must be that $g^m = e_G$. But the order of g is n, which means that if $g^m = e_G$, then it must be that $m \geq n$. We can now conclude that $|\phi(g)| = n$.

Case 2: We will now fix an arbitrary $g \in G$ and assume that $|g| = \infty$. This means that there is no natural number n such that $g^n = e_G$. We will prove that there is no natural number n such that $[\phi(g)]^n = e_H$.

Since our goal is to conclude a negative statement, a proof by contradiction is appropriate. Suppose, then, to the contrary, that there *is* a natural number n such that $[\phi(g)]^n = e_H$. Then by Lemma 6.2.8, we have $\phi(g^n) = e_H$. Since

ϕ is one-to-one, we can conclude (just as in Case 1) that $g^n = e_G$. However, this contradicts the fact that $|g| = \infty$. Therefore, it cannot be that there is a natural number n such that $[\phi(g)]^n = e_H$, so it must be that $|\phi(g)| = \infty$. We therefore have in this case as well that $|g| = |\phi(g)|$. □

Theorem 6.2.9 provides a very useful way to determine when two groups are *not* isomorphic.

Activity 6.2.10. The groups $U(30)$ and $\mathbb{Z}_8$ are both groups of order 8. They are also both Abelian. It seems that they might therefore be isomorphic. Show that they are not.

If two groups have the same order and have the same lists of orders of elements, must they be isomorphic? The answer is "yes" if both groups are Abelian but "not necessarily" if at least one of the groups in non-Abelian. We don't yet have enough tools at our disposal to justify this statement, but we will return to it in Chapter 8.

Activity 6.2.11. Some properties of groups are not preserved by isomorphisms and are therefore not considered essential.

1. Can two groups, one of which has a multiplicative binary operation and the other of which has an additive one, be isomorphic? Try to think of a pair of isomorphic groups, one which uses multiplicative notation and the other which uses additive.

2. Can two groups which consist of entirely different types of mathematical objects as elements be isomorphic? Hint: Revisit Example 6.1.6.

6.3 Writing Proofs: Proof by Cases and "Or" Statements

A few times in this and previous chapters, we've attacked a proof by breaking it into separate cases. For example, in the proof of Theorem 6.2.9, we first proved that $|g| = |\phi(g)|$ in the case that $|g|$ is finite and then in the case that $|g|$ is infinite. We did this because the definition of $|g|$ is different in each of these cases and had to therefore be handled differently.

We can also use the logic of proofs by cases to prove "or statements". These are statements in which we have to conclude that an outcome P or an outcome Q occurs. This does *not* mean that only one of P or Q can occur. To say that P or Q occurs means that at *at least one but maybe both* of P or Q will occur.

For example, suppose we want to prove that if n is an even natural number, then $n \bmod 4 = 0$ or $n \bmod 4 = 2$. We could at first approach this as a proof by cases. When choosing cases, it's important that they exhaust all possibilities. Let's take Case 1 to be $n \bmod 4 = 0$ and Case 2 to be $n \bmod 4 \neq 0$. These cases cover all of our bases; there's no room for other possibilities.

Now let's suppose Case 1 is true: $n \bmod 4 = 0$. If that's the case, then there's nothing to prove. The "or" statement is true since one of its constituent statements is true.

Now let's suppose Case 2 is true: $n \bmod 4 \neq 0$. Since we have to conclude that $n \bmod 4 = 0$ or $n \bmod 4 = 2$, the only way we can do this is to conclude $n \bmod 4 = 2$ since we're assuming $n \bmod 4 \neq 0$. Now for the actual proof. We're given that n is even, and we're assuming in this case that $n \bmod 4 \neq 0$. This means that n is not divisible by 4. Thus, if we divide n by 4, we get a remainder which can only be one of 1, 2, or 3. Let r represent this remainder, and let q be the quotient obtained by this division. Then $n = 4q + r$, or equivalently, $r = n - 4q$. We know n is even, and since 2 divides $4q$, $4q$ is also even. Thus $r = n - 4q$ is also even. Since the only possibilities for r were 1, 2, and 3, r must be 2. Therefore, $n \bmod 4 = 2$.

To summarize, the way to prove a "P or Q" statement is thus to suppose that P is false, and prove that Q must be true (or vice versa). Here's another easy example just to illustrate the technique. We're trying to prove an "or" statement, so we'll assume one of the possible conclusions is false and then prove that the other is true.

Theorem. *If $x^2 = x$, then $x = 0$ or $x = 1$.*

Proof. Suppose $x \neq 0$. We will prove that $x = 1$. Since $x \neq 0$, $\frac{1}{x}$ exists. Multiplying both sides of the equation $x^2 = x$ by $\frac{1}{x}$ gives $x = 1$. □

6.4 Exercises

1. Verify that the set G from Example 6.1.6 is a subgroup of $GL_3(\mathbb{R})$.
2. Fill in the blanks with one of the prefixes "iso", "homo", or "auto".
   (a) _____morphisms are not required to be one-to-one or onto.
   (b) _____morphisms are isomorphisms from groups to themselves.
   (c) Isomorphisms are automatically _____morphisms but not necessarily _____morphisms.
   (d) Automorphisms are both _____morphisms and _____morphisms.
3. Show that $\mathbb{Z}_4 \cong U(10)$, but $\mathbb{Z}_4 \ncong U(8)$.
4. **Prove** that every group is isomorphic to itself. (In other words, prove that every group has at least one automorphism.)

5. **Prove** that for a group G, the function $\alpha : G \to G$ defined by $\alpha(g) = g^{-1}$ is an automorphism if and only if G is Abelian.

6. Show that the function $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^x$ is an isomorphism. (Recall that $\mathbb{R}^+$ is the set of positive real numbers and is a group with respect to multiplication.)

7. State three groups of order 12, none of which are isomorphic to each other. Explain why no two of them are isomorphic.

8. **Prove** Theorem 6.2.3.

9. **Prove** Lemma 6.2.8. (Hint: Do this as a proof by cases with Case 1 being $n > 0$, Case 2 being $n = 0$, and Case 3 being $n < 0$.)

10. Let p be a prime number, and suppose G is a group of order p^2. **Prove** that G is cyclic or $g^p = e$ for every $g \in G$.

Chapter 7

Cyclic Groups

Some of the most important and celebrated results in the history of mathematics are *classification* theorems. For example, it's been known since the heyday of Ancient Greece that the convex regular polyhedra are completely classified: there are exactly five of them (the five Platonic solids).

While it's impossible to classify groups in this way, we can instead try to classify *isomorphism classes* of groups. An **isomorphism class** containing a group G is the collection of all of the groups which are isomorphic to G. You can think of it as the collection of groups which are essentially G "in disguise". We often refer to an isomorphism class by using one of its groups as a representative.

In Chapter 2, we classified the isomorphism classes of groups of small order. For example, there is exactly one isomorphism class of groups of order 3. We can take $\mathbb{Z}_3$ as its representative (or C_3 or A_3 or any group of order 3). In Exercise 5 from Chapter 2, we classified the isomorphism classes of groups of order 4: there are exactly two of them. One is represented by $\mathbb{Z}_4$, and the other is represented by a group of order 4 which is not isomorphic to $\mathbb{Z}_4$, such as $U(8)$.

This chapter and the next will culminate with one of the most famous theorems in group theory: the classification of (isomorphism classes of) finite Abelian groups. We'll see a very straightforward way to write down a representative group for every isomorphism class of finite Abelian groups. It turns out that every such group can be "built up" (in a sense that will be made precise in the next chapter) from cyclic groups.

7.1 Classification of Cyclic Groups

Recall from Chapter 4 that a group G is **cyclic** provided that there is an element $g \in G$ such that every element of G is of the form g^n for some integer n. The element g is called a **generator** of G. Using the notation of Chapter 4, we can

say that if G is cyclic and g is a generator of G, then $G = \langle g \rangle$.

Activity 7.1.1. Each of the following groups is cyclic. For each, state one of its generators.

1. C_n
2. $\mathbb{Z}_n$
3. Z
4. $U(18)$

Suppose G is a cyclic group generated by g. What does G "look like"? By definition, G is the set of all integer powers of g, so if G is infinite, we could say that $G = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$. (Recall that $e = g^0$ and $g = g^1$.)

What would a *finite* cyclic group look like? Suppose G is finite and that the generator g has order n. Then G consists of exactly n powers of g: $G = \{e, g, g^2, \ldots, g^{n-1}\}$. Notice that every other power of g is equal to one of these n powers.

Activity 7.1.2. Suppose G is a cyclic group and g is its generator. Suppose also that $|g| = 5$.

1. Write out the elements of G.
2. Which of these five elements is equal to g^{33}? Which is equal to g^{-16}?
3. Construct the Cayley table for G.
4. To what familiar group does G seem to be isomorphic?
5. Prove your answer to the previous problem.

The outcome of the above activity can be generalized:

Theorem 7.1.3 (Classification of Cyclic Groups)**.** *If G is a cyclic group of order n, then $G \cong \mathbb{Z}_n$. If G is a cyclic group of infinite order, then $G \cong \mathbb{Z}$.*

Proof. We'll start with the case where $|G| = n$. Then as seen above, $G = \{e, g, g^2, \ldots, g^{n-1}\}$. Define a function $\phi : G \to \mathbb{Z}_n$ by $\phi(g^k) = k$, where k is one of $0, 1, 2, \ldots, n-1$. We claim that ϕ is an isomorphism.

Activity 7.1.4.

1. Prove that ϕ is one-to-one.

Activity 7.1.4. (continued)

2. Prove that ϕ is onto.
3. For any integer k, explain why $g^k = g^{k \bmod n}$. (Recall that $|g| = n$.)
4. Use the previous problem to prove that ϕ is a homomorphism, i.e., that $\phi(g^i g^j) = \phi(g^i) + \phi(g^j)$.

The case where G is infinite is done very similarly and is left for Exercise 6. □

This is a very powerful statement in that it allows us to study abstract cyclic groups by instead studying the specific groups $\mathbb{Z}_n$ and $\mathbb{Z}$. All we have to do is:

1. translate a problem about abstract cyclic groups to the corresponding problem about $\mathbb{Z}_n$ or $\mathbb{Z}$,
2. solve the problem for $\mathbb{Z}_n$ or $\mathbb{Z}$ (which is usually easy since it would just involve familiar number arithmetic), and
3. translate the solution we found for $\mathbb{Z}_n$ or $\mathbb{Z}$ back to the abstract cyclic group.

The translations between G and $\mathbb{Z}_n$ or $\mathbb{Z}$ work as follows. It's necessary to have a generator of G – let's call it g.

$G = \langle g \rangle$		$\mathbb{Z}_n$ or $\mathbb{Z}$
mult. notation	$\longleftrightarrow$	add. notation
g	$\longleftrightarrow$	1
e	$\longleftrightarrow$	0
g^k	$\longleftrightarrow$	k

We'll perform these translations in the next couple of sections to answer the questions: (1) How do you compute the orders of elements in cyclic groups? and (2) How do you find the subgroups of cyclic groups?

7.2 Orders of Elements in Cyclic Groups

In this section, our goal is to answer the question: How do you compute the orders of elements in cyclic groups? We'll do so by translating the question to $\mathbb{Z}_n$ or $\mathbb{Z}$, answering it for those groups, and translating the solution back to the general setting. This is valid since, by Theorem 6.2.9, isomorphic groups have the same lists of orders of elements.

Activity 7.2.1.

1. Does $\mathbb{Z}$ have any elements of finite order? What are they?
2. Use your answer to the previous problem to answer the same question about an infinite cyclic group G with generator g.

Now for a finite cyclic group G of order n generated by g. What are the orders of the elements in G? The process is the same as what we just saw for infinite cyclic groups: translate the question to $\mathbb{Z}_n$, get an answer, translate the answer back to G. It turns out, though, that it takes more work to find element orders in $\mathbb{Z}_n$.

Activity 7.2.2. Find the orders of the elements of $\mathbb{Z}_{10}$. As you do so, think about how the method you develop might generalize to $\mathbb{Z}_n$ for an arbitrary positive integer n.

Theorem 7.2.3. *The order of a nonzero element k in $\mathbb{Z}_n$ is*

$$\frac{\text{lcm}(k,n)}{k}.$$

We've just completely solved the element order problem for $\mathbb{Z}_n$, so now we can translate the solution back to the abstract cyclic group $G = \langle g \rangle$.

Activity 7.2.4. Let G be a cyclic group of order n generated by g. Use Theorem 7.2.3 and the isomorphism from G to $\mathbb{Z}_n$ to determine the order of g^k when $k \neq 0$.

What is the order of g^0?

Activity 7.2.5. Suppose G is a cyclic group of order 8 generated by g. Find the orders of all eight elements of G. Which of these elements are generators of G?

7.3 Subgroups of Cyclic Groups

Activity 7.3.1.

1. Find three different subgroups of D_4. (Hint: Look for *cyclic* subgroups because they're the easiest to find.)

Activity 7.3.1. (continued)

2. Show that $\{R_0, R_{180}, V, H\}$ is also a subgroup of D_4, though not a cyclic one.

The above activity shows that a given group can have non-cyclic subgroups. This is bad news because non-cyclic subgroups are often hard to find, and this makes the problem of determining all of the subgroups of a given group a very difficult one in general. However, the situation is *much* better when the given group is cyclic:

Theorem 7.3.2. *Every subgroup of a cyclic group is cyclic.*

Proof. Because of the classification of cyclic groups, it will suffice to prove this theorem under the assumption that our cyclic group is $\mathbb{Z}_n$ (when the group is finite) or $\mathbb{Z}$ (when the group is infinite). We will prove the theorem only for $\mathbb{Z}_n$, although the proof for $\mathbb{Z}$ is identical.

Let H be an arbitrary subgroup of $\mathbb{Z}_n$. Our goal is to show that H is cyclic. To do so, we have to show that some element of H is a generator of H.

We will break this proof into two cases: Case 1 is that H is a 1-element group containing only the identity, 0. Case 2 is that H contains more than just 0. Case 1 is very easy, for if $H = \{0\}$, then H is cyclic since 0 would be a generator for H.

Now for Case 2, we will assume H contains nonzero elements. Let a be the smallest nonzero element of H. We claim that a is our sought-after generator. To verify this, we have to show that every element of H can be written as an integer multiple of a (remember that we're in an *additive* group). Let h be an arbitrary element of H. Let's divide h by a, getting a quotient q and a remainder r. Then $h = qa + r$. We know that $h \in H$, and $a \in H$. Since H is closed under addition, $qa \in H$, and since the inverse of every element of H is in H, we also know $-qa \in H$. Therefore, $h - qa \in H$. Since $h = qa + r$, $r = h - qa$, so this means $r \in H$. But r is a remainder obtained upon division by a, which means that $0 \leq r \leq a - 1$. In particular, $r < a$. But a was taken to be the smallest nonzero element of H, and as we've seen, $r \in H$. Thus r can't be a nonzero element of H (since a is the smallest), so the only option left is $r = 0$. But if $r = 0$, then $h = qa$, which means that h is an integer multiple of a. Since h was chosen to be an arbitrary element of H, we can thus say that *every* element of H is an integer multiple of a; in other words, a is a generator of H. Therefore, H is cyclic. □

Activity 7.3.3. Find all of the subgroups of $\mathbb{Z}_{10}$.

Activity 7.3.4. Notice that several of the subgroups in the previous example are repeated. In particular, $\langle 1\rangle = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle$, and $\langle 2\rangle = \langle 4\rangle = \langle 6\rangle = \langle 8\rangle$.

What property do 1, 3, 7, and 9 share in $\mathbb{Z}_{10}$? What property do 2, 4, 6, and 8 share? (The answer is not being odd or even. If that were the answer, then why would 5 be missing from the first set of numbers?)

Hopefully the above activity leads you to the conjecture that two elements generate the same subgroup of $\mathbb{Z}_n$ if and only if they have the same order in $\mathbb{Z}_n$. This turns out to be true! And thanks to Theorem 7.2.3, it's really easy to determine whether two elements of $\mathbb{Z}_n$ have the same order, as we'll see in the following activity. We will need a general fact:

$$\text{For two natural numbers } r \text{ and } s,\ \gcd(r,s)\cdot \operatorname{lcm}(r,s) = rs. \tag{7.1}$$

(This can be proved by writing r and s as products of their prime factors.)

Activity 7.3.5. Let a and b be nonzero elements of $\mathbb{Z}_n$. In this activity, we will prove that $|a| = |b|$ if and only if $\gcd(a,n) = \gcd(b,n)$.

1. Using Statement 7.1, show that
$$\operatorname{lcm}(a,n) = \frac{an}{\gcd(a,n)} \qquad \text{and} \qquad \operatorname{lcm}(b,n) = \frac{bn}{\gcd(b,n)}.$$
2. Using Theorem 7.2.3, show that
$$\operatorname{lcm}(a,n) = a|a| \qquad \text{and} \qquad \operatorname{lcm}(b,n) = b|b|.$$
3. Use the outcomes of the previous two problems to conclude that
$$\gcd(a,n) = \frac{n}{|a|} \qquad \text{and} \qquad \gcd(b,n) = \frac{n}{|b|}.$$

Now for the "if and only if" statement. We'll first start with the assumption that $|a| = |b|$ and use it to prove that $\gcd(a,n) = \gcd(b,n)$.

4. Assuming that $|a| = |b|$, use the outcomes of Problems 1, 2, and 3 to prove that $\gcd(a,n) = \gcd(b,n)$.

Activity 7.3.5. (continued)
Now let's assume $\gcd(a, n) = \gcd(b, n)$ and prove that $|a| = |b|$.

5. Assuming that $\gcd(a, n) = \gcd(b, n)$, use the outcomes of Problems 1, 2, and 3 to prove that $|a| = |b|$.

We're ready to completely determine the subgroup structure of $\mathbb{Z}_n$.

Theorem 7.3.6. *Two elements a and b generate the same subgroup of $\mathbb{Z}_n$ if and only if $\gcd(a, n) = \gcd(b, n)$.*

Proof. This is also an "if and only if" statement, so we'll first start with the assumption that two elements a and b generate the same subgroup of $\mathbb{Z}_n$ and prove that $\gcd(a, n) = \gcd(b, n)$. We're assuming that $\langle a \rangle = \langle b \rangle$, and in particular, $\langle a \rangle$ and $\langle b \rangle$ have the same number of elements. But the number of elements in $\langle a \rangle$ equals $|a|$ and the number in $\langle b \rangle$ equals $|b|$. Therefore, $|a| = |b|$. By Activity 7.3.5, we can conclude that $\gcd(a, n) = \gcd(b, n)$.

Now suppose a and b are elements of $\mathbb{Z}_n$ such that $\gcd(a, n) = \gcd(b, n)$. We have to show that $\langle a \rangle = \langle b \rangle$. Let's abbreviate $\gcd(a, n)$ (or equivalently, $\gcd(b, n)$) by d. Since d is an integer in the interval $[0, n - 1)$, we can think of d as an element of $\mathbb{Z}_n$. Thus, d generates its own subgroup of $\mathbb{Z}_n$, namely $\langle d \rangle$. Furthermore, $d = \gcd(d, n)$, so by Activity 7.3.5, we know that $|d| = |a| = |b|$. If we can show that $\langle a \rangle$ and $\langle b \rangle$ both equal $\langle d \rangle$, then $\langle a \rangle$ and $\langle b \rangle$ must of course equal each other, and we'll be done.

We'll start by showing $\langle a \rangle = \langle d \rangle$. Normally, we would do this using a set equality proof, but we can bypass a full set equality proof this time thanks to the facts we've already established. Instead, we'll show that $\langle a \rangle \subseteq \langle d \rangle$ and then conclude that $\langle a \rangle = \langle d \rangle$ using some of our results about d.

Let x be an arbitrary element of $\langle a \rangle$. Then x is an integer multiple of a; let's say $x = ma$ for some integer m. Since $d = \gcd(a, n)$, d divides a. Thus d divides ma. In other words, d divides x. This means x is an integer multiple of d, and so $x \in \langle d \rangle$. We've thus shown that $\langle a \rangle \subseteq \langle d \rangle$.

However, we know that $|a| = |d|$, which implies that $\langle a \rangle$ and $\langle d \rangle$ have the same number of elements. So $\langle a \rangle$ is a subset of $\langle d \rangle$ with the same number of elements as $\langle d \rangle$. This can only happen if $\langle a \rangle = \langle d \rangle$. The exact same argument (replacing a with b) proves that $\langle b \rangle = \langle d \rangle$. We therefore have that $\langle a \rangle = \langle b \rangle$. □

Activity 7.3.7. We now have a very practical way to quickly find all of the subgroups of $\mathbb{Z}_n$ because we now know that the distinct (nonzero) subgroups of $\mathbb{Z}_n$ correspond exactly to the distinct values of $\gcd(a, n)$ for nonzero a in $\mathbb{Z}_n$.

Activity 7.3.7. (continued)

1. List all of the distinct values of $\gcd(a, 20)$ for nonzero $a \in \mathbb{Z}_{20}$.
2. For each gcd d listed in the previous problem, find a number $a \in \mathbb{Z}_{20}$ such that $\gcd(a, 20) = d$.
3. Write down the nontrivial subgroups of $\mathbb{Z}_{20}$.
4. The list of subgroups from Problem 3 is *almost* complete. What one do we still need?

The activity above shows us that the nontrivial subgroups of $\mathbb{Z}_n$ are the ones generated by the divisors of n in $\mathbb{Z}_n$. We automatically get a similar statement for general finite cyclic groups:

Theorem 7.3.8. *The distinct subgroups of $G = \langle g \rangle$, where $|g| = n$, are $\langle e \rangle$ and the ones generated by g^k, where k is a divisor of n (other than n itself).*

The situation for infinite cyclic groups is a little different, and is explored in Exercise 10.

The main theme of this chapter is that the classification theorem (Theorem 7.1.3) allows us to obtain a complete analysis of cyclic groups by reducing our investigations to familiar integer arithmetic. This is abstract algebra at its best.

7.4 Exercises

1. (a) Find the order of each element in $\mathbb{Z}_{12}$.
   (b) Write down all the subgroups of $\mathbb{Z}_{12}$.
2. Let G be a cyclic group generated by g, where $|g| = 15$.
   (a) Find the order of each element in G.
   (b) Write down all the subgroups of G.
3. (a) If g is a generator of a group G, how are $|g|$ and $|G|$ related?
   (b) Use part (a) and Theorem 7.2.3 to find the generators of $\mathbb{Z}_{18}$.
   (c) Suppose G is a cyclic group of order 18 generated by g. Use part (b) to determine the generators of G. (Remember that your generators are elements of G and thus should all have the form g^k for various integers k.)
4. **Prove** that if $a \in \mathbb{Z}_n$ and a and n are relatively prime, then a is a generator of $\mathbb{Z}_n$. (Hint: Use Theorem 7.2.3 and Statement 7.1.)

5. Given that $U(49)$ is a cyclic group of order 42, use the previous exercise to determine how many generators $U(49)$ has.

6. **Prove** that any infinite cyclic group is isomorphic to $\mathbb{Z}$.

7. Let i denote the imaginary number $\sqrt{-1}$. Consider the subgroup $\langle i \rangle$ of $\mathbb{C}^*$ (the group of nonzero numbers with respect to multiplication) generated by i. To what familiar group is $\langle i \rangle$ isomorphic?

8. (a) Show that $U(18)$ is cyclic. State the order of this group as well as a generator.

   (b) State the other generators of $U(18)$ without actually testing any of them as generators.

   (c) Find the distinct cyclic subgroups of $U(18)$.

9. **Prove** that if G is a group of order p, where p is a prime number, then $G \cong \mathbb{Z}_p$. (Hint: Use Corollary 4.4.6.)

10. Can two elements of an infinite cyclic group ever generate the same subgroup? First investigate what happens in $\mathbb{Z}$, and then translate your answer to the setting of an abstract infinite cyclic group.

11. Activity 7.3.5 and Theorem 7.3.6 together state that two elements of $\mathbb{Z}_n$ generate the same subgroup of $\mathbb{Z}_n$ if and only if they have the same order. Show by example that this is not necessarily true when $\mathbb{Z}_n$ is replaced by a non-cyclic group.

12. We know that *every* cyclic group has the property that all of its subgroups are cyclic. Some non-cyclic groups also have the property that every subgroup (except the full group itself) is cyclic. Give an example of such a non-cyclic group. (Hint: Try a group whose order is a product of distinct prime numbers.)

13. In Exercise 3 in Chapter 4, you proved that if H and K are subgroups of a group G, then $H \cap K$ must be a subgroup of G. This implies that for $a, b \in \mathbb{Z}_n$, $\langle a \rangle \cap \langle b \rangle$ is a subgroup of $\mathbb{Z}_n$. But by Theorem 7.3.2, the subgroup $\langle a \rangle \cap \langle b \rangle$ must be cyclic itself, so $\langle a \rangle \cap \langle b \rangle = \langle c \rangle$ for some $c \in \mathbb{Z}_n$. Make a conjecture about how this element c is related to a and b by finding a generator of the subgroup $\langle 9 \rangle \cap \langle 15 \rangle$ in $\mathbb{Z}_{135}$.

14. Suppose G is a cyclic group whose only subgroups are itself, $\{e\}$, and a subgroup of order 17. What is the order of G?

15. Explain why the converse of Lagrange's Theorem holds for finite cyclic groups. In other words, explain why it is that if G is a cyclic group of order n and if k is a divisor of n, then G has a subgroup of order k. (Hint: Remember that you can translate this to a question about $\mathbb{Z}_n$.)

16. Suppose G is a cyclic group of order 50 with generator g. List all of the elements of G of order 10.

17. Give an example of a group that has exactly 5 subgroups, including itself and $\{e\}$. Then generalize to exactly n subgroups for any natural number n.

18. Let H be the subset of $GL_2(\mathbb{R})$ consisting of all matrices of the form

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

where n is any integer.

(a) Show that H is a subgroup of $GL_2(\mathbb{R})$.

(b) Show that H is cyclic.

Chapter 8

Direct Products of Groups

In Activity 1.1.1 from Chapter 1, we showed that the symmetry group of a non-square rectangle is $\{R_0, R_{180}, H, V\}$ (where the notation is the same we use for the dihedral group D_4). This group is often called the *Klein 4-group* after Felix Klein. We'll refer to it as V_4. (The German word for "four" is *vier*.)

Activity 8.0.1.

1. Construct the Cayley table for V_4.
2. Show that V_4 is Abelian but not cyclic.
3. Let $L = \{R_0, R_{180}\}$ and $M = \{R_0, H\}$. Show that L and M are both cyclic subgroups of V_4.
4. Show that every element of V_4 can be written as a product of an element of L and an element of M *in a unique way.*

The above activity says that, in a sense we'll soon make clear, V_4 can be "built up from" the subgroups L and M. This is a special case of a very important theorem in group theory, which says that every finite Abelian group can be "built up from" cyclic groups. This chapter is devoted to this notion of "building up" one group from others.

8.1 Definition and Properties

In linear algebra, you saw how to add vectors in $\mathbb{R}^2$. The sum of two such vectors, (a_1, a_2) and (b_1, b_2), is the vector obtained by coordinate-wise addition: $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$. The set $\mathbb{R}^2$ equipped with component-wise addition is an example of a *direct product* of two groups, defined in general

below:

Definition 8.1.1. Let G_1 be a group with a binary operation $*$, and let G_2 be a group with a binary operation $\bullet$. The **direct product** of G_1 and G_2 is the set $\{(g_1, g_2) : g_1 \in G_1 \text{ and } g_2 \in G_2\}$. This set is denoted $G_1 \oplus G_2$. The **component-wise** operation on $G_1 \oplus G_2$ is the one defined by $(g_1, g_2) \cdot (h_1, h_2) = (g_1 * h_1, g_2 \bullet h_2)$. The groups G_1 and G_2 are called the **components** of $G_1 \oplus G_2$.

You should be able to guess what's coming:

Theorem 8.1.2. *The direct product of two groups is a group with respect to the component-wise operation.*

The way to "build up" a group from other groups mentioned above is to form their direct product. In Exercise 3, you will show that, using the notation of Activity 8.0.1, $V_4 \cong L \oplus M$.

Activity 8.1.3. Prove Theorem 8.1.2 by checking the four group axioms.

Given our background, there would be lots of questions to ask at this point: If G_1 and G_2 are Abelian, must $G_1 \oplus G_2$ be Abelian? If G_1 and G_2 are cyclic, must $G_1 \oplus G_2$ be cyclic? What is the order of $G_1 \oplus G_2$? What are the orders of the elements of $G_1 \oplus G_2$? How do you work with isomorphisms involving direct products?

We'll answer the order questions here, the cyclic question in the next section, and the others in the exercises. The order of a direct product $G_1 \oplus G_2$ is, as usual, the number of elements in $G_1 \oplus G_2$. We'll see a quick way to compute this after the next activity.

Recall that the order of a group element g is the smallest natural number n such that $g^n = e$. The order of a group element (g_1, g_2) in $G_1 \oplus G_2$ is defined the same way: just replace g with (g_1, g_2) and e with the identity element in $G_1 \oplus G_2$, which we saw above was (e_1, e_2), where e_1 is the identity in G_1 and e_2 is the identity in G_2. Thus, $|(g_1, g_2)|$ is the smallest natural number n such that $(g_1, g_2)^n = (e_1, e_2)$. And how does $(g_1, g_2)^n$ work? Well, by definition, $(g_1, g_2)^n$ is the product of n copies of (g_1, g_2). Since the group operation in $G_1 \oplus G_2$ is component-wise, $(g_1, g_2)^n$ is therefore the same as (g_1^n, g_2^n).

Activity 8.1.4. In this activity, we'll find the order of the group $\mathbb{Z}_3 \oplus U(5)$ as well as the orders of each of its elements.

1. The order of $\mathbb{Z}_3 \oplus U(5)$ is the number of elements it contains. In this case, it would be the number of ordered pairs where the first coordinate is an element of $\mathbb{Z}_3$ and the second is an element of $U(5)$. Write down all such ordered pairs.

Activity 8.1.4. (continued)

2. What is the order of $\mathbb{Z}_3 \oplus U(5)$? How might you have predicted this without writing down all of the elements?

3. Explain why it is that the order of an element (a, b) in $\mathbb{Z}_3 \oplus U(5)$ is the smallest positive integer n such that both $na = 0$ and $b^n = 1$.

3. Use Problem 3 to start finding the orders of the elements of $\mathbb{Z}_3 \oplus U(5)$. Stop when you see what's really going on.

4. Use the pattern you noticed in Problem 4 to find the orders of the rest of the elements of $\mathbb{Z}_3 \oplus U(5)$.

This example reveals a few structural properties of direct products that hold in general.

Theorem 8.1.5. *For finite groups G_1 and G_2, the order of the direct product $G_1 \oplus G_2$ is $|G_1| \cdot |G_2|$. If either of G_1 or G_2 is infinite, then so is $G_1 \oplus G_2$.*

Theorem 8.1.6. *For an element a of finite order in a group G_1 and an element b of finite order in a group G_2, the order of the element (a, b) in $G_1 \oplus G_2$ is $\text{lcm}(|a|, |b|)$. If either of $|a|$ or $|b|$ is infinite, then so is $|(a, b)|$.*

Sometimes in linear algebra, you considered the vector space $\mathbb{R}^3$, which would be the direct product of *three* copies of $\mathbb{R}$. We can generalize this three-component version of direct products to any finite number of groups as well. We first need a sort of associative property for the component groups of direct products.

Theorem 8.1.7. *Let G_1, G_2, and G_3 be groups. Then*

$$(G_1 \oplus G_2) \oplus G_3 \cong G_1 \oplus (G_2 \oplus G_3).$$

Proof. We need an isomorphism $\phi : (G_1 \oplus G_2) \oplus G_3 \to G_1 \oplus (G_2 \oplus G_3)$. The most obvious way to define ϕ is by $\phi((g_1, g_2), g_3) = (g_1, (g_2, g_3))$. You will prove in Exercise 9 that ϕ is an isomorphism. □

The practical purpose of Theorem 8.1.7 is that it tells us that we can form direct products in which one of the components is a direct product itself and that the way we group adjacent components together does not matter. Since it doesn't matter where we put the parentheses in $(G_1 \oplus G_2) \oplus G_3$ or $G_1 \oplus (G_2 \oplus G_3)$, we might as well just denote this direct product as $G_1 \oplus G_2 \oplus G_3$.

Activity 8.1.8. Now that We have a way to define the direct product $G_1 \oplus G_2 \oplus G_3$ of three groups, how do you think you would define the direct product $G_1 \oplus G_2 \oplus G_3 \oplus G_4$ of four groups? What if you want to define the direct product of 17 groups?

The above activity indicates that for any positive integer n, we can inductively form the direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of n groups. The elements of such a direct product are the ordered n-tuples of the form $(g_1, g_2, \ldots, g_n)$, where each $g_i \in G_i$.

Activity 8.1.9. Use a proof by induction to prove that for any positive integer n, Theorems 8.1.5 and 8.1.6 generalize to direct products of n groups. In other words, prove that

$$|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1| \cdot |G_2| \cdot \cdots \cdot |G_n|$$

and

$$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|).$$

The following theorem shows that direct products possess a sort of commutative property on their component groups as well. We'll need this in the next few sections.

Theorem 8.1.10. *For groups G_1 and G_2, $G_1 \oplus G_2 \cong G_2 \oplus G_1$.*

You will prove the above theorem in Exercise 10.

We will also need a description of what the subgroups of direct products look like.

Theorem 8.1.11. *Suppose $G_1, G_2, \ldots, G_n$ are groups and that H_i is a subgroup of G_i for each i such that $1 \leq i \leq n$. Then $H_1 \oplus H_2 \oplus \cdots \oplus H_n$ is a subgroup of $G_1 \oplus G_2 \oplus \cdots \oplus G_n$.*

Activity 8.1.12. Prove Theorem 8.1.11 using the Subgroup Test.

8.2 Direct Products of Cyclic Groups

In the next section, we'll see the famous theorem that says every finite Abelian group is (isomorphic to) a direct product of cyclic groups. To use this theorem, though, we first have to answer the question: When is the direct product of cyclic groups itself cyclic? We'll only discuss *finite* cyclic groups in this section, which means, as usual, that we can state our question even more specifically: When is $\mathbb{Z}_m \oplus \mathbb{Z}_n$ cyclic?

Activity 8.2.1.

1. Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is not cyclic.
2. Show that $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ is cyclic. To what familiar group must $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ therefore be isomorphic?

(For these two problems, it would be easiest to show that the given direct products either do not or do contain an element with the same order as that of the whole group.)

The activity above hints at the following theorem:

Theorem 8.2.2. *For natural numbers m and n, $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.*

Activity 8.2.3. To prove Theorem 8.2.2, we need to show that $\mathbb{Z}_m \oplus \mathbb{Z}_n$ has a generator (which would have to be an ordered pair (a, b) with $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$) if and only if $\gcd(m, n) = 1$.

1. Suppose a is not a generator of $\mathbb{Z}_m$ or b is not a generator of $\mathbb{Z}_m$. Show that the order of (a, b) as an element of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is less than mn. What can you thus conclude about (a, b)?
2. Explain why the previous problem shows that the only possible candidates for generators of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ are ordered pairs (a, b) where both $|a| = m$ and $|b| = n$.
3. Suppose (a, b) is an ordered pair in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ with $|a| = m$ and $|b| = n$. Prove that if $\gcd(m, n) = 1$, then $|(a, b)| = mn$. Conclude that $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic.
4. Suppose again that (a, b) is an ordered pair in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ with $|a| = m$ and $|b| = n$. Prove that if $\gcd(m, n) > 1$, then $|(a, b)| < mn$. (Use Statement 7.1.) Conclude that $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is not cyclic.
5. Explain why the outcome of the previous problem is equivalent to saying that if $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic, then $\gcd(m, n) = 1$.

For example, $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{20}$, but $\mathbb{Z}_4 \oplus \mathbb{Z}_6 \ncong \mathbb{Z}_{24}$. We can also use Theorem 8.2.2 to simplify direct products of cyclic groups, as seen in the following activities.

Activity 8.2.4. Use the isomorphism from Theorem 8.2.2 to find a simpler looking isomorphic version of the direct product

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{11}.$$

(You can use Theorems 8.1.7 and 8.1.10 to rearrange and reassociate the components of the above direct product.)

In the above activity, notice that we were able to express the direct product as a direct product of cyclic groups in which each subscript (except for the first one) divides the one that precedes it. This can always be done, but we might have to first decompose some of the component groups first using Theorem 8.2.2 in reverse, as in the next activity.

Activity 8.2.5. Express the direct product

$$\mathbb{Z}_6 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{60}$$

as a direct product of cyclic groups in which each subscript except the first one divides the one that precedes it.

(Start by decomposing each component group using Theorem 8.2.2. For example, starting with $\mathbb{Z}_6$, we factor the subscript 6 into factors which are relatively prime to each other: $6 = 2 \times 3$. By Theorem 8.2.2, we know then that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ since 2 and 3 are relatively prime. Now do the same for the other components.)

8.3 Classification of Finite Abelian Groups

Activity 8.3.1. In this activity, we will practice factoring a given number into a product of powers of prime numbers in as many ways as possible. For example, we can factor 40 in this way as: 5×8, $5 \times 4 \times 2$, and $5 \times 2 \times 2 \times 2$. (Notice that 10×4, for example, is missing since 10 is not the power of a prime number.) Do the same for each of the following numbers:

1. 81
2. 24
3. 200

Activity 8.3.2. Each of the factorizations in the previous activity corresponds to a direct product of cyclic groups. For example, the three stated factorizations of 40 correspond to $\mathbb{Z}_5 \oplus \mathbb{Z}_8$, $\mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$, and $\mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Verify that no two of the direct products just listed are isomorphic to each other.

Activity 8.3.3. Use your factorizations from Activity 8.3.1 to write down the corresponding direct products of cyclic groups.

8.3.1 The Classification Theorem

Activities 8.3.1, 8.3.2, and 8.3.3 illustrate a method for finding several Abelian groups of a given order. The following theorem, the promised classification of finite Abelian groups, states that this method is guaranteed to produce *all* of the Abelian groups of that given order.

Theorem 8.3.4 (Classification of Finite Abelian Groups)**.** *Suppose G is a finite Abelian group. Then G is isomorphic to a direct product of the form*

$$\mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}},$$

where $p_1, p_2, \ldots, p_n$ are prime numbers and $k_1, k_2, \ldots, k_n$ are natural numbers. The subscripts $p_1^{k_1}, p_2^{k_2}, \ldots, p_n^{k_n}$ are uniquely determined by G and are not necessarily distinct from each other.

Though we have all the tools to do so, we won't prove this theorem here because the proof is pretty long. It would be easy to find online if you're interested.

Classification theorems are a big deal in abstract algebra, and we've seen a few already on a much smaller scale: In Chapter 2, we classified all the groups of orders 1, 2, and 3 – up to isomorphism, there's only one of each of these. In Exercise 5 in Chapter 2, you classified all the groups of order 4, finding that there are two of them. Theorem 7.1.3 provides a classification of all cyclic groups – each one is isomorphic either to a $\mathbb{Z}_n$ or $\mathbb{Z}$. In Exercise 9 in Chapter 7, you classified the groups of prime order – for each prime p, the only group (up to isomorphism) of order p is $\mathbb{Z}_p$.

Using the classification theorem, we can write down all of the Abelian groups (up to isomorphism) of any given finite order. In Activities 8.3.1, 8.3.2, and 8.3.3, according to the classification theorem, we found every Abelian group of orders 40, 81, 24, and 200.

As we saw in Activity 8.2.5, we can always show that a direct product of cyclic groups is isomorphic to one in which each subscript (except the first one) divides the preceding subscript. A direct product written in this way is said to be in *standard form*.

Example 8.3.5. We've seen that the three Abelian groups of order 40 are $\mathbb{Z}_5 \oplus \mathbb{Z}_8$, $\mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$, and $\mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Let's write these in standard form.

By Theorem 8.2.2, any time two subscripts are relatively prime, we can "combine" the two components into one. So since 5 and 8 are relatively prime, $\mathbb{Z}_5 \oplus \mathbb{Z}_8 \cong \mathbb{Z}_{40}$.

In the direct product $\mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$, 5 is relatively prime to both 4 and 2. Pairing 5 with 4 rather than 2 (because it's larger) and combining the corresponding components gives $\mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_{20} \oplus \mathbb{Z}_2$.

Likewise, since 5 and 2 are relatively prime, $\mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Thus, the three Abelian groups of order 40, written in standard form are $\mathbb{Z}_{40}$, $\mathbb{Z}_{20} \oplus \mathbb{Z}_2$, and $\mathbb{Z}_{10} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Activity 8.3.6. Express all of the Abelian groups of orders 81, 24, and 200 in standard form.

Activity 8.3.7. Find all of the Abelian groups of order 360, and write them in standard form. (You'll have to first find all the ways to factor 360 into a product of powers of prime numbers.)

8.3.2 Consequences of the Classification Theorem

The Classification of Finite Abelian Groups has several consequences, two of which we will state here. We'll provide examples that help to show why they're true rather than full proofs.

Recall Lagrange's Theorem, which says that if G is a finite group, and H is a subgroup of G, then $|H|$ mus divide $|G|$. The converse of Lagrange's Theorem is not always true: If n divides $|G|$, then G is not required to have a subgroup of order n. As stated in Chapter 5, a counterexample is the group A_4. This group has order 12, but it has no subgroup of order 6.

Sometimes the converse to Lagrange's Theorem does hold, though. For example, in Exercise 15 in Chapter 7, you showed that if G is a finite *cyclic* group, then G has a subgroup of every order which is a divisor of $|G|$.

In light of the classification theorem and Exercise 15 in Chapter 7, it turns

out that the converse of Lagrange's Theorem *does* hold for all finite Abelian groups as well.

Theorem 8.3.8. *Let G be a finite Abelian group. If m is a natural number which divides $|G|$, then G contains a subgroup of order m.*

Activity 8.3.9. We'll get a feel for why the above theorem is true by working through some examples. By the classification theorem, we can assume G is the direct product of cyclic groups of prime power order.

1. Suppose G has just one component, for example, $G = \mathbb{Z}_{125}$. Find an element of G of order 5. Then state a subgroup of G of order 5.
2. Suppose now that G has two components, let's say $G = \mathbb{Z}_{16} \oplus \mathbb{Z}_{27}$. This is a group of order $16 \times 27 = 432$, which has 24 as a divisor. Find a subgroup of G of order 24. (By Theorem 8.1.11, if you can find a subgroup H_1 of $\mathbb{Z}_{16}$ and a subgroup H_2 of $\mathbb{Z}_{27}$ such that $|H_1| \cdot |H_2| = 24$, then $H_1 \oplus H_2$ will be a subgroup of G of order 24.)
3. Suppose $G = \mathbb{Z}_{25} \oplus \mathbb{Z}_{343} \oplus \mathbb{Z}_{121}$, which has order 1,037,575. A divisor of 1,037,575 is 2695. Find a subgroup of G of order 2695. (Use the method from the previous problem.)
4. Explain a general technique for carrying out this process for any direct product of cyclic groups and any divisor of the group's order.

Another consequence of the classification theorem was alluded to in Chapter 6 when we stated the following, which we can now justify:

Theorem 8.3.10. *Suppose G and H are finite Abelian groups of the same order. If the list of the orders of the elements of G is the same as that for H, then $G \cong H$.*

"Proof". The idea is to address the contrapositive of the theorem statement: Assuming that G and H are finite Abelian groups of the same order, if $G \ncong H$, then the list of element orders of G and H are not identical.

We will work through an example to give a sense for why this is true. By the classification theorem, we can assume that G and H are both direct products of cyclic groups. It will also help to assume that both of these direct products are written in standard form.

Supposing that G and H are not isomorphic, their component groups must be different. Let's suppose

$$G = \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$$

and

$$H = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

(These are both Abelian groups of order 32.)

We will show a systematic way to detect a difference in the lists of element orders. Begin by finding the first component at which the two groups differ: The first component is the same, but the second components ($\mathbb{Z}_4$ for G and $\mathbb{Z}_2$ for H) are different. The larger of these two components has an element of order 4, whereas the smaller does not. The claim is that G must contain more elements of order 4 than H does.

The order of an element $(a, b, c, d) \in H$ is $\text{lcm}(|a|, |b|, |c|, |d|)$. Since b, c, and d are in $\mathbb{Z}_2$ and $|\mathbb{Z}_2|$ divides but is less than $|\mathbb{Z}_4|$, $|b|$, $|c|$, and $|d|$ must divide but be less than $|\mathbb{Z}_4| = 4$. Thus, the only way for the order of (a, b, c, d) to be 4 would be for $|a|$ to be 4. This is the case when $a = 1$ and $a = 3$. We thus have that the number of element of order 4 in H is equal to the number of elements of $\mathbb{Z}_4$ that have order 4 times the number of elements $(b, c, d) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The total count is $2 \times 8 = 16$.

How many elements of order 4 are there in G? We can start the same way: Take all elements of the form (a, b, c), where $|a| = 4$. Since $|b|$ and $|c|$ must both divide 4, then (b, c) can be any of the $4 \times 2 = 8$ elements of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. This produces $2 \times 8 = 16$ elements of order 4 so far.

However, in G, $|b|$ can possibly equal 4 unlike the orders of b, c, and d in H. Thus, a does not necessarily have to have order 4 in order for (a, b, c) to have order 4. We then get at least one more element of order 4 in G, namely $(0, 1, 0)$. Therefore G contains more elements of order 4 than H does, so their lists of element orders cannot be identical. □

Activity 8.3.11. For the record, it *is* possible for two non-isomorphic groups to have the same order and lists of element orders; they just can't both be Abelian. For example, let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and let H be the subgroup of $GL_3(\mathbb{Z}_3)$ consisting of matrices of the form

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

1. Prove that H is a subgroup of $GL_3(\mathbb{Z}_3)$.
2. Show that H is non-Abelian, and comclude that $G \ncong H$.
3. Show that G and H both have order 27.
4. Explain why, for both G and H, every element except the identity must have order 3. Conclude that the groups' lists of element orders are identical.

The classification theorem makes it easy (if somewhat tedious) to find all of the Abelian groups of any given order. You could write a short computer program to do it. Finding the *non*-Abelian groups of a given order is a very different story. There is no classification theorem which gives a systematic way to find these as there is for Abelian groups. For some orders, non-Abelian groups can be very numerous – there are 12 non-Abelian groups of order 24, for example – and for other orders, there are none – there are no non-Abelian groups of order 15, for example. We'll return to classification theorems in Chapter 10 when we briefly discuss the even more famous classification of finite *simple* groups.

8.4 Exercises

1. Is the direct product of two infinite cyclic groups cyclic? (Hint: Remember that you can translate this question to one about $\mathbb{Z} \oplus \mathbb{Z}$.)

2. **Prove** that the direct product $G_1 \oplus G_2$ is Abelian if and only if both component groups G_1 and G_2 are Abelian.

3. **Prove** that, using the notation of Activity 8.0.1, $V_4 \cong L \oplus M$. (Hint: Since V_4 and $L \oplus M$ are small groups, it might be easiest to just compare their Cayley tables.)

4. Find the order of the group $\mathbb{Z}_2 \oplus S_3$ as well as the order of each of its elements.

5. Give an example of a subgroup of $D_4 \oplus S_4$.

6. Is $\mathbb{Z}_5 \oplus \mathbb{Z}_6$ cyclic? How about $\mathbb{Z}_5 \oplus \mathbb{Z}_{10}$? Explain your answers. If either group is cyclic, state which Z_n it's isomorphic to.

7. Express the direct product $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{11} \oplus \mathbb{Z}_{11}$ in standard form.

8. Express the direct product $\mathbb{Z}_4 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{18}$ in standard form.

9. **Prove** that the function ϕ in the proof of Theorem 8.1.7 is an isomorphism.

10. **Prove** Theorem 8.1.10.

11. Give a complete classification (up to isomorphism) of all Abelian groups of order less than or equal to 12.

12. Find all Abelian groups (up to isomorphism) of order 625.

13. Find all Abelian groups (up to isomorphism) of order 77,077.

14. What is the order of the Abelian group $U(40)$? Find a direct product of cyclic groups which is isomorphic to $U(40)$. (Hint: There will be several possibilities. Narrow them down by finding the orders of the elements in $U(40)$.)

15. Find a subgroup of order 50 of the group $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4$.

16. **Prove** that the group $M_{2\times 2}(\mathbb{R})$ is isomorphic to $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$.

17. Suppose p and q are distinct primes. Up to isomorphism, how many Abelian groups of order pq are there?

Chapter 9

Quotient Groups, Part 1

In Exercise 10a in Chapter 1, we considered the symmetry group of a circle. Focusing just on the rotational symmetries for now, we can say that for every real number θ, a rotation of the circle through θ degrees is a symmetry. Before we say, though, that the rotation group of a circle is isomorphic to $\mathbb{R}$, we have to remember that different real numbers can determine the same rotation of a circle. For example, a counterclockwise rotation of the circle through 10° is the same as one though 370° or 730° or a clockwise rotation (represented by a negative angle) of -350°. In this context, we'd want the real numbers 10, 370, 730, -350, and any of the other infinitely many real numbers that differ from 10 by a multiple of 360 to be identified together as one entity that we think of as a single rotation of a circle. The specific numbers 10, 370, etc, would just be possible names for this entity.

So it seems that it's actually the case that the rotation group of the circle is the group $\mathbb{R}$, but with angles that differ by a multiple of 360° identified together. The way to carry out the process of starting with a group and identifying its elements together in a certain way is to form a *quotient group*. Quotient groups are the subject of this and the next chapter.

9.1 Cosets and Their Properties

We introduced cosets in Chapter 4 in order to prove Lagrange's Theorem, but they turn out to be exactly what we need to achieve the identification process mentioned above.

We should review some of the basics of cosets. Let G be any group, and let H be a subgroup of G. Let a be an element of G. The **left coset** of H in G represented by a is the set $\{ah : h \in H\}$. It's denoted by aH. We should think of aH as the set obtained by multiplying all of the elements of H by a on the

left. If G is an additive group, then the left coset of H represented by a is the set $\{a + h : h \in H\}$, which we instead denote by $a + H$.

Though we didn't need them in Chapter 4, we can also define the **right coset** of H in G represented by a to be the set $\{ha : h \in H\}$, denoted by Ha. (We make the obvious adjustments when G is additive.) It's certainly not always the case that the left and right cosets coincide for the same representative, although as we'll see, they sometimes do.

We proved the following facts in Chapter 4 for left cosets, but they hold for right cosets as well:

- If G is a finite group, then any two cosets of H in G have the same number of elements. (Lemma 4.4.11)
- Every element of G is in a coset of H. (Lemma 4.4.12)
- Two distinct cosets have no elements in common. (Lemma 4.4.13)

These properties make it easier to find all of the cosets of a given subgroup in a given group. The set of cosets of H in G is denoted G/H. (This is read aloud as "G mod H". The use of the word "mod" is not a coincidence as we'll eventually see.) It will have to be made clear from the context whether G/H is referring to the set of left or right cosets.

Activity 9.1.1. For each of the following groups G and subgroups H, find G/H using left cosets as well as G/H using right cosets.

1. $G = \mathbb{Z}$, $H = 4\mathbb{Z}$ (the subgroup of integer multiples of 4)
2. $G = S_3$, $H = \{(1), (1\,2)\}$
3. $G = D_4$, $K = \{R_0, R_{180}\}$ (We're using K for the subgroup name rather than H to avoid confusion with the element $H \in D_4$.)
4. $G = S_4$, $H = A_4$

Activity 9.1.2. Explain why the cosets in $\mathbb{R}/360\mathbb{Z}$ are in one-to-one correspondence with the rotations of a circle.

The following is another property of cosets that will be exceedingly important. It's stated and proved here for left cosets, but it's also true for right cosets and the proof is almost identical.

Theorem 9.1.3. *Let G be a group and H a subgroup of G. For two elements a and b of G, $aH = bH$ if and only if $b^{-1}a \in H$.*

Proof. This is an "if and only if" statement, so we'll begin by assuming that $aH = bH$ and prove that $b^{-1}a \in H$.

First, notice that $a \in aH$. This is because H is a subgroup and thus contains e, the identity of G. Therefore, $ae \in aH$, but since $ae = a$, we have $a \in aH$.

Second, since $a \in aH$ and $aH = bH$, we have that $a \in bH$. This means that $a = bh$ for some $h \in H$. Multiplying this equation on both sides on the left by b^{-1}, we get $b^{-1}a = h$, and thus $b^{-1}a \in H$.

Now we'll assume that $b^{-1}a \in H$ and prove that $aH = bH$. Since we need to prove that the sets aH and bH are equal, we'll use a set equality proof.

Let x be an arbitrary element of aH. Then $x = ah$ for some $h \in H$. Multiplying both sides of this equation on the left by b^{-1}, we get $b^{-1}x = (b^{-1}a)h$. We're assuming that $b^{-1}a \in H$ and since H is closed, we thus know that $(b^{-1}a)h \in H$, and hence also, $b^{-1}x \in H$. We can say then that $b^{-1}x = h_0$ for some $h_0 \in H$, or equivalently, $x = bh_0$. This shows that $x \in bH$, and therefore, $aH \subseteq bH$.

The proof that $bH \subseteq aH$ is nearly identical, so we can conclude that $aH = bH$. □

An easy, but useful, corollary is:

Corollary 9.1.4. *For a group G and a subgroup H, $hH = H$ if and only if $h \in H$.*

Activity 9.1.5. Use Theorem 9.1.3 to prove Corollary 9.1.4.

A helpful way to view this corollary is to say that subgroups "absorb" their own elements. In other words, if you're representing a coset of a subgroup H by an element that's already in H, you always have the option of replacing that representative by the identity element.

9.2 Coset Multiplication

In Activity 9.1.2, we saw that the elements of the set $\mathbb{R}/360\mathbb{Z}$ are in one-to-one correspondence with the elements of the rotation group of the circle. But does $\mathbb{R}/360\mathbb{Z}$ actually have a binary operation that makes it into a group? And if so, would $\mathbb{R}/360\mathbb{Z}$ and the rotation group of the circle be isomorphic as groups? In this section, we will define a natural way to "multiply" cosets and see that there are sometimes unavoidable problems in trying to do so.

The definition of the binary operation on cosets can be motivated by the cosets in $\mathbb{R}/360\mathbb{Z}$. Suppose we have two such cosets: $227+360\mathbb{Z}$ and $301.5+360\mathbb{Z}$. Remember that $227 + 360\mathbb{Z}$ is the infinite set of all real numbers that differ from 227 by an integer multiple of 360, and $301.5 + 360\mathbb{Z}$ is the infinite set of all real numbers that differ from 301.5 by an integer multiple of 360. What would be

the most natural way to define $(227 + 360\mathbb{Z}) + (301.5 + 360\mathbb{Z})$? (We're using additive notation because the "parent group" $\mathbb{R}$ is additive.)

Since we'd like to think of each of these cosets as a single rotation of the circle (each with infinitely many possible names), then we should combine them the same way we would compose two rotational symmetries: by adding the angles. Thus, it would make sense to define $(227 + 360\mathbb{Z}) + (301.5 + 360\mathbb{Z})$ to be the coset $(227+301.5)+360\mathbb{Z}$, which equals $528.5+360\mathbb{Z}$. If we wanted to, we could even replace the representative of 528.5 with any number which differs from it by a multiple of 360, such as 168.5. We could thus say that

$$(227 + 360\mathbb{Z}) + (301.5 + 360\mathbb{Z}) = 168.5 + 360\mathbb{Z}.$$

In general, we will define coset multiplication this way: Choose a representative of each coset and let the product of the two cosets be the coset represented by the product of the representatives. Symbolically, for two left cosets aH and bH, we let

$$(aH) \cdot (bH) = (ab)H,$$

and we define the operation for right cosets in the same way:

$$(Ha) \cdot (Hb) = H(ab).$$

WARNING: We have *not* yet proved that the set of cosets G/H is a group. For now, it's only a set with a binary operation.

Activity 9.2.1. Let $G = D_4$ and $K = \{R_0, R_{90}, R_{180}, R_{270}\}$. (As usual, we're using K as the name of the subgroup rather than H to avoid confusion with the element $H \in D_4$.)

1. Verify that K is a subgroup of G.
2. Determine G/K using left cosets.
3. Multiply the two cosets in G/K by each other.
4. Repeat the previous problem, choosing different representatives for your cosets. Do you get the same result?
5. Repeat Problem 3 again with different representatives. Do you still get the same result?
6. Would you guess that you will *always* get the same result, regardless of the representatives you choose?

Activity 9.2.2. Repeat the previous activity with the following groups and subgroups:

1. $G = U(32)$, $H = \{1, 17\}$
2. $G = S_3$, $H = \{(1), (1\,2)\}$ (You considered this example in Activity 9.1.1.)

In Problem 2 in the above activity, we encountered a situation where the results of our coset multiplication depended on the representatives we chose. We know that a coset is considered to be the same regardless of the choice of representative used to denote it, so coset multiplication should *not* depend on the representative choice, either. When coset multiplication *does* depend on the representative choices (as in Problem 2), we say that the operation is not **well-defined**.

Well-definedness is necessary when studying algebraic structures and is an issue with any operation on objects that can be represented in more than one way. For example, the real number 0.5 can be represented in infinitely many different ways, such as $\frac{1}{2}$, $\frac{2}{4}$, $\frac{-15.6}{-31.2}$, etc. The same is true for 0.25, which can be represented as $\frac{1}{4}$, $\frac{10}{40}$, $\frac{\pi}{4\pi}$, etc. But no matter how we represent 0.5 and 0.25 as fractions, when we add them, we *always* get a fraction which represents 0.75. Addition in $\mathbb{Q}$ is well-defined.

So what do we do with coset multiplication? Sometimes it's well-defined and sometimes it's not. Instead of just throwing it all out as worthless since it sometimes doesn't work, it would be better to find out *why* it's not working and to establish a criterion that, if satisfied, will guarantee that it *does* work. We'll do this in the next section. Then after we clear up the well-definedness issue, we'll finally be able to address the question about a set of cosets G/H being a group.

9.3 Normal Subgroups

For a group G and a subgroup H, recall the way we're defining coset multiplication in G/H (using left cosets): (1) Pick a representative of each coset, (2) multiply them in G, and (3) report the product of the two cosets to be the coset containing the result from Step (2). Symbolically, this amounts to saying

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

However, we saw in Problem 2 in Activity 9.2.2 that coset multiplication defined this way is not always well-defined. For coset multiplication to be well-defined, we need to ensure that if we change the representatives of the cosets

being multiplied, then we still get the same product. (Remember that changing the representative of a coset does not actually change the coset itself, only the way it's named.)

Our goal in this section is to impose an extra condition on G and/or H that will ensure that coset multiplication in G/H is well-defined. Once this condition is in place, we will be able to show that when it's satisfied, G/H will be a group with respect to coset multiplication.

The condition we'll use is given by the following definition:

Definition 9.3.1. Let G be a group and let H be a subgroup of G. We say H is a **normal subgroup** of G provided that $aH = Ha$ for all $a \in G$. If H is a normal subgroup of G, we denote this by $H \triangleleft G$.

In other words, $H \triangleleft G$ when the left and right cosets of H coincide for all representatives.

Referring to Activity 9.1.1, the subgroups in Problems 1, 3, and 4 are normal since the left and right cosets are the same for each representative. The subgroup in Problem 2 is not. It's not a coincidence that coset multiplication in Problem 2 in Activity 9.2.2 is not well-defined as the following theorem states:

Theorem 9.3.2. *Let G be a group and let H be a subgroup of G. If H is a normal subgroup of G, then coset multiplication in G/H is well-defined.*

Activity 9.3.3. Let's see why Theorem 9.3.2 is true.

1. Suppose we want to multiply the coset aH by the coset bH. What would the product be?
2. Suppose now that we change the representative of aH to some other element of G, let's call it c. Since we're only changing the representative, the coset itself doesn't change. In other words, $aH = cH$. Suppose we also change the representative of bH to some other element d of G. Then $bH = dH$. For coset multiplication to be well-defined, what will we want to conclude about $(ab)H$ and $(cd)H$?
3. By Theorem 9.1.3, what is an equivalent way to say that $aH = cH$ and $bH = dH$?
4. By Theorem 9.1.3 again, what is an equivalent way to say $(ab)H = (cd)H$, which is what we want to conclude with? (Use the Socks-Shoes Property to simplify your answer.)

Activity 9.3.3. (continued)

5. By Problem 3, we know $c^{-1}a \in H$. Explain why $c^{-1}ab \in Hb$.
6. Explain why we can also say that $c^{-1}ab \in bH$.
7. Use the previous problem to explain why $c^{-1}ab = bh$ for some $h \in H$.
8. Now consider again the expression $d^{-1}c^{-1}ab$ which showed up in Problem 4. Remember our goal is to show that this expression is an element of H. Using the previous problem, show that $d^{-1}c^{-1}ab = d^{-1}bh$.
9. Explain why $d^{-1}bh \in H$. (Use Problem 3.)
10. Conclude that $(cd)^{-1}(ab) \in H$ and explain why we've achieved our goal from Problem 4.
11. Pinpoint the exact spot in the above argument where we used that H is normal.

We now have a condition on the subgroup H that we can check that will ensure that multiplication in G/H is well-defined. However, this can tedious to do directly, as seen in even the relatively small examples from Activity 9.1.1. If H has a lot of cosets in G, or if G and H are defined abstractly, then Definition 9.3.1 is not helpful. So we'll develop some methods for checking subgroup normality that don't require using Definition 9.3.1 directly.

Activity 9.3.4. Look again at the subgroups in Problems 1 and 4 in Activity 9.1.1. It shouldn't have been a surprise at the time that the left and right cosets coincided, or to use the right terminology, that the subgroups were normal. Why not?

The above activity leads to the following two shortcuts for detecting normal subgroups. Note that they do not always apply, but when they do, they're much easier to use than Definition 9.3.1:

1. If G is Abelian, then every subgroup of G is normal.
2. If $|H| = \frac{1}{2}|G|$, then $H \triangleleft G$.

If G is non-Abelian and $|H| \neq \frac{1}{2}|G|$, then we need a more general test for the normality of H. This is provided by the following **Normal Subgroup Test**.

Theorem 9.3.5 (Normal Subgroup Test)**.** *Let G be a group. A subgroup H is normal in G if and only if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.*

Proof. We'll begin by assuming that $H \triangleleft G$ and proving that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Since we're aiming to prove a "for every" statement, we'll fix an arbitrary $g \in G$ and an arbitrary $h \in H$ and prove that $ghg^{-1} \in H$. Since $h \in H$, $gh \in gH$. Since we're assuming $H \triangleleft G$, $gH = Hg$. Thus $gh \in Hg$. This means $gh = h_0 g$ for some $h_0 \in H$. Multiplying both sides of this equation on the right by g^{-1}, we get $ghg^{-1} = h_0$. Since $h_0 \in H$, $ghg^{-1} \in H$.

Now we'll assume that $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$ and prove that $H \triangleleft G$. We thus have to show that for an arbitrary $g \in G$, $gH = Hg$. We'll apply a set equality proof.

Let x be an arbitrary element of gH. Then $x = gh$ for some $h \in H$. This allows us to say $xg^{-1} = ghg^{-1}$. The element on the right side of this equation is assumed to be in H, so therefore, $xg^{-1} \in H$ as well. Thus $xg^{-1} = h_0$ for some $h_0 \in H$. We can rewrite this as $x = h_0 g$ and therefore conclude that $x \in Hg$. Therefore $gH \subseteq Hg$. The proof that $Hg \subseteq gH$ is very similar and is omitted.

Since $gH \subseteq Hg$ and $Hg \subseteq gH$, we have that $gH = Hg$, meaning that $H \triangleleft G$. □

The Normal Subgroup Test is an "if and only if" statement, which means that the condition given is *equivalent* to being normal. This means that it doesn't only apply in general circumstances like the two shortcuts above, but rather it can always be applied instead of the Definition 9.3.1 when convenient.

Activity 9.3.6. Recall that $GL_n(\mathbb{R})$ is the group of invertible $n \times n$ matrices with real number entries and $SL_n(\mathbb{R})$ is the subgroup of $GL_n(\mathbb{R})$ consisting of $n \times n$ matrices with real number entries with a determinant of 1. Let's show that $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$.

1. Do you think Definition 9.3.1 would be helpful here?
2. Do either of the two normal subgroup shortcuts apply?
3. Since we'll have to use the Normal Subgroup Test, let's start with an arbitrary element $A \in GL_n(\mathbb{R})$ and an arbitrary element $B \in SL_n(\mathbb{R})$. What will we have to show for A and B?
4. Recalling some of the properties of determinants listed in Section 3.2.1, what can you say about $\det(ABA^{-1})$ and $\det(A^{-1})$?
5. Use the previous problem to show that $\det(ABA^{-1}) = \det(B)$.
6. What do you know about $\det(B)$?
7. Using the previous two problems, explain why $ABA^{-1} \in SL_n(\mathbb{R})$ as desired.

9.4 Quotient Groups

We now have a condition in place that will ensure that a set of cosets G/H has a well-defined binary operation (namely that $H \triangleleft G$) and several ways to check that condition. We're finally ready to address the group structure of G/H. The following theorem is stated for left cosets, but since we'll be assuming that H is normal, we could just as well state it for right cosets (since they coincide in this case).

Theorem 9.4.1. *Let G be a group and let H be a normal subgroup of G. Then the set G/H of cosets of H in G is a group with respect to the binary operation on G/H defined by $(aH)(bH) = (ab)H$.*

Activity 9.4.2. We'll prove this theorem by verifying the four group axioms. First, notice that since $H \triangleleft G$, multiplication in G/H as defined in the statement of the theorem is well-defined by Theorem 9.3.2.

1. To check the closure axiom, fix two arbitrary cosets in G/H: aH and bH. Show that their product is in G/H.
2. To check the associative axiom, fix three arbitrary cosets in G/H: aH, bH, and cH. Explain why $(aH \cdot bH) \cdot cH = aH \cdot (bH \cdot cH)$.
3. An identity element in G/H would have to be a coset aH such that for any coset bH, $(aH)(bH) = bH$ and $(bH)(aH) = bH$. What coset aH would serve as the identity in G/H?
4. To show that every element of G/H has an inverse in G/H, fix an arbitrary coset aH in G/H. Find a coset bH such that $(aH)(bH) = eH$ and $(bH)(aH) = eH$.

Definition 9.4.3. Let G be a group and H a normal subgroup of G. The group G/H is called the **quotient group** of G by H.

Quotient groups are sometimes called **factor groups**. The word "quotient" (or "factor") and the notation G/H are appropriate since quotient groups are formed by dividing up the elements of G into equal-sized cosets of H.

Example 9.4.4. We saw in Activity 9.3.6 that $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$. Let's investigate the quotient group $GL_n(\mathbb{R})/SL_n(\mathbb{R})$.

The elements of this quotient group, of course, are cosets of $SL_n(\mathbb{R})$ in $GL_n(\mathbb{R})$. What do the cosets look like? Do the elements in the same coset share some common feature? How does coset multiplication work?

To ease the notation, we'll let G represent $GL_n(\mathbb{R})$ and H represent $SL_n(\mathbb{R})$. Let's first check whether two elements in a given coset of H have anything in common. Suppose A and B are matrices in G which are in the same coset of

H. Then the cosets AH and BH are equal. By Theorem 9.1.3, this is the same as saying

$$B^{-1}A \in H.$$

Since H consists of the matrices in G whose determinant is 1, we thus have that

$$\det(B^{-1}A) = 1.$$

By the multiplicative property of determinants, this last equation is equivalent to

$$\det(B^{-1})\det(A) = 1.$$

Since $\det(B^{-1}) = \frac{1}{\det(B)}$, we have that

$$\det(A) = \det(B).$$

Therefore, two matrices are in the same coset if and only if they have the same determinant. So for each real number d other than 0, there is a coset of H in G that consists of all matrices in G whose determinant equals d. (Remember that every matrix in G has a nonzero determinant by definition, so there is no coset consisting of matrices with determinant 0.) For example, there's a "2 coset", which consists of all the matrices of determinant 2, a "-4.5 coset", which consists of all the matrices of determinant -4.5, etc. We thus have a one-to-one correspondence between G/H and the multiplicative group $\mathbb{R}^*$ of nonzero real numbers.

What about the binary operation in G/H? What happens if we multiply the "d_1 coset" (i.e., the coset whose matrices have determinant d_1) by the "d_2 coset" (i.e., the coset whose matrices have determinant d_2)? By the definition of coset multiplication, we can do this by picking a representative of each coset, multiplying these representatives in G, and reporting our answer to be the coset containing the product of the two representatives. And importantly:

> It doesn't matter which representatives we choose since $H \triangleleft G$ and thus coset multiplication is well-defined!

This is a very big deal since we can be absolutely sure that whatever representatives we choose will cover all of our bases.

So for our representatives, we'll let A be a matrix whose determinant is d_1 and B a matrix whose determinant is d_2. Which coset does AB land in? Well, $\det(AB) = \det(A)\det(B) = d_1d_2$, so AB lands in the "d_1d_2 coset". Thus, the "d_1 coset" times the "d_2 coset" equals the "d_1d_2 coset". Therefore, not only is there a one-to-one correspondence between G/H and $\mathbb{R}^*$, but the binary operation of each group works the same way. Though we didn't carry out a full isomorphism proof in the spirit of Chapter 6, we can comfortably say that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$. In Chapter 10, we'll see the standard and rigorous way to prove that a quotient group is isomorphic to another group.

Activity 9.4.5. Why is $4\mathbb{Z}$ a normal subgroup of $\mathbb{Z}$? Construct the Cayley table for $\mathbb{Z}/4\mathbb{Z}$. What familiar group are you reminded of? (This will explain why we refer to G/H as "G mod H".)

What would you guess is true about the quotient group $\mathbb{Z}/n\mathbb{Z}$ for any positive integer n?

With a new type of group in front of us, we have all of our usual questions: When are quotient groups Abelian? When are they cyclic? How do you compute the order of a quotient group? How do you compute the orders of their elements? What do their subgroups look like? How do they interact with isomorphisms? We'll answer some of these questions here and save some as exercises.

Theorem 9.4.6. *Let G be a finite group and let H be a normal subgroup of G. Then the order of the quotient group G/H is $\frac{|G|}{|H|}$.*

Activity 9.4.7. Prove the theorem above.

Activity 9.4.8. What about the order of G/H when G is infinite?

1. Give an example of an infinite group G and a normal subgroup H such that G/H is infinite.
2. Give an example of an infinite group G and a normal subgroup H such that G/H is finite.

Now for orders of elements. Recall that the order of a group element a is the smallest natural number n such that $a^n = e$. This definition applies to elements of quotient groups (i.e., cosets) as well. Recalling that the identity element in G/H is eH, or just H, the order of an element aH of a quotient group G/H is the smallest natural number n such that $(aH)^n = H$. Here, $(aH)^n$ means the same thing it always does:

$$(aH)^n = \overbrace{(aH)(aH)\cdots(aH)}^{n \text{ copies of } aH}.$$

By the definition of coset multiplication, the right side of this equation is $(a^n)H$. We can thus say that n is the order of aH provided that it is the smallest natural number such that $(a^n)H = H$. By Corollary 9.1.4, this is equivalent to saying that $a^n \in H$. We thus have the following:

Theorem 9.4.9. *Let G be a group and let $H \triangleleft G$. The order of aH in G/H is the smallest natural number n such that $a^n \in H$.*

Activity 9.4.10. Explain why $\{1, 17\}$ is normal in $U(32)$. Then find the order of each element of $U(32)/\{1, 17\}$.

What about subgroups of quotient groups?

Activity 9.4.11. If G is a group and $H \triangleleft G$, then suppose K is a subgroup "between" H and G, meaning that H is a subgroup of K and K is a subgroup of G. Suppose further that $H \triangleleft K$.

Use the Subgroup Test to show that K/H is a subgroup of G/H.

What's not obvious is that *every* subgroup of a quotient group is formed as in the above activity. We'll state this fact here but will skip the proof:

Theorem 9.4.12. *The subgroups of the quotient group G/H are the quotient groups K/H, where K is a subgroup of G which contains H as a normal subgroup.*

Activity 9.4.13. Since the subgroups of cyclic groups are particularly easy to find, we can immediately apply the previous theorem to finding subgroups of quotient groups of cyclic groups.

1. Write down all of the subgroups of $\mathbb{Z}_{24}$.
2. Why is $\langle 8 \rangle$ a normal subgroup of $\mathbb{Z}_{24}$?
3. Use Theorem 9.4.12 to write down all of the subgroups of $\mathbb{Z}_{24}/\langle 8 \rangle$.

Example 9.4.14. We can now finally return to the example which motivated our introduction to quotient groups: the rotation group of the circle. We've seen that the rotational symmetries of the circle are in one-to-one correspondence with the cosets in $\mathbb{R}/360\mathbb{Z}$. We now know, though, that $360\mathbb{Z} \triangleleft \mathbb{R}$ since $\mathbb{R}$ is Abelian, and thus $\mathbb{R}/360\mathbb{Z}$ is a group.

We can illustrate the binary operation in $\mathbb{R}/360\mathbb{Z}$ with specific cosets and see that some of the properties of cosets automatically handle the reduction to

a smaller angle that we saw earlier:

$$\begin{aligned}(227 + 360\mathbb{Z}) + (301.5 + 360\mathbb{Z}) &= (227 + 301.5) + 360\mathbb{Z} \\ &= 528.5 + 360\mathbb{Z} \\ &= (168.5 + 360) + 360\mathbb{Z} \\ &= (168.5 + 360\mathbb{Z}) + (360 + 360\mathbb{Z}) \\ &= (168.5 + 360\mathbb{Z}) + (0 + 360\mathbb{Z}) \\ &= (168.5 + 0) + 360\mathbb{Z} \\ &= 168.5 + 360\mathbb{Z}.\end{aligned}$$

Notice that in lines 4 and 5, the coset $360 + 360\mathbb{Z}$ was replaced by $0 + 360\mathbb{Z}$. This is because 360 and 0 differ by a multiple of 360 and can thus both equally well serve as a representative for the coset. The act of replacing 360 by 0 is an example of a subgroup "absorbing" one of its own elements, as stated in Corollary 9.1.4.

We can see now that the binary operation in $\mathbb{R}/360\mathbb{Z}$ works the same way as that in the rotation group of the circle. It's intuitively clear that these two groups are isomorphic, but we'll wait till the next chapter to prove this after we develop a technique for working with isomorphisms involving quotient groups,

9.5 Exercises

1. Write the statements of Theorem 9.1.3 and its corollary in additive notation.

2. Let H be a subgroup of a group G and let a and b be elements of G. Suppose $a^{-1}b \in H$. Explain why $b^{-1}a$ must also be in H. (This means that Theorem 9.1.3 can equivalently be stated with $b^{-1}a$ in place of $a^{-1}b$.)

3. (a) Check whether the subgroup $\{(1), (2\,3)\}$ is normal in S_3 by comparing the left and right cosets.

   (b) Explain why the subgroup $\langle(1\,2\,3)\rangle$ of S_3 is normal *without* comparing the left and right cosets.

4. Let $G = U(16)$ and let $H = \{1, 15\}$.

   (a) Explain why H is normal in G.
   (b) What is the order of G/H?
   (c) Find the order of each element in G/H.
   (d) Make the Cayley table for G/H.
   (e) Determine which familiar group G/H is isomorphic to.

5. Explain why $A_n \triangleleft S_n$ for $n \geq 4$.

6. To what familiar group is S_n/A_n (for $n \geq 4$) isomorphic? Justify your answer.

7. Let G be a group and let e be the identity element.

   (a) Explain why G and $\{e\}$ are both normal subgroups of G.

   (b) What group is $G/\{e\}$ isomorphic to?

   (c) What group is G/G isomorphic to?

8. Let G be a group and H a normal subgroup of G. **Prove** that if G is Abelian, then G/H is Abelian.

9. Show by counterexample that the converse of the statement in Exercise 8 is false. In other words, find a non-Abelian group that has an Abelian quotient group.

10. (a) In light of Exercise 8, explain why $U(32)/\{1, 17\}$ is an Abelian group of order 8.

    (b) Up to isomorphism, list all of the Abelian groups of order 8.

    (c) Which of the groups from part (b) is $U(32)/\{1, 17\}$ isomorphic to? (Hint: Use Activity 9.4.10.)

11. Let $G = D_4$, $K = \{R_0, R_{180}, H, V\}$, and $L = \{R_0, R_{180}\}$. Show that $L \triangleleft K$ and $K \triangleleft G$, but $L \not\triangleleft G$. (This shows that normality is not transitive.)

12. What is the order of $\mathbb{Z}_{80}/\langle 20 \rangle$?

13. Suppose H and K are normal subgroups of a group G. **Prove** that $H \cap K$ is a normal subgroup of G.

14. Show that $\mathbb{R}/\mathbb{Z}$ is an infinite group.

15. (a) Find all of the subgroups of $\mathbb{Z}_{64}/\langle 16 \rangle$.

    (b) Find the order of each of the subgroups from part (a).

16. Let G be a finite group and H a normal subgroup of G. **Prove** that for any $g \in G$, the order of the element gH in G/H divides $|g|$.

Chapter 10

Quotient Groups, Part 2

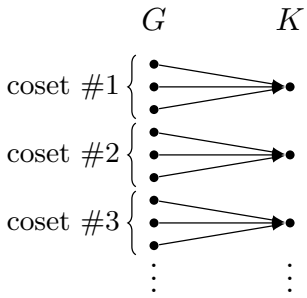
Quotient groups are one of the most important and commonly used constructions in group theory. In this chapter, we'll develop a way to verify isomorphisms involving quotient groups, and we'll take a short look at a very ambitious program to classify all finite groups which uses quotient groups in a central way.

10.1 The First Isomorphism Theorem

A few times in Chapter 9, we encountered situations in which we strongly suspected that a certain quotient group is isomorphic to some other group, but we stopped short of proving it. For example, in Example 9.4.4 we claimed that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong R^*$, in Activity 9.4.5 we hinted that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, and in Example 9.4.14 we claimed that the rotation group of the circle is isomorphic to $\mathbb{R}/360\mathbb{Z}$. But in none of these cases did we actually define a function from one of these groups to the other and then show it's an isomorphism. In this section, we'll show how to do this when one of the groups is a quotient group.

Suppose we want to prove that a quotient group G/H is isomorphic to a group K. By Chapter 6, we know this means we have to define a function $\phi : G/H \to K$ which is one-to-one, onto, and a homomorphism.

Let's start by defining a function $\phi : G/H \to K$. One way to do this would be to first define a function $f : G \to K$ which sends any two elements of G that are in the same coset of H to the same element of K.



In other words, we will define a function $f : G \to K$ with the property that if $aH = bH$, then $f(a) = f(b)$. We can now define our function $\phi : G/H \to K$ by $\phi(aH) = f(a)$.

Activity 10.1.1. We want the function $\phi : G/H \to K$ defined above in terms of $f : G \to K$ to be an isomorphism. What conditions must we place on f to ensure that this is so?

1. We'll need ϕ to be a homomorphism. In other words, we need it to be true that for any a and b in G, $\phi(aH \cdot bH) = \phi(aH) \cdot \phi(bH)$. What condition on f will guarantee this?
2. We'll need ϕ to be onto. In other words, for any $k \in K$, we need it to be true that there is an element $g \in G$ such that $\phi(gH) = k$. What condition on f will guarantee this?
3. We'll need ϕ to be one-to-one. In other words, we need it to be true that if $\phi(aH) = \phi(bH)$, then $aH = bH$. What condition on f will guarantee this?

Problem 3 of the above activity motivates the following definition, which we'll need to state our main theorem:

Definition 10.1.2. Let G and H be groups and let e_H be the identity of H. Suppose $f : G \to H$ is a homomorphism. The set $\{g \in G : f(g) = e_H\}$ is called the **kernel** of f. It is denoted by $\ker(f)$.

Lemma 10.1.3. *Let G and H be groups, and suppose $f : G \to H$ is a surjective homomorphism. Then $\ker(f)$ is a normal subgroup of G.*

Activity 10.1.4. Prove the theorem. (Don't forget to first prove that $\ker(f)$ is a subgroup of G.)

Thanks to this lemma, we can form the quotient group $G/\ker(f)$.

Theorem 10.1.5 (First Isomorphism Theorem)**.** *Suppose G and H are groups and that $f : G \to H$ is a homomorphism. If f is onto, then*

$$G/\ker(f) \cong H.$$

There are also Second, Third, and Fourth Isomorphism Theorems, but we won't be covering them.

The First Isomorphism Theorem provides a recipe for establishing an isomorphism when one of the groups involved is a quotient group. To prove a quotient group G/H is isomorphic to some group K:

1. Define a function $f : G \to K$.
2. Show that f is a homomorphism.
3. Show that f is onto.
4. Show that $\ker(f) = H$.

You can then conclude that $G/H \cong K$ without having to define functions on cosets. The First Isomorphism Theorem takes care of that for you!

Activity 10.1.6. Use the four-step recipe above to prove that $\mathbb{R}/360\mathbb{Z}$ is isomorphic to the rotation group of the circle.

The First Isomorphism Theorem also lets us explore interactions between direct products and quotient groups. We'll look at one of them here and leave others as exercises.

Example 10.1.7. Let G_1 and G_2 be groups, and let e_2 be the identity in G_2. First, we'll show that the set $G_1 \oplus \{e_2\}$ is a normal subgroup of $G_1 \oplus G_2$ which is isomorphic to G_1. We'll denote $G_1 \oplus \{e_2\}$ by $\overline{G_1}$.

We already know by Theorem 8.1.11 that $\overline{G_1}$ is a subgroup of $G_1 \oplus G_2$ since G_1 is a subgroup of G_1 and $\{e_2\}$ is a subgroup of G_2. To show $\overline{G_1}$ is normal in $G_1 \oplus G_2$, we can use the Normal Subgroup Test. Let (g_1, g_2) be an arbitrary element of $G_1 \oplus G_2$, and let (h_1, e_2) be an arbitrary element of $\overline{G_1}$. Then

$$\begin{aligned}(g_1, g_2)(h_1, e_2)(g_1, g_2)^{-1} &= (g_1, g_2)(h_1, e_2)(g_1^{-1}, g_2^{-1}) \\ &= (g_1 h_1 g_1^{-1}, g_2 e_2 g_2^{-1}) \\ &= (g_1 h_1 g_1^{-1}, e_2) \\ &\in \overline{G_1}.\end{aligned}$$

Thus, $\overline{G_1} \triangleleft G_1 \oplus G_2$.

It's easy to see that $G_1 \cong \overline{G_1}$. Define a function $\theta : G_1 \to \overline{G_1}$ by $\theta(g_1) = (g_1, e_2)$. You will prove that θ is an isomorphism in Exercise 4.

Now let's show that $(G_1 \oplus G_2)/\overline{G_1} \cong G_2$. Since we have to establish an isomorphism involving a quotient group, we'll use the First Isomorphism Theorem.

1. Define a function $f : G_1 \oplus G_2 \to G_2$ by $f((g_1, g_2)) = g_2$.

2. To show f is a homomorphism, let (g_1, g_2) and (h_1, h_2) be two arbitrary elements of $G_1 \oplus G_2$. Then

$$\begin{aligned} f((g_1, g_2)(h_1, h_2)) &= f(g_1h_1, g_2h_2) \\ &= g_2h_2 \\ &= f((g_1, g_2))f((h_1, h_2)). \end{aligned}$$

   Therefore, f is a homomorphism.

3. To show that f is onto, let g_2 be an arbitrary element of G_2. We have to find an element of $G_1 \oplus G_2$ that f sends to g_2. By the definition of f, the first coordinate of this element of $G_1 \oplus G_2$ doesn't matter. Since we know G_1 has an identity, call it e_1, $f((e_1, g_2)) = g_2$, and f is thus onto.

4. We have to show that $\ker(f) = \overline{G_1}$. We have

$$\begin{aligned} (g_1, g_2) \in \ker(f) &\iff f((g_1, g_2)) = e_2 \\ &\iff g_2 = e_2 \\ &\iff (g_1, g_2) = (g_1, e_2) \\ &\iff (g_1, g_2) \in \overline{G_1}. \end{aligned}$$

   Therefore, $\ker(f) = \overline{G_1}$.

Thus by the First Isomorphism Theorem, $(G_1 \oplus G_2)/\overline{G_1} \cong G_2$.

This example seems to indicate that the relationship between direct products and quotient groups is similar to the relationship between products and quotients of numbers. The isomorphism we just saw is reminiscent of the basic rule from algebra:

$$\frac{mn}{m} = n.$$

In some instances this is true, but not always. For example, in Exercise 2, we'll see that the direct product / quotient group version of the algebra rule:

$$\frac{m}{n} \cdot n = m$$

does *not* hold.

10.2 Extensions and Simple Groups

By the 20th century, group theory had grown into a very broad and very deep area of research, and an idea started to develop that maybe it would be possible to classify all of the finite groups (up to isomorphism, as usual). We've seen that this has been done with finite Abelian groups. This project has become known as the Jordan-Hölder program after two mathematicians who contributed much of the underlying theory, Camille Jordan (1828-1922) and Otto Hölder (1859-1937). We'll briefly discuss the outcome of the Jordan-Hölder program in this section and introduce some central ideas of group theory along the way.

An **extension** of a group K by a group N is a group G that has a normal subgroup H which is isomorphic to N and such that $G/H \cong K$.

Activity 10.2.1.

1. Explain why any group G is an extension of the trivial group $\{e\}$ by G itself. (This is like saying that any number is the product of 1 and itself.)
2. Explain why $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ are both extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2$.
3. Use Example 10.1.7 to say why, for any two groups G_1 and G_2, $G_1 \oplus G_2$ is an extension of G_1 by G_2.

Activity 10.2.2. You can form extensions starting with more than two groups as follows: Suppose we have three groups, A, B, and C. We can first form an extension G_1 of A by B. We can then form an extension G_2 of G_1 by C.

Show that $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, and $\mathbb{Z}_2 \oplus Z_2 \oplus \mathbb{Z}_2$ are all extensions that could be formed by starting with three copies of $\mathbb{Z}_2$.

The above two activities indicate that direct products are examples of extensions, but not the *only* examples. We thus see that forming an extension of one group by another is a more general way of "building up" a new, bigger group out of smaller ones.

If forming extensions is a way to build new groups out of old ones, then a natural question to ask is: What are the basic, most elemental groups from which we can build more complex ones? These would be like the prime numbers in number theory, the elements in chemistry, or phonemes in linguistics. Such groups would be the "building block" groups that cannot be formed as extensions of simpler groups (except as the trivial extension from Problem 1 in Activity 10.2.1).

Activity 10.2.3. Suppose a group G has a normal subgroup H, where H is not $\{e\}$ or G itself. Why must G be a nontrivial extension of two groups?

The above activity shows that if a group G is *not* a nontrivial extension, then it must *not* have any normal subgroups other than $\{e\}$ or G itself. This leads to the following definition, which will serve as our definition of the "building block" groups:

Definition 10.2.4. A group G is **simple** provided that it has no normal subgroups other than the trivial subgroup and G itself.

Simple groups are hard to come by. In Exercise 13, you'll explain why any group of prime order is simple. The only other simple groups from our experience in this course are the alternating groups of degree greater than 4.

Theorem 10.2.5. *The alternating groups A_n for $n \geq 5$ are simple.*

This is not at all easy to prove. We can, however, prove this when $n = 5$ if we allow ourselves the following fact which we cannot prove here without a very long detour.

Lemma 10.2.6. *Any group of order 15 or 30 has an element of order 15.*

Proof that A_5 is simple. Suppose, to the contrary, that A_5 *does* have a normal subgroup H other than itself and the trivial group. By Lagrange's Theorem, $|H|$ would have to divide $|A_5|$, which is $\frac{1}{2}(5!) = 60$. So $|H|$ could be 2, 3, 4, 5, 6, 10, 12, 15, 20, or 30. If we were to write down the 60 elements of A_5, we could compute their orders and find that there are 20 elements of order 3, 24 elements of order 5, and no elements of order 15.

Before proceeding, we need to prove that if G is a finite group with normal subgroup K and g is an element of G whose order is relatively prime to $|G/K|$, then $g \in K$. To see why this is so, consider the element $gK \in G/K$. By Exercise 16 in Chapter 9, $|gK|$ as an element of G/K divides $|g|$ as an element of G. Thus, $|gK|$ is a common divisor of both $|g|$ and $|G/K|$. But $|g|$ and $|G/K|$ are relatively prime and thus have no common divisor except 1. Therefore, $|gK| = 1$. This means gK is the identity element of G/K. Thus $gK = K$, so $g \in K$.

If $|H|$ equals 3, 6, 12, or 15, then $|A_5/H|$ equals 4, 5, 10, or 20. In each case, $|A_5/H|$ is relatively prime to 3, which means, by the previous paragraph, that H contains all 20 elements of A_5 of order 3. This contradicts the order of H being 3, 6, 12, or 15.

If $|H|$ equals 5, 10, or 20, then $|A_5/H|$ equals 3, 6, or 12. In each case, $|A_5/H|$ is relatively prime to 5, which means H would contain all 24 elements of A_5 of order 5. This would contradict the order of H being 5, 10, or 20.

The same argument shows that if $|H| = 30$, then H must contain all the elements of A_5 of order 3 and 5, 44 elements in total. Another contradiction.

The only remaining possibilities for $|H|$ are 2 and 4. In these cases, $|A_5/H|$ equals 15 or 30. By Lemma 10.2.6, H must contain an element of A_5 of order 15, but as noted above, there are none.

We can therefore conclude that A_5 has no normal subgroup other than the trivial subgroup and G itself, which means that A_5 is simple. □

Simple groups were known about as early as 1830 by Galois, whom we met earlier. He was actually the first to prove that A_5 is simple, and this turned out to be a fundamental part of his proof that quintic polynomial equations, in general, cannot be solved by radicals.

Other simple groups were found over the next hundred years, and during that time, it was proposed that it might be possible to completely classify the finite simple groups. This is the first part of the Jordan-Hölder program. This classification would be like compiling a version of chemistry's periodoc table for finite groups. Knowing the basic building block groups would be the first step in knowing all the finite groups.

The first major contribution to this classification program was a 255-page paper published in 1962 by Walter Feit (1930-2004) and John Griggs Thompson (1932-). By the mid-1980's, it was generally thought that the classification was complete, until a gap was found. It wasn't until 2004 that this gap was filled in by a proof that totaled 1221 pages! The total proof of the classification theorem comes to tens of thousands of pages written by about 100 authors over a period of about 50 years. There is currently an effort underway to simplify and condense the proof. It's estimated that the final simplified proof will still number about 5000 pages.

Here's what the classification theorem says, although not all of the terminology will be familiar to us:

Theorem 10.2.7 (Classification of Finite Simple Groups)**.** *Every finite simple group is isomorphic to one of the following types of group:*

- *a cyclic group of prime order,*
- *an alternating group A_n with $n \geq 5$,*
- *a finite group of Lie type, or*
- *one of the 26 "sporadic groups".*

The theorem provides our periodic table. Notice that the left-most column displays the alternating groups and the right-most displays the cyclic groups of prime order (denoted here by C_p rather than $\mathbb{Z}_p$):

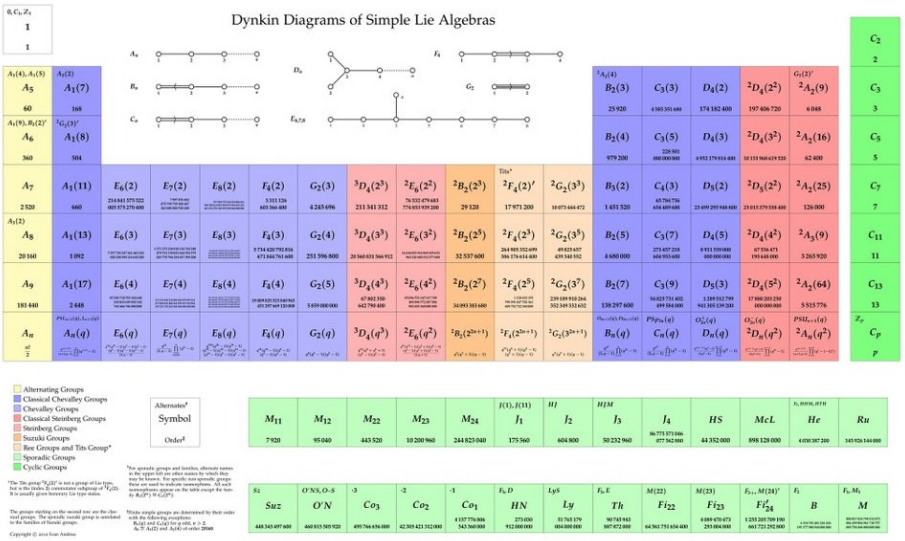


Figure 10.1: Periodic Table of Finite Simple Groups

The classification is stated for *finite* simple groups. There is no such theorem for *infinite* simple groups, nor does anyone expect there ever to be one.

The finite groups of Lie (pronounced "lee") type are named after the Norwegian mathematician Sophus Lie (1842-1899) and are closely related to matrix groups. One example is known as the *projective special linear group*. This group is formed by first replacing the real number entries in the special linear group $SL_n(\mathbb{R})$ by the group $\mathbb{Z}_q$ for some prime q. We then take the subgroup H of $SL_n(\mathbb{Z}_q)$ consisting of all the diagonal matrices in $SL_n(\mathbb{Z}_q)$ that have the same entry all down the diagonal. The projective special linear group is the quotient $SL_n(\mathbb{Z}_q)/H$, which is denoted $PSL_n(q)$. If $n > 2$ and $q > 3$, then $PSL_n(q)$ turns out to be simple. Most finite simple groups are finite groups of Lie type.

The sporadic groups mentioned in the theorem are fascinating. They don't belong to any of the three infinite families of simple groups listed in the first three bullets. They stand alone. They also get pretty big. The largest of these 26 sporadic groups has been dubbed the "monster group". It's order is:

808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.

That's about 8×10^{53}. The monster group contains 20 of the sporadic groups as subgroups or quotients of subgroups. These 20 subgroups are often called the "Happy Family", and the 6 others are called "Pariahs". A very entertaining video about the classification theorem and the monster group in particular can be found on the Numberphile YouTube channel. Search YouTube for "numberphile monster group" to view it. It features the mathematician John Conway

(1937-2020), who discovered three of the sporadic groups himself in the late 1960's.

But what about the extension problem? Now that all of the finite simple groups are known, how would one complete the Jordan-Hölder program by describing all the ways to form extensions of the finite simple groups? Unfortunately, this task is so daunting as to make the classification of finite simple groups seem easy. For example, it's known that if you start with just nine copies of the smallest simple group, $\mathbb{Z}_2$, there are 10,494,213 isomorphism classes of possible extensions! Try to imagine the sheer multitude of extensions that would result if one of your simple groups were the monster!

Needless to say, forming extensions is a much more complicated way to build groups than is multiplying prime numbers to build integers. The general consensus is that the extension part of the Jordan-Hölder program is hopeless.

Regardless, the classification of finite simple groups is a truly staggering accomplishment. Maybe even more amazing is that it's really just a logical consequence of the four group axioms stated in Chapter 2. Group theory has come quite a ways since Theorem 2.2.1 when we proved that groups have unique identity elements!

10.3 Exercises

1. **Prove** that $\mathbb{R}^*/\{1,-1\} \cong \mathbb{R}^+$. (Recall that $\mathbb{R}^+$ is the set of positive real numbers and is a group with respect to multiplication.)

2. Explain why $\mathbb{Z}/3\mathbb{Z} \oplus 3\mathbb{Z} \ncong \mathbb{Z}$. This shows that in general, $G/H \oplus H$ is *not* isomorphic to G. (Hint: Show that $\mathbb{Z}/3\mathbb{Z} \oplus 3\mathbb{Z}$ contains elements of finite order other than the identity.)

3. In Exercise 15 in Chapter 1, we saw an analogy between composing rotations and reflections with each other and multiplying the numbers 1 and -1. We can now finally make this precise as follows: Let K be the subgroup of D_4 generated by R_{90}. Explain by K is normal in D_4 and **prove** that $D_4/K \cong \{1,-1\}$.

4. **Prove** that the function θ from Example 10.1.7 is an isomorphism.

5. **Prove** that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$.

6. **Prove** that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ for any positive integer n.

7. Show that the function $f : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ defined by $f((a,b)) = a - b$ is a homomorphism. Then find its kernel.

8. Show that the function $f : \mathbb{R} \to GL_2(\mathbb{R})$ defined by

$$f(x) = \begin{bmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{bmatrix}$$

is a homomorphism. Then find its kernel.

9. Let G_1 be a group and H_1 a normal subgroup of G_1. Let G_2 be a group an H_2 a normal subgroup of G_2.

   (a) **Prove** that $H_1 \oplus H_2$ is a normal subgroup of $G_1 \oplus G_2$.

   (b) **Prove** that $(G_1 \oplus G_2)/(H_1 \oplus H_2) \cong (G_1/H_1) \oplus (G_2/H_2)$.

10. Show that if H and K are finite groups and G is an extension of H by K, then $|G| = |H| \cdot |K|$.

11. Find two non-isomorphic extensions of $\mathbb{Z}_2$ by A_5.

12. If H and K are Abelian groups, must any extension of K by H be Abelian? (Hint: See Exercise 3 above.)

13. **Prove** that any group of prime order is simple.

14. Explain why an Abelian group whose order is not prime is not simple.

15. Let G be a finite group. In the collection of all normal subgroups of G (excluding G itself), let H be the one with the largest order. Explain why G/H is simple. (This proves that every finite group has a simple quotient.)

Index