Elementary Abstract Algebra: Examples and Applications

Contributing editors:

Justin Hill, Chris Thron
Temple College / Texas A&M University-Central Texas

Incorporating source materials by

Thomas Judson (Stephen F. Austin State University)
Dave Witte Morris and Joy Morris (University of Lethbridge)
A. J. Hildebrand (University of Illinois Urbana-Champaign)

Additional contributions by

Holly Webb, David Weathers, Johnny Watts, and Semi Harrison
(TAMU-CT)

January 6, 2016

Material from "Abstract Algebra, Theory and Applications" by Thomas Judson may be found throughout much of the book. A current version of "Abstract Algebra, Theory and Applications" may be found at:

abstract.ups.edu.

The Set Theory and Functions chapters are largely based on material from "Proofs and Concepts"(version 0.78, May 2009) by Dave Witte Morris and Joy Morris, which may be found online at:

https://archive.org/details/flooved3499, or
http://people.uleth.ca/~dave.morris/books/proofs+concepts.html

The material on induction was modified from LaTeXcode originally obtained from A. J. Hildebrand, whose course web page is at:
http://www.math.uiuc.edu/~hildebr/

Justin and Chris would like to express their deepest gratitude to Tom, Dave and Joy, and A. J. for generously sharing their original material. They were not involved in the preparation of this manuscript, and are not responsible for any errors or other shortcomings.

Please send comments and corrections to: thron@tamuct.edu. You may also request the LaTeXsource code from this same email address.

YouTube videos are available: search on YouTube for the title of this book.

ISBN: 978-1-312-85635-6

Contents

1

Forward

To the student:

Many students start out liking math. Some like it well enough that they even want to teach it. However, when they reach advanced math classes (such as abstract algebra), they feel bewildered and frustrated. Their textbooks talk about mathematical concepts they've never heard of before, which have various properties which come from who knows where. In lectures, the prof. pronounces oracles (a.k.a theorems) and utters long incantations called "proofs" , but it's hard to see the point of either.

If the above paragraph describes you, then this book is meant for you!

There's a good reason why higher math classes are bewildering for most students. I believe that we math instructors tend to take too much for granted.[1] We've forgotten that we are able to understand abstractions because we have concrete *examples* in the back of our minds that we keep referring back to, consciously or subconsciously. These examples enable us to fit abstract ideas in with specific behaviors and patterns that we're very familiar with. But students who don't have a firm hold on the examples have nothing to hold on to, and are left grasping (and gasping) for air.

To be sure, most students have previously been exposed to various important examples that (historically) gave rise to abstract algebra. These examples include the complex numbers, integers mod n, symmetries, and so on. They can give definitions and do some computations according to the

[1] My dad always says that math is excruciatingly difficult to learn, but once you get it it's excruciatingly difficult to see why others can't understand it like you do.

rules. But they haven't been given a chance to *internalize* these examples. They can kind of follow along, but they don't really "speak the language".

Our hope is that after reading this book students will be able to say, "I've seen complex numbers, permutations and other such things before, but now I understand what makes them tick. I also see they have some very deep similarities with each other, and with other mathematical objects that I'm familiar with."

This is actually a very good time to be learning abstract algebra. Long the province of specialists and puzzle enthusiasts, abstract algebra has recently made impressive showings on the center stage of modern science and technology. Two areas where abstract algebra has made strong contributions stand out particularly: information processing and physics. Coding of information is at the heart of information technology, and abstract algebra provides all of the methods of choice for information coding that is both reliable (impervious to errors) and private. On the other hand, many of the recent advances in physics is due to understanding of physical symmetries and the groups that produce them. We try as much as possible to make connections with these two areas, and hope to do so increasingly in future editions.

Enjoy the book, and send us your comments!

To the instructor

This book is not intended for budding mathematicians. It was created for a math program in which most of the students in upper-level math classes are planning to become secondary school teachers. For such students, most if not all published abstract algebra texts are totally incomprehensible, both in style and in content. Faced with this situation, we decided to create a book that our students could actually read for themselves. In this way we have been able to dedicate class time to problem-solving and two-way interaction rather than rehashing the same material in lecture format.

Some instructors may feel that this book doesnt cover enough, and admittedly it falls short of the typical syllabus. But in far too many abstract algebra classes, the syllabus is covered and the students retain nothing. We feel it is much better to cover less but have the material stick. We have also avoided an "abstract" treatment and instead used specific examples (complex numbers, modular arithmetic, permutations, and so on) as stepping stones to general principles. The unhappy fact is that many students at this level have not yet mastered these important basic examples, and it is useless

to expect them to grasp abstractifications of what they dont understand in the first place. Furthermore, these are the just the basic examples that will be most useful to them in their future career as high school teachers.

The book is highly modular, and chapters may be readily omitted if students are already familiar with the material. Some chapters ("In the Beginning" and "Sigma Notation") are remedial. Other chapters cover topics that are often covered in courses in discrete mathematics, such as sets, functions, and equivalence classes. (Much of this material is taken from the Morris' book, with some amplifications.) We have found from experience that students need this re-exposure in order to gain the necessary facility with these concepts, on which so much of the rest of the book is based.

Whenever possible we have introduced applications, which may be omitted at the instructor's discretion. However, we feel that it is critically important for preparing secondary teachers to be familiar with these applications. They will remember these long after they have forgotten proofs they have learned, and they may even be able to convey some of these ideas to their own students.

Additional resources

This is the Information Age, and a mere textbook is somewhat limited in its ability to convey information. Accordingly, as we continue to use the book in our classes, we are continuing to build an "ecosystem" to support the book's use:

- The latest version of the book (and any accessory materials) may be found at the TAMU-CT Mathematics Department web page (go to www.tamuct.edu and search for "Mathematics Resources").
- An electronic version of the book is available online: the link may be found on the "Mathematics Resources" page cited above.
- A comprehensive set of short video presentations of the book's content may be found on YouTube (search for the book's title).
- An "Instructor's Supplement" is available upon request: email the editor (C.T.) from a verifiable faculty email address.
- Any instructor wishing to customize the material or extract certain portions may email the editor (C.T.) to request the LaTeX source code. We have received freely from others, so we are happy to freely give.

Acknowledgements

In our preparation of this text, we were fortunate to find via the web some extraordinarily generous authors (Tom Judson, Dave Witte Morris and Joy Morris, A. J. Hildebrand) who freely shared their material with us. Thanks to them, we were able to put the first version of this textbook together within the span of a single semester (not that we're finished – this is a living book, not a dead volume). We hope that other instructors will similarly benefit from the material offered here.

Several Master's students at Texas A&M-Central Texas have made contributions to the book as part of a projects course or thesis. The original version was Justin Hill's Master's thesis. Holly Webb wrote the Group Actions chapter and David Weathers wrote parts of "In the Beginning", "A Sticky Problem", "Sigma Notation" and "Polynomials" as part of their coursework.

Others have made contributions to both content and format. Johnny Watts our "math technician" helped with technical details. Khoi Tran contributed his excellent exercise solutions.

Above all we want to acknowledge the One to whom all credit is ultimately due. "Unless the LORD builds the house, the builders labor in vain. Unless the LORD keeps the city, the watchman is wakeful in vain. It is vanity to rise up early, stay up late, and eat the bread of sorrows, for He gives sleep to those He loves." (Psalm 127:1-2)

2

In the Beginning

Let's start at the very beginning
A very good place to start
When you read you begin with A B C
When you sing you begin with Do Re Me

(Oscar Hammerstein, *The Sound of Music*)

2.1 Prologue

If Maria had been the Trapp children's math tutor, she might have continued: "When you count, you begin with 1 2 3". Ordinarily we think of the "counting numbers" (which mathematicians call the *natural numbers* or *positive integers*) as the "very beginning" of math.[1]

It's true that when we learn math in school, we begin with the counting numbers. But do we really start at the "very beginning"? How do we know that $1 + 1 = 2$? How do we know that the methods we learned to add, multiply, divide, and subtract will always work? We've been taught how to factor integers into prime factors. But how do we know this always works?

Mathematicians are the ultimate skeptics: they won't take "Everyone knows" or "It's obvious" as valid reasons. They keep asking "why", breaking things down into the most basic assumptions possible. The very basic assumptions they end up with are called ***axioms***. They then take these

[1] A famous mathematician once said, "God made the integers; all else is the work of man." (Leopold Kronecker, German mathematician, 1886)

axioms and play with them like building blocks. The arguments that they build with these axioms are called ***proofs***, and the conclusions of these proofs are called ***propositions*** or ***theorems***.

The mathematician's path is not an easy one. It is exceedingly difficult to push things back to their foundations. For example, arithmetic was used for thousands of years before a set of simple axioms was finally developed (you may look up "Peano axioms" on the web).[2] Since this is an elementary book, we are not going to try to meet rigorous mathematical standards. Instead, we'll lean heavily on examples, including the integers, rationals, and real numbers. Once you are really proficient with different examples, then it will be easier to follow more advanced ideas.[3]

This text is loaded with proofs, which are as unavoidable in abstract mathematics as they are intimidating to many students. We try to "tone things down" as much as possible. For example, we will take as "fact" many of the things that you learned in high school and college algebra–even though you've never seen proofs of these "facts". In the next section we remind you of some of these "facts". When writing proofs or doing exercise feel free to use any of these facts. If you have to give a reason, you can just say "basic algebra".

We close this prologue with the assurance that abstract algebra is a beautiful subject that brings amazing insights into the nature of numbers, and the nature of Nature itself. Furthermore, engineers and technologists are finding more and more practical applications, as we shall see in the coming chapters.

2.2 Integers, rational numbers, real numbers

We assume that you have already been introduced to the following number systems: integers, rational numbers, and real numbers.[4] These number systems possess the well-known arithmetic operations of addition, subtraction, multiplication, and division. The following statements hold for all of these number systems.

[2]The same is true for calculus. Newton and Leibniz first developed calculus around 1670, but it was not made rigorous until 150 years later.

[3]Historically, mathematics has usually progressed this way: examples first, and axioms later after the examples are well-understood.

[4]This section and the following were written by David Weathers (edited and expanded by C.T.)

Warning There are number systems for which the following properties do NOT hold (as we shall see later). So they may be safely assumed ONLY for integers, rational numbers, and real numbers. ◊

2.2.1 Operations and relations

We assume the following properties of these arithmetic operations:

(a) *Commutative*: When two numbers are added together, the two numbers can be exchanged without changing the value of the result. The same thing is true for two numbers being mulitiplied together.

(b) *Associative*: When three or more numbers are added together, changing the grouping of the numbers being added does not change the value of the result. The same goes for three or more numbers multiplied together. (Note that in arithmetic expressions, the "grouping" of numbers is indicated by parentheses.)

(c) *Distributive*: Multiplying a number by a sum gives the same result as taking the sum of the products.

(d) *Order*: Given two numbers, exactly one of these three are true: either the first number is greater than the second, or the second number is greater than the first, or the two numbers are equal.

(e) *Identity*: Addition by 0 or multiplication by 1 result in no change of original number.

(f) The sum of two positive numbers is positive. The sum of two negative numbers is negative.

(g) The product of two nonzero numbers with the same sign is positive. The product of two numbers with different signs is negative.

(h) If the product of two numbers is zero, then one or the other number must be zero.

Exercise 1.

(a) For the properties a,b,c,e above, give (i) a specific example for addition, using numbers, and (ii) a general statement for multiplication, using variables. For example, for property (a) (the commutative property) a specific example would be $3+5=5+3$, and a general statement would be $x \cdot y = y \cdot x$.

(b) For properties d,f,g,h above, give a specific example which illustrates the property using numbers.

$\Diamond$

Exercise 2.

(a) Give an example (using numbers) that shows that subtraction is *not* commutative .

(b) Give an example (using numbers) that shows that division is *not* associative.

$\Diamond$

Exercise 3. Suppose $a > b$, $b \geq 0$ and $ab = 0$. What can you conclude about a and b? Use one (or more) of the properties we have mentioned to justify your answer. $\Diamond$

Exercise 4. Which of the above properties must be used to prove each of the following statements?

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

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

(c) $(a \cdot x + a \cdot y) + a \cdot z = a \cdot ((x + y) + z)$

(d) $((a \cdot b) \cdot c + b \cdot c) + c \cdot a = c \cdot ((a + b) + a \cdot b)$

$\Diamond$

Note that the associative property allows us to write expressions without putting in so many parentheses. So instead of writing $(a + b) + c$, we may

simply write $a + b + c$. By the same reasoning, we can remove parentheses from any expression that involves only addition, or any expression that involves only multiplication: so for instance, $(a \cdot (b \cdot c) \cdot d) \cdot e = a \cdot b \cdot c \cdot d \cdots e$. Using the associative and distributive property, it is possible to write any arithmetic expression without parentheses. So for example, $(a \cdot b) \cdot (c + d)$ can be written as $a \cdot b \cdot c + a \cdot b \cdot d$. (Remember that according to operator precedence rules, multiplication is always performed before addition: thus $3 \cdot 4 + 2$ is evaluated by first taking $3 \cdot 4$ and then adding 2.)

Exercise 5. Rewrite the following expressions without any parentheses, using *only* the associative and distributive properties. (Don't use commutative in this exercise!)

(a) $(((x + y) + (y + z)) \cdot w) - 2y \cdot w$

(b) $0.5 \cdot ((x + y) + (y + z) + (z + x))$

(c) $((((((a + b) + c) \cdot d) + e) \cdot f) + g) + h$

◊

Exercise 6. For parts (a–c) of the preceding exercise, now apply the commutative property to the results to simplify the expressions as much as possible. ◊

Exercise 7. Evaluate the following expressions by hand (no calculators!).

(a) $3 \cdot 4 + 5 + 6 \cdot 2$

(b) $3 + 4 \cdot 5 \cdot 6 + 2$

(c) $1 + 2 \cdot 3 + 3 \cdot 4 \cdot 5 + 5 \cdot 6 \cdot 7 \cdot 2$

◊

2.2.2 Manipulating equations and inequalities

Following are some common rules for manipulating equations and inequalities. Notice there are two types of inequalities: ***strict inequalities*** (that use the $>$ or $<$ symbols) and ***nonstrict inequalities*** (that use the $\geq$ or $\leq$ symbols).

(A) *Substitution*: If two quantities are equal then one can be substituted for the other in any true equation or inequality and the result will still be true.

(B) *Balanced operations*: Given an equation, one can perform the same operation to both sides of the equation and maintain equality. The same is true for inequalities for the operation of addition, and for multiplication or division by a *positive* number.

(C) Multiplying or dividing an inequality by a negative value will reverse the inequality symbol.

(D) The ratio of two integers can always be reduced to lowest terms, so that the numerator and denominator have no common factors.

Exercise 8. Give specific examples for statements (A–D) given above. You may use either numbers or variables (or both) in your examples.. For (A) and (B), give one example for each of the following cases: (i) equality, (ii) strict inequality, (iii) nonstrict inequality. ♢

2.2.3 Exponentiation (VERY important)

Exponentiation is one of the key tools of abstract algebra. It is *essential* that you know your exponent rules inside and out!

(I) Any nonzero number raised to the power of 0 is equal to 1. [5]

(II) A number raised to the sum of two exponents is the product of the same number raised to each individual exponent.

[5] Technically 0^0 is undefined, although often it is taken to be 1. Try it on your calculator!

(III) A number raised to the power which is then raised to another power is equal to the same number raised to the product of the two powers.

(IV) A number raised to a negative exponent is equal to the reciprocal of the number raised to a positive .

(V) Taking the product of two numbers and raising to a given power is the same as taking the powers of the two numbers separately, then multiplying the results.

Exercise 9. For each of the above items (I–V), give a general equation (using variables) that expresses the rule. For example one possible answer to (II) is: $x^{y+z} = x^y \cdot x^z$. ◊

Exercise 10. Write an equation that shows another way to express a number raised to a power that is the difference of two numbers. ◊

2.3 Test yourself

Test yourself with the following exercises. If you feel totally lost, I strongly recommend that you improve your basic algebra skills before continuing with this course. This may seem harsh, but I only mean to spare you agony. All too often students go through the motions of learning this material, and in the end they learn nothing because their basic skills are deficient. If you want to play baseball, you'd better learn how to throw, catch, and the ball first.

Exercise 11. Simplify the following expressions. Factor whenever possible

(a) $2^4 4^2$

(b) $\dfrac{3^9}{9^3}$

(c) $\left(\dfrac{5}{9}\right)^7 \left(\dfrac{9}{5}\right)^6$

(d) $\dfrac{a^5}{a^7} \cdot \dfrac{a^3}{a}$

(e) $x(y-1) - y(x-1)$

◊

Exercise 12. Same instructions as the previous exercise. These examples are harder. (*Hint*: It's usually best to make the base of an exponent as simple as possible. Notice for instance that $4^7 = (2^2)^7 = 2^{14}$.)

(a) $6^{1/2 \cdot} 2^{1/6} \cdot 3^{3/2} \cdot 2^{1/3}$

(b) $(9^3)(4^7)\left(\frac{1}{2}\right)^8\left(\frac{1}{12}\right)^6$

(c) $4^5 \cdot 2^3 \cdot \left(\frac{1}{2}\right)^5 \cdot \left(\frac{1}{4}\right)^3$

(d) $2^3 \cdot 3^4 \cdot 4^5 \cdot 2^{-5} \cdot 3^{-4} \cdot 4^{-3}$

(e) $\dfrac{x(x-3)+3(3-x)}{(x-3)^2}$

◊

Exercise 13. Same instructions as the previous exercise. These examples are even harder. (*Hint*: Each answer is a single term, there are no sums or differences of terms.)

(a) $\dfrac{a^5+a^3-2a^4}{(a-1)^2}$

(b) $a^x b^{3x}(ab)^{-2x}(a^2b)^{x/2}$

(c) $(x+y^{-1})^{-2}(xy+1)^2$

(d) $\dfrac{(3^x+9^x)(1-3^x)}{1-9^x})$

(e) $\dfrac{3x^2-x}{x-1}+\dfrac{2x}{1-x}$

◊

Exercise 14. Find ALL real solutions to the following equations.

(a) $x^2 = 5x$

(b) $(x-\sqrt{7})(x+\sqrt{7}) = 2$

(c) $2^{4+x} = 4(2^{2x})$

(d) $3^{-x} = 3(3^{2x})$

(e) $16^5 = x^4$

(f) $\dfrac{1}{1+1/x} - 1 = -1/10$

◊

3

Complex Numbers

HORATIO: O day and night, but this is wondrous strange!

HAMLET: And therefore as a stranger give it welcome. There are more things in heaven and earth, Horatio, Than are dreamt of in your philosophy.

(Source: Shakespeare, *Hamlet*, Act 1 Scene 5.)

Although complex numbers are defined to include "imaginary" numbers, the practical applications of complex numbers are far from "imaginary". We shall touch on some of the applications in this chapter: but there are many many more in engineering, in physics, and in other sciences as well.[1]

3.1 The origin of complex numbers

3.1.1 A number that can't be real (and we can prove it!)

Way back in your first algebra class, you saw equations like:

- $x^2 = 4$
- $x^2 = 36$
- $x^2 = 7$

[1] Thanks to Tom Judson for material used in this chapter.

You also learned how to solve them either by hand, or using the SQRT button on a simple calculator. The solutions to these equations are

- $x = \pm 2$
- $x = \pm 6$
- $x = \pm 2.64575131106459...$

But what about equations like:

$$x^2 = -1$$

Your simple calculator can't help you with that one![2] If you try to take the square root of -1, the calculator will choke out ERROR or some similar message of distress. But why does it do this? Doesn't -1 have a square root?

In fact, we can prove mathematically that -1 does not have a *real* square root. As proofs will play a very important part in this course, we'll spend some extra time and care explaining this first proof.

Proposition 1. -1 has no real square root.

Proof. We give two proofs of this proposition. The first one explains all the details, while the second proof is more streamlined. It is the streamlined proof that you should try to imitate when you write up proofs for homework exercises.

Long drawn-out proof of Proposition 1 with all the gory details:

We will use a common proof technique called ***proof by contradiction***. Here's how it goes:

First we *suppose* that there exists a real number a such that $a^2 = -1$. Now we know that any real number is either positive, or zero, or negative−there are no other possibilities. So we consider each of these three cases: $a > 0$, or $a = 0$, or $a < 0$.

- In the case that $a > 0$ then $a^2 = a \cdot a = (positive) \cdot (positive) =$ a positive number (that is, $a^2 > 0$). But this couldn't possibly be true, because we have already supposed that $a^2 = -1$: there's not way that $a^2 > 0$ and $a^2 = -1$ can both be true at the same time!

[2] It's true that the fancier graphing calculators can handle it, but that's beside the point.

- In the case that $a = 0$, then $a^2 = a \cdot a = (0) \cdot (0) = 0$. But $a^2 = 0$ also contradicts our *supposition* that $a^2 = -1$.
- In the case that $a < 0$, then $a^2 = a \cdot a = (negative) \cdot (negative) =$ a positive number, so $a^2 > 0$. As in the first case, this contradicts our *supposition* that $a^2 = -1$.

So no matter which of the three possible cases is true, we're still screwed: in every case, we always have a contradiction. We seem to have reached a dead end – a logically impossible conclusion. So what's wrong?

What's wrong is the *supposition*. It must be the case that the supposition is not true. Consequently, the statement "there exists a real number a such that $a^2 = -1$" must be false. In other words, -1 has no real square root. This completes the proof. □ [3]

The above proof is pretty wordy. When mathematicians write up proofs they leave out many of the details–and you should too. Following is a more typical proof:

Streamlined proof of Proposition 1 (suitable for writing up homework exercises)

The proof is by contradiction. Suppose $\exists a \in \mathbb{R}$ such that $a^2 = -1$ (note the symbol "$\exists$" means "there exists," the symbol $\mathbb{R}$ denotes the real numbers, and the expression "$a \in \mathbb{R}$" means that a is a real number).

There are two cases: either (i) $a \geq 0$ or (ii) $a < 0$.

In Case (i), then $a^2 = a \cdot a = (nonnegative) \cdot (nonnegative) \geqq 0$, which contradicts the supposition.

In Case (ii), then $a^2 = a \cdot a = (negative) \cdot (negative) > 0$, which contradicts the supposition.

By contradiction, it follows that -1 has no real square root. □

You may note that in the streamlined case, we reduced the number of cases from three to two. That's because we noticed that we really could combine the "positive" and the "zero" case into a single case.

Exercise 2. Imitate the proof of Propostion 1 to prove that -2 has no real fourth root. ♢

[3] The '□' symbol will be used to indicate the end of a proof. In other words: Ta-da!

Exercise 3. Try to use the method of Propostion 1 to prove that -4 has no real cube root. At what step does the method fail? ◊

Exercise 4.

(a) Sketch the function $f(x) = x^2 + 9$. Does the function have any real roots? Explain how you can use the graph to answer this question.

(b) Prove that the function $f(x) = x^2 + 9$ has no real roots. (You may prove by contradiction, as before).

(c) Graph the function $f(x) = x^6 + 7x^2 + 5$ (you may use a graphing calculator). Determine whether $f(x)$ has any real roots. *Prove* your answer (note: a picture is not a proof!).

◊

Exercise 4 underscores an important point. A graph can be a good visual aid, but it's not a mathematical proof. We will often use pictures and graphs to clarify things, but in the end we're only certain of what we can prove. After all, pictures can be misleading.

Exercise 5. *[4] Suppose that $a \cdot x^{2n} + b \cdot x^{2m} + a = 0$ has a real root, where a, b, m, n are nonzero integers. What can you conclude about the signs of a and b? *Prove* your answer. ◊

3.1.2 Unreal, but unavoidable

Mathematicians have known Proposition 1 for thousands of years, and for a long time that settled the question. Unfortunately, that nasty $\sqrt{-1}$ kept popping up in all sorts of inconvenient places. For example, about 400 years ago, it was very fashionable to study the roots of cubic polynomials such as $x^3 - 15x - 4 = 0$. A mathematician named Bombelli came up with a formula for a solution that eventually simplified to: $x = (2 + \sqrt{-1}) + (2 - \sqrt{-1})$. By cancelling out the $\sqrt{-1}$ terms, he got the correct solution $x = 4$. But how can you cancel something that doesn't exist?

Since mathematicians couldn't completely avoid those embarrassing $\sqrt{-1}$'s, they decided to put up with them as best they could. They called $\sqrt{-1}$ an

[4] Asterisks (*) indicate problems that are more difficult. Take the challenge!

imaginary number, just to emphasize that it wasn't up to par with the *real* numbers. They also used the symbol i to represent $\sqrt{-1}$, to make it less conspicuous (and easier to write). Finally, they created a larger set of numbers that included both real and imaginary numbers, called the *complex numbers.* [5]

Definition 6. The ***complex numbers*** are defined as

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

where $i^2 = -1$. If $z = a + bi$, then a is the ***real part*** of z and b is the ***imaginary part*** of z. (Note that the imaginary part of a complex number is a *real number*. It is the coefficient of i in the expression $z = a + bi$.) △

Examples of complex numbers include

- $1 + i$
- $5.387 - 6.432i$
- $\frac{1}{2} - \frac{\sqrt{3}}{2}i$
- $3i$ (equal to $0 + 3i$)
- 7.42 (equal to $7.42 + 0i$).
- 0 (equal to $0 + 0i$).

Exercise 7.

(a) Write down the complex number with real part 0 and imaginary part 7.

(b) Write down a complex number whose real part is the negative of its imaginary part.

(c) Write down a complex number that is also a real number.

◊

[5] The web site http://math.fullerton.edu/mathews/n2003/ComplexNumberOrigin.html gives more information about the origin of complex numbers.

3.1.3 A mathematical revolution

The creation of complex numbers was a revolutionary event in the history of mathematics. Mathematicians were forced to recognize that their beloved "real" numbers just weren't good enough to deal with the mathematical problems they were encountering. So they had to create a *new number system* (the complex numbers) with *new* symbols (i) and *new* arithmetic rules (like $i \cdot i = -1$).

In fact, this was not the first time that a controversial new number system was founded. The ancient Greeks thought that all numbers could be expressed as a ratio of integers $\frac{m}{n}$ — in other words, the Greeks thought all numbers were rational. It came as a huge shock when someone proved that some real numbers are *not* rational. We will presently give the original proof, but first we will need some properties odd and even integers:

Exercise 8.

(a) Fill in the blanks: The product of two odd integers is _____, and the product of two even integers is _____.

(b) Use proof by contradiction to prove the following statement: If m is an integer and m^2 is even, then m is also even. (*Hint*)

(c) It is possible to make a more general statement than part (b).Use proof by contradiction to prove the following statement: If m is an integer d is a positive integer, and m^d is even, then m is also even. (*Hint*)

$\Diamond$

Proposition 9. Given a right isosceles triangle where both legs have length 1 (see Figure 3.1) . Let x be the length of the hypotenuse. Then x is irrational–that is, it cannot be expressed as a ratio of integers.

PROOF. The proof is by contradiction. *Suppose* that x is rational: that is, $x = \frac{m}{n}$ for some integers m and n. We can always reduce a fraction to lowest terms, so we can assume m and n have no common factors.[6]

[6]Note that this is another one of those facts that "everyone knows", but is not easy to prove mathematically. We will make use of it in our current discussion, but note that technically it requires a proof.

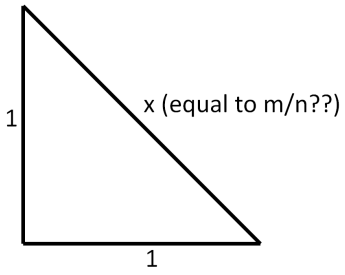


Figure 3.1. Isosceles right triangle

Since x is the hypotenuse of a right triangle, the Pythagorean Theorem gives us $x^2 = 1^2 + 1^2 = 2$. We can plug $x = \frac{m}{n}$ into $x^2 = 2$ to get $\left(\frac{m}{n}\right)^2 = 2$, which can be rearranged to give

$$m^2 = 2n^2. \tag{3.1}$$

From this we see that m^2 is divisible by 2, which means that m^2 is even. Exercise 8 part (b) then tells us that m is even, so there must be an integer j such that $m = 2j$. Plugging $m = 2j$ into Equation 3.1 gives $4j^2 = 2n^2$, which simplifies to $2j^2 = n^2$. Hence n^2 is even, and as before we conclude that n is even. So $n = 2k$ for some integer k.

At this point, we have $m = 2j$ and $n = 2k$, which means that m and n have a common factor of 2. But at the beginning of the proof, we said that m and n were reduced to lowest terms, so they have no common factor. This is a contradiction. Therefore our *supposition* must be false, so x cannot be rational. □

We have seen in our proofs that whenever we make a statement, we also need to give a reason that justifies the statement. In many cases, it's possible to state a proof very succinctly in "statement−reason" format. For instance, here is a "statement−reason" proof of Proposition 9:

Statement	Reason
x is the hypoteneuse of the right triangle in Figure 3.1	Given
x is rational	*supposition* (will be contradicted)
$x^2 = 2$	Pythagorean Theorem
$x = m/n$ where m, n are integers	Definition of rational
m, n are relatively prime	Fraction can always be reduced
$(m/n)^2 = 2$	Substitution
$m^2 = 2n^2$	Rearrangement
$m = 2k$ where k is an integer	Exercise 8 part (b)
$(2k/n)^2 = 2$	Substitution
$n^2 = 2k^2$	Rearrangement
$n = 2j$ where j is an integer	Exercise 8 part (b)
m and n are not relatively prime	Definition of relatively prime
supposition is false	Contradictory statements
x cannot be rational	Negation of supposition

Note that the preceding proof amounts to a proof that $\sqrt{2}$ is irrational, since we know that $\sqrt{2}$ is the length of the hypothesis in question. Given the results of Exercise 8, we can use a similar proof to find more irrational numbers.

Exercise 10.

(a) Prove that the cube root of 2 is irrational. (*Hint*)

(b) Prove that the nth root of 2 is irrational, if n is a positive integer greater than 1.

(c) Prove that $2^{1/n}$ is irrational, if n is a negative integer less than -1.

$\Diamond$

In the proof of Proposition 9, we "plugged in" or substituted one expression for another. For example, when we discovered that m was divisible by 2 we substituted $2j$ for m, which was useful for the algebra that followed. *Substitution* is a key technique used throughout all of abstract algebra.

Exercise 11. Use substitution to prove the following statement: if $3|n$ and $4|m$, then $12|mn$ (the notation "$3|n$" means that 3 divides n). (*Hint*) $\Diamond$

Exercise 12. Use substitution to prove the following statement: if $12|n$ and $n|4m$, where n and m are integers, then $3|m$. (*Hint*) ♢

We should also come clean and admit that our proof of Proposition 9 falls short of true mathematical rigor. The reason is that we made use of Exercise 8, and we never actually *proved* part (a) of the exercise. Even though it's something that "everybody knows", mathematicians still want a proof! Now, part (a) is a consequence of the following more general proposition, which is known as ***Euclid's Lemma***:

Proposition 13. Let a and b be integers, and let p be a prime number. Then either p divides a, or p divides b.

Remark 14. In mathematics, when we say "either X is true or Y is true", we also include the possibility that both X and Y are true. So in this case, when we say "p divides a, or p divides b", it's possible that p divides both a and b. △

Proof. We're not ready to give a proof yet, but we'll give one later (see Exercise 86 in Section 4.5.4). □

Exercise 15. Modify the proof of Proposition 9 to prove that $\sqrt{3}$ is irrational. (You will find Proposition 13 to be useful in the proof.) ♢

Exercise 16. Prove that $\sqrt{6}$ is irrational. ♢

Exercise 17. Prove that $p^{1/n}$ is irrational, if p is a prime and n is any integer with $|n| > 1$. ♢

The inconvenient truth expressed in Proposition 9 forced mathematicians to extend the 'real' numbers to include *irrational* as well as *rational* numbers. But complex numbers opened the floodgates by setting a precedent. New generations of mathematicians became so used to working with "unreal" numbers that they thought nothing of making up other number systems! Within a few centuries after the complex numbers, several new number systems were created; and eventually there were so many that mathematicians started studying the properties of general numbers systems. This was the beginning of what we today call abstract algebra!

To close this section, here's another exercise to practice using substitution:

Exercise 18.

(a) Suppose that:

- a is a negative number;
- n is a positive integer;
- the equation $x^n = a$ has a real solution for the unknown x.

What can you conclude about n? Make a clear statement and *prove* your statement. (*Hint*)

(b) Replace the condition "n is a positive integer" in part (a) with "n is a negative integer." Now what can you conclude about n? Make a clear statement and *prove* your statement.

◊

Exercise 19. Do imaginary numbers "really" exist? Write two or three sentences to express your opinion.[7] ◊

3.2 Arithmetic with complex numbers

3.2.1 Complex arithmetic

To add two complex numbers $z = a + bi$ and $w = c + di$, we just add the corresponding real and imaginary parts:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Using this definition, we may prove directly that complex addition (like regular addition) is commutative:[8]

Proposition 20. Addition on complex numbers is commutative.

[7] There is no "right" answer to this question.

[8] It is important to realize that this *must* be proved and *can't* just be assumed. Later on we will define operations that are *not* commutative.

PROOF. We just need to show that for any two complex numbers z and w, it's always true that $z + w = w + z$. Writing $z = a + bi$ and $w = c + di$ as above, the proof using statement-reason format runs as follows:

Statement	Reason
$z + w = (a + bi) + (c + di)$	substitution
$= (a + c) + (b + d)i$	definition of complex addition
$= (c + a) + (d + b)i$	real addition is commutative
$= (c + di) + (a + bi)$	def. of complex addition
$= w + z.$	substitution

□

Notice how we started in this proof with one side of the equality, and through a series of steps ended up with the other side. This is a good method to follow, when you're trying to prove two things are equal.

Exercise 21. Prove that addition on complex numbers is associative. ◊

Now that we have addition worked out, let's do multiplication. We observe that the complex number $a + bi$ looks just like the polynomial $a + bx$, except the imaginary i replaces the unknown x. So we'll take a cue from polynomial multiplication, and multiply complex numbers just like polynomial factors, using the FOIL (first, outside, inside, last) method. (Actually, with complex numbers it's more convenient to use FLOI (first, last, outside, inside) instead.) The product of z and w is

$$(a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i.$$

Question: How did we get rid of the i^2 in the final equality? Answer: Remember, we defined $i^2 = -1$, and we just made the substitution.

A bevy of nice properties follow from this definition:

Example 22. Complex multiplication is commutative. This may be proved as follows. (Note that here we are combining statement−reason and paragraph proof formats. It's OK to mix and match formats, as long as you get the job done!)

$$\begin{aligned} (a + bi)(c + di) &= (ac - bd) + (bc + ad)i && \text{(FLOI)} \\ &= (ca - db) + (cb + da)i && \text{(commutativity of real multiplication)} \end{aligned}$$

On the other hand:

$$(c + di)(a + bi) = (ca - db) + (cb + da)i \qquad \text{(FLOI)}$$

Since we obtain the same expression for $(a+bi)(c+di)$ and $(c+di)(a+bi)$, it follows that $(a+bi)(c+di) = (c+di)(a+bi)$. ♦

Similar proofs can be given for other multiplicative properties:

Exercise 23. Prove the associative law for multiplication of nonzero complex numbers. (Follow the style of Example 22). ◊

Exercise 24. Prove the distributive law for complex arithmetic: that is, if u, w, and z are complex numbers, then $(u)(w+z) = uw + uz$. ◊

Two arithmetic operations down, two to go! Let's consider subtraction of complex numbers. We may define $z - w$ using complex addition and multiplication as: $z - w = z + (-1) \cdot w$.

Exercise 25. Using this definition of complex subtraction, Given that $z = a + bi$ and $w = c + di$ then express $z - w$ as (Real part) + (Imaginary part)i. ◊

Division is a little more complicated. First we consider division of a complex number by a real number. In this case we can define division as multiplication by the reciprocal, just as with real numbers:

$$\frac{a+bi}{c} = (a+bi) \cdot \frac{1}{c} = a \cdot \frac{1}{c} + (bi) \cdot \frac{1}{c} = \frac{a}{c} + \cdot\frac{b}{c}i, \tag{3.2}$$

where we have used the distributive, associative, and commutative properties of complex multiplication.

Now let's try to make sense of the ratio of two complex numbers: $w/z = (c+di)/(a+bi)$. This notation suggests that it should be true that $w/z = (c+di) \cdot 1/(a+bi)$. But what is $1/(a+bi)$? To understand this, let's go back to arithmetic with real numbers. If we have an ordinary real number r, then $1/r$ is the *multiplicative inverse* of r: that is, $r \cdot 1/r = 1/r \cdot r = 1$. We also write $1/r$ as r^{-1}. By analogy, to make sense of $1/z = 1/(a+bi)$, we need to find a complex number z^{-1} such that $z^{-1} \cdot z = z \cdot z^{-1} = 1$.

Exercise 26. Given that $z = a + bi$ is a complex number and $z \neq 0$ (recall that 0 is the same as $0 + 0i$). Show that the complex number

$$z^{-1} = \frac{a - bi}{a^2 + b^2}.$$

satisfies $zz^{-1} = z^{-1}z = 1$, where $z = a + bi$. (*Hint*) $\Diamond$

Based on the previous exercise, we finally arrive at the formula for dividing two complex numbers:

$$\frac{c+di}{a+bi} = (c+di) \cdot \frac{a-bi}{a^2+b^2},$$

or alternatively

$$\frac{c+di}{a+bi} = \frac{a-bi}{a^2+b^2} \cdot (c+di).$$

(These formulas holds as long as $a + bi \neq 0$).

It seems obvious that we should be able to write this formula more compactly as

$$\frac{c+di}{a+bi} = \frac{(c+di)(a-bi)}{a^2+b^2},$$

and in fact we can. This is because the distributive and associative laws once again comes to our rescue. Starting with the first expression above for $(c + di)/(a + bi)$ we have:

$$\begin{aligned}
\frac{c+di}{a+bi} &= (c+di) \cdot \frac{a-bi}{a^2+b^2} && \text{(from above)} \\
&= (c+di) \cdot \left((a-bi) \cdot \frac{1}{a^2+b^2} \right) && \text{(distributive law)} \\
&= ((c+di) \cdot (a-bi)) \cdot \frac{1}{a^2+b^2} && \text{(associative law)} \\
&= \frac{(c+di) \cdot (a-bi)}{a^2+b^2} && \text{(definition of division).}
\end{aligned}$$

We summarize the formulas for complex addition, multiplication, and division below:

- Addition: $(a + bi) + (c + di) = (a + c) + (b + d)i$
- Multiplication: $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$
- Division: $\dfrac{c+di}{a+bi} = \dfrac{(c+di)(a-bi)}{a^2+b^2}$

Exercise 27. Evaluate each of the following.

(a) $(3-2i)+(5i-6)$

(b) $(5-4i)(7+2i)$

(c) $(\sqrt{7}+\sqrt{6}i)(\sqrt{7}-\sqrt{6}i)$

(d) $(a-bi)(a+bi)$

(e) $(a+bi)(b+ai)$

(f) $(2+\sqrt{3}i)^2$

(g) $(1+i)(-1+i)(-1-i)(1-i)$

(h) $(\sqrt{3}+i)(-1+\sqrt{3}i)(-\sqrt{3}-i)(1-\sqrt{3}i)$

(i) $\left(\sqrt{5+\sqrt{5}}+i\sqrt{5-\sqrt{5}}\right)^4$ (*Hint*)

(j) $\dfrac{1+2i}{2-3i}$

(k) $\dfrac{a+bi}{b-ai}$

(l) $\dfrac{1+i}{1-i}+\dfrac{1-i}{1+i}$

(m) $\dfrac{\sqrt{3}-\sqrt{5}i}{\sqrt{5}+\sqrt{3}i}$

(n) i^{45} (*Hint*)

(o) $(1+i)^4$ (*Hint*)

(p) $(1+i)^{41}$

(q) $(1+\sqrt{3}i)^{11}$

(r) $i^{1001}+i^{1003}$

◊

Exercise 28. If the nonzero complex number z has equal real and imaginary parts, then what can you conclude about z^2? What can you conclude about z^4? (*Hint*) ◊

Exercise 29. $z=3+i$ is a solution to $z^2-6z+k=0$. What is the value of k? ◊

You are probably familiar with the fact that the product of two nonzero real numbers is also nonzero. Is the same true for complex numbers? The answer is yes.

Proposition 30. Given that $z=a+bi$, $w=c+di$, and $z\cdot w=0$. Then it must be true that either $z=0$ or $w=0$.

The proof of Proposition 30 is outlined in the following exercise.

Exercise 31. Complete the proof of Proposition 30 by filling in the blanks.

(a) The proof is by contradiction. So we begin by *supposing* $z \neq$ ____ and $w \neq$ ____.

(b) Since $z \neq$ ____, it follows that z has an inverse z^{-1} such that $z^{-1} \cdot z =$ ____.

(c) Since $z \cdot w = 0$, we can multiply both sides of this equation by ____ and obtain the equation $w =$ ____. This equation contradicts the *supposition* that ____.

(d) Since our supposition has led to a false conclusion, it follows that our supposition must be ____. Therefore it cannot be true that ____, so it must be true that ____.

$\Diamond$

3.2.2 Comparison of integer, rational, real and complex addition properties

It is obvious that addition with integers, rational numbers, and real numbers have very similar properties. In this section, we explore some of these properties.

For instance, integers have an ***additive identity***, that is, one special unique integer that can be added to any integer without changing that integer. The additive identity of the integers is 0, because for instance $5+0=5$ and $0+5=5$. In general, if we let n be an arbitrary integer, then $n+0=0+n=n$. It's pretty easy to see that 0 is also the additive identity of the rationals, and the additive identity of the reals.

Every integer also has an ***additive inverse***,that is a corresponding number that can be added to the integer such that the sum is the additive identity (that is, 0). For example, the additive inverse of the number 5 is -5, because $5+(-5)=0$ and $(-5)+5=0$. In general, if we let n be an arbitrary integer, then $n+(-n)=(-n)+n=0$.

Notice an **important difference** between additive identity and additive inverse: the number 0 is the identity for all integers, but each integer has a *different* inverse.

Exercise 32. Complete all entries of Table 3.1, which shows the additive properties of integers, rationals, reals, and complex numbers.

$\Diamond$

	Integers (n, m, k)	Rationals $(\frac{n}{m}, \frac{p}{q}, \frac{j}{k})$	Reals (x, y, z)	Complex $(a+bi, c+di, e+fi)$
Additive identity	$n+0=0+n=n$	$\frac{n}{m}+0=0+\frac{n}{m}=\frac{n}{m}$	$x+0=0+x=x$	$(a+bi)+$ ____ $=$ ____$+(a+bi)=$ ____
Additive inverse	$n+(-n)=(-n)+n=0$	$\frac{n}{m}+$ ____ $=$ ___$+\frac{n}{m}=$ ___		
Associative law	$n+(m+k)=(n+m)+k$	$\frac{n}{m}+(\frac{p}{q}+\frac{j}{k})=$ _____		
Commutative law	$n+m=m+n$			

Table 3.1: Additive properties of different number systems

3.2.3 Comparison of integer, rational, real and complex multiplication properties

Just as we've talked about the *additive* identity and inverse for different number systems, in the same way we can talk about the *multiplicative* identity and inverse for different number systems.

The integers have multiplicative identity 1 because $n \cdot 1 = 1 \cdot n = n$. However, most integers do *not* have a multiplicative inverse. Take the number 5, for example. There is no *integer* that multiplies 5 to give 1 (of course, $5 \cdot \frac{1}{5} = \frac{1}{5} \cdot 5 = 1$, but $\frac{1}{5}$ is not an integer, so it doesn't count).

On the other hand, the real numbers do have multiplicative inverses, with just one exception.

Exercise 33. Which real number does not have a multiplicative inverse? *Explain* your answer. ◊

Exercise 34. Complete all entries of Table 3.2, which shows the multiplicative properties of *nonzero* rationals, reals, and complex numbers.

◊

Exercise 35. Prove FOIL for complex numbers: that is, if u, v, w, and z are complex numbers, then $(u+v)(w+z) = uw + uz + vw + vz$. ◊

	Rationals ($\frac{n}{m}$, $\frac{p}{q}$, $\frac{j}{k}$)	Reals (x,y,z)	Complex ($a+bi$, $c+di$,$e+fi$)
Multiplicative identity		$x \cdot 1 = 1 \cdot x = x$	$(a+bi) \cdot \_\_ = \_\_ \cdot (a+bi) = \_\_\_$
Multiplicative inverse		$x \cdot \frac{1}{x} = \frac{1}{x} \cdot x =$ 1 if x $\neq 0$	
Associative law		$x(yz) = (xy)z$	
Commutative law		$xy = yx$	

Table 3.2: Multiplicative properties of different number systems

3.2.4 Modulus and complex conjugate

We are familiar with the absolute value of a real number: for instance, $|-\sqrt{7}| = \sqrt{7}$. In general, for a real number x the absolute value can be defined as $|x| \equiv +\sqrt{x^2}$.

Definition 36. For a complex number z, the ***absolute value*** or ***modulus*** of $z = a + bi$ is $|z| = \sqrt{a^2 + b^2}$. △

Complex numbers have an additional operation that real numbers do not have.

Definition 37. The ***complex conjugate*** of a complex number $z = a + bi$ is defined to be $\overline{z} = a - bi$. △

Example 38. Let $z = 2 + 3i$ and $w = 1 - 2i$. Then

$$z + w = (2 + 3i) + (1 - 2i) = 3 + i$$

and

$$zw = (2 + 3i)(1 - 2i) = 8 - i.$$

Also,

$$z^{-1} = \frac{2}{13} - \frac{3}{13}i$$
$$|z| = \sqrt{13}$$
$$\overline{z} = 2 - 3i.$$

♦

Exercise 39. Evaluate each of the following.

(a) $\overline{i}$

(b) $(4-5i)-\overline{(4i-4)}$

(c) $(9-i)\overline{(9-i)}$

(d) $(3+4i)+\overline{(3+4i)}$

(e) $(\sqrt{7}+8i)-\overline{(\sqrt{7}+8i)}$

(f) $\left(\overline{\sqrt{3}-i}\right)^{-1}$

(g) $\overline{\left(\sqrt{3}-i\right)^{-1}}$

(h) $\left(\overline{\left(\overline{4-9i}\right)^{-1}}\right)^{-1}$

(i) $(a+bi)\overline{(a+bi)}$

(j) $(a+bi)+\overline{(a+bi)}$

◊

Here is an example of a proposition involving complex conjugates.

Proposition 40. Given z and w are complex numbers, then $\overline{z}+\overline{w}=\overline{z+w}$.

PROOF. We may write z as $a+bi$ and w as $c+di$. Then

$$\begin{aligned}
\overline{z}+\overline{w} &= \overline{a+bi}+\overline{c+di} \\
&= (a-bi)+(c-di) && \text{by definition of conjugate} \\
&= (a+c)-(b+d)i && \text{by basic algebra} \\
&= \overline{(a+c)+(b+d)i} && \text{by definition of conjugate} \\
&= \overline{z+w} && \text{by definition of complex addition}
\end{aligned}$$

□

Exercise 41. Prove each of the following statements (follow the style of Proposition 40).

(a) $(\overline{z})(\overline{w})=\overline{(zw)}$

(b) If a is real, then $a\overline{z}=\overline{az}$

(c) $|z|=|\overline{z}|$

(d) $z\overline{z}=|z|^2$

(e) $|zw|=|z||w|$

(f) $|z|^3=|z^3|$ (*Hint*)

(g) $z^{-1} = \dfrac{\overline{z}}{|z|^2}$ (*Hint*)

(h) $|z^{-1}| = \dfrac{1}{|z|}$ (*Hint*)

(i) $(\overline{z})^{-1} = \overline{(z^{-1})}$

◊

Exercise 42.

(a) Show that the complex number $z = a + bi$ is a pure real number if and only if $\overline{z} = z$. (*Note* that you actually need to prove two things here: (i) If z is real, then $\overline{z} = z$; (ii) If $\overline{z} = z$, then z is real).

(b) In view of part (a), complete the following statement: "The complex number $z = a+bi$ is a pure imaginary number if and only if $\overline{z} = \ldots\ldots$" *Prove* your statement.

◊

Now that we have proved properties of complex numbers in the previous two exercises, we may make use of these properties to prove facts about complex numbers without having to write everything out as $a + bi$.

Exercise 43. * If $|z| = 1$ and $z \neq 1$, show that $\frac{z-1}{z+1}$ is a pure imaginary number. (*Hint*) ◊

Exercise 44.

(a) *Show that for any nonzero complex number z, the absolute value of $z + \bar{z}^{-1}$ is greater than $\sqrt{(3)}$. (*Hint*)

(b) Give an example of z such that $|z + \bar{z}^{-1}| = 2$.

(c) Give three additional examples of z such that $|z + \bar{z}^{-1}| = 2$.

(d) **Show that for any nonzero complex number z, $|z+\bar{z}^{-1}| \geq 2$. (*Hint*)

(e) Show by example that part (d) is *not* true if $z + \bar{z}^{-1}$ is replaced with $z + z^{-1}$. Find the smallest possible value for $|z + z^{-1}|$.

◊

Exercise 45. The intricate *Mandelbrot set* (see Figure 3.2) is a beautiful application of complex numbers. The Mandelbrot set is defined by means of *iteration* of the function $f(z) = z^2 + c$. The definition is a little complicated: we show how it works using a couple of examples.

First consider $c = 1$, so $f(z) = z^2 + 1$. We start with $z = 0$, which gives $f(0) = 1$; and we iterate by evaluating the function on the result of the previous evaluation. So we compute $f(1) = 2, f(2) = 5, f(5) = 26, \ldots$. It is clear that $|f(z)|$ is getting larger and larger after repeated iterations.

On the other hand, if we use $c = i$ and start with $z = 0$, we get $f(0) = i$ at first, and repeated iteration gives $f(i) = -1 + i, f(-1 + i) = i, f(i) = -1 + i, \ldots$ so that this time $|f(z)|$ doesn't continue to grow indefinitely after repeated iterations.

The Mandelbrot set is defined to be the set of values c for which the iterations do *not* grow indefinitely upon iteration. Thus i is in the Mandelbrot set, while 1 is not.

Which of the following numbers is in the Mandelbrot set? *Demonstrate* your answer.

(a) $c = 0$

(b) $c = -1$

(c) $c = -i$

(d) $c = 1 + i$

◊

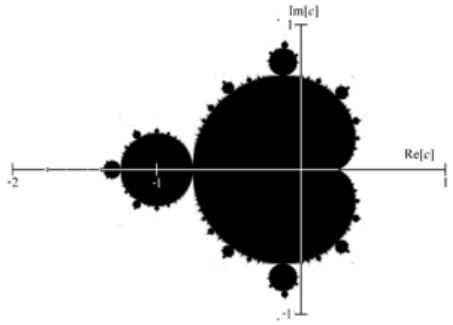


Figure 3.2. Mandelbrot set (from Wikipedia): the set is colored black.

Exercise 46. (*for geeks*)

(a) Write an Excel spreadsheet that can multiply two complex numbers. Put the real and imaginary parts of the first number in cells A1 and B1; Put the real and imaginary parts of the second number in cells C1 and D1; Put the real and imaginary parts of the result in cells E1 and F1. Use your sheet to compute $(3+4i)(7-8i)$.

(b) Modify your Excel sheet to compute the square of a complex number. Put the real and imaginary parts of the first number in cells A1 and B1; Put the real and imaginary parts of the result in cells C1 and D1. Use your sheet to compute $(12-5i)^2$.

(c) (*for ubergeeks*) Modify your Excel sheet to compute $z^2, (z^2)^2, ((z^2)^2)^2, \ldots$ (10 number altogether) for a given complex number z. Put the real and imaginary parts of z in cells A1 and B1; Put the real and imaginary parts of the results in columns C and D. Use your sheet with $z = 1 + 0.25i$. Plot the results as 10 points in the plane (use Scatter Plot).

(d) (*for super-ubergeeks*) Modify your Excel sheet to compute the first 100 iterates of the function $f(z) = z^2 + c$ for given complex numbers z, c (see Exercise 45). Put the real and imaginary parts of z in cells A1 and B1; Put the real and imaginary parts of c in cells A2 and B2; put the results in columns C and D. Using your sheet, determine which of the following numbers is in the Mandelbrot set: (i) $z = -1.04039 + 0.2509294i$; (ii) $z = -0.1155989 + 0.7639405$.

$\Diamond$

3.3 Alternative representations of complex numbers

3.3.1 Cartesian representation of complex numbers

There are several ways to represent complex numbers, that have different conceptual advantages. For instance, a complex number $z = a + bi$ can be considered simply as a pair of real numbers (a, b), where the first number is the real part and the second number is the imaginary part. We are used to plotting ordered pairs (a, b) on an xy plane, where a is the x coordinate

and b is the y coordinate. Representing a complex number in this way as an ordered pair (a, b) is called the ***rectangular*** or ***Cartesian*** representation. The rectangular representations of $z_1 = 2+3i$, $z_2 = 1-2i$, and $z_3 = -3+2i$ are depicted in Figure 3.3.

Often the notation $a + bi$ is also referred to as "rectangular representation", since it's so similar to (a, b). In the following, we will refer to $a + bi$ as the "rectangular form" of the complex number z.

Mathematicians naturally think of complex numbers as points on a plane – in fact, the complex numbers are often referred to as the "complex plane".

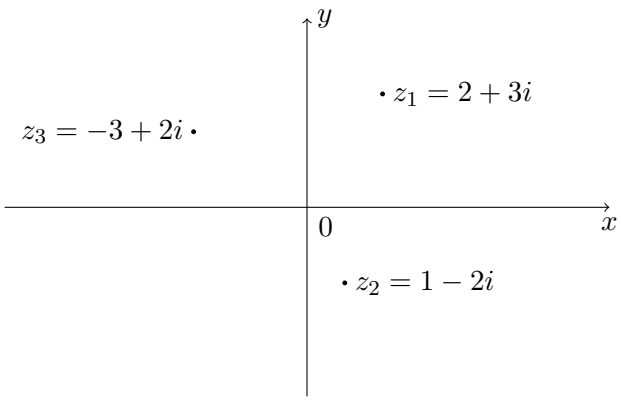


Figure 3.3. Rectangular coordinates of a complex number

3.3.2 Vector representation of complex numbers

You should already know that a point in a plane can also be considered as a *vector*: in other words, the ordered pair (a, b) can be identified with the vector $a\mathbf{i} + b\,\mathbf{j}$, where $\mathbf{i}$ and $\mathbf{j}$ are the unit vectors in the $x+$ and $y+$ directions, respectively. So complex numbers can also be considered as two-dimensional vectors.

Exercise 47.

(a) Write the numbers $3 + 7i$ and $-5 + 9i$ as vectors.

(b) Find the sum of the two vectors that you found in (a).

(c) Find the sum$(3 + 7i) + (-5 + 9i)$

(d) What is the relation between your answers to (b) and (c)? Explain.

$\Diamond$

Although the preceding exercise may seem sort of pointless, in fact it is extremely significant. This is our first example of an *isomorphism*: a correspondence between mathematical systems that are essentially identical. At this point we will not give a formal definition of isomorphism, but to get the gist of the idea consider two mathematicians (Stan and Ollie) with very different tastes. Stan thinks geometrically, so he always thinks of complex numbers as vectors in a plane; while Ollie thinks algebraically, so he writes complex numbers as $a + bi$. If Stan and Ollie work on the same problem involving complex addition, even though Stan's answer will be a vector and Ollie's will look like $a + bi$, their answers will always agree (that is, if they both do the problem right).

Of course this correspondence between complex numbers and vectors breaks down when we consider multiplication, because we have never seen multiplication of 2-D vectors before. But it works perfectly well if we stick with addition.

3.3.3 Polar representation of complex numbers

Nonzero complex numbers can also be represented using ***polar coordinates***. To specify any nonzero point on the plane, it suffices to give an angle θ from the positive x axis in the counterclockwise direction and a distance r from the origin, as in Figure 3.4. The distance r is the absolute value or modulus defined previously, while the angle θ is called the ***argument*** of the complex number z.

3.3.4 Converting between rectangular and polar form

We can see from the figure that

$$z = a + bi = r(\cos\theta + i\sin\theta).$$

Hence,

$$r = |z| = \sqrt{a^2 + b^2}$$

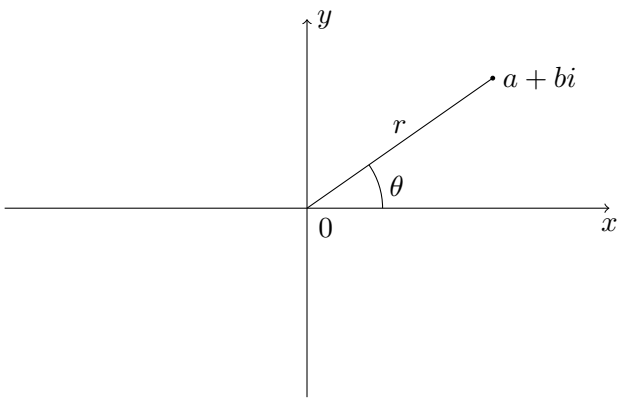


Figure 3.4. Polar coordinates of a complex number

and

$$a = r\cos\theta$$
$$b = r\sin\theta.$$

We will frequently use the abbreviation

$$\operatorname{cis}\theta := \cos\theta + i\sin\theta$$

(note the symbol ":=" means "is defined as"), so that

$$r\operatorname{cis}\theta := r(\cos\theta + i\sin\theta).$$

We know from trigonometry that adding 2π to θ does not change $\cos\theta$ or $\sin\theta$. This means for example that the following complex numbers are equal: $2.6\operatorname{cis}\left(\frac{\pi}{9}\right), 2.6\operatorname{cis}\left(2\pi+\frac{\pi}{9}\right), 2.6\operatorname{cis}\left(-2\pi+\frac{\pi}{9}\right), \ldots$. However, we can always find a θ between 0 and 2π such that $z = r\operatorname{cis}\theta$; so the standard representation of $z = r\operatorname{cis}\theta$ has $0 \le \theta < 2\pi$.

Example 48. Let $z = 2\operatorname{cis}\frac{\pi}{3}$. Then

$$a = 2\cos\frac{\pi}{3} = 1$$

and

$$b = 2\sin\frac{\pi}{3} = \sqrt{3}.$$

Hence, the rectangular representation is $z = 1 + \sqrt{3}\,i$. ♦

Conversely, if we are given a rectangular representation of a complex number, it is often useful to know the number's polar representation.

Example 49. Let $z = 3\sqrt{2} - 3\sqrt{2}\,i$ (see Figure 3.5). Then the modulus of z is

$$r = \sqrt{a^2 + b^2} = \sqrt{36} = 6.$$

We can find the argument θ by noticing that the tangent is equal to $\frac{-3\sqrt{2}}{3\sqrt{2}}$ or -1. This means that $\theta = \arctan(-1)$. Since the angle is in the fourth quadrant, this means that $\theta = \frac{7\pi}{4}$.

In general, for the complex number $a + b\,i$ we have

$$\theta = \arctan\left(\frac{b}{a}\right),$$

where we must be careful to choose the value of θ corresponding to the quadrant where $a + b\,i$ is located. ♦

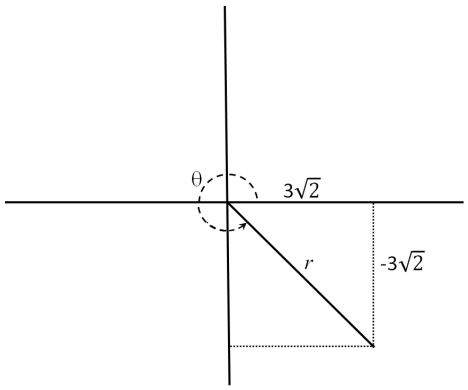


Figure 3.5. Modulus and argument of $z = 3\sqrt{2} - 3\sqrt{2}\,i$

Exercise 50. Convert the following complex numbers to rectangular form (that is, write as $a + bi$). Give *exact* answers and not decimals (use square roots if necessary).

(a) $2\,\mathrm{cis}(\pi/6)$

(b) $5\,\mathrm{cis}(9\pi/4)$

(c) $3\,\mathrm{cis}(\pi)$

(d) $\dfrac{\mathrm{cis}(7\pi/4)}{2}$

(e) $\sqrt{2}\,\mathrm{cis}(5\pi/3)$

(f) $\frac{1}{\sqrt{7}}\,\mathrm{cis}(-7\pi/6)$

(g) $14\,\mathrm{cis}(30\pi/12)$

$\Diamond$

Exercise 51. Convert the following complex numbers to polar representation (Give exact answers, no decimal approximations).

(a) $1-i$

(b) $-1+i$

(c) -5

(d) $2+2i$

(e) $-2-2i$

(f) $\sqrt{3}+i$

(g) $-3i$

(h) $2i+2\sqrt{3}$

(i) $\sqrt{6}-\sqrt{6}i$

(j) $-3\sqrt{2}-\sqrt{6}i$

(k) $-\sqrt{50}-\sqrt{50}i$

$\Diamond$

Exercise 52. There is a very close relationship between plane geometry and complex numbers.

(a) Consider the following set of complex numbers:

$$\{z \text{ such that } |z| < 2.\}$$

In the complex plane, what does this set look like?

(b) Use complex numbers to specify the set of all points on a circle of radius 5 with center at the origin (your answer should look like the set specification given in part (a)).

(c) Consider the following set of complex numbers:

$$\{z \text{ such that } |z-i| = 2.\}$$

In the complex plane, what does this set look like?

(d) Use complex numbers to specify the set of all points on a circle of radius 3 that passes through the origin and has center on the positive x-axis.

$\Diamond$

3.3.5 Multiplication and powers in complex polar form

The polar representation of a complex number makes it easy to find products, quotients, and powers of complex numbers.

Proposition 53. Let $z = r\,\mathrm{cis}\,\theta$ and $w = s\,\mathrm{cis}\,\phi$ be two nonzero complex numbers. Then

$$z \cdot w = rs\,\mathrm{cis}(\theta + \phi).$$

Alternatively, we may write

$$r\,\mathrm{cis}\,\theta \cdot s\,\mathrm{cis}\,\phi = rs\,\mathrm{cis}(\theta + \phi).$$

PROOF. The proof uses the following trigonometric formulas (surely you remember them!):

$$\begin{aligned}\cos(\theta + \phi) &= \cos\theta\cos\phi - \sin\theta\sin\phi \\ \sin(\theta + \phi) &= \cos\theta \cdot \sin\phi + \sin\theta \cdot \cos\phi\end{aligned}$$

Exercise 54. Fill in the blanks to complete the proof:

$$\begin{aligned}z \cdot w &= r\,\mathrm{cis}\,\theta \cdot (\_\_\_\_\_) \\ &= r\,(\cos\theta + i\sin(\_\_\_\_\_)) \cdot s\,(\_\_\_\_\_) \\ &= rs \cdot (\cos\theta + i\sin(\_\_\_\_\_)) \cdot (\_\_\_\_\_) \\ &= rs\,((\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\_\_\_\_\_)) \\ &= rs\,(\cos(\theta + \phi) + i\sin(\_\_\_\_\_)) \\ &= rs\,\mathrm{cis}(\_\_\_\_\_)\end{aligned}$$

◊

□

We will also want to divide complex numbers in polar form. But first, we need to characterize multiplicative inverses. Note for example that $[2\,\mathrm{cis}(3\pi/4)]^{-1} = (1/2)\,\mathrm{cis}(-3\pi/4)$ since

$$2\,\mathrm{cis}(3\pi/4) \cdot (1/2)\,\mathrm{cis}(-3\pi/4) = 2 \cdot (1/2) \cdot \mathrm{cis}(3\pi/4 - 3\pi/4) = \mathrm{cis}(0) = 1,$$

and similarly

$$(1/2)\operatorname{cis}(-3\pi/4)\cdot 2\operatorname{cis}(3\pi/4) = \operatorname{cis}(0) = 1.$$

Exercise 55.

(a) Let $z = 13\operatorname{cis}\left(\frac{5\pi}{7}\right)$. Find a complex number w (in complex polar form) such that $zw = wz = 1$. Write w so that its argument is between 0 and 2π. What is the sum of the arguments of z and w?

(b) Let $z = \frac{3}{8}\operatorname{cis}(0.39\pi)$. Find a complex number w (in complex polar form) such that $zw = wz = 1$. Write w so that its argument is between 0 and 2π. What is the sum of the arguments of z and w?

(c) Given that $z = r\operatorname{cis}\theta$ and $w = s\operatorname{cis}\phi$. Determine what s and ϕ must be so that $w = z^{-1}$. That is, find a value for s and ϕ so that

$$z \cdot s\operatorname{cis}\phi = s\operatorname{cis}\phi \cdot z = 1.$$

Specify ϕ in such a way that it lies in the interval $[0, 2\pi]$.

$\Diamond$

From Exercise 55 we may deduce that the inverse of a complex number $w = s\operatorname{cis}\phi$ is

$$w^{-1} = \frac{1}{s}\operatorname{cis}(2\pi - \phi),$$

which we could also write as

$$w^{-1} = \frac{1}{s}\operatorname{cis}(-\phi)$$

since changing the argument by 2π does not change the value of the number.

Now recall that to divide two complex numbers z and w, we rewrite $\frac{z}{w}$ as $z \cdot w^{-1}$. So with $z = r\operatorname{cis}\theta$ and $w = s\operatorname{cis}\phi$ we may divide as follows:

$$\frac{z}{w} = (r\operatorname{cis}\theta)\cdot\left(\frac{1}{s}\operatorname{cis}(-\phi)\right) = \frac{r}{s}\operatorname{cis}(\theta - \phi).$$

The previous discussion proves the following proposition.

Proposition 56. Let $z = r\operatorname{cis}\theta$ and $w = s\operatorname{cis}\phi$ be two nonzero complex numbers. Then

$$\frac{z}{w} = \frac{r}{s}\operatorname{cis}(\theta - \phi).$$

Alternatively, we may write

$$\frac{r\,\mathrm{cis}\,\theta}{s\,\mathrm{cis}\,\phi} = \frac{r}{s}\,\mathrm{cis}(\theta - \phi).$$

In summary, multiplication and division of complex numbers in polar form proceeds as follows:

Multiplication:

- Multiply the two moduli together to get the modulus of the product.
- Add the two arguments together to get the argument of the product.

Division:

- Divide the modulus of the numerator by the modulus of the denominator to get the modulus of the quotient.
- Subtract the argument of the denominator from the argument of the numerator to get the argument of the quotient.

Example 57. If $z = 3\,\mathrm{cis}(\pi/3)$ and $w = 2\,\mathrm{cis}(\pi/6)$, then

$$zw = (2 \cdot 3)\,\mathrm{cis}(\pi/3 + \pi/6) = 6\,\mathrm{cis}(\pi/2) = 6i.$$

♦

Exercise 58. Calculate each of the following products using complex polar arithmetic. Give the answer in rectangular form if you can do so without using roots or decimals. Otherwise, leave the answer in polar form.

(a) $2\,\mathrm{cis}\left(\frac{\pi}{4}\right) \cdot \frac{1}{2}\,\mathrm{cis}\left(\frac{3\pi}{4}\right)$

(b) $14\,\mathrm{cis}\left(\frac{6\pi}{5}\right) \cdot \frac{1}{7}\,\mathrm{cis}\left(\frac{4\pi}{5}\right)$

(c) $\mathrm{cis}\left(\frac{9\pi}{7}\right) \cdot 2\,\mathrm{cis}\left(\frac{8\pi}{7}\right) \cdot 3\,\mathrm{cis}\left(\frac{4\pi}{7}\right)$

(d) $\sqrt{3}\,\mathrm{cis}\left(\frac{\pi}{12}\right) \cdot \sqrt{56}\,\mathrm{cis}\left(\frac{\pi}{15}\right) \cdot \sqrt{21}\,\mathrm{cis}\left(\frac{\pi}{15}\right)$

(e) $\sqrt{5}\,\mathrm{cis}\left(\frac{\pi}{19}\right) \cdot 3^{1/3}\,\mathrm{cis}\left(\frac{\pi}{3}\right) \cdot 45^{1/3}\,\mathrm{cis}\left(\frac{-10\pi}{57}\right)$

◊

Exercise 59. Calculate each of the following quotients using complex polar arithmetic. Give the answers in polar form.

(a) $\dfrac{5\operatorname{cis}\left(\frac{5\pi}{6}\right)}{2\operatorname{cis}\left(\frac{\pi}{2}\right)}$

(b) $\dfrac{27\operatorname{cis}\left(\frac{7\pi}{12}\right)}{6\operatorname{cis}\left(\frac{5\pi}{3}\right)}$

(c) $\dfrac{2\sqrt{2}+2\sqrt{2}i}{\frac{\sqrt{3}}{4}+\frac{1}{4}i}$

(d) $\dfrac{3-3i}{2-\sqrt{12}i}$

(e) $\dfrac{\sqrt{27}i}{\sqrt{3}-3i}$

(f) $\dfrac{\sqrt{17}-\sqrt{51}i}{-17-17i}$

$\Diamond$

Proposition 53 is the key fact used in finding the following formula for powers of complex numbers in polar form:

Proposition 60. (***de Moivre's Theorem***)

Let $z = r\operatorname{cis}\theta$ be a nonzero complex number. Then for $n = 1, 2, \ldots$ we have

$$[r\operatorname{cis}\theta]^n = r^n\operatorname{cis}(n\theta). \qquad (P(n))$$

(We identify this statement as "$P(n)$" for later convenience.)

Before giving the proof, we first give some general explanation of the ideas behind the proof.

Ideas Behind the Proof: We will use a very common proof technique called ***induction***. [9] Induction is commonly used to prove statements of the form "$P(n)$ is true for $n = 1, 2, 3, \ldots$", where n is some equation or statement involving the quantity n.

Notice that we actually want to prove an *infinite* number of statements: that is, we want to prove:

- $[r\operatorname{cis}\theta]^1 = r^1\operatorname{cis}\theta$
- $[r\operatorname{cis}\theta]^2 = r^2\operatorname{cis}(2\theta)$
- $[r\operatorname{cis}\theta]^3 = r^3\operatorname{cis}(3\theta)\ \ldots$

[9] In the Appendix we give a more thorough treatment of the topic of induction. Here we give only a brief presentation.

The first statement is obviously true. The second statement (for $n = 2$) can be proved using Proposition 53:

Exercise 61. Prove $[r \operatorname{cis} \theta]^2 = r^2 \operatorname{cis}(2\theta)$ using Proposition 53. ◊

The third statement (for $n = 3$) can be proved using the statement for $n = 2$:

Exercise 62. Fill in the blanks to complete the proof:

$$\begin{aligned}
[r \operatorname{cis} \theta]^3 &= r \operatorname{cis} \theta \cdot (_____)^2 && \text{(by basic algebra)} \\
&= r \operatorname{cis} \theta \cdot (r^2 \cdot _____) && \text{(by the previous exercise)} \\
&= r^3 \cdot \operatorname{cis}(\theta + _____) && \text{(by Proposition 53)} \\
&= _____ && \text{(by basic algebra)}
\end{aligned}$$

◊

So we have actually used the statement for $n = 2$ to prove the statement for $n = 3$. We could continue in this fashion to prove $n = 4$ from $n = 3$:

Exercise 63. Prove $[r \operatorname{cis} \theta]^4 = r^4 \operatorname{cis}(4\theta)$, using Proposition 53 and the result of the previous exercise (*Hint*) ◊

Obviously it would take a long time to prove $n = 5$ from $n = 4$, $n = 6$ from $n = 5$, and so on. So instead, we will prove the following statement that covers all these cases:

If $[r \operatorname{cis} \theta]^k = r^k \operatorname{cis}(k\theta)$ is true, then $[r \operatorname{cis} \theta]^{k+1} = r^{k+1} \operatorname{cis}((k+1)\theta)$ is also true.

This allows us to "ladder up": if the statement is true for some integer, then it's also true for the *next* integer.

In summary, the induction proof has two basic elements:

- Prove the statement $P(n)$ for $n = 1$ (this is called the "base case");
- Assuming that $P(n)$ is true for $n = k$, it follows that $P(n)$ is also true for for $n = k + 1$ (this is called the "induction step").

Now that we've given the ideas, here is the actual proof of Proposition 60:

PROOF. We will use induction on n. First, for $n = 1$ the proposition is trivial. This establishes the "base case".

Next, assume that $P(n)$ is true for $n = k$: that is, $z^k = r^k \operatorname{cis}(k\theta)$. Then using this fact and exponent rules, we may rewrite z^{k+1} as

$$\begin{aligned} z^{k+1} &= z^k z \\ &= r^k(\operatorname{cis}(k\theta)\, r(\operatorname{cis}\theta) \\ &= r^{k+1}[(\operatorname{cis}(k\theta + \theta)] \\ &= r^{k+1}[\operatorname{cis}[(k+1)\theta]. \end{aligned}$$

This establishes the "induction step", which completes the proof. □

Example 64. We will compute z^{10} where $z = 1+i$. Rather than computing $(1+i)^{10}$ directly, it is much easier to switch to polar coordinates and calculate z^{10} using de Moivre's Theorem:

$$\begin{aligned} z^{10} &= (1+i)^{10} \\ &= \left(\sqrt{2}\operatorname{cis}\left(\frac{\pi}{4}\right)\right)^{10} \\ &= (\sqrt{2}\,)^{10}\operatorname{cis}\left(\frac{5\pi}{2}\right) \\ &= 32\operatorname{cis}\left(\frac{\pi}{2}\right) \\ &= 32i. \end{aligned}$$

♦

Notice that de Moivre's Theorem says nothing about a complex number raised to negative powers. For any real number x, we know x^{-n} means $(x^n)^{-1}$. Complex numbers happen to work the same way.

Definition 65. Given a complex number $z = r\operatorname{cis}\theta$,

$$z^{-n} = (z^n)^{-1}.$$

△

Example 66. Let $z = 2\,\mathrm{cis}(\pi/4)$. What is z^{-3}?

$$\begin{aligned} z^{-3} &= (z^3)^{-1} \\ &= ([2\,\mathrm{cis}(\pi/4)]^3)^{-1} \\ &= (8\,\mathrm{cis}(3\pi/4))^{-1} \quad \text{(by de Moivre's Theorem)} \\ &= \frac{1}{8}\,\mathrm{cis}(5\pi/4) \qquad \text{(by Exercise 55)} \end{aligned}$$

♦

Exercise 67. Calculate each of the following expressions. Write the answer as $a + bi$ if you can do so without using roots or decimals. Otherwise, you may leave the answer in polar form.

(a) $(1+i)^{-3}$

(b) $(1-i)^6$

(c) $(\sqrt{3}+i)^5$

(d) $(-i)^{10}$

(e) $((1-i)/2)^4$

(f) $(-\sqrt{2}-\sqrt{2}\,i)^{12}$

(g) $(-2+2i)^{-5}$

(h) $(\sqrt{2+\sqrt{2}}-i\sqrt{2-\sqrt{2}})^{16}$

◊

3.3.6 A Remark on representations of complex numbers

We have seen that a complex number z can be expressed in a number of different ways:

- As $a + bi$, where a and b are real numbers;
- As a point in the Cartesian (two-dimensional) plane;
- As a pair of real numbers (a,b) that give the rectangular coordinates of the point in the plane;
- As a pair of numbers (r, θ) where $r \geq 0$ and $0 \leq \theta < 2\pi$, that give the polar coordinates of the point in the plane;
- As $r \cdot (\cos\theta + i \cdot \sin\theta)$, or the equivalent form $r \cdot \mathrm{cis}\theta$.

In abstract mathematics, it is very common to represent the "same" entity in a number of different ways. One of the main goals of abstract algebra is to identify mathematical structures that are the "same" algebraically even though they appear to be different. Mathematical structures that are the "same" algebraically are said to be ***isomorphic***. We will be seeing isomorphic structures throughout this course.

The importance of isomorphism in mathematics cannot be overstated.[10] Realizing that the same thing can be represented in two different ways is often the key to mathematical progress, and can lead to enormous simplifications. For instance, we have seen that it's easier to add complex numbers in Cartesian form, while it's much simpler to multiply complex numbers in polar form. Since Cartesian and polar forms are are simply two different ways of representing the same thing, we can freely switch back and forth between the two forms, using whichever is most convenient at the moment.

Exercise 68.

(a) Using de Moivre's formula for z^3 where $z = r\,\mathrm{cis}\,\theta$, find formulas for $\cos 3\theta$ and $\sin 3\theta$ in terms of $\cos\theta$ and $\sin\theta$.

(b) Using part (a), find a formula for $\cos 3\theta$ in terms of $\cos\theta$. (*Hint*)

(c) * Show that for any n, it is always possible to find a formula for $\cos n\theta$ in terms of $\cos\theta$.

(d) * Show that for any *even* n, it is always possible to find a formula for $\cos n\theta$ in terms of *even* powers of $\cos\theta$.

$\Diamond$

We also wish to emphasize the importance of representations using *pictures*. These are essential for developing a deep, intuitive grasp of how complex numbers work.

Exercise 69.

(a) Figure 3.4 shows polar and Cartesian representations of a complex number z in the complex plane. Redraw the figure, and put $\overline{z}$ in the picture as well. Show the Cartesian coordinates of $\overline{z}$, as well as the modulus and the complex argument (angle).

[10] There are other types of "morphisms" as well, such as homeomorphism (in topology), diffeomorphism (in differential topology), and just plain morphism (in category theory).

(b) Use your picture to obtain the polar representation of $\bar{z}$ in terms of the modulus and complex argument of z.

$\Diamond$

3.4 Applications of complex numbers

3.4.1 General remarks on the usefulness of complex numbers

We have already discussed that it took some time for complex numbers to be generally accepted by mathematicians, who tended to have a preference for "pure" numbers such as the integers. But complex numbers have had their revenge. Today the "purest" form of mathematics, namely number theory, is heavily dependent on complex numbers. The famous Fermat's Last Theorem was proved using techniques that involved complex numbers.[11]

But quite apart from pure mathematics, complex numbers have proved to be extremely practical. Complex numbers are indispensable tools for scientists and engineers. Virtually all of modern physics is based on complex numbers. Engineers build bridges using complex numbers. Without complex numbers, there would probably be no computers, cell phones or most other electronics. A strong argument could be made that complex numbers are far more useful than "real" numbers.

Much of the practical usefulness of complex numbers comes from their close relationship with the trigonometric functions cosine and sine. We have seen a little bit of this already in the representation $z = r\,\mathrm{cis}\,\theta$. Complex numbers give a powerful way to express complicated functions of sine and cosine in a very simple way. We will give an introduction of this in the next section–you may see it again, or have already seen it, in your differential equations course.

3.4.2 Complex numbers, sine and cosine waves, and phasors

We have already seen there is a close relationship between complex numbers and the trigonometric functions sine and cosine. This relationship is the

[11] See http://www-history.mcs.st-and.ac.uk/HistTopics/Fermat's_last_theorem.html for some of the long and sordid history of Fermat's Last Theorem.

basis for much of the usefulness of complex numbers – as we shall explain in this section.

Figure 3.6 shows the graphs of the cosine and sine functions. They look like waves: for instance, the graph of $y = \cos(t)$ is a wave that includes the point $(0, 1)$. The ***amplitude*** of this wave is 1. The ***period*** of this wave is 2π radians.

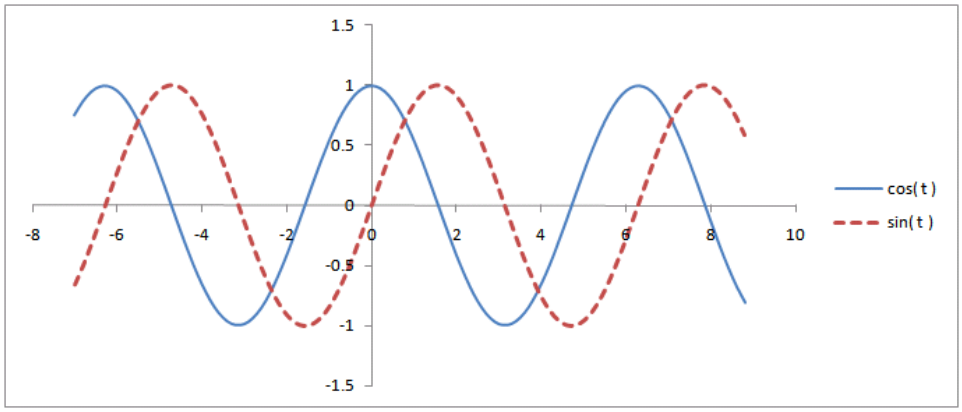


Figure 3.6. Graphs of cosine and sine

Note that some references use the word "wavelength" instead of "period". This is because they are considering equations like $y = \cos(x)$ where the independent variable x represents distance. We are considering the independent variable to be time: so it is appropriate to use the word "period" instead.

Of course, there are cosine and sine waves with different periods. However, in this section we will *only* be looking at cosine and sine waves with period 2π. We re-emphasize: all the cosine and sine waves in this chapter (and any that you use in the homework problems) have period 2π.

Now we can create other waves by using the cosine as a "parent function". For instance, the graph of $y = A\cos(t + \theta)$ where $A > 0$ is similar to the graph of $y = \cos(t)$, with the following differences:

- The amplitude is A
- The ***phase shift*** (relative to the cosine curve) is θ.

Remark 70.

- You may have studied "parent functions" in high school, and if so you may remember that the graph of $y = f(t + c)$ is shifted to the *left* compared to the graph of $y = f(t)$. It follows that a positive phase shift will shift the graph to the *left*, while a negative phase shift will shift it to the *right* (see Figure 3.7).[12]

- If the variable t is considered as time, then $y = A\cos(t+\theta)$ is *advanced* by θ (corresponding to a left shift of the graph), while $y = A\cos(t-\theta)$ is *delayed* by θ (corresponding to a right shift of the graph).

△

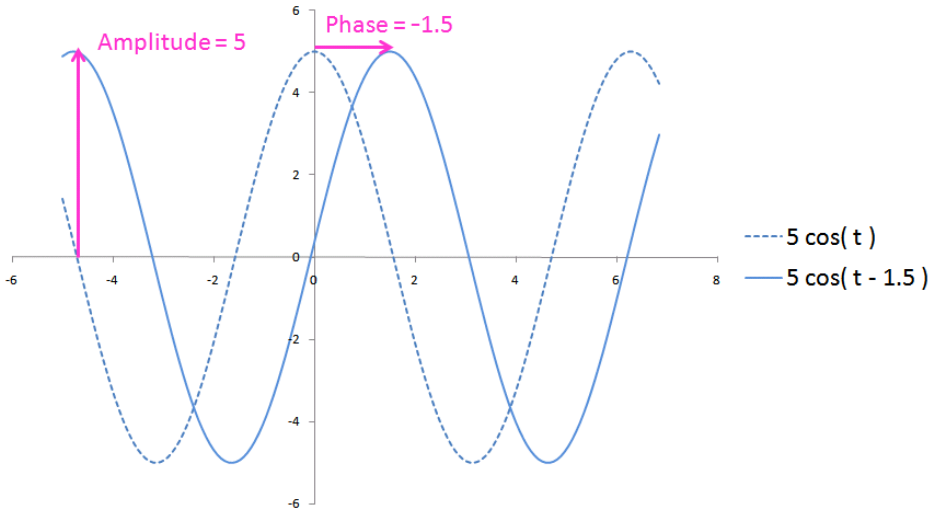


Figure 3.7. Cosine wave with amplitude and phase shift

Exercise 71. Sketch the function $y = 1.5\cos(t+\pi/3)$. Label the amplitude and phase shift on your graph. ◊

Exercise 72. Give the equation of a cosine wave with amplitude 7 and phase shift $-\pi/2$. Graph the function. How is this function related to a sine wave? ◊

[12] You should be careful when you encounter the term "phase shift" in other books, because some books define a positive phase shift as moving the graph to the *right*. This is not wrong: it's just different terminology.

Exercise 73. Give the equation of a cosine wave with amplitude $1/2$ and phase shift 2π. Graph the function. How is this wave related to the original cosine wave with phase shift 0? ♢

Exercise 74.

(a) Sketch the function $y = \sin(t)$.

(b) Find three different choices of A, θ such that $\sin(t) = A\cos(t+\theta)$. What are the possible values of A? (*Hint*)

♢

In summary, amplitude and phase are two important properties of cosine and sine waves; and in fact the amplitude and phase uniquely determine the actual wave, as you saw in Exercises 72 and 73. Now earlier in this chapter, we saw a different mathematical object that was characterized by amplitude and phase. Naturally, we're referring to the complex numbers. We will now make a deep connection between these two types of mathematical objects that, on the surface, are very different.

Recall that the *real part* of the complex number $z = a + bi$ is a, and the *imaginary part* is b. We also use the notation $\mathrm{Re}[z]$ to denote the real part of the complex number z, and the notation $\mathrm{Im}[z]$ to denote the imaginary part.

Exercise 75. Show that $\mathrm{Re}[A\,\mathrm{cis}\,\theta \cdot \mathrm{cis}(t)] = A\cos(t+\theta)$. (*Hint*) ♢

Exercise 76. Show that $\mathrm{Im}[A\,\mathrm{cis}\,\theta \cdot \mathrm{cis}(t)] = A\sin(t+\theta)$. ♢

The previous two exercises show that:

- A cosine wave with amplitude A and phase shift θ can be represented as the real part of the complex number $A\,\mathrm{cis}\,\theta$ times the complex function $\mathrm{cis}(t)$.
- A sine wave with amplitude A and phase shift θ can be represented as the imaginary part of the complex number $A\,\mathrm{cis}\,\theta$ times the complex function $\mathrm{cis}(t)$.

We may also understand this situation in terms of two-dimensional vectors with the help of Figure 3.8. We've already shown how complex numbers can be seen as two-dimensional vectors: in particular, the complex number $\operatorname{cis}\theta$ is identified with $\cos\theta\mathbf{i} + \sin\theta\,\mathbf{j}$. As t varies, the point $\operatorname{cis}(t+\theta)$ moves around the unit circle,and the real part of $\operatorname{cis}(t+\theta)$ is the projection of the moving point onto the x-axis. In other words, the cosine wave on the right side of Figure 3.8 tells us the vector's horizontal distance to the y-axis as a function of time t.

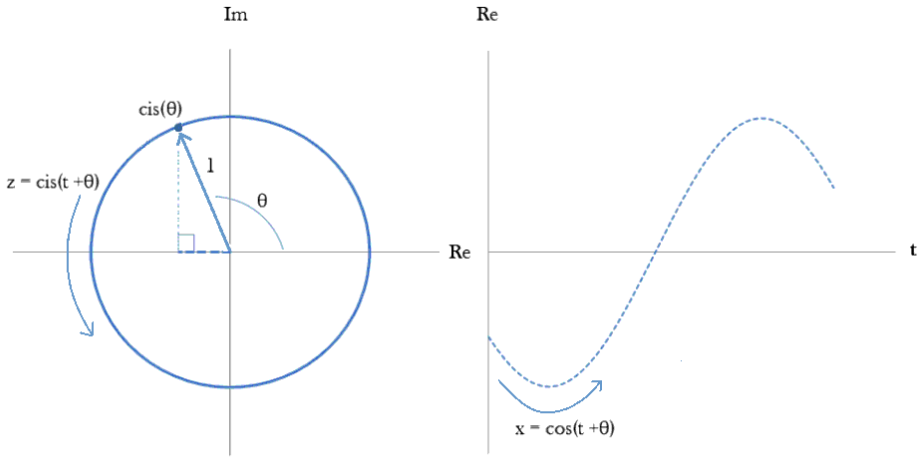


Figure 3.8. Graphs of the vector representation and the wave representation of cosine

Now it's possible to add two waves together; we've all seen at the beach or pool (or physics class) how two water waves that cross each other create another wave of with a different shape. This is called ***wave superposition***. In general, the superposition of two waves is a wave with a different shape; we will now see how complex numbers make it easy to compute this new wave.

Exercise 77.

(a) Using $\operatorname{cis}\theta = \cos\theta + i\sin\theta$, complete the following argument by filling in the blanks:

$$\begin{aligned} 2\cos(t+\pi/2) + 2\cos(t-5\pi/6) &= \operatorname{Re}[2\operatorname{cis}(t+\pi/2)] + \operatorname{Re}[\_\_\_\_\_] \\ &= \operatorname{Re}[2\operatorname{cis}(t)\cdot\operatorname{cis}(\pi/2)] + \operatorname{Re}[\_\_\_\_\_] \\ &= \operatorname{Re}\left[\left(\,2\operatorname{cis}(\pi/2) + 2\operatorname{cis}(-5\pi/6)\,\right)\cdot \_\_\_\_\_\right] \end{aligned}$$

(b) Convert $2\operatorname{cis}(\pi/2)$ and $2\operatorname{cis}(-5\pi/6)$ to cartesian form, and find the sum. Then convert back to polar form.

(c) Use your result in (b) to simplify the right-hand side of (a).

(d) Your result in (c) shows that the sum of the two cosine waves $2\cos(t+\pi/2)$ and $2\cos(t-5\pi/6)$ is also equal to a cosine wave. Find the amplitude and phase shift of the sum. Is the amplitude equal to the sum of the amplitudes? Explain.

$\Diamond$

Let us summarize our findings:

- Associated with each sine or cosine wave is a complex number $A\operatorname{cis}(\theta)$ such that A is the amplitude and θ is the phase shift of the wave. This complex number is called the ***phasor*** associated with the wave.
- The sum of two sine or cosine waves is also equal to a cosine wave
- The amplitude and phase shift of the sum of two cosine waves may be obtained by adding the phasors of the two consituent cosine waves.

Exercise 78. A radio antenna receives three cosine-wave signals. The first signal has an amplitude of 4 and a phase shift of 0. The second has an amplitude of 3 and a phase shift of $\pi/2$. The third signal has an amplitude of 2 and a phase shift of $-\pi/3$.

(a) On graph paper, plot the three phasors corresponding to the three signals. (The three phasors are $4\operatorname{cis}(0), 3\operatorname{cis}(\pi/2)$, and $2\operatorname{cis}(-\pi/3)$)

(b) Use your picture in (a) to graphically add the three phasors. (Remember how to add vectors: add the x-components, and add the y-components.)

(c) Convert the three phasors to rectangular form, and add them together algebraically.

(d) Use your result from (c) to find the amplitude and phase shift of the sum of the three signals.

$\Diamond$

Exercise 79. As in the previous problem, a radio antenna receives three cosine-wave signals. The three signals have equal amplitude. The first signal have a phase shift of 0. The second has a phase shift of $2\pi/3$. The third signal has a phase shift of $4\pi/3$.

(a) What is the amplitude of the sum of the three signals?

(b) What is the phase shift of the sum of the three signals?

$\Diamond$

We hope that from the examples in this section, you may get some idea of how important complex numbers are in the study of signals. In fact, for many electrical engineers complex numbers are their "bread and butter".

3.4.3 Roots of unity and regular polygons

As we mentioned before, complex numbers got their start when mathematicians started considering the solutions to algebraic equations. One particularly important equation is

$$z^n = 1.$$

For example, when $n = 4$ the complex numbers which solve $z^4 = 1$ are $z = 1$, -1, i, and $-i$. In general, the complex numbers that satisfy the equation $z^n = 1$ are called the ***nth roots of unity***.

Exercise 80.

(a) Give two distinct square roots of unity (that is, $z^n = 1$ for $n = 2$).

(b) For what integers n is -1 an nth root of unity?

$\Diamond$

It turns out that in general we can find n different nth roots of unity, as per the following proposition:

Proposition 81. The following n numbers are nth roots of unity:

$$z = \text{cis}\left(\frac{2k\pi}{n}\right),$$

where $k = 0, 1, \ldots, n-1$.

PROOF. By de Moivre's Theorem,

$$z^n = \text{cis}\left(n\frac{2k\pi}{n}\right) = \text{cis}(2k\pi) = 1.$$

The z's are distinct since the numbers $2k\pi/n$ are all distinct and are greater than or equal to 0 but less than 2π. $\square$

Exercise 82.

(a) Using Proposition 81, write three cube roots of unity in polar form. Convert to the form $a + bi$.

(b) Using Proposition 81, write four 4th roots of unity in polar form. Convert to the form $a + bi$.

$\Diamond$

We have not actually shown that Proposition 81 gives *all* of the nth roots of unity, but in fact it does. First we'll show this is true in the case where $n = 4$:

Proposition 83. The only 4th roots of unity are the elements of the set $\{1, -1, i, -i\}$.

PROOF. What this proposition is saying is that any complex number w that is not in the set $\{1, -1, i, -i\}$ can't possibly be a fourth root of unity. We'll show this in the following exercise:

Exercise 84.

(a) Suppose that w is a complex number that is not equal to 1, -1, i, or $-i$ (in mathematical shorthand we write this as: $w \notin \{1, -1, i, -i\}$). Show that $(w-1)(w+1)(w-i)(w+i) \neq 0$. (*Hint*)

(b) Show that this implies that w is not a 4th root of unity. (*Hint*)

♢

□

Exercise 85.

(a) Multiply out the product $(z-1)(z-\text{cis}\left(\frac{2\pi}{3}\right))(z-\text{cis}\left(\frac{4\pi}{3}\right))$ and simplify. (*Hint*)

(b) Use youre result in (a) to show that there are exactly 3 cube root of unity.

♢

The roots of unity have interesting interesting geometric properties, as follows.

Example 86. The 8th roots of unity can be represented as eight equally spaced points on the unit circle (Figure 3.9). For example, some 8th roots of unity are

$$\omega = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$$
$$\omega^3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$$
$$\omega^5 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$$
$$\omega^7 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.$$

In fact, the 8th roots of unity form a *regular octagon.* ♦

Exercise 87. Sketch the cube roots of unity in the complex plane. Use the distance formula (from geometry) to show that the three points are all

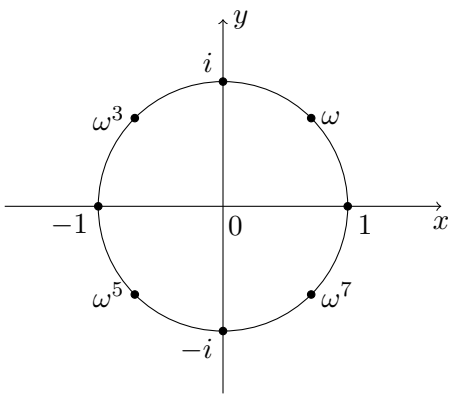


Figure 3.9. 8th roots of unity

the same distance from one another. Connect the three points to form a triangle. What kind of triangle is it? ♢

Exercise 88. Prove (using geometry) that the 4th roots of unity form a square. (*Hint*: Besides showing that all sides are equal, you also have to show that they are perpendicular.) ♢

Exercise 89. *Prove (using geometry) that the 6th roots of unity form a regular hexagon. (*Hint*: Draw lines from each point to the origin, forming 6 triangles. What can you say about these triangles?) ♢

Incredibly as it seems, apparently complex numbers are closely related to geometry! Let us explore this relationship a little further.

Exercise 90.

(a) Draw a picture of the 6th roots of unity in the complex plane. Label them A, B, C, D, E, F with $A = 1, B = \text{cis}\left(\frac{2\pi}{6}\right)$, and C, D, E, F going counterclockwise around the circle.

(b) Fill in each of the following blanks with the letter corresponding to the product of the two complex numbers. For example, $B \cdot B = \text{cis}\left(\frac{2\pi}{6}\right) \cdot \text{cis}\left(\frac{2\pi}{6}\right) = \text{cis}\left(\frac{2\pi}{3}\right) = C$.

$B \cdot A =$ ____ $B \cdot C =$ ____ $B \cdot E =$ ____
$B \cdot B =$ ____ $B \cdot D =$ ____ $B \cdot F =$ ____

(c) Using your answers from part (b), on your picture draw an arrow from A to $B \cdot A$; similarly draw arrows from B to $B \cdot B$, C to $B \cdot C$, and so on. What do you observe about the arrows?

(d) It appears that multiplying all of the corners of the hexagon $ABCDEF$ by B produces a *rotation* of the hexagon. What is the angle of rotation?

(e) Fill in the blanks:

$E \cdot A =$ ____ $E \cdot C =$ ____ $E \cdot E =$ ____
$E \cdot B =$ ____ $E \cdot D =$ ____ $E \cdot F =$ ____.

(f) Just as in part (c), use your answers from part (d) to draw arrows from A to $E \cdot A$, B to $E \cdot B$,etc. What do you observe about the arrows?

(g) Fill in the blanks: If you choose one particular 6th root of unity and multiply it with all the other 6th roots, the new values correspond to different _____ of the original hexagon. The angle of _____ is equal to the complex argument of the _____.

$\Diamond$

Exercise 91.

(a) Just as in part (b) of Exercise 90 fill in the blanks with the correct letter A, B, C, D, E or F (recall that $\overline{A}$ denotes the complex conjugate of A).

$\overline{A} =$ ____ $\overline{C} =$ ____ $\overline{E} =$ ____
$\overline{B} =$ ____ $\overline{D} =$ ____ $\overline{F} =$ ____.

(b) Just as in part (c) of Exercise 90, draw arrows from A to $\overline{A}$, B to $\overline{B}$, etc. What do you observe about the arrows?

(c) We refer to the geometrical motion produced by complex conjugation as "flipping". What is the axis of the "flip" that is produced by taking the complex conjugates of the sixth roots of unity?

◊

The previous exercises (when suitably generalized) lead to the following stupendous conclusion:

- Every *rigid* motion of a regular n-gon is equivalent to some combination of complex conjugation and multiplication by one of the nth roots of unity.

Exercise 92.

(a) What geometrical motion corresponds to the following algebraic operation: Multiply all 6th roots by D, then take the complex conjugates.

(b) What geometrical motion corresponds to the following algebraic operation: Take the complex conjugates of all 6th roots, then multiply by D.

(c) What geometrical motion corresponds to the following algebraic operation: Multiply all 6th roots by C, then take the complex conjugates.

(d) What geometrical motion corresponds to the following algebraic operation: Take the complex conjugates of all 6th roots, then multiply by C.

◊

Exercise 92 also gives us our first exposure to a phenomenon that is quite common in abstract algebra, namely the existence of ***non-commutative*** operations (also known as ***non-abelian*** operations). We saw that both multiplication by a nth root of unity and complex conjugation corresponded to motions of a regular n-gon. However, the *order* of the motions matters: rotating first and then conjugating (i.e. "flipping") gives a *different* result than conjugating first, then performing the rotation afterwards.

Exercise 93. If you've studied matrix multiplication, then you may have seen non-commutative operations before:

(a) Give an example of two 2×2 matrices that do *not* commute: that is $AB \neq BA$.

(b) Give an example of two 2×2 matrices that *do* commute.

$\Diamond$

The previous exercises give a small hint as to the extensive and beautiful relationship between the complex numbers and plane geometry. The following exercises further explore this relationship. (*Hint*: you may find that complex polar form is useful in these exercises.)

Exercise 94. Consider a plane with Cartesian coordinates. Let O be the point $(0, 0)$, let A be the point (a, b), and let C be the point (c, d). Also, let $z = a + bi$ and $w = c + di$.

(a) * Show that

$$\text{Area of triangle } OAC = \left| \frac{z\bar{w} - \bar{z}w}{4} \right|.$$

(b) * Show that $\overline{OA}$ is perpendicular to $\overline{OC}$ if and only if $z\bar{w} + \bar{z}w = 0$.

(c) * Use complex arithmetic to prove the *Law of cosines*:

$$AC^2 = OA^2 + OC^2 - 2(OA)(OC)\cos(\angle AOC),$$

where AC, OA, and OC denote the lengths of segments $\overline{AC}, \overline{OA}$ amd $\overline{OC}$ respectively. (*Hint*)

$\Diamond$

In fact, many intricate theorems in plane geometry that require long proofs using conventional methods can be proven much more easily using complex numbers. We will not be exploring this further; but we hope these examples will whet your appetite!

3.4.4 Arbitrary nth roots

In the previous section, we characterized all complex solutions of the equation $z^n = 1$; we called these solutions the nth roots of unity. A natural question to ask then is, What about the nth roots of any complex number? That is, given a complex number $a + bi$, can we find all solutions to the equation $z^n = a + bi$? Let's explore some simple cases first.

Exercise 95.

(a) Find all square roots of -1.

(b) The complex number $1+i$ is one square root of $2i$. Can you find another one?

(c) Find all square roots of $8i$. (*Hint*)

(d) In parts (a), (b), and (c) you found two square roots in each case. In each case, what is the relation between the two square roots?

$\Diamond$

Next, let us consider the case of cube roots. Consider for example the cube roots of $1+i$, which are the solutions to

$$z^3 = 1 + i.$$

It turns out that it is easier to use polar form, so we rewrite this as

$$z^3 = \sqrt{2}\,\mathrm{cis}\left(\frac{\pi}{4}\right).$$

Recalling de Moivre's theorem, one solution should be clear:

$$\begin{aligned} z &= (\sqrt{2})^{1/3}\,\mathrm{cis}\left(\frac{\pi}{4}/3\right) \\ &= 2^{1/6}\,\mathrm{cis}(\pi/12). \end{aligned}$$

But are there others? In fact, if we multiply this solution by the three cube roots of unity, we obtain

$$2^{1/6}\,\mathrm{cis}\left(\frac{\pi}{12}\right); \qquad 2^{1/6}\,\mathrm{cis}\left(\frac{\pi}{12}\right)\cdot\mathrm{cis}\left(\frac{2\pi}{3}\right); \qquad 2^{1/6}\,\mathrm{cis}\left(\frac{\pi}{12}\right)\cdot\mathrm{cis}\left(\frac{4\pi}{3}\right).$$

You may check that all three of these complex numbers satisfy $z^3 = 1+i$.

Exercise 96. Verify that these three numbers all satisfy $z^3 = 1+i$ (use the complex polar form for $1+i$). $\Diamond$

This example suggests a general procedure for finding n distinct nth roots of complex numbers:

- Find a single root using de Moivre's Theorem;
- Multiply your result by all n roots of unity to obtain n distinct roots.

Exercise 97. (In this exercise, you may leave your answers in polar form)

(a) Find all fifth roots of $-i$.

(b) Find all fourth roots of $-1 + \sqrt{3}i$.

(c) Find all fourth roots of $\sqrt{1/2 + \sqrt{2}/4} + i\sqrt{1/2 - \sqrt{2}/4}$. (*Hint*)

$\Diamond$

3.5 Complex roots of polynomial equations

Next we consider more general algebraic equations than the basic n'th root equations we've been looking at so far. As a first example, consider the equation $z^2 + pz = q$, where p and q are real numbers. Using the quadratic formula, it is not too hard to show that if $a+bi$ is a solution of $z^2+pz = q$ then the complex conjugate $a - bi$ is also a solution. This is because $z^2 + pz = q$ can also be written as $z^2 + pz - q = 0$, and the quadratic formula tells us that there are two solutions, given by:

$$z = \frac{-p \pm \sqrt{p^2 - (4)(1)(-q)}}{2} = \frac{-p}{2} \pm \frac{\sqrt{p^2 + 4q}}{2}.$$

The $-p/2$ term is always real, but the square root term is either real or imaginary depending on the sign of $p^2 + 4q$ (since q could be negative). If the square root term is real, then both roots are real, and each root is its own complex conjugate. If the square root term is imaginary, then the $\pm$ means that the imaginary parts of the two roots are negatives of each other, so that the two roots are complex conjugates.

Exercise 98. Consider the cubic equation $z^3 + pz^2 + qz = r$, where p, q and r are all real numbers.

(a) Using a previous exercise (which?), show that $\overline{z^3} = \overline{z}^3$.

(b) Similarly, show $\overline{pz^2} = p\overline{z}^2$ and $\overline{qz} = q\overline{z}$, and $\overline{r} = r$.

(c) Use (a) and (b) to show that $\overline{z^3 + pz^2 + qz - r} = \overline{z}^3 + p\overline{z}^2 + q\overline{z} - r$.

(d) Using (c), show that $z^3+pz^2+qz-r = 0$ implies that $\overline{z}^3+p\overline{z}^2+q\overline{z}-r = 0$.

(e) Using (d), show that if z is a solution to $z^3 + pz^2 + qz = r$ then $\overline{z}$ is also a solution.

$\Diamond$

Exercise 99. Based on the result of the previous exercise, fill in the blank: Given that the complex number z is a solution of $z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \ldots + a_1 z = a_0$, where $a_0, a_1, \ldots a_{n-1}$ are real numbers. Then _____ is also a solution to the same equation. $\Diamond$

Exercise 100.

(a) Given that $3 - 7i$ and $-2 + i$ are solutions to an equation of the form $z^4 + a_3 z^3 + a_2 z^{n-2} + a_1 z + a_0 = 0$ where a_0, a_1, a_2, a_3 are real. Find two other solutions to the same equation.

(b) *Find a_0, a_1, a_2, a_3. (*Hint*)

$\Diamond$

Exercise 101. Using the statement in Exercise 99, prove the following proposition: Given the equation $z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \ldots + a_1 z = a_0$, where $a_0, a_1, \ldots a_{n-1}$ are real numbers. Let N be the number of solutions of the equation that are *not* real. Then either $N = 0$ or N is divisible by 2. (*Hint*) $\Diamond$

The most famous result concerning complex roots of polynomials is known as the ***Fundamental Theorem of Algebra***:

Proposition 102. Given any equation of the form $z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \ldots + a_1 z = a_0$, where $n > 0$ and $a_0, a_1, \ldots a_{n-1}$ are real numbers. Then there exists at least one and at most n distinct complex numbers which solve the given equation.

The Fundamental Theorem of Algebra actually has two parts. The easy part is the "at most n distinct complex roots" part, and the hard part is the "at least one complex root" part. We will eventually prove the easy part in Chapter 18, but sadly the hard part is beyond our scope.[13]

Exercise 103.

[13] You may see a proof if you take a class in complex analysis

(a) Give an example of an equation of the form $z^2 + a_1 z = a_0$ that has only one solution.

(b) Give an example of an equation of the form $z^3 + a_2 z^2 + a_1 z = a_0$ that has only one solution.

(c) Can you give an example of an equation of the form $z^3 + a_2 z^2 + a_1 z = a_0$ that has exactly two solutions?

$\Diamond$

Exercise 104. Using the Fundamental Theorem of Algebra and our previous results on roots of unity, prove that for every positive integer n there are *exactly* n distinct nth roots of unity (so far, we have only shown that there are *at least* n distinct nth roots). $\Diamond$

Exercise 105. Using the Fundamental Theorem of Algebra and Exercise 101, prove the following proposition: Given an equation of the form $z^n + a_{n-1} z^{n-1} + a_{n-2} z^{n-2} + \ldots + a_1 z = a_0$, where $n > 0$ and $a_0, a_1, \ldots a_{n-1}$ are real numbers. Suppose the equation has no real solutions. Then the equation has at least two distinct solutions. $\Diamond$

Exercise 106. Give an example of a polynomial of the form $z^6 + a_5 z^5 + a_4 z^4 + \ldots + a_1 z = a_0$, that has no real solutions, and exactly two distinct complex solutions. $\Diamond$

Historical Note

Several great mathematicians (Euler, Lagrange, Laplace, and Gauss) produced "proofs" that every polynomial has at least one complex root which turned out to be faulty. The first correct proof was given by Argand in 1806. See en.wikipedia.org/wiki/Fundamental_theorem_of_algebra for the fascinating detals.

4

Modular Arithmetic

What goes up, must come down
Spinnin' wheel, got ta go round
Talkin' 'bout your troubles it's a cryin' sin
Ride a painted pony, Let the spinnin' wheel spin

(Source: "Spinnin' Wheel", Blood, Sweat, and Tears)

Cycles are everywhere. So are integers. Modular arithmetic combines the two by wrapping the integers around a circle.[1]

4.1 Introductory examples

Modular arithmetic was originally motivated by common, real-life situations. So we begin our introduction by describing several problems based on practical situations for you to think about. We don't ask you to find the solutions just yet – instead, focus on the similarities between the different problems.

Example 1. Don has whipped up some stew that he wants to slow-cook in his crockpot. The stew is supposed to cook for exactly 40 hours. The crockpot is not automatic, so Don has to turn it on and off by hand. When would be a good time for Don to turn on the crockpot? (Additional information: Don is away at work from 8 a.m. to 5 p.m. every day. Also, Don would like

[1] Thanks to Tom Judson for material used in this chapter. David Weathers also contributed a section.

to avoid waking up in the middle of the night to turn the crockpot on or off.) ♦

Example 2. Jennifer owns a vintage 1957 Thunderbird which has had two previous owners. She claims that the car's first owner drove it 129,000 miles, the second owner drove it 77,000 miles, and she's driven 92,500 miles. If her claim is true, then what should the odometer read? Note that on old cars the odometer only goes up to 99,999. ♦

Example 3. April 15, 2012 was on a Friday. What day of the week was December 24 of 2011? (Note 2012 is a leap year!) ♦

Example 4. A lunar year is 354 days. If Chinese New Year is determined according to the lunar year, and Chinese New Year is February 14 in 2010, then when is Chinese New Year in 2011? In 2012? In 2009? [2] ♦

Example 5. The hour hand on Tad's old watch is broken and does not move. Currently the watch shows a time of 3:46. Tad has just begun a 3-part test, where each part takes 75 minutes (plus a 10-minute break between parts). What time will the watch read when the first part is over? The second part? The entire test? ♦

Example 6. A racing car starts at the 3 mile mark of a 5-mile circuit. It goes another 122 miles. Then, it turns around and drives 444 miles in the reverse direction. Where does the car end up? ♦

Example 7. Suppose our race car is driving around the 5-mile track again. If it starts at the 3 mile mark and makes 17 consecutive runs of 24 miles each, what mile marker does it end up at? ♦

Exercise 8. Try to describe what all of the preceding problems have in common. Describe some differences. ♢

[2] Note that the Chinese calendar actually adds extra months in some years, so not every Chinese year is 354 days. So this example is not 100% accurate

Notice that in each example the set of possible answers is restricted to a finite set of integers. For instance, in the odometer example (Example 2) we know even before working the problem that the answer must be an integer between 0 and 99,999 (inclusive). In other words, there are 100,000 possible answers to the question, regardless of the particular mileages involved.

Exercise 9. Give the number of possible answers for Examples 1 and 3. ◊

Each example above requires arithmetic to solve, but it's arithmetic with a twist. For example, in Example 6 if the car is at the 3-mile mark and travels another 3 miles, then it arrives at the 1-mile marker. This is a strange equation: $3 + 3 = 1$. The reason of course is that the location "cycles" back to 0 instead of increasing to $5, 6, 7, \ldots$ This "arithmetic with cycles" is actually called ***modular arithmetic***. The size of one cycle (which is equal to the number of possible answers described in Exercise 9 is called the ***modulus***.

Exercise 10. Give the modulus for the seven examples at the beginning of this chapter. ◊

In summary, modular arithmetic refers to arithmetic done according to a modulus, so that the numbers reset (or cycle around) every time you reach the modulus.

4.2 Modular equivalence and modular arithmetic

In order to understand the situation more thoroughly, let us focus on the 5-mile racetrack example used in Examples 6 and 7. The racetrack (with mile markers) is shown in Figure 4.1.

Let's say the car starts at mile marker 0. The car may then travel forward (counterclockwise) or backwards (clockwise) any number of miles; we may define the car's *net displacement* as the the total number of forward miles traveled minus the the total number of backward miles. Net displacement is a very useful concept if you are a racecar driver. For example, the winner of the Indianapolis 500 is the the first driver to achieve a net displacement of 500 miles (in this case, only forward motion is allowed!)

We may characterize the displacement of the car using a conventional number line, as shown in Figure 4.2. Moving forward around the racetrack

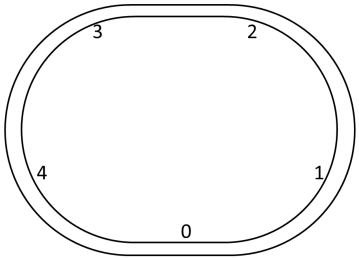


Figure 4.1. 5-mile racetrack

corresponds to moving left (positive direction) on the number line; while moving backward around the racetrack corresponds to moving right (negative direction).

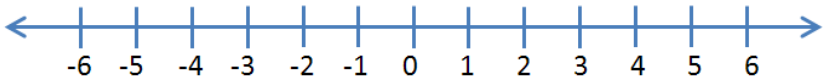


Figure 4.2. Displacements on a 5-mile racetrack

Exercise 11. Compute the net displacement for the following multi-stage trips:

(a) 346 miles in the forward direction, then 432 miles in the backward direction, then 99 miles in the forward direction.

(b) A forward displacements of 44 miles, followed by 13 additional forward displacements of 53 miles (one after the other).

(c) Repeat the following sequence 25 times: a forward displacement of 17 miles, followed by a backward displacement of 9 miles, followed by a forward displacement of 22 miles.

◊

From the preceding exercise, it appears that we may use ordinary addition, subtraction and/or multiplication to compute the car's net displacement after a trip involving several stages.

On the other hand, if we want to represent the *position* of the car on the track as it relates to net displacement, we would have to relabel the number line as shown in Figure 4.3, using only the integers $0, 1, 2, 3, 4$.

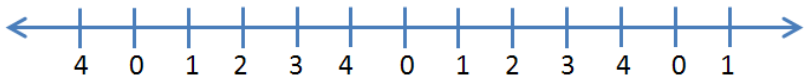


Figure 4.3. Positions on the 5-mile racetrack

Exercise 12.

(a) Compute the positions on the racetrack corresponding to each of the net displacements that you computed in Exercise 11.

(b) How are your answers in (a) related to the corresponding answers in Exercise 11?

$\Diamond$

You may have noticed that different displacements correspond to the same position. For example, displacements of 8, 23, and -17 all correspond to the same position (namely 3). This prompts us to ask the question, How can you tell when two displacements correspond to the same position? One way to do this is make use of the answer to part (b) of Exercise 12. Most likely, you answered part (a) of Exercise 12 by dividing the net displacements by 5 and taking the remainder. If two different net displacements correspond to the same position, then they have the same remainder when divided by 5.

We say that two displacements that correspond to the same position are *equivalent*. For a 5-mile racetrack, for example, we have that 13 is equivalent to 18. We write this as: $13 \equiv 18 \pmod 5$.

In general, if we're dealing with a situation that uses modulus m, then we define modular equivalence as follows:

Definition 13. Two integers a and b are ***equivalent*** mod m if both a and b have the same remainder when divided by m. To denote that a and b are ***equivalent*** mod m, we write: $a \equiv b \pmod m$. $\triangle$

Remark 14. This definition uses the notion of *remainder*, which we're assuming you're familiar with from basic algebra. To be precise, the remainder of a when divided by m is a number r between 0 and $m-1$ such that $a = q \cdot m + r$ for some integer q (q is called the "quotient"). In your basic algebra class you we always able to find a remainder for any division problem, and there was always just one right answer for the remainder. In other words, you found that the remainder always exists, and is unique. This "basic" fact is actually not so easy to prove. It may be proved using the so-called *division algorithm.*. You may find a proof in any book on number theory. △

Remark 15. Notice that Definition 13 uses the 3-lined "≡" here instead of the usual = sign. This notation is used to emphasize the fact that modular equivalence resembles equality, but is not quite the same thing. For example, we have already seen that 8 and 23 are equivalent mod 5, even though they are not equal. In a later chapter we'll discuss equivalence relations, and we'll see that equivalence is in some sense a generalization of equality. For now, be alerted to the fact that "≡" and "=" do not necessarily have the same properties. It's tempting for instance to make statements such as, "$a \equiv b \pmod{m}$ implies $a - b \equiv 0 \pmod{m}$". But just because this is true for = doesn't mean it's also true for ≡! In this case the statement turns out to be true, but it requires proof – and in this class you are not allowed to make assertions that have not been proven.[3] △

Remark 16. **(*Important*) Many references use the expression "$a \bmod m$" to denote the remainder when a is divided by m. We prefer not to use this notation, since it can sometimes be confusing. For example, according to this notation it is not true that $12 = 17 \bmod 5$, even though it is true that $12 \equiv 17 \pmod{5}$. We will use instead the expression "$\bmod(a, m)$" to indicate the remainder of a when divided by m. This is the notation used in most mathematical software (such as Excel and Matlab), and it reflects the fact that the remainder is a function of a and m. △

There is an alternative (and very useful) way to determine modular equivalence. Suppose that $a \equiv b \pmod{m}$, so that a and b have the same remainder when divided by m. Let's call this remainder r. Then we can write $a = p \cdot m + r$ and $b = q \cdot m + r$ for some integers p, q It follows from

[3] This may be one reason why not many mathematicians are politicians, and vice-versa.

basic algebra that $a - p \cdot m = b - q \cdot m$. We then proceed step-by-step using basic algebra as follows:

$$\begin{aligned} & a - p \cdot m = b - q \cdot m \\ \Rightarrow \quad & a - b = p \cdot m - q \cdot m \\ \Rightarrow \quad & a - b = (p - q) \cdot m. \\ \Rightarrow \ & a - b \text{ is divisible by } m. \end{aligned}$$

In summary, we have shown that

$$\text{If } a \equiv b \pmod{m} \text{ then } a - b \text{ is divisible by } m.$$

which we can also write as

$$a \equiv b \pmod{m} \Rightarrow \ a - b \text{ is divisible by } m.$$

It turns out that the *converse* statement is also true.[4] The converse statement is:

$$\text{If } a - b \text{ is divisible by } m \text{ then } a \equiv b \pmod{m}.$$

One way to prove this is to prove the *contrapositive*, which is logically equivalent.[5] In this case, the contrapositive statement is, "If $a \not\equiv b \pmod{m}$, then $a - b$ is not divisible by m").

Exercise 17. Finish the proof of the contrapositive by filling in the blanks:

Suppose $a \not\equiv b \pmod{m}$. Let r be the remainder of a when divided by $\underline{\ < 1 > \ }$, and let s be the remainder of $\underline{\ < 2 > \ }$ when divided by $\underline{\ < 3 > \ }$. Since the remainders are unequal, it follows that one must be bigger than the other: let us choose a to be the number with the larger remainder, so that $r > \underline{\ < 4 > \ }$. By the definition of remainder, we may write $a = p \cdot m + \underline{\ < 5 > \ }$, and we may also write $b = q \cdot \underline{\ < 6 > \ } + \underline{\ < 7 > \ }$. Then by basic algebra, $a - b = (p - q) \cdot \underline{\ < 8 > \ } + (r - \underline{\ < 9 > \ })$.

We want to show that $r - s$ is the remainder of $a - b$ when divided by m. To do this, we need to show that $r - s$ is between 0 and $\underline{\ < 10 > \ }$. Since $r > s$ it follows that $r - s > \underline{\ < 11 > \ }$. Furthermore, Since $r < m$ and $s \geq 0$,

[4] In general, if you have a statement of the form "If A then B", then the converse is "If B then A". Similarly, the converse of "A $\Rightarrow$ B" is, "B $\Rightarrow$ A".

[5] In general, the contrapositive of "If A as true then B is also true", is "If B is not true then A is not true". Alternatively: if you have a statement "A $\Rightarrow$ B", then the contrapositive is "not B $\Rightarrow$ not A". Unlike the converse, the contrapositive is *always* true if the original statement is true

it follows that $r - s <$ $\underline{\quad < 12 > \quad}$. So we have shown that $r - s$ is between $\underline{\quad < 13 > \quad}$ and $\underline{\quad < 14 > \quad}$, so $r - s$ is the remainder of $a - b$ when divided by m. However, $r - s > 0$, which means that $a - b$ is not divisible by $\underline{\quad < 15 > \quad}$. This is exactly what we needed to prove, so the proof is complete. ◊

We summarize Exercise 17 and the preceding discussion together in the following proposition.

Proposition 18. Given any two integers a and b, and a modulus m (m is a positive integer). Then

$$a \equiv b \pmod{m} \text{ if and only if } a - b = k \cdot m,$$

where k is an integer.

We may rewrite Proposition 18 more elegantly using mathematical shorthand as follows: Given $a, b, m \in \mathbb{Z}$, then

$$a \equiv b \pmod{m} \text{ iff } m|(a - b).$$

Note the two shorthand expressions we have used here: the symbol '$\in$' means 'contained in' or 'elements of', while the single vertical line '—' means "divides'.

The following proposition establishes important facts about modular equivalence that we'll need later.[6]

Proposition 19. Given any integers a, b, c and a positive integer n such that $a \equiv b \pmod{n}$ and $c \equiv b \pmod{n}$. Then it is also true that $a \equiv c, c \equiv a, b \equiv a$, and $b \equiv c$ (all these equivalences are $\pmod{n}$) .

Exercise 20. Prove Proposition 19. (*Hint*) ◊

Exercise 21. Suppose January 25 is a Thursday.

(a) Use Definition 13 to determine whether January 3 is a Thursday. Show your reasoning.

[6] This proposition actually establishes that modular equivalence is both *transitive* and *symmetric*. We'll talk more about transitive, symmetric relations in the Equivalence Relations chapter.

(b) Use Proposition 18 to determine whether January 31 is a Thursday. Show your reasoning.

(c) Find the nearest Thursday to January 15. Show your reasoning.

(d) Find the nearest Thursday to April 18. Show your reasoning. (Note: the year is not a leap year.)

◊

Exercise 22. Determine whether or not the following equivalences are true. Explain your reasoning. If the equivalence is not true, change one of the numbers to make it true.

(a) $71 \equiv 13 \pmod 4$

(b) $-23 \equiv 13 \pmod 6$

(c) $101 \equiv 29 \pmod 6$

(d) $50 \equiv 13 \pmod 7$

(e) $654321 \equiv 123456 \pmod 5$

(f) $1476532 \equiv -71832778 \pmod{10}$

◊

Let us now return to the problem of finding the position corresponding to the net displacement following a multi-stage trip. When you computed racetrack positions in Exercise 12, most likely you simply took the net displacements you computed in Exercise 11, divided by 5 and took remainder. However, our new concept of modular equivalence gives us another way of solving this problem – one that can be much, much easier if we're dealing with large displacements.

Example 23. Suppose Dusty drives around the 5-mile track 112 miles in a positive direction, then 49 miles in a negative direction, then 322 miles in a positive direction. To find Dusty's net displacement we may take $112 - 49 + 322 = 385$ and then take the remainder mod 5 (which turns out to be 0). But notice that:

$$\begin{aligned} 112 &\equiv 2 \pmod 5, \\ -49 &\equiv 1 \pmod 5, \\ 322 &\equiv 2 \pmod 5, \end{aligned}$$

and we compute

$$2 + 1 + 2 = 5 \equiv 0 \pmod 5.$$

We have obtained the same answer with much less work. How did we do it? By *replacing each number with its remainder.* ⧫

Can we do the same thing with multiplication?

Example 24. Suppose I travel on my racetrack at a 113 miles per hour in the positive direction for 17 hours. We may compute:

$$\text{Net displacement} : 113 \cdot 17 = 1921 \text{ miles}$$
$$\text{Final position} : 1921 = 384 \cdot 5 + 1 \Rightarrow \text{final position} = 1.$$

On the other hand, we may reach the same conclusion by a somewhat easier route:

$$113 \equiv 3 \pmod 5,$$
$$17 \equiv 2 \pmod 5,$$

and we compute

$$3 \cdot 2 = 6 \equiv 1 \pmod 5.$$

Again, we have obtained the correct answer by *replacing each number with its remainder.* ⧫

Does this work in general? In fact it does! However, this requires a mathematical proof. We will discuss the proof in a later section – but at least our discussion shows that *arithmetic with remainders* is meaningful and useful.

If we're doing arithmetic $\pmod n$, then the remainders will necessarily be between 0 and $n - 1$ (inclusive). This set of remainders has a special name, which later on we'll use extensively.

Definition 25. The set $\{0, 1, \ldots, n - 1\}$ is called the *integers mod n*, and is denoted by the symbol $\mathbb{Z}_n$. △

We will need the following proposition later:

Proposition 26. Suppose $a, b \in \mathbb{Z}_n$ and $a \equiv b \pmod n$. Then $a = b$.

Figure 4.4. A UPC code

Exercise 27. Fill in the blanks in the following proof of Proposition 26.

We are given that $a, b \in \mathbb{Z}_n$, which implies that $a \geq 0$ and $b \leq$ $\underline{\quad < 1 > \quad}$, so that $-b \geq$ $\underline{\quad < 2 > \quad}$. It follows by adding these inequalities that $a - b \geq$ $\underline{\quad < 3 > \quad}$. Furthermore, since $a, b \in \mathbb{Z}_n$, we have $a \leq$ $\underline{\quad < 4 > \quad}$ and $b \geq$ $\underline{\quad < 5 > \quad}$, so that $-b \leq$ $\underline{\quad < 6 > \quad}$. It follows by adding these two results that $a - b \leq$ $\underline{\quad < 7 > \quad}$. In other words, $a - b$ is between $\underline{\quad < 8 > \quad}$ and $\underline{\quad < 9 > \quad}$.

Furthermore, we were given that $a \equiv b \pmod{n}$. It follows from Proposition 18 that $\underline{\quad < 10 > \quad}$ is a multiple of $\underline{\quad < 11 > \quad}$. The only multiple of $\underline{\quad < 12 > \quad}$ between $\underline{\quad < 13 > \quad}$ and $\underline{\quad < 14 > \quad}$ is $\underline{\quad < 15 > \quad}$, so that $a - b =$ $\underline{\quad < 16 > \quad}$. It follows by algebra that $a =$ $\underline{\quad < 17 > \quad}$, and the proof is complete. ◊

Exercise 28. Now you're ready! Give answers for the seven examples at the beginning of this chapter. ◊

4.3 Modular equations

4.3.1 More uses of modular arithmetic

Supermarkets and retail stores have a dirty little secret. Every time you scan your purchases, they're using modular arithmetic on you! In fact, modular arithmetic is the basis for UPC and ISBN bar codes. We will use these practical examples to introduce *modular equations*.

Exercise 29. *Universal Product Code* (UPC) symbols are now found on most products in grocery and retail stores. The UPC symbol (see Figure 4.4) is a 12-digit code which identifies the manufacturer of a product and the product itself. The first 11 digits contain the information, while the twelfth digit is used to check for errors that may occur while scanning. If $d_1 d_2 \cdots d_{12}$ is a valid UPC code, then

$$3 \cdot d_1 + 1 \cdot d_2 + 3 \cdot d_3 + \cdots + 3 \cdot d_{11} + 1 \cdot d_{12} \equiv 0 \pmod{10}.$$

So the scanning device that cashiers use reads the code and adds up the numbers mod 10. If they don't add to zero, then the device knows it hasn't scanned properly. (Smart little bugger, that scanner is!)

(a) Show that the UPC number 0-50000-30042-6, which appears in Figure 4.4, is a valid UPC number.

(b) Show that the number 0-50000-30043-6 is not a valid UPC number.

(c) (*for geeks*) Write a program or Excel spreadsheet that will determine whether or not a UPC number is valid.

(d) One common scanning error occurs when two consecutive digits are accidentally interchanged. This is called a ***transposition error***. The UPC error detection scheme can catch most transposition errors. Using the UPC in (a) as the correct UPC, show that the transposition error 0-50003-00042-6 is detected. Find a transposition error that is not detected.

(e) Using the UPC in (a) as the correct UPC, show that the single-digit error 0-50003-30042-6 is detected.

(f) **Prove that the UPC error detection scheme detects all single digit errors. (*Hint*)

$\Diamond$

It is often useful to use an ***inner product*** notation for these types of error detection schemes.[7] In the following text, the notation

$$(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$$

[7] You may have seen inner products (a.k.a. "dot products") in one of your math classes talking about vectors.

will be used to mean

$$d_1w_1 + d_2w_2 + \cdots + d_kw_k \equiv 0 \pmod{n}.$$

Exercise 30. Every book has an *International Standard Book Number* (ISBN-10) code. This is a 10-digit code indicating the book's language, publisher and title. The first digit indicates the language of the book; the next three identify the publisher; the next five denote the title; and the tenth digit is a check digit satisfying

$$(d_1, d_2, \ldots, d_{10}) \cdot (1, 2, \ldots, 10) \equiv 0 \pmod{11}.$$

ISBN-10 codes are nice in that all single-digit errors and most transposition errors can be detected. One complication is that d_{10} might have to be a 10 to make the inner product zero; in this case, the character 'X' is used in the last place to represent 10.

(a) Show that 3-540-96035-X is a valid ISBN-10 code.

(b) Is 0-534-91500-0 a valid ISBN-10 code? What about 0-534-91700-0 and 0-534-19500-0?

(c) How many different possible valid ISBN-10 codes are there?

(d) Write a formula of the form $d_{10} \equiv \ldots \pmod{\ldots}$ to calculate the check digit in an ISBN-10 code. (*Hint*)

(e) *Prove that any valid ISBN-10 code also satisfies:

$$(d_1, d_2, \ldots, d_{10}) \cdot (10, 9, \ldots, 1) \equiv 0 \pmod{11}.$$

(f) * Prove that if $(d_1, d_2, \ldots, d_9, d_{10})$ is a valid ISBN-10 code, then $(d_{10}, d_9, \ldots, d_2, d_1)$ is also a valid ISBN-10 code (as long as d_{10} is not equal to X).

(g) (*for geeks*) Write a computer program or Excel spreadsheet that calculates the check digit for the first nine digits of an ISBN code.

(h) A publisher has houses in Germany and the United States. Its German prefix is 3-540. Its United States prefix will be 0-*abc*. Find four possibilities for *abc* such that the rest of the ISBN code will be the same for a book printed in Germany and in the United States.

(i) **Prove that the ISBN-10 code detects all single digit errors. (*Hint*)

(j) **Prove that the ISBN-10 code detects all transposition errors. (*Hint*)

◊

4.3.2 Solving modular equations

In Exercise 30 part (h) you solved a modular equation with three variables by trial and error: you couldn't solve for one variable at a time, so you had to test out sets of values for a, b, c together and see if the the ISBN equation held. The UPC and ISBN error detection schemes themselves, given again below, are examples of modular equations with 12 and 10 variables, respectively:

$$(3 \cdot d_1) + (1 \cdot d_2) + (3 \cdot d_3) + \cdots + (3 \cdot d_{11}) + (1 \cdot d_{12}) \equiv 0 \pmod{10}.$$

$$(d_1, d_2, \ldots, d_{10}) \cdot (10, 9, \ldots, 1) \equiv 0 \pmod{11}.$$

Can the above equations be solved? You may remember from college algebra that you can't uniquely solve a single equation for 10 or 12 variables.[8] But if we supply additional information so that only variable is left to solve for, then we can use the resulting equation to find the value of the variable. Let's try.

Exercise 31. Suppose you're given the following UPC: 1-54637-28190-?. Write a modular equation to solve for the missing check digit, then solve it. ◊

In the preceding exercise you should have come up with an equation that looks like:

$$(3 \cdot 1) + \ldots + (3 \cdot 0) + (1 \cdot x) \equiv 0 \pmod{10}.$$

How did you solve this? One possible method is to add up all the terms the left side of the equation short of the variable, and then figure out how much you need to add to that sum to get a number divisible by 10. Keep

[8] Actually, there are many possible combinations of 10 or 12 variables which make the equations work.

this method and your own method (if different) in mind, as they are good intuition on how to solve these problems in general.

Is there a *unique* answer for x? Practically, for a UPC code x must be between 0 and 9 (that is, $x \in \mathbb{Z}_{10}$: with this restriction, there is indeed only one solution. But if we remove that restriction, then there are many solutions. For instance $x = 12$ and $x = 22$ both work (check this for yourself). Can you think of any other integers that work?

In fact any integer equivalent to 2 (mod 10) also works. But from our intuitive methods, would we have come up with these other possible solutions? In most cases not. Therefore we need to come up with a general method that will give us all possible integer solutions of a modular equation. Just as in basic algebra, we'll start with simpler equations and move to more complicated ones.

Example 32. Let's start with a basic modular equation involving addition:

$$8 + x \equiv 6 \pmod{11}$$

From algebra we understand how to solve an equation with an $=$ sign, but what do we do with this $\equiv$ sign? In fact, we can turn it in to an $=$ sign by using Proposition 18, which says that $8 + x \equiv 6 \pmod{11}$ means the same as:

$$8 + x = k \cdot 11 + 6$$

And then we can solve for x like any other equation. The result is

$$x = k \cdot 11 - 2$$

So we solved for x, but what numbers does x actually equal? What does $k \cdot 11 - 2$ mean? k is an integer, therefore x can equal -2 (if $k = 0$), or -13 (if $k = -1$), or 9 (if $k = 1$), and so on. In other words x equals -2 plus any integer multiple of 11, which, by the definition of modular equivalence, means

$$x \equiv -2 \pmod{11}$$

This is a correct solution: but it's not the only way to write it. It would be just as valid to write

- $x \equiv -13 \pmod{11}$
- $x \equiv 20 \pmod{11}$

- $x \equiv 130 \pmod{11}$
- ...

Notice however that there is only one way to write the solution in terms of a number in $\mathbb{Z}_{11}$, namely:

$$x \equiv 9 \pmod{11}$$

In order to avoid ambiguity, mathematicians and textbooks always write solutions mod n in terms of numbers in $\mathbb{Z}_n$. In our current example, it's easy enough to obtain the standard solution ($x \equiv 9 \pmod{11}$) directly from the equation $x = k \cdot 11 - 2$? by taking one of the 11's and adding it to the -2 to get

$$x = (k-1) \cdot 11 + 11 - 2 = (k-1) + 9,$$

giving $x \equiv 9 \pmod{11}$.

♦

To summarize our general method for solving modular equations so far:

1. Turn the $\equiv$ sign into an $=$ sign using the definition of modular equivalence. This introduces an additional variable k.
2. Find (by trial and error if necessary) the value of k that puts x in the appropriate range.
3. Change the equation back into an equivalence.

Exercise 33. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $5 + x \equiv 1 \pmod{3}$

(b) $25 + x \equiv 6 \pmod{12}$

◊

Now let's spice things up with some multiplication:

Example 34. Given the equation

$$5x + 3 \equiv 9 \pmod{11}.$$

Using the definition of modular equivalence, this becomes

$$5x + 3 = 11k + 9.$$

Solving this equality using basic algebra gives us

$$x = \frac{11k + 6}{5}.$$

Now remember that x must be an *integer*. In order for the right side to be an integer, we need to find a k that makes $\frac{11k+6}{5}$ an integer. At this point we may use trial and error to find a k in $\mathbb{Z}_5$ such that $11 \cdot k + 6$ is a multiple of 5. We get $k = 4$; and in fact adding $5 \cdot n$ to 4 also works for any $n \in \mathbb{Z}$, since $5n$ is always divisible by 5. Now we can solve for x by substituting $k = 4 + 5n$ back in to the previous equation:

$$\begin{aligned} x =& \frac{11(4 + 5 \cdot n) + 6}{5} \\ &= \frac{11 \cdot 4 + 6}{5} + \frac{11 \cdot (5n)}{5} \\ &= 10 + 11n \end{aligned}$$

Therefore $x \equiv 10 \pmod{11}$ is the general solution. You may check (which is always a good idea!) by plugging $10 + 11n$ for a couple values of n back into the original equation, and you'll see these numbers work. ♦

Just to make sure you've mastered the process, we'll give another example:

Example 35. To solve the equation $4x+5 \equiv 7 \pmod{11}$ we proceed step by step (note that the symbol $\Rightarrow$ is mathematicians' shorthand for "implies"):

$$\begin{aligned} & 4x + 5 \equiv 7 \pmod{11} \\ \Rightarrow & 4x + 5 = 11k + 7 && \text{(by modular equivalence)} \\ \Rightarrow & x = \frac{11k + 2}{4} && \text{(basic algebra)} \end{aligned}$$

Now, $11k + 2$ is a multiple of 4 when $k = 2$, as well as when k equals 2 plus any multiple of 4. Therefore $k = 2 + 4n$, hence we may continue from the previous equation:

$$\begin{aligned} x &= \frac{2+11k}{4} \\ \Rightarrow x &= \frac{2+11\cdot(2+4n)}{4} && \text{(substitution)} \\ \Rightarrow x &= 6+11n. && \text{(simplification)} \end{aligned}$$

♦

Remark 36. Example 35 demonstrates some good practices that you can make use of when you write up your own proofs:

- Instead of using a sentence to explain your reasoning for each step, place the reason to the right (like I did). This shrinks down the size of the proof.
- Another way to shrink the proof is to use mathematical equations, expressions, and symbols (such as $\Rightarrow, \forall$) whenever you can to accurately communicate your steps in the proof.

△

In summary, a general method for solving modular equations is:

1. Turn the $\equiv$ sign into an $=$ sign using the definition of modular equivalence (just as with modular addition). This introduces another constant k.
2. Solve the resulting equation for your variable x. If the expression is a fraction, then go to step 5. Otherwise, go to step 3.
3. By trial and error, find a value k_0 for k which makes the fraction into an integer.
4. Substitute k_0 + n·(denominator) in for k, and simplify.
5. Change the equation back into an equivalence.

Exercise 37. Find all $x \in \mathbb{Z}$ satisfying each of the following equations. (If there's no solution, then you can say "no solution"– but show why!)

(a) $9x \equiv 3 \pmod 5$

(b) $5x \equiv 1 \pmod 6$

(c) $7x \equiv 9 \pmod{13}$

(d) $8x \equiv 4 \pmod{12}$

(e) $11x \equiv 2 \pmod 6$

(f) $27x \equiv 2 \pmod 9$

(g) $3 + x \equiv 2 \pmod 7$

(h) $5x + 1 \equiv 13 \pmod{23}$

(i) $5x + 1 \equiv 13 \pmod{26}$

(j) $3x + 2 \equiv 1 \pmod 6$

$\Diamond$

One major disadvantage of our solution method is the use of trial and error in step 3. If large numbers are involved, then this step can take a long time. However, there are techniques to speed things up:

Example 38. Consider the equation $79x \equiv 9 \pmod{15}$. In Section 4.2 we mentioned that when we're doing arithmetic mod n, we can replace any number with its remainder mod n without changing the answer. In this example then, we can replace the 79 with its remainder mod 15, which is 4. Thus we have

$$4x \equiv 9 \pmod{15},$$

which leads to

$$x = \frac{15k + 9}{4}.$$

By rewriting the numerator, we can simplify the right-hand side:

$$x = \frac{(12k + 3k) + (8 + 1)}{4} = 3k + 2 + \frac{3k + 1}{4}.$$

and we readily discover that $k = 1+4n$ makes the right-hand side an integer, so that

$$x = \frac{15 \cdot (1 + 4n) + 9}{4} = 6, \text{ or } x \equiv 6 \pmod{15}.$$

$\blacklozenge$

Just one more similar example:

Example 39. To solve the equation $447x+53 \equiv 712 \pmod{111}$ we proceed as follows:

$$\begin{aligned}
447x + 53 &\equiv 712 \pmod{111} && \\
\Rightarrow 3x + 53 &\equiv 46 \pmod{111} && \text{(modular equivalence)} \\
\Rightarrow 3x + 53 &= 46 + 111k && \text{(modular equivalence)} \\
\Rightarrow 3x &= -7 + 111k && \text{(basic algebra)} \\
\Rightarrow x &= \frac{-7 + 111k}{3} && \text{(basic algebra)} \\
\Rightarrow x &= \frac{-7}{3} + 37k && \text{(basic algebra)}
\end{aligned}$$

It should be clear that no value of k makes the right side an integer. Hence x has no solution. You may have run into a similar situation in a previous exercise. ♦

Exercise 40. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $112x \equiv 2 \pmod{6}$

(b) $74x \equiv 9 \pmod{13}$

(c) $856x \equiv 4 \pmod{123}$ (*Hint*)

(d) $272x \equiv 24 \pmod{9}$

(e) $242x + 39 \equiv 489 \pmod{236}$

(f) $469x + 122 \equiv 1321 \pmod{231}$

(g) $246x + 200 \equiv 401 \pmod{81}$

(h) $339 + 411x \equiv 2 \pmod{297}$

(i) $530x - 183 \equiv 215 \pmod{128}$

◊

From parts (h) and (i) of Exercise 40 we see that even our trick with modular equivalences doesn't make all modular equations easy to solve. When the coefficient of x and the modulus are both large, you may end up needing *lots* of trial and error. And mathematicians are a bit snobby: we prefer solution methods that don't require *any* trial and error. There is actually a method that both eliminates trial and error and solves *any* modular equation: this is the Euclidean algorithm, which we'll discuss later.

4.4 The integers mod n (also known as $\mathbb{Z}_n$)

4.4.1 Arithmetic with remainders

Several times now in this chapter we've simplified our modular calculations by replacing numbers with their remainders mod n (remember, we have defined these remainders as the set $\mathbb{Z}_n$). We will now fulfill the promise we made at the end of the first section by proving that if you replace numbers with their remainders, we don't change the result of our modular calculations. That is, we'll show that modular arithmetic can be thought of as *arithmetic with remainders*.

Before we do this, we need to address an important issue. Consider the case of $Z_5 = \{0, 1, 2, 3, 4\}$, so 3 and 4 are in Z_5. However the sum $3 + 4$ is 7, which is not in Z_5. If we're going to do arithmetic with the remainders, we should define a "sum" on Z_n such that the result is also in Z_n. This motivates the following two definitions:

Definition 41. ***Modular Addition***

The sum mod n of two integers mod n is the remainder left after dividing their regular sum by n; that is, if $x, y \in \mathbb{Z}_n$ then

$$x \oplus y = r \text{ iff } x + y = r + sn \text{ and } r \in \mathbb{Z}_n.$$

△

Note that in Definition 41 we write $x \oplus y = r$ rather than $x \oplus y \equiv r \pmod{n}$, since $x \oplus y$ is defined to be *equal* to the remainder. The same holds for the following definition:

Definition 42. ***Modular Multiplication***

The product mod n of two integers mod n is the remainder left after dividing their regular product by n; that is, if $x, y \in \mathbb{Z}_n$ then

$$x \odot y = r \text{ iff } x \cdot y = r + sn \text{ and } r \in \mathbb{Z}_n.$$

△

It is important to note that the operations $\oplus$ and $\odot$ *depend on the modulus involved*. We must always make sure that the modulus is clearly specified before talking about $\oplus$ and $\odot$.

Our first step towards showing that ordinary arithmetic can be replaced with arithmetic with remainders is the following proposition:

Proposition 43. Given $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}_n$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

(a) $a + c \equiv b \oplus d \pmod{n}$,

(b) $a \cdot c \equiv b \odot d \pmod{n}$.

We will furnish the proof of part (a): part (b) will be left as an exercise.

PROOF. Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a = b + sn \quad \text{and} \quad c = d + tn \qquad \text{(definition of modular equivalence)}$$

Therefore,

$$a + c = b + d + (s + t)n \qquad \text{(subs. and basic algebra)}$$

Now by the definition of $\oplus$ there is some $p \in \mathbb{Z}$ such that $b+d = (b \oplus d)+pn$; therefore

$$a+c = (b \oplus d)+pn+(s+t)n = (b \oplus d)+(p+s+t)n. \qquad \text{(subs. and basic algebra)}$$

Hence by the definition of modular equivalence,

$$a + c \equiv b \oplus d \pmod{n}.$$

□

Exercise 44.

(a) Prove part (b) of Proposition 43.

(b) Come up with a definition for modular subtraction (use the symbol $\ominus$).

(c) Using your definition, prove the following:

Given $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}_n$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b \ominus d \pmod{n}$.

◊

Now that we have proven Proposition 43, we can combine operations into more complicated equations and show equivalence.

Exercise 45.

(a) Using part (b) of Proposition 43 above, show that if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_n$ and $a \equiv b \pmod{n}$ then $a^2 \equiv b \odot b \pmod{n}$.

(b) Using part (a) prove a similar relation involving a^3.

(c) Using part (b) prove a similar relation involving a^4.

(d) From parts (a),(b) and (c), what do you conclude about a^k where k is any natural number?

◊

Exercise 46.

(a) Given $a, c, e \in \mathbb{Z}$ and $b, d, f \in \mathbb{Z}_n$ where $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, and $e \equiv f \pmod{n}$. Show using Proposition 43 that

$$(a + c) + e \equiv (b \oplus d) \oplus f \pmod{n}.$$

(*Hint*)

(b) Given $a, c, e \in \mathbb{Z}$ and $b, d, f \in \mathbb{Z}_n$ where $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, and $e \equiv f \pmod{n}$. Show using Proposition 43 that

$$(a \cdot c) + e \equiv (b \odot d) \oplus f \pmod{n}.$$

(c) Given $a, c, e \in \mathbb{Z}$ and $b, d, f \in \mathbb{Z}_n$ where $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, and $e \equiv f \pmod{n}$. Show using Proposition 43 that

$$(a + c) \cdot e \equiv (b \oplus d) \odot f \pmod{n}.$$

◊

In the same way as in Exercise 46, it is possible to show that *any* arithmetical expression involving integers with no matter how many additions,

multiplications, and subtractions, can be shown to be equivalent mod n to the corresponding arithmetical expression in $\mathbb{Z}_n$ using the modular operations $\oplus, \odot, \ominus$.

This completes our discussion showing that arithmetic mod n can be reduced to arithmetic in $\mathbb{Z}_n$. What we've shown can simplify other modular arithmetic arguments as well:

Exercise 47. Prove the following proposition.

Proposition: Given $a, b, c, d \in \mathbb{Z}$ where $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

(a) $a + c \equiv b + d \pmod{n}$,

(b) $a \cdot c \equiv b \cdot d \pmod{n}$.

Note these are slightly different from (a) and (b) of Proposition 43 (in fact, to prove (a) here you need to use part (a) of Proposition 43 twice, and similarly for (b)). ◊

Exercise 48. Prove or disprove:

(a) $833 \cdot 222 \cdot 949 \equiv 133 \cdot 922 \cdot 249 \pmod{7}$

(b) $(12345 \cdot 6789) + 1357 \equiv (98765 \cdot 13579) + 9876 \pmod{10}$

◊

4.4.2 Cayley tables for $\mathbb{Z}_n$

The fact that we can replace integers with their remainders mod n leads us to a simpler way of thinking about modular arithmetic. First, recall the integer number line, pictured (again) in Figure 4.5: We may relabel the integers with their remainders mod 5, pictured in Figure 4.6: All the numbers equivalent to 0 mod 5 are labeled 0; all the numbers equivalent to 1 mod 5 are labeled 1; and so on. The whole infinite set of integers then is reduced to repetitive cycles of the integers 0 through 4. In other words, all the integers are equivalent to either $0, 1, 2, 3$, or 4, mod 5.

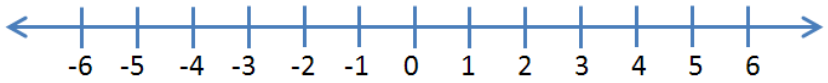


Figure 4.5. The usual number line

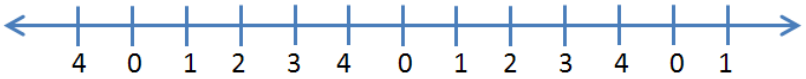


Figure 4.6. The number line mod 5

Furthermore, as we just discussed, the sum and product mod 5 of any two numbers is exactly equivalent to the sum and product mod 5 of their corresponding remainders. Therefore, the sum or product of *any* two numbers mod 5 can be determined by the sum or product of the integers $0 - 4$. So we only have to focus on the sums and products of these five numbers to get the result of any modular calculation mod 5.

Let's calculate these sums and products then. We are only using the remainders for mod 5 (recall we have already defined this set as $\mathbb{Z}_5$). The following table then gives the results of addition mod 5 for $\mathbb{Z}_5$:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 4.1: Addition table for $\mathbb{Z}_5$

As an example of how to read this table, the entry in the "2" row and the "3" column is 0, which tells us that $2 \oplus 3 = 0$ (remember, this result depends on fact that we're working in mod 5).

The following table gives the results of multiplication mod 5 for $\mathbb{Z}_5$:

Again, looking at the entry in the "2" row and the "3" column we see 1, which tells us that $2 \odot 3 = 1$.

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 4.2: Multiplication table for $\mathbb{Z}_5$

Similarly, for each set of numbers $\mathbb{Z}_n$ we can construct a table to determine the result of any possible calculation mod n. These type of tables are known as ***Cayley tables***. We will see them often throughout the course.

Exercise 49. Use the Cayley table to calculate each of the following using $\oplus$ and $\odot$ in $\mathbb{Z}_5$ (remember, compute the remainders *before* doing the arithmetic).

(a) $\mod (456 \cdot (252 + 54), 5)$

(b) $\mod (523 + (4568 \cdot (43 + 20525)), 5)$

(c) $\mod ((456 \cdot 252) + (456 \cdot 54), 5)$

(d) $\mod (523 + ((4568 \cdot 43) + (4568 \cdot 20525)), 5)$

◊

Later on (in the chapter on Equivalence Relations) we'll show another way of looking at the integers mod n.

4.4.3 Closure properties of $\mathbb{Z}_n$

Recall that in Chapter 1 we introduced the complex numbers, then studied their arithmetic properties. In this section, we'll do the same thing with the numbers $\mathbb{Z}_n$ that we have just defined.

Example 50. To start exploring, first consider $\mathbb{Z}_8$. Tables 4.3 and 4.4 are the addition and multiplication tables for $\mathbb{Z}_8$, respectively.

♦

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Table 4.3: Addition table for $\mathbb{Z}_8$

$\odot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Table 4.4: Multiplication table for $\mathbb{Z}_8$

There is an important feature exhibited in both Table 4.3 and Table 4.4 that is easy to overlook. Notice that every entry in the table is also an element of $\mathbb{Z}_8$. You can think of the set $\{0, ..., 7\}$ as a closed box, and when you add or multiply any two numbers in that box mod 8, you always get another number in that box, never outside of it (indeed because addition and multiplication mod 8 return a remainder that is some number $0 - 7$). We express this mathematically by saying that $\mathbb{Z}_8$ is ***closed*** under addition and multiplication mod 8. It seems reasonable that the same should be true for any $\mathbb{Z}_n$, and we state this formally as a proposition (as mathematicians are wont to do):

Proposition 51. $\mathbb{Z}_n$ is closed under modular addition and multiplication, for all positive integers n.

Exercise 52. Prove Proposition 51. That is, show that the modular sum and modular product of two elements of $\mathbb{Z}_n$ are also in $\mathbb{Z}_n$. (*Hint*) $\Diamond$

Please note that closure is not in general a trivial property, and there are many examples of number systems that are not closed under various operations. For instance, the positive integers are not closed under the operation of subtraction, because (for example) $5-7$ is not a positive integer. Similarly, the positive integers are not closed under the operation of square root, because the square root of 2 is not an integer.

Exercise 53. For each of the following number systems, indicate whether or not they are closed under (i) addition (ii) subtraction (iii) multiplication (iv) division (v) square root. (*Hint*)

(a) The integers

(b) The rational numbers

(c) The real numbers

(d) The positive rational numbers

(e) The positive real numbers

(f) The nonzero real numbers

◊

Exercise 54. Prove that the complex numbers are closed under complex addition and multiplication. ◊

4.4.4 Identities and inverses in $\mathbb{Z}_n$

Next, we want to look at some additional properties that were introduced in Chapter 3, namely identities and inverses (both additive and multiplicative). This time we'll go through these properties more quickly.

Do the integers mod n have an additive identity for all n? In other words, is there a specific integer mod n that added to a leaves a unchanged? For the specific case of $\mathbb{Z}_8$, we can see from the first row of Table 4.3 that $0 \oplus a = a$ for any $a \in \mathbb{Z}_8$. Similarly, the first column of Table 4.3 show that $a \oplus 0 = a$ for any $a \in \mathbb{Z}_8$. Is this true for *any* $\mathbb{Z}_n$? the following proposition shows that it is.

Proposition 55. $0 \in \mathbb{Z}_n$ is the additive identity of $\mathbb{Z}_n$.

Proof. Given any $a \in \mathbb{Z}_n$, then $a \oplus 0$ is computed by (a) compute $a+0$ using ordinary addition, then (b) taking the remainder mod n. Since $a + 0 = a$,

and $0 \leq a < n$, it follows that the remainder is also a. Hence $a \oplus 0 = a$. We can show that $0 \oplus a = a$ in the same way. Thus 0 satisfies the definition of identity for $\mathbb{Z}_n$. □

Exercise 56. Give a similar proof that 1 is the multiplicative identity for $\mathbb{Z}_n$ when $n > 1$. What is the multiplicative identity for $\mathbb{Z}_n$ when $n = 1$? ◊

4.4.5 Inverses in $\mathbb{Z}_n$

Now let's look to see if the integers mod n have additive and multiplicative inverses. For each element of $\mathbb{Z}_n$ is there a corresponding element of $\mathbb{Z}_8$ such that their modular sum is the additive identity (that is, 0)? You may see in Table 4.3 that each row of the addition table contains the additive identity, 0 (for example, $1 \oplus 7 = 0$). It follows that in $\mathbb{Z}_8$, each element has an additive inverse. If we shrink or expand the table to cover all moduli n, would we find the same thing in every table? We should. This motivates the following:

Proposition 57. Let $\mathbb{Z}_n$ be the integers mod n and $a \in \mathbb{Z}_n$. Then for every a there is an additive inverse $a' \in \mathbb{Z}_n$.

In other words: for any $a \in \mathbb{Z}_n$ in we can find an a' such that:

$$a \oplus a' = a' \oplus a = 0.$$

We structure the proof of Proposition 57 as an exercise. We prove the two cases $a = 0$ and $a \neq 0$ separately.

Exercise 58.

(a) Show that $0 \in \mathbb{Z}_n$ has an additive inverse in $\mathbb{Z}_n$.

(b) Suppose a is a nonzero element of $\mathbb{Z}_n$ (in mathematical shorthand, we write this as: $a \in \mathbb{Z}_n \setminus \{0\}$), and let $a' = n - a$.

  (i) Show that a' is in $\mathbb{Z}_n$. (*Hint*)

  (ii) Show that $a \oplus a' = a' \oplus a = 0 \pmod{n}$: that is, a' is the additive inverse of a.

$\Diamond$

Now can we do the same thing for multiplication? That is, for all integers a mod n, is there a corresponding integer mod n such that their product is the multiplicative identity?

Let's see if this is true in $\mathbb{Z}_8$. Consider the multiplication table for $\mathbb{Z}_8$ in Table 4.4. Scanning the rows do we find the multiplicative identity 1 in every row?

Looking at the table, we find that rows 0, 2, 4, and 6 do not contain a 1. We would state this formally in the following way: for $n = 0$, 2, 4, or 6, there is no integer $k \in \mathbb{Z}_8$ such that $k \odot n \equiv 1 \pmod 8$. Hence not every integer mod 8 has a multiplicative inverse.

A little thought should convince you that 0 *never* has a multiplicative inverse for any $\mathbb{Z}_n$. This means that it's not possible to prove a multiplicative version of Proposition 57, since we have a ***counterexample*** that shows that not every element of $\mathbb{Z}_n$ has an inverse, no matter what n is.

Remark 59. This example shows that it's often easier to *disprove* something than to prove it! To disprove a general statement, you only need to find *just one* counterexample, whereas an unlimited number of examples can never prove a general statement. $\triangle$

However, all is not lost as far as multiplicative inverses are concerned. We will see later that they play a very important role when we consider arithmetic with the *nonzero* elements of $\mathbb{Z}_n$:

Exercise 60.

(a) Find an integer $n > 2$ such that all *nonzero* elements of $\mathbb{Z}_n$ have multiplicative inverses.

(b) Find two additional values of $n > 5$ such that all nonzero elements of $\mathbb{Z}_n$ have multiplicative inverses.

(c) What do the three numbers you found in (a) and (b) have in common?

$\Diamond$

4.4.6 Other arithmetic properties of $\oplus$ and $\odot$

In many respects, $\oplus$ and $\odot$ are very similar to the ordinary arithmetic operations $+$ and $\cdot$. It makes sense that they too should be associative, distributive, and commutative (recall these properties were defined in Section 2.2.1). But as mathematicians, it's not enough for something to "make sense". We need solid proof. So, voilà:

Proposition 61. In the following n is an arbitrary positive integer and a, b, c denote arbitrary elements of $\mathbb{Z}_n$.

1. *Modular addition and multiplication are commutative:*

$$a \oplus b = b \oplus a$$
$$a \odot b = b \odot a.$$

2. *Modular addition and multiplication are associative:*

$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$
$$(a \odot b) \odot c = a \odot (b \odot c).$$

3. *Modular multiplication distributes over modular addition:*

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c).$$

Proof. We'll do the proof that modular addition is associative, and you will prove the other statements as exercises (the proofs are pretty similar). The proof strategy is a familiar one: prove modular arithmetic properties by making use of the corresponding properties of ordinary arithmetic.

Modular addition is associative: Given a, b, c are elements of $\mathbb{Z}_n$, it's also true that a, b, c are integers. By Proposition 43, it follows that:

$$a \oplus b \equiv a + b \pmod{n}.$$

We may use Proposition 43 a second time to obtain:

$$(a \oplus b) \oplus c \equiv (a + b) + c \pmod{n}.$$

Using the same reasoning (applying Proposition 43 twice), we can also show that:

$$a \oplus (b \oplus c) \equiv a + (b + c) \pmod{n}.$$

Now here's where we use regular arithmetic. The associative property of integer addition tells us that $a+(b+c)=(a+b)+c$, and we can substitute into the previous equivalence to obtain:

$$a \oplus (b \oplus c) \equiv (a+b)+c \pmod{n}.$$

We now have two different expressions (namely, $(a \oplus b) \oplus c$ and $a \oplus (b \oplus c)$ that are both equivalent to $(a+b)+c$. So we can apply Proposition 19 (the "transitive property") to get that

$$(a \oplus b) \oplus c \equiv a \oplus (b \oplus c) \pmod{n}.$$

Since $(a \oplus b) \oplus c$ and $a \oplus (b \oplus c)$ are both in $\mathbb{Z}_n$, it follows from Proposition 26 that $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, and the proof is complete. □

Exercise 62.

(a) Prove that addition mod n is commutative.

(b) Prove that multiplication mod n is commutative.

(c) Prove that multiplication mod n is associative.

(d) Prove part (3) of Proposition 61.

◊

4.4.7 Definition of a group

It's time for us to make a confession. All this time we've been talking about modular arithmetic, we've had an ulterior motive. We're not so interested in modular arithmetic for its own sake:[9] rather, we've spent all this time and effort discussing modular arithmetic because it provides good examples of the central concept in abstract algebra, namely, the concept of a *group*.

Notice that the set $\mathbb{Z}_n$ with the operation of $\oplus$ has an identity, and inverses, and the property of closure. Furthermore, $\mathbb{Z}_n$ is associative under $\oplus$, as we just showed. Any combination of a set and an operation that has those three properties, as well as the associative property, is called a **group**

Definition 63. A ***group*** is a set combined with an operation that has the following properties:

[9] Although you have to admit it *is* interesting.

- *Closure*: the set is closed under the operation;
- *Identity*: the set has an identity element for the operation;
- *Inverse*: every element of the set has an inverse under the operation;
- *Associative*: the operation is associative.

△

Notice that we do *not* include the commutative property in this list. Later on we'll see examples of groups that are *not* commutative.

We have shown that $\mathbb{Z}_n$ is a group under the operation $\oplus$ for *any* integer n. What about multiplication? The answer isn't quite so easy.

Exercise 64.

(a) Show that for $n \geq 2$, $\mathbb{Z}_n$ is *not* a group under $\odot$. (*Hint*)

(b) Show that the nonzero elements of $\mathbb{Z}_3$ (that is, $\mathbb{Z}_3 \setminus \{0\}$) is a group under $\odot$. Is $\mathbb{Z}_n \setminus \{0\}$ a group under $\odot$ for *every* integer $n \geq 2$? *Justify* your answer.

◊

4.5 Modular division

Before we get to modular division, we'll first look at some preliminary stuff. This all may seem irrelevant, but please be patient: we'll get to the point soon enough.

4.5.1 A sticky problem

The following problem may not seem to have anything to do with modular arithmetic, but it's an interesting problem and fun to think about. (And it will also turn out to be relevant after all!)[10]

Example 65. Someone gives us a pencil and two unmarked sticks of lengths 52 cm and 20 cm respectively (see Figure 4.7). We are told to make measuring sticks by using the pencil to make markings on the sticks. Question:

[10] This section is by David Weathers (edited by CT).

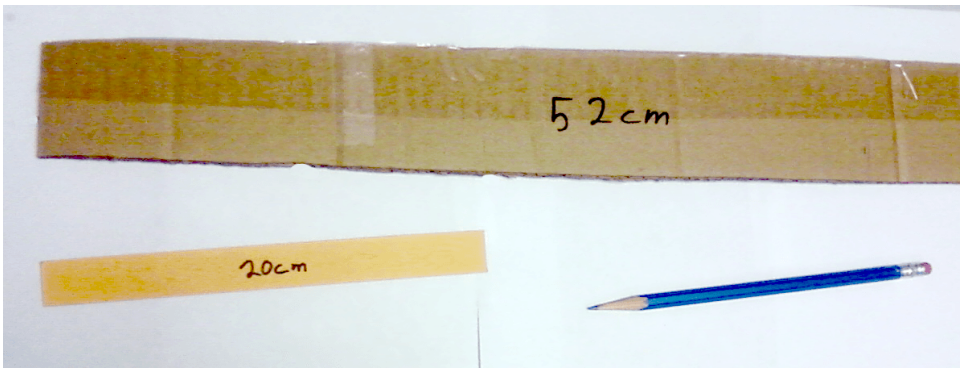


Figure 4.7. Two sticks

Figure 4.8. First mark

what is the smallest length that we can accurately measure? Clearly we can measure 20 cm lengths with the shorter rod, but is it possible to make smaller measurements?

Here's one way to look at the situation. Imagine for a moment that we lay the 20 cm measuring stick next to the 52 cm stick such that the ends line up. At that point we could make a 20 cm mark on the 52 cm stick (see Figure 4.8).

At this point we move the 20 cm stick further down the the 52 cm stick such that one end is on the pencil mark, and and make another mark. Now there are two 20 cm sections marked on the 52 cm stick, as shown in Figure 4.9.

Since we know the sum of the marked sections is 40 cm, and the length of the large stick is 52 cm, the remainder of the distance must be 12 cm, as shown in Figure 4.10. So we've actually made progress. At the beginning

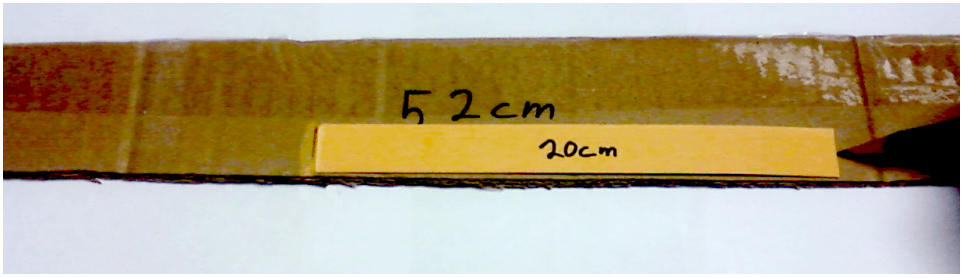


Figure 4.9. Second mark

Figure 4.10. Remaining distance

we were only able to measure lengths larger than 20 cm: but now we can measure 12 cm with the latest mark we've made.

But let's not stop there. We can use the 12 cm section to divide up the 20cm stick. This will subdivide the 20 cm stick into a 12 cm section and a 8 cm section, as shown in Figure 4.11.

Now we're rolling! Let's subdivide the 12 cm section using the 8 cm section. This will produce an 8 cm section and a 4 cm section (see Figure 4.12). Now if we try to use the 4 cm section to subdivide any of the other sections, we will no longer have a remainder. This is because 4 cm evenly divides all the other lengths we have created, as shown in Figure 4.13.

♦

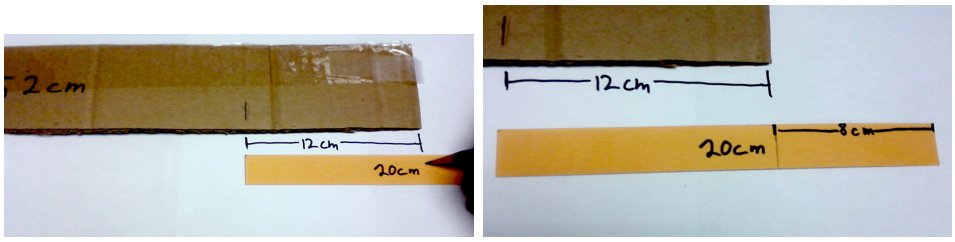


Figure 4.11. More subdivision

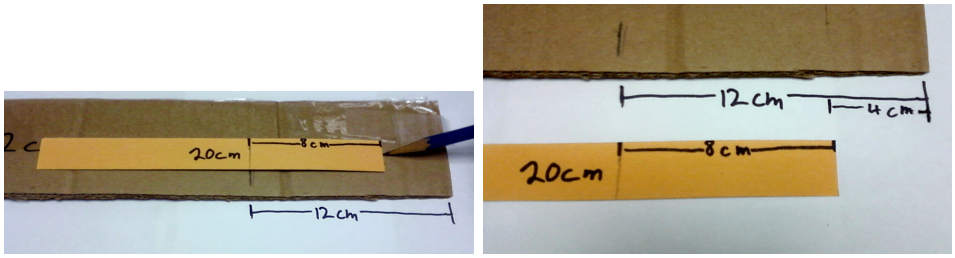


Figure 4.12. More subdivision

Exercise 66. Using the method above, find the smallest measure given sticks of length:

(a) 30 cm and 77 cm.

(b) 7 feet and 41 feet (Pretty long sticks!).

(c) 33 in and 72 in.

◊

While working on the exercises, you may have noticed that the units of measure used do not matter. The only thing that matters is the actual count of those units of measure.

Exercise 67. Using the method above:

(a) Convert the measurements in Exercise 66 part (a) into millimeters, and solve the problem again. How is your result using millimeters related to your answer to part (a) in the previous exercise?

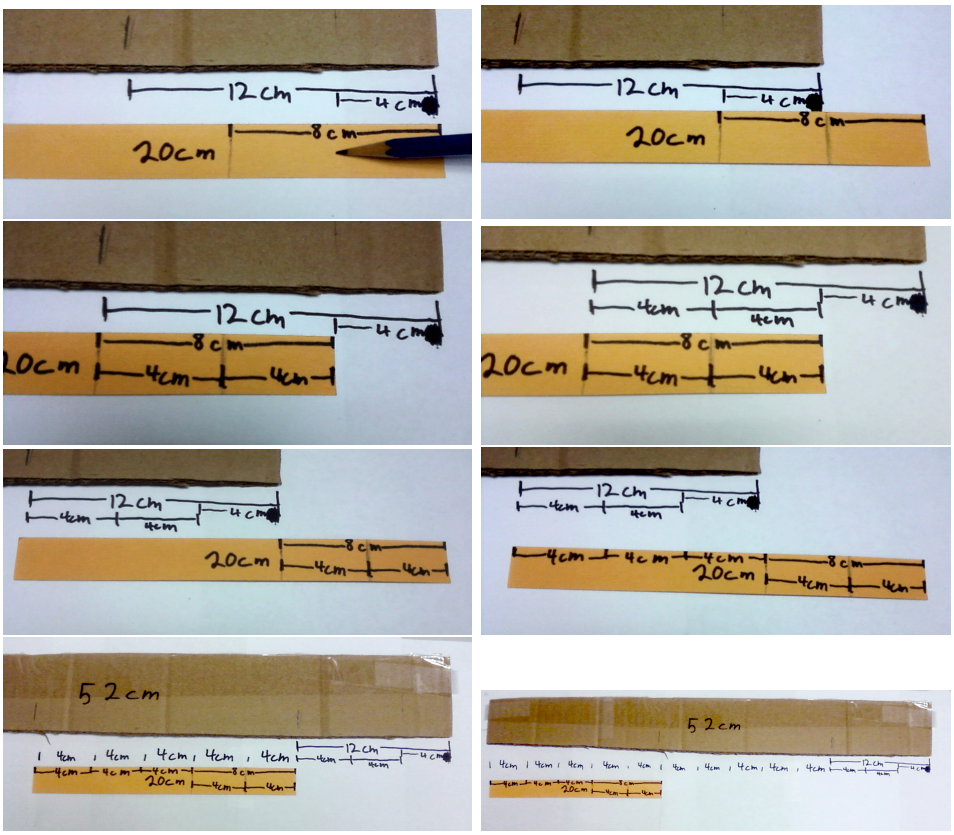


Figure 4.13. More subdivision

(b) Convert the measurements in Exercise 66 part (b) into inches, and solve the problem again. How is your result using inches related to your answer to part (a) in the previous exercise?

(c) Use what you've discovered in part (b) to quickly find a solution to the two-sticks problem when one stick is 720 inches and the other is 600 inches.

◊

4.5.2 Greatest common divisors

You may be familiar with the notion of greatest common divisor (gcd) of two numbers. The gcd is defined as the greatest number that divides the two given numbers. gcd's play a key role in modular arithmetic, as we shall see.

The general question we now consider is: What's a good way to find the gcd of two integer numbers? It may be easy to find the gcd of small numbers like 12 and 20, but what if you have to find the gcd of 583768 and 260568447?

At this point, let's think back to our two-sticks problem. We saw that when we began with sticks of length 52 and 20, we ended up with a minimum measurable distance of 4–which just so happens to be the gcd of 52 and 20! So to get the gcd of 583768 and 260568447, in theory we could try creating one stick of length 583768 and another of length 260568447 and follow the same procedure. Of course this isn't practical. So instead, we'll try to duplicate the same procedure using just algebra, without actually creating the sticks. Notice that when we subdivided a larger stick of length a into sections of the length of b, the result was essentially the same as dividing a by b while leaving a remainder r. See if you can complete the connection in the following example.

Example 68. Let's use algebraic language to express the two-sticks algorithm applied to 52 and 20. Let's start by setting this up as a division problem with a remainder, again since this is effectively what is being done in the stick example above.

$$52 = 20 \cdot x + b$$

By division with remainder we find $x = 2$ and $b = 12$ Now we set up the problem again, this time dividing 12 into 20.

$$20 = 12 \cdot x + b$$

This yields $x = 1, b = 8$. Then set up the problem again, this time dividing 8 into 12.

$$12 = 8 \cdot x + b$$

This yields $x = 1, b = 4$. Then set up the problem again, this time dividing 4 into 8.

$$8 = 4 \cdot x + b$$

This yields $x = 2, b = 0$.

Now notice that 8 is divisible by 4. In the equation before that, we have $12 = 4 \cdot 2 + 4$. Since the right hand side is a sum of multiples of 4, the left hand side must also be a multiple of 4. In the next equation up $20 = 12 \cdot x + 8$ again, the right hand side is a sum of multiples of 4, so the left hand side must also be a multiple of 4. Continuing this logic upward shows that all intervals created along the way are divisible by 4. Hence the algorithm has generated a divisor of the original lengths 52 and 20.

The procedure we have just described is called the ***Euclidean algorithm***.(An *algorithm* is a mathematical procedure designed to compute a specific result). The Euclidean algorithm is very powerful, and in fact can be used to calculate gcd's of large numbers as we'll see below.

In the above example, by factoring 52 and 20 into primes: $20 = 2 \cdot 2 \cdot 5$ and $52 = 2 \cdot 2 \cdot 13$, it is plain to see that the only common factors are 2 and 4. Thus the divisor produced by the Euclidean algorithm happened to be the greatest common divisor. This turns out to be true in general, as we will now prove.

♦

Proposition 69. The Euclidean algorithm applied to two integers will give the gcd of those two integers.

Proof. This proof is broken up into two parts, (A) and (B). Part (A) shows that the algorithm always produces a divisor of the two given integers. Part (B) shows that the produced divisor is indeed the gcd.

(A) Given integers a and b and $a > b$ if we were to plug them into the Euclidean Algorithm we get:

$$a = b \cdot q_1 + r_1$$

$$b = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

$$\vdots$$

until there is an equation with no remainder left.

$$r_{k-2} = r_{k-1} \cdot q_{k-1} + r_k$$

$$r_{k-1} = r_k \cdot q_k + 0$$

It is clear that r_k divides r_{k-1}. Consider the next equation up.

$$r_{k-2} = r_{k-1} \cdot q_{k-1} + r_k = r_k \cdot q_{k-1} \cdot q_k + r_k$$

This shows that r_k divides the right hand side, so r_k must divide r_{k-2}. In the next equation up, the right can be set up as multiples of r_k which means the next r term is divisible by r_k Continue all the way to the top and it must be that r_k divides both a and b

(B) Now suppose there is another number c that divides a and b such that $a_1 \cdot c = a$ and $b_1 \cdot c = b$. We can rewrite the initial equation of the algorithm as follows.

$$a_1 \cdot c = (b_1 \cdot c) \cdot q_1 + r_1 \Rightarrow a_1 \cdot c - (b_1 \cdot c) \cdot q_1 = r_1$$

This shows that c must divide r_1. Consider the next equation.

$$b_1 \cdot c = (r_1) \cdot q_2 + r_2 \Rightarrow b_1 \cdot c - (r_1) \cdot q_2 = r_2$$

Since c divides both r_1 and b_1 then c must divide r_2 also. Repeat all the way to the bottom and c will have to divide r_k.

Since c divides r_k, c is no larger than r_k. So all divisors of a and b must be no larger than r_k. From part (A) we know that r_k divides both a and b. Therefore r_k must be the gcd of a and b.

□

The Euclidean algorithm may be summarized as follows.

1: Start with two integers a and b where $a > b$

2: Divide b into a and find the remainder r

3: If $r = 0$, b is the greatest common divisor.

4: If the remainder is not 0, set $a = b$ and $b = r$, go to step 1.

Exercise 70. What is the greatest common divisor of:

(a) 1168 and 2338?

(b) 2343 and 4697?

(c) 1006 and 13581?

$\Diamond$

Let us analyze this algorithm just a little further. In the first step when we divide a by b, the remainder satisfies the equation, $r_1 = a - q_1 \cdot b$, where q is an integer. In other words, r_1 can be written in the general form: $r_1 = n \cdot a + m \cdot b$, where n and m are integers.

Exercise 71.

(a) Show that r_2 can also be written in the form: $r_2 = n \cdot a + m \cdot b$, where n and m are integers.

(b) Show that for $k > 2$, if r_{k-2} and r_{k-1} can both be written in the form $n \cdot a + m \cdot b$ where n and m are integers, then r_k can also be written in the same form.

(c) Show that the gcd of two numbers a and b can be written in the form $n \cdot a + m \cdot b$ where n and m are integers.

$\Diamond$

The above exercise amounts to an inductive proof of the following proposition.

Proposition 72. The gcd of two numbers a and b can be written in the form $n \cdot a + m \cdot b$ where n and m are integers.

This proposition will be useful in the next section.

4.5.3 Computer stuff

For those that are computationally inclined, here are two examples, in c++ syntax, of functions that calculate the greatest common divisor.

```
int gcdLoop (int a, int b){
 int divisee=a;
 int divisor=b;
 int remainder;
 //if they are the same, then either is the greatest divisor
 if (a == b)
  return a;
  //If a < b, then switch, otherwise the algorithm will not work.
 if (a < b){
divisee=b;
divisor=a;
}
// At this point, a is the larger of the two numbers
 do{
// '%' returns the remainder of the integer division.
  remainder = divisee % divisor;
//Set up the next iteration if the remainder is not 0 --
// if the remainder is 0, then we're done
 if (remainder !=0){
 divisee = divisor;
  divisor = remainder;}
  else
  {break;}
 while (1);
return divisor;
}
```

This second example is also in c++, but uses recursion.

```
 int gcdRecurse (int a, int b){
  int remainder;
  if (a == b)
     return a;
  if (a <$ b)
```

```
    {
     //'%' returns the remainder of the integer division
     remainder = b % a;
     if (remainder == 0)
       return a;
     else
       return gcdRecurse(a, remainder);
  }
  else
  {
     remainder = a % b;
     if (remainder == 0)
       return b;
     else
       return gcdRecurse(b, remainder);
    }
  //By calling itself, it will repeat the process until the remainder is 0
}
```

Exercise 73. Create a spreadsheet (with Excel, LibreOffice, or OpenOffice) that calculates the gcd of two integers that uses the procedure above. (Excel has a built-in gcd function, but you're not allowed to use it for this exercise.) However, you may use the MOD function: "=MOD(A2,B2)" will compute the remainder when A2 is divided by B2. You may refer to the spreadsheet in Figure 4.14 for ideas. ◊

4.5.4 Diophantine equations

Let's look now at another type of problem, which has played a key role in the history of mathematics.

Example 74. Find all integers m and n such that $16m + 42n = 8$.

To solve this, let us list each of the steps in finding the gcd of 42 and 16, as we explained in the previous section:

$$42 = (16) \cdot 2 + 10$$

$$16 = (10) \cdot 1 + 6$$

	A	B	C
1	Larger #	Smaller #	Remainder
2	1053	863	190
3	863	190	103
4	190	103	87
5	103	87	16
6	87	16	7
7	16	7	2
8	7	2	1
9	2	1	0

Figure 4.14. Spreadsheet for computing gcd

$$10 = (6) \cdot 1 + 4$$
$$6 = (4) \cdot 1 + 2$$
$$4 = (2) \cdot 2 + 0$$

Now let's start over again, but this time we'll keep track of what we're doing. If we start at the top of the list, but move the $16 \cdot 2$ to the other side of the equation, this yields:

$$42 \cdot 1 + 16 \cdot (-2) = 10.$$

Let's define a shorthand "pair notation" for the left-hand side. Let's represent any expression of the form $42 \cdot x + 16 \cdot y$ as (x, y). Using this rule, we denote $42 \cdot 1 + 16 \cdot (-2)$ by the pair $(1, -2)$. Then our previous equation can represented in "pair notation" as:

$$(1, -2) = 10.$$

This "vector notation" can save a lot of writing over the course of a long computation.

Now consider the next equation down the list, which is $16 = (10) \cdot 1 + 6$. Using pair notation, we can write 16 with (0,1) (since $16 = 42 \cdot 0 + 16 \cdot 1$). We've already seen that $10 = (1, -2)$, so we get:

$$(0, 1) = (1, -2) + 6.$$

Now we can move the $(1, -2)$ to the left-hand side and subtract it from $(0, 1)$ to get:

$$(-1, 3) = 6.$$

Now the next equation down the list is $10 = (6) \cdot 1 + 4$. Making similar replacements, we find:

$$(1, -2) = (-1, 3) + 4 \quad \Rightarrow \quad (2, -5) = 4.$$

Repeat again for the next equation down the list: $6 = (4) \cdot 1 + 2$, which gives:

$$(-1, 3) = (2, -5) + 2 \quad \Rightarrow \quad (-3, 8) = 2.$$

At this point, we've gone as far as we can go. (Verify this: what happens if you try to continue?) Now if we replace the pair notation $(-3, 8)$ with what it originally represents, we get:

$$42 \cdot (-3) + 16 \cdot 8 = 2.$$

If we multiply this equation by 4, we have

$$42 \cdot (-12) + 16 \cdot 32 = 8.$$

It follows that $m = -12, n = 32$ is an integer solution to our original equation, $16m + 42n = 8$.

Unfortunately we're not quite done yet, because we're supposed to find *all* integer solutions. But we do have a particular solution, and we can leverage this information as follows.[11] Suppose that m, n is an arbitrary solution, so that $42n + 16m = 8$. We may subtract from this equality the equation for the particular solution $m = -12, n = 32$:

$$\begin{array}{rcr} 42n & + & 16m = 8 \\ -\ (42(-12) & + & 16(32) = 8) \\ \hline 42(n + 12) & + & 16(m - 32) = 0 \end{array}$$

Rearranging and dividing by common factors, we obtain:

$$21(n + 12) = -8(m - 32).$$

[11] What we're doing here is a common ploy in mathematics. We're using a *particular* solution to reduce the problem to a *homogeneous* equation (if you're not familiar with this terminology, then don't worry about it). Exactly the same method is used in differential equations, and in linear algebra.

Now since the right-hand side is divisible by 8, then the left-hand side must also be divisible by 8. This implies that $n + 12$ must be divisible by 8, or

$$n + 12 = 8k \quad \text{(for some integer } k\text{)}.$$

If we plug this in to the equation just above, we get:

$$21(8k) = -8(m - 32), \quad \text{or} \quad m - 32 = 21k.$$

We may rearrange to obtain finally:

$$m = 32 + 21k \quad \text{and} \quad n = -12 + 8k \quad \text{(where } k \text{ is an arbitrary integer)}$$

as the most general solution to $16m + 42n = 8$. ♦

Example 75. We'll give another example, giving just the computations and no other words. We find integer solutions to $1053x + 863y = 245$ as follows:

$$\begin{aligned}
1053 &= 863 + 190 \Rightarrow 190 = (1, -1) \\
863 &= 4 \cdot 190 + 103 \Rightarrow 103 = (0, 1) - 4 \cdot (1, -1) = (-4, 5) \\
190 &= 103 + 87 \Rightarrow 87 = (1, -1) - (-4, 5) = (5, -6) \\
103 &= 87 + 16 \Rightarrow 16 = (-4, 5) - (5, -6) = (-9, 11) \\
87 &= 5 \cdot 16 + 7 \Rightarrow 7 = (5, -6) - 5 \cdot (-9, 11) = (50, -61) \\
16 &= 2 \cdot 7 + 2 \Rightarrow 2 = (-9, 11) - 2 \cdot (50, -61) = (-109, 133) \\
7 &= 3 \cdot 2 + 1 \Rightarrow 1 = (50, -61) - 3 \cdot (-109, 133) = (377 - 460).
\end{aligned}$$

This means that: $377 \cdot 1053 - 460 \cdot 863 = 1$ (You may check this on a calculator.)

Now we may multiply both sides by 245, which gives:

$$(245 \cdot 377) \cdot 1053 - (245 \cdot 460) \cdot 863 = 245.$$

Thus $x = (245 \cdot 377) = 92365$ and $y = -(245 \cdot 460) = -112700$, so that

$$1053 \cdot 92365 - 863 \cdot 112700 = 245$$

is an integer solution.

To find *all* integer solutions, we suppose that (x, y) is an arbitrary solution to $1053x + 863y = 245$. We can subtract our computed solution to give:

$$1053(x - 92365) + 863(y + 112700) = 0,$$

or

$$1053(x - 92365) = -863(y + 112700).$$

Our computation shows that gcd(1053,863)=1, so by *Euclid's Lemma* (Proposition 13 in Chapter 3) and the left-hand side is divisible by 1053, so it must be the case that by $y + 112700$ is also divisible by 1053. If we write $y + 112700 = 1053k$, it follows by algebra that $x - 92365 = -863k$. This means that

$$x = 92365 - 863k, \quad y = -112700 + 1053k$$

is the most general solution.

This solution is correct, but we can simplify by shifting the value of k. Note that $92365 = 107 \cdot 863 + 24$ and $112700 = 107 \cdot 1053 + 29$. So we may replace k with $(\ell + 107)$ to obtain:

$$x = 92365 - 863(\ell + 107), y = -112700 + 1053(\ell + 107),$$

which after working out the algebra gives us:

$$x = 24 + 863\ell, y = 29 + 1053\ell.$$

♦

Exercise 76. Using the process above, find all integer solutions to the following equations.

(a) $45m + 16n = 27$

(b) $360m + 14n = 32$

(c) $389m + 50n = 270$

(d) $4801m + 500n = 1337$

(e) $3524m + 7421n = 333$

◊

Exercise 77. Modify the spreadsheet from Exercise 73 to find the coefficients n and m such that $na + mb = \gcd(a, b)$ for given integers a, b. Refer to Figure 4.15 for ideas. ◊

	A	B	C	D	E	F
1	Larger #	Smaller #	Remainder	Quotient	First coef	Second coef
2			1053		1	0
3			863		0	1
4	1053	863	190	1	1	-1
5	863	190	103	4	-4	5
6	190	103	87	1	5	-6
7	103	87	16	1	-9	11
8	87	16	7	5	50	-61
9	16	7	2	2	-109	133
10	7	2	1	3	377	-460
11	2	1	0	2	-863	1053

Figure 4.15. Spreadsheet for computing gcd

Do all Diophantine equation have solutions? Let's investigate.

Exercise 78. Explain why the following Diophantine equations have no integer solutions.

(a) $2m + 4n = 1$ (*Hint*)

(b) $3m + 27n = 2$

◊

The previous exercise shows that apparently not all Diophantine equations can be solved. The following proposition shows which can and cannot be solved.

Proposition 79. A Diophantine equation of the form $an + bm = c$ has integer solutions for n and m if and only if c is a multiple of the gcd of a and b.

PROOF. Since this is an "if and only if" proof, we need to prove it both ways. We'll do "only if" here, and leave the other way as an exercise.

Since we're doing the "if" part, we assume that $an + bm = c$ is solvable. We'll represent the gcd of a and b by the letter d. Since $\gcd(a, b)$ divides

both a and b, we may write $a = da'$ and $b = db'$ for some integers a', b'. By basic algebra, we have $an + bm = d(a'n + b'm)$. If we substitute this back in the original Diophantine equation, we get:

$$d(a'n + b'm) = c$$

It follows that c is a multiple of, d, which is the gcd of a and b. □

Exercise 80. Prove the "if" part of Proposition 79. (*Hint*) ♢

At the beginning of this section, we "introduced" Diophantine equations. But we have seen them before:

Exercise 81.

(a) Find the general solution to: $242m + 119n = 53$.

(b) Use your solution to solve the modular equation: $242x \equiv 53 \pmod{119}$.

(c) Use your solution to solve the modular equation: $119y \equiv 53 \pmod{242}$.

♢

This example shows that Diophantine equations are just modular equations in a disguised form! Furthermore, each Diophantine equation is associated with *two* modular equations:

Exercise 82. Given that (m, n) is a solution to $a \cdot m + b \cdot n = c$, give (a) a modular equation involving a, b, c that m satisfies; and (b) a modular equation involving a, b, c that n satisfies. ♢

In Example 39, we saw that not all equations of the form $ax \equiv c \pmod{b}$ have an answer. We now have the means to determine which modular arithmetic equations have an answer:

Proposition 83. Given the equation $ax \equiv c \pmod{b}$, where a, b, c are all given integers and x is the variable we're solving for, one can find an integer answer for x if and only if c is an integer multiple of the greatest common divisor of a and b.

Exercise 84. Prove both the "if" and the "only if" parts of Proposition 83. (*Hint*) ◊

Exercise 85. Which of the following equations have integer solutions? If solutions exist, find them all. If no solutions exist, prove it!

(a) $15x = 3 \pmod{12}$

(b) $4x = 17 \pmod{23}$

(c) $503x = 919 \pmod{1002}$

(d) $504x = 919 \pmod{1002}$

◊

To close off this section, we take care of some unfinished business. Way back when we were showing the existence of irrational numbers, we made use of *Euclid's Lemma* (Proposition 13 in Chapter 3). We weren't able to give a real proof then–but we're able to now, thanks to Proposition 79:

Exercise 86.

(a) Let p be a prime, and let a be an integer. Show that a is relatively prime to p if and only if there exist integers m and n such that $pm + an = 1$. (*Hint*)

(b) Suppose p is prime, and suppose a is relatively prime to p. Suppose also that p divides ab. By multiplying the equation in part (a) by b, show that p must divide b. (*Hint*)

(c) Prove ***Euclid's Lemma***: Let p be a prime number, and let a and b be integers. If p divides ab, then either p divides a or p divides b. (*Hint*)

◊

4.5.5 Multiplicative inverse for modular arithmetic

This section is supposed to be about modular division, but so far we've been talking about all kinds of other stuff. You may be wondering, So where's the modular division? You're about to find out!

Recall that the set Z_n under the operation $\oplus$ forms a group: it has closure, it's associative, it has an additive identity, and all elements have inverses. On the other hand Z_n does not form a group under $\odot$ for any $n \geq 2$.

Why is this? Because the inverse property fails for the element 0. The multiplicative identity must be 1, yet $0 \cdot m \neq 1$ for all $m \in Z_n$.

But let's not give up so easily in our quest to form multiplicative groups. Since it appears that 0 is a problem, suppose we take all the elements of Z_n *except* 0? We write the set of nonzero elements of Z_n as $Z_n \setminus \{0\}$. Let's see whether this a group under $\odot$. We remind you that $a \odot b$ is defined by: $a \odot b = r$ where $a, b, r \in Z_n$ and $a \cdot b = kn + r$ where k an integer.)

Example 87. The Cayley table for $Z_3 \setminus \{0\}$ is:

$\odot$	1	2
1	1	2
2	2	1

Notice that each column has 1, meaning that each element has an inverse. It is also closed, associative and has an identity. Thus $Z_3 \setminus \{0\}$ is a group under $\odot$. ♦

Example 88. The Cayley table for $Z_4 \setminus \{0\}$ is

$\odot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Notice that the 2 column does not have a 1 in it, meaning that 2 does not have an inverse in Z_4. Thus, $Z_4 \setminus \{0\}$ is not a group under $\odot$. ♦

The fact that 2 has no inverse is due to 2 being a divisor of 4. This makes all integer multiples of 2 to cycle between the values 0 and 2 (mod 4).

Example 89.

Finding the multiplicative inverse in $Z_n \setminus \{0\}$ for small values of n is not difficult. But what about finding the multiplicative inverse of 3 in $Z_{31} \setminus \{0\}$?

Really all we're looking for is a number k such that $3k \equiv 1 \pmod{31}$. Since 31 is prime, it must be relatively prime to 3, meaning the gcd of 31 and 3 must be 1. 1 is a multiple of 1, so there is a solution and in fact this is just a special case of an earlier proposition. We convert it to a Diophantine equation:

$$3k + 31j = 1$$

Using the gcd algorithm, we find:

$$31 + 3 \cdot (-10) = 1,$$

and applying $\pmod{31}$ gives

$$3 \cdot (-10) \equiv 1 \pmod{31}.$$

Finally, we use the definition of modular arithmetic to convert -10 into a member in Z_{31}:

$$3 \cdot (21) \equiv 1 \pmod{31}.$$

♦

Exercise 90. Prove or disprove that the following sets form a group by either finding a multiplicative inverse for all members, or by finding a member that does not have a multiplicative inverse.

(a) $Z_5 \setminus \{0\}$

(b) $Z_7 \setminus \{0\}$

(c) $Z_9 \setminus \{0\}$

(d) Make a conjecture for which sets $Z_n \setminus \{0\}$ form a group under multiplication.

◊

Proposition 91. All elements in $Z_p \setminus \{0\}$ have an inverse under multiplication mod p.

PROOF. Let a, p be known integers where $a < p$ and p is prime. There exists an inverse to a under multiplication $\pmod{p}$ when there is a solution k to the equation $ak = 1 \pmod{p}$ where k is an integer. By Proposition 83, this equation can be solved if and only if the gcd of a and p is equal to 1. Since p is prime and $a < p$ then the gcd of a and p must be 1. □

Proposition 92. An element a of $Z_p \setminus \{0\}$ have an inverse under multiplication mod p if and only if $\gcd(a, p)=1$ (that is, a is relatively prime to p).

The proof of this proposition is up to you:

Exercise 93. Prove both the "if" and "only if" parts of Proposition 92. (*Hint*) ♢

Exercise 94. Show that if n is not prime, then $Z_n \setminus \{0\}$ is not a group under multiplication. (*Hint*) ♢

4.5.6 Chinese remainder theorem

We now are experts at finding solutions to congruences of the form $ax \equiv c \pmod{b}$. But what about multiple congruences? Take for example:

$$x \equiv 4 \pmod{7}; \qquad x \equiv 5 \pmod{9}.$$

Can we find an x that solves both at the same time?

The first-century Chinese mathematician Sun Zi considered problems like this, and was able to come up with a general method of solution. His result is now known as the ***Chinese Remainder Theorem***.

We may apply Sun Zi's solution (expressed in modern algebraic language) to our particular case as follows. For the first congruence we have the general solution $x = 4 + 7k$, where k is any integer in $\mathbb{Z}$. If we substitute $4 + 7k$ for x in the second congruence, we get:

$$4 + 7k \equiv 5 \pmod{9} \Rightarrow 7k \equiv 1 \pmod{9}.$$

At this point we could use the Euclidean algorithm to find k. But it's often easier to use the trial-and-error methods that we developed earlier. In this

case, the method amounts to adding multiples of 9 to the right-hand side until you get something that is divisible by 7. In this case, we find:

$$7k \equiv 1 + 3 \cdot 9 \pmod 9 \Rightarrow 7k \equiv 28 \pmod 9 \Rightarrow k \equiv 4 \pmod 9.$$

This means $k = 9j + 4$ for some integer j. We substitute $9j + 4$ for k back into $x = 4 + 7k$ to get:

$$x = 4 + 7(9j + 4) = 4 + 63j + 28 = 32 + 63j.$$

So the answer must be $x \equiv 32 \pmod{63}$ When we check, $32 = 9 \cdot 3 + 5 = 7 \cdot 4 + 4$ and $95 = 9 \cdot 10 + 5 = 7 \cdot 13 + 4$ and indeed that is the case. Notice the ending modulus was the least common multiple of the first and second modulus (7 and 9, respectively) in the original set of modular equations.

Now, not all multiple congruences have an answer. Take the following pair of congruences:

$$x \equiv 3 \pmod 4; \qquad x \equiv 4 \pmod 6.$$

We follow the same pattern. There is a solution for the first congruence $x = 4k + 3$ where k is any integer. Plug this into the second congruence to yield:

$$4k + 3 \equiv 4 \pmod 6 \Rightarrow 4k \equiv 1 \pmod 6.$$

From the Euclidean algorithm, we know there is a solution to this congruence if and only if $\gcd(4, 6) = 1$, but we know $\gcd(4, 6) = 2$. Therefore there is no solution.

Exercise 95. Solve the following pairs of congruences or show that they do not have a solution:

(a) $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 4$.

(b) $x \equiv 12 \pmod{23}$; $x \equiv 7 \pmod{11}$.

(c) $x \equiv 3 \pmod{13}$; $x \equiv 20 \pmod{31}$.

(d) $x \equiv 2 \pmod 6$; $x \equiv 56 \pmod{72}$.

$\Diamond$

Exercise 96.

(a) Find a pair of congruences of the form: $x \equiv a \pmod 9$; $x \equiv b \pmod{15}$ that no common solution.

(b) Show that *any* pair of congruences of the form

$$ax \equiv b \pmod 3; \qquad cx \equiv d \pmod 7$$

will have a common solution.

(c) *Prove the following: Given a pair of congruences

$$ax \equiv b \pmod m; \qquad cx \equiv d \pmod n$$

which both have solutions, such that $\gcd(m, n)=1$. Then the congruences also have a common solution. (*Hint*)

(d) *Prove the following: Given a pair of congruences

$$x \equiv b \pmod m; \qquad x \equiv d \pmod n.$$

such that $\gcd(m, n)=1$. Then there exist common solutions to both congruences; and all common solutions are congruent mod mn.

$\Diamond$

We can use the same method to solve any number of simultaneous congruences. Take for example:

$$x \equiv 4 \pmod 7; \quad x \equiv 5 \pmod 9; \quad x \equiv 1 \pmod 2.$$

From the above example we know the general solution for the first two congruences is $x \equiv 32 \pmod{63}$. So we need to solve:

$$x \equiv 32 \pmod{63}; \qquad x \equiv 1 \pmod 2$$

We solve this by the same process as before:

$$\begin{aligned} x = 1 + 2k \Rightarrow 1 + 2k \equiv 32 \pmod{63} &\Rightarrow 2k \equiv 31 \pmod{63} \\ \Rightarrow 2k \equiv 31 + 63 \pmod{63} &\Rightarrow 2k \equiv 94 \pmod{63} \\ \Rightarrow k \equiv 47 \pmod{63}&. \end{aligned}$$

Substitute to obtain $x = 1 + 2(47 + 63j) = 95 + 126j \equiv 95 \pmod{126}$..

Exercise 97. Solve the following sets of congruences or show that they do not have a solution:

(a) $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 4$; $x \equiv 4 \pmod 5$.

(b) $x \equiv 12 \pmod{23}$; $x \equiv 7 \pmod{11}$; $x \equiv 3 \pmod 4$.

$\Diamond$

5

Introduction to Cryptography

Cryptography is the study of sending and receiving secret messages. [1] The aim of cryptography is to send messages across a channel so only the intended recipient of the message can read it. In addition, when a message is received, the recipient usually requires some assurance that the message is authentic; that is, that it has not been sent by someone who is trying to deceive the recipient. Modern cryptography is heavily dependent on abstract algebra and number theory.

The message to be sent is called the ***plaintext*** message. The disguised message is called the ***ciphertext***. The plaintext and the ciphertext are both written in an ***alphabet***, consisting of ***letters*** or ***characters***. Characters can include not only the familiar alphabetic characters A, ..., Z and a, ..., z but also digits, punctuation marks, and blanks. A ***cryptosystem***, or ***cipher***, has two parts: ***encryption***, the process of transforming a plaintext message to a ciphertext message, and ***decryption***, the reverse transformation of changing a ciphertext message into a plaintext message.

There are many different families of cryptosystems, each distinguished by a particular encryption algorithm. Cryptosystems in a specified cryptographic family are distinguished from one another by a parameter to the encryption function called a ***key***. A classical cryptosystem has a single key, which must be kept secret, known only to the sender and the receiver of the message. If person A wishes to send secret messages to two different people B and C, and does not wish to have B understand C's messages or vice versa, A must use two separate keys, so one cryptosystem is used for

[1] Thanks to Tom Judson for material used in this chapter.

exchanging messages with B, and another is used for exchanging messages with C.

Systems that use two separate keys, one for encoding and another for decoding, are called ***public key cryptosystems***. Since knowledge of the encoding key does not allow anyone to guess at the decoding key, the encoding key can be made public. A public key cryptosystem allows A and B to send messages to C using the same encoding key. Anyone is capable of encoding a message to be sent to C, but only C knows how to decode such a message.

5.1 Private key cryptography

In ***single*** or ***private key cryptosystems*** the same key is used for both encrypting and decrypting messages. To encrypt a plaintext message, we apply to the message some function which is kept secret, say f. This function will yield an encrypted message. Given the encrypted form of the message, we can recover the original message by applying the inverse transformation f^{-1}. The transformation f must be relatively easy to compute, as must f^{-1}; however, f must be extremely difficult to guess at if only examples of coded messages are available.

5.1.1 Shift codes

Example 1. One of the first and most famous private key cryptosystems was the shift code used by Julius Caesar. We first represent the alphabet numerically by letting $\mathrm{A} = 0, \mathrm{B} = 1, \ldots, \mathrm{Y} = 25, \mathrm{Z} = 25$. This means for example that the word BAY would be represented numerically as:

$$1, 0, 25.$$

An example of a shift encoding function is

$$f(p) = \mathrm{mod}(p + 3, 26).$$

which can also be written as

$$f(p) = p \oplus 3,$$

with the understanding that $\oplus$ refers to addition in $\mathbb{Z}_{26}$. This encoding function takes

$$0 \to 3, 1 \to 4, \ldots, 25 \to 1, 26 \to 2,$$

so that our numerical representation of BAY is changed to: $4, 3, 1$, which is the numerical representation of EDB.

The decoding function is the inverse of $f(p)$, which we can find by solving the equation $c = p \oplus 3$ for p. The result is $p = c \ominus 3$, so that

$$f^{-1}(c) = c \ominus 3 \qquad \text{or} \qquad f^{-1}(c) = c \oplus 23.$$

Suppose we receive the encoded message DOJHEUD. To decode this message, we first represent it numerically:

$$3, 14, 9, 7, 4, 20, 3.$$

Next we apply the inverse transformation to get

$$0, 11, 6, 4, 1, 17, 0,$$

which is the numerical representation of ALGEBRA. Notice here that there is nothing special about either of the numbers 3 or 26. We could have used a larger alphabet or a different shift. ♦

Exercise 2.

(a) Encode IXLOVEXMATH using the cryptosystem in Example 1.

(b) Encode the same message using the encoding function $f(p) = p \oplus 10$.

◊

Exercise 3.

(a) Decode ZLOOA WKLVA EHARQ WKHA ILQDO, which was encoded using the cryptosystem in Example 1.

(b) Decode: OFOBIDRSXQIYENYPVYGCPBYWDROROKBD, which was encoded using a shift code with a shift of 10.

◊

Exercise 4.

(a) The following is a ciphertext that was encoded using a shift code with a shift of 18.

FWHKYVOGVFGCVQWFIHOKYVQGVFGCVHSPOKYVQGVFGCV

Find the plaintext.

(b) A plaintext is encoded using a shift code with a shift of 14. The resulting ciphertext is shift-encoded again, using a shift of 14. The result is:

VJGOQTGAQWMPQYVJGNGUUUWTGAQWCTGXQNVCKTG

Find the plaintext.

◊

Cryptanalysis is concerned with deciphering a received or intercepted message. Methods from probability and statistics are great aids in deciphering an intercepted message; for example, the frequency analysis of the characters appearing in the intercepted message often makes its decryption possible.

Example 5. Suppose we receive a message that we know was encrypted by using a shift transformation on single letters of the 26-letter alphabet. To find out exactly what the shift transformation was, we must compute b in the equation $f(p) = p + b \bmod 26$. We can do this using ***frequency analysis***. The letter E = 04 is the most commonly occurring letter in the English language. Suppose that S = 18 is the most commonly occurring letter in the ciphertext. Then we have good reason to suspect that $18 = 4 \oplus b$, or $b = 14$. Therefore, the most likely encoding function is

$$f(p) = p \oplus 14.$$

The corresponding decoding function is

$$f^{-1}(c) = c \oplus 12.$$

It is now easy to determine whether or not our guess is correct. ♦

Exercise 6. The following ciphertext was encoded using a shift code. Both the letters E and I are encoded as vowels.

IWPDAIWPEYOEOPDAMQAAJKBPDAOYEAJYAOYWNHBCWQOO

Find the plaintext. ◊

Exercise 7. In the following shift-coded ciphertext, one of the double-letter patterns represents 'ss'.

SGD DRRDMBD NE LZSGDLZSHBR HR HM HSR EQDDCNL. FDNQF BZMSNQ

Find the plaintext. ◊

Exercise 8.

(a) For the English alphabet, how many different shift codes are there?

(b) Thai script has 44 letters. How many different shift codes are there for the Thai language?

◊

5.1.2 Affine codes

Let us investigate a slightly more sophisticated cryptosystem. Suppose that the encoding function is given by

$$f(p) = \mathrm{mod}(ap + b, 26),$$

which can also be written as

$$f(p) = (a \odot p) \oplus b.$$

We first need to find out when a decoding function f^{-1} exists. Such a decoding function exists when we can solve the equation

$$c \equiv ap + b \pmod{26} \qquad \text{or} \qquad a \odot p = c \ominus b$$

for p in $\mathbb{Z}_{26}$. By Proposition 83 in Chapter 4, this is possible exactly when a has an inverse in $\mathbb{Z}_{26}$, which means that $\gcd(a, 26) = 1$. Such a cryptosystem is called an ***affine cryptosystem***.

Exercise 9.

(a) Which of the numbers 0, 1, 2, ..., 10 have inverses mod 26?

(b) For the numbers in (a) which have inverses mod 26, compute the inverses.

◊

Exercise 10. Find the decoding function for the following affine encoding functions (used on the English alphabet).

(a) $f(p) = 3 \odot p + 14$

(b) $f(p) = 5 \odot p + 15$

(c) $f(p) = 7 \odot p + 23$

◊

Exercise 11. Show that the general formula for the decoding function for $f(p) = a \odot p \oplus b$ is

$$f^{-1}(c) = (a^{-1} \odot c) \ominus (a^{-1} \odot b).$$

(That is, show that $f \circ f^{-1}(c) = c$, and $f^{-1} \circ f(p) = p$.) ◊

Example 12. Let's consider the affine cryptosystem encoding function $f(p) = (a \odot p) \oplus b$ (the $\odot$ and $\oplus$ are multiplication and addition mod 26). For this cryptosystem to work we must choose an $a \in \mathbb{Z}_{26}$ that is invertible. This is only possible if $\gcd(a, 26) = 1$. Recognizing this fact, we will let $a = 5$ since $\gcd(5, 26) = 1$. The reader may check that $a^{-1} = 21$. Therefore, we can take our encryption function to be $f(p) = (5 \odot p) \oplus 3$. Thus, ALGEBRA is encoded as $3, 6, 7, 23, 8, 10, 3$, or DGHXIKD. The decryption function will be

$$f^{-1}(p) = (21 \odot p) \ominus (21 \odot 3) = (21 \odot p) \oplus 15.$$

⧫

Exercise 13. For each of the following functions, (i) determine whether the function is a valid encoding function; (ii) if the function is valid, find the decoding function. (Assume the function is working on an alphabet with 26 letters.)

(a) $f(p) = (4 \odot p) \oplus 7$

(b) $f(p) = (5 \odot p) \oplus 13$

(c) $f(p) = (11 \odot p) \oplus 14$

(d) $f(p) = (13 \odot p) \oplus 22$

$\Diamond$

Exercise 14.

(a) The general form for an affine cryptosystem encoding function is $f(p) = (a \odot p) \oplus b$. How many different possible values of a are there, for an affine cryptosystem that works on the English alphabet of 26 letters?

(b) For the same situation as (a), how many different possible values are there for b?

(c) What is the total number of affine cryptosystems that work on an alphabet of 26 letters?

$\Diamond$

Exercise 15. The Spanish alphabet has 29 letters. Give answers to parts (a), (b), and (c) of Exercise 14, but with the Spanish alphabet instead of the English alphabet. $\Diamond$

Exercise 16. The Hebrew alphabet has 22 letters. Give answers to parts (a), (b), and (c) of Exercise 14, but with the Hebrew alphabet instead of the English alphabet. $\Diamond$

Exercise 17. Suppose that the encoding function for an affine cryptosystem is $f(p) = (a \odot p) \oplus b$, and the decoding function is $f^{-1}(c) = (a' \odot c) \oplus b'$. Suppose that a different cryptosystem uses the encoding function $g(p) = (a' \odot p) \oplus b'$. What is the decoding function for this second cryptosystem? $\Diamond$

Exercise 18.

(a) The following message was encoded using an affine cryptosystem that encodes A as M and B as B.

CKMYCZMLCOZCWKOHUCKDOHLMZLLNMZGZOEVUFYU

Find the plaintext.

(b) The following message was encoded using an affine cryptosystem that encodes A as G and C as C.

MQTNOELNWNETEHCEWHISCFKYHHFYKGCCEIPXQWFISCF

Find the plaintext.

(c) The following message was encoded using an affine cryptosystem that encodes R as S and S as D.

OMFMFNSOMNDSFNDLADOMNOSFNDLAJNAALOZAUFSDONAU

Find the plaintext.

(d) The following message was encoded using an affine cryptosystem that encodes M as N and O as D.

NVEMBNVEHLJHJEMBNZJHLDWOBVJDI

Find the plaintext.

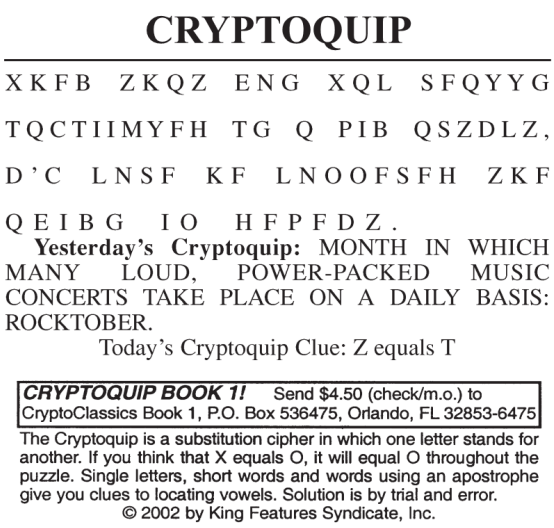
◊

5.1.3 Monoalphabetic codes

In both shift codes and affine codes, one character in the encoded message represents exactly one character in the original message. Cryptosystems that employ such a one-to-one substitution are called ***monoalphabetic cryptosystems***. The "cryptoquips" that appear regularly in many newspapers make use of this type of cryptosystem (see Figure 5.1).

Exercise 19. What is the total number of monoalphabetic cryptosystems? ◊

Although there are many different possible monoalphabetic cryptosystems, they are relatively easy to break using frequency analysis. (You may even find web sites that can automatically decode cryptoquips.)



CRYPTOQUIP

XKFB ZKQZ ENG XQL SFQYYG

TQCTIIMYFH TG Q PIB QSZDLZ,

D'C LNSF KF LNOOFSFH ZKF

QEIBG IO HFPFDZ.

Yesterday's Cryptoquip: MONTH IN WHICH MANY LOUD, POWER-PACKED MUSIC CONCERTS TAKE PLACE ON A DAILY BASIS: ROCKTOBER.

Today's Cryptoquip Clue: Z equals T

CRYPTOQUIP BOOK 1! Send $4.50 (check/m.o.) to CryptoClassics Book 1, P.O. Box 536475, Orlando, FL 32853-6475

The Cryptoquip is a substitution cipher in which one letter stands for another. If you think that X equals O, it will equal O throughout the puzzle. Single letters, short words and words using an apostrophe give you clues to locating vowels. Solution is by trial and error.

Figure 5.1. Example of cryptoquip (source: "Cecil Whig", www.cecildaily.com/diversions/cryptoquip/).

5.1.4 Polyalphabetic codes

A cryptosystem would be more secure if a ciphertext letter could represent more than one plaintext letter. To give an example of this type of cryptosystem, called a ***polyalphabetic cryptosystem***, we will generalize affine codes by using matrices. The idea works roughly the same as before; however, instead of encrypting one letter at a time we will encrypt pairs of letters. We can store a pair of letters p_1 and p_2 in a vector

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}.$$

Let A be a 2×2 invertible matrix with entries in $\mathbb{Z}_{26}$. We can define an encoding function by

$$f(\mathbf{p}) = (A \odot \mathbf{p}) \oplus \mathbf{b},$$

where $\mathbf{b}$ is a fixed column vector and matrix operations are performed in $\mathbb{Z}_{26}$. The formula for the decoding function (which is the inverse of the encoding function) is very similar to the decoding function formula that we found for affine encoding:

$$f^{-1}(\mathbf{p}) = (A^{-1} \odot \mathbf{p}) \ominus (A^{-1} \odot \mathbf{b}),$$

where A^{-1} is the *matrix inverse* of A: that is, $A^{-1}A = AA^{-1} = I$, where I is the 2×2 identity matrix. *Note* that in these formulas, we are using *modular* matrix multiplication instead of *regular* matrix multiplication: that is, the regular $\cdot$ and $+$ operations are replaced by $\odot$ and $\oplus$:

Exercise 20. Perform the following operations using modular matrix multiplication (mod 26):

(a) $\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 4 \\ 4 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 13 \\ 16 & 2 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix}$

(c) $\begin{pmatrix} 12 & 4 \\ 13 & 5 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 20 & 20 \end{pmatrix}$

(d) $\begin{pmatrix} 13 & 2 \\ 2 & 13 \end{pmatrix}\begin{pmatrix} 2 & 13 \\ 13 & 2 \end{pmatrix}$

$\Diamond$

Example 21. Suppose that we wish to encode the word HELP. The corresponding digit string is $7, 4, 11, 15$. If

$$A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix},$$

then

$$A^{-1} = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}.$$

(You may check that $\text{mod}(AA^{-1}, 26) = \text{mod}(A^{-1}A, 26) = I$.) If $\mathbf{b} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$, then our message is encrypted as RRGR, where HE encrypts as RR and LP encrypts as GR. $\blacklozenge$

In order to make use of polyalphabetic cryptosystems, we need to be able to find the inverse of a 2×2 matrix with entries in $\mathbb{Z}_{26}$. As we *noted* above, this inverse is under matrix multiplication mod 26, rather than regular matrix multiplication. Still, we can try to make use of the matrix inverse formula from regular matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} kd & -kb \\ -kc & ka \end{pmatrix},$$

where

$$k = \frac{1}{ad - bc}.$$

This suggests that the following formula may be valid mod 26:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} k \odot d & -k \odot b \\ -k \odot c & k \odot a \end{pmatrix},$$

where

$$k = ((a \odot d) \ominus (b \odot c))^{-1},$$

and $(\cdots)^{-1}$ means inverse under multiplication in $\mathbb{Z}_{26}$. We will see in the following exercise that this works as long as $(a \odot d) \ominus (b \odot c)$ has a multiplicative inverse in $\mathbb{Z}_{26}$.

Exercise 22. Suppose that $(a \odot d) \ominus (b \odot c)$ has an inverse in $\mathbb{Z}_{26}$: that is to say, suppose there is a $k \in \mathbb{Z}_{26}$ such that $k \odot ((a \odot d) \ominus (b \odot c)) = 1$. Show that the matrices:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} k \odot d & -k \odot b \\ -k \odot c & k \odot a \end{pmatrix}$$

are inverses of each other in $\mathbb{Z}_{26}$. That is, show that $AB = BA = I$ under matrix multiplication mod 26.

$\Diamond$

The previous exercise leaves open the question of whether $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has an inverse when $(a \odot d) \ominus (b \odot c)$ has no inverse in $\mathbb{Z}_{26}$. Once again, we can reach back to our previous matrix knowledge to resolve this issue. Recall that the quantity $ad - bc$ is called the ***determinant*** of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. There is also a famous formula for the determinant of the product of matrices:

$$\det(A)\det(B) = \det(AB).$$

This same formula carries over to matrix multiplication mod 26, because (as we've seen) in any equation using only the operations of multiplication, addition, and subtraction, we can replace these operations with their modular versions and still have a true equation. We can use this to show that $(a \odot d) \ominus (b \odot c)$ *must* have an inverse in $\mathbb{Z}_{26}$ in order for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to have an inverse:

Exercise 23. Suppose that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix with entries in $\mathbb{Z}_{26}$, such that $(a \odot d) \ominus (b \odot c)$ has no inverse in $\mathbb{Z}_{26}$. Show that A has no inverse in $\mathbb{Z}_{26}$. (*Hint*) $\Diamond$

Exercise 24. Find matrix inverses in $\mathbb{Z}_{26}$ for the following matrices. If no inverse exists, then prove there is no inverse.

(a) $\begin{pmatrix} 9 & 2 \\ 20 & 31 \end{pmatrix}$ (c) $\begin{pmatrix} 4 & 11 \\ 3 & 2 \end{pmatrix}$

(b) $\begin{pmatrix} 2 & 3 \\ 23 & 2 \end{pmatrix}$ (d) $\begin{pmatrix} 2 & 2 \\ 3 & 4 \end{pmatrix}$

◊

Exercise 25. For the same matrices as in Exercise 24, find the matrix inverses in $\mathbb{Z}_{29}$. ◊

Exercise 26. Given that

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}, \quad \text{and } \mathbf{b} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}.$$

(a) Use the encryption function $f(\mathbf{p}) = A\mathbf{p} + \mathbf{b}$ to encode the message CRYPTOLOGY.

(b) What is the decoding function?

◊

Frequency analysis can still be performed on a polyalphabetic cryptosystem, because we have a good understanding of how pairs of letters appear in the English language. The pair *th* appears quite often; the pair *qz* never appears. To avoid decryption by a third party, we must use a larger matrix than the one we used in Example 21.

5.1.5 Spreadsheet exercises

Spreadsheets can be used to automate many of the calculations that we have looked at in the previous sections.

Exercise 27. In this exercise, you will use a spreadsheet to create an automated shift encoder for English. Please refer to Figure 5.2 for guidance:

	A	B	C	D	E	F	G	H	I	J
1	AUTOMATED SHIFT ENCODING FOR ENGLISH									
2	Shift:		15							
3										
4	Tables:									
5	A	0	A		Plaintext:	H	E	L	L	O
6	B	1	B		Numerical:	7	4	11	11	14
7	C	2	C		Shifted:	22	19	0	0	3
8	D	3	D		Ciphertext:	W	T	A	A	D
9	E	4	E		Numerical:	22	19	0	0	3
10	F	5	F		Unshifted:	7	4	11	11	14
11	G	6	G		Recovered:	H	E	L	L	O
12	H	7	H							

Figure 5.2. Automatic shift encoder for English.

(i) Put the Shift value in cell C2.

(ii) Put the alphabet (starting with A), numerical values for the letters (starting with 0), and the alphabet again in columns A, B, C starting on line 5.

(iii) Type your plaintext in row 5, starting in column F.

(iv) Row 6 beginning in column F contains the numerical values for the plaintext. The formula in cell F6 is: "=VLOOKUP(F5, $A$5:$B$30,2)". The significance of this formula is as follows:

- The function VLOOKUP means that the program will look up a given value in a given table;
- The F5 is the first argument of VLOOKUP, which means that the value being looked up is in cell F5;
- The $A$5:$B$30 is the second argument of VLOOKUP, which means that it represents the cells containing the table that the value will be looked up in. The dollar signs are used to guarantee that the table will remain fixed when the formula is copied and pasted into another cell; The 2 which is the third lookup of VLOOKUP indicates that the value in the second column in the same row as the looked-up value is placed in the cell where the formula is located.

(v) Row 7 beginning in column F gives the encoded numerical values. The formula in cell F7 is "=MOD(F6+$C$2,26)". The dollar signs on C2 guarantee that when the formula is copied, the shift still refers to the value in C2.

(vi) Row 8 beginning in column F gives the ciphertext. The formula in cell F8 is: "=VLOOKUP(F7,$B$5:$C$30,2)".

(vii) Rows 9,10, and 11 are similar to rows 6,7,8 respectively. Try to do this yourself.

Once you have completed the formulas, select cells F6 through J11, and use the spreadsheet's "Fill Right" capability to carry the formulas to the other columns. (If your plaintext is longer, you can select more columns and fill right. ◊

Exercise 28. The Spanish alphabet has 3 more letters than English: 'Ch' (comes after C in the alphabet), 'Ll' (comes after L in the alphabet), and 'Nn' (comes after N). Modify the sheet you created in Exercise 27 to make a Spanish language shift encoder. Use your sheet to decode the following message:

MS KIUPVA UID NIKPS VA MD DPMUBChM MS UMQACh

(Note that 'Ch' counts as a single letter.) ◊

Exercise 29. Create a spreadsheet that can perform any affine encoding on English plaintext. You may model your spreadsheet on the sheet in Figure 5.3. Use your spreadsheet to decode the following message:

EMBNDOBFDZXIDPEMBSBJJJZOBFDZVOBUDSEVHOB

which was encoded using an affine encoding function with $b = 21$. ◊

Exercise 30. In order to decode an affine cryptosystem on English letters with encoding function $f(p) = (a \odot p) \oplus b$, it is necessary to find the inverse of a under multiplication mod 26. We have ways of finding inverses of individual numbers. But we can also use spreadsheet software to find all inverses in one fell swoop as described below.

Open a sheet in your favorite spreadsheet software (Excel, LibreOffice, or OpenOffice). Put the numbers 0 through 25 in column A, starting at

	A	B	C	D	E	F	G	H	I	J
1	**Spreadsheet for affine encode/decode**									
2	**a:**		**3**							
3	**b:**		**8**							
4	**a^{-1}**		**9**							
5										
6	A	0	A		Plaintext:	H	E	L	L	O
7	B	1	B		Numerical:	7	4	11	11	14
8	C	2	C		Affine:	3	20	15	15	24
9	D	3	D		Ciphertext	D	U	P	P	Y
10	E	4	E		Numerical:	3	20	15	15	24
11	F	5	F		Affine inverse:	7	4	11	11	14
12	G	6	G		Plaintext:	H	E	L	L	O
13	H	7	H							

Figure 5.3. Automatic affine encoder for English.

row 3, and also in row 2 starting in column B. To fill up the table, put the formula "=MOD($A3*B$2,26)" in cell B3, as shown in Figure 5.4. This formula causes the software to take the product of the contents of cells A3 and B2, and put the result mod 26 into cell B3. The dollar signs are important: these indicate "fixed reference". For example, the '$A3' means that when this formula is copied to other cells, the reference to column A remains unchanged while the column may change. On the other hand, the 'B$2' means that when the formula is copied to other cells, the reference to column 2 remains unchanged.

At this point, select the range of cells from B3 to AA28 (this will be a square region of 26×26 cells. Use your spreadsheet's "Fill down" and "Fill right" feature to fill all the cells in this region. The location of all of the '1"s in this table shows all of the inverses. For example, there is a '1' in the row labeled 9 and column labeled 3. This means that 9 and 3 are inverses of each other mod 26.

Use this spreadsheet table to create a 2-column table: in the first column, put the numbers 0 through 26, and in the second column, put the inverses (if the number has no inverse, just put a '$-$'). ◊

Exercise 31. Following the previous exercise, find all inverses of the numbers mod 29 (this can be used in affine encoding of Spanish, which has 29 letters). ◊

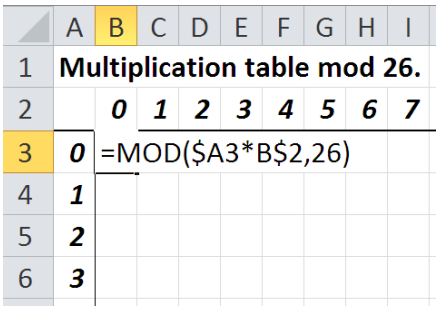


Figure 5.4. Mod 26 multiplication table.

Exercise 32. Make a spreadsheet that can do polyalphabetic coding. you may base your sheet's design on Figure 5.5. The figure shows the encoding of the word CRYPTOLOGY using $A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$.

Use your spreadsheet to decode the following words that were encoded using $f(\mathbf{p}) = A\mathbf{p} + \mathbf{b}$ with the given A and $\mathbf{b}$.

(a) VVDGOFOKLY, $A = \begin{pmatrix} 13 & 5 \\ 9 & 2 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 7 \\ 13 \end{pmatrix}$.

(b) VWFGTWQKTA, $A = \begin{pmatrix} 17 & 13 \\ 6 & 3 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 14 \\ 18 \end{pmatrix}$.

(c) EXUFQPRRGA, $A = \begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$.

$\Diamond$

5.2 Public key cryptography

If traditional cryptosystems are used, anyone who knows enough to encode a message will also know enough to decode an intercepted message. In 1976, W. Diffie and M. Hellman proposed public key cryptography, which is based on the observation that the encryption and decryption procedures need not have the same key. This removes the requirement that the encoding key be kept secret. The encoding function f must be relatively easy to compute, but f^{-1} must be extremely difficult to compute without some additional

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	***Matrix A:***				***Vector b:***											***Ainv mod 26***				***-Ainv*b***		
2	3	5			2			*mod(ad - bc,26)*		1						2	21			6		
3	1	2			2			*inverse mode 26 by hand)*		1						25	3			22		
4	***Tables:***																					
5	A	0	A		***Plaintext:***	C	Y	T	L	G												
6	B	1	B			R	P	O	O	Y												
7	C	2	C																			
8	D	3	D		***Numerical:***	2	24	19	11	6												
9	E	4	E			17	15	14	14	24												
10	F	5	F																			
11	G	6	G		***Encoded***	15	19	25	1	10												
12	H	7	H		***numerical:***	12	4	23	15	4												
13	I	8	I																			
14	J	9	J		***Ciphertext:***	P	T	Z	B	K												
15	K	10	K			M	E	X	P	E												
16	L	11	L																			
17	M	12	M		***Numerical:***	15	19	25	1	10												
18	N	13	N		***ciphertext***	12	4	23	15	4												
19	O	14	O																			
20	P	15	P		***Decoded***	2	24	19	11	6												
21	Q	16	Q		***numerical:***	17	15	14	14	24												
22	R	17	R																			
23	S	18	S		***Decoded***	C	Y	T	L	G												
24	T	19	T		***plaintext:***	R	P	O	O	Y												

Figure 5.5. (Semi-)automatic polyalphabetic encoder/decoder for English. Note that cell N3 is entered by hand, based on the value in N2.

information, so that someone who knows only the encrypting key cannot find the decrypting key without prohibitive computation. It is interesting to note that to date, no system has been proposed that has been proven to be "one-way;" that is, for any existing public key cryptosystem, it has never been shown to be computationally prohibitive to decode messages with only knowledge of the encoding key.

5.2.1 The RSA cryptosystem

The RSA cryptosystem introduced by R. Rivest, A. Shamir, and L. Adleman in 1978, is based on the difficulty of factoring large numbers. Though it is not

a difficult task to find two large random primes and multiply them together, factoring a 150-digit number that is the product of two large primes would take 100 million computers operating at 10 billion instructions per second about 50,000 years under the fastest algorithms currently known.

Let us look at how RSA works in a practical context. Suppose that Jennifer is running an online boutique, and wants to receive credit card information from customers over the internet. Unfortunately it's all too easy to snoop the internet, and it certainly wouldn't be good for Jennifer's customers if their credit card numbers were stolen. So she needs a suitable code for the credit card information in order to protect her customer's privacy. The code may be constructed as follows:

(a) Choose two random 150-digit prime numbers p and q. (This is easier said than done! We will consider some possible ways of doing this in Section 5.2.4.)

(b) Compute the product $n = pq$ as well as $m = (p-1)(q-1)$. (It can be shown that m is actually the number of positive integers in $\mathbb{Z}_n$ that are relatively prime to n.)

(c) Find a large random integer E that is relatively prime to m. This is done by making a guess for E, then using the Euclidean algorithm to check whether $\gcd(E, m) = 1$. If not, then keep guessing until you find an E that works. In general relatively prime numbers are not uncommon, and the Euclidean algorithm is pretty quick (especially for a computer), so E is not too difficult to find.

(d) Using the Euclidean algorithm, find D such that $DE \equiv 1 \pmod{m}$.

Now, let's say that Jennifer has a customer whose credit card number is x. Before requesting the credit card information, Jennifer's computer sends the numbers E and n to the customer's computer, which then calculates $y = x^E \mod n$ and sends y to Jennifer's computer, Jennifer recovers x by computing $y^D \mod n$, which (as we shall show in a minute) turns out to be x, as long as x is less than n.

Notice some amazing things here. First, E and n are sent out *openly* over the internet. Jennifer doesn't care if snoopers find out this information. In fact, she sends the *same* E and n to each customer! But this does not compromise her customers' security, because only Jennifer knows m, and it takes both E and m to find D. As long as no one can figure out m, the credit card numbers are safe!

To summarize: once the public key (E, n) and the private key D have been constructed, the process of encoding and decoding is simple:

- To encode a numerical plaintext x: compute $\mod (x^E, n)$.
- To decode a numerical ciphertext y: compute $\mod (y^D, n)$.

Example 33. Before exploring the theory behind the RSA cryptosystem or attempting to use large integers, we will use some small integers just to see that the system does indeed work. Suppose that we wish to send some message, which when digitized is 395. Let $p = 23$ and $q = 29$. Then

$$n = pq = 667 \qquad \text{and} \qquad m = (p-1)(q-1) = 616.$$

We can let $E = 487$, since $\gcd(616, 487) = 1$. The encoded message is computed to be

$$\mod(395^{487}, 667) = 570.$$

(This may seem like a very long computation, but there are fast ways of doing this: see Exercise 35 below.) Using the Euclidean algorithm, we determine that $191E = 1 + 151m$; therefore, the decrypting key is $(n, D) = (667, 191)$. We can recover the original message by calculating

$$\mod(570^{191}, 667) = 395.$$

♦

This really seems like magic. How in the world does it work? First of all, we know that $DE \equiv 1 \bmod m$; so there exists a k such that

$$DE = km + 1.$$

This means that

$$y^D = (x^E)^D = x^{DE} = x^{km+1} = (x^m)^k x.$$

At this point we need *Euler's theorem* from Chapter 12, which states the following. Suppose m is the number of positive integers less than n that are relatively prime to n. Then it is true that:

$$x^m \equiv 1 \pmod{n}.$$

for *any* x that is relatively prime to n.

We can use this to simplify our previous expression for y^D:

$$y^D = (x^m)^k x \equiv (1)^k x \equiv x \bmod n,$$

and presto! We have our result.

We can now ask how one would go about breaking the RSA cryptosystem. To find D given n and E, we simply need to factor n and solve for D by using the Euclidean algorithm. If we had known that $667 = 23 \cdot 29$ in Example 5, we could have recovered D.

Exercise 34. Show that if p and q are primes, then the number of positive integers less than pq which are relatively prime to pq is $(p-1)(q-1)$. (*Hint*) ◊

5.2.2 Message verification

There is a problem of message verification in public key cryptosystems. Since the encoding key is public knowledge, anyone has the ability to send an encoded message. If Alice receives a message from Bob, she would like to be able to verify that it was Bob who actually sent the message. Suppose that Bob's encrypting key is (n', E') and his decrypting key is (n', D'). Also, suppose that Alice's encrypting key is (n, E) and her decrypting key is (n, D). Since encryption keys are public information, they can exchange coded messages at their convenience. Bob wishes to assure Alice that the message he is sending is authentic. Before Bob sends the message x to Alice, he decrypts x with his own key:

$$x' = \bmod(x^{D'}, n').$$

Anyone can change x' back to x just by encryption, but only Bob has the ability to form x'. Now Bob encrypts x' with Alice's encryption key to form

$$y' = \bmod(x'^E, n),$$

a message that only Alice can decode. Alice decodes the message and then encodes the result with Bob's key to read the original message, a message that could have only been sent by Bob.

5.2.3 RSA exercises

Exercise 35. This problem demonstrates a fast method for computing very large powers of numbers in modular arithmetic using a spreadsheet. You will need this method in order to do the subsequent problems. We will demonstrate the method by computing $\mathrm{mod}(23^{485}, 617)$.

(a) Use a spreadsheet to compute the following sequence of numbers:

$$23, \mathrm{mod}(23^2, 617), \mathrm{mod}(23^4, 617), \ldots, \mathrm{mod}(23^{256}, 617)$$

Note that each power of 23 in this series is the *square* of the previous power. So to compute any number in this series, square the previous number and reduce mod 617. You may use the MOD spreadsheet function. It is easiest to put all the numbers in a single column. (This way, you can use the spreadsheet's "Fill down" feature.)

(b) Write 485 as a sum of powers of 2. (This is the same thing as finding the *binary expansion* of 485.)

(c) Using the results of (b), identify a set of entries from the table you found in part (a), such that the product of these entries is equivalent to 23^{485} (mod 617). (*Hint*)

(d) Use your result from (c) to compute $\mathrm{mod}(23^{485}, 617)$.

$\Diamond$

Exercise 36. Building off the previous exercise, create a spreadsheet that can compute $\mathrm{mod}(n^q, b)$ for general n, q, b. You may follow the pattern of the spreadsheet in Figure 5.6. Some of the formulas in the spreadsheet are:

- Cell A8: =B3
- Cell B8: =MOD(A8,2)
- Cell A9: =(A8 - B8)/2
- Cell D9: = D8*2
- Cell E9: = MOD(E8*E8, $B$4)

- Cell F8: = B8
- Cell G8: = E8^F8
- Cell H8: = G8
- Cell H9: = MOD(G9*H8,$B$4)

You may obtain the rest of the formulas using the spreadsheet's "fill down" capability.

	A	B	C	D	E	F	G	H
1	COMPUTING LARGE POWERS MODULO A BASE							
2	*number*	222						
3	*power*	3894						
4	*base*	617						
5								
6	Binary expansion of power							
7	*Reduced power*	*Binary expansion*		*Exponent (power of 2)*	*mod(num.^exp., base)*	*Bin. Exp. Of power*	*Factors of power*	*Running product mod base*
8	3894	0		1	222	0	1	1
9	1947	1		2	541	1	541	541
10	973	1		4	223	1	223	328
11	486	0		8	369	0	1	328
12	243	1		16	421	1	421	497
13	121	1		32	162	1	162	304
14	60	0		64	330	0	1	304
15	30	0		128	308	0	1	304
16	15	1		256	463	1	463	76
17	7	1		512	270	1	270	159
18	3	1		1024	94	1	94	138
19	1	1		2048	198	1	198	176
20	0	0		4096	333	0	1	176

Figure 5.6. Spreadsheet for taking large powers modulo a given base.

◊

Exercise 37. Encrypt each of the following RSA messages x so that x is divided into blocks of integers of length 2; that is, if $x = 142528$, encode 14, 25, and 28 separately.

(a) $n = 3551, E = 629, x = 31$ **(b)** $n = 2257, E = 47, x = 23$ ◊

(c) $n = 120979, E = 13251,$ $x = 142371$

(d) $n = 45629, E = 781,$ $x = 231561$

Exercise 38. Decrypt each of the following RSA messages y. (In this case, do not break y into blocks–decode the entire number.)

(a) $n = 3551, D = 1997, y = 2791$

(b) $n = 5893, D = 81, y = 34$

(c) $n = 120979, D = 27331, y = 112135$

(d) $n = 79403, D = 671, y = 129381$

◊

Exercise 39. Encrypted messages are often divided into blocks of n letters. A message such as THE WORLD WONDERS WHY might be encrypted as JIW OCFRJ LPOEVYQ IOC but sent as JIW OCF RJL POE VYQ IOC. What are the advantages of using blocks of n letters? ◊

Exercise 40. Construct an RSA cryptosystem as follows:

(a) On the web, find two four-digit primes

(b) Use these primes to compute n and m.

(c) Choose a value of E which is less than m, and use you Diophantine Equation spreadsheet (Exercise 77 in the Modular Arithmetic chapter) to find the inverse D under multiplication mod m. If it turns out that E is not relatively prime to m, try again.

(d) Test your cryptosystem by encoding '123', and then decoding it. To encode, use the spreadsheet that you created in Exercise 36 earlier in this chapter. To decode, make another copy of the same sheet.

◊

5.2.4 Additional exercises: identifying prime numbers

We saw in Section 5.2.1 that the RSA algorithm depends on finding very large primes. In practice, large primes are found using trial and error. That is, we choose a large random number and test to see whether it's prime. If the test fails, then try, try again.

So it all comes down to figuring out how to test whether a number is prime. In this section, we consider some possible ways of doing this.

"Brute force" method, and sieve of Eratosthenes

On way to do this is sheer brute force: try dividing by 2,3,4, ..., and if nothing divides then the number is prime. There are various ways to make this process more efficient, as we will see in the following exercises.

Exercise 41. To test whether the number n is a prime, you divide n all the integers $1, 2, 3, \ldots$ up to a, and see if any of them divides evenly. How large does a have to be in order to guarantee that n really is a prime? (*Hint*) $\Diamond$

When testing whether n is prime, by the "brute force" method, as long as n is odd we don't need to divide by even numbers (Why?). This means that you only need to test about half of the numbers up to a–more precisely, we only need to test $\lceil a/2 \rceil$ numbers, where $\lceil x \rceil$ means "the next integer larger than x". ($\lceil x \rceil$ is called the *ceiling* of x.)

We can pull the same trick with factors that are divisible by 3. Once we've tested 3 as a factor, we don't need to check $9, 15, 21, \ldots$ or any other number that is divisible by 3. (Why?) So it seems that this reduces the number of factors that we need to check by about a third, since every third integers are divisible by 3. However, we need to be careful here. We've already ruled out the numbers that are divisible by 2, so the numbers that are divisible by both 2 and 3 have already been ruled out. In other words (using m to denote a positive integer, and using the the notation $|\{\cdots\}|$ to denote the size of sets):

$$|\{m \le a \text{ and } (2 \mid m \text{ or } 3 \mid m)\}| =$$
$$|\{m \le a \text{ and } 2 \mid m\}| + |\{m \le a \text{ and } 3 \mid m\}| - |\{m \le a \text{ and } 6 \mid m\}|.$$

If we are not so careful with the "ceiling function" (which changes the result by at most 1 anyway), this tells us:

$$|\{m \le a \text{ and } 2 \mid m \text{ or } 3 \mid m\}| \approx \frac{a}{2} + \frac{a}{3} - \frac{a}{6}.$$

We can turn this around and find the number of integers which are *not* divisible by 2 or 3:

$$\begin{aligned} |\{m \le a \text{ and } 2 \nmid m \text{ and } 3 \nmid m\}| &\approx a - \frac{a}{2} - \frac{a}{3} + \frac{a}{6} \\ &\approx a\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \\ &\approx \frac{a}{3}. \end{aligned}$$

This gives the number of trial divisions required to test whether n is prime. (Of course we also need to test divisibility by 2 and 3, which are 2 additional divisions.)

The same reasoning can be extended to take into account divisibility by 5, 7, 11, and so on:

Exercise 42. Using the same reasoning as above, show that after dividing by $2, 3, 5$ the number of additional divisions required to test for primality is:

$$a\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right).$$

$\Diamond$

It turns out that the formula in Exercise 42 can be generalized. The resulting function of a when *all* primes less than a are taken into account is called the ***Euler totient function***. The technique of eliminating numbers to check based on previous divisibility is called the ***sieve of Eratosthenes***.

Fermat's test for primality

Even using various tricks to reduce the number of computations, the brute force method requires far too many calculations to be useful for RSA encoding. A different algorithm for testing primality is ***Fermat's factorization algorithm***, which depends on the following fact:

Exercise 43. Let $n = ab$ be an odd composite number. Prove that n can be written as the difference of two perfect squares:

$$n = x^2 - y^2 = (x-y)(x+y).$$

Consequently, a positive odd integer can be factored exactly when we can find integers x and y such that $n = x^2 - y^2$. (*Hint*) $\Diamond$

We can use this fact to factor n by trying different pairs of squares in order to get n as the difference of the two. Of course, we want to do this systematically. So we want to see what values of x and y we actually need to check:

Exercise 44. In the formula $n = x^2 - y^2 = (x-y)(x+y)$, what is the smallest possible value for x that needs to be tested? (*Hint*) $\Diamond$

There are other special conditions that x and y must satisfy:

Exercise 45.

(a) Assuming that n is an odd number, show that if x is odd then y is even, and if x is even then y is odd. (*Hint*)

(b) Show that for any odd number m, then $\mod(m^2, 4) = 1$. (*Hint*)

(c) Let $m = x + y$. Show that m is odd, and that we can rewrite $n = (x - y)(x + y)$ as: $n = m(m - 2y)$.

(d) Show that if $\mod(n, 4) = 1$, then y must be even. (*Hint*)

(e) Show that if $\mod(n, 4) = 3$, then y must be odd. (*Hint*)

$\Diamond$

The Fermat primality testing scheme is better for finding factors that are nearly equal. The brute force method of Exercise 41 is much better when one factor is much better than the other one.

Exercise 46.

(a) Create a spreadsheet that factors large numbers using the brute force scheme. You may use the spreadsheet in Figure 5.7 for inspiration. Some of the formulas in the spreadsheet are:

- Cell A7: =A6+2
- Cell B6: =$B$2/A6
- Cell C6: =IF(B6=FLOOR(B6,1),A6,0)
- Cell E2: =MAX(C6:C99999)

You may obtain the rest of the formulas using the spreadsheet's "fill down" capability.

(b) Use this spreadsheet to factor $n = 3551$. Then, use your result to find the decoding key D for Exercise 37 part (a).

(c) Use this spreadsheet to find the decoding key D for Exercise 37 part (b).

(d) Use this spreadsheet to find the decoding key D for Exercise 37 part (c).

(e) Use this spreadsheet to find the decoding key D for Exercise 37 part (d).

(f) Given the encryption key $(n, E) = (451, 231)$, find D.

(g) Given the encryption key $(n, E) = (3053, 1921)$, find D.

♢

	A	B	C	D	E
1	**BRUTE FORCE FACTORING**				
2	***Number n:***	45629		***Max. factor***	443
3	***sqrt(n)***	213.609			
4					
5	Trial factors	Quotient	Which are factors?		
6	3	15209.7	0		
7	5	9125.8	0		
8	7	6518.43	0		
9	9	5069.89	0		

Figure 5.7. Spreadsheet for brute force factoring method

Exercise 47.

(a) Make a spreadsheet for Fermat's factoring method. You may use the spreadsheet in Figure 5.8 for inspiration. Some of the formulas in the spreadsheet are:

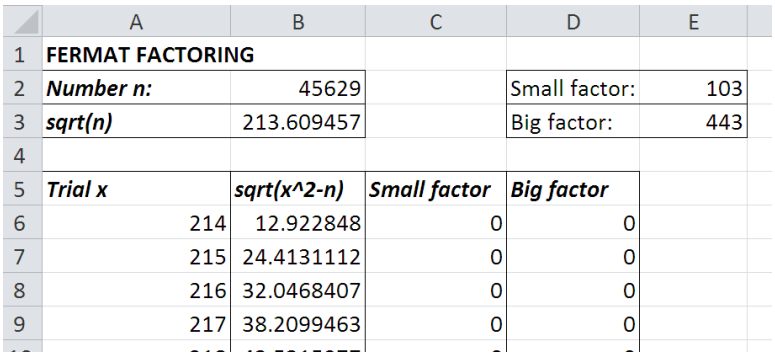
- Cell A7: =A6+1
- Cell B6: =SQRT(A6*A6 - $B$2)
- Cell C6: =IF(B6=FLOOR(B6,1),A6-B6,0)
- Cell D6: =IF(B6=FLOOR(B6,1),A6+B6,0)
- Cell E2: =MAX(C6:C99999)
- Cell F2: =MAX(D6:D99999)

You may obtain the rest of the formulas using the spreadsheet's "fill down" capability.

(b) Use this spreadsheet to factor $n = 7433551$. Then, use your result to find the decoding key D for $(n, E) = (7433551, 12345)$.

(c) Use this spreadsheet to factor $n = 16394854313$. Then, use your result to find the decoding key D for $(n, E) = (16394854313, 34578451)$.

◊



	A	B	C	D	E
1	**FERMAT FACTORING**				
2	***Number n:***	45629		Small factor:	103
3	***sqrt(n)***	213.609457		Big factor:	443
4					
5	***Trial x***	***sqrt(x^2-n)***	***Small factor***	***Big factor***	
6	214	12.922848	0	0	
7	215	24.4131112	0	0	
8	216	32.0468407	0	0	
9	217	38.2099463	0	0	

Figure 5.8. Spreadsheet for Fermat difference-of-squares factoring method

Exercise 48. * Using the results from Exercise 45 parts (d) and (e), modify the spreadsheet that you created in Exercise 47 to make it twice as efficient. In other words, modify the formula in cell A6 so that you can replace the formula in A7 with the formula: '=A6+2'. ◊

Probabilistic methods using the "little Fermat theorem"

In practice, neither the brute force nor the Fermat method is used to verify large prime numbers. Instead, *probabilistic methods* are used: these methods can show that it's very, very likely that n is a prime, but they don't prove for certain. The principal test of this type is the ***Miller-Rabin test*** for primality. This test uses some of the principles described below.

In Exercise 37 in Section 12.3.2, we will prove the following fact (which is widely known as *Fermat's little theorem*):

If p is any prime number and a is any nonzero integer, then $a^{p-1} \equiv 1 \pmod{p}$.

We can use Fermat's little theorem as a screening test for primes. For example, 15 cannot be prime since

$$2^{15-1} \equiv 2^{14} \equiv 4 \pmod{15}.$$

However, 17 is a potential prime since

$$2^{17-1} \equiv 2^{16} \equiv 1 \pmod{17}.$$

We say that an odd composite number n is a ***pseudoprime*** if

$$2^{n-1} \equiv 1 \pmod{n}.$$

Exercise 49. Which of the following numbers are primes and which are pseudoprimes?

(a) 341 **(b)** 811

(c) 601 **(d)** 561

(e) 771 **(f)** 631

$\Diamond$

Let n be an odd composite number and b be a positive integer such that $\gcd(b, n) = 1$. If $b^{n-1} \equiv 1 \pmod{n}$, then n is a ***pseudoprime base*** b. We can get a more accurate test for the primality of n if we test n versus a number of prime bases. If n is a pseudoprime for several prime bases, then we can say with high confidence that n is most probably a prime.

Exercise 50. Show that 341 is a pseudoprime base 2 but not a pseudoprime base 3. $\Diamond$

There exist composite numbers that are pseudoprimes for all bases to which they are relatively prime. These numbers are called ***Carmichael numbers***. The first Carmichael number is $561 = 3 \cdot 11 \cdot 17$. In 1992, Alford, Granville, and Pomerance proved that there are an infinite number of Carmichael numbers [4]. However, Carmichael numbers are very rare. There are only 2163 Carmichael numbers less than 25×10^9. For more sophisticated primality tests, see [1], [6], or [7].

Historical Note

Encrypting secret messages goes as far back as ancient Greece and Rome. As we know, Julius Caesar used a simple shift code to send and receive messages. However, the formal study of encoding and decoding messages probably began with the Arabs in the 1400s. In the fifteenth and sixteenth centuries mathematicians such as Alberti and Viete discovered that monoalphabetic cryptosystems offered no real security. In the 1800s, F. W. Kasiski established methods for breaking ciphers in which a ciphertext letter can represent more than one plaintext letter, if the same key was used several times. This discovery led to the use of cryptosystems with keys that were used only a single time. Cryptography was placed on firm mathematical foundations by such people as W. Friedman and L. Hill in the early part of the twentieth century.

During World War II mathematicians were very active in cryptography. Efforts to penetrate the cryptosystems of the Axis nations were organized in England and in the United States by such notable mathematicians as Alan Turing and A. A. Albert. The period after World War I saw the development of special-purpose machines for encrypting and decrypting messages. The Allies gained a tremendous advantage in World War II by breaking the ciphers produced by the German Enigma machine and the Japanese Purple ciphers.

By the 1970s, interest in commercial cryptography had begun to take hold. There was a growing need to protect banking transactions, computer data, and electronic mail. In the early 1970s, IBM developed and implemented LUZIFER, the forerunner of the National Bureau of Standards' Data Encryption Standard (DES).

The concept of a public key cryptosystem, due to Diffie and Hellman, is very recent (1976). It was further developed by Rivest, Shamir, and Adleman with the RSA cryptosystem (1978). It is not known how secure any of these systems are. The trapdoor knapsack cryptosystem, developed by Merkle and Hellman, has been broken. It is still an open question whether or not the RSA system can be broken. At the time of the writing of this book, the largest number factored is 135 digits long, and at the present moment a code is considered secure if the key is about 400 digits long and is the product of two 200-digit primes. There has been a great deal of controversy about research in cryptography in recent times: the National Security Agency would like to keep information about cryptography secret, whereas the academic community has fought for the right to publish basic research.

Modern cryptography has come a long way since 1929, when Henry Stimson, Secretary of State under Herbert Hoover, dismissed the Black Chamber (the State Department's cryptography division) in 1929 on the ethical grounds that "gentlemen do not read each other's mail." □

5.3 References and suggested readings

[**1**] Bressoud, D. M. *Factorization and Primality Testing.* Springer-Verlag, New York, 1989.

[**2**] Diffie, W. and Hellman, M. E. "New Directions in Cryptography," *IEEE Trans. Inform. Theory* **22** (1976), 644–54.

[**3**] Gardner, M. "A New Kind of Cipher that Would Take a Million Years to Break," *Scientific American* **237** (1977), 120–24.

[**4**] Granville, A. "Primality Testing and Carmichael Numbers," *Notices of the American Mathematical Society* **39**(1992), 696–700.

[**5**] Hellman, M. E. "The Mathematics of Public Key Cryptography," *Scientific American* **241** (1979), 130–39.

[**6**] Koblitz, N. *A Course in Number Theory and Cryptography.* Springer-Verlag, New York, 1987.

[**7**] Pomerance, C., ed. *Cryptology and Computational Number Theory.* Proceedings of Symposia in Applied Mathematics, vol. 42. American Mathematical Society, Providence, RI, 1990.

[**8**] Rivest, R. L., Shamir, A., and Adleman, L., "A Method for Obtaining Signatures and Public-key Cryptosystems," *Comm. ACM* **21**(1978), 120–26.

6

Set Theory

6.1 Set Basics

6.1.1 What's a set? (mathematically speaking, that is)

You've probably seen sets, set relations, and set operations in previous classes. In fact, in the previous two chapters of this book you've already been working with sets. So we'll review them quickly before moving on to further properties and proofs concerning sets and their accessories.[1]

First of all, we provide a precise mathematical definition for "set":

Definition 1. A ***set*** is a well-defined collection of objects: that is, it is defined in such a manner that we can determine for any given object x whether or not x belongs to the set. The objects that belong to a set are called its ***elements*** or ***members***. We will denote sets by capital letters, such as A or X; if a is an element of the set A, we write $a \in A$. △

6.1.2 How to specify sets

Two common ways of specifying sets are:

- by listing all of its elements inside a pair of braces; or
- by stating the property that determines whether or not an object x belongs to the set.

[1] This chapter is an adapted and expanded version of a chapter by D. and J. Morris.

For example, we might write

$$X = \{x_1, x_2, \ldots, x_n\}$$

for a set containing elements $x_1, x_2, \ldots, x_n$ or

$$X = \{x : x \text{ satisfies } \mathcal{P}\}$$

if each x in X satisfies a certain property $\mathcal{P}$.

Specifically: if E is the set of even positive integers, we can describe E by writing either

$$E = \{2, 4, 6, \ldots\} \quad \text{or} \quad E = \{x : x \text{ is an even integer and } x > 0\}.$$

We write $2 \in E$ when we want to say that 2 is in the set E, and $-3 \notin E$ to say that -3 is not in the set E.

Realize also that a set does not have to involve numbers. The next exercise provides some examples of this.

Exercise 2.

(a) What elements are in the following set: $S = \{x : x$ is the name of a U.S. state and x begins with 'W'$\}$? Write the set as a list of objects.

(b) Rewrite the following set by using a property: $T =$\{Jan. 4th 2011, Jan. 11th 2011, Jan. 18 2011, Jan. 25 2011,. . ., Dec. 27 2011 \} (Note: January 1 2011 was on a Saturday).

(c) Write the set of odd integers O: (i) as a list, and (ii) by using a property.

$\Diamond$

It is possible for the elements of a set to be sets in their own right. For instance, we could define

$$T = \{x : x \text{ is a National League baseball team}\}.$$

A more mathematical (but less interesting) example would be

$$S = \{x : x \text{ is a set of integers}\}.$$

Then elements of S would include the sets $\{1, 2, 3, 4\}$, {the set of odd integers}, $\{0\}$, and so on.

We can even go farther, and define sets of sets of sets. For instance, the set L of major baseball leagues in the U.S. has two elements:

$$L = \{\text{American League, National League}\}.$$

However, the American League A consists of a set of teams:

$$A = \{\text{Yankees, Red Sox}, \ldots\},$$

whle the National League N also consists of a set of teams:

$$N = \{\text{Cubs, Phillies}, \ldots\}.$$

Each of these teams consists of a set of players: so altogether the set L is a set of sets of sets!

Exercise 3. Give an example of a set which is set of sets of sets of sets (have fun!) ◊

This notion of "sets of sets" can bring us into dangerous territory. For example, consider the set

$$S = \{x : x \text{ is a set which is not an element of itself}\}.$$

Then the question arises: is S an element of itself?

Let us consider the possibilities:

- Suppose first that S is an element of itself. Then S must satisfy the defining property of elements of S – that is, S must be an example of a set x for which "x is not an element of itself." It follows that S is not an element of itself. This contradicts our supposition – so apparently our supposition is wrong, and S must not be an element of itself.

- On the other hand, suppose that S is not an element of itself. Then S satisfies the defining property of elements of S – that is, S is an example of a set x for which "x is not an element of itself." It follows that S is an element of S. Once again this contradicts our supposition – so apparently S must be an element of itself!

How do we get out of this mess? No matter what we assume, we end up with a contradiction! The problem, as is often the case, lies in *hidden assumptions* that we have made. Our definition of S makes reference to the unknown x,

where x is an "arbitrary" set. Herein lies the rub: the notion of "arbitrary" set is *not well-defined*. Put another way: the set of "all possible sets" is NOT a set!

In the following discussion we will avoid this problem by always starting out with a well-defined set that contains all the sets and elements of interest in a particular example or problem. Such an all-encompassing set is referred to as a ***universal set***. Note each particular problem will have its own universal set. For instance, if we are talking about public opinion polls in the United States, an appropriate universal set might be the set of American citizens. If we're talking about sets of prime and composite numbers, our universal set could be either the set of integers, or the set of natural numbers. If we are talking about roots of algebraic equations, depending on our particular interest we might choose the universal set to be the set of real numbers, or the set of complex numbers. When we talk about sets in a general way, we often denote sets by captial letters $A, B, C, ...$, and it's assumed that all these sets are subsets of some universal set U.

6.1.3 Important sets of numbers

We will refer often to the following sets of numbers. Although we are presuming that these sets are "given", the reader should be aware that it's not at all easy to formally define them in a mathematically precise way. (Although we won't give any definitions here, you may encounter them in other mathematics courses, such as logic or analysis.)

- $\mathbb{N} = \{n : n \text{ is a natural number}\} = \{1, 2, 3, \ldots\}$; (Note that according to our definition the natural numbers do <u>not</u> include 0. Some books include 0 as a natural number.)
- $\mathbb{Z} = \{n : n \text{ is an integer}\} = \{\ldots, -1, 0, 1, 2, \ldots\}$;
- $\mathbb{Q} = \{r : r \text{ is a rational number}\}$;
- $\mathbb{R} = \{x : x \text{ is a real number}\}$;

You may recall that in Chapter 3, we defined the set of complex numbers $\mathbb{C}$ as

$$\mathbb{C} := \{x + iy, \text{ such that } x, y \in \mathbb{R}\}.$$

This is just one example of a favorite gambit of mathematicians, namely creating new sets from existing sets in various imaginative ways. You'll be seeing many more examples of this as we go along.

Subsets and proper subsets

Definition 4. A set A is a ***subset*** of B, written $A \subset B$ or $B \supset A$, if every element of A is also an element of B. △

For example, using this notation we may write:

$$\{\text{sons of parents John and Jane Doe}\} \subset \{\text{children of John and Jane Doe}\}$$

and

$$\{4, 5, 8\} \subset \{2, 3, 4, 5, 6, 7, 8, 9\}$$

and

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

According to Definition 4, every set is a subset of itself. That is, for any set A, $A \subset A$, since every element in A is, of course, in A. This is true, but like we said, it's trivial, a nuisance, because the prefix of the word subset causes us to think of a set that is smaller than, or "less than" the other set. To distinguish then between this trivial case and what we would expect subset to mean, we introduce the term ***proper subset***: a set B is a ***proper subset*** of a set A if $B \subset A$ but $B \neq A$. For instance, if John and Jane Doe had only sons, then

$$\{\text{sons of John and Jane Doe}\} \subset \{\text{children of John and Jane Doe}\}, \text{ but}$$

$$\{\text{sons of John and Jane Doe}\} \text{ is not a } \textbf{\textit{proper}} \text{ subset of}$$
$$\{\text{children of John and Jane Doe}\}$$

Remark 5. In this book, we use '$\subset$' for subset, and we have no special symbol to distinguish "proper subset" from "subset". Some authors use '$\subseteq$' to denote subset, and '$\subset$' to denote proper subset. This has the advantage that then '$\subseteq$' and '$\supseteq$' are similar to '$\leq$' and '$\geq$', while '$\subset$' and '$\supset$' are like '$<$' and '$>$'. But we rarely have to distinguish the case of proper subsets, so it's not worth defining a special symbol for them. △

If A is not a subset of B, we write $A \not\subset B$; for example, $\{4, 7, 9\} \not\subset \{2, 4, 5, 8, 9\}$. Two sets are ***equal***, written $A = B$, if we can show that $A \subset B$ and $B \subset A$.

It is convenient to have a set with no elements in it. This set is called the ***empty set*** and is denoted by $\emptyset$. For instance, if John and Jane Doe had only daughters, then

$$\{\text{sons of John and Jane Doe}\} = \emptyset$$

Note that the empty set is a subset of every set.

Exercise 6. Let S be a set with a single element.

(a) How many subsets does it have?

(b) How many proper subsets does it have?

(c) How many nonempty subsets does it have?

(d) How many nonempty proper subsets does it have?

$\Diamond$

Exercise 7.

(a) Can you give an example of a set with exactly three subsets? How about exactly three proper subsets?

(b) What is the smallest number of elements a set must have in order to have eight proper subsets?

$\Diamond$

6.1.4 Operations on sets

In our halcyon days of youth, we were introduced to ***operations*** on integers, rational numbers, etc.. An operation on the integers takes two integers and always comes up with another integer. For instance, the '+' operation gives $2 + 3 = 5$ (of course, we know now that this means that + has the property of *closure*).

Exercise 8. What's wrong with the following statement: "Subtraction is an operation on the natural numbers." $\Diamond$

In a similar way, we can construct new sets out of old sets using *set operations*. The mathematical definitions of the basic set operations are as follows:

Definition 9. The ***union*** $A \cup B$ of two sets A and B is defined as

$$A \cup B = \{x : x \in A \text{ or } x \in B\};$$

△

Definition 10. the ***intersection*** of A and B is defined by

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

△

For example: if $A = \{1, 3, 5\}$ and $B = \{1, 2, 3, 9\}$, then

$$A \cup B = \{1, 2, 3, 5, 9\} \quad \text{and} \quad A \cap B = \{1, 3\}.$$

We may also consider the union and the intersection of more than two sets. For instance, the union of three sets A_1, A_2, and A_3 can be written $A_1 \cup A_2 \cup A_3$ or $\bigcup_{i=1}^{3} A_i$.

Similarly, the intersection of the same three sets can be written as $A_1 \cap A_2 \cap A_3$ or $\bigcap_{i=1}^{3} A_i$.

Remark 11. There's actually a technical difficulty with our notations for $A_1 \cup A_2 \cup A_3$ and $A_1 \cap A_2 \cap A_3$. The problem is that the notation is ambiguous: does $A_1 \cup A_2 \cup A_3$ mean $(A_1 \cup A_2) \cup A_3$ or $A_1 \cup (A_2 \cup A_3)$? As it turns out, it doesn't make any difference (we'll show this in the next section). Since it doesn't matter which order we do the $\cup$, we just leave off the parentheses (and the same for $\cap$). This is really nothing new: you're used to writing $3 + 4 + 7 + 9$ instead of $((3 + 4) + 7) + 9$, because it doesn't matter what order you add the numbers. △

Exercise 12.

(a) Find three sets A_1, A_2, A_3 such that $A_1 \cup A_2 \cup A_3 = \mathbb{Z}$ and $A_1 \cap A_2 \cap A_3 = \emptyset$

(b) Find three sets A_1, A_2, A_3 such that (i) $A_1, A_2, A_3 \subset \mathbb{C}$; (ii) $A_1 \cap A_2 \neq \emptyset, A_2 \cap A_3 \neq \emptyset, A_1 \cap A_3 \neq \emptyset$; and (iii) $A_1 \cap A_2 \cap A_3 = \emptyset$

(c) Find three sets that satisfy all conditions of part (b) and in addition satisfy $A_1 \cup A_2 \cup A_3 = \mathbb{C}$.

$\Diamond$

We may generalize to intersections and unions of collections of n sets by writing:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n$$

and

$$\bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n$$

for the union and intersection, respectively, of the collection of sets $A_1, \ldots A_n$.

Example 13. Specify the following sets, either by:

- listing the elements;
- describing with a property; or
- giving another set that we've already defined that has the same elements.

(a) $\bigcup_{i=1}^{n}\{i\}$

(b) $\bigcup_{i=1}^{n}\{1, \ldots, i\}$

(c) $\bigcup_{i=1}^{\infty}\{1, \ldots, i\}$

Solutions:

(a) $\bigcup_{i=1}^{n}\{i\} = \{1\}\bigcup\{2\}\bigcup\{3\}\bigcup\ldots\bigcup\{n\}$
$= \{1, \ldots, n\}$ $[list\ of\ elements]$
$=$ all integers from 1 to n. $[property]$

(b) $\bigcup_{i=1}^{n}\{1,\ldots,i\} = \{1\}\bigcup\{1,2\}\bigcup\{1,2,3\}\bigcup\ldots\bigcup\{1,\ldots,n\}$
$= \{1,\ldots,n\}$ $[list\ of\ elements]$
$=$ all integers from 1 to n. $[property]$

(c) $\bigcup_{i=1}^{\infty}\{1,\ldots,i\} =$ [by part (b)] $\{1,\ldots,\infty\} = \mathbb{N}$

♦

Exercise 14. Specify the following sets, either by:

- listing the elements;
- describing with a property; or
- giving another set that we've already defined that has the same elements.

(a) $\bigcap_{i=1}^{n}\{i\}$

(b) $\bigcap_{i=1}^{n}\{1,\ldots,i\}$

(c) $\bigcap_{i=1}^{\infty}\{1,\ldots,i\}$

(d) $\bigcup_{r=0}^{n-1}\{$Integers that have remainder r when divided by $n\}$

(e) $\bigcap_{r=0}^{n-1}\{$Integers that have remainder r when divided by $n\}$

◊

Exercise 15.

(a) Find an infinite collection of sets $\{A_i\}, i = 1,2,3,\ldots$ such that (i) $A_i \subset \mathbb{R}, i = 1,2,3,\ldots$; (ii) each A_i is a closed interval of length 1 (that is, $A_i = [a_i, a_i + 1]$ for some a_i; and (iii) $\bigcup_{i=1}^{\infty} A_i = [0,\infty)$. (That is, the union of all the A_i's is the set of all nonnegative real numbers.)

(b) Find an infinite collection of sets $\{A_i\}, i = 1,2,3,\ldots$ such that (i) $A_i \subset \mathbb{R}, i = 1,2,3,\ldots$; (ii) each A_i is an open interval of length 1 (that is, $A_i = (a_i, a_i + 1)$ for some a_i; and (iii) $\bigcup_{i=1}^{\infty} A_i = (0,\infty)$. (That is, the union of all the A_i's is the set of all positive real numbers.)

(c) Find an infinite collection of sets $\{A_n\}, n = 1, 2, 3, \ldots$ such that (i) $A_n \subset [-1/2, 1/2], n = 1, 2, 3, \ldots$; (ii) each A_n is an open interval of length $1/n$; and (iii) $\bigcap_{n=1}^{\infty} A_n = \{0\}$.

(d) **Find an infinite collection of sets $\{A_n\}, n = 1, 2, 3, \ldots$ such that (i) $A_n \subset [0, 1], n = 1, 2, 3, \ldots$; (ii) each A_n is an open interval of length $1/n$; (iii) $A_{n+1} \subset A_n, n = 1, 2, 3, \ldots$; and (iv) $\bigcap_{n=1}^{\infty} A_n = \emptyset$.

$\Diamond$

When two sets have no elements in common, they are said to be ***disjoint***; for example, if E is the set of even integers and O is the set of odd integers, then E and O are disjoint. Two sets A and B are disjoint exactly when $A \cap B = \emptyset$.

Exercise 16.

(a) Find four disjoint sets A_1, A_2, A_3, A_4 such that $\bigcup_{i=1}^{4} A_i = \mathbb{Z}$.

(b) Find four disjoint sets A_1, A_2, A_3, A_4 such that $\bigcup_{i=1}^{4} A_i = \mathbb{R}$.

(c) Find four disjoint sets A_1, A_2, A_3, A_4 such that $\bigcup_{i=1}^{4} A_i = \mathbb{C}$.

$\Diamond$

If we are working within the universal set U and $A \subset U$, we define the ***complement***[2] of A (denoted by A'), to be the set

$$A' = \{x : x \in U \text{ and } x \notin A\}.$$

Definition 17. The ***difference*** of two sets A and B is defined as

$$A \setminus B = A \cap B' = \{x : x \in A \text{ and } x \notin B\}.$$

$\triangle$

Exercise 18. Suppose that $A \subset B$. What is the largest subset of B that is disjoint from A? $\Diamond$

[2]Please note the spelling: 'complement', not 'compliment', thank you!

The set difference concludes our set operations for now. The following example and exercises will give you an opportunity to sharpen your set operation skillls.

Example 19. Let $\mathbb{N}$ be the universal set, and suppose that

$$\begin{aligned} A &= \{x \in \mathbb{N} : x \text{ is divisible by } 2\} \\ B &= \{x \in \mathbb{N} : x \text{ is divisible by } 3\} \\ C &= \{x \in \mathbb{N} : x \text{ is divisible by } 6\} \\ D &= \{\text{the odd natural numbers}\} \end{aligned}$$

Then specify the following sets:

(a) $A \cap B$

(b) $C \cup A$

(c) $D \setminus B$

(d) B'

Solutions:

(a)

$$\begin{aligned} A \cap B &= \{x \in \mathbb{N} : x \text{ is divisible by 2 and } x \text{ is divisible by } 3\} \\ &= \{x \in \mathbb{N} : x \text{ is divisible by } 6\} \\ &= C \end{aligned}$$

(b)

$$\begin{aligned} C \cup A &= \{x \in \mathbb{N} : x \text{ is divisible by 6 or } x \text{ is divisible by } 2\} \\ &= \{2, 4, 6, 8, 10, 12, \ldots\} \\ &= A \end{aligned}$$

(c)

$$\begin{aligned} D \setminus B &= \{x \in \mathbb{N} : x \in D \text{ and } x \notin B\} \\ &= \{x \in \mathbb{N} : x \text{ is an odd natural number and } x \text{ is } \textit{not} \text{ divisible by } 3\} \\ &= \{x \in \mathbb{N} : x \text{ is an odd natural number that is not divisible by } 3\} \end{aligned}$$

(d)

$$\begin{aligned} B' &= \{x \in \mathbb{N} : x \text{ is divisible by } 3\}' \\ &= \{x \in \mathbb{N} : x \text{ is not divisible by } 3\} \end{aligned}$$

♦

Exercise 20. Let $\mathbb{N}$ be the universal set and suppose that

$$\begin{aligned} A &= \{x \in \mathbb{N} : x \text{ is divisible by } 2\} \\ B &= \{x \in \mathbb{N} : x \text{ is divisible by } 3\} \\ C &= \{x \in \mathbb{N} : x \text{ is divisible by } 6\} \\ D &= \{\text{the odd natural numbers}\} \end{aligned}$$

Specify each of the following sets. You may specify a set either by describing a property, by enumerating the elements, or as one of the four sets A, B, C, D:

(a) $(A \cap B) \setminus C$

(b) $A \cap B \cap C \cap D$

(c) $A \cup B \cup C \cup D$

◊

Exercise 21. Let $\mathbb{N}$ be the universal set and suppose that

$$\begin{aligned} A &= \{x : x \in \mathbb{N} \text{ and } x \text{ is even}\}, \\ B &= \{x : x \in \mathbb{N} \text{ and } x \text{ is prime}\}, \\ C &= \{x : x \in \mathbb{N} \text{ and } x \text{ is a multiple of } 5\}. \end{aligned}$$

Describe each of the following sets. Make your description as concise as possible.

(a) $A \cap B$

(b) $(A \cap B)'$

(c) $A' \cap B'$

(d) $A \cup B$

(e) $(A \cup B)'$

(f) $A' \cup B'$

(g) $B \cap C$

(h) $A \cap (B \cup C)'$

◊

6.2 Properties of set operations

Now that we have the basics out of the way, let's look at the some of the properties of set operations. The individual steps of the following proofs depend on *logic*; and a rigorous treatment of these proofs would require that we introduce formal logic and its rules. However, many of these logical rules are intuitive, and it should be possible for you to follow the proofs even if you haven't studied mathematical logic.

First, we give two rather obvious (but very useful) properties of $\cup$ and $\cap$:

Proposition 22. Given any sets A, B, It is always true that

$$A \cap B \subset A \quad \text{and} \quad A \subset A \cup B.$$

PROOF. The style of proof we'll use here is often described as *element by element*, because the proofs make use of the definitions of $A \cap B$ and $A \cup B$ in terms of their elements.

First, suppose that x is an element of $A \cap B$. we then have:

$$\begin{aligned} & x \in A \cap B && \text{[supposition]} \\ \Rightarrow & x \in A \text{ and } x \in B && \text{[def. of } \cap\text{]} \\ \Rightarrow & x \in A. && \text{[logic]} \end{aligned}$$

Since every element of $A \cap B$ is an element of A, it follows by the definition of $\subset$ that $A \cap B \subset A$.

Exercise 23. Give a similar proof of the second part of Proposition 22. ◊

□

Many useful properties of set operations are summarized in the following multi-part proposition:

Proposition 24. Let A, B, and C be subsets of a universal set U. Then

1. $A \cup A' = U$ and $A \cap A' = \emptyset$
2. $A \cup A = A$, $A \cap A = A$, and $A \setminus A = \emptyset$;
3. $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$;
4. $A \cup U = U$ and $A \cap U = A$;
5. $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$;
6. $A \cup B = B \cup A$ and $A \cap B = B \cap A$;
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
8. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

PROOF. We'll prove parts (1), (2), (5), and (7), and leave the rest to you!

(1) From our definitions we have:

$$\begin{aligned} A \cup A' &= \{x : x \in A \text{ or } x \in A'\} && \text{[def. of } \cup\text{]} \\ &= \{x : x \in A \text{ or } x \notin A\} && \text{[def. of complement]} \end{aligned}$$

But every $x \in U$ must satisfy either $x \in A$ or $x \notin A$. It follows that $A \cup A'$ includes all elements of U; so $A \cup A' = U$.

We also have

$$\begin{aligned} A \cap A' &= \{x : x \in A \text{ and } x \in A'\} && \text{[def. of } \cap\text{]} \\ &= \{x : x \in A \text{ and } x \notin A\} && \text{[def. of complement]} \end{aligned}$$

But there is no element x that is both in A and not in A, it follows that there are no elements in $A \cap A'$; so $A \cap A' = \emptyset$.

(2) Observe that

$$\begin{aligned} A \cup A &= \{x : \ x \in A \text{ or } x \in A\} && \text{[def. of } \cup\text{]} \\ &= \{x : \ x \in A\} \\ &= A \end{aligned}$$

and

$$\begin{aligned} A \cap A &= \{x : \ x \in A \text{ and } x \in A\} && \text{[def. of } \cap] \\ &= \{x : \ x \in A\} \\ &= A. \end{aligned}$$

Also,

$$\begin{aligned} A \setminus A &= A \cap A' && \text{[def. of } \setminus] \\ &= \emptyset. && \text{[by part 1]} \end{aligned}$$

(5) For sets A, B, and C,

$$\begin{aligned} A \cup (B \cup C) &= A \cup \{x : \ x \in B \text{ or } x \in C\} && \text{[def. of } \cup] \\ &= \{x : \ x \in A \text{ or } x \in B \text{ or } x \in C\} && \text{[def. of } \cup] \\ &= \{x : \ x \in A \text{ or } x \in B\} \cup C && \text{[def. of } \cup] \\ &= (A \cup B) \cup C. && \text{[def. of } \cup] \end{aligned}$$

A similar argument proves that $A \cap (B \cap C) = (A \cap B) \cap C$.

(7) We show that these two sets are equal by showing that:

(I) Every element x in $A \cup (B \cap C)$ is also an element of $(A \cup B) \cap (A \cup C)$;

(II) Every element x in $(A \cup B) \cap (A \cup C)$ is also an element of $A \cup (B \cap C)$.

(It's actually a rather common strategy to prove that two sets are equal by showing that every element of one set is an element of the other set, and vice versa.)

Let's begin by proving (I). Take any element $x \in A \cup (B \cap C)$. Then $x \in A$ or $(x \in B \cap C)$, by the definition of $\cup$. We may therefore consider two cases: (i) $x \in A$, or (ii) $x \in B \cap C$. (Actually some x's are included in both cases, but that's not a problem.)

Case i: If $x \in A$, the by Proposition 22 we know $x \in A \cup B$ and $x \in A \cup C$. By the definition of $\cap$, we then have $x \in (A \cup B) \cap (A \cup C)$.

Case ii: If $x \in B \cap C$, then by Proposition 22 we know $x \in B$ and $x \in C$. By Proposition 22, then $x \in A \cup B$ and $x \in A \cup C$. By the definition of $\cap$, this means that $x \in (A \cup B) \cap (A \cup C)$.

This completes the proof of (I). Now we'll prove (II). Take any element $x \in (A \cup B) \cap (A \cup C)$. Then we may consider two cases: (i) $x \in A$, or (ii) $x \notin A$.

Case i: If $x \in A$, then by by Proposition 22 it's also true that $x \in A \cup B$ and $x \in A \cup C$. By the definition of $\cap$, this means that $x \in (A \cup B) \cap (A \cup C)$.

Case ii: Suppose $x \notin A$. Now, since $x \in (A \cup B) \cap (A \cup C)$, by the definitions of $\cap$ and $\cup$ we know that ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$). But since $x \notin A$, it must be true that $x \in B$, and also $x \in C$. By the definition of $\cap$, this means that $x \in B \cap C$. by Proposition 22, we have that $x \in A \cup (B \cap C)$. This completes the proof of (II), which completes the proof of (7). □

Exercise 25. Fill in the blanks in the following proof of Proposition 24 part (3):

Observe that

$$\begin{aligned} A \cup \emptyset &= \{x : x \in A \text{ or } x \in \emptyset\} && \text{[Def. of } \cup\text{]} \\ &= \{x : x \in \_\_\_\_\_\} && \text{[}\emptyset\text{ has no elements]} \\ &= A && \text{Def. of set A} \end{aligned}$$

and

$$\begin{aligned} A \cap \emptyset &= \{x : \ x \in \_\_\_\_\_ \text{ and } x \in \_\_\_\_\_\} && \_\_\_\_\_ \\ &= \emptyset && \_\_\_\_\_. \end{aligned}$$

◊

Exercise 26. Prove parts 4,6,8 of Proposition 24 using element-by-element proofs. ◊

The following rules that govern the operations $\cap, \cup$ and $'$ follow from the definitions of these operations:

Proposition 27.[De Morgan's Laws] Let A and B be sets. Then

(1) $(A \cup B)' = A' \cap B'$;

(2) $(A \cap B)' = A' \cup B'$.

We will use the same strategy we used to prove Proposition 24 part (7): we show sets are equal by showing they are subsets of each other.

PROOF.

(1) First we show that $(A \cup B)' \subset A' \cap B'$. Let $x \in (A \cup B)'$. Then $x \notin A \cup B$. So x is neither in A nor in B, by the definition of $\cup$. By the definition of $'$, $x \in A'$ and $x \in B'$. Therefore, $x \in A' \cap B'$ and we have $(A \cup B)' \subset A' \cap B'$. To show the reverse inclusion, suppose that $x \in A' \cap B'$. Then $x \in A'$ and $x \in B'$, and so $x \notin A$ and $x \notin B$. Thus $x \notin A \cup B$ and so $x \in (A \cup B)'$. □

Exercise 28. Prove Proposition 27 part (2). ◊

Proposition 24 and Proposition 27 provide us with an arsenal of rules for set operations. You should consider these as your "rules of arithmetic" for sets: just as you used arithmetic rules in high school to solve algebraic equations, so now you can use these rules for set operations to solve set equations. Here is an example of how to do this:

Example 29. Prove that

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

PROOF. To see that this is true, observe that

$$\begin{aligned}
(A \setminus B) \cap (B \setminus A) &= (A \cap B') \cap (B \cap A') && \text{[definition of } \setminus\text{]} \\
&= A \cap A' \cap B \cap B' && \text{[by Proposition 24 parts 5 and 6]} \\
&= \emptyset \cap \emptyset && \text{[by Proposition 24 part 1]} \\
&= \emptyset.
\end{aligned}$$

□ ♦

Exercise 30. Prove the following statements by mimicking the style of proof in Example 29; that is use the definitions of $\cap, \cup, \setminus$, and $'$ as well as their properties listed in Proposition 24 and Proposition 27. This type of proof is called an "algebraic" proof. Every time you use a property, remember to give a reference!

(a) $(A \cap B) \setminus B = \emptyset$.

(b) $(A \cup B) \setminus B = A \setminus B$.

(c) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

(d) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

(e) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

(f) $(A \cup B \cup C) \cap D) = (A \cap D) \cup (B \cap D) \cup (C \cap D)$.

(g) $(A \cap B \cap C) \cup D) = (A \cup D) \cap (B \cup D) \cap (C \cup D)$.

$\Diamond$

6.3 Do the subsets of a set form a group?

Some of the properties in Proposition 24 may ring a bell. Recall that in the Section 4.4.7 of the Modular Arithmetic chapter we defined a ***group*** to be a set combined with an operation that has the following properties:

1. The group operation has the property of *closure*
2. The set has a unique *identity*
3. Every element of the set has its own *inverse*.
4. The set elements satisfy the *associative property* under the group operation.
5. *Some* groups satisfy the *commutative property* under the group operation.

If you forgot what these properties mean, look back at Definition 41and the surrounding discussion in the Integers Mod n section (this is a good chance to review!).

What we're going to do now is a first taste of a magic recipe that you're going to see again and again in Abstract Algebra. We're going to turn *sets* into *elements*. Abracadabra!

What do we mean by this? Let's take an example. Take the 3-element set $S = \{a, b, c\}$.

Exercise 31.

(a) List the *subsets* of $S = \{a, b, c\}$. Include the empty set and non-proper subsets of S. How many subsets are in your list?

(b) If you listed the subsets of $\{a, b\}$, how many subsets would be in your list?

(c) If you listed the subsets of $\{a, b, c, d\}$, how many subsets would be in your list?

(d) **If you listed the subsets of $\{a, b, c, \ldots, x, y, z\}$, how many subsets would be in your list? (*Hint*)

$\Diamond$

Let's take the list of subsets of $\{a, b, c\}$ that you came up with in part (a) of the previous exercise. We can consider this list as a set of 8 elements, where each element is a subset of the original set $S = \{a, b, c\}$. Let's call this 8-element set G. Remember, the elements of G are *subsets* of the original set S.

So now let's face the question: Is G a group?

Recall that a group has a single *operation*: that is, a way of combining two elements to obtain a third element. We actually have two candidates for an operation for G: either intersection or union. So we actually have two questions:

- Is G with the operation $\cup$ a group?
- Is G with the operation $\cap$ a group?

We'll take these questions one at a time. First we investigate group properties for the set G with the operation $\cup$:

Exercise 32. Let G be the set of subsets of the set $\{a, b, c\}$.

(a) Does the set G with the operation $\cup$ have the closure property? *Justify* your answer.

(b) Does the set G with the operation $\cup$ have an identity? If so, what is it? Which part of Proposition 24 enabled you to draw this conclusion?

(c) Is the operation $\cup$ defined on the set G associative? Which part of Proposition 24 enabled you to draw this conclusion?

(d) Is the operation $\cup$ defined on the set G commutative? Which part of Proposition 24 enabled you to draw this conclusion?

(e) Does each element of G have a unique inverse under the operation $\cup$? If so, which part of Proposition 24 enabled you to draw this conclusion? If not, provide a counterexample.

(f) Is the set G a group under the $\cup$ operation? *Justify* your answer.

$\Diamond$

Although Exercise 32 deals with a particular set of subsets, the results of the exercise are completely general and apply to the set of any subsets of *any* set (and not just $\{a, b, c\}$.

Now we'll consider $\cap$:

Exercise 33. Given a set A, let G be the set of all subsets of A.

(a) Does the set G with the operation $\cap$ have the closure property? *Justify* your answer.

(b) Does the set G with the operation $\cap$ have an identity? If so, what is it? Which part of Proposition 24 enabled you to draw this conclusion?

(c) Is the operation $\cap$ defined on the set G associative? Which part of Proposition 24 enabled you to draw this conclusion?

(d) Is the operation $\cap$ defined on the set G commutative? Which part of Proposition 24 enabled you to draw this conclusion?

(e) Does each element of G have a unique inverse under the operation $\cap$? If so, which part of Proposition 24 enabled you to draw this conclusion? If not, provide a counterexample.

(f) Is the set G a group under the $\cap$ operation? *Justify* your answer.

$\Diamond$

No doubt you're bitterly disappointed that neither $\cap$ nor $\cup$ can be used to define a group. However, take heart! Mathematicians use the $\cap$ nor $\cup$ operations to define a different sort of algebraic structure called (appropriately enough) a *Boolean algebra*. We won't deal further with Boolean algebras

in this course: suffice it to say that mathematicians have defined a large variety of abstract algebraic structures for different purposes.

Although $\cap$ and $\cup$ didn't work, there is a consolation prize:

Exercise 34. Besides $\cup$ and $\cap$, there is another set operation called *symmetric difference*, which is sometimes denoted by the symbol Δ and is defined as:

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Given a set A, let G be the set of all subsets of A. Repeat parts (a)–(f) of Exercise 33, but this time for the set operation Δ instead of $\cap$. $\Diamond$

7

Functions: basic concepts

The idea of a function should be familiar to you from previous math classes. Your calculus class no doubt was all about functions defined on real numbers. In this book, we will be more interested in functions on *finite* sets. Rather than "doing things" to these functions (such as integrating and differentiating), instead we will dig more deeply into the basic nature of functions themselves. This will eventually lead us to discover profound connections between groups and functions (see the Permutations chapter).[1]

7.1 The Cartesian product: a different type of set operation

In the previous chapter, we introduced set operations such as $\cup$ and $\cap$. In this chapter we are going to need yet another set operation. This operation is called the "Cartesian product", and is denoted by the symbol $\times$. In order to define the Cartesian product, we will first need a preliminary definition:

Definition 1. For any objects x and y, mathematicians use (x, y) to denote the **ordered pair** whose first coordinate is x and whose second coordinate is y. Two ordered pairs are equal if and only if both coordinates are equal:

$$(x_1, y_1) = (x_2, y_2) \text{ iff } x_1 = x_2 \text{ and } y_1 = y_2.$$

$\triangle$

[1] This chapter is an adapted and expanded version of a chapter by D. and J. Morris.

Example 2. The "coordinate plane" (or "xy-plane") that is used for graphing functions is one example of a set of ordered pairs. The xy-plane corresponds to $\mathbb{R} \times \mathbb{R}$ (sometimes written as $\mathbb{R}^2$), and is the set of ordered pairs of real numbers:

$$\mathbb{R} \times \mathbb{R} = \{(x, y) | x \in \mathbb{R}, y \in \mathbb{R}\}$$

Notice that the elements of $\mathbb{R}^2$ are *not* real numbers, but rather ordered pairs of real numbers. In other words,

$$x \in \mathbb{R} \text{ and } y \in \mathbb{R}, \text{ but } (x, y) \notin \mathbb{R}.$$

♦

We arrive at our general definition of Cartesian product by replacing $\mathbb{R}$ and $\mathbb{R}$ in our previous example with arbitrary sets A and B:

Definition 3. For any sets A and B, we define the ***Cartesian product*** of A and B (denoted $A \times B$ as:

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

In other words, x is an element of $A \times B$ if and only if x is an ordered pair of the form (a, b), where a is an element of A and b is an element of B.

△

Example 4.

1. $\{2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A\} \times \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\} =$ {a standard deck of cards }
2. $\{1, 2, 3\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.
3. $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.

♦

Exercise 5. In view of the previous example, is $\times$ commutative? *Explain* your answer. ◊

Exercise 6. Specify each set by listing its elements.

(a) $\{a, i\} \times \{n, t\}$

(b) $\{Q, K\} \times \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$

(c) $\{1, 2, 3\} \times \{3, 4, 5\}$

(d) $\{y, g, Y, G\} \times \{y, g, Y, G\}$

$\Diamond$

Now $A \times B$ can be considered an operation on the sets A and B, just like $A \cup B$ and $A \cap B$. But there is a very significant difference. Recall that if A and B are both subsets of the same universal set U, then so are $A \cup B$ and $A \cap B$. This is *not* the case for $A \times B$! The operation $A \times B$ takes the sets A and B and creates another set with a *completely new* type of element!

Exercise 7. Let $A = \{a, b\}$ and let $B = \{b, c\}$.

(a) Write the elements of $A \times B$ (there are four).

(b) What is $A \cap (A \times B)$? (Another way of thinking about this is: what elements of A are also elements of $A \times B$?)

(c) What is $B \cap (A \times B)$? (Another way of thinking about this is: what elements of B are also elements of $A \times B$?)

(d) We have shown in the previous chapter that the subsets of $\{a, b, c\}$ are closed under $\cup$ and $\cap$. Are the subsets of $\{a, b, c\}$ also closed under $\times$? *Explain* your answer.

$\Diamond$

We have been trying to emphasize that $A \times B$ is a very different set from the sets A and B. One question we could ask is: how does the number of elements in $A \times B$ compare with the numbers of elements in the sets A and B? By considering the above examples, you may be able to figure out a formula for yourself. Go ahead and try, before reading the answer below.

Proposition 8. Given any sets A and B, then:

$$\|A \times B| = |A| \cdot |B|.$$

Here the notation "$|S|$" means the number of elements in S.

PROOF. We can prove this formula by some creative arranging. Suppose the sets A and B hav m and n elements, respectively. We may list these elements as follows:

$$A = \{a_1, a_2, a_3, ..., a_m\} \text{ and } B = \{b_1, b_2, b_3, ..., b_n\}.$$

It follows that the elements of $A \times B$ are:

$$\begin{array}{ccccc}
(a_1, b_1), & (a_1, b_2), & (a_1, b_3), & \cdots & (a_1, b_n), \\
(a_2, b_1), & (a_2, b_2), & (a_2, b_3), & \cdots & (a_2, b_n), \\
(a_3, b_1), & (a_3, b_2), & (a_3, b_3), & \cdots & (a_3, b_n), \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
(a_m, b_1), & (a_m, b_2), & (a_m, b_3), & \cdots & (a_m, b_n).
\end{array}$$

In the above table that represents the elements of $A \times B$:

- each row has exactly n elements, and
- there are m rows,

It follows that the number of entries in the table is $m \cdot n$. □

Exercise 9.

(a) If $B = \{\text{vanilla, chocolate, strawberry}\}$, then what is $B \times \emptyset$?

(b) Using the definition of Cartesian product, show that for any set A, $A \times \emptyset = \emptyset$.

◊

7.2 Introduction to functions

7.2.1 Informal look at functions

You have seen many examples of functions in your previous math classes. Most of these were probably given by formulas, for example $f(x) = x^3$. But

functions can also be given in other ways. The key property of a function is that it accepts inputs, and provides a corresponding output value for each possible input.

Example 10. For the function $f(x) = x^3$, the input x can be any real number. Plugging a value for x into the formula yields an output value, which is also a real number. For example, using $x = 2$ as the input yields the output value $f(2) = 2^3 = 8$. ♦

The following properties are true of any function f:

1. Any function has a set of allowable inputs, which we call the ***domain*** of the function.
2. Any function also has a a set that contains all of the possible outputs, which we call the ***codomain*** of the function.

In Example 10, any real number can be used as the input x, so the domain is $\mathbb{R}$, the set of all real numbers. Similarly, any output is a real number, so the codomain can also be taken as $\mathbb{R}$.

Example 11. For the function $f(x) = x^2$, the input x can be any real number. The output is always a real number, so we can use $\mathbb{R}$ as the codomain. So we can take the domain and the codomain as the same set – but we don't have to. You may have already noticed that the output of f is never a negative number, so we could have used the interval $[0, \infty) = \{ x \in \mathbb{R} \mid x \geq 0 \}$ as the codomain. This shows that *the codomain of a function is not unique* – you can choose a different codomain and not change the function. However, *the domain of a function is unique*. If the set of allowable inputs is changed, then the function is changed in an essential fashion. ♦

Example 12. $g(x) = 1/x$ is *not* a function from $\mathbb{R}$ to $\mathbb{R}$. This is because 0 is an element of $\mathbb{R}$, but the formula does not define a value for $g(0)$. Thus, 0 cannot be in the domain of g. To correct this problem, one could say that g is a function from the set $\{ x \in \mathbb{R} \mid x \neq 0 \}$ of *nonzero* real numbers, to $\mathbb{R}$. ♦

Intuitively, a function from A to B can be thought of being any process that accepts inputs from the set A, and assigns an element of the set B to

each of these inputs. The process need not be given by a formula. Indeed, most of the functions that arise in science or in everyday life are not given by exact formulas, as illustrated in the following exercise.

Example 13.

1. Each point on the surface of the earth has a particular temperature right now, and the temperature (in degrees centigrade) is a real number. Thus, temperature defines a function temp from the surface of the earth to $\mathbb{R}$: temp(x) is the temperature at the point x.

2. The items in a grocery store each have a particular price, which is a certain number of cents, so price can be thought of as a function from the set of items for sale to the set $\mathbb{N}$ of all natural numbers: price(x) is the price of item x (in cents).

3. If we let People be the set of all people (alive or dead), then mother is a function from People to People. For example,

   $$\text{mother}(\text{Prince Charles}) = \text{Queen Elizabeth}.$$

   (To avoid ambiguity, we need to say that, by "mother," we mean "biological mother.")

4. In contrast, grandmother is *not* a function from People to People. This is because people have not just one grandmother, but two (a maternal grandmother and a paternal grandmother). For example, if we say that Prince Charles wrote a poem for his grandmother, we do not know whether he wrote the poem for the Queen Mother, or for his other grandmother. A function is not ever allowed to have such an ambiguity. (In technical terms, grandmother is a "relation," not a function. This will be explained in a later section)

♦

Functions are often represented as a *table* of values.

Example 14. The following table represents the prices of items in a grocery store:

item	price (in cents)
apple	65
banana	83
cherry	7
donut	99
eggs	155

This table represents a function price with the following properties:

- The domain of price is $\{\mathsf{apple}, \mathsf{banana}, \mathsf{cherry}, \mathsf{donut}, \mathsf{eggs}\}$.
- $\mathsf{price}(\mathsf{banana}) = 83$.
- $\mathsf{price}(\mathsf{guava})$ does not exist, because guava is not in the domain of the function.
- The codomain of price can be taken as $\mathbb{N}$, since all our prices are natural numbers. Now of course we don't really need all of $\mathbb{N}$: we can kick some numbers out of $\mathbb{N}$ that aren't actual prices, and the resulting set would still be a codomain. In fact, we could keep kicking numbers out until we get the set ...
- $\{65, 83, 7, 99, 155\}$. This "smallest possible codomain" is what we call the ***range*** of price. The range is the set of *actual* outputs of a function. No matter what codomain we choose, it is always true that the range is a subset of the codomain.

♦

It is also possible to represent each row of the table by an ordered pair. For example, the first row of the table is $\mathsf{apple} \mid 65$. This has apple on the left and 65 on the right, so we represent it by the ordered pair $(\mathsf{apple}, 65)$, which has apple on the left and 65 on the right. The second row is represented by $(\mathsf{banana}, 83)$. Continuing in this way yields a total of 5 ordered pairs (one for each row). To keep them gathered together, we can put the 5 ordered pairs into a single set:

$$\big\{\, (\mathsf{apple}, 65), (\mathsf{banana}, 83), (\mathsf{cherry}, 7), (\mathsf{donut}, 99), (\mathsf{eggs}, 155) \,\big\}.$$

This set of ordered pairs contains exactly the same information as a table of values, but the set is a more convenient form for mathematical manipulations.

Exercise 15. Here is a function f given by a table of values.

x	$f(x)$
1	7
2	3
3	2
4	4
5	9

(a) What is the domain of f?

(b) What is the range of f?

(c) What is $f(3)$?

(d) Represent f as a set of ordered pairs.

(e) Find a formula to represent f. (*Hint*)

◊

Example 16. Not every table of values represents a function. For example, suppose we have the following price list, which is a slight change from Example 14:

item	price (in cents)
apple	65
banana	83
cherry	7
donut	99
banana	155

There is a problem here, because there are two possible prices for a banana, depending on which line of the table is looked at. (So you might pick up a banana, expecting to pay 83 cents, and end up having the cashier charge you $1.55.) This is not allowed in a function: each input must have exactly one output, not a number of different possible outputs. Thus, if a table represents a function, and an item appears in the left side of more than one row, then all of those rows must have the same output listed on the right side. ⧫

Remark 17. A 2-column table represents a function from A to B if and only if:

1. every value that appears in the left column of the table is an element of A,
2. every value that appears in the right column of the table is an element of B,
3. every element of A appears in the left side of the table, and
4. no two rows of the table have the same left side, but different right sides.

△

In a similar way to tables, not all sets of ordered pairs represent a function. For instance, if we convert the table in Example 16 into a set of ordered pairs, we get:

$$\{ (\mathsf{apple}, 65), (\mathsf{banana}, 83), (\mathsf{cherry}, 7), (\mathsf{donut}, 99), (\mathsf{banana}, 155) \}.$$

How can we tell that this set of ordered pairs doesn't represent a function? Because the input "banana" has two outputs: 83 and 155 cents.

Suppose we used the set of ordered pairs from Example 16, but we deleted one of the ordered pairs, say the one corresponding to the input donut. Our set then becomes

$$C = \{ (\mathsf{apple}, 65), (\mathsf{banana}, 83), (\mathsf{cherry}, 7), (\mathsf{eggs}, 155) \}.$$

Why would C not represent a function? Bear in mind that the domain is still $A = \{\mathsf{apple}, \mathsf{banana}, \mathsf{cherry}, \mathsf{donut}, \mathsf{eggs}\}$; that is, when I walk into the store, I can still pick up a donut. But when I scan the donut at the register, what price do I pay? Our set of ordered pairs doesn't say. Therefore C is not a function because it doesn't define an output for all possible inputs of A, just as in the beginning of the chapter $g(x) = 1/x$ was not a function from $\mathbb{R}$ to $\mathbb{R}$ because the input 0 had no output in $\mathbb{R}$.

Exercise 18. Let $A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\}$ and $B = \{1, 3, 5, 7, 9\}$. Which of the following sets of ordered pairs represent functions from A to B?

a. $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{d}, 7)\}$

b. $\{(\mathsf{a}, 1), (\mathsf{b}, 2), (\mathsf{c}, 3), (\mathsf{d}, 4)\}$

c. $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{d}, 3)\}$

d. $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{d}, 7), (\mathsf{a}, 9)\}$

e. $\{(\mathsf{a},1),(\mathsf{b},3),(\mathsf{c},5)\}$

f. $\{(\mathsf{a},1),(\mathsf{b},1),(\mathsf{c},1),(\mathsf{d},1)\}$

g. $\{(\mathsf{a},\mathsf{a}),(\mathsf{b},\mathsf{a}),(\mathsf{c},\mathsf{a}),(\mathsf{d},\mathsf{a})\}$

h. $\{(\mathsf{a},1),(\mathsf{b},3),(\mathsf{c},5),(\mathsf{d},5),(\mathsf{e},3)\}$

i. $\{(1,\mathsf{a}),(3,\mathsf{a}),(5,\mathsf{a}),(7,\mathsf{a}),(9,\mathsf{a})\}$

j. $\{(\mathsf{c},1),(\mathsf{b},3),(\mathsf{a},7),(\mathsf{d},9)\}$

k. $A \times B$

◊

Exercise 19. In parts (b) - (k) of Exercise 18, notice that all the sets that correspond to functions are subsets of $A \times B$. Explain why the set of ordered pairs describing a function from A to B must be a subset of $A \times B$. ◊

In summary, a set of ordered pairs C is a function from A to B if and only if :

- $C \subset A \times B$
- each input $a \in A$ is part of an ordered pair in C
- and each input $a \in A$ is paired with only one output $b \in B$.

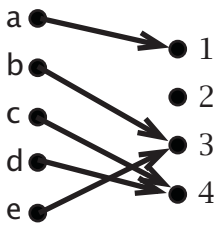
It is sometimes helpful to represent a function $f\colon A \to B$ by drawing an ***arrow diagram***:

- a dot is drawn for each element of A and each element of B, and
- an arrow is drawn from a to $f(a)$, for each $a \in A$.

For example, suppose

- $A = \{\mathsf{a},\mathsf{b},\mathsf{c},\mathsf{d},\mathsf{e}\}$,
- $B = \{1,2,3,4\}$, and
- $f = \{(\mathsf{a},1),(\mathsf{b},3),(\mathsf{c},4),(\mathsf{d},4),(\mathsf{e},3)\}$.

Here is an arrow diagram of f:



Notice that:

1. There is exactly one arrow coming out of each element of A. This is true for the arrow diagram of any function.

2. There can be any number of arrows coming into each element of B (perhaps none, perhaps one, or perhaps many). The elements of B that do have arrows into them are precisely the elements of the range of f. In this example, the range of f is $\{1, 3, 4\}$.

7.2.2 Official definition of functions

The preceding section provided some intuition about how and why functions are represented as sets of ordered pairs, and since ordered pairs are elements created by a Cartesian product, we learned how to view a function from A to B as a particular subset of $A \times B$. This view leads to our official definition of a function:

Definition 20. Suppose A and B are sets.

A set f is a ***function from*** A ***to*** B if

(a) $f \subset A \times B$

(b) $\forall a \in A, \exists$ a unique $b \in B$ s.t. $(a, b) \in f$

(Condition (b) can also be stated as follows: every $a \in A$ is in one and only one ordered pair in f).

We write "$f\colon A \to B$" to denote that f is a function from A to B. We also call A the ***domain*** of f, and B the ***codomain*** of f.

If the pair $(a, b) \in f$, then we say that b is the ***image*** of a under the function f.

△

Notation 21. Suppose $f\colon A \to B$.

1. For $a \in A$, it is convenient to have a name for the element b of B, such that $(a, b) \in f$. The name we use is $f(a)$:

$$f(a) = b \text{ if and only if } (a, b) \in f.$$

2. Each element a of A provides us with an element $f(a)$ of B. The ***range*** of f is the set that includes all of these elements $f(a)$. That is,

$$\text{Range of } f = \{b \in B \text{ such that } \exists a \in A \text{ with } f(a) = b.$$

   The range is always a subset of the codomain. The range can be denoted $\{\, f(a) \mid a \in A \,\}$.

△

Example 22. Suppose that the function f is defined by $f(x) = x^2$, on the domain $\{0, 1, 2, 4\}$. Then

1. to represent f as a set of ordered pairs, each element of the domain must appear exactly once as a first coordinate, with the corresponding output given in the second coordinate. Since there are four elements in the domain, there will be four ordered pairs: $\{(0, 0), (1, 1), (2, 4), (4, 16)\}$;

2. to give a table for f, we include one row for every element of the domain. The table will be:

n	$f(n)$
0	0
1	1
2	4
4	16

3. if we are asked what is $f(3)$, the answer is that $f(3)$ is *undefined*, because 3 is not in the domain of f. Even though we know that $3^2 = 9$, the formula we gave for f only applies to elements that are in the domain of f! It is not true that $f(3) = 9$;

4. the range of f is the set of possible outputs: in this case, $\{0, 1, 4, 16\}$;
5. if we are asked what is $f(2)$, the answer is $f(2) = 4$;
6. is f a function from $\{n \in \mathbb{N} \mid n \leq 4\}$ to $\{0, 1, 4, 16\}$? The answer is no, because the first set is $\{0, 1, 2, 3, 4\}$, which includes the value 3, but 3 is not in the domain of f.
7. is f a function from $\{0, 1, 2, 4\}$ to $\{n \in \mathbb{N} \mid n \leq 16\}$? The answer is yes; even though the second set has many values that are not in the range, it is a possible codomain for f. A codomain can be any set that contains all of the elements of the range.

♦

Exercise 23. The following table describes a certain function g.

n	$g(n)$
2	7
4	9
6	11
8	13
10	15

(a) What is the domain of g?

(b) What is the range of g?

(c) What is $g(6)$?

(d) What is $g(7)$?

(e) Represent g as a set of ordered pairs.

(f) Draw an arrow diagram to represent g.

(g) Write down a formula that describes g.
(Express $g(n)$ in terms of n.)

◊

Exercise 24. Suppose

- f is a function whose domain is $\{0, 2, 4, 6\}$, and
- $f(x) = 4x - 5$, for every x in the domain.

Describe the function in each of the following ways:

(a) Make a table.

(b) Use ordered pairs.

(c) Draw an arrow diagram involving two sets.

$\Diamond$

Exercise 25. Which of the following sets of ordered pairs are functions from $\{\mathsf{x}, \mathsf{y}, \mathsf{z}\}$ to $\{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}\}$?

- If it is such a function, then what is its range?
- If it is not such a function, then explain why not.

(a) $\{(\mathsf{y}, \mathsf{a}), (\mathsf{x}, \mathsf{b}), (\mathsf{y}, \mathsf{c})\}$

(b) $\{(\mathsf{y}, \mathsf{a}), (\mathsf{x}, \mathsf{b}), (\mathsf{z}, \mathsf{c})\}$

(c) $\{(\mathsf{y}, \mathsf{a}), (\mathsf{x}, \mathsf{c}), (\mathsf{z}, \mathsf{a})\}$

$\Diamond$

Exercise 26. Which of the following are functions from $\{1, 2, 3\}$ to $\{\mathsf{w}, \mathsf{h}, \mathsf{o}\}$? (If it is not such a function, then explain why not.)

(a) $\{(1, \mathsf{w}), (1, \mathsf{h}), (1, \mathsf{o})\}$

(b) $\{(1, \mathsf{h}), (2, \mathsf{h}), (3, \mathsf{h})\}$

(c) $\{(1, \mathsf{h}), (2, \mathsf{o}), (3, \mathsf{w})\}$

(d) $\{(\mathsf{w}, 1), (\mathsf{h}, 2), (\mathsf{o}, 3)\}$

$\Diamond$

Exercise 27. For the given sets A and B:

(a) Write each function from A to B as a set of ordered pairs. (It turns out that if $|A| = m$ and $|B| = n$, then the number of functions from A to B is n^m. Do you see why?)

(b) Find the range of each function.

i. $A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$, $B = \{\mathsf{d}\}$

ii. $A = \{\mathsf{a}, \mathsf{b}\}$, $B = \{\mathsf{c}, \mathsf{d}\}$

iii. $A = \{\mathsf{a}\}$, $B = \{\mathsf{b}, \mathsf{c}, \mathsf{d}\}$

iv. $A = \{\mathsf{a}, \mathsf{b}\}$, $B = \{\mathsf{c}, \mathsf{d}, \mathsf{e}\}$

$\Diamond$

7.2.3 Summary of basic function concepts

- A function accepts inputs, and provides a single output for each input.
- The set of allowable inputs is called the domain of the function.
- Some ways of representing functions are:
  - a formula;
  - a table;
  - a set of ordered pairs;
  - an arrow diagram.
- Important definitions:
  - function
  - domain
  - codomain, range
- Notation:
  - $f\colon A \to B$
  - $f(a)$
  - $\{\, f(a) \mid a \in A \,\}$

7.3 One-to-one functions

7.3.1 Concept and definition

We begin this chapter with an example.

Example 28.

- Suppose Inspector Gadget knows two facts:
  1. Alice is the thief's wife, and
  2. Alice is Bob's wife.

  Then the Inspector can arrest Bob for theft, because a woman cannot (legally) be the wife of more than one husband.
- On the other hand, suppose the Inspector knows:
  1. Alice is the forger's mother, and
  2. Alice is Charlie's mother.

  Then the Inspector does not know enough to be sure who the forger is, because it could be some other child of Alice.

This example illustrates a fundamental difference between the wife function and the mother function: two different people can have the same mother, but only one person can have any particular person as their wife. In mathematical terms, this important property of the wife function is expressed by saying that the wife function is "one-to-one." [2] ⧫

Example 29. Now let's revisit the function we saw in Example 13 part (1). Temp is the function from the set of points on the earth to the set of measured temperatures at those points. Is Temp a one-to-one function? Not at all: it is very likely that at any given time, at least two points on earth have the same temperature. [3]

Another way to say this is that at any given time,

there exists a temperature b for which we can find two points on earth x and y such that $\mathsf{Temp}(\mathsf{x}) = \mathsf{Temp}(\mathsf{y}) = \mathsf{b}$.

⧫

Exercise 30. Is the function AtomicNumber from the set of chemical elements to the set of natural numbers a one-to-one function? Explain why or why not. ◊

[2] Some math terms use the word "injective" instead of "one-to-one": the two are synonymous.

[3] It's not only likely: it's a sure thing. This can be proven mathematically, given that Temp is a continuous function. Can you prove it?

Remark 31. If you have an arrow diagram of a function, then it is easy to tell whether or not the function is one-to-one. For example:

1. The function f of 7.1(a) on page 188 is *not* one-to-one. This is because the arrow from b and the arrow from c go to the same place, so $f(\mathsf{b}) = \mathsf{f}(\mathsf{c})$. In general, if arrows from two different elements of the domain go to the same element of the range, then the function is not one-to-one.
2. The function g of 7.1(b) is one-to-one. This is because the arrows from two different elements of the domain never go to the same element of the range. In short, there is only *one* element of the domain that goes *to* any *one* element of the range.

△

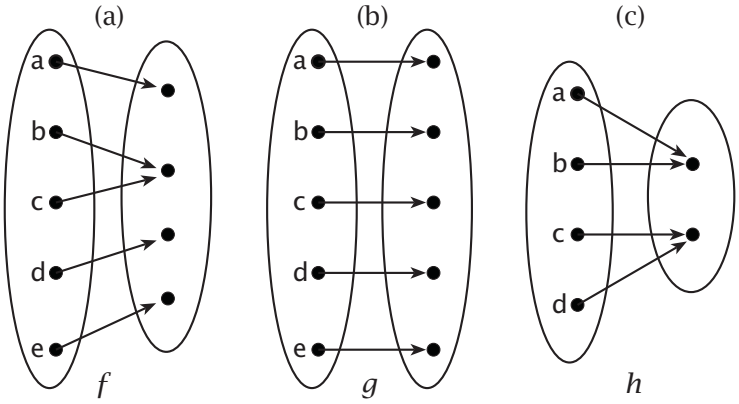


Figure 7.1. Arrow diagrams of three functions f, g, and h.

Exercise 32. Is function h of Figure 7.1 one-to-one? Explain why or why not. ◊

This concept of one-to-one is very useful. If we know A is a function, we know that every input of A has exactly one output. But if we know that A is a one-to-one function, then we also know that every output in the range of A is caused by **exactly** one input. This notion is formalized in the following definition:

Definition 33. Suppose $f\colon A \to B$. We say f is a ***one-to-one function*** iff for all $a_1, a_2 \in A$, such that $f(a_1) = f(a_2)$, we have $a_1 = a_2$. △

Exercise 34.

Each of the following sets of ordered pairs is a function from $\{1, 2, 3, 4\}$ to $\{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}\}$. Either prove that the function is one-to-one, or prove that it is not.

(a) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{d}), (4, \mathsf{e})\}$

(b) $g = \{(1, \mathsf{c}), (2, \mathsf{d}), (3, \mathsf{d}), (4, \mathsf{e})\}$

(c) $h = \{(1, \mathsf{e}), (2, \mathsf{d}), (3, \mathsf{c}), (4, \mathsf{b})\}$

(d) $i = \{(1, \mathsf{e}), (2, \mathsf{e}), (3, \mathsf{e}), (4, \mathsf{e})\}$

(e) $j = \{(1, \mathsf{a}), (2, \mathsf{c}), (3, \mathsf{e}), (4, \mathsf{c})\}$

(f) $k = \{(1, \mathsf{a}), (2, \mathsf{c}), (3, \mathsf{e}), (4, \mathsf{d})\}$

$\Diamond$

7.3.2 Proving that a function is one-to-one

The concept of one-to-one will be very important in this course, and one of the tools we will need is the ability to prove that a function is one-to-one. Though many of the functions we will encounter throughout this book are not algebraic, we will learn this style of proof using algebraic functions, as they are a bit easier to deal with. Here are some examples of this type of proof.

Example 35. Determine which of the following functions are one-to-one. If so, give a proof. If not, give a counterexample.

1. $f\colon \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x + 1$.

   This is one-to-one. The arc of this proof comes directly from the definition of a one-to-one function. I need to pick two different general numbers x and y, set their images equal to each other, and show that in actuality $x = y$.

   So, for any real numbers x and y, $f(x) = f(y)$ means that $x+1 = y+1$. Subtracting 1 from both sides of the equation, we conclude that $x = y$ whenever $f(x) = f(y)$. Hence, f is one-to-one.

2. $g\colon \mathbb{R} \to \mathbb{R}$, defined by $g(x) = |x|$.

   This is not one-to-one. We demonstrate this by finding two distinct real numbers whose image is the same:

   $$g(1) = |1| = 1 = |-1| = g(-1),$$

   but $1 \neq -1$. This shows that g is *not* one-to-one.

3. $f\colon \{1,2,3\} \to \{\mathsf{a},\mathsf{b},\mathsf{c}\}$ defined by $f = \{(1,b),(2,a),(3,a)\}$.

   This is not one-to-one. We demonstrate this by finding two distinct values in $\{1,2,3\}$ whose image is the same:

   $$f(2) = a = f(3),$$

   but $2 \neq 3$. This shows that f is *not* one-to-one.

4. $h\colon \mathbb{N} \to \mathbb{N}$, defined by $h(x) = |x|$.

   This is one-to-one. Since all natural numbers are nonnegative, we have $|x| = x$ for every natural number x. So if $h(x) = h(y)$, then

   $$x = |x| = h(x) = h(y) = |y| = y,$$

   making $x = y$. Hence h is one-to-one.

♦

Remark 36. In your college algebra and calculus classes you may have used the ***horizontal line test*** to get an idea of whether a function was one-to-one. For instance, consider the function $f(x) = x + 1$ from Part 1 of Example 35 above. Figure 7.2 is the graph of f with a horizontal line passing through the function at a particular point.

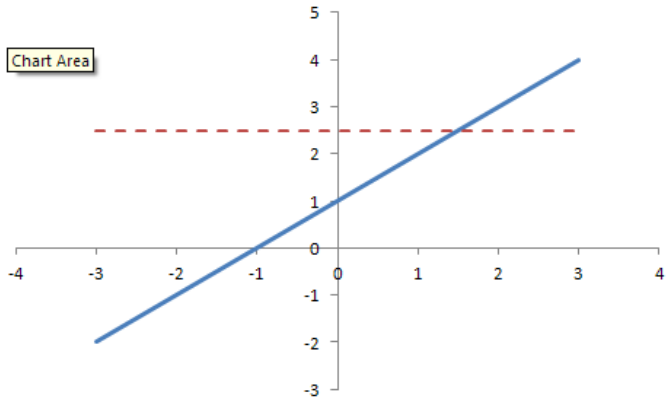


Figure 7.2. Graph of function $f(x) = x + 1$.

Based on the horizontal line test, would f be a one-to-one function? Indeed it seems so, because as we move the horizontal line up and down, it

always passes through at most one point. But how do we know somewhere outside the range of the graph we don't have a y-value in which the horizontal line intersects the graph at more than one point? To prove there isn't such a y-value, we would need either an infinite graph, or an infinite number of graphs to view our infinite domain and range; neither of which is possible. If you remember, in the Modular Arithmetic chapter we had this same problem for using addition and multiplication tables to prove that $\mathbb{Z}_n$ is closed for all $n \in \mathbb{N}$.

So while the horizontal line test *suggests* that f is one-to-one, we would still need the proof in Part 1 of Example 35 to *prove* that it is.

On the other hand, to disprove a function is one-to-one, you only need a single counterexample. Consider the function $g(x) = |x|$ from Part 2 of Example 35, which is graphed in Figure 7.3.

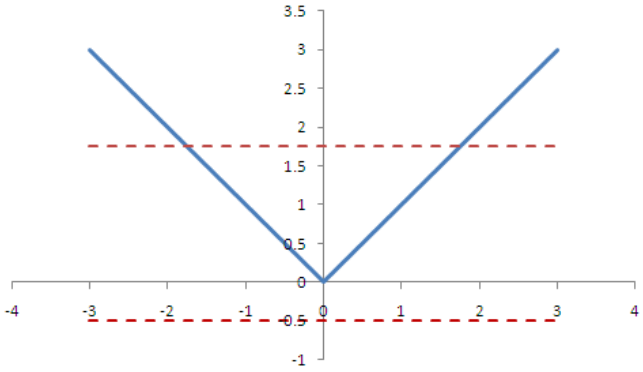


Figure 7.3. Graph of function $f(x) = |x|$.

Using the graph we can easily identify two values in the domain that produce the same value in the codomain. However, while the horizontal line test here suggests our counterexample, we still need to verify that the counterexample works. So again we need the disproof in Part 2 of Example 35, not just a picture.

In summary, the horizontal line test can only *suggest* whether a function is one-to-one or not; you still need proof or disproof. Furthermore, the horizontal line test is usually only a good tool for functions whose domain and codomain are $\mathbb{R}$ (or subsets of $\mathbb{R}$). △

Exercise 37.

Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Either prove the function is one-to-one, or prove that it is not.

(a) $f(x) = 1$.

(b) $g(x) = x$.

(c) $h(x) = x^2$.

(d) $i(x) = 3x + 2$.

(e) $j(x) = 1/\big(|x| + 1\big)$.

$\Diamond$

There is an equivalent way to show functions are one-to-one that is also useful. To see it, recall the wife function from the beginning of the section. The wife function is one-to-one because one woman can't be (legally) married to two different husbands. We can express the same thing in a different way by saying that two different husbands must be married to two different wives. These two statements are ***contrapositives*** of each other, and are in fact equivalent. ("contrapositive" is a logical term–you may have run across it before in a Discrete Math class.)

If we generalize this reasoning to arbitrary one-to-one functions, we have the following two equivalent statements:

- A function is one-to-one iff any element of the range is mapped from only one element of the domain;
- A function is one-to-one iff two different elements of the domain always map to two different elements of the range.

We formalize this equivalence in the following alternative definition of one-to-one:

Definition 38. *(Alternate)* Suppose $f\colon A \to B$. We say f is a ***one-to-one function*** iff for all $a_1, a_2 \in A$, such that $a_1 \neq a_2$, we have $f(a_1) \neq f(a_2)$. $\triangle$

When you don't know whether or not a particular function is one-to-one, a good strategy is to try to prove that it's one-to-one. If the proof works, great! – we are done. If the proof fails, the manner in which it fails may indicate an example to show that the function is not one-to-one. Here is an example of this technique.

Example 39. Let $f\colon \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = (n-2)^2 + 1$. Is f one-to-one?

First let's try to prove that f is one-to-one. Start with arbitrary elements $m, n \in \mathbb{N}$, and suppose that $f(m) = f(n)$. By the definition of f, this means that $(m-2)^2+1 = (n-2)^2+1$, or $(m-2)^2 = (n-2)^2$. Two numbers have the same square, if and only if they are equal in absolute value, so it follows that $m-2 = \pm(n-2)$. There are now two cases:

- If $m-2 = +(n-2)$ then adding 1 to each side, we get $m = n$.
- If $m-2 = -(n-2) = -n+2$, then adding 1 to each side, we get $m = -n+4$.

Since $m, n \in \mathbb{N}$, it's not hard to see that if $n \geq 4$, then $-n+4$ is not a natural number. But if n is 1,2,3 then $-n+4 \in \mathbb{N}$. For example $n = 1$ gives $m = 3$, which suggests that $f(1) = f(3)$. We may indeed check that $f(1) = f(3)$.

Now the great thing about cases where f is not one-to-one is, the writeup of the solution is very simple. All you have to do is give one example of two different values that return the same function value. In the current example we have:

Solution f is *not* one-to-one because $f(1) = 2$ and $f(3) = 2$. ◊

So the writeup is easy: two values is all it takes. The hard thing is finding the two values! ⧫

Exercise 40. For each function, either prove that it is one-to-one, or prove that it is not.

(a) $f\colon \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = 3x/5 - 2$.

(b) $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$.

(c) $g\colon \mathbb{R} \to \mathbb{R}$ defined by $g(x) = |(x+1)/2|$.

(d) $g\colon \mathbb{Z}_6 \to \mathbb{Z}_6$ defined by $g(x) = x \oplus 2$.

(e) $g\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ defined by $g(x) = x \odot 2$.

(f) $g\colon \mathbb{Z}_{11} \to \mathbb{Z}_{11}$ defined by $g(x) = x \odot 2$.

(g) $g\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ defined by $g(x) = x \odot x$.

(h) $g\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ defined by $g(x) = x \odot x \odot x$.

(i) $g\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ defined by $g(x) = x \odot x \odot x$.

(j) $g\colon \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ defined by $g(z) = z^{-1}$.

$\Diamond$

7.4 Onto functions

7.4.1 Concept and definition

In an arrow diagram of a function $f\colon A \to B$, the definition of a function requires that there is exactly one arrow out of each element of A, but it says nothing about the number of arrows into each element of B. There may be elements of B with lots of arrows into them (unless the function is one-to-one), and there may be other elements of B that have no arrows into them. The function is called "onto" [4] if all of the elements of B are hit by arrows; none are missed.

Example 41. Figure 7.4 shows arrow diagrams of various functions, some onto and some not. In Figure 7.4,

- f is onto, but not one-to-one.
- g is both one-to-one and onto.
- h is neither one-to-one nor onto.
- i is one-to-one, but not onto.

$\blacklozenge$

[4] Some math terms use the word "surjective" instead of "onto": the two are synonymous.

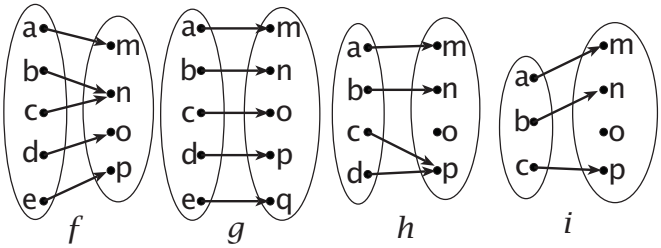


Figure 7.4. Arrow diagrams for various functions

Example 42. Not every woman is a mother. This means that if you draw an arrow from each person to his or her mother, there will be some women who have no arrows into them. So the function

$$\mathsf{mother}\colon \mathsf{People} \to \mathsf{Women}$$

is *not* onto. ⧫

Exercise 43. Is the function $\mathsf{AtomicNumber}\colon \{$ Chemical Elements $\} \to \mathbb{N}$ onto? Explain why or why not. ◊

The following is the "official" definition of onto.

Definition 44. Suppose $f\colon A \to B$. We say f is ***onto*** if for all $b \in B$, there is some $a \in A$, such that $f(a) = b$. △

In words: if I pick any value in the codomain of f, there is some value in the domain that produces it.

Exercise 45. If the function f is onto, then what is the relation between the range of f and the codomain of f? (*Hint*) ◊

7.4.2 Proving that a function is onto

The following examples show how to prove that a function is onto.

Example 46.

- Consider the function:

  $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x + 1$.

  Recall that a function is onto if for every value in the codomain, there is a value in the domain that produces it. So pick an arbitrary value in the codomain $\mathbb{R}$ and call it y. By the definition of our function f, $f(x) = y$ means that $x + 1 = y$. Solving for x gives $x = y - 1$. Now x is also a real number (by closure of $\mathbb{R}$ under $-$): so we have found an x in the domain of f such that $f(x) = y$. Therefore f is onto.

- Consider the function $h\colon \mathbb{N} \to \mathbb{N}$, defined by $h(x) = |x|$.

  Since all natural numbers are nonnegative, we have $h(x) = |x| = x$ for every natural number x. So for an arbitrary value y in the codomain $\mathbb{N}$, we have $h(y) = y$ (note y is also in the domain of h). Therefore h is onto.

♦

It is typically easier to prove that a function is *not* onto. All you have to do is provide a counterexample:

Example 47.

- Consider the function $f\colon \{1, 2, 3\} \to \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$ defined by $f = \{(1, \mathsf{b}), (2, \mathsf{a}), (3, \mathsf{a})\}$. Notice that c never appears as an image in this function. This shows that f is not onto.

- Consider the function $g\colon \mathbb{R} \to \mathbb{R}$ defined by $g(x) = |x|$. To show that g is not onto, we only need to find a single number y in the codomain that is not mapped onto. $y = -1$ is one example: we can never have $|x| = -1$ for any real number x. This shows that g is not onto.

- Consider the function $h\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $h(x) = x \odot x$. We may list the values of $h(x)$ for $x = 0, 1, 2, 3, 4$: they are $0, 1, 4, 4, 1$ respectively. There is no x such that $h(x) = 3$, so h is not onto.

♦

Since "onto" proofs require working backwards, sometimes some preliminary scratchwork is required before writing out the actual proof.

Example 48. Define $g\colon \mathbb{R} \to \mathbb{R}$ by $g(x) = 5x - 2$. Show g is onto.

Just as in the previous examples, given any $y \in \mathbb{R}$ we need to find a value of x that makes $g(x) = y$. So we start with the equation $g(x) = y$ and solve for x:

$$\begin{aligned} g(x) = y &\Rightarrow 5x - 2 = y && \text{[by substitution]} \\ &\Rightarrow x = \frac{y+2}{5} && \text{[solve for } x \text{ using basic algebra]} \end{aligned}$$

Now that we have x, lets do our proof.

PROOF. Given $y \in \mathbb{R}$, let $x = (y+2)/5$. Since the reals are closed under addition and non-zero division, it follows that $x \in \mathbb{R}$. Then

$$g(x) = 5x - 2 = 5\left(\frac{y+2}{5}\right) - 2 = (y+2) - 2 = y.$$

Therefore g is onto. □

Although you need the scratchwork to come up with the formula for x, you don't need to include the scratchwork in your proof. It's actually much cleaner without it. ♦

Remark 49. In your college algebra and calculus classes you may have used the horizontal line test to show whether a function was onto. For instance, recall the function $f(x) = x + 1$ shown in Figure 7.2. is the graph of f with a horizontal line passing through the function at a particular point. Based on the horizontal line test, would f be a onto function? What we're looking for is whether or not each horizontal line intersects the graph in *at least* one point. The figure suggests this is true, but to prove it for *all* horizontal lines we would need an infinite graph. So again, the horizontal line test *suggests* that f is onto, but we still need the proof in Part 1 of Example 46 to *prove* that it is.

On the other hand, to disprove a function is onto, you only need a counterexample. Consider the function $g(x) = |x|$ shown in Figure 7.3. Using the graph, we can easily find a horizontal line that doesn't intersect the graph: this corresponds to a value in $\mathbb{R}$ that is not in the range of g. But while the horizontal line test here suggests a counterexample to show g is not onto, we still need to verify that it works. △

Exercise 50. Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Either prove that the function is onto, or prove that it is not.

(a) $a(x) = 1$.

(b) $b(x) = x$.

(c) $c(x) = x^2$.

(d) $d(x) = 3x + 2$.

(e) $e(x) = 1/\big(|x| + 1\big)$.

(f) $f(x) = 4x - 6$.

(g) $g(x) = \sqrt[3]{x + 5} - 5$.

$\Diamond$

Exercise 51. Each of the following sets of ordered pairs is a function from $\{1, 2, 3, 4, 5\}$ to $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$. Either prove that the function is onto, or prove that it is not.

(a) $a = \{(1, \clubsuit), (2, \diamondsuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$

(b) $b = \{(1, \clubsuit), (2, \heartsuit), (3, \clubsuit), (4, \heartsuit), (5, \clubsuit)\}$

(c) $c = \{(1, \heartsuit), (2, \heartsuit), (3, \heartsuit), (4, \heartsuit), (5, \heartsuit)\}$

(d) $d = \{(1, \diamondsuit), (2, \spadesuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$

(e) $e = \{(1, \clubsuit), (2, \spadesuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$

$\Diamond$

Exercise 52. For each of the following functions, either prove that it is onto, or prove that it is not.

(a) $g\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $g(x) = (x \odot 2) \oplus 3$.

(b) $g\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ defined by $g(x) = (x \odot x) \oplus 1$.

(c) $g\colon \mathbb{Z}_9 \to \mathbb{Z}_9$ defined by $g(x) = x \odot x \odot x$.

(d) $g\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ defined by $g(x) = x \odot x \odot x$.

(e) $g\colon \mathbb{C} \setminus \{1\} \to \mathbb{C} \setminus \{0\}$ defined by $g(z) = \frac{1}{z-1}$.

$\Diamond$

When a function is defined *piecewise*, the one-to-one and onto proofs are a little harder:

Example 53.

For instance, consider the function f from $\mathbb{R}$ to $\mathbb{R}$ defined by:

$$f(x) = \begin{cases} e^x & \text{if } x > 0 \\ 1 - x^2 & \text{if } x \leq 0 \end{cases}$$

If you graph this function, you wil find that the horizontal line tests suggest $f(x)$ is indeed one-to-one and onto. To complete the actual proof, we need to prove four separate statements:

(a) If $y > 1$, there exists a unique $x > 0$ such that $e^x = y$.

(b) If $y \leq 1$, there exists a unique $x \leq 0$ such that $1 - x^2 = y$.

From these two facts, it follows that $f(x)$ is onto, because for any y (whether > 1 or ≤ 1) there exists an x such that $f(x) = y$.

To show that $f(x)$ is one-to-one, we will need two additional statements:

(c) If $y > 1$, there exists no $x \leq 0$ such that $1 - x^2 = y$.

(d) If $y \leq 1$, there exists a unique $x \leq 0$ such that $1 - x^2 = y$.

From these two facts (together with (a) and (b)) we find that for any y (whether > 1 or ≤ 1) there is *exactly* one x such that $f(x) = y$. ♦

Exercise 54. Prove statements (a)−(d) in Example 53. For example, you can prove (a) as follows. Given $y > 1$, setting $x = \ln(y)$ gives $e^x = y$; furthermore if $x > \ln(y)$ (respectively $x < \ln(y)$) then $e^x > y$ (respectively $e^x < y$). ◊

Exercise 55. Define function f from $\mathbb{R}$ to $\mathbb{R}$ by:

$$f(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x + 1 & \text{if } x \leq 0. \end{cases}$$

Prove or disprove:

(a) f is onto; (b) f is one-to-one;

$\Diamond$

Exercise 56. Define function g from $\mathbb{R}$ to $\mathbb{R}$ by:

$$g(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x - 1 & \text{if } x \leq 0. \end{cases}$$

Prove or disprove:

(a) g is onto; (b) g is one-to-one.

$\Diamond$

Exercise 57. Define function h from $\mathbb{R}$ to $\mathbb{R}$ by:

$$h(x) = \begin{cases} x^3 & \text{if } |x| > 1 \\ x^{1/3} & \text{if } |x| \leq 1. \end{cases}$$

Prove or disprove:

(a) h is onto; (b) h is one-to-one.

$\Diamond$

7.5 Bijections

7.5.1 Concept and definition

Some "especially nice" functions are both one-to-one and onto.

Definition 58. A function is a ***bijection*** if and only if it is both one-to-one and onto. $\triangle$

In words, a bijection has the following properties:

- All inputs have only one output (function)
- All outputs are paired with only one input (one-to-one)
- And all possible outputs of the codomain are paired (onto)

Example 59. Consider a hypothetical country Married, in which

- everyone is married (to only one person — there is no polygamy), and
- every marriage is between a man and a woman (there are no same-sex marriages).

Let Men = {men in the country}, and Women = {women in the country}. Then wife: Men $\to$ Women is a bijection, since:

- Two different men cannot have the same wife, so we know that wife is one-to-one.
- Every woman is the wife of some man (because everyone is married), so wife is also onto.

Similarly, the function husband: Women $\to$ Men is also a bijection. ⧫

Remark 60. In the country Married described above, it is clear that the number of men is exactly equal to the number of women. (If there were more men than women, then not every man could have a wife; if there were more women than men, then not every women could have a husband.) This is an example of the following important principle:

If A and B are finite sets, and there exists a bijection from A to B, then A and B have the same number of elements.

Finding a bijection is one way to show two sets have the same number of elements. △

Exercise 61. Draw an arrow diagram of a bijection. ◊

Exercise 62. Is the function AtomicNumber: { Chemical elements } $\to \mathbb{N}$ a bijection? Justify your answer. ◊

7.5.2 Proving that a function is a bijection

Since a bijection is both one-to-one and onto, a proof that a function is a bijection (usually) has two parts:

1. Show that the function is one-to-one.
2. Show that the function is onto.

The two parts can come in either order: it is perfectly acceptable to first prove that the function is onto, and then prove that it is one-to-one.

How would you show that function is not a bijection? You guessed it, by counterexample. You only need a counterexample that shows either the function is not onto, or is not one-to-one, because a bijection requires both.

Example 63. Define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = 5x - 7$. Then f is a bijection.

PROOF. It suffices to show that f is both one-to-one and onto:

- *(one-to-one)* Given $x_1, x_2 \in \mathbb{R}$, such that $f(x_1) = f(x_2)$, we have

  $$5x_1 - 7 = 5x_2 - 7.$$

  Adding 7 to both sides and dividing by 5, we have

  $$\frac{(5x_1 - 7) + 7}{5} = \frac{(5x_2 - 7) + 7}{5},$$

  Which implies $x_1 = x_2$. So f is one-to-one.

- *(onto)* Given $y \in \mathbb{R}$, let $x = (y + 7)/5$. Then

  $$f(x) = 5x - 7 = 5\left(\frac{y+7}{5}\right) - 7 = (y + 7) - 7 = y,$$

  So f is onto.

  Since f is both one-to-one and onto, we conclude that f is a bijection.

□ ♦

Exercise 64. Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Either prove the function is a bijection, or prove that it is not.

(a) $a(x) = 5x + 2$

(b) $b(x) = 2x - 5$

(c) $c(x) = 12x - 15$

(d) $d(x) = -15x - 12$

(e) $e(x) = x^3$

(f) $f(x) = \sqrt[3]{x - 4}$

(g) $a(x) = 1$.

(h) $b(x) = x$.

(i) $c(x) = x^2$.

(j) $d(x) = 3x + 2$.

(k) $e(x) = 1/\big(|x| + 1\big)$.

(l) $f(x) = 4x - 6$.

(m) $g(x) = \sqrt[3]{x} - 5$.

(n) $h(x) = \sqrt{x^2 + 1}$

$\Diamond$

Exercise 65. Let $a, b \in \mathbb{R}$, and define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$.

(a) Show that if $a \neq 0$, then f is a bijection.

(b) Show that if $a = 0$, then f is *not* a bijection.

$\Diamond$

Exercise 66. For each function, either prove that it is a bijection, or prove that it is not.

(a) $g\colon \mathbb{Z}_9 \to \mathbb{Z}_9$ defined by $g(x) = (x \odot 3) \oplus 3$.

(b) $g\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ defined by $g(x) = (x \odot 4) \oplus 4$.

(c) $g\colon \mathbb{Z}_{11} \to \mathbb{Z}_{11}$ defined by $g(x) = x \odot 2$.

(d) $g\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ defined by $g(x) = x \odot x$.

(e) $g\colon \mathbb{Z}_8 \to \mathbb{Z}_8$ defined by $g(x) = x \odot x \odot x$.

(f) $h\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $h(x) = (3 \odot x \odot x \odot x) \oplus 2$.

(g) $h\colon \mathbb{C} \setminus \{-3\} \to \mathbb{C} \setminus \{0\}$ defined by $h(z) = \dfrac{1}{z + 3}$.

◊

Exercise 67. Define $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(m,n) = m^2 + n - 1$.

(a) Show that f is onto. (*Hint*)

(b) Show that f is *not* one-to-one. (*Hint*)

(c) Is f a bijection?

◊

Exercise 68. Define $g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $g(m,n) = (m+n, m+2n)$.

(a) Show that g is onto. (*Hint*)

(b) Show that g is one-to-one. (*Hint*)

(c) Is g a bijection?

◊

Exercise 69. Define $g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $g(m,n) = (m+n, m-n)$.

(a) *Show that g is *not* onto.

(b) Show that g is one-to-one.

(c) Is g a bijection?

◊

Exercise 70. Suppose A, B, and C are sets. Define

$$f\colon (A \times B) \times C \to A \times (B \times C) \quad \text{by} \quad f\big((a,b),c\big) = \big(a,(b,c)\big).$$

Show that f is a bijection. ◊

7.6 Composition of functions

7.6.1 Concept and definition

The term "composition" is a name that mathematicians use for applying one function to the result of another. Actually, this comes up fairly often in everyday life.

Example 71.

1. The father of the mother of a person is the grandfather the person. (To be precise, it is the *maternal* grandfather of the person — and his or her other grandfather is *paternal*.) To express the relationship in a mathematical formula, we can write:

$$\forall x, \Big(\mathsf{grandfather}(\mathsf{x}) = \mathsf{father}\big(\mathsf{mother}(\mathsf{x})\big)\Big).$$

   A mathematician abbreviates this formula by writing

$$\mathsf{grandfather} = \mathsf{father} \circ \mathsf{mother}$$

   and says that the (maternal) grandfather function is the *composition* of father and mother.

2. The brother of the mother of a person is an uncle of the person, so uncle is the composition of brother and mother:

$$\forall x, \Big(\mathsf{uncle}(\mathsf{x}) = \mathsf{brother}\big(\mathsf{mother}(\mathsf{x})\big)\Big),$$

   or, more briefly,

$$\mathsf{uncle} = \mathsf{brother} \circ \mathsf{mother}.$$

   (For the sake of this example, let us ignore the issue that uncle and brother are not functions in general.)

3. The daughter of a child is a granddaughter, so granddaughter is a composition of daughter and child:

$$\mathsf{granddaughter} = \mathsf{daughter} \circ \mathsf{child}.$$

♦

Exercise 72. State the usual name for each composition. (Ignore the fact that sister, daughter, and many of the other relations are not functions in general.)

(a) husband ∘ sister

(b) husband ∘ mother

(c) husband ∘ wife

(d) husband ∘ daughter

(e) mother ∘ sister

(f) daughter ∘ sister

(g) parent ∘ parent

(h) child ∘ child

(i) parent ∘ parent ∘ parent

(j) child ∘ brother ∘ parent

◊

Definition 73. Suppose $f\colon A \to B$ and $g\colon B \to C$. The ***composition*** of g and f (denoted $g \circ f$) is the function from A to C defined by

$$(g \circ f)(a) = g\big(f(a)\big) \text{ for all } a \in A.$$

△

The notation $g \circ f$ is read as "g compose f" or "g composed with f." Since $g \circ f(a) = g\big(f(a)\big)$, the notation $g \circ f(a)$ is sometimes read as "g of f of a."

Example 74. Define $f\colon \mathbb{R} \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = 3x$ and $g(x) = x^2$. Then $g \circ f$ and $f \circ g$ are functions from $\mathbb{R}$ to $\mathbb{R}$. For all $x \in \mathbb{R}$, we have

$$(g \circ f)(x) = g\big(f(x)\big) = g(3x) = (3x)^2 = 9x^2$$

and

$$(f \circ g)(x) = f\big(g(x)\big) = f(x^2) = 3(x^2) = 3x^2.$$

Notice that (in this example) $f \circ g \neq g \circ f$, so *composition is not commutative.*
♦

Warning To calculate the value of the function $g \circ f$ at the point a, do *not* begin by calculating $g(a)$. Instead, you need to calculate $f(a)$. Then plug that value into the function g. ◊

Exercise 75. Fill in the blanks of the following proof to show that function composition is associative.

PROOF. Suppose $f : X \to Y$, $g : Y \to W$, and $h : W \to Z$. Now suppose $x \in X$, $y \in Y$, $w \in W$, and $z \in Z$ such that

- $f(x) = y$;
- $g(y) = w$;
- $h(w) = z$.

Then

$$(h \circ (g \circ f))(x) = h \circ (g(\_\_\_\_\_)) = h(g(\_\_\_\_\_)) = h(g(\_\_\_\_)) = h(\_\_\_\_) = \_\_\_\_$$

and

$$((h \circ g) \circ f)(x) = (h \circ g)(\_\_\_\_\_) = h(g(\_\_\_\_\_)) = h(g(\_\_\_\_)) = h(\_\_\_\_) = \_\_\_\_$$

Hence $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$; in other words function composition is associative. □ ◊

Example 76. Figure 7.5 provides an arrow diagram to illustrate the composition $g \circ f$.

- Starting from any point of A, follow the arrow (for the function f that starts there to arrive at some point of B.
- Then follow the arrow (for the function g) that starts there to arrive at a point of C.

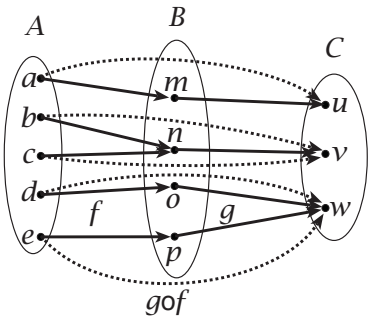


Figure 7.5. Arrows for the composition $g \circ f$ are dotted.

For example, the f-arrow from a leads to m and the g-arrow from m leads to u. So $(g \circ f)(a) = u$. Notice how we write the result as $g \circ f$ with g on the left and f on the right even though f appears on the left in Figure 7.5. This is an unfortunate consequence of the fact that when we calculate $g\big(f(x)\big)$ we work right to left, computing $f(x)$ first and applying g to the result. ♦

Note that in the definition of $g \circ f$ (Definition 73), the domain of $g : B \to C$ is required to be equal to the codomain of $f : A \to B$. Actually $g \circ f$ can be defined as long as the domain of g *contains* the specified codomain of f. This is true because the codomain of a function is not unique: if $f : A \to D$ and $D \subset B$, then B is also a valid codomain of f. The reason for the requirement on the domain of g is further explored in the following exercise.

Exercise 77. Let $f\colon \mathbb{N} \to \mathbb{Z}_5$ defined by $f(n) \equiv n \pmod 5$. Let $g\colon \mathbb{R} \to \mathbb{R}$ defined by:

$$g(x) = x^2.$$

(a) Is it possible to define $f \circ g$? *Explain* your answer.

(b) Is it possible to define $g \circ f$? *Explain* your answer.

◊

Exercise 78. The formulas define functions f and g from $\mathbb{R}$ to $\mathbb{R}$. Find formulas for $(f \circ g)(x)$ and $(g \circ f)(x)$.

(a) $f(x) = 3x + 1$ and $g(x) = x^2 + 2$

(b) $f(x) = 3x + 1$ and $g(x) = (x - 1)/3$

(c) $f(x) = ax + b$ and $g(x) = cx + d$ (where $a, b, c, d \in \mathbb{R}$)

(d) $f(x) = |x|$ and $g(x) = x^2$

(e) $f(x) = |x|$ and $g(x) = -x$

$\Diamond$

Exercise 79. Let $A = \{1, 2, 3, 4\}$, $B = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\}$, and $C = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$. The sets of ordered pairs in each part are functions $f\colon A \to B$ and $g\colon B \to C$. Represent $g \circ f$ as a set of ordered pairs.

(a) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{c}), (4, \mathsf{d})\}$,
$g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \diamondsuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \spadesuit)\}$

(b) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{c}), (4, \mathsf{d})\}$,
$g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \clubsuit), (\mathsf{c}, \clubsuit), (\mathsf{d}, \clubsuit)\}$

(c) $f = \{(1, \mathsf{b}), (2, \mathsf{c}), (3, \mathsf{d}), (4, \mathsf{a})\}$,
$g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \spadesuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \diamondsuit)\}$

(d) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{c}), (4, \mathsf{d})\}$,
$g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \clubsuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \spadesuit)\}$

(e) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{a}), (4, \mathsf{b})\}$,
$g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \clubsuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \spadesuit)\}$

$\Diamond$

7.6.2 Proofs involving function composition

The properties of $f \circ g$ depend on the properties of f and g, and vice versa. Usually these properties are proven by using the definition of composition,

along with the definitions of other functional properties. Here is one example.

Example 80. Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if

$$(g \circ f)(a) = a, \text{ for every } a \in A,$$

then f is one-to-one.

We want to show that f is one-to-one; that is if $f(a_1) = f(a_2)$, then $a_1 = a_2$. We are given that $(g \circ f)(a) = a$, for every $a \in A$. Therefore for our proof we should assume $f(a_1) = f(a_2)$, and use the given statement to somehow get to $a_1 = a_2$.

PROOF. Given that $(g \circ f)(a) = a$, for every $a \in A$, by the definition of composition, this means that, for any $a_1, a_2 \in A$ we have

$$g\big(f(a_1)\big) = a_1 \text{ and } g\big(f(a_2)\big) = a_2.$$

Now suppose $f(a_1) = f(a_2)$. Then by the definition of a function,

$$g\big(f(a_1)\big) = g\big(f(a_2)\big)$$

By our original hypothesis we then get $a_1 = a_2$, and thus f is one-to-one. □ ♦

Example 81. Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if f and g are onto, then $g \circ f$ is onto.

PROOF. Let c be an arbitrary element of C. Since g is onto, there exists a b in B such that $g(b) = c$. Since f is onto, there exists a a in A such that $f(a) = b$. It follows that $g \circ f(a) = g(f(a)) = g(b) = c$. Since c is an arbitrary element of C, this implies that $g \circ f$ is onto. □ ♦

Example 82. Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is one-to-one, and the range of f is B, then g is one-to-one.

PROOF. Suppose b_1 and b_2 are distinct elements of B. Since the range of f is B, it follows that there exist $a_1 \neq a_2$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. Since $g \circ f$ is one-to-one, it follows that $g \circ f(a_1) \neq g \circ f(a_2)$. But by definition of $\circ$, $g \circ f(a_1) = g(f(a_1)) = g(b_1)$; and similarly $g \circ f(a_2) = g(b_2)$. By substitution, it follows that $g(b_1) \neq g(b_2)$. Thus distinct elements of B

always map to distinct elements of C under the function g: which is the same as saying that g is one-to-one.

An alternative proof runs as follows. Let $c \in C$ be such that $c = g(b_1)$ and $c = g(b_2)$. Then since the range of f is B, there exist a_1 and a_2 such that $f(a_1) = b_1$ and $f(a_2) = b_2$. It follows by substitution that $g(f(a_1)) = g(f(a_2))$. But this is the same as saying that $g \circ f(a_1) = g \circ f(a_2)$. Since $g \circ f$ is one-to-one, it follows that $a_1 = a_2$. Applying f to both sides of this equation gives $f(a_1) = f(a_2)$, or $b_1 = b_2$. We have shown that for any $c \in C$, there is at most one $b \in B$ such that $g(b) = c$. This means that g is one-to-one. □ ⧫

Exercise 83.

(a) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if f and g are one-to-one, then $g \circ f$ is one-to-one.

(b) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is one-to-one, then f is one-to-one.

(c) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is onto, then g is onto.

(d) Give an example of functions $f\colon A \to B$ and $g\colon B \to C$, such that $g \circ f$ is onto, but f is not onto.

(e) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is onto, and g is one-to-one, then f is onto.

(f) Define $f\colon [0, \infty) \to \mathbb{R}$ by $f(x) = x$. Find a function $g\colon \mathbb{R} \to \mathbb{R}$ such that $g \circ f$ is one-to-one, but g is *not* one-to-one.

(g) Suppose f and g are functions from A to A. If $f(a) = a$ for every $a \in A$, then what are $f \circ g$ and $g \circ f$?

◊

The preceding exercises and examples can be used to prove the following:

Exercise 84. Suppose $f\colon A \to B$ and $g\colon B \to C$.

(a) Show that if f and g are bijections, then $g \circ f$ is a bijection. (*Hint*)

(b) Show that if f and $g \circ f$ are bijections, then g is a bijection.

(c) Show that if g and $g \circ f$ are bijections, then f is a bijection.

$\Diamond$

Exercise 85. Suppose

- $f\colon A \to B$,
- $g\colon B \to A$,
- $(g \circ f)(a) = a$, for every $a \in A$, and
- $(f \circ g)(b) = b$, for every $b \in B$.

Show that f is a bijection. $\Diamond$

7.7 Inverse functions

7.7.1 Concept and definition

The word "inverse" commonly means something that is "backwards" or "opposite" to something else. So an inverse of a function should be a function that is somehow backwards or opposite to the original function. You have actually seen inverse functions many times before, perhaps without realizing it.

Example 86. In Example 63, it was shown that $f(x) = 5x-7$ is a bijection. A quick look at the proof reveals that the formula

$$x = \frac{y+7}{5}$$

plays a key role. This formula is obtained by replacing $f(x)$ in $f(x) = 5x-7$ with y, and solving for x.

In order to see $x = \frac{y+7}{5}$ as an "inverse function," we translate into the language of functions, by defining $g\colon \mathbb{R} \to \mathbb{R}$ by $g(y) = (y+7)/5$. Then the above assertion can be restated as:

$$y = f(x) \qquad \Leftrightarrow \qquad x = g(y).$$

This tells us that g does exactly the opposite of what f does: if f takes x to y, then g takes y to x. We will say that g is an "inverse" of f. ♦

The following proof provides a restatement of this result that will be used in the official definition of inverse functions. I will prove part (a); you will prove part (b).

Example 87. Suppose that $f\colon X \to Y$ and $g\colon Y \to X$ are functions such that

$$\forall x \in X, \forall y \in Y, \big(y = f(x) \Leftrightarrow x = g(y)\big).$$

Then the following statements are also true:

(a) $f\big(g(y)\big) = y$ for all $y \in Y$, and

(b) $g\big(f(x)\big) = x$ for all $x \in X$.

Proof.

(a) For any $y \in Y$, from the above statement we know two things:

$$\exists x \in X \text{ s.t. } g(y) = x$$

and

$$\text{for that particular } x, f(x) = y$$

Therefore,

$$f\big(g(y)\big) = f(x) = y, \forall y \in Y$$

□

Exercise 88. Prove part (b) of Example 87. ◊

♦

Finally, we can give the definition of an inverse function:

Definition 89. Suppose

- $f\colon X \to Y$, and
- $g\colon Y \to X$,

We say that g is an ***inverse*** of f if and only if:

a. $f\big(g(y)\big) = y$ for all $y \in Y$, and

b. $g\big(f(x)\big) = x$ for all $x \in X$.

△

Example 90. The husband of the wife of any married man is the man himself – in other words,

$$\mathsf{husband}\big(\mathsf{wife}(\mathsf{y})\big) = \mathsf{y}.$$

Also, the wife of the husband of any married woman is the woman herself, so that

$$\mathsf{wife}\big(\mathsf{husband}(\mathsf{x})\big) = \mathsf{x}.$$

It follows that the wife function is an inverse of the husband function. In fact, it's pretty clear that husband is the *only* inverse of wife. ♦

Exercise 91. In each case, use Definition 89 to determine whether g is an inverse of f.

(a) $f\colon \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = 9x - 6$ and
$g\colon \mathbb{R} \to \mathbb{R}$ is defined by $g(x) = (x + 6)/9$.

(b) $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $f(x) = 2x^2$ and
$g\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $g(x) = \sqrt{x}/2$.

(c) $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $f(x) = 2/x$ and
$g\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $g(x) = 2/x$.

(d) $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $f(x) = \sqrt{x+1} - 1$ and
$g\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $g(x) = x^2 + 2x$.

◊

7.7.2 Which functions have inverses?

It turns out that most functions do *not* have inverses.

Exercise 92. Which of the functions depicted in Figure 7.4 have inverses? ◊

From the previous exercise, you may have guessed the following rule:

Proposition 93. Suppose $f\colon X \to Y$. Then f has an inverse $g\colon Y \to X$ if and only if f is a bijection.

This is another "if and only if" proof, so it must be proved in both directions. We will prove the forward direction of this proposition. You will prove the reverse direction.

The forward direction of Proposition 93 says that if $f\colon X \to Y$ has an inverse $g\colon Y \to X$, then f is a bijection. In other words we must assume the first statement, and from that prove that f is one-to-one and onto.

PROOF. *(forward direction)* Assume there is a function $g\colon Y \to X$ that is an inverse of f. Then by the definition of an inverse function,

(a) $f\big(g(y)\big) = y$ for all $y \in Y$, and

(b) $g\big(f(x)\big) = x$ for all $x \in X$.

Suppose then that $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X$. Then since g is a function we have

$$g\big(f(x_1)\big) = g\big(f(x_2)\big)$$

Therefore by (b), $x_1 = x_2$. Hence f is one-to-one.

Now suppose $y_1 \in Y$. Then since g is a function, there exists a unique $x_1 \in X$ such that $g(y_1) = x_1$. Substituting into (a) we get

$$f\big(x_1\big) = y_1.$$

Therefore $\forall y \in Y, \exists x \in X$ s.t. $f(x) = y$. Hence f is onto. So f is both one-to-one and onto: thus f is a bijection. □

Exercise 94. Prove the reverse direction of Proposition 93. ◊

Exercise 95.

(a) Prove that any inverse of a bijection is a bijection.

(b) Show that the inverse of a function is *unique*: if g_1 and g_2 are inverses of f, then $g_1 = g_2$.

$\Diamond$

Remark 96.

(a) Exercise 95 is key because it enables us to talk about *the* inverse of a function, since there is at most one. We will use the special notation f^{-1} to denote the inverse of the function f.

(b) If f is a function that has an inverse, then it is easy to find f^{-1} as a set of ordered pairs. Namely,

$$f^{-1} = \{\, (y, x) \mid (x, y) \in f \,\}.$$

This is simply a restatement of the fact that

$$y = f(x) \Leftrightarrow x = f^{-1}(y).$$

$\triangle$

Definition 97. For any set A, define the ***identity map*** $\mathsf{Id}_\mathsf{A} \colon \mathsf{A} \to \mathsf{A}$ by $\mathsf{Id}_\mathsf{A}(\mathsf{a}) = \mathsf{a}$ for every $a \in A$. $\triangle$

Exercise 98.

(a) Show that Id_A is invertible

(b) Find the inverse of Id_A

$\Diamond$

Exercise 99.

(a) Suppose $f \colon A \to B$ and $g \colon B \to C$ are bijections. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(b) Suppose $f\colon X \to Y$ and $g\colon Y \to X$. Show that g is the inverse of f if and only if

$$f \circ g = \mathsf{Id}_Y \quad \text{and} \quad g \circ f = \mathsf{Id}_X.$$

(c) Suppose $f\colon X \to Y$ is a bijection. Show that the inverse of f^{-1} is f. That is, $(f^{-1})^{-1} = f$.

$\Diamond$

8

Equivalence Relations and Equivalence Classes

This can be thought of as a "pivotal" chapter. It generalizes the notion of "function", and relates this generalization to properties that we discussed in the Modular Arithmetic chapter. We will find that the new concepts we develop in this chapter will be foundational to the notions of *coset* and *conjugate*, two key group-theoretic structures which play central roles in group theory. [1]

8.1 Binary relations

Recall that, by definition, any function $f\colon A \to B$ is a set of ordered pairs. More precisely, each element of f is an ordered pair (a, b), such that $a \in A$ and $b \in B$. Therefore, every element of f is an element of $A \times B$, so f is a subset of $A \times B$. Every function from A to B is a subset of $A \times B$.

Example 1. The function $\mathsf{mother}\colon \mathsf{PEOPLE} \to \mathsf{PEOPLE}$ is represented by the set

$$\{\, (p, m) \in \mathsf{PEOPLE} \times \mathsf{PEOPLE} \mid m \text{ is the mother of } p \,\}.$$

$\Diamond$

Exercise 2.

[1] This chapter is an adapted and expanded version of a chapter by D. and J. Morris.

Let MY_GENERATION be the set consisting of you, your siblings, and any cousins you have.

(a) List the mothers of all individuals in MY_GENERATION.

(b) Now for each individual in MY_GENERATION, write an ordered pair that belongs to the function mother: PEOPLE $\rightarrow$ PEOPLE. (For example, if Ben's mother is Lucy, then (Ben,Lucy) is an ordered pair that belongs to the function mother.)

$\Diamond$

Many other relationships can also be represented by subsets of PEOPLE$\times$ PEOPLE, even though they are not functions. For example, son is not a function, because some people have more than one son (or because some people have no sons at all). However, we can represent this relation by the set

$$\{\,(p, s) \in \text{PEOPLE} \times \text{PEOPLE} \mid s \text{ is a son of } p\,\}.$$

Exercise 3.

(a) List your parents, siblings, aunts, uncles, and cousins, as a set. Denote this set as F.

(b) Define the relation called son on $F \times F$ as

$$\{(x, y) \in F \times F \mid y \text{ is a son of } x\}$$

List the ordered pairs in son. (For example, if Paula and Joseph are both in F and Joseph is Paula's son, then (Paula, Joseph) is an ordered pair in son. Note however if Nathan is in F and Nathan's son Luke is not in F, then (Nathan, Luke) is *not* an ordered pair in son.)

$\Diamond$

In fact, any relationship that you can define between two people (or, to say this in the official language of logic, any binary predicate on the set PEOPLE) can be represented by an subset of PEOPLE $\times$ PEOPLE. A few examples of possible relationships are:

- x is a sister of y

- x knew y in high school
- x is taller than y
- x and y are in the same math class
- etc.

In recognition of this, mathematicians simply *define* a relation to be a set of ordered pairs; that is, a relation is any subset of $A \times B$. Unlike the case of functions, there are no restrictions — every subset is a relation.

Definition 4. Suppose A and B are sets.

(a) Any subset of $A \times B$ is called a ***relation from*** A ***to*** B.

(b) For the special case where $A = B$, any subset of $A \times A$ is called a ***binary relation*** on A.

△

Example 5. If $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$, some examples of relations from A to B are:

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

Notice that all of these sets are subsets of $A \times B$. The final example is the set $A \times B$ itself. Notice that $\emptyset$ is a valid relation because it's a subset of $A \times B$ (a subset with no elements). On the other hand, the set $\{\emptyset\}$ is *not* a relation, because it is a set with one element (namely $\emptyset$), and this element is not an element of $A \times B$. For similar reasons, $\{(1, \emptyset)\}$ is *not* a relation. ◊

Example 6. Let $A = \{\text{all cities in the U.S.}\}$ and $B = \{\text{all states in the U.S.}\}$. two examples of relations from A to B are:

$$\{(\text{Austin,Texas}),(\text{Boston,Massachusetts}),(\text{Tucson,Arizona})\},$$

$$\{(x, y) \text{ such that } x \text{ is the capital of } y\}.$$

The first of these relations is a *subset* of the second. ♢

Exercise 7.

(a) Let $A = \{a\}$ and $B = \{1\}$. List *all* relations from A to B. (*Hint*)

(b) Let $A = \{a\}$ and $B = \{1, 2\}$. List *all* relations from A to B. (*Hint*)

(c) Let $A = \{a, b\}$ and $B = \{1\}$. List *all* relations from A to B. (*Hint*)

(d) ** Let $A = \{a, b\}$. List all the binary relations on A. (*Hint*)

(e) ** Let $A = \{a, b, c\}$. How many binary relations are there on the set A? (*Hint*)

♢

We will mostly be concerned with binary relations, not relations from some set A to some other set B.

Example 8. Some examples of binary relations on PEOPLE are: brother, sister, aunt, uncle, mother, father, grandfather, cousin, etc. ♢

Definition 9. We can draw a picture to represent any given binary relation on any given set A:

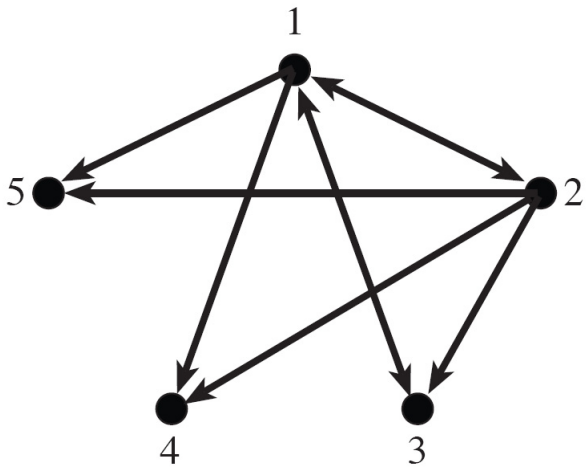
- Draw a dot for each element of A.
- For $a, b \in A$, draw an arrow from a to b if and only if (a, b) is an element of the relation.

The resulting picture is called a ***digraph***. (The word is pronounced "DIE-graff" — it is short for "directed graph." △

Example 10. Let $A = \{1, 2, 3, 4, 5\}$. We can define a binary relation R on A by letting

$$R = \{\, (x, y) \mid x \neq y \text{ and } x^2 + y \leq 10 \,\}.$$

This binary relation is represented by the following digraph:



For example, note that $(x, 4) \in R$ iff $x \in \{1, 2\}$, and the digraph has arrows from 1 to 4 and from 2 to 4. ◊

Exercise 11. Using the set F you defined in Exercise 3, draw a digraph for each of the following binary relations on F:

(a) son (as defined above)

(b) sister

(c) The relation "has ever been married to."

(d) The relation "has ever lived with."

◊

Exercise 12. Let $A = \{-2, -1, 0, 1, 2\}$ Draw a digraph for each of the following binary relations on A:

(a) $R_a = \{ (x, y) \mid x^2 = y^2 \}$.

(b) $R_b = \{ (x, y) \mid x^2 - y^2 < 2 \}$.

(c) $R_c = \{ (x, y) \mid (x - y)^2 < 2 \}$.

(d) $R_d = \{ (x, y) \mid x \equiv y \pmod 3 \}$.

◊

Exercise 13. It is also possible to draw digraphs for relations that are not binary relations.

(a) Draw digraph representations of the relations given in Example 5.

(b) The graphs you drew in (a) are all examples of ***bipartite*** graphs. Complete the following definition: A bipartite graph is a graph in which the vertices (dots) can be divided into two sets, such that .....

◊

We commonly use symbols such as $=, <, \subset, \ldots$ that are used to compare elements of a set. You may have called these "relations" in your high school algebra class – and in fact, they can all be considered as binary relations in the sense of Definition 4. For example, using the symbol $<$ we can define the following binary relation on $\mathbb{R}$:

$$R_< := \{ (x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y \}$$

(here the symbol ":=" means "defined as"). Note that $R_<$ here is a subset of $\mathbb{R} \times \mathbb{R}$, so it is indeed a binary relation according to Definition 4.

Exercise 14.

(a) Define the set $R_>$ associated with the symbol ">" applied to the natural numbers.

(b) Define the set $R_=$ associated with the symbol "=" applied to the complex numbers. In your definition assume that equality of real numbers has been defined, and write complex numbers in rectangular form (for example, $a + bi$ or $c + di$).

(c) List all the elements of the set $R_\subset$ associated with the symbol "$\subset$" applied to the subsets of $A := \{1, 2\}$. (The set of subsets of A is denoted as $P(A)$, the ***power set*** of A.) (*Hint*)

(d) Consider the set $R_\subset$ associated with the symbol "$\subset$" applied to the subsets of $A := \{1, 2, 3\}$. How many elements does $R_\subset$ have?

$\Diamond$

Exercise 14 shows that any comparison symbol applied to a set gives rise to a binary relation. So rather than writing $R_<, R_>, R_=$ and so on, we simply use the comparison symbol itself to represent the binary relation. Notice that technically, '$<$' defined on $\mathbb{R}$ is a different relation from '$<$' defined on $\mathbb{N}$: we will always make it very clear which set the relation is being defined on.

We will use the symbol $\sim$ to denote a generic comparison symbol. If we are working with the set A, then the symbol $\sim$ also represents the binary relation $A_\sim := \{ (x, y) \in A \times A \mid x \sim y\}$.

We have shown that comparison symbols give rise to equivalence relations: the reverse is also true. Given a relation R defined on the set A, we can define a comparison symbol $\sim$ applied to $a, b \in A$ as follows: $a \sim b$ iff $(a, b) \in R$.

There are three basic properties that any given binary relation may or may not have:

Definition 15. Suppose $\sim$ is a binary relation on a set A.

- We say that $\sim$ is ***reflexive*** iff

$$\forall a \in A, a \sim a.$$

  In other words, a binary relation on A is reflexive if every element of A is related to itself.

- We say that $\sim$ is ***symmetric*** iff

$$\forall a, b \in A, (a \sim b) \Rightarrow (b \sim a).$$

  In other words, a binary relation on A is symmetric if whenever a is related to b, then b is also related to a. (Here a and b represent elements of the set A.)

- We say that $\sim$ is ***transitive*** iff

$$\forall a, b, c \in A, \big((a \sim b) \text{ and } (b \sim c)\big) \Rightarrow (a \sim c).$$

  In other words, a binary relation on A is transitive if whenever a is related to b and b is related to c, then a is related to c. (Here a, b and c represent elements of the set A.)

△

Example 16. Consider the following binary relations on $\mathbb{R}$:

(a) $=$ is reflexive, symmetric, and transitive.

- Reflexive: any real number x equals itself, so $x = x$ $\forall x \in \mathbb{R}$.
- Symmetric: for any real numbers x and y, if $x = y$, then $y = x$.
- Transitive: for any real numbers x, y, and z, if $x = y$ and $y = z$, then $x = z$.

(b) $<$ is transitive, but neither reflexive nor symmetric.

- Not Reflexive: For example, it is not true that $1 < 1$.
- Not Symmetric: For example, $1 < 2$ but it is not true that $2 < 1$.
- Transitive: given three real numbers x, y, and z, if $x < y$ and $y < z$, then $x < z$.

(c) The binary relation $a \sim b$ iff $a = b + 1$ [for instance $(3.5, 2.5) \in \mathbb{R}_{\sim}$] is neither reflexive, symmetric, or transitive.

- Not Reflexive: $3 \neq 3 + 1$.
- Not Symmetric: $4 \sim 3$, since $4 = 3 + 1$, but $3 \not\sim 4$, since $3 \neq 4 + 1$.
- Not Transitive: $4 \sim 3$ and $3 \sim 2$, but $4 \not\sim 2$ $(4 \neq 2 + 1)$.

◊

Notice that in the above examples, we used specific counterexamples to demonstrate when properties were not true. We recommend that you do this also, because it is both clear and convincing (and it's usually the easiest way). It only takes *one* counterexample to show a property is not true!

Exercise 17. For each of the following, explain your answers.

(a) Is $\leq$ defined on the set $\mathbb{R}$ transitive? Is it reflexive? Is it symmetric? (*Hint*)

(b) Is $\subset$ defined on the set $P(\mathbb{N})$ transitive? Is it reflexive? Is it symmetric? (Recall that $P(\mathbb{N})$ is the set of subsets of $\mathbb{N}$).

(c) Define the relation $\sim$ on $\mathbb{C}$ as follows: $z_1 \sim z_2$ iff $z_1 = |z_2|$. Is $\sim$ transitive? Is it reflexive? Is it symmetric?

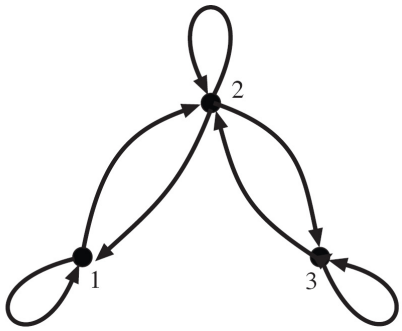
(d) Define the relation $\sim$ on $\mathbb{Z}$ as follows: $a \sim b$ iff $|a - b| < 4$. Is $\sim$ transitive? Is it reflexive? Is it symmetric?

$\Diamond$

Example 18. Given the set $B = \{1, 2, 3\}$, consider the relation $\sim$ on B defined by

$$B_\sim = \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2)\}$$

The relation is shown in the picture below.



- $\sim$ is reflexive, because $1 \sim 1$, $2 \sim 2$, and $3 \sim 3$ (Note we had to check *all* elements of the set B),
- $\sim$ is symmetric, because, for each $(a, b) \in \sim$, the reversal (b, a) is also in $\sim$.
- $\sim$ is *not* transitive, because $1 \sim 2$ and $2 \sim 3$, but $1 \not\sim 3$.

$\Diamond$

Transitivity can sometimes be a little tricky:

Exercise 19.

(a) Explain why the binary relation

$$R_{\sim} = \{(1,4),(1,1),(4,1)\}$$

is *not* transitive. (*Hint*)

(b) Explain why the binary relation

$$R_{\sim} = \{(1,2),(1,3),(1,4)\}$$

is transitive. (*Hint*)

◊

Exercise 20. Find binary relations on $\{1,2,3\}$ that meet each of the following conditions (Express each relation as a set of ordered pairs, and draw the corresponding digraph.)

(a) symmetric, but neither reflexive nor transitive.

(b) reflexive, but neither symmetric nor transitive.

(c) transitive and symmetric, but not reflexive.

(d) neither reflexive, nor symmetric, nor transitive.

◊

Digraphs are useful because they represent the relation in such a way that it is easy to deduce the relation's properties:

Exercise 21.

(a) How can you tell from looking at a digraph whether or not the corresponding relation is reflexive?

(b) How can you tell from looking at a digraph whether or not the corresponding relation is symmetric?

(c) **How can you tell from looking at a digraph whether or not the corresponding relation is transitive? (*This one is harder.*)

◊

8.2 Definition and basic properties of equivalence relations

People often need to sort through a collection of objects, putting similar objects together in a group.

Example 22. When making an inventory of the animals in a zoo, we may wish to count the number of antelopes, the number of baboons, the number of cheetahs, and so forth. In this case, all of the animals of the same species might be grouped together. Mathematically speaking, we would define a binary relation S on the set of animals in the zoo by

$$x \sim_S y \quad \text{iff} \quad x \text{ and } y \text{ are in the same species.}$$

$\Diamond$

Now if we consider the relation $\sim_S$ in light of the properties defined in Definition 15, we may discover:

- $\sim_S$ is reflexive (x is always the same species as itself);
- $\sim_S$ is symmetric (x is the same species as y iff y is the same species as x);
- $\sim_S$ is transitive (if x is the same species as y and y is the same species as z, then x is the same species as z);

Example 23.

(a) If we are concerned only with people's first names, we could define a relation $\sim_N$ on the set of all people by

$$x \sim_N y \text{ iff } x \text{ has the same first name as } y.$$

(b) In geometry, sometimes we are interested only in the shape of a triangle and not its location or orientation. In this case, we talk about *congruent* triangles. We may define a relation $\cong$ on the set of all triangles by

$$T_1 \cong T_2 \text{ iff } T_1 \text{ is congruent to } T_2.$$

Here "congruent" means that corresponding sides of the two triangles are equal, and corresponding angles are also equal.

◊

Exercise 24.

(a) For the relation $\sim_N$ in part (a) of Example 23, explain why it is reflexive, symmetric, and transitive.

(b) For the relation $\cong$ in part (b) of Example 23, explain why it is reflexive, symmetric, and transitive.

◊

The above examples motivate the following definition:

Definition 25. An ***equivalence relation*** on a set A is a binary relation on A that is reflexive, symmetric, and transitive. △

Exercise 26.

(a) "Congruence" is an equivalence relation on triangles, that you studied in your geometry class. Can you think of another equivalence relation on triangles that you studied in high school geometry?

(b) Define an equivalence relation on the set of all polygons, such that in particular all triangles are equivalent. Explain why your relation is reflexive, symmetric, and transitive. (There are many possible answers to this question.)

(c) Define an equivalence relation on the set of all polygons, such that in particular not all triangles are equivalent but all rectangles are equivalent. (There are many possible answers to this question.)

◊

Example 27. Define a binary relation $\sim$ on $\mathbb{R}$ by $x \sim y$ iff $x^2 = y^2$. Then $\sim$ is an equivalence relation.

PROOF. We wish to show that $\sim$ is reflexive, symmetric, and transitive.

(reflexive) Given $x \in \mathbb{R}$, we have $x^2 = x^2$, so $x \sim x$.

(symmetric) Given $x, y \in \mathbb{R}$, such that $x \sim y$, we have $x^2 = y^2$. Since equality is symmetric, this implies $y^2 = x^2$, so $y \sim x$.

(transitive) Given $x, y, z \in \mathbb{R}$, such that $x \sim y$ and $y \sim z$, we have $x^2 = y^2$ and $y^2 = z^2$. Therefore $x^2 = z^2$, since equality is transitive. Hence $x \sim z$. □ ◊

Example 28. Define a binary relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1 + b_2 = a_2 + b_1$. Then $\sim$ is an equivalence relation.

PROOF. We wish to show that $\sim$ is reflexive, symmetric, and transitive.

(reflexive) Given $(a, b) \in \mathbb{N} \times \mathbb{N}$, we have $a + b = a + b$, so $(a, b) \sim (a, b)$.

(symmetric) Given $(a_1, b_1), (a_2, b_2) \in \mathbb{N} \times \mathbb{N}$, such that $(a_1, b_1) \sim (a_2, b_2)$, we have $a_1 + b_2 = a_2 + b_1$. Since equality is symmetric, this implies $a_2 + b_1 = a_1 + b_2$, so $(a_2, b_2) \sim (a_1, b_1)$.

(transitive) Given $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{N} \times \mathbb{N}$, such that $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$, we have

$$a_1 + b_2 = a_2 + b_1 \text{ and } a_2 + b_3 = a_3 + b_2. \tag{8.1}$$

Therefore

$$\begin{aligned} (a_1 + b_3) + (a_2 + b_2) &= (a_1 + b_2) + (a_2 + b_3) && \text{(rearrange terms)} \\ &= (a_2 + b_1) + (a_3 + b_2) && \text{Equation (8.1) above} \\ &= (a_3 + b_1) + (a_2 + b_2) && \text{(rearrange terms).} \end{aligned}$$

Subtracting $a_2 + b_2$ from both sides of the equation, we conclude that $a_1 + b_3 = a_3 + b_1$, so $(a_1, b_1) \sim (a_3, b_3)$. □ ◊

Exercise 29. Show that each of these binary relations is an equivalence relation.

(a) The binary relation $\sim$ on $\mathbb{R}$ defined by $x \sim y$ iff $x^2 - 3x = y^2 - 3y$.

(b) The binary relation $\sim$ on $\mathbb{R}$ defined by $x \sim y$ iff $x - y \in \mathbb{Z}$. (*Hint*)

(c) The binary relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ defined by $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1 b_2 = a_2 b_1$. (*Hint*)

(d) The binary relation $\sim$ on $\mathbb{C}$ defined by $z_1 \sim z_2$ iff $|z_1| = |z_2|$.

(e) The binary relation $\sim$ on $\mathbb{C}$ defined by $z_1 \sim z_2$ iff $\mathrm{Re}[z_1] = \mathrm{Re}[z_2]$. (Recall that $\mathrm{Re}[z]$ is the real part of z)

(f) The binary relation $\sim$ on the collection of all finite sets defined by

$$A \sim B \quad \text{iff} \quad |A| = |B| \text{ (that is, } A \text{ and } B \text{ have the same number of elements)}$$

$\Diamond$

Any time we have a function, we also get an equivalence relation on its domain:

Example 30.

(a) Every animal has only one species, so Species is a function that is defined on the set of all animals. The equivalence relation $\sim_S$ of Example 22 can be characterized by

$$x \sim_S y \quad \text{iff} \quad \mathsf{Species(x)} = \mathsf{Species(y)}.$$

(b) If we assume that every person has a first name, then FirstName is a function on the set of all people. The equivalence relation $\sim_N$ of Example 23 can be characterized by

$$x \sim_N y \quad \text{iff} \quad \mathsf{FirstName(x)} = \mathsf{FirstName(y)}.$$

$\Diamond$

The following result generalizes this idea to all functions.

Proposition 31. Suppose $f\colon A \to B$. If we define a binary relation $\sim$ on A by

$$a_1 \sim a_2 \quad \text{iff} \quad f(a_1) = f(a_2),$$

then $\sim$ is an equivalence relation.

Exercise 32. Prove Proposition 31. (That is, prove that the relation defined in the proposition is (a) reflexive, (b) symmetric, and (c) transitive. $\Diamond$

8.3 Equivalence classes

If we are interested in first names (as in Example 23), then we may also be interested in the set of all people who have the same first name as you. This is called your "equivalence class."

Definition 33. Suppose $\sim$ is an equivalence relation on a set A. For each $a \in A$, the ***equivalence class*** of a is the following subset of A:

$$[a] = \{\, s \in A \mid s \sim a \,\}.$$

That is, the equivalence class of the element $a \in A$ is the set of all elements of A that are equivalent to a. △

Example 34. For the equivalence relation N described in Example 23, we have

$$[\mathsf{AliceCooper}] = \{\, \mathsf{x} \in \mathsf{People} \mid \mathsf{FirstName(x)} = \mathsf{FirstName(AliceCooper)} \,\}.$$

In other words, [AliceCooper] is the set of all people whose first name is Alice. ♢

Warning The notation $[a]$ does not tell us which equivalence relation is being used. You should be able to figure out which relation it is from the context. ♢

Example 35. Suppose $A = \{1, 2, 3, 4, 5\}$ and

$R =$
$\{(1,1), (1,3), (1,4), (2,2), (2,5), (3,1), (3,3), (3,4), (4,1), (4,3), (4,4), (5,2), (5,5)\}$

One can verify that R is an equivalence relation on A. The equivalence classes are:

$$[1] = \{1,3,4\}, \quad [2] = \{2,5\}, \quad [3] = \{1,3,4\} \quad [4] = \{1,3,4\}, \quad [5] = \{2,5\}.$$

♢

Exercise 36.

(a) Let $B = \{1, 2, 3, 4, 5\}$ and

$$S = \{(1, 1),\ (1, 4),\ (2, 2),\ (2, 3),\ (3.2),\ (3, 3),\ (4, 1),\ (4, 4),\ (5, 5)\}.$$

Assume (without proof) that S is an equivalence relation on B. Find the equivalence class of each element of B.

(b) Let $C = \{1, 2, 3, 4, 5\}$ and define $\sim_C$ by

$$x \sim_C y \text{ iff } x + y \text{ is even.}$$

Assume (without proof) that $\sim_C$ is an equivalence relation on C. Find the equivalence class of each element of C.

(c) Draw the arrow diagrams for $\sim_A, \sim_B$, and $\sim_C$.

$\Diamond$

The following proposition presents some very important properties of equivalence classes:

Proposition 37. Suppose $\sim$ is an equivalence relation on a set S. Then:

(a) For all $a \in S$, we have $a \in [a]$.

(b) For all $a \in S$, we have $[a] \neq \emptyset$.

(c) The union of the equivalence classes is all of S. This can be written mathematically as follows:

$$\bigcup_{a \in S} [a] = S$$

(d) For any $a_1, a_2 \in S$, such that $a_1 \sim a_2$, we have $[a_1] = [a_2]$.

(e) For any $a_1, a_2 \in S$, such that $a_1 \not\sim a_2$, we have $[a_1] \cap [a_2] = \emptyset$.

Exercise 38. Prove the assertions in Proposition 37. You may use the following hints:

(a) Use the reflexive property of $\sim$, together with Definition 33

(b) Use part (a).

(c) This can be done by showing:

(i) $\bigcup_{a \in S}[a] \subset S$

(ii) $S \subset \bigcup_{a \in S}[a]$

In (i), use the fact that $[a] \subset S$. In (ii), use (a) above to show that every element of S is in at least one equivalence class.

(d) Remember that two sets are equal if they have all their elements in common. So you want to show that given $a_1 \sim a_2$, then every element of $[a_1]$ is also an element of $[a_2]$, and vice versa. Do this as follows:

- Choose any $a_3 \in [a_1]$. Use Definition 33 together with the transitive property to show that $a_3 \in [a_2]$. Conclude that every element of $[a_1]$ is also an element of $[a_2]$.
- Use a similar proof to show that every element of $[a_2]$ is also an element of $[a_1]$.

(e) You can prove this one by contradiction. Suppose the intersection is non-empty. Choose an element in the intersection. Use Definition 33 and the transitive property to derive a contradiction.

$\Diamond$

Proposition 37 also gives us this important fact:

Proposition 39. Suppose $\sim$ is an equivalence relation on a set S. Then any two equivalence classes are either equal or disjoint; that is, either they have exactly the same elements, or they have no elements in common.

Exercise 40. Fill in the blanks to complete the proof of Proposition 39:

PROOF. It's enough to show that any two equivalence classes $[a_1]$ and $[a_2]$ that are not disjoint must in fact be equal.

(a) Since the equivalence classes are not disjoint, their intersection is nonempty: so there is some $a \in [a_1] \cap$ _____.

(b) Hence, $a \in$ _____ and $a \in$ _____.

(c) By Definition 33, this means $a \sim$ _____ and $a \sim$ _____.

(d) Hence, Proposition 37 part _____ tells us that $[a] =$ _____ and $[a] =$ _____.

(e) Therefore _____ $= [a] =$ _____, as desired.

□ ◊

8.4 Modular arithmetic redux

Abstract algebra often involves looking at familiar concepts and structures in a more general more abstract and "elegant" way. As an example of this, we will now revisit modular arithmetic and describe it from an entirely different point of view, with the benefit of the concepts we have been developing in previous sections.

In the Modular Arithmetic chapter we defined the concept of "modular equivalence". You may recall that we actually gave two definitions, which we repeat here:

Definition 41. *(Modular Equivalence, first definition)*

$a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. △

Definition 42. *(Modular Equivalence, second definition)*

$a \equiv b \pmod{n}$ iff $a - b = k \cdot n$, where k is an integer (that is, $k \in \mathbb{Z}$). △

Exercise 43. Using Definition 33 and Definition 42, show that equivalence mod n is an equivalence relation. (That is, show that equivalence mod n is (a) reflexive, (b) symmetric, and (c) transitive) ◊

Exercise 43 enables us to apply the concepts we've been developing to modular arithmetic. In particular, it enables us to describe modular arithmetic in terms of equivalence classes. We will do this first with a simple example: the integers mod 3.

8.4.1 The integers modulo 3

We have proven in Exercise 43 that equivalence mod 3 is a bona fide equivalence relation. So what are the equivalence classes? And how many are there?

We can use Definition 41 to answer this question. The possible remainders when an integer is divided by 3 are either 0, 1, or 2. This tells us that every integer is equivalent (modulo 3) to either 0, 1, or 2. Using Proposition 37 part (d), it follows that:

> for every $k \in \mathbb{Z}$, the equivalence class $[k]_3$ must be either $[0]_3$, $[1]_3$, or $[2]_3$.

(To emphasize the fact that $n = 3$, we have included a subscript $_3$ in the notation for the equivalence classes).

Specifically:

$$[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$

$$[1]_3 = \{\ldots, -5, -2, 1, 4, 7, \ldots\},$$

$$[2]_3 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

are three equivalence classes that partition the set of all integers. In the Modular Arithmetic chapter we defined the integers mod 3 as the set of remainders under division mod 3. Here we will give an alternative definition that amounts to the same thing:

Definition 44. *(Integers mod 3, equivalence class definition)* The set of equivalence classes $\{[0]_3, [1]_3, [2]_3\}$ is identified as the set of ***integers mod 3***, and is represented by the symbol $\mathbb{Z}_3$.

We may also use the simpler notation $\overline{k}$ to represent the equivalence class $[k]_3$. So we may write either $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ or $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. △

Notice the subtle (but critically important) difference between this description of modular integers and our previous description. Previously we took the remainders $\{0, 1, 2\}$ and defined addition and multiplication operations that had the property of closure. But now we are taking a different tack. We are saying that the elements of $\mathbb{Z}_3$ are *equivalence classes* rather than numbers. In other words, the elements of $\mathbb{Z}_3$ are *sets*.

We now define arithmetic operations on $\mathbb{Z}_3$, using our new definition of $\mathbb{Z}_3$ as a set of equivalence classes. Note the additional level of abstraction here: these arithmetic operations are defined on equivalence classes, which are *sets* rather than numbers. But we've seen this before: recall that in the Sets chapter we defined operations on sets. So you're old hands at this!

Definition 45. (Rules of modular arithmetic) The ***arithmetic operations modulo*** 3 are defined as follows:

- $[a]_3 + [b]_3 = [a+b]_3$ (or $\overline{a} + \overline{b} = \overline{a+b}$),
- $[a]_3 - [b]_3 = [a-b]_3$ (or $\overline{a} - \overline{b} = \overline{a-b}$),
- $[a]_3 \cdot [b]_3 = [ab]_3$ (or $\overline{a} \cdot \overline{b} = \overline{ab}$).

△

In Definition 45 we are actually giving *new meanings* to the symbols $+$,$-$, and $\cdot$. We could make this explicit by using different symbols. But this is not really necessary: whenever we're doing arithmetic with equivalence classes mod 3 (or mod n, for that matter), you should always presume that we're using the modular definitions of $+$,$-$, and $\cdot$.

Example 46. We have $[1]_3 + [2]_3 = [1+2]_3 = [3]_3$. However, since 3 and 0 are in the same equivalence class, we have $[3]_3 = [0]_3$, so the above equation can also be written as $[1]_3 + [2]_3 = [0]_3$. Equivalently, $\overline{1} + \overline{2} = \overline{0}$. ◊

Example 46 illustrates the following general rule:

If r is the remainder when $a+b$ is divided by 3, then $\overline{a} + \overline{b} = \overline{r}$.

You may recognize that this is essentially the same rule that we used in our previous discussion of modular arithmetic.

Exercise 47. Write down similar rules for (a) subtraction mod 3; (b) multiplication mod 3. ◊

Example 48. Here is a table that shows the results of addition modulo 3:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\Diamond$

Exercise 49. Make tables that show the results of:

(a) multiplication modulo 3.

(b) subtraction modulo 3 (For $\overline{a}-\overline{b}$, put the result in row $\overline{a}$ and column; $\overline{b}$.)

For both (a) and (b), all table entries should be either $\overline{0}$, $\overline{1}$, or $\overline{2}$. $\Diamond$

8.4.2 The integers modulo n

The preceding discussion can be generalized to apply with any integer n in place of 3. This results in ***modular arithmetic***.

Definition 50. Fix some natural number n.

(a) For any integer k, we use $[k]_n$ to denote the equivalence class of k under congruence modulo n. When n is clear from the context, we may write $\overline{k}$, instead of $[k]_n$.

(b) The set of these equivalence classes is called the ***integers modulo*** n. It is denoted $\mathbb{Z}_n$.

(c) Addition, subtraction, and multiplication modulo n are defined by:

- $\overline{a}+\overline{b}=\overline{a+b}$,
- $\overline{a}-\overline{b}=\overline{a-b}$, and
- $\overline{a}\cdot\overline{b}=\overline{ab}$.

Just as in the case of mod 3, whenever we're doing arithmetic mod n you should understand that we are using these definitions of $+$, $-$, and $\cdot$.

△

Note that $|\mathbb{Z}_n| = n$.[2] More precisely:

Proposition 51. For any $n \in \mathbb{N}^+$, we have

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

and $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ are all distinct.

Exercise 52. Make tables that show the results of:

(a) addition modulo 4.

(b) subtraction modulo 5.

(c) multiplication modulo 6.

◊

Exercise 53. Find $x, y \in \mathbb{Z}_{12}$ such that $x \neq \overline{0}$ and $y \neq \overline{0}$, but $x \cdot y = \overline{0}$. ◊

8.4.3 Something we have swept under the rug

The discussion of modular arithmetic ignored a very important point. When we evaluate $\overline{a} + \overline{b}$, we use the following process:

- Choose an element from $\overline{a}$ and an element from $\overline{b}$;
- Add them together (using regular integer arithmetic);
- Find the equivalence class of the result.

But suppose we had chosen *different* elements to represent $\overline{a}$ and $\overline{b}$: how do we know that we would come up with the same answer? In other words: how do we know that $\overline{a} + \overline{b}$ is independent of the choice of representatives from $\overline{a}$ and $\overline{b}$?

So there's a little more work we have to do here to make sure that we don't get into trouble. We need to show that the operations of addition, subtraction, and multiplication are ***well-defined***: that is, if a_1, a_2, b_1, and b_2 are integers such that $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$, then we need to show that

[2] Recall that for a set S, $|S|$ means the number of elements in S.

(a) $\overline{a_1} + \overline{b_1} = \overline{a_2} + \overline{b_2}$,

(b) $\overline{a_1} - \overline{b_1} = \overline{a_2} - \overline{b_2}$,

(c) $\overline{a_1} \cdot \overline{b_1} = \overline{a_2} \cdot \overline{b_2}$.

Fortunately, these statements are all true, as you will show in the following exercise.

Exercise 54.

(a) Fill in the blanks in the following proof of statement (a) above that $+$ is well-defined:

Suppose $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$.

(i) From the definition of equivalence class, it follows that $a_1 \equiv$ _____ (mod n) and $b_1 \equiv$ _____ (mod n).

(ii) By Definition 42, it follows that $a_1 - a_2 = k_1 \cdot$ _____ and $b_1 - b_2 =$ $k_2 \cdot$ _____, where k_1 and k_2 are _____.

(iii) By integer arithmetic it follows that $(a_1+b_1)-(a_2+b_2) =$ _____

(iv) Since $k_1 + k_2$ is an integer it follows from Definition 42 that $(a_1 +$ $b_1) \equiv$ _____ (mod ____).

(v) It follows from Proposition 37 part (d) that _____.

(vi) By Definition 50 (c) then $\overline{a_1} + \overline{b_1} =$ _____; so $+$ is well-defined.

(b) By following the proof in part (a), prove that subtraction mod n is well-defined.

(c) By following the proof in part (a), prove that multiplication mod n is well-defined.

$\Diamond$

Actually, finding operations that are well-defined on equivalence classes is somewhat of a big deal. In many cases, candidate operations turn out to be *not* well-defined:

Exercise 55. Suppose we try to define an exponentiation operation on $\mathbb{Z}_3$ by:

$$[a]_3 \,\hat{}\, [b]_3 = [a^b]_3 \quad \text{for } [a]_3, [b]_3 \in \mathbb{Z}_3.$$

Show that $^\wedge$ is not well-defined: that is, find $a, b, c, d \in \mathbb{Z}$, such that $[a]_3 = [c]_3$ and $[b]_3 = [d]_3$, but $\left[a^b\right]_3 \neq \left[c^d\right]_3$. ◊

Exercise 56.

(a) Show that absolute value does *not* provide a well-defined function from $\mathbb{Z}_7$ to $\mathbb{Z}_7$. That is, show there exist $a, b \in \mathbb{Z}$, such that

$$[a]_7 = [b]_7, \text{ but } \left[|a|\right]_7 \neq \left[|b|\right]_7.$$

(b) Show that part (a) is true for *every* $n > 2$. That is, show that absolute value does *not* provide a well-defined function from $\mathbb{Z}_n$ to $\mathbb{Z}_n$.

◊

Exercise 57.

(a) Show that there is a well-defined function

$$f\colon \mathbb{Z}_4 \to \mathbb{Z}_{12}, \text{ given by } f\big([a]_4\big) = [a]_{12}.$$

That is, show that if $[a]_{12} = [b]_{12}$, then $f\big([a]_4\big) = f\big([b]_4\big)$.

(b) Generalize part (a) by showing that if m divides n, then there is a well-defined function $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$, given by $f\big([a]_n\big) = [a]_m$. That is, show that if $[a]_n = [b]_n$, then $f\big([a]_n\big) = f\big([b]_n\big)$.

◊

Exercise 58.

(a) Show that if we try to define a function $g\colon \mathbb{Z}_3 \to \mathbb{Z}_2$ by $g\big([a]_3\big) = [a]_2$, then the result is *not* well-defined. That is, show that $\exists a, b \in \mathbb{Z}$ such that $[a]_3 = [b]_3$ but $[a]_2 \neq [b]_2$.

(b) Generalize part (a) by showing that if m does not divide n, then the function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $f\big([a]_n\big) = [a]_m$ is *not* well-defined. That is, show that there exists integers a, b such that $[a]_n = [b]_n$ and $f\big([a]_n\big) \neq f\big([b]_n\big)$.

◊

8.5 Partitions

Whenever we classify the elements of a particular set, essentially what we are doing is dividing the set up into several disjoint subsets. This is called a ***partition*** of the set. Figure 8.5 below shows a schematic representation of a partition.

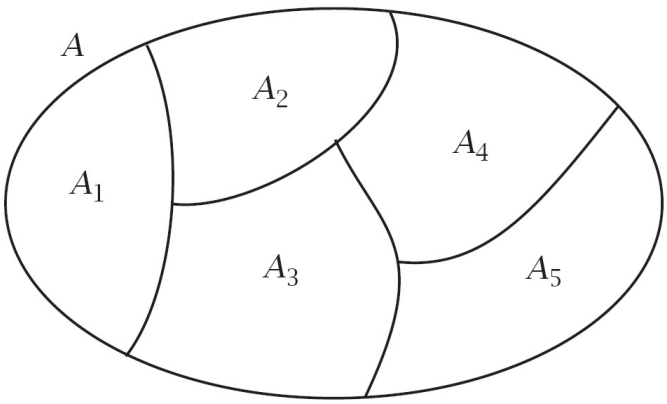


Figure 8.1. A partition of A into subsets $A_1, \ldots, A_5$. (Each element of A is in one and only one of the subsets.)

Example 59. Mary is leaving for university, and does not want her childhood toys any more, so she will divide them up among her younger siblings: Alice, Bob, and Cindy. Let

- T be the set of all of Mary's toys, and
- A, B, and C be the set of toys that she will give to Alice, to Bob, and to Cindy, respectively.

Then A, B, and C are subsets of T, and they should be chosen so that:

(a) the union of A, B and C is T (that is, $A \cup B \cup C = T$), so all of the toys are given away, and

(b) the sets A, B, and C are pairwise disjoint (that is, $A \cap B = \emptyset$, $A \cap C = \emptyset$, and $B \cap C = \emptyset$), so there will not be any confusion about who is the new owner of each toy (confusion of ownership among siblings is a dangerous situation).

Here $\{A, B, C\}$ is a partition pf T into three disjoint subsets (as long as A, B, C are all nonempty). ◊

We generalize this example in the following definition:

Definition 60. A ***partition*** of a set A is a collection of nonempty subsets of A, such that each element of A is in exactly one of the subsets. In other words:

(a) the union of the subsets in the collection is all of A, and

(b) the subsets in the collection are pairwise disjoint.

△

Example 61. In Example 35, the equivalence classes are $\{1, 3, 4\}$ and $\{2, 5\}$. Since $1, 2, 3, 4, 5$ each belong to exactly one of these sets, we see that the set

$$\big\{\{1, 3, 4\}, \{2, 5\}\big\}$$

of equivalence classes is a partition of $\{1, 2, 3, 4, 5\}$. ◊

The following result is an immediate consequence of Proposition 37. It says that equivalence classes always provide a partition.

Proposition 62. Suppose $\sim$ is an equivalence relation on a set A. Then

$$\{\, [a] \mid a \in A \,\}$$

is a partition of A.

PROOF. From parts b, c, and e of Proposition 37, we know that the equivalence classes are nonempty, that their union is A, and that they are pairwise disjoint. □

Proposition 62 tells us that every equivalence relation gives us a partition. Conversely, the following proposition shows that any partition comes

from an equivalence relation. In other words, equivalence relations and partitions are just two different ways of looking at the same thing.

Proposition 63. Suppose $\mathcal{P}$ is a partition of a set A. Define a binary relation $\sim$ on A by

$$a \sim b \quad \text{iff} \quad \exists C \in \mathcal{P}, (a \in C \text{ and } b \in C).$$

Then:

(a) $\sim$ is an equivalence relation on A, and

(b) the set of equivalence classes is the partition $\mathcal{P}$.

Recall that $\mathbb{Z}_n$ replaces integers a and b that are congruent modulo n with objects $\overline{a}$ and $\overline{b}$ that are exactly equal to each other. This was achieved by letting $\mathbb{Z}_n$ be the set of all equivalence classes. The set $\mathbb{Z}_n$ applies only to congruence modulo n, but the same thing can be done for any equivalence relation:

Definition 64. Suppose $\sim$ is an equivalence relation on a set A. The set of all equivalence classes is called A ***modulo*** $\sim$. It is denoted $A/\sim$. △

Example 65. Suppose we define an equivalence relation $\sim$ on $\mathbb{Z}$ by $a \sim b$ iff $a \equiv b \pmod{n}$. Then $\mathbb{Z}/\sim$ is simply another name for $\mathbb{Z}_n$. ◊

Exercise 66. Let $f\colon \{-3,-2,-1,0,1,2,3\} \to \mathbb{N}$ be defined by $f(x) = x^2$. Define a relation $\sim$ on $\{-3,-2,-1,0,1,2,3\}$ by: $n \sim m$ iff $f(n) = f(m)$.

(a) Show that $\sim$ is an equivalence relation: that is, show that $\sim$ is reflexive, symmetric, and transitive.

(b) According to Proposition 62, this equivalence relation produces a partition on $\{-3,-2,-1,0,1,2,3\}$. List the sets in the partition.

◊

Exercise 67. Consider the Cartesian plane $\mathbb{R}^2$. Let C_r be the circle of radius r centered at $(0,0)$, for $r \in [0,\infty)$.(Note that in mathematics, "circle" means just the circumference and not the interior: the interior of the circle is called a "disk".)

(a) If the point $(x, y) \in C_r$, then write an equation that (x, y) must satisfy. (*Hint*)

(b) Show that C_r and C_s are disjoint whenever $r \neq s$. (Do this by showing that any element of C_r is not an element of C_s, and vice versa).

(c) Show that the union of the set of all circles $\{C_r, r \in [0, \infty)$ is all of $\mathbb{R}^2$. (Do this by showing that every element of $\mathbb{R}^2$ is in at least one circle.)

(d) Show that the set of circles centered at $(0, 0)$ form a partition of the Cartesian plane. (*Hint*)

(e) According to Proposition 63 part a, this partition defines an equivalence relation $\sim$ on $\mathbb{R}^2$. Use the equation in part (a) of this exercise to complete the following sentence: $(x_1, y_1) \sim (x_2, y_2)$ iff _____.

$\Diamond$

Summary

- Important definitions:
  - relation, binary relation
  - reflexive, symmetric, transitive
  - equivalence relation
  - equivalence class
  - modular arithmetic
  - integers modulo n
  - well-defined
  - partition
- Modular arithmetic is an important example of the use of equivalence classes.
- Functions must be well-defined.
- Every binary relation can be drawn as a digraph.
- Every partition gives rise to an equivalence relation, and vice versa.

- Notation:
  - $\sim$, $\cong$, or $\equiv$ are used for equivalence relations
  - $[a]$, or $\overline{a}$
  - $\mathbb{Z}_n$

$\Diamond$

9

Symmetries of Plane Figures

> "In all the arts it is symmetry that gives pleasure, preserving unity, and making the whole beautiful." (Augustine, *Of True Religion*, xxx.55 (Tr. J. H. S. Burleigh)

> "It is only slightly overstating the case to say that physics is the study of symmetry." (Philip W. Anderson, 1977 Nobel laureate in physics)

> "So our problem is to explain where symmetry comes from. Why is nature so nearly symmetrical? No one has any idea why." (Richard Feynman, 1965 Nobel laureate in physics)

The above quotes give some flavor of the importance and the mystery of symmetry, in both art and science. In keeping with our practice throughout this book, we will introduce this general topic by means of a basic example, namely symmetries of plane figures. Many of the concepts that you will learn in this chapter are applicable to symmetries in general. In particular: wherever you find a symmetry, you will always find a *group* lurking behind it (see Section 4.4.7 for the mathematical definition of a group).[1]

9.1 Definition and examples

We begin this section with a definition:

Definition 1. A ***symmetry*** of a geometrical figure is a rearrangement of the figure that (i) preserves distances and angles between points of the

[1]Thanks to Tom Judson for material used in this chapter.

figure, and (ii) leaves the appearance and location of the figure unchanged. △

Remark 2. The meaning of "preserves distances" can be expressed more precisely as follows. Take any two points A and B of the original figure. The figure is then rearranged so that A and B are sent to points A' and B' respectively. Then in order for the rearrangement to be a symmetry, the distance between A and B must always be equal to the distance between A' and B'.

Similarly, the meaning of "preserves angles" can be expressed more precisely as follows. Take any three points A, B, C of the original figure. The figure is then rearranged so that A, B, C are sent to A', B', C' respectively. In order for the rearrangement to be a symmetry, $\angle ABC$ must always be equal to $\angle A'B'C'$ regardless of the choice of A, B, C. [2] △

A motion that preserves distances and angles between parts of a figure is also called a ***rigid motion***. Intuitively, you may think of the figure as a rigid object, and the "rearrangement" is effected by moving the rigid object in some fashion. For example, any ***rotation*** that does not change the shape of the object is a rigid motion.

Figure 9.1. Mercedes Logo

Example 3. Consider the Mercedes logo shown in Figure 9.1.

- Imagine pinning the center of the logo to the page and spinning the logo 120° counterclockwise about its center. The resulting image looks

[2] It can be shown mathematically that a rearrangement that preserves distances must necessarily preserve angles as well. So strictly speaking, the additional angle preservation requirement is not necessary.

exactly like the original, because each of the three points on the circumference moves to the location of the next point over. So a 120° counterclockwise rotation is a symmetry of the logo.

- If you rotate the image 180° counterclockwise about the center, the resulting image is no longer identical to the original (try it!). So a 180° counterclockwise rotation is not a symmetry of the logo.
- We could also "flip over" the logo (like flipping a pancake) in such a way that the left half moves to the right, and vice versa. Then the vertical point stays in the same place while the left and right point exchange positions, leaving the appearance of the logo unchanged. The motion has the same effect as if the logo were ***reflected*** across the vertical axis. After the motion, the logo looks the same.
- Shifting the original image (shifts are also called ***translations*** in any direction is a rigid motion, and the resulting image looks the same as the original, but the location is different. Hence this shift is *not* not a symmetry of the Mercedes logo.

♦

Exercise 4. List six different symmetries of the Mercedes logo. (*Hint*) ◊

This is not the first time we've played with symmetries of a figure. At the end of Chapter 1, we saw that the complex sixth roots of unity determined a regular hexagon in the complex plane, and that complex multiplication and complex conjugation could be used to rotate or reflect the hexagon. Let us investigate the hexagon a bit further.

Example 5. Figure 9.2 shows a 60° counterclockwise rotation of a regular hexagon.

The rotation moves A to B, B to C, and so on. Now of course there are other points on our figure, namely all the points on the line segments between the vertices. But notice that if we account for where the vertices are moved to, then the movement of the line segments is automatically accounted for. If we know where A and B are moved to, we know exactly where $\overline{AB}$ is. Therefore, our 60 degree rotation can be defined by the movement of the vertices $\{A, B, C, D, E, F\}$.

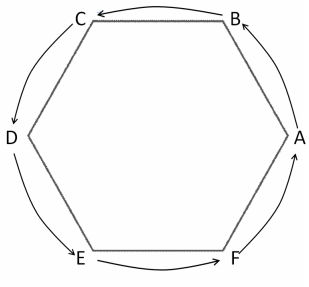


Figure 9.2. Hexagon and 60° rotation

Now if we input a point from $\{A, B, C, D, E, F\}$, our rotation outputs a point from $\{A, B, C, D, E, F\}$. We have used this "input-output" language before, namely in the Functions chapter.

In fact, we can think of the 60 degree rotation as a function r_{60} from $\{A, B, C, D, E, F\} \to \{A, B, C, D, E, F\}$, where (using ordered pair notation)

$$r_{60} = \{(A, B), (B, C), (C, D), (D, E), (E, F), (F, A)\}$$

♦

Exercise 6.

(a) Is r_{60} one-to-one? Explain why or why not.

(b) Is r_{60} onto? Explain why or why not.

(c) Is r_{60} a bijection? Explain why or why not.

◊

Exercise 6 exemplifies a general property of symmetries:

Proposition 7. If S is the set of points that represent a figure, all symmetries of the figure are bijections from $S \to S$.

PROOF. Since the result of any symmetry acting on S must be all of S, then every point of S must be in the range of S. Thus any symmetry is onto.

Furthermore, the symmetry must map two different points to two different points, since the distance between points must be left unchanged by the symmetry. Hence any symmetry is one-to-one. So since any symmetry is both onto and one-to-one, it follows that any symmetry is a bijection. □

Proposition 7 says that all symmetries are bijections, but the *converse* is not true: all bijections are not symmetries.

Exercise 8. Create a bijection from $\{A, B, C, D, E, F\} \to \{A, B, C, D, E, F\}$ that does not correspond to a symmetry of the regular hexagon in Figure 9.2. *Explain* why it is not a symmetry. ◊

Example 9. Figure 9.3 below shows all symmetries of a rectangle.

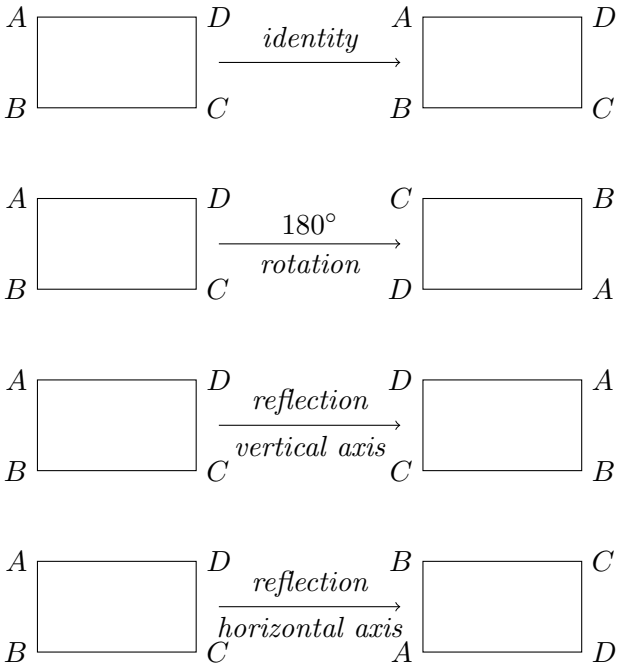


Figure 9.3. Symmetries of a rectangle

♦

Exercise 10.

(a) Explain why a 90° rotation, a 270° rotation, or reflection across a diagonal are not symmetries of the rectangle ABCD.

(b) What subcategory of rectangle would have a 90° rotation, 270° rotation, and a reflection across a diagonal as symmetries?

(c) What rotation does the identity symmetry correspond to?

(d) Write each of the symmetries of a rectangle as a function (use either a table, ordered pairs, arrow diagram, etc.)

◊

9.2 Composition of symmetries

Since the symmetries of a figure are functions, we can do anything with symmetries that we can do with functions–including composition. That is, we can perform two symmetries on a figure back-to-back, and since they are both functions, by definition of function composition the result is a function. In fact, we saw in the Functions chapter that the composition of two bijections is a bijection. So the composition (or net motion) resulting from two symmetries is a bijection. But a bijection of a figure is not necessarily a symmetry. as we showed in Exercise 8 above. This raises the question: is the composition of two symmetries a symmetry? That is: if one symmetry is followed by another on a figure, is the net motion a symmetry? You will investigate this question in the following exercise.

Exercise 11. With reference to the symmetries of a rectangle in Example 9, let r_{180} be the 180° counterclockwise rotation and let s_v be the reflection across the vertical axis. (Note that reflection across the vertical axis is sometimes called "horizontal reflection," since the figure "flips" from left to right. Admittedly this is confusing, but that's what people call it so what can you do?)

(a) Write the function r_{180} in ordered pair notation.

(b) Write the function s_v in ordered pair notation.

(c) Write the function $r_{180} \circ s_v$ in ordered pair notation. Is it a symmetry of the rectangle? If so, then which one?

(d) Write the function $s_v \circ r_{180}$ in ordered pair notation. Is it a symmetry of the rectangle? If so, then which one?

$\Diamond$

At this point let us introduce an alternative notation for symmetries that's easier to write. This notation is called ***tableau form***, and for r_{180} it looks like the following:

$$r_{180} = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

To form these, we simply put the inputs of our function on the top row and their corresponding outputs on the bottom row.

Example 12. For example, since

$$s_v = \{(A, D), (B, C), (C, B), (D, A)\},$$

then the top row of the tableau for s_v would read, "$ABCD$", and the bottom row of the tableau would read, "$DCBA$". Hence

$$s_v = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}.$$

$\blacklozenge$

Example 13. Suppose we wanted to find $r_{180} \circ s_v$ using the tableau forms for r_{180} and s_v above. That is

$$r_{180} \circ s_v = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} \circ \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = ?$$

To see how this works, let's "follow" each possible input (A, B, C, D) as we put it into the composition. Remember that the composition of functions works right to left; we are first reflecting the rectangle and then rotating it. So starting from the right,

- s_v takes $A \to D$, and r_{180} takes $D \to B$. Therefore $r_{180} \circ f_h$ takes $A \to B$; i.e. $(r_{180} \circ s_v)(A) = B$.

- s_v takes $B \to C$, and r_{180} takes $C \to A$; therefore $r_{180} \circ s_v$ takes $B \to A$
- s_v takes $C \to B$, and r_{180} takes $B \to D$; therefore $r_{180} \circ s_v$ takes $C \to D$
- s_v takes $D \to A$, and r_{180} takes $A \to C$; therefore $r_{180} \circ s_v$ takes $D \to C$

Figure 9.4 shows this process using tableaus. If you think about it, it's really just a variation on an arrow diagram.

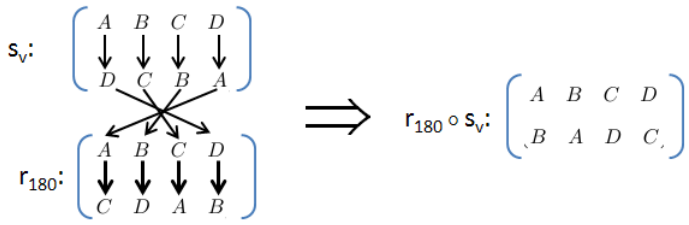


Figure 9.4. Composition of symmetries using tableaus.

In summary we have

$$r_{180} \circ s_v = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} \circ \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$$

♦

Exercise 14.

(a) Write s_h in tableau form, where s_h is reflection across the horizontal axis. (Note s_h is sometimes referred to as "vertical reflection,", since the two reflected halves are stacked on top of each other.)

(b) Does $r_{180} \circ s_v = s_h$?

(c) Compute $s_h \circ s_v$. Is this a symmetry? If so, which one?

(d) Compute $s_v \circ r_{180}$. Is this a symmetry? If so, which one?

◊

Exercises 14 and 11 seem to indicate that the composition of two symmetries of a figure is a symmetry of the figure. We can actually prove that this is always true.

Proposition 15. Suppose f and g are both symmetries of a figure. Then $f \circ g$ is itself a symmetry of the same figure.

PROOF. Recall that composition works from right to left. Since g is a symmetry, g takes the points of the figure and rearranges them so that the angles and distances of points in the figure are preserved. The symmetry f then takes the points of this preserved figure and moves them in such a way that the angles, and distances of points in the figure are preserved. Hence the net result of $f \circ g$ preserves angles and distances between points in the figure. Therefore by definition, $f \circ g$ is a symmetry of the figure. □

Exercise 16. With reference to the hexagon in Figure 9.2, for the symmetries f and g in parts (a)-(d) below:

(i) Write the symmetries f and g in tableau form.

(ii) Compute $f \circ g$ and $g \circ f$, expressing your answers in tableau form.

(iii) Describe the symmetries that correspond to $f \circ g$ and $g \circ f$, respectively.

Note id denotes the identity symmetry, that is the symmetry that leaves all points unchanged.

(a) $f =$ rotation by $240°, g =$ rotation by $120°$

(b) $f = \mathsf{id}, g =$ rotation by $120°$

(c) $f =$rotation by $240°, g =$reflection across the line BE

(d) $f =$rotation by $180°, g =$reflection across the line CF

◊

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Table 9.1: Composition of the symmetries of an equilateral triangle

9.3 Do the symmetries of an object form a group?

With reference to the set of symmetries of a particular figure, Proposition 15 tell us that this set is closed under the operation of composition. Given this fact, the next natural inquiry is to see if this set of symmetries forms a group under composition. Let's look first at a particular example to see if it works.

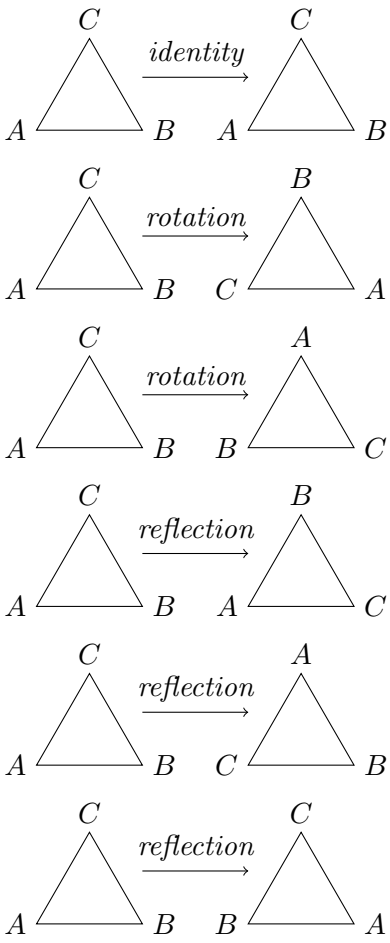
Example 17. Figure 9.5 shows all the symmetries of an equilateral triangle: id is the identity ; ρ_1 is the 120° counterclockwise rotation; ρ_2 is the 240° counterclockwise rotation; μ_1 is the reflection across the median through A; μ_2 is the reflection across the median through B; and μ_3 is the reflection across the median through C.

♦

Table 9.1 displays all possible compositions of the symmetries shown in Figure 9.5. The table is arranged like a multiplication table: for example, the table entry in the row marked "ρ_1" and the column marked "μ_1" corresponds to the composition $\rho_1 \circ \mu_1$. From now on we will refer to all such tables as ***Cayley tables***, regardless of the operation being represented (addition, multiplication, composition, ...)

Remark 18. NOTE it is very easy to get mixed up with Cayley tables for the composition operation. When *looking up* the value of $f \circ g$, you use the row headings for f and the column headings for g, but when *computing* $f \circ g$, it is g that is applied first and then f. △

Exercise 19. Verify the following entries in Table 9.1 by (i) writing the symmetries in tableau form and (ii) computing the composition directly.



$$\mathsf{id} = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Figure 9.5. Symmetries of an Equilateral Triangle

(a) Row 2, column 4

(b) Row 4, column 2

(c) Row 3, column 6

(d) Row 6, column 3

◊

Exercise 20. Use Table 9.1 to answer the following questions.

(a) Explain why Table 9.1 shows that id satisfies the definition of an identity element.

(b) Does every element in S have an inverse? List the inverses for each symmetry that has an inverse.

(c) Explain why Table 9.1 shows that composition is *not* commutative.

◊

So far so good. The composition operation on S has closure, an identity, and inverses for each element. There is one more group property left to check – the associative property. It is difficult to check this property on the Cayley table of S; we would have to prove it for all 3-symmetry combinations in S, which would be a bit exhausting.[3] However, luckily we can prove the symmetries of any figure are associative in general.

Proposition 21. The set of symmetries S of any figure under composition is associative.

PROOF. By definition, we know any symmetry of a figure is a function. From the Functions chapter, we know that composition of functions is associative. Therefore for any three symmetries $s_1, s_2, s_3 \in S$, by the associative property of functions,

$$\big(s_1 \circ s_2\big) \circ s_3 = s_1 \circ \big(s_2 \circ s_3\big).$$

[3] In mathematics, there is a type of proof called "proof by exhaustion," but this is typically a last resort. One famous mathematician (George Polya) once said, "Mathematics is being lazy. Mathematics is letting the principles do the work for you so that you do not have to do the work for yourself."

Therefore S is associative under composition. □

Tada! The set of symmetries of an equilateral triangle are indeed a group under function composition.

We've managed to prove this for one example; what about for the set of symmetries of any figure? Could we prove the set of symmetries of any figure are a group under composition? We've already proved the closure and associative properties hold for any figure (Propositons 21 and 15). Now what about the identity and existence of inverses? We could create Cayley tables for the infinite number of figures, but we have better things to do. So let's prove these properties generally.

Proposition 22. The set of symmetries S of any figure has an identity.

PROOF. By the definition of a symmetry, the "non-movement" of a figure is a symmetry: it corresponds to the identity function id. Then for any symmetry $s \in S$, using results from the Functions chapter we have

$$\mathsf{id} \circ s = s \circ \mathsf{id} = s$$

So by the definition of identity, id is the identity of S. □

Proposition 23. All elements of the set S of symmetries of any figure have inverses.

PROOF. Given a symmetry $s \in S$, by definition s is a bijection. In the Functions chapter, we showed that every bijection has an inverse s^{-1}. It remains to show that s^{-1} is itself a symmetry. This means that we have to show:

(i) s^{-1} leaves distances unchanged between points in the figure;

(ii) s^{-1} leaves angles unchanged between points in the figure;

(iii) s^{-1} leaves the appearance of the figure unchanged.

These three items are proved as follows:

(i) This proof is similar to (ii), and we leave it as an exercise.

(ii) We show that s^{-1} leaves angles and distances between points unchanged as follows:

- Choose any three points A, B, C in the figure, and let $A' = s^{-1}(A), B' = s^{-1}(B), C' = s^{-1}(C)$.
- By the definition of inverse, it follows that $s(A') = A, s(B') = B, s(C') = C$.
- Since s is a symmetry, it follows that $\angle A'B'C' = \angle ABC$.
- Since A, B, C were arbitrary points in the figure, we have shown that s^{-1} leaves angles between points unchanged.

(iii) In the Functions chapter, we showed that s^{-1} is also a bijection. Hence it leaves the appearance of the figure unchanged.

□

Exercise 24. Write out the proof of Proposition 23 part (i). (*Hint*) ◊

Hence we've shown it! By Propositions 15, 21, 22, and 23, we've proved that the set of symmetries of *any* figure is a group under function composition.

Exercise 25.

(a) Write the Cayley table for the symmetries of a rectangle.

(b) List the inverses of each symmetry of the symmetries of a rectangle.

◊

Exercise 26.

(a) Describe all symmetries of a square (for example: "reflection about the vertical axis " describes one symmetry: give similar descriptions of all symmetries of the square)

(b) Label the square's vertices as A, B, C, D, and write down each symmetry in tableau form. As in Figure 9.5, denote each symmetry by a variable (you may use $\rho_1, \rho_2, \ldots$ for the rotations and $\mu_1, \mu_2, \ldots$ for the reflections).

(c) Write the Cayley table for the symmetries of a square.

(d) For each symmetry of a square, list its inverse.

$\Diamond$

Exercise 27. With reference to the logos in Figure 9.6:

(a) For which logos do the set of symmetries include all symmetries of the equilateral triangle?

(b) For which logos do the set of symmetries include all symmetries of the rectangle?

(c) For which logos do the set of symmetries include all symmetries of the hexagon?

(d) For which logos do the set of symmetries a proper subset of the set of all symmetries as the rectangle?

(e) Give two logos such that all symmetries of the first logo are also symmetries of the second logo.

(f) Which logos have no symmetries except for the identityl?

$\Diamond$

9.4 The dihedral groups

We have investigated the symmetries of equilateral triangle, square, and regular hexagon. But what about other regular polygons: heptagon, octagon, nonagon, decagon, and so on? [4] In this section, we will take a general look at the symmetries of n-sided regular polygons.

[4] Recall from geometry that a *regular* polygon has all sides equal and all angles equal

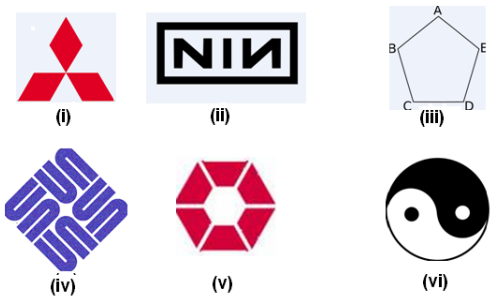


Figure 9.6. Logos for Exercise 27

We already know that the symmetries of an n-sided regular polygon will form a group. We define the ***nth dihedral group*** to be the group of symmetries of a regular n-gon. [5] We will denote this group by D_n.

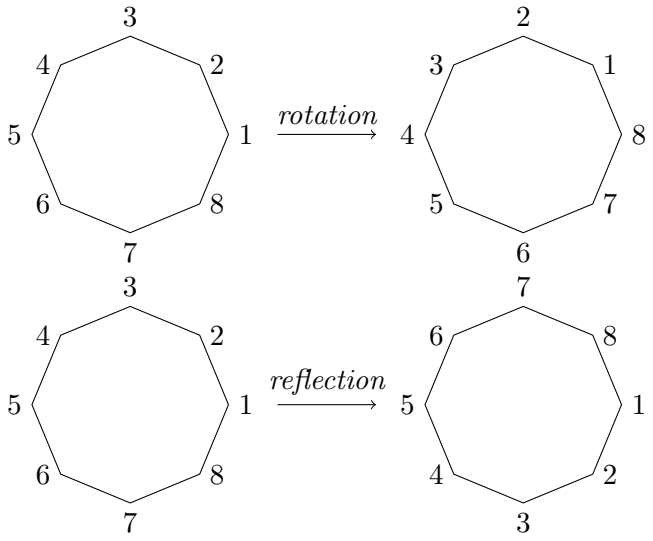


Figure 9.7. Rotations and reflections of a regular n-gon

Let us try to count the number of elements of D_n . We can number the vertices of a regular n-gon by $1, 2, \ldots, n$ (Figure 9.7). Any symmetry will

[5] Just a reminder that "symmetry" here means a rigid motion that leaves the n-sided polygon invariant.

move the n-gon so that each vertex is replaced by another vertex. Notice that any vertex can replace the first vertex: so there are exactly n choices to replace the first vertex. Suppose we replace vertex 1 by vertex k: then vertex 2 must be replaced either by vertex $k+1$ or by vertex $k-1$, because these are the only vertices next to vertex k. So for each of the n choices for replacing vertex 1, there are two choices for replacing vertex 2: which makes $2n$ possible choices altogether. If you think about it, you'll see that once the replacements for vertices 1 and 2 are determined, the entire symmetry is fixed (again, because vertices must remain next to each other). We summarize our conclusion in the following proposition.

Proposition 28. The dihedral group, D_n, is a group of order $2n$.

Let us try to characterize these $2n$ elements of the dihedral group D_n.

First, we know that the elements of the dihedral group includes n rotations:

$$\mathsf{id}, \frac{360^\circ}{n}, 2 \cdot \frac{360^\circ}{n}, \ldots, (n-1) \cdot \frac{360^\circ}{n}.$$

We will denote the rotation $360^\circ/n$ by r. Notice that:

- $r \circ r =$ rotation by $2 \cdot \frac{360^\circ}{n}$
- $r \circ r \circ r =$ rotation by $3 \cdot \frac{360^\circ}{n}$

We can generalize this pattern by writing:

$$r^k = \text{ rotation by } k \cdot \tfrac{360^\circ}{n} \quad (k = 1, 2, 3, \ldots),$$

where the notation r^k means that we compose r with itself k times: $r \circ r \ldots \circ r$. We can also continue this pattern with $k = 0$ and write:

$$r^0 = \text{ rotation by } 0 \cdot \tfrac{360^\circ}{n} = \mathsf{id}.$$

We also have

$$r^n = \text{ rotation by } n \cdot \tfrac{360^\circ}{n} = \text{ rotation by } 360^\circ = \mathsf{id},$$

since rotation by 360 degrees is tantamount to not moving the figure at all.

Exercise 29.

(a) Using the above definition of r^k, show that $r^k \circ r^m = r^{m+k}$ for any natural numbers k, m.

(b) Show that $r^k \circ r^{n-k} = r^{n-k} \circ r^k = \mathsf{id}$ for $1 < k < n$.

(c) What does (b) tell us about the inverse of r^k?

$\Diamond$

From the above discussion, it should be clear that the n rotations in D_n can be expressed as:

$$\mathsf{id}, r, r^2, \ldots, r^{n-1},$$

where we have included id since it is "rotation by 0 degrees" (as mentioned above, we could also write id as r^0). This gives us a nice way of characterizing the rotations in D_n. But until now we don't have a nice way of writing the reflections. We'll take care of that now!

We have labeled the vertices of the n-gon as $1, 2, \ldots, n$. In the following discussion, we will use the letter s to denote the reflection that leaves the vertex labeled 1 *fixed*, that is, $s(1) = 1$.[6] Another way of saying the same thing is: the vertex labeled 1 is "fixed by" s.

Exercise 30.

(a) Write the reflection s for the pentagon in tableau form.

(b) How many vertices are fixed by s? What are they?

(c) What is s^2? (Recall that s^2 means the same as $s \circ s$.)

$\Diamond$

Exercise 31.

(a) Write the reflection s for the octagon in tableau form.

(b) How many vertices are fixed by s? What are they?

(c) What is s^2?

[6] In math books you may also find the termi "invariant" instead of "fixed".

$\Diamond$

By generalizing the arguments used in the preceding exercises, it is possible to prove for any n that:

$$s^2 = \mathsf{id}.$$

Now we have already shown there are n distinct rotations. Suppose we follow each of these rotations by the reflection s: that is, consider the set

$$S \equiv \{s \circ \mathsf{id}, s \circ r, s \circ r^2, \ldots, s \circ r^{n-1}\}$$

It appears that S has n elements: but are these elements distinct? The following exercise provides an answer:

Exercise 32. Prove the following proposition by filling in the blanks:

Proposition. If $0 < p, q < n$ and $p \neq q$, then $s \circ r^p$ and $s \circ r^q$ are distinct elements of D_n: that is, $s \circ r^p \neq s \circ r^q$.

PROOF.

- The proof is by contradiction. Given $0 < p, q < n$ and $p \neq q$, and suppose that $s \circ r^p$ $\underline{\quad < 1 > \quad}$ $s \circ r^q$
- Compose both sides of the equation with s, and obtain the equation: $s \circ (s \circ r^p) =$ $\underline{\quad < 2 > \quad}$.
- By the associative property of composition, this can be rewritten: $(s \circ$ $s) \circ$ $\underline{\quad < 3 > \quad}$ $=$ $\underline{\quad < 4 > \quad}$
- Since $s \circ s =$ $\underline{\quad < 5 > \quad}$, this can be rewritten: $\mathsf{id} \circ$ $\underline{\quad < 6 > \quad}$ $=$ $\underline{\quad < 7 > \quad}$.
- Since id is a group identity, we have: $r^p =$ $\underline{\quad < 8 > \quad}$.
- But we have already shown that r^p and r^q are distinct symmetries if $0 < p, q < n$ and $p \neq q$. This is a contradiction.
- Therefore we conclude that our supposition was incorrect, and $s \circ$ r^p $\underline{\quad < 9 > \quad}$ $s \circ r^q$. This completes the proof.

□ ♢

Exercise 33. Prove the following proposition:

Proposition If $0 < q < n$ then s and $s \circ r^q$ are distinct elements of D_n: that is, $s \neq s \circ r^q$. (*Hint*) ♢

Exercise 34. Fill in the blanks to prove that given any integers p, q with $0 < p, q < n$, $s \circ r^p \neq r^q$:

- The proof is by contradiction: so given integers p, q with $0 < p, q < n$, we suppose $\underline{\quad < 1 > \quad}$.
- By multiplying both sides on the *right* by r^{n-p}, we obtain $s \circ r^p \circ \underline{\quad < 2 > \quad} = r^q \circ \underline{\quad < 3 > \quad}$
- By associativity, we have $s \circ \underline{\quad < 4 > \quad} = \underline{\quad < 5 > \quad}$
- Using the fact that $\underline{\quad ¡6¿ \quad} = \mathsf{id}$, we obtain $s = \underline{\quad < 7 > \quad}$
- The left side of this equation is a reflection, and the right side is a $\underline{\quad < 8 > \quad}$, which is a contradiction.
- This contradiction implies that our supposition is incorrect, so given integers p, q with $0 < p, q < n$, we conclude $\underline{\quad < 9 > \quad}$.

♢

The preceding exercises have shown that the rotations and $\{s, s \circ r, s \circ r^2, \ldots, s \circ r^{n-1}\}$ are all distinct elements of D_n. Since there are $2n$ of these symmetries altogether, and since D_n has $2n$ elements, we have proved the following:

Proposition 35. The $2n$ elements of D_n may be listed as:

$$\{\mathsf{id}, r, r^2, \ldots, r^{n-1}, s, s \circ r, s \circ r^2, \ldots, s \circ r^{n-1}\},$$

or alternatively as

$$\{s^j \circ r^k, \quad (j = 0, 1;\ k = 0, 1, \ldots n-1\},$$

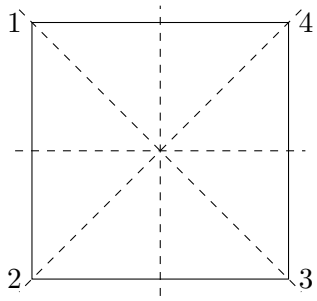


Figure 9.8. Lines of reflection for a square (D_4)

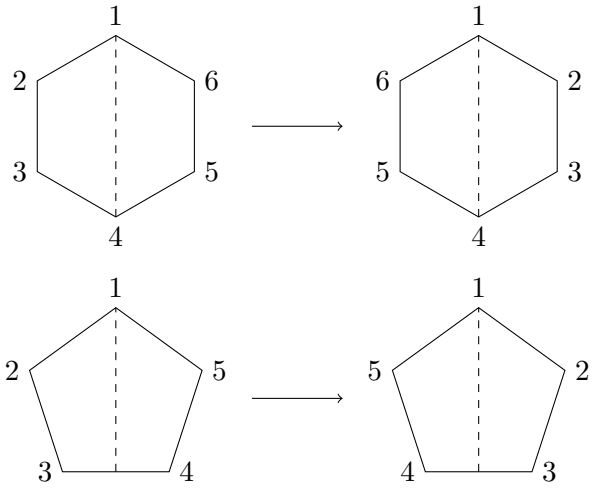


Figure 9.9. Types of reflections of a regular n-gon

where we are using the notation: $s^0 = r^0 = \mathsf{id}$.

There is actually another way to characterize the elements of D_n, as we shall see in the following exercises:

Exercise 36.

(a) List four reflections of the square in tableau form. (*Hint*)

(b) Let μ be any of the reflections in part (a). What is $\mu \circ \mu$?

(c) How many reflections have no fixed vertices?

(d) How many reflections fix exactly one vertex?

(e) How many reflections fix exactly two vertices?

◊

Exercise 37.

(a) List five reflections of the pentagon in tableau form. (*Hint*)

(b) Let μ be any of the reflections in part (a). What is $\mu \circ \mu$?

(c) How many reflections have no fixed vertices?

(d) How many reflections fix exactly one vertex?

(e) How many reflections fix exactly two vertices?

◊

Exercise 38.

(a) List six reflections of the hexagon in tableau form. (*Hint*)

(b) Let μ be any of the reflections in part (a). What is $\mu \circ \mu$?

(c) How many reflections have no fixed vertices?

(d) How many reflections fix exactly one vertex?

(e) How many reflections fix exactly two vertices?

◊

Exercise 39.

(a) Complete the second row of the following tableau that represents the reflection of the nonagon that fixes vertex 4:

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ -- & -- & -- & 4 & -- & -- & -- & -- & -- \end{pmatrix}$$

(b) Complete the second row of the following tableau that represents the reflection of the 10-gon that fixes vertex 4:

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ -- & -- & -- & 4 & -- & -- & -- & -- & -- & -- \end{pmatrix}$$

(c) Complete the second row of the following tableau that represents the reflection of the 10-gon that exchanges vertices 6 and 7:

$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ -- & -- & -- & -- & -- & 7 & 6 & -- & -- & -- \end{pmatrix}$$

(d) What is $\mu_1 \circ \mu_1$? What is $\mu_2 \circ \mu_2$? What is $\mu_3 \circ \mu_3$?

$\Diamond$

The preceding exercises are generalized to arbitrary n in the following proposition. Although we do not give a complete proof, it is reasonable that we can generalize Exercise 37 to all *odd* n-gons, and we can generalize Exercise 38 to all *even* n-gons:

Proposition 40.

- The dihedral group D_n contains n distinct reflections (in addition to n distinct rotations);
- For any reflection $\mu \in D_n$, we have $\mu \circ \mu = \mathsf{id}$.

Exercise 41.

(a) Based on results we've shown, prove that $s \circ r^p$ must be a reflection, for $0 < p < n$.

(b) Using part (a) and other results we've shown, show that $(s \circ r^p) \circ (s \circ r^p) = \mathsf{id}$. (*Hint*)

(c) Using part (b) and composing on the left by $r^{n-p} \circ s$, show that $r^{n-p} \circ s = s \circ r^p$ for $0 < p < n$.

◊

All of our results on dihedral groups can now be summarized in the following proposition:

Proposition 42. Every element of the group D_n, $n \geq 3$, consists of all compositions of the two elements r and s, satisfying the relations:

(a) $r^n = \mathsf{id}$

(b) $s^2 = \mathsf{id}$

(c) $r^p \circ s = s \circ r^{n-p}$ for $0 < p < n$.

Proposition 42 enables us to compute any composition of elements of D_n directly, without the need of tableau form:

Example 43. In D_5, to compute $(s \circ r^3) \circ (s \circ r^4)$ we have (using Proposition 42 and associativity):

$$\begin{aligned}(s \circ r^3) \circ (s \circ r^4) &= s \circ (r^3 \circ s) \circ r^4 \text{ by associativity} \\ &= s \circ (s \circ r^2) \circ r^4 \text{ by Prop. 42(c)} \\ &= (s \circ s) \circ r \circ r^5 \text{ by associativity} \\ &= \mathsf{id} \circ r \circ \mathsf{id} \text{ by Prop. 42(a) and (b)} \\ &= r\end{aligned}$$

⧫

In fact, following the method of Example43 it is possible to derive a general formula for the composition of two reflections. Such a formula may be very useful in certain situations: for instance, in the following exercises.

Exercise 44. Using only associativity and Proposition 42, complete the entire Cayley table for D_4. Remember, there is a row and a column for each element of D_4. List the elements as indicated in Proposition 35. You don't need to show all your computations. *(But don't use tableau form–no cheating!)* ◊

Exercise 45. Using only associativity and Proposition 42, complete the entire Cayley table for D_5. You don't need to show all your computations. *(But don't use tableau form – no cheating!)* ◊

9.5 For further investigation

In this chapter, we have looked at the groups involved with symmetries of plane figures. But really, there is no need to restrict ourselves to two dimensions. Three-dimensional regular figures (such as the tetrahedron, cube, icosahedron, and dodecahedron) also have symmetry groups associated with them. These symmetry groups also make for fascinating study.

Neither do we need to restrict ourselves to symmetries of objects. The symmetries of *patterns* also play an important role in art and architecture. For instance, every possible regular repeating pattern that can be put on wallpaper (or used as floor tiling) is associated with a symmetry group. It turns out that there are exactly 17 of these symmetry groups: they are called the *wallpaper groups*. For an excellent elementary reference on this subject, I highly recommend "17 Plane Symmetry Groups" by Anna Nelson, Holli Newman, and Molly Shipley, available on the web (as of January 2014) at http://caicedoteaching.files.wordpress.com/2012/05/nelson-newman-shipley.pdf.

In physics, symmetry groups are used to describe the regular three-dimensional patterns associated with crystals. Many references for the crystallographic groups can also be found on the web: one I recommend is "Crystallographic Point Groups (short review)" by Mois I. Aroyo, available on the web at: http://www.crystallography.fr/mathcryst/pdf/uberlandia/Aroyo_Point.pdf.

9.6 An unexplained miracle

It is good for us to step back for a moment and take stock of what we've accomplished so far. We'll begin with some exercises.

Exercise 46.

(a) Give the Cayley table for the integers mod 4 under addition.

(b) Give the Cayley table for the four rotations of the square (4-sided polygon). You may use r to denote rotation by 90 degrees, so that the rotations will be $\{\mathsf{id}, r, r^2, r^3\}$.

(c) Give the Cayley table for the four complex $4'th$ roots of unity. You may use z to denote $\mathrm{cis}(\pi/2)$ so that the roots will be $\{1, z, z^2, z^3\}$.

(d) Do you see any connection between your answers to (a), (b), and (c) above?

◊

Exercise 47.

(a) Consider equivalence mod 5 as an equivalence relation on the natural numbers. Write down the 5 equivalence classes for this equivalence relation. (*Hint*)

(b) Consider the group D_5, and let $r \in D_5$ be rotation by 72 degrees. Define an equivalence relation $\sim$ on the natural numbers as follows: we say $n \sim m$ if $r^n = r^m$. (For instance, $3 \sim 8$ since rotation by $3 \cdot 72 = 216$ degrees is the same as rotation by $8 \cdot 72 = 576 = 216 + 360$ degrees). Write down the 5 equivalence classes for the equivalence relation .

◊

These exercises show a deep connection between three extremely diverse concepts that arose from three totally different fields of study:

- Arithmetic mod n, which first arose from the study of the natural numbers and their divisibility properties;
- The nth complex roots of unity, a concept that arose from the study of roots of polynomials.
- The rotations of a regular n-gon, which is a purely geometrical phenomenon.

We express the amazing similarity between these three diverse concepts by saying that they are all described by the "same" group. (The technical term for this is "isomorphism": we will study this concept in detail in Chapter 15.)

Take a moment to appreciate how incredible this is. How is it that three concepts with totally different backgrounds and completely different applications end up being described in exactly the same way?

But the wonders do not stop there. It turns out that an infinite version of this same group is an important part of the so-called Standard Model of

quantum physics, that is used to explain the existence of particles such as electrons, protons, and neutrons. How is it that a mathematical structure introduced by an 18^{th} century mathematician [7] to study integer division could end up influencing the theory of elementary particles that were not even dreamed of in the 18^{th} century?

This mystical unity of description across widely different phenomena says something very profound about the universe. Galileo [8] expressed it this way: "Mathematics is the language with which God has written the universe." When Galileo said this, his mathematics consisted of little more than what today we would call "high school algebra" – he had not an inkling of abstract algebra. But what Galileo expressed based on his limited mathematics has turned been fulfilled with a vengeance by abstract algebra.

Physicist Eugene Paul Wigner[9] won the 1963 Nobel Prize in Physics, in part because of his application of the theory of groups to quantum physics. In 1960 Wigner wrote a famous paper called "the Unreasonable Effectiveness of Mathematics in the Natural Sciences," [10] in which he states: "The miracle of the appropriateness of the language of mathematics for the formulation of the laws of physics is a wonderful gift which we neither understand nor deserve." Until now, apparently no physicist or mathematician has offered a satisfactory explanation for Wigner's "miracle".

[7] This mathematician was Leonhard Euler (1707-1783). The integers mod n were further developed by Carl Friedrich Gauss (1777-1855).

[8] Galileo Galilei, Italian physicist (1564-1642), whose work on the motion of objects was foundational to the later work of Isaac Newton.

[9] 1902-1995

[10] The paper can be found at: http://www.dartmouth.edu/∼matc/MathDrama/reading/Wigner.html

10

Permutations

> "For the real environment is altogether too big, too complex, and too fleeting for direct acquaintance. We are not equipped to deal with so much subtlety, so much variety, so many permutations and combinations. And although we have to act in that environment, we have to reconstruct it on a simpler model before we can manage it."
>
> (Source: Walter Lippmann, Pulitzer prize-winning journalist)

We mentioned at the beginning of the "Functions" chapter that we would be interested in functions on finite sets. In this chapter we will investigate the gory details of one-to-one onto functions whose domain and range are the same finite set. Until now we have looked at functions as mappings that take set elements to other set elements. In this chapter, we will begin to consider functions as elements in their own right. This new point of view will culminate in the realization that *all* finite groups are in some sense groups of functions (if you don't understand this yet, don't worry–you will by the end of the chapter). [1]

[1] Thanks to Tom Judson for material used in this chapter.

10.1 Introduction to permutations

In Chapter 9 we saw that all symmetries are bijections whose domain and codomain were the same. Thus symmetries are special cases of *permutations*, which are defined mathematically as follows.

Definition 1. A bijection whose domain and codomain are equal is called a ***permutation***. The set of all bijections from a finite set X to itself is called the ***set of permutations on*** X and is denoted as S_X. △

Example 2. Let us recall for a moment the equilateral triangle $\triangle ABC$ from the Symmetries chapter. Let T be the set of vertices of $\triangle ABC$; i.e. $T = \{A, B, C\}$. We may list the permutations of T as follows. For input A, we have 3 possible outputs; then for B we would have two possible outputs (to keep the one-to-one property of each combination); and finally for C only one possible output. Therefore there are $3 \cdot 2 \cdot 1 = 6$ permutations of T. Below are the six permutations in S_T:

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$
$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

♦

Which of these permutations are symmetries of the equilateral triangle? In the Symmetries chapter we saw that they all are: so in this case the set of symmetries on T is equal to S_T.

Now suppose instead we label the vertices of an *isosceles* triangle as A, B, C, and let T represent these vertices. In this case, S_T is the same as before: it doesn't matter what arrangement or position the vertices are in, or even if A, B, and C are vertices at all. The permutations depend only on the set T, and are oblivious to whether or not they correspond to the vertices of some figure.

But what about the symmetries of an isosceles triangle? It turns out that an isosceles triangle has only two symmetries (see exercise below). So the set of symmetries on T is a subset of S_T, but not the whole set.

Exercise 3. Suppose that the two congruent sides of triangle ABC are $\overline{AB}$ and $\overline{BC}$). Give the two symmetries, in tableau form. ◊

Exercise 4. Suppose T is used to represent any three-sided figure. Which permutation(s) does the set of symmetries of T always contain? ◊

Exercise 5. Suppose $X = \{A, B, C, D\}$.

(a) How many permutations are there on X?

(b) List S_X.

(c) List the elements in S_X that are not symmetries of the square.

(d) What additional elements in S_X are not symmetries of the rectangle?

◊

In fact, it's obvious to see that *any* symmetry is a permutation, since a symmetry is by definition a bijection from a finite set of points to itself. But as we've seen in Exercises 3, 4, 5 (as well as Exercise 8 from the Symmetries chapter), *not* all permutations (bijections) correspond to a symmetry. Given a set X then that represents a figure, the set of symmetries from $X \to X$ is a subset of S_X.

10.2 Permutation groups and other generalizations

We saw in the Symmetries chapter that the set of symmetries of any figure form a group under the operation of function composition. Since we've already seen that permutations are closely related to symmetries, this naturally leads to the question: is S_X a group under function composition? Fortunately, this time the answer is easier to prove.

Proposition 6. Given any set X, S_X is a group under function composition.

PROOF.

- First then, if $f, g \in S_X$, then $f \circ g$ would be, by definition of composition, a function from $X \to X$. Further, since it is a composition of two bijections, $f \circ g$ would be a bijection (proved in Functions chapter). Therefore by definition $f \circ g$ is permutation from $X \to X$. In other words $f \circ g \in S_X$. So S_X is closed under function composition.
- Second, the identity of S_X is just the permutation that sends every element of X to itself (We will call this permutation id, just like we did with symmetries.).
- Third, if $f \in S_X$, then by definition f is a bijection; hence from the Inverse section of the Functions chapter we know f has an inverse f^{-1} from $X \to X$ that is also a bijection. Hence $f^{-1} \in S_X$. Therefore every permutation in S_X has an inverse.
- Finally, composition of functions is associative, which makes the group operation associative.

Hence S_X is a group under function composition. □

10.2.1 The symmetric group of n letters

We can label the vertices of a triangle as A, B, C or $1, 2, 3$ or $\mathsf{apple}, \mathsf{pear}, \mathsf{cherry}$ or whatever, without changing the triangle. No matter how we label the triangle, the symmetries of the triangle will be the "same" in some sense (although we write them down differently).

Since symmetries are special cases of permutations, this motivates us to investigate the effect of relabeling on permutations in general.

For starters, we'll look at a simple example. Let $X = \{A, B, C, D\}$ and $Y = \{1, 2, 3, 4\}$. Suppose

$$\mu = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}, \sigma = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Is $\mu = \tau$? Technically no, because they their domain/codomains are different, yet we can clearly see that they are somehow equivalent. But how do we express this equivalence?

Suppose we start with the tableau for μ. We cross out every 'A' in the tableau and replace with '1'. Similarly, we replace B, C, D with $2, 3, 4$ respectively. Then what we end up with is exactly τ. In other words, performing a "face-lift" on μ gives τ. Therefore μ and τ are equivalent, as are σ and ρ.

Exercise 7.

(a) Write $\mu \circ \sigma$ in tableau form.

(b) Write $\tau \circ \rho$ in tableau form.

(c) Is $\mu \circ \sigma$ equivalent to $\tau \circ \rho$? *Explain* your answer.

(d) Is $\sigma \circ \mu$ equivalent to $\rho \circ \tau$? *Explain* your answer.

$\Diamond$

Let's summarize our findings so far:

- The *sets* S_X and S_Y are equivalent in the following sense: for each element of S_X we can find an equivalent element of S_Y by replacing A, B, C, D with $1, 2, 3, 4$.
- Further, as we saw in the exercises, the composition of two elements in S_X is equivalent to the composition of the two equivalent elements in S_Y. So we can say that composition acts the "same" on both sets.

So far we have only looked at sets with four elements. Now it's time to generalize these results to sets of any size. First, some notation:

Notation 8. The ***order of a set*** Y is the number of elements of Y, and is written as $|Y|$. [2] $\triangle$

[2] You're probably used to seeing $|\ldots|$ as representing absolute value. Of course a set is not a number, so it has no absolute value. We use $|Y|$ to denote order because it's a measure of the *size* of set Y, just as the absolute value of a number is the "size" of the number.

Now let $X = \{1, 2, \ldots, n\}$, and consider any set Y with $|Y| = n$. We could do a similar "face-lifting" as above to show that $S_X \equiv S_Y$. So the group S_X is equivalent to the permutations of *any* set of n elements.

Notation 9. Let $X = \{1, 2, \ldots, n\}$. Instead of writing S_X, we write S_n. S_n is called the ***symmetric group on*** n ***letters***. △

10.2.2 Isomorphic groups

At the end of the Symmetries chapter, we compared the groups $\mathbb{Z}_n$, the n rotations of a regular n-gon, and the n^{th} roots of unity. We saw that, as long as you made a suitable pairing (bijection) between the elements of any two of these sets, then their Cayley tables were exactly the same.

We've just seen the very same thing for S_n. The above statement that "the composition of two elements in S_X is equivalent to the composition of the two equivalent elements in S_Y" is the same thing as saying that the Cayley table entries are equivalent between the two groups.

This "equivalence of groups" is one of the premier concepts in abstract algebra, almost as important as the concept of a group itself. When two groups are equivalent like this, we say that they are ***isomorphic groups***; we also say that the bijection that causes the groups to be equivalent is an ***isomorphism***. We will see in a later chapter how to show in general that two groups are isomorphic; but for now, forming the groups' Cayley Tables and seeing if you can match elements to make the tables the same is a very good strategy.

Exercise 10. Let $W = \{G, H\}$ and $Z = \{J, K\}$.

(a) Write the Cayley Tables for S_W and S_Z. It would be helpful to write the entries of S_W and S_Z in tableau form.

(b) Give a bijection from W to Z, and the corresponding bijection from S_W to S_Z, that would show S_W is isomorphic to S_Z. (Remember that a bijection can be thought of as a "relabeling" of elements of W as elements of Z.)

(c) *How many possible bijections from W to Z give rise to isomorphisms from S_W to S_Z?

$\Diamond$

Exercise 11. Let $X = \{A, B, C\}$ and $Y = \{M, N, P\}$.

(a) Write the Cayley Tables for S_X and S_Y

(b) Give a bijection from X to Y, and the corresponding bijection from S_X to S_Y, that would show S_X is isomorphic to S_Y.

(c) *How many possible bijections from X to Y produce isomorphisms from S_X to S_Y?

(d) *Now let $X = \{A, B, \ldots M\}$ and $Y = \{N, O, \ldots Z\}$. How many different bijections from X to Y produce isomorphsims from S_X to S_Y?

$\Diamond$

10.2.3 Subgroups and permutation groups

Let's summarize this section so far. The permutations on a set X of n elements is a group under function composition (denoted by S_n). Further, for any figure with n sides, the symmetries of that figure is a subset of S_n containing at least the identity permutation, and that subset is itself a group under function composition. This example motivates the following definition.

Definition 12. A subset of a group G that is itself a group under the same operation as G is called a ***subgroup*** of G. $\triangle$

The notion of subgroup is a key concept in abstract algebra, which will be used throughout the rest of the book.

Example 13. From the above definition of subgroup it follows that:

- The symmetries of a rectangle are a subgroup of S_4.
- The symmetries of an isosceles triangle are a subgroup of S_3.
- D_5 is a subgroup of S_5.

- The permutations of $\{1,2,3\}$ are a subgroup of the permutations of $\{1,2,3,4\}$. Hence S_3 is a subgroup of S_4. By the same token, S_m can be considered as a subgroup of S_n whenever $m < n$.

♦

Definition 14. A subgroup of S_n is called a ***permutation group***. △

Exercise 15. Consider the subset G of S_5 consisting of the identity permutation id and the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$
$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

(a) Write the Cayley table for G (Label your rows and columns as: $\mathsf{id}, \sigma, \tau, \mu$).

(b) Use the Cayley table to explain whether G is a subgroup of S_5 or not.

Remember: you don't need to show the associative property, since function composition is associative.

◊

Exercise 16. Consider the subset G of S_4 consisting of the identity permutation id and the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$
$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

(a) Write the Cayley table for G (Label your rows and columns as: $\mathsf{id}, \sigma, \tau, \mu$).

(b) Use the Cayley table to explain whether or not G is a subgroup of S_4.

$\Diamond$

As the example shows, a permutation group need not comprise all symmetries of a figure or all rearrangements of a set. Many permutation groups have no evident practical interpretation whatsoever. Nonetheless they are still useful, because as we shall see they can be used to characterize the groups that contain them.

10.3 Cycle notation

10.3.1 Tableaus and cycles

In the Symmetries chapter, we introduced tableau notation to deal with bijections because of its brevity and ease of use for function composition. But as you may have noticed in the last section, even tableaus can become cumbersome to work with. To work effectively with permutation groups, we need a more streamlined method of writing down and manipulating permutations. This method is known as cycle notation.

Example 17. Suppose $\rho \in S_6$ and $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$. Then

$$\rho(1) = 2, \rho(2) = 3, \rho(3) = 4, \rho(4) = 5, \rho(5) = 6, \text{ and } \rho(6) = 1$$

A shorter way to represent this is

$$1 \to 2, 2 \to 3, 3 \to 4, 4 \to 5, 5 \to 6 \text{ and } 6 \to 1.$$

We can visualize this as a "wheel", as shown in Figure 10.1

We shall write this trail of inputs and outputs as (123456); and rather than "wheel", we call this a ***cycle*** Reading the cycle from left to right indicates that 1 goes to 2, 2 goes to 3, ..., and the 6 at the end goes back to 1.

Exercise 18. Show that (123456) = (345612) by drawing a figure similar to Figure 10.1 for each cycle. $\Diamond$

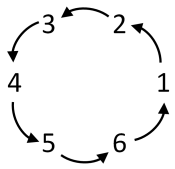


Figure 10.1. Cycle representation of the permutation (123456).

Exercise 19. Show that (123456) and (234561) both have the same tableau (so they are in fact the same permutation). ◊

From the previous two exercises, it is clear that there are many ways to write the same cycle: we can begin with any element we ant, and work our way around until we get back to the same element. To avoid possible confusion, from now on we will follow the convention of starting the cycle with the "smallest" or "first" element of the domain.

For this particular permutation, since our cycle contains all the inputs in the domain of ρ it represents the whole function, because it gives us the outputs for every input. Therefore in cycle notation,

$$\rho = (123456)$$

⧫

Exercise 20. Write the following permutation of S_6 in cycle notation:

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{pmatrix}.$$

◊

Exercise 21. Given the permutation in S_6 $\mu = (152634)$:

(a) Write μ in tableau form.

(b) Write μ as a figure similar to Figure 10.1

◊

Exercise 22. Given the permutation in S_6 $\mu = (165432)$:

(a) Write μ in tableau form.

(b) Write μ as a figure similar to Figure 10.1

(c) Compare your answer to (b) with Figure 10.1 of $\rho = (123456)$. Explain the difference between μ and ρ.

$\Diamond$

Definition 23. The ***length*** of a cycle is how many elements the cycle contains; i.e. how many elements are in the parentheses. Formally,

$$\text{if } (a_1, a_2, \ldots, a_n) \text{ is a cycle, then the length of } (a_1, a_2, \ldots, a_n) = n.$$

$\triangle$

For example, the permutation ρ in Example 17 above is represented by a cycle of length six.

Remark 24. Notice how we have used the notation a_j to indicate arbitrary elements in a cycle. This is a common practice in abstract algebra. $\triangle$

Now not all permutations in S_6 correspond to a cycle of length six. For instance:

Example 25. Suppose $\tau \in S_6$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$. Then

- $1 \to 1$, which means that 1 "stays put." So we don't use 1.
- $2 \to 4$, $4 \to 3$, and $3 \to 2$; so we have (243).
- Finally, $5 \to 5$ and $6 \to 6$; so they also stay put.

Hence

$$\tau = (243)$$

$\blacklozenge$

Based on the procedure in the previous example then, how would we represent the identity permutation on a set of n elements? All the elements stay put, so technically id would equal the "empty cycle". Some references

in fact use "()" to denote the identity: but in this book we will always denote the identity permutation by id as a reminder that this is in fact the group's identity element.

Warning Cycle notation does not indicate the domain of the permutation.

For instance, the permutation (243) in Example 25 had domain $\{1, 2, 3, 4, 5, 6\}$, but (243) could also refer to a permutation on the domain $\{1, 2, 3, 4\}$. When working with permutations in cycle notation, make sure you know what the domain is. (In most cases, it's clearly specified by the context.) ◊

Exercise 26. Write each of the following permutations in S_7 in tableau form.

(a) $\omega = (243)$

(b) $\omega = (2365)$

(c) $\omega = (14257)$

◊

Exercise 27. Draw a figure similar to Figure 10.1 depicting each of the following permutations in S_5.

(a) $\sigma = (25)$

(b) $\sigma = (135)$

(c) $\sigma = (1342)$

◊

A final question that may come to mind is, Do all permutation correspond to some cycle? Certainly, as we've seen, all cycles correspond to some permutation in S_n. However, can all permutations in S_n be represented as a cycle? We will take the next several parts of this section to explore this question.

10.3.2 Composition (a.k.a. product) of cycles

Since cycles represent permutations, they can be composed together. If we change the cycles to tableaus, we know how to compose them. Now let's figure out how to compose them using the cycles themselves.

Notation 28. Given permutations σ and τ, instead of writing $\sigma \circ \tau$ we write the shorthand notation: $\sigma\tau$. Furthermore, instead of calling this the composition of σ and τ, we refer to it as the ***product*** of σ and τ. [3] △

Example 29. Suppose we want to form the product (that is, composition) $\sigma\tau$, where $\sigma, \tau \in S_6$ and $\sigma = (1532), \tau = (126)$.

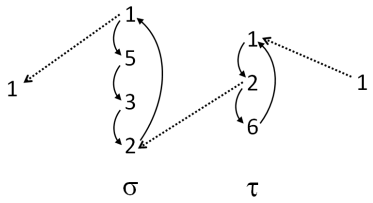


Figure 10.2. Product of cycles σ and τ, showing the derivation of $\sigma\tau(1) = 1$.

Figure 10.2 provides a visual representation of how the product $\sigma\tau$ acts on 1. Remember that we operate from right to left, so the figure shows '1' coming in from the right. The action of τ takes 1 to 2. (For convenience we have "flattened" the permutations τ and σ, so they no longer appear as circles.) Then we pass over to σ, which takes 2 to 1. The final result is 1: therefore $\sigma(\tau(1)) = 1$.

Evidently 1 remains unchanged by the permutation, so let's look at what happens to 2. We see this in Figure 10.3. First, τ moves 2 to 6. Moving on to σ, we find that σ leaves the 6 unchanged. The result is that $\sigma(\tau(2)) = 6$.

We have seen that $\sigma\tau$ takes 2 to 6: so now let's see where $\sigma\tau$ takes 6. (Perhaps you can see that we're trying to build a cycle here.) The top part of Figure 10.4 uses the same process to show the result: $\sigma(\tau(6)) = 5$. The

[3] Once again we see mathematicians' annoying habit of reusing familiar terms to mean something new in a different contexts. In this case, the "product" of permutations has nothing at all to do with multiplication.

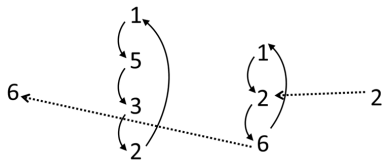


Figure 10.3. Product of cycles σ and τ (continued), showing $\sigma\tau(2) = 6$.

middle part of Figure 10.4 shows that $\sigma(\tau(5)) = 3$; and the bottom part of Figure 10.4 shows that $\sigma(\tau(3)) = 2$. We already know that $\sigma(\tau(2)) = 6$, so we have closed out our cycle. We have shown $2 \to 6 \to 5 \to 3 \to 2$, which amounts to the cycle: (2653).

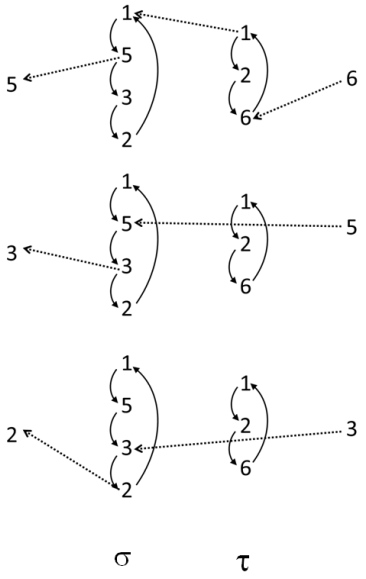


Figure 10.4. Product of cycles σ and τ (continued), showing $6 \to 5 \to 3 \to 2$.

So far 4 is unaccounted for: but a quick inspection of Figure 10.4 shows that 4 is not affected by either τ or σ. So the entire action of τ followed by σ is summarized by the cycle (2653), meaning that we can write: $\sigma\tau =$ (2653). ♦

Exercise 30. Using the same permutations σ and τ as above:

(a) Write the product $\tau\sigma$ in cycle notation.

(b) By comparing your results for $\sigma\tau$ and $\tau\sigma$, fill in the blank in the following statement: In general, permutations do not _____.

$\Diamond$

Example 31. At the beginning it may be helpful to draw a picture, as in the previous example. However, once you gain experience, you should be able to find the product of cycles directly. Consider the product $\sigma\tau$ where $\sigma = (AEDBF)$ and $\tau = (ABDFE)$. Then we have:

- τ takes $A \to B$ and σ takes $B \to$F; hence $\sigma\tau$ takes $A \to F$.
- τ takes $F \to E$, and σ takes $E \to D$; hence $\sigma\tau$ takes $F \to D$.
- τ takes $D \to F$, and σ takes $F \to A$; hence $\sigma\tau$ takes $D \to A$.

We have finished a cycle: (AFD). Let us check where the other letters B, C, E go:

- τ takes $B \to D$, and σ takes $D \to B$; hence $\sigma\tau$ takes $B \to B$.
- Neither τ nor σ affects C; hence $\sigma\tau$ takes $C \to C$.
- τ takes $E \to A$, and σ takes $A \to E$; hence $\sigma\tau$ takes $E \to E$.

Since B, C, E are unaffected by $\sigma\tau$, we conclude that $\sigma\tau = (AFD)$. $\blacklozenge$

Exercise 32. Given that $\delta = (135)$, $\sigma = (347)$, and $\rho = (567)$ are permutations in S_7, compute the following:

(a) $\delta\sigma$ (c) $\delta\rho$ (e) $\sigma\rho$

(b) $\sigma\delta$ (d) $\rho\delta$ (f) $\rho\sigma$

$\Diamond$

10.3.3 Product of disjoint cycles

Definition 33. Two cycles are ***disjoint*** if their parentheses contain no elements in common. Formally, two cycles $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_l)$, are ***disjoint*** if $a_i \neq b_j, \forall i, j$ such that $1 \leq i \leq k$ and $1 \leq j \leq l$. △

For example, the cycles (135) and (27) are disjoint, whereas the cycles (135) and (347) are not.

Example 34. Given $\sigma = (135)$, $\tau = (27)$, and $\sigma, \tau \in S_7$. Let us compute $\sigma\tau$. We may do this using the following diagram:

$$\text{home} \leftarrow \underbrace{\sigma}_{(135)} \leftarrow \underbrace{\tau}_{(27)} \leftarrow \text{home}$$

Take each number in $\{1, 2, 3, 4, 5, 6, 7\}$, start from "home" on the right, and pass through the two "coatrooms" τ and σ one by one. If the number agrees with one of the numbers in the first "coatroom", then the number "changes its coat" and turns into the next number in the list. Then, it passes to the next "coatroom" where it does the same thing. Once it reaches "home" on the left, we have the result of $\sigma\tau$ acting on the original number.

Notice that every number affected by τ is unaffected by σ; and vice versa. Since the two cycles always remain separate, it is appropriate to represent $\sigma\tau$ as (135)(27), because the cycles don't reduce any farther. ⧫

This example also illustrates another point. Since S_7 is closed under function composition, it follows that $\sigma\tau$ must be a permutation in S_7.

Exercise 35. Write the permutation $\sigma\tau$ from Example 34 in tableau form. ◊

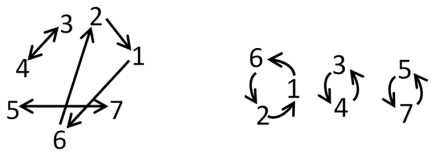
This permutation can't be represented by one cycle, but rather by *two* disjoint cycles. So we have an answer to our previous question: all cycles are permutations, but not all permutations are cycles. Some are represented by two disjoint cycles: and in fact some are represented by more than two disjoint cycles.

Example 36. Suppose $\mu \in S_7$ and $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 4 & 3 & 7 & 2 & 5 \end{pmatrix}$. Then

- $1 \to 6$, $6 \to 2$, and $2 \to 1$; therefore we have the cycle (162).
- $3 \to 4$ and $4 \to 3$; therefore we have (34).
- Finally, $5 \to 7$ and $7 \to 5$; therefore we have (57).

Hence $\mu = (162)(34)(57)$, as we may verify by computing the product $(162) \circ (34) \circ (57)$ directly.

We may represent this process graphically as follows. The permutation μ is also a binary relation, and thus can be represented as a digraph as shown in Figure 10.5(a). We can make the digraph appear much simpler by rearranging the vertices as in Figure 10.5(b). We shall see that *all* permutations can be simplified in this manner. ♦



(a) (b)

Figure 10.5. (a) Digraph representation of permutation (b) Rearrangement of digraph into cycles

Exercise 37. Write the following permutations in cycle notation.

(a)

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \end{pmatrix}$$

(b)

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

(c)

$$\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 6 & 2 & 3 \end{pmatrix}$$

(d)

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 1 & 2 & 6 \end{pmatrix}$$

♢

Exercise 38. Write each of the following permutations in S_9 in tableau form.

(a) $\mu = (259)(347)$.

(b) $\sigma = (25678)(14)(39)$.

(c) $\tau = (286)(193)(457)$.

(d) $\omega = (257)(18)$.

◊

Exercise 39. Write the permutations of D_6 in cycle notation (recall that D_6 is the group of symmetries of a hexagon). ◊

Exercise 40. Write the symmetries of a square in cycle notation. ◊

There is one more issue we need to explore with the product of disjoint cycles, which we will do in the following exercise.

Exercise 41. In parts (a)–(d) below, write both permutations on the set {1,2,3,4,5,6} in tableau form.

(a) (123)(45) and (45)(123).

(b) (14)(263) and (263)(14)

(c) (1352)(46) and (46)(1352)

(d) (135)(246) and (246)(135)

(e) From your results in (a)-(d), what do you conjecture about the product of disjoint cycles?

◊

The examples in Exercise 41 seem to indicate that the product of disjoint cycles is commutative. This is in fact true, as we shall now prove.

Proposition 42. Disjoint cycles commute: that is, given two disjoint cycles $\sigma = (a_1, a_2, \ldots, a_j)$ and $\tau = (b_1, b_2, \ldots, b_k)$ we have

$$\sigma\tau = \tau\sigma = (a_1, a_2, \ldots, a_j)(b_1, b_2, \ldots, b_k)$$

PROOF. We present this proof as a fill-in-the-blanks exercise:

Exercise 43. Fill in the $\underline{< \# >}$ to complete the proof:

Recall that permutations are defined as bijections on a set X. In order to show that the two permutations $\sigma\tau$ and $\tau\sigma$ are equal, it's enough to show

that they are the same function. In other words, we just need to show that $\sigma\tau(x) =$ $\underline{\quad < 1 > \quad}$ for all $x \in X$.

We'll define $A = \{a_1, a_2, \ldots, a_j\}$ and $B = \{b_1, b_2, \ldots, b_k\}$. By hypothesis A and B are disjoint, so A $\underline{\quad < 2 > \quad}$ $B =$ $\underline{\quad < 3 > \quad}$. Given an arbitrary $x \in X$, there are three possibilities: (i) $x \in A$ and $x \notin B$; (ii) $x \in$ $\underline{\quad < 4 > \quad}$ and $x \notin$ $\underline{\quad < 6 > \quad}$; (iii) $x \notin$ $\underline{\quad < 7 > \quad}$ and $x \notin$ $\underline{\quad < 8 > \quad}$.

(i) In this case, since $x \notin B$ it follows that $\tau(x) = x$. We then have $\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x)$. Furthermore, since $x \in A$ it follows that $\sigma(x) \in A$, so $\sigma(x) \notin B$. We then have $\tau\sigma(x) = \tau(\sigma(x)) = \sigma(x)$. It follows that $\sigma\tau(x) = \tau\sigma(x)$.

(ii) In this case, since $x \notin$ $\underline{\quad < 9 > \quad}$ it follows that $\underline{\quad < 10 > \quad}(x) = x$. We then have $\tau\sigma(x) =$ $\underline{\quad < 11 > \quad}$ $=$ $\underline{\quad < 12 > \quad}(x)$. Furthermore, since $x \in$ $\underline{\quad < 13 > \quad}$ it follows that $\underline{\quad < 14 > \quad}(x) \in$ $\underline{\quad < 15 > \quad}$, so $\underline{\quad < 16 > \quad}(x) \notin$ $\underline{\quad < 17 > \quad}$. We then have $\sigma\tau(x) =$ $\underline{\quad < 18 > \quad}$ $=$ $\underline{\quad < 19 > \quad}(x)$. It follows that $\sigma\tau(x) = \tau\sigma(x)$.

(iii) In this case, since $x \notin A$ it follows that $\underline{\quad < 20 > \quad}(x) = x$. Similarly since $x \notin$ $\underline{\quad < 21 > \quad}$ it follows that $\underline{\quad < 22 > \quad}(x) = x$.We then have $\tau\sigma(x) =$ $\underline{\quad < 23 > \quad}$ and $\sigma\tau(x) =$ $\underline{\quad < 24 > \quad}$. It follows that $\sigma\tau(x) = \tau\sigma(x)$.

In all three cases we have $\sigma\tau(x) =$ $\underline{\quad < 25 > \quad}$, so therefore $\sigma\tau = \tau\sigma$. $\Diamond$

$\square$

What we've discovered about products of two disjoint cycles is also true for products of any number of disjoint cycles. Since disjoint cycles act independently, they all commute.

Exercise 44. Write each of the following permutations on $X = \{1, 2, \ldots, 9\}$ in tableau form.

(a) $(1346)(298)(57)$ (b) $(57)(1346)(298)$ (c) $(298)(57)(1346)$

(d) Which of the above permutations are the same? Which are different? *Explain* your answer.

$\Diamond$

Exercise 45. Write each of the following permutations 3 different ways using cycle notation.

(a) (147)(258)(369) (b) (12)(35)(46)(78) (c) (14359)(28)(67)

$\Diamond$

10.3.4 Products of permutations using cycle notation

Finally, now that we know how to deal with permutation compositions that simplify to disjoint cycles, we can now compose any set of permutations we want. Let us begin with a relatively small example.

Example 46. Given the permutations $\mu = (257)(134)$ and $\rho = (265)(137)$ in S_7, write $\mu\rho$ in cycle notation.

This is actually not that much different from what we've done already. Using our "coatroom" representation, we have:

$$\text{home} \leftarrow \underbrace{(257) \leftarrow (134)}_{\mu} \leftarrow \underbrace{(265) \leftarrow (137)}_{\rho} \leftarrow \text{home}$$

We have written arrows between the cycles in μ and ρ to emphasize that in this case we essentially have four coatrooms, one after the other. So starting from the right with 1, we have

- $1 \to 3$, $3 \to 3$, $3 \to 4$, and $4 \to 4$; therefore $1 \to 4$.
- $4 \to 4$, $4 \to 4$, $4 \to 1$, and $1 \to 1$; therefore $4 \to 1$.

This gives us the cycle (14). Continuing,

- $2 \to 2$, $2 \to 6$, $6 \to 6$, and $6 \to 6$; therefore $2 \to 6$.
- $6 \to 6$, $6 \to 5$, $5 \to 5$, and $5 \to 7$; therefore $6 \to 7$.
- $7 \to 1$, $1 \to 1$, $1 \to 3$, and $3 \to 3$; therefore $7 \to 3$.
- $3 \to 7$, $7 \to 7$, $7 \to 7$, and $7 \to 2$; therefore $3 \to 2$.

So we have the cycle (2673). Now the only input not included in our cycles is 5, so logically it should stay put. But let's test it just in case we made a mistake in our work above.

- $5 \to 5$, $5 \to 2$, $2 \to 2$, and $2 \to 5$; therefore 5 does indeed stay put.

So, we finally have: $\mu\rho = (14)(2673)$ ♦

Example 47. Find the product $(156)(2365)(123)$ in S_6 .

- $1 \to 2$, $2 \to 3$, and $3 \to 3$; therefore $1 \to 3$.
- $3 \to 1$, $1 \to 1$, and $1 \to 5$; therefore $3 \to 5$.
- $5 \to 5$, $5 \to 2$, and $2 \to 2$; therefore $5 \to 2$.
- $2 \to 3$, $3 \to 6$, and $6 \to 1$; therefore $2 \to 1$.

So we have (1352).

- 4 does not appear in any of the cycles, so we know it won't be acted on by any of the cycles. Hence 4 stays put.
- $6 \to 6$, $6 \to 5$, and $5 \to 6$; hence 6 stays put.

Therefore $(156)(2365)(123) = (1352)$. ♦

Exercise 48. Given the following permutations in S_8,

$$\sigma = (1257)(34), \tau = (265)(137), \text{ and } \rho = (135)(246)(78)$$

write the following in cycle notation:

(a) $\sigma\tau$ (c) $\tau\rho$

(b) $\tau\sigma$ (d) $\sigma\rho$

◊

Exercise 49. Compute each of the following.

(a) $(1345)(234)$ (d) $(1423)(34)(56)(1324)$ (g) $(1254)^2(123)(45)$

(b) $(12)(1253)$ (e) $(1254)(13)(25)$

(c) $(143)(23)(24)$ (f) $(1254)(13)(25)^2$

$\Diamond$

10.3.5 Cycle structure of permutations

Over the last several subsections, we've seen permutations represented as no cycles (id), one cycle, or the product of any number of disjoint cycles. This worked because both a single cycle and a product of disjoint cycles can't be reduced to a simpler form in cycle notation. Are there any other possibilities? Are there permutations that can't be represented as either a single cycle or a product of disjoint cycles? The answer to this compelling question is given in the following proposition.

Proposition 50. Every permutation in S_n can be written either as the identity, a single cycle, or as the product of disjoint cycles.

The following proof is a formalized version of the procedure we've been using to change permutations from tableau form to cycle notation. Admittedly, it looks intimidating. However, we include it for your "cultural enrichment", because higher-level mathematics is typically like this. It's often the case that particular examples of a certain principle are relatively easy to explain, but constructing a general proof that covers *all* cases is much more difficult.

Also, recall that the notation $\sigma = (a_1, a_2, \ldots, a_n)$ means:

$$\sigma(a_1) = a_2 \qquad \sigma(a_2) = a_3 \ldots \qquad \ldots\sigma(a_k) = a_1,$$

and $\sigma(x) = x$ for all other elements $x \in X$.

Proof. We can assume that $X = \{1, 2, \ldots, n\}$. Let $\sigma \in S_n$, and define $X_1 = \{1, \sigma(1), \sigma^2(1), \ldots\}$. The set X_1 is finite since X is finite. Therefore the sequence $1, \sigma(1), \sigma^2(1), \ldots$ must repeat. Let j_1 be the first index where the sequence repeats: that is, $\sigma^{j_1}(1) = \sigma^k(1)$ for some $k < j_1$. Then if we apply σ^{-1} to both sides of the equation we get $\sigma^{j_1-1}(1) = \sigma^{k-1}(1)$. Repeating this $k-1$ more times gives $\sigma^{j_1-k}(1) = 1$. This implies that the sequence repeats at index $j_1 - k$: but we've already specified that j_1 is the

first index where the sequence repeats. The only way this can happen is if $k = 0$. It follows that $X_1 = \{1, \sigma(1), \sigma^2(1), \ldots \sigma^{j_1-1}(1)\}$, where $\sigma_1^j(1) = 1$.

Now there are two possible cases:

(i) X_1 accounts for all the integers in X; i.e. $X_1 = X$

(ii) there are some integers in X not accounted for in X_1 (that is, $X \backslash X_1 \neq \emptyset$).

If case (ii) holds, then let i be the smallest integer in $X \backslash X_1$ and define X_2 by $\{i, \sigma(i), \sigma^2(i), \ldots\}$. Just as with X_1, we may conclude that X_2 is a finite set, and that $X_2 = \{i, \sigma(i), \ldots, \sigma^{j_2-1}(i)\}$ where $\sigma^{j_2}(i) = i$.

We claim furthermore that X_1 and X_2 are disjoint. We can see this by contradiction: *suppose* on the other hand that X_1 and X_2 are not disjoint. Then it must be the case that $\sigma^p(1) = \sigma^q(i)$ for some natural numbers p, q with $0 \leq p < j_1$ and $0 \leq q < j_2$. Applying σ to both sides of this equation, gives $\sigma^{p+1}(1) = \sigma^{q+1}(i)$. If we continue applying σ to both sides a total of $j_2 - q$ times then we obtain $\sigma^{p+j_2-q}(1) = \sigma^{j_2}(i)$. But since $\sigma^{j_2}(i) = i$, it follows that $\sigma^{p+j_2-q}(1) = i$, which implies that $i \in X_1$. This is a contradiction, because we know $i \in X \backslash X_1$. The contradiction shows that the *supposition* must be false, so X_1 and X_2 are disjoint.

Continuing in the same manner, we can define finite disjoint sets $X_3, X_4, \ldots$. Since X is a finite set, we are guaranteed that this process will end and there will be only a finite number of these sets, say r. If σ_i is the cycle defined by

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i, \end{cases}$$

then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$. Since the sets $X_1, X_2, \ldots, X_r$ are disjoint, the cycles $\sigma_1, \sigma_2, \ldots, \sigma_r$ must also be disjoint.

Now recall case (i) above. In this case, $\sigma = \sigma_1$. Hence, σ is either a single cycle or the product of r disjoint cycles.

Note that this proof also works in case $\sigma = \mathsf{id}$: In this case all of the X_m's are single-element sets, and each cycle has length 1. □

Proposition 50 is a *classification theorem*. You have seen classification theorems before: for instance, you know that any natural number > 1 can be written uniquely as the product of primes. Proposition 50 similarly gives us a standard way to represent permutations. It allows us to characterize

the types of permutations in S_n according to their cycle sizes, as shown in the following example.

Example 51. We know that every permutation in S_5 is the product of disjoint cycles. Let us list all possible cycle lengths and number of cycles for the permutations of S_5.

- First of all, S_5 contains the identity, which has no cycles.
- Second, some permutations in S_5 consist of a single cycle. The single cycle could have length 2, 3, 4, or 5 (remember, we don't count cycles of length 1).
- Third, some permutations in S_5 consist of the product of two disjoint cycles. To enumerate these, suppose first that one of the cycles is a cycle of length 2. Then the other cycle could be a cycle of length 2 (for instance in the case (12)(34)) or a cycle of length 3 (as in the case (14)(235)). There are no other possibilities, because we only have 5 elements to permute, and a larger disjoint cycle would require more elements.
- It's not possible to have three or more disjoint cycles, because that would require at least six elements.

To summarize then, the types of permutations in S_5 are:

- The identity
- single cycles of lengths 5, 4, 3, or 2
- two disjoint cycles of lengths 2 and 3; and two disjoint cycles of lengths 2 and 2

♦

Exercise 52. Following Example 51, list the types (cycle structures) of permutations in the following:

(a) S_6 (b) S_7 (c) S_8

◊

10.4 Algebraic properties of cycles

10.4.1 Powers of cycles: definition of order

Let's revisit the product of cycles. We will look at what happens when you compose a cycle with itself multiple times.

Example 53. Consider the product (1264)(1264). As in the previous section, we can use a diagram (see Figure 10.6) to compute this product. But let's try to understand better what's really going on.

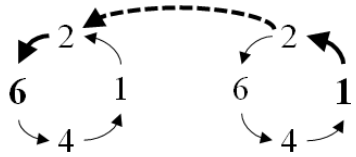


Figure 10.6. Diagram of $(1264)^2$, showing in particular how the permutation takes 1 to 6.

(1) Notice for all elements $x \neq 1, 2, 6, 4$, x stays put in (1264); hence x stays put in $(1264)^2$. So the product $(1264)^2$ does not involve any elements except $1, 2, 6$ and 4.

(2) Now let's look at what happens when $x = 1, 2, 6$, or 4. By squaring the cycle, we are applying it twice to each input; hence each input is moved two spots around the wheel (see Figure 10.7) . In other words,

$$1 \to 6; \quad 6 \to 1; \quad 2 \to 4; \quad 4 \to 2,$$

Altogether: $(1264)^2 = (16)(24)$.

♦

With this methodology in mind, let's explore powers of cycles a bit further.

Exercise 54. Compute each of the following.

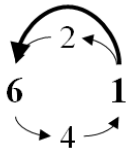


Figure 10.7. $(1264)^2$: streamlined notation

(a) $(1264)^3$ (b) $(1264)^4$ (c) $(1264)^5$

◊

Exercise 55. Compute each of the following:

(a) $(125843)^2$ (c) $(125843)^4$ (e) $(125843)^6$

(b) $(125843)^3$ (d) $(125843)^5$ (f) $(125843)^7$

◊

Do you notice a pattern from these two exercises? Let us investigate in a bit more detail: this will help us build up towards a proof of a general statement.

Exercise 56. Let $X = \{1, 2, \ldots, 10\}$, let $A = \{2, 5, 7, 8\}$, and let $\sigma \in S_X$ be the cycle $\sigma = (2578)$.

(a) What is $\sigma(2)$? What is $\sigma^2(2)$? What is $\sigma^3(2)$? What is $\sigma^4(2)$ What is $\sigma^{3,482,991}(2)$?

(b) What is $\sigma(5)$? What is $\sigma^2(5)$? What is $\sigma^3(5)$? What is $\sigma^4(5)$ What is $\sigma^{3,482,991}(5)$?

(c) Fill in the blank: If $x \in A$ then $\sigma^k(x) = \sigma^{\bmod(k,\_)}$.

(d) What is $\sigma(1)$? What is $\sigma(3)$?

(e) What general statement can you make about $\sigma^k(x)$ for $x \in X \backslash A$?

(f) ** Let $K = \{k : \sigma^k(x) = x \quad \forall x \in X\}$. Is $2 \in K$? Is $3 \in K$? Is $4 \in K$? Given any positive integer k, what's a simple way of telling whether or not $k \in K$?

$\Diamond$

Hopefully you're beginning to see the picture! To generalize these results, we need some additional terminology:

Definition 57. The ***order*** of a cycle σ is the smallest natural number k such that $\sigma^k = \mathsf{id}$. The order of σ is denoted by the notation $|\sigma|$. [4] $\triangle$

After that long build-up, we now have (Ta-da!):

Proposition 58. The order of a cycle is always equal to the cycle's length.

PROOF. To prove this, we essentially have to prove two things:

(A) If σ is a cycle of length k, then $\sigma^k = \mathsf{id}$;

(B) If σ is a cycle of length k, then $\sigma^j \neq \mathsf{id} \quad \forall j : 1 \leq j < k$.

The proof for (A) follows the same lines as our investigations in Exercise 56. In that exercise, we considered separately the elements of X that are moved by the cycle, and those elements that are not moved by the cycle.

Exercise 59. Prove part (A) by filling in the blanks.

Let $\sigma \in S_X$ be an arbitrary cycle of length k. Then σ can be written as $(a_1, a_2, \ldots a_k)$, for some set of elements $a_1, a_2, \ldots a_k$ in X. In order to show that $\sigma^k = \mathsf{id}$, it is sufficient to show that $\sigma^k(x) = \underline{\quad < 1 > \quad} \forall x \in X$. Let A be the set $\{a_1, a_2, \ldots a_k\}$. Now for any $x \in X$, there are two possibilities:

(i) $x \in X \backslash A$;

(ii) $x \in A$.

We'll deal with these two cases separately (as we did in Exercise 56).

[4] This is in keeping with our practice of using $|\ldots|$ to denote the "size" of things.

(i) In this case, $\sigma(x) =$ $\underline{\quad < 2 > \quad}$ It follows that $\sigma^2(x) = \sigma(\sigma(x)) = \sigma($ $\underline{\quad < 3 > \quad}$ $) =$ $\underline{\quad < 4 > \quad}$. We can use the same argument to show that $\sigma^3(x) =$ $\underline{\quad < 5 > \quad}$, and that $\sigma^k(x) =$ $\underline{\quad < 6 > \quad}$ for any natural number $\underline{\quad < 7 > \quad}$.

(ii) In this case, then $x = a_j$ for some integer $j, 1 \leq j \leq$ $\underline{\quad < 8 > \quad}$. It follows from the definition of cycle that $\sigma(x) = \sigma(a_j) = \text{mod}(a_{j+1}, k)$. Furthermore, $\sigma^2(x) = \sigma(a_{j+1}) =$ $\underline{\quad < 9 > \quad}$. Similarly it follows that $\sigma^k(x) = a_{\text{ mod }(j+\underline{<10>},k)} = a_{\underline{<11>}} = x$.

Cases (i) and (ii) establish that $\forall x \in X,$ $\underline{\quad < 12 > \quad}$ $= x$. It follows that $\sigma^k =$ $\underline{\quad < 13 > \quad}$.

$\Diamond$

The proof of (B) is also structured as an exercise.

Exercise 60.. In this exercise we use the same notation as part (A), that is: $\sigma \in S_X$ has length k and is represented as: $\sigma = (a_1, a_2, \ldots a_k)$.

(a) What is $\sigma(a_1)$? What is $\sigma^2(a_1)$? What is $\sigma^3(a_1)$? What is $\sigma^{k-1}(a_1)$?

(b) Conclude from part (a) that $\sigma^j \neq \mathsf{id}$ for $j = 1, 2, 3, \ldots, k-1$.

$\Diamond$

$\square$

Example 61. Here's a nice application of Proposition 58, which simply uses rules of function composition. This should also give you a good start on the next exercise.

$$(1264)^6 = (1264)^4(1264)^2 = \mathsf{id}\ (16)(24) = (16)(24)$$

$\blacklozenge$

Exercise 62. Compute the following:

(a) $(1264)^{11}$

(b) $(125843)^{53}$

(c) $(352)(136)(1254)^{102}$

(d) $(348)(456)^5(1325)^{10}$

$\Diamond$

10.4.2 Powers and orders of permutations in general

Now that we know the order of cycles, let's see if we can tackle other permutations as well:

Definition 63. The ***order*** of a permutation τ is the smallest positive integer k such that $\tau^k = \mathsf{id}$. As before, the order of τ is denoted by the notation $|\tau|$. $\triangle$

Proposition: Let τ be a permutation, and let $k = |\tau|$. Then $\tau^\ell = \mathsf{id}$ if and only if $\ell \equiv 0 \bmod k$.

Exercise 64. Fill in the $\underline{\quad < \# > \quad}$ with the appropriate variables in the following proof of the proposition. (*Hint*)

Proof: For any integer ℓ we may write $\ell = ak + b$, where $b \in \mathbb{Z}_{\underline{<1>}}$. It follows that

$$\tau^\ell = \tau^{\underline{<2>}\cdot k + \underline{<3>}} = (\tau^{\underline{<4>}\cdot k})\tau^{\underline{<5>}} = (\tau^k)^{\underline{<6>}}\tau^{\underline{<7>}} = (\mathsf{id})^{\underline{<8>}}\tau^{\underline{<9>}} = \tau^{\underline{<10>}}.$$

Therefore $\tau^\ell = \mathsf{id}$ if and only if $\tau^{\underline{<11>}} = \mathsf{id}$. However, we know that $\underline{\quad < 12 > \quad} < k$, and we also know that $\underline{\quad < 13 > \quad}$ is the smallest positive integer such that $\tau^{\underline{<14>}} = \mathsf{id}$. Hence it must be the case that $b \equiv \underline{\quad < 15 > \quad} \bmod k$, which is the same thing as saying that $\ell \equiv \underline{\quad < 16 > \quad} \bmod \underline{\quad < 17 > \quad}$. $\Diamond$

Can we characterize the order of a permutation that is a product of disjoint cycles? Let's explore.

Example 65. Let $\tau = (24)(16)$. Notice that (24) and (16) are disjoint, so they commute (recall Proposition 42). We also know that permutations are associative under composition. So we may compute τ^2 as follows:

$$\begin{aligned}
\tau^2 &= ((24)(16))((24)(16)) \\
&= (24)((16)(24))(16) && \text{(associative)} \\
&= (24)((24)(16))(16) && \text{(commutative)} \\
&= ((24)(24))((16)(16)) && \text{(associative)}
\end{aligned}$$

$= \mathsf{id}\ \mathsf{id}$ (2-cycles have order 2)

$= \mathsf{id}$

♦

Exercise 66.

(a) Let $\sigma = (237)$ and $\tau = (458)$. By following the format of Example 65, show that $(\sigma\tau)^3 = \mathsf{id}$ (write out each step, and cite the property used).

(b) ** If σ and τ are disjoint cycles with $|\sigma| = |\tau| = k$, what may you conclude about $|\sigma\tau|$? (You don't need to give a proof).

◊

Associativity and commutativity are powerful tools for rearranging products of disjoint cycles, and bear in mind that any disjoint cycles commute.

Exercise 67.

(a) Let σ and τ be *any* disjoint cycles. By following the format of Example 65, show that $(\sigma\tau)^2 = \sigma^2\tau^2$ (write out each step, and cite the property used).

(b) If σ and τ are disjoint cycles and k is a natural number, what may you conclude about $(\sigma\tau)^k$? (You don't need to give a proof).

◊

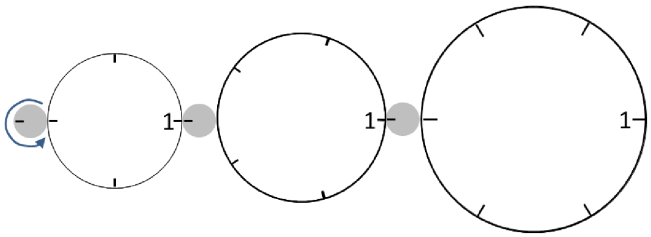


Figure 10.8. How many times does the small gear(at left) need to turn to return all gears to their original position? (Each turn rotates all gears clockwise by 1 position.)

Exercise 68. Suppose then $\tau = (123)(45)$. Compute each of the following

(a) τ^2 (c) τ^4 (e) τ^6

(b) τ^3 (d) τ^5 (f) τ^7

$\Diamond$

Notice what happened to the disjoint cycles in the previous exercise. For instance $|(123)| = 3$, and in parts (a)-(e) of the exercise you had the repeating pattern $\{(132), \mathsf{id}, (123), (132), \mathsf{id}, \ldots\}$. Similarly, the 2-cycle (45) yielded the repeating pattern $\{\mathsf{id}, (45), \mathsf{id}, (45) \ldots\}$.

In $\tau^3, \tau^6, \tau^9, \ldots$ the $(123)^k$ part of τ^k becomes id,while in $\tau^2, \tau^4, \tau^6, \ldots$ the $(45)^k$ part becomes id. In order for $\tau^k = \mathsf{id}$, we must have both $(123)^k = \mathsf{id}$ and $(45)^k = \mathsf{id}$, which first happens when $k = 6$. It is no accident that $|(123)|$ and $|(45)|$ both divide 6. In fact, we can prove the following proposition.

Proposition 69. If σ and τ are disjoint cycles, then

$$|\sigma\tau| = \text{ lcm } (|\sigma|, |\tau|),$$

where 'lcm' denotes least common multiple.

PROOF. Let $j \equiv |\sigma|, k \equiv |\tau|$, and $m \equiv$ lcm (k, j). Then it's enough to prove:

(i) $(\sigma\tau)^m = \mathsf{id}$;

(ii) $(\sigma\tau)^n \neq \mathsf{id}$ if $n \in \mathbb{N}$ and $n < m$.

To prove (i), first note that k divides m, so that $m = j \cdot p$ for some natural number p. Similarly, $m = k \cdot q$ for some $q \in \mathbb{N}$. It follows:

$$\begin{aligned}
(\sigma\tau)^m &= \sigma^m\tau^m && \text{(by Exercise 67)} \\
&= \sigma^{j\cdot p}\tau^{k\cdot q} && \text{(by definition of lcm)} \\
&= (\sigma^j)^p(\tau^k)^q && \text{(by exponentiation rules) [5]} \\
&= \mathsf{id}^p\mathsf{id}^q && \text{(by definition of order)} \\
&= \mathsf{id} && \text{(by definition of id).}
\end{aligned}$$

[5] These are the same exponentiation rules you saw in high school algebra: $x^{ab} = (x^a)^b$

To prove (ii), let $n < m$. It follows either k or j does *not* divide n. Let's suppose it's k (the case where it's j is virtually identical). In this case we must have $n = p \cdot k + r$ where p,r$\in \mathbb{N}$ and $r < k$. It follows:

$$\begin{aligned}(\sigma\tau)^n &= \sigma^n\tau^n && \text{(by Exercise 67)}\\ &= \sigma^{j\cdot p+r}\tau^n && \text{(substitution)}\\ &= (\sigma^j)^p\sigma^r\tau^n && \text{(by exponentiation rules)}\\ &= \mathsf{id}^p\sigma^r\tau^n && \text{(by definition of order)}\\ &= \sigma^r\tau^n && \text{(by definition of identity)}\end{aligned}$$

Now since $r < k$, and $|\sigma| = k$, it follows that $\sigma^r \neq \mathsf{id}$. Thus there is some x such that $\sigma^r(x) \neq x$. But since σ and τ are disjoint, it must be the case that $\tau(x) = x$. It follows that:

$$\sigma^r\tau^n(x) = \sigma^r(x) \neq x.$$

From this we may conclude that $(\sigma\tau)^n$ is *not* the identity. This completes the proof of (ii). □

What Proposition 69 establishes for two disjoint cycles is also true for multiple disjoint cycles. We state the proposition without proof, because it is similar to that of Proposition 69 except with more details.

Proposition 70. Suppose $\sigma_1, \sigma_2, \ldots, \sigma_n$ are n disjoint cycles, where $k_1, k_2, \ldots, k_n$ are the lengths, respectively, of the n disjoint cycles. Then

$$|\sigma_1\sigma_2\cdots\sigma_n| = \text{ lcm } (k_1, k_2, \ldots, k_n).$$

Now we can find the order of any permutation by first representing it as a product of disjoint cycles.

Exercise 71. What are all the possible orders for the permutations in each of the following sets (look back at your work for Exercise 52).

(a) S_6 (b) S_7 (c) S_8

◊

Exercise 72. Compute the following:

(a) $|(1254)^2|$

(b) $|(13658)^2(473)^2(125)|$

(c) $|(13658)^{13}(1254)^{11}(473)|$

(d) $|(123456789)^{300}|$

$\Diamond$

10.4.3 Transpositions and inverses

The simplest nontrivial cycles are those of length 2. We will show that these 2-cycles are convenient "building blocks" which can be used to construct all other cycles.

Definition 73. Cycles of length 2 are called ***transpositions***. We will often denote transpositions by the symbol τ (the greek letter "tau"). $\triangle$

Exercise 74. Compute the following products:

(a) $(14)(13)(12)$

(b) $(14)(18)(19)$

(c) $(16)(15)(14)(13)(12)$

(d) $(49)(48)(47)(46)(45)$

(e) $(12)(13)(14)(15)(16)(17)(18)$

$\Diamond$

Exercise 75. In light of what you discovered in the previous exercise, write each cycle as a product of transpositions:

(a) (1492)

(b) (12345)

(c) (472563)

(d) $(a_1a_2a_3)$

(e) $(a_1a_2a_3a_5a_6)$

(f) $(a_1a_2a_3a_5a_6a_7a_8)$

$\Diamond$

The preceding exercises demonstrate the following proposition:

Proposition 76. Every cycle can be written as the product of transpositions:

$$(a_1, a_2, \ldots, a_n) = (a_1a_n)(a_1a_{n-1}) \cdots (a_1a_3)(a_1a_2)$$

PROOF. The proof involves checking that left and right sides of the equation agree when they act on any a_j. We know that the cycle acting on a_j gives a_{j+1} (or a_1, if $j = n$); while the product of transpositions sends a_j first to a_1, then to a_{j+1}. □

Recall that we also know that any permutation can be written as a product of disjoint cycles, which leads to:

Proposition 77. Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

PROOF. First write the permutation as a product of cycles: then write each cycle as a product of transpositions. □

Exercise 78. Express the following permutations as products of transpositions.

(a) (14356)

(b) (156)(234)

(c) (1426)(142)

(d) (17254)(1423)(154632)

(e) (142637)(2359)

(f) (13579)(2468)(19753)(2864)

◊

Even the identity permutation id can be expressed as the product of transpositions:

Exercise 79. Compute the following products:

(a) (12)(12) (b) (57)(57) (c) $(a_1a_2)(a_1a_2)$

(d) What can you conclude about the inverse of a transposition?

◊

The preceding exercise amounts to a proof of the following:

Proposition 80. If τ is a transposition, $\tau^{-1} = \tau$.

We can use the inverses of transpositions to build up the inverses of larger cycles:

Proposition 81. Suppose μ is a cycle: $\mu = (a_1 a_2 \dots a_n)$. Then $\mu^{-1} = (a_1 a_n a_{n-1} \dots a_2)$.

PROOF. By Proposition 76 we can write

$$\mu = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2).$$

Now consider first just the last two transpositions in this expression. In the Functions chapter, we proved the formula $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ for invertible functions f and g. Since transpositions are invertible functions, we have

$$((a_1 a_3)(a_1 a_2))^{-1} = (a_1 a_2)^{-1}(a_1 a_3)^{-1} = (a_1 a_2)(a_1 a_3)$$

(the second equality follows because every transposition is its own inverse.)

If we apply similar reasoning to the last three transpositions in the expression, we find

$$((a_1 a_4)(a_1 a_3)(a_1 a_2))^{-1} = [(a_1 a_3)(a_1 a_2)]^{-1}(a_1 a_4)^{-1} = (a_1 a_2)(a_1 a_3)(a_1 a_4)$$

Applying this result inductively, we obtain finally:

$$\mu^{-1} = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_{n-1})(a_1 a_n),$$

from this epression we may see that $a_1 \to a_n$, $a_n \to a_{n-1}, a_{n-1} \to a_{n-2}, \dots, a_2 \to a_1$, which corresponds to the cycle we want. □

We can now find the inverse of any product of cycles, by taking the inverses of the cycles in reverse order:

Example 82. $[(1498)(2468)]^{-1} = (2468)^{-1}(1498)^{-1} = (2864)(1894) = (164)(289)$. ♦

Example 83. $(1357)^{-2} = \left[(1357)^{-1}\right]^2 = (1753)^2 = (1753)(1753) = (15)(37)$. ♦

Exercise 84. Calculate each of the following.

(a) $(12537)^{-1}$

(b) $[(12)(34)(12)(47)]^{-1}$

(c) $[(1235)(467)]^{-2}$

(d) $(1254)^{-1}(123)(45)(1254)$

(e) $(123)(45)(1254)^{-2}$

(f) $(742)^{-7}(286)^{-13}$

$\Diamond$

10.5 "Switchyard" and generators of the permutation group

Switchyards are used by railroads to rearrange the order of train cars in a train (see Figure 10.9. In this section we will study a "switchyard" of sorts. The design of our mathematical "switchyard" is not realistic, but the example will help us understand some important fundamental properties of permutations.

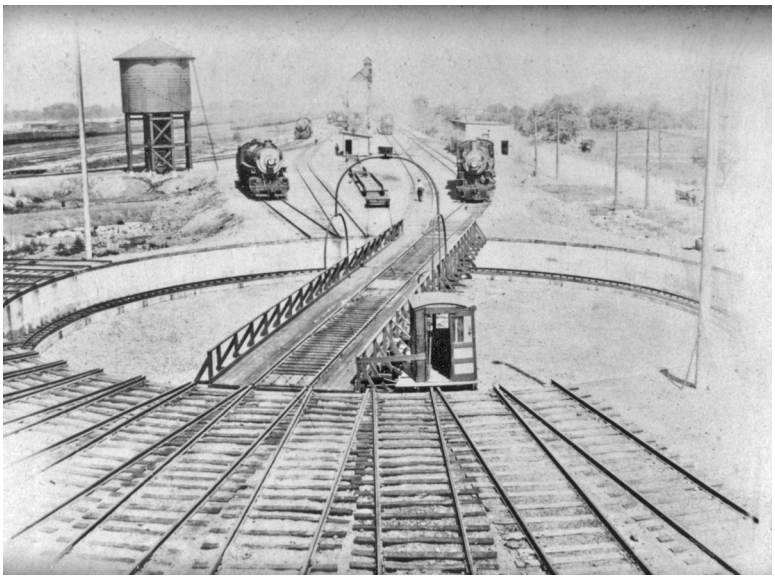


Figure 10.9. Grandview Yard (Pennsylvania Railorad) in Grandview Heights, OH around 1900 (source: http://www.ghmchs.org/thisweek/photo-listing10.htm.

Figure 10.10 shows how the switchyard works. The figure shows the particular case of a switchyard with 12 positions. A railroad train with 12 cars pulls in from the right, and circles around until it fills the circular track.

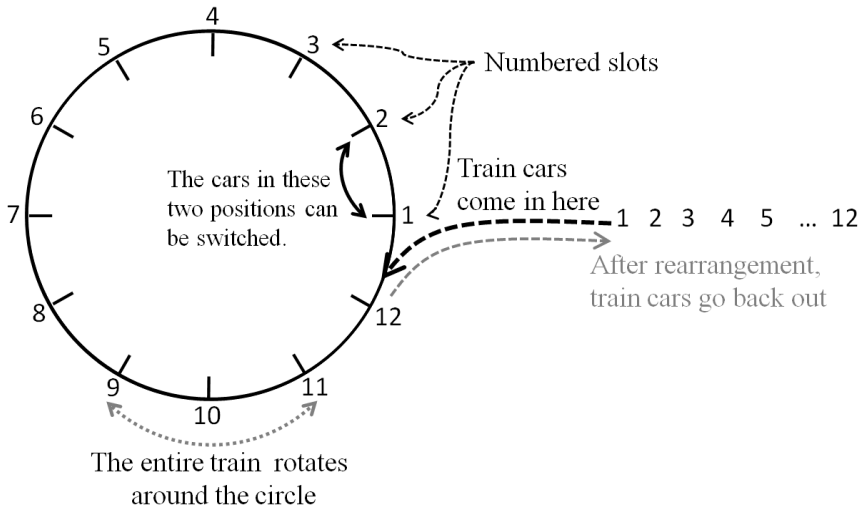


Figure 10.10. "Switchyard" diagram

The positions (we'll call them *slots* for short) are numbered 1 through 12 as are the railroad cars. At the *starting position*, each railroad car is at the corresponding numbered slot: car 1 is in slot 1, ... car 12 is in slot 12.

From the starting position, the train can move in one of two ways:

- The train can move circularly around the track, so that car 1 can end up at any one of the 12 slots.
- Alternatively, the cars in slots 1 and 2 can switch places.

These two types of motions can be represented as permutations. In tableau notation, the first row of the tableau corresponds to the train car, while the second row corresponds to the slot it moves to. For example, if the train cars $1, 2, 3, \ldots, 11, 12$ move counterclockwise one slot to occupy slots $2, 3, 4, \ldots, 12, 1$ respectively, then the permutation (in tableau notation) is:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 \end{pmatrix}$$

In cycle notation, the same permutation would be $(1, 2, 3, 4, \ldots, 12)$, where we have put commas between cycle entries to distinguish the number 12 from consecutive 1 and 2. We will denote this permutation by r. On the other hand, if cars 1 and 2 are switched, then this corresponds to the permutation (12). We will denote this permutation by t. In summary:

$$r = (1, 2, \ldots, 12); \qquad t = (1, 2).$$

Let's look at some other motions of the train. Suppose for example we shift the train counterclockwise by two positions. This corresponds to performing the permutation r twice in succession, which is $r \circ r$ or r^2. If we think about the process of composition, what's going on is the first r moves car #1 (which occupies slot #1) to position #2; while the second r moves whatever's in slot 2 (which happens to be car #1) to slot 3. The resulting composition can be interpreted as showing where each of the cars end up after both moves. The same thing will be true if we compose any number of permutations.

It follows that all rearrangements of the cars that can be accomplished by the switchyard may be obtained as compositions of the permutations r and t. So what rearrangements are possible? I'm glad you asked that question! The following exercises are designed to help you figure this out. But first, let's consider at one type of rearrangement that's particularly important. Suppose we want to switch two consecutive cars that are not 1 and 2: say for example we want to switch cars 5 and 6, and leave the rest of the cars unchanged. Can we do this?

At this point, in order to follow along the reader may find it helpful to make his/her own model of a switchyard.[6] Figure 10.11 shows a simple model made out of a jar lid with numbers stuck on with putty. We'll illustrate the motions necessary to switch cars 5 and 6 using the model. First, we rotate cars 5 and 6 to slots 1 and 2 by rotating 4 slots clockwise. This permutation is shown in Figure 10.12, and is written mathematically as r^{-4}.

Next, we exchange the two cars (which we can do since they're in the first two positions). Figure 10.13 shows the switch, which is denoted by t.

Finally, all we need to do is rotate counterclockwise 4 slots (r^4), as shown in Figure 10.14.

Altogether, these three steps give the composition $r^4 \circ t \circ r^{-4}$ (remember that permutations are applied right to left, just like functions). Note also

[6]The models in this section (and photos) were made by Holly Webb.

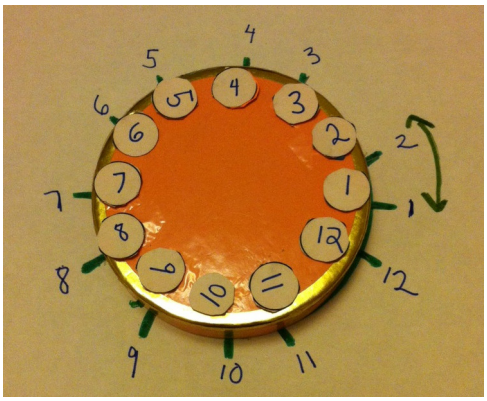


Figure 10.11. "Switchyard" model in home position

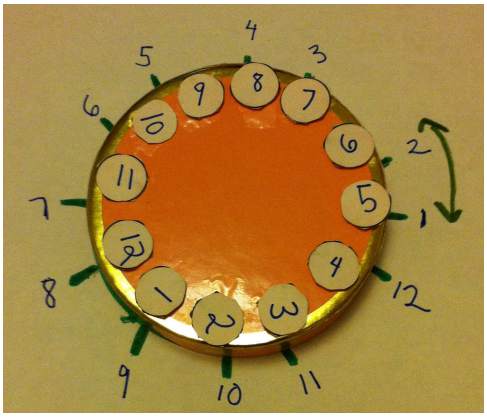


Figure 10.12. First stage in switching cars 5 and 6: clockwise rotation (r^{-4}.

that in the case of a 12-slot switchyard, r^{-4} could also be written r^8, since a clockwise rotation of 4 slots is the same as a counterclockwise rotation of 8 slots. (If the switchyard has n positions, the general rule is that $r^{-m} = r^{n-m}$, as we saw in the Symmetries chapter.)

Exercise 85. First we'll look at a switchyard with 4 positions. As above, r = counterclockwise rotation by 1 position = $(1, 2, 3, 4)$; while t exchanges two cars: $t = (1, 2)$.

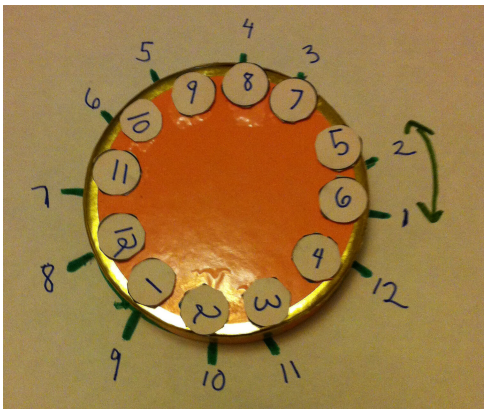


Figure 10.13. Second stage in switching cars 5 and 6: switch (t).

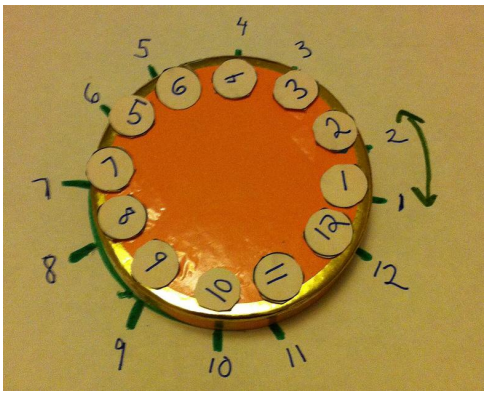


Figure 10.14. Third stage in switching cars 5 and 6: counterclockwise rotation (r^4).

(a) Write $(2,3)$, $(3,4)$, and $(4,1)$ as products of powers of r and t. (Together with (12), these are all the consecutive 2-cycles.)

(b) Write $(1,2,3)$, $(2,3,4)$, $(3,4,1)$, $(4,1,2)$ as products of powers of r and t. (These are all the counterclockwise consecutive 3-cycles.)

(c) Write $(1,3,2)$, $(2,4,3)$, $(3,1,4)$, $(4,2,1)$ as products of powers of r and t. (These are all the clockwise consecutive 3-cycles.) (*Hint*)

(d) Write $(1,3)$ as products of powers of r and t.

(e) Show that any transposition can be written as products of powers of r and t.

(f) Show that any permutation on 4 elements (that is, any permutation in S_4) can be obtained as a product of powers of r and t).

$\Diamond$

Exercise 86. Now we'll look at a general switchyard with n positions. In this case, rotation by 1 position is given by $r = (1, 2, \ldots, n)$. We use the same transposition, $t = (1, 2)$.

(a) Write the transposition $(k, k \oplus 1)$ as a product of powers of r and t. Here $\oplus$ denotes addition mod n.

(b) Show that any consecutive cycle $(m, m \oplus 1, \ldots, m \oplus p)$ can be written as a product of powers of r and t by filling in the blanks:

- First, $(m, m \oplus 1, \ldots, m \oplus p)$ can be written as a product of consecutive transpositions as _____.
- Then, by replacing each transposition in this expression with its expression in terms of products of _____, then we obtain an expression for _____ as a product of _____.

(c) Write the transposition $(1, k)$ as a product of a cycle of length k and a cycle of length $k - 1$.

(d) Prove that any transposition $(1, k)$ can be written as a product of consecutive transpositions.

(e) Prove that any transposition $(1, k)$ can be written as a product of powers of r and t.

(f) Prove that any transposition (p, q) can be written as a product of powers of r and t.

(g) Prove that any permutation in S_n can be obtained as a product of powers of r and t.

$\Diamond$

What we have shown in the previous exercise is that the two permutations r and t *generate* the group S_n. In other words, all of the information contained in the huge and complicated group S_n is characterized in just two permutations! The study of group generators is an important part of group theory, but unfortunately it is beyond the level of this course.

10.6 Other groups of permutations

10.6.1 Even and odd permutations

We saw in the previous section that any permutation can be represented as a product of transpositions. However, this representation is not unique. Consider for instance:

- $\mathsf{id} = (12)(12)$
- $\mathsf{id} = (13)(24)(13)(24)$
- $\mathsf{id} = (15)(26)(79)(14)(34)(34)(14)(79)(26)(15)$

Although these representations of id are vastly different, by some "strange coincidence" they all involve the product of an even number of transpositions.

Exercise 87. ***** Write id as a product of an odd number of transpositions (If you succeed, you automatically get an A in this course!) ♢

As you might guess from the previous exercise, there's something fishy going on here. To get to the bottom of this, we need to get a better handle on what happens when you multiply a permutation by a transposition. In particular, we know that any permutation can be written as a product of disjoint cycles: so what happens to these cycles when we multiply by a transposition? To get warmed up, let's first look at some special cases.

Exercise 88. Write $\tau\sigma$ as the products of disjoint cycles, where $\sigma = (12345678)$ and: (a) $\tau = (25)$; (b) $\tau = (16)$; (c) $\tau = (48)$; (d) $\tau = (35)$. ♢

As always it is helpful to have a good representation of the situation, preferably in pictures. For the following argument, we will represent a cycle as a "pearl necklace", as shown in Figure 10.15. This is not so different from

our previous representation of cycles (for instance, in Figure 10.1), but we are not including labels for the particular elements in the cycle because we want to emphasize the general structure and not get bogged down in details.

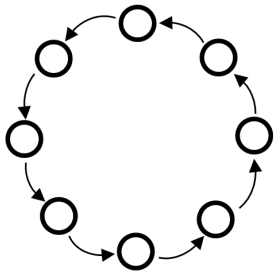


Figure 10.15. "Pearl necklace" representation of a cycle.

Figure 10.16 shows how we may represent the multiplication $(ab)C$ of transposition (ab) with cycle C, where a and b are elements included within C. The transposition effectively redirects the arrow pointing into a, so that now it points into b. The transposition also redirects the arrow pointing into b so that it now points into a. As a result, there are now two cycles instead of one. The sum of the lengths of the two cycles is equal to the length of the original cycle.

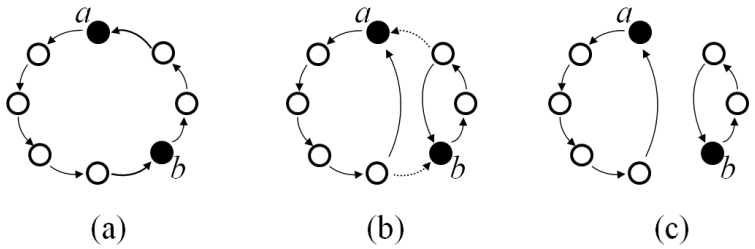


Figure 10.16. (a) Cycle C, including elements a and b; (b) Product of transposition (ab) with cycle C, showing redirection of arrows into a and b; (c) The result of $(ab)C$ is two separate cycles.

Using this representation, we can now investigate what happens when we multiply a transposition (ab) times an *arbitrary* permutation P. We already know that P can be thought of as a collection of disjoint cycles (plus stationary elements, that are unaffected by P). There are several

possibilities for how a and b can fit within the cycles of P, as shown in Figure 10.17. Each possibility may or may not change the number of cycles, as well as the sum of the lengths of all cycles.

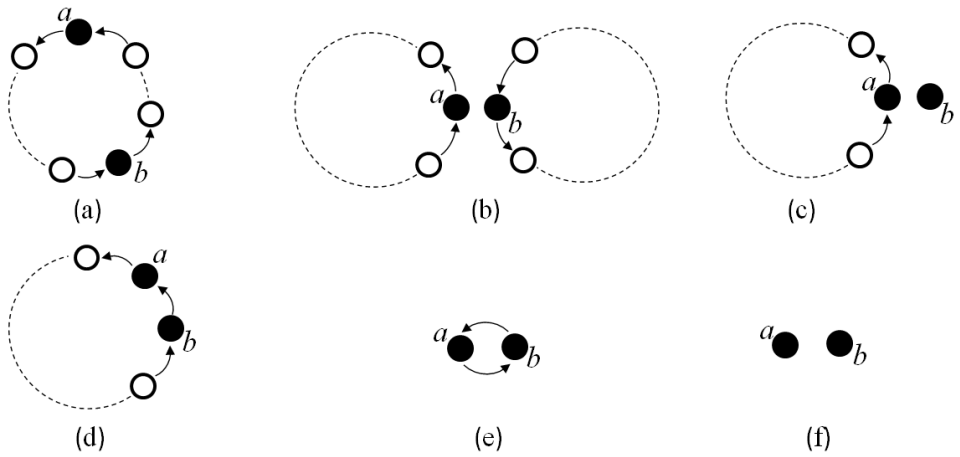


Figure 10.17. Multiplication of (ab) times a permutation P, showing the different ways that a and b can fit within the cycles (and stationary elements) of P. Note that case (a) corresponds to the situation described in Figure 10.16.)

Exercise 89. Draw a picture (similar to Figure 10.16(c)) for each of the possibilities (a)–(f) in Figure 10.17 showing the effect of the transposition (ab) on the cycles. Keep in mind that the transposition merely redirects the arrows into a and b so that they point into b and a, respectively. ◊

Exercise 90. Using your results from the previous exercise, complete Table 10.1. ◊

If you did the previous exercise correctly, you will find that no matter where the transposition falls, the column entry under "$(\Delta_{\text{cyc}} - \Delta_{\text{sum}})$ mod 2" is always 1. This motivates the following definition:

Definition 91. for any permutation P, the number (sum of cycle lengths – number of cycles) mod 2 is called the ***parity*** of P. A permutation with parity 0 is called an ***even permutation***, while a permutation with parity

Diagram in Figure 10.17	Change in number of cycles (Δ_{cyc})	Change in sum of cycle lengths (Δ_{sum})	$(\Delta_{\text{cyc}} - \Delta_{\text{sum}}) \pmod 2$
(a)	$+1$	0	1
(b)	-----	-----	-----
(c)	-----	-----	-----
(d)	-----	-----	-----
(e)	-1	-2	-----
(f)	-----	-----	-----

Table 10.1: Multiplication of permutation by transpositions

1 is called an ***odd permutation***. . Often books will use the terms "even parity" and "odd parity" instead of parity 0 and 1, respectively. △

Note that the disjoint sets of even and odd permutations of n objects form a *partition* of the set S_n. As we saw in the equivalence relations chapter, this means that we can define an equivalence relation such that all permutations with the same parity are equivalent.

Using this new terminology we may summarize our findings from Table 10.1 as follows. Every time I multiply a permutation by a transposition, I change the parity. So if I multiply together an even number of transpositions, the parity is 0; while if I multiply together an odd number of transpoitions, the parity is 1.

Now here's the punch line. We know that *every* permutation can be written as a product of transpositions. From what we have just shown, an odd permutation must be the product of an odd number of transpositions; while an even permutation must be the product of an even number of transpositions. It is *impossible* to write an even permutation as the product of an odd number of transpositions; and vice versa. We summarize our conclusions in the following theorem.

Proposition 92. A permutation P can be written as the product of an even number of transpositions if and only if P is an even permutation. Also, P can be written as the product of an odd number of transpositions if and only if P is an odd permutation.

Exercise 93. Prove that it is impossible to write the identity permutation as the product of an odd number of cycles. ◊

Exercise 94. Suppose P is an n-cycle. How can you tell whether P is an even or odd permutation? ◊

In the following exercises you will explore a bit further the parity properties of permutations.

Exercise 95.

(a) Prove that the product of two even permutations is even.

(b) Prove that the product of two odd permutations is even.

(c) What is the parity of the product of an even permutation and an odd permutation? What about the product of an odd permutation and an even permutation? *Prove* your answers.

◊

Exercise 96. For each of the following sets, describe which permutations are even and which are odd, according to their cycle structure. (*Hint*)

(a) S_6 (b) S_7 (c) S_8

◊

10.6.2 The alternating group

We have shown that all permutations are either even or odd. In other words, for any $n \in \mathbb{Z}$ we have that S_n is the union of two disjoint sets: $S_n = A_n \cup B_n$, where A_n and B_n are the even and odd permutations respectively.

Exercise 97. Use the sets A_n and B_n to define an equivalence relation on S_n, and verify that it is an equivalence relation. (*Hint*) ◊

We are particularly interested in the set A_n, because it has nice properties with respect to permutation product:

Exercise 98.

(a) Show that $\mathsf{id} \in A_n$.

(b) Show that if $\sigma \in A_n$, then $\sigma^{-1} \in A_n$. (*Hint*)

(c) Show that if $\sigma, \mu \in A_n$, then $\sigma\mu \in A_n$. (*Hint*)

$\Diamond$

In light of the previous exercise, it's beginning to look like A_n could be a group under permutation product. Let's check off the group properties:

- Is A_n closed under permutation product? Yes, according to Ex. 98(c).
- Does A_n have an identity element? Yes, according to Ex. 98(a).
- Does A_n have inverses for every element? Yes, according to Ex. 98(b).
- Is A_n associative? Yes, because the operation is composition, and composition is associative.

We have thus essentially proven the following proposition:

Proposition 99. The set A_n is a group.

Definition 100. The group A_n of even permutations is called the ***alternating group on*** n ***letters***. $\triangle$

Exercise 101. Prove or disprove: the set of odd permutations B_n is also a group. $\Diamond$

We know that A_n is a group – but how big is it? Of course, it depends on the number of odd permutations B_n, since A_n and B_n together make up S_n. So which is bigger: A_n or B_n? The answer is . . . neither!

Proposition 102. The number of even permutations in S_n, $n \geq 2$, is equal to the number of odd permutations; hence, $|A_n| = n!/2$.

PROOF. The key to the proof is showing that there is a *bijection* between A_n and B_n. Since a bijection is one-to-one and onto, this means that A_n and B_n must have exactly the same number of elements.

To construct a bijection, notice that $(12) \in S_n$ and define a function $f : A_n \to S_n$ by: $f(\sigma) = (12) \circ \sigma$. (Notice that we are taking A_n as our domain, and not S_n). To show that f is a bijection, we need to show three things:

(a) B_n is a valid codomain for f: that is, $f(\sigma) \in B_n \ \forall \sigma \in A_n$;

(b) $f : A_n \to B_n$ is onto: that is, $\forall \mu \in B_n \ \exists \sigma \in A_n$ such that $f(\sigma) = \mu$;

(c) f is one-to-one: that is, $f(\sigma_1) = f(\sigma_2)$ implies $\sigma_1 = \sigma_2$.

Parts (a) – (c) will be proven by (none other than) you, in the following exercise:

Exercise 103.

(a) Show part (a). (*Hint*)

(b) Show part (b). (*Hint*)

(c) Show part (c). (*Hint*)

◊

□

Exercise 104.

(a) What is $|A_4|$?

(b) List all the permutations of A_4 (Write them in cycle notation. Make sure you have them all – you should have as many as part (a) indicates).

◊

Exercise 105. Give all possible cycle structures for elements in each of the following sets.

(a) A_6 (b) A_7 (c) A_8

◊

10.7 Additional exercises

1. Show that A_{10} contains an element of order 15. (*Hint*)
2. Does A_8 contain an element of order 26?
3. Find an element of largest order in S_n for $n = 3, \ldots, 10$.
4. In Chapter 3 we used the term 'non-abelian' to describe groups in which not all elements commute. To show that a group is non-abelian, it's enough to find a single pair of elements $a, b \in S_n$ which do not commute (that is, $ab \neq ba$).
   (a) Prove that S_n is non-abelian for $n \geq 3$.
   (b) Show that A_n is non-abelian for $n \geq 4$.
   (c) Prove that D_n is non-abelian for $n \geq 3$.
5. Let σ be a permutation in S_n.
   (a) Show that there exists an integer $k > 1$ such that $sigma^k = \sigma$.
   (b) Show that there exists an integer $\ell > 1$ such that $sigma^\ell = \sigma^{-1}$.
   (c) Let K be the set of *all* integers $k > 1$ such that $sigma^k = \sigma$. Show that K is an infinite set (that is, K has an infinite number of elements).
   (d) Let L be the set of *all* integers $\ell > 1$ such that $sigma^\ell = \sigma^{-1}$. Show that L is an infinite set.
   (e) What is the relationship between the sets K and L?
6. Let $\sigma \in S_n$. Prove that σ can be written as the product of at most $n - 1$ transpositions. (*Hint*)
7. Let $\sigma \in S_n$. If σ is not a cycle, prove that σ can be written as the product of at most $n - 2$ transpositions. (*Hint*)
8. If σ is a cycle of odd length, prove that σ^2 is also a cycle. (*Hint*)
9. Prove that in A_n with $n \geq 3$, any permutation is a product of cycles of length 3.
10. Using "switchyard", we proved that S_n is generated by the permutations (12) and $(12 \ldots n)$. Prove that the group S_n is generated by the following sets of permutations.
    (a) $(12), (13), \ldots, (1n)$
    (b) $(12), (23), \ldots, (n-1, n)$
11. Let G be a group and define a function $f_g : G \to G$ by $f_g(a) = ga$. Prove that f_g is a permutation of G.
12. Let $\tau = (a_1, a_2, \ldots, a_k)$ be a cycle of length k.

(a) Prove that if σ is any permutation, then

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$$

is a cycle of length k.

(b) Let μ be a cycle of length k. Prove that there is a permutation σ such that $\sigma\tau\sigma^{-1} = \mu$.

13. For α and β in S_n, define $\alpha \sim \beta$ if there exists an $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Show that $\sim$ is an equivalence relation on S_n.

14. Let $\sigma \in S_X$. If $\sigma^n(x) = y$, we will say that $x \sim y$.

(a) Show that $\sim$ is an equivalence relation on X.

(b) If $\sigma \in A_n$ and $\tau \in S_n$, show that $\tau^{-1}\sigma\tau \in A_n$.

(c) Define the ***orbit*** of $x \in X$ under the permutation $\sigma \in S_X$ to be the set

$$\mathcal{O}_{x,\sigma} = \{y : x \sim y\}.$$

Compute the orbits of α, β, γ where

$$\alpha = (1254)$$
$$\beta = (123)(45)$$
$$\gamma = (13)(25).$$

(d) If $\mathcal{O}_{x,\sigma} \cap \mathcal{O}_{y,\sigma} \neq \emptyset$, prove that $\mathcal{O}_{x,\sigma} = \mathcal{O}_{y,\sigma}$. The orbits under a permutation σ are the equivalence classes corresponding to the equivalence relation $\sim$.

(e) A subgroup H of S_X is ***transitive*** if for every $x, y \in X$, there exists a $\sigma \in H$ such that $\sigma(x) = y$. Prove that $\langle\sigma\rangle$ is transitive if and only if $\mathcal{O}_{x,\sigma} = X$ for some $x \in X$.

15. Show that $\alpha^{-1}\beta^{-1}\alpha\beta$ is even for all $\alpha, \beta \in S_n$.

11

Abstract Groups: Definitions and Basic Properties

You may have noticed that we have been voyaging deeper and deeper into unfamiliar mathematical territory. We're using more symbols and fewer numbers. We introduce unfamiliar terminology and strange notation. We deal with outlandish mathematical objects that are harder and harder to visualize.

Please rest assured that these elaborations have a practical purpose[1]. We live in a complicated world, and complicated mathematical structures are needed to describe it well. However, underlying this confusing tangle of complicated structures are some deep commonalities. The purpose of abstraction is to identify and characterize these commonalities. In this way we can make connections between very different fields of mathematics, and gain a much more wholistic view of how things work together.

One of the commonalities that we have been (more or less) subtly emphasizing in the previous chapters is the ubiquity of *groups*, together with related notions such as isomorphisms and subgroups. Now that you've studies several specific groups (such as $\mathbb{C}, \mathbb{Z}_n, D_n, S_n, A_n$ and so on) our hope is that from these examples you've begun to get a feel for how groups work, and how one should think about groups in general. In this chapter, we will study groups *in the abstract*: that is, we will describe properties that are common to *all* groups, whether finite or infinite, abelian or non-abelian, and so on. [2]

[1] (that is, besides tormenting math students)

[2] Thanks to Tom Judson for material used in this chapter.

11.1 Formal definition of a group

Historically, the theory of groups first arose from attempts to find the roots of polynomials in terms of their coefficients. But groups have moved far beyond their original application, and now play a central role in such areas as coding theory, counting, and the study of symmetries. Many areas of biology, chemistry, and physics have benefited from group theory. In the preceding chapters we've already worked with a number of different groups, including the integers mod n and the symmetries of a rectangle or regular polygon. Recall that a group basically consists of a set and a "compatible" operation:

Exercise 1.

(a) What operation is the set $\mathbb{Z}_n$ a group under?

(b) What operation is the set S_3 a group under?

$\Diamond$

The following definition formalizes the notion of "operation".

Definition 2. A ***binary operation*** or ***law of composition*** on a set G is a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$, or ab in G, called the ***composition*** of a and b. $\triangle$

Remark 3.

- Notice that the word "composition" is now used to denote any operation on the elements of a set, and not just composition of functions.
- When the law of composition on a set is a basic algebraic operation such as multiplication or addition, we'll call it with its usual name. When it isn't, we will often refer to $a \circ b$ as the "product" of a and b (as we did in the Permutations chapter).

$\triangle$

In the Modular Arithmetic chapter we introduced what properties a set and operation must have to be called a group:

Exercise 4. What are the four properties a set G and a binary operation must exhibit in order for the set to be a group under that binary operation? $\Diamond$

Building on our previous discussion, we now proudly present the following formal definition.

Definition 5. A ***group*** $(G, \circ)$ is a set G together with a law of composition $(a, b) \mapsto a \circ b$ that satisfies the following axioms.

1. The set G is ***closed*** under the law of composition. That is,

$$\forall a, b \in G, a \circ b = c \text{ for some } c \in G.$$

2. There exists an element $e \in G$, called the ***identity element***, such that for any element $a \in G$

$$e \circ a = a \circ e = a.$$

3. For each element $a \in G$, there exists an ***inverse element*** in G, denoted by a^{-1}, such that

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

4. The law of composition is ***associative***. That is,

$$(a \circ b) \circ c = a \circ (b \circ c)$$

for $a, b, c \in G$.

$\triangle$

Remark 6. When the group operation is obvious or has been previously specified, we may denote the group by G rather than $(G, \circ)$. For instance, the group of integers under addition is typically denoted by $\mathbb{Z}$ and not $(\mathbb{Z}, +)$, since the operation $+$ is understood. $\triangle$

One very important class of groups is the commutative groups, which are given their own special designation:

Definition 7. A group $(G, \circ)$ with the property that $a \circ b = b \circ a$ for all $a, b \in G$ is called ***abelian***[3] or ***commutative***. Groups not satisfying this property are said to be ***non-abelian*** or ***noncommutative***. △

Finally, based on our discussion before about the order of sets, we have:

Definition 8. A group is ***finite***, or has ***finite order***, if it contains a finite number of elements The ***order*** of a finite group is the number of elements that it contains. If G is a group containing n elements, we write $|G| = n$. A group that is not finite is called ***infinite***, and such a group is said to be of ***infinite order***. △

The group $\mathbb{Z}_5$ is a finite group of order 5, so $|\mathbb{Z}_5 = 5$; while the integers $\mathbb{Z}$ form an infinite group under addition, and we sometimes write $|\mathbb{Z}| = \infty$.

Definition 9. The ***trivial group***, consists of the single element e (or id, in our previous notation). △

Exercise 10. Prove that the trivial group is in fact a group according to Definition 5. ♢

11.2 Examples

There are multitudes upon multitudes of groups besides those we've seen so far. Some are modification of groups we are very familiar with.

Example 11. The set $\mathbb{R} \setminus \{0\}$ of non-zero real numbers is written as $\mathbb{R}^*$. Let's prove that $(\mathbb{R}^*, \cdot)$ is a group.

[3] In honor of Neils Henrik Abel (1802-1829), an astounding mathematician who sadly died very young of tuberculosis. There is some discussion among mathematicians over whether 'abelian' should be capitalized. The word has become so common in mathematics that it's usually treated as a regular word and not a proper name. This should be considered as a special honor to Abel, since his name has become part of the fundamental language of mathematics.

(1) Closure:

Suppose $a, b \in \mathbb{R}^*$. Then to prove closure we must show $ab \in \mathbb{R}^*$; that is, we must show (i) $ab \in \mathbb{R}$ and (ii) $ab \neq 0$:

(i): Since $a, b \in \mathbb{R}$, and we know $\mathbb{R}$ is closed under multiplication, then $ab \in \mathbb{R}$.

(ii): Suppose $ab = 0$. Then by basic arithmetic, we know either $a = 0$ or $b = 0$. But $a, b \in \mathbb{R}^*$; i.e. $a, b \neq 0$. So we have a contradiction. Hence $ab \neq 0$.

Therefore $ab \in \mathbb{R}^*$; and so $\mathbb{R}^*$ is closed under multiplication.

To finish the proof that $\mathbb{R}^*$ is a group, we must establish axioms (2) through (4) in Definition 5. We leave this up to you in the following exercise:

Exercise 12.

(a) Finish proving that $(\mathbb{R}^*, \cdot)$ is a group.

(b) Either prove or disprove that $(\mathbb{R}^*, +)$ is a group.

(c) What is the order of $(\mathbb{R}^*, \cdot)$?

$\Diamond$

$\blacklozenge$

Exercise 13. Let $\mathbb{C}^*$ be the set of non-zero complex numbers.

(a) Why is $\mathbb{C}^*$ not a group under the operation of complex addition?

(b) Prove $\mathbb{C}^*$ is a group under the operation of (complex) multiplication.

(c) What is $|(\mathbb{C}^*, \cdot)|$?

(d) Is $(\mathbb{C}^*, \cdot)$ an abelian group? Justify your answer.

◊

Remark 14. Groups based on sets of numbers that *include* 0 (such as $\mathbb{R}, \mathbb{C}, \mathbb{Q}$)are assumed to have the group operation $+$ (unless otherwise stated). For groups based on sets of numbers that *exclude* 0 such as $\mathbb{R}^*, \mathbb{C}^*, \mathbb{Q}^*$, the group operation is assumed to be multiplication (unless otherwise stated). △

Exercise 15.

(a) Why is it impossible for a set of numbers S that includes 0 to be a group under multiplication? (There is one exception to this rule: what is it?)

(b) Why is it impossible for a set of numbers S that excludes 0 to be a group under addition?

◊

Some groups use exotic operations that you may never have seen before:

Example 16. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. It turns out that $(S, *)$ is an abelian group. We will prove closure and the commutative property; the rest of the proof will be left to you.

(1) Closure: Suppose $a, b \in S$. We need to show that $a * b \in S$; i.e. that (i) $a * b \in \mathbb{R}$ and (ii) $a * b \neq -1$.

   (i) By the closure of $(\mathbb{R}, +)$, $(a+b) \in \mathbb{R}$. By the closure of $(\mathbb{R}, *)$, $(ab) \in \mathbb{R}$. Finally, by the closure of $(\mathbb{R}, +)$, $((a+b)+(ab)) \in \mathbb{R}$. It follows that $a * b \in \mathbb{R}$, so S is closed under $*$.

   (ii) Suppose that $a * b = -1$. Then by definition of $*$, $a + b + ab = -1$. Solving for a, we get

$$a = \frac{-1(b+1)}{b+1}, \text{ or } a = -1$$

   But since $a \in S, a \neq -1$. So we have a contradiction. Hence $a * b \neq -1$. This completes the proof that $(S, *)$ is closed.

(2) Commutativity: Suppose $a, b \in S$. We need to show that $a * b = b * a$:

- First, by the definition of the operation $*$ we have $a*b = a+b+ab$.
- Next, since $\mathbb{R}$ is commutative under addition and multiplication, it follows that $a+b = b+a$ and $ab = ba$. Adding these two equations, we have $(a+b)+(ab) = (b+a)+(ba)$.
- By the definition of $*$, $(b+a)+(ba) = b*a$.
- Putting all these equalities together, we have $a*b = a+b+ab = b+a+ba = b*a$

This completes the proof that $(S, *)$ is commutative.

Exercise 17. Finish the proof that $(S, *)$ is an abelian group. ◊

⧫

Other groups use operations that are not the usual addition or multiplication.

Exercise 18. Let $H = \mathbb{Z} \times \mathbb{Z}$ (all integer coordinate-pairs).

(a) Define a binary operation $\circ$ on H by $(a,b) \circ (c,d) = (a+c, b+d)$, for $(a,b),(c,d) \in H$. This operation is in fact just coordinate-pair addition. Is $(H, \circ)$ a group? If so, is $(H, \circ)$ abelian? Justify your answers.

(b) Define a binary operation $\circ$ on H by $(a,b) \circ (c,d) = (ac, bd)$, for $(a,b),(c,d) \in H$. This is just coordinate-pair multiplication. Is $(H, \circ)$ a group? If so, is $(H, \circ)$ abelian? Justify your answers.

◊

Exercise 19. Let $G = \mathbb{R}^* \times \mathbb{Z}$ (all pairs such that the first element is a nonzero real number, and the second is an integer)

(a) Define a binary operation $\circ$ on G by $(a,m) \circ (b,n) = (a+b, m+n)$. Is $(G, \circ)$ a group? If so, is $(G, \circ)$ abelian? Justify your answers.

(b) Define a binary operation $\circ$ on G by $(a,m) \circ (b,n) = (ab, mn)$. Is $(G, \circ)$ a group? If so, is $(G, \circ)$ abelian? Justify your answers.

(c) Define a binary operation $\circ$ on G by $(a, m) \circ (b, n) = (ab, m + n)$. Is $(G, \circ)$ a group? If so, is $(G, \circ)$ abelian? Justify your answers.

$\Diamond$

The previous two exercises follow a pattern that we may generalize:

Definition 20. Given two groups G and H, we define the ***product*** of groups G and H (denoted by $G \times H$) as the set of pairs $\{(g, h), g \in G, h \in H\}$. If (g_1, h_1) and (g_2, h_2) are two elements of $G \times H$, then we define the group operation $(g_1, h_1) \circ (g_2, h_2)$ as follows:

$$(g_1, h_1) \circ (g_2, h_2) := (g_1 g_2, h_1 h_2),$$

where $g_1 g_2$ uses the group operation in G and $h_1 h_2$ uses the group operation in H. $\triangle$

Exercise 21.

(a) Consider $(3, 6)$ and $(2, 4)$ as elements of $\mathbb{Z}_7 \times \mathbb{Z}_7$. Compute $(3, 6) \circ (2, 4)$.

(b) Consider $(3, 6)$ and $(2, 4)$ as elements of $\mathbb{R}^* \times \mathbb{Z}_{10}$. Compute $(3, 6) \circ (2, 4)$.

(c) Consider $(3, 6)$ and $(2, 4)$ as elements of $\mathbb{Q}^* \times \mathbb{Q}^*$. Compute $(3, 6) \circ (2, 4)$.

$\Diamond$

In previous chapters we've used Cayley tables to describe group operations. With Cayley tables we can prove a set and operation are a group even when we don't know what the elements in the set really are or what the binary operation is.

The next two exercises are very useful in the subsequent exercises.

Exercise 22. Given two elements g, h of a group $(G, \circ)$. Show that g is the identity element of G if and only if $g \circ h = h$. (*Hint*) $\Diamond$

Exercise 23. Show that if G is a group, then for every row of the Cayley table for G no two entries are the same. Show also that for every column of the Cayley table no two entries are the same. (*Hint*) $\Diamond$

Exercise 24. For each of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ tell whether $(G, \circ)$ represents a group, and if so, whether it is abelian. Support your answer in each case. Assume that the associative property holds in each case. *Note* the identity element is not necessarily in the first row!

(a)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	a	b	c

(b)

$\circ$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

(c)

$\circ$	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	c	d	a
d	a	b	c	d

(d)

$\circ$	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

$\Diamond$

Exercise 25. For each of the following multiplication tables, fill in the blanks to make a Cayley table for a group.

(a)

$\circ$	a	b	c	d
a	a	b	c	_
b	_	a	_	_
c	c	_	a	_
d	d	_	_	_

(b)

$\circ$	a	b	c	d
a	c	_	_	_
b	_	b	c	d
c	_	_	_	_
d	_	_	_	_

(c)

$\circ$	a	b	c	d
a	d	_	_	_
b	_	d	_	_
c	_	_	d	_
d	_	_	_	d

(d)

$\circ$	a	b	c	d
a	a	b	_	d
b	_	a	_	_
c	c	_	_	_
d	d	_	_	_

(There are two different ways to complete this one: find both)

$\Diamond$

Exercise 26. * Show that it is *impossible* to complete the following Cayley tables to make a group.

(a)

$\circ$	a	b	c	d
a	_	_	_	_
b	b	_	_	_
c	d	_	_	_
d	c	_	_	_

(b)

$\circ$	a	b	c	d
a	a	_	_	_
b	_	b	_	_
c	_	_	_	_
d	_	_	_	_

(c)

$\circ$	a	b	c	d
a	a	_	_	_
b	_	c	_	_
c	_	_	b	_
d	_	_	_	_

(d)

$\circ$	a	b	c	d
a	b	_	_	_
b	_	c	_	_
c	_	_	d	_
d	_	_	_	_

$\Diamond$

11.2.1 The group of units of $\mathbb{Z}_n$

Back in the Modular Arithmetic chapter, we used the addition table for $\mathbb{Z}_8$ to show that $\mathbb{Z}_8$ with modular addition was a group. We extended this and showed that $\mathbb{Z}_n$ under modular addition is a group for any n. But we ran into problems with modular multiplication on $\mathbb{Z}_8$, as we can see from the Cayley table (reproduced below),

$\odot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Table 11.1: Cayley table for $(\mathbb{Z}_8, \cdot)$

From Table 11.1 we can see several problems. Notice that $0, 2, 4, 6$ have no inverses. In fact, from Table 11.1 we see that only numbers that are relatively prime to 8 have inverses in $\mathbb{Z}_8$. The same is true for any $\mathbb{Z}_n$. It

follows that in order to get a group under modular multiplication using the elements of $\mathbb{Z}_n$, we'll have to kick out the non-relatively prime numbers in order to guarantee that every element has an inverse. For instance,Table 11.2 is the result when Table 11.1 is restricted to the rows and columns labelled $(1, 3, 5, \text{ and } 7)$.

$\odot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Table 11.2: Multiplication table for $U(8)$

Exercise 27. Prove that the Cayley table in Table 11.2 represents a group. (Note that associativity holds because we already know that modular multiplication is associative.) ♢

Exercise 28. Is the group in Table 11.2 abelian? Justify your answer. ♢

For convenience, let's define some notation:

Definition 29. The set of nonzero numbers in $\mathbb{Z}_n$ that are relatively prime to n is called the ***set of units of*** $\mathbb{Z}_n$, denoted by $U(n)$. △

We have just seen that $U(8)$ is a group under modular multiplication. One might suspect that $U(n)$ is a group for any n. For starters, it is clear that 1 serves as an identity element, because $1 \cdot k \equiv k \cdot 1 \equiv k \bmod n$ for any n. In fact, $U(n)$ is an abelian group, as you will show in the following exercises.

Exercise 30. In this exercise, we prove that $U(n)$ is a group under multiplication mod n for any n. We know that modular multiplication is associative, so it remains to show the closure and inverse properties.

(a) Fill in the blanks to show that $U(n)$ is closed under modular multiplication:

Let k, m be arbitrary elements of $U(n)$. It follows that both k and $\underline{\quad < 1 > \quad}$ are relatively prime to $\underline{\quad < 2 > \quad}$. So neither k nor $\underline{\quad < 3 > \quad}$ has

any prime factors in common with $< 4 >$. It follows that the product $< 5 >$ also has no prime factors in common with $< 6 >$. Furthermore, the remainder of $< 7 >$ under division by $< 8 >$ also has no prime factors in common with $< 9 >$. Therefore the product of $< 10 >$ and $< 11 >$ under modular multiplication is also an element of $< 12 >$, so $< 13 >$ is closed under modular multiplication.

(b) It remains to show that $U(n)$ is closed under inverse. Suppose that $m \in U(n)$ and x is the inverse of m. What equation must x satisfy? (*Hint*)

(c) Show that the equation in x that you wrote in part (b) has a solution as long as m is relatively prime to n.

$\Diamond$

Exercise 31. Show that $U(n)$ is abelian. $\Diamond$

Remark 32. Whenever we talk about the group $U(n)$, we always assume the operation is multiplication. Similarly, whenever we talk about $\mathbb{Z}_n$, we always assume the operation is addition. $\triangle$

11.2.2 Groups of matrices

Finally, matrices provide many examples of interesting groups.

Exercise 33. We use $\mathbb{M}_2(\mathbb{R})$ to denote the set of all 2×2 matrices. That is

$$\mathbb{M}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

(a) Is $\mathbb{M}_2(\mathbb{R})$ a group under matrix addition? Is it abelian? Justify your answers.

(b) Is $\mathbb{M}_2(\mathbb{R})$ a group under matrix multiplication? Is it abelian? Justify your answers.

(c) What is the order of the group from a) or b) above?

◊

Exercise 34. Let $GL_2(\mathbb{R})$ be the subset of $\mathbb{M}_2(\mathbb{R})$ consisting of invertible matrices; that is, a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $GL_2(\mathbb{R})$ if there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$, where I is the 2×2 identity matrix. For A to have an inverse is equivalent to requiring that the determinant of A be nonzero; that is, $\det A = ad - bc \neq 0$. The set of invertible matrices forms a group called the ***general linear group***.

(a) Prove that $GL_2(\mathbb{R})$ is a group under matrix multiplication.

(b) Is the general linear group abelian? Justify your answer.

(c) What is $|GL_2(\mathbb{R})|$?

◊

11.3 Basic properties of groups

Now that we have a general definition of groups, we can use this definition to prove properties that are true of *all* groups. We'll begin by proving some essential properties that we've shown for specific groups, but need to know in general:

Proposition 35. The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.

Remark 36. The following proof follows the classic format used to prove that something is unique: assume instead there are two of them, then either derive a contradiction or show that the two things are really equal. We will employ the latter. △

PROOF. Suppose that e and e' are both identities in G. Then $eg = ge = g$ and $e'g = ge' = g$ for all $g \in G$. We need to show that $e = e'$. If we think

of e as the identity, then $ee' = e'$; but if e' is the identity, then $ee' = e$. Combining these two equations, we have $e = ee' = e'$. □

Proposition 35 shows that group identities are unique – it turns out that inverses in a group are also unique:

Proposition 37. If g is any element in a group G, then the inverse of g , is unique.

Exercise 38. Fill in the blanks to complete the following proof of Proposition 37.

(a) By the definition of inverse, if g' is an inverse of an element g in a group G, then $g \cdot \underline{\quad < 1 > \quad} = g' \cdot \underline{\quad < 2 > \quad} = e$.

(b) Similarly, if g'' is an inverse of g then $g \cdot \underline{\quad < 3 > \quad} = \underline{\quad < 4 > \quad} \cdot g = e$.

(c) We may show that $g' = g''$ as follows:

$$\begin{aligned} g' &= g' \cdot \underline{\quad < 5 > \quad} && \text{(definition of identity)} \\ &= g' \cdot (\underline{\quad < 6 > \quad} \cdot g'') && \text{(part b above, def. of inverse)} \\ &= (g' \cdot g) \cdot \underline{\quad < 7 > \quad} && \text{(associative property of group G)} \\ &= \underline{\quad < 8 > \quad} \cdot g'' && \text{(part a above, def. of inverse)} \\ &= g'' && \text{(def. of identity)} \end{aligned}$$

◊

Exercise 39.

(a) Consider the group $\mathbb{C}^*$, and let $a = 5 + 3i \in \mathbb{C}^*$. What is a^{-1}?

(b) Consider the group defined by the set $S = \mathbb{R} \setminus \{-1\}$ and the binary operation $a * b = a + b + ab$. What is 5^{-1}?

(c) Consider the group defined by the set $G = \mathbb{R}^* \times \mathbb{Z}$ and the operation $(a, m) \circ (b, n) = (ab, m + n)$. What is $(3, 2)^{-1}$?

(d) Consider the group $U(12)$. What is 5^{-1}?

(e) Consider the group $GL_2(\mathbb{R})$. What is $\begin{pmatrix} 4 & 3 \\ 3 & 2 \end{pmatrix}^{-1}$?

◊

An important property of inverses is:

Proposition 40. Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Remark 41. We've actually seen this property before, in the permutations chapter: recall that for two permutations σ and τ, we showed that $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$. △

PROOF. By the inverse property, $\exists a^{-1}, b^{-1} \in G$. By the closure property, $ab \in G$ and $b^{-1}a^{-1} \in G$. So we only need to verify that $b^{-1}a^{-1}$ satisfies the definition of inverse (from Proposition 37, we know the inverse is unique). First, we have:

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \text{ (associative property of group G)}\\ &= aea^{-1} \text{ (def. of inverse)}\\ &= aa^{-1} \text{ (def. of identity)}\\ &= e. \text{ (def. of inverse)}\end{aligned}$$

The remainder of the proof is left as an exercise:

Exercise 42. Fill in the blanks to complete the proof of Proposition 40

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b && (\text{\_\_\_\_\_})\\ &= b^{-1}eb && (\text{\_\_\_\_\_})\\ &= b^{-1}b && (\text{\_\_\_\_\_})\\ &= e. && (\text{\_\_\_\_\_})\end{aligned}$$

◊

□

Proposition 40 characterizes the inverse of a product: now we shall characterize the inverse of an inverse. From ordinary algebra we know that $-(-a) = a$ and $1/(1/a) = a$. This generalizes to arbitrary groups as follows:

Proposition 43. Let G be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.

PROOF. If $a \in G$, then since G is a group, then $a^{-1} \in G$ exists. And again, since G is a group, there also exists $(a^{-1})^{-1} \in G$.

Now, by the definition of inverse, $a^{-1}(a^{-1})^{-1} = e$. Consequently, multiplying both sides of this equation by a, we have (the argument continues in the following exercise):

Exercise 44.

$$\begin{aligned} a(a^{-1}(a^{-1})^{-1}) &= ae && \text{(multiplication by } a\text{)} \\ (aa^{-1})(a^{-1})^{-1} &= ae && (\text{\_\_\_\_\_}) \\ e(a^{-1})^{-1} &= ae && (\text{\_\_\_\_\_}) \\ (a^{-1})^{-1} &= a. && (\text{\_\_\_\_\_}) \end{aligned}$$

$\Diamond$

$\square$

Exercise 45.

(a) Suppose $a, b \in \mathbb{C}^*$, where $a = 4 + 3i$ and $b = 5 - 12i$. What is $(ab)^{-1}$? What is $(ba)^{-1}$?

(b) Suppose $a, b \in G$, where G is the group defined by the set $S = \mathbb{R} \setminus \{-1\}$ and the binary operation $a * b = a + b + ab$. If $a = 10, b = 1$, what is $(ab)^{-1}$? What is $(ba)^{-1}$?

(c) Suppose $\sigma, \tau \in S_6$, where $\sigma = (3456), \tau = (1625)$. What is $(\sigma\tau)^{-1}$? What is $(\tau\sigma)^{-1}$?

(d) Consider the group $U(5)$. What is $(4 \cdot 3)^{-1}$? What is $(3 \cdot 4)^{-1}$?

(e) Suppose $a, b \in GL_2(\mathbb{R})$, where

$$a = \begin{pmatrix} 6 & 7 \\ 2 & 3 \end{pmatrix} \text{ and } b = \begin{pmatrix} 5 & -2 \\ 2 & -1 \end{pmatrix}$$

What is $(ab)^{-1}$? What is $(ba)^{-1}$?

$\Diamond$

Exercise 46. Given a group G and $a, b \in G$, prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$. $\Diamond$

In high school algebra we wrote equations like $6 + x = -\sqrt{2}$ or $5x = 6$, and we could always find a real number x that was a solution. Now we know that $\mathbb{R}$ is a group under addition and multiplication. Similarly, we have seen that equations like $ax = b \pmod{n}$ and $a + x = b \pmod{n}$ had solutions for $x \in U(n)$ and $x \in \mathbb{Z}_n$, respectively.

Noticing a pattern here, the question then is this: does the equation $ax = b$ have a solution for any group G? In other words, if a and b are two elements in a group G, does there exist an element $x \in G$ such that $ax = b$? If such an x does exist, is it unique? The following proposition answers both of these questions affirmatively.

Proposition 47. Let G be a group and a and b be any two elements in G. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.

Note we need separate proofs to show that x exists and is unique for both $ax = b$ and $xa = b$, since we don't know whether the group is abelian. The proof for $ax = b$ is a fill-in-the-blank exercise, while the proof for $xa = b$ you'll do on your own:

Exercise 48.

(a) Complete the proof that $ax = b$ has a unique solution by filling in the blanks:

Suppose that $ax = b$. First we must show that such an x exists. Since $a \in G$ and G is a group, it follows that a^{-1} exists. Multiplying both sides of $ax = b$ on the left by a^{-1}, we have

$$\begin{aligned} a^{-1}(ax) &= a^{-1}b && \text{(left multiplication by } a^{-1}\text{)} \\ (a^{-1}a)x &= a^{-1}b && (\text{\_\_\_\_\_}) \\ ex &= a^{-1}b && (\text{\_\_\_\_\_}) \\ x &= a^{-1}b. && (\text{\_\_\_\_\_}) \end{aligned}$$

To show that the solution is unique, suppose that x_1 and x_2 are both solutions of $x_1 = a^{-1}b$ and $x_2 = a^{-1}b$. It follows that $x_1 = x_2$, which implies that the solution is unique.

(b) Prove now the existence and uniqueness of the solution of $xa = b$ (similar to part (a)).

$\Diamond$

The key method used in these proofs, the composition of both sides of the equation by a^{-1}, is something you've seen many times before. For instance in high school algebra, to solve the equation $5x = 6$ above, we teach our kids to divide each side by 5. Remember that dividing by 5 is the same as multiplying by its reciprocal 1/5. And 1/5 is the multiplicative inverse of 5. So in fact we are composing each side of the equation by 5^{-1} in order to solve for x.

As in our example then, composing both sides of the equation by a^{-1} is not only useful for the proofs, but in actually solving for x. Therefore, no matter what crazy elements and strange binary operation make up our group, we can still solve for x using the same algebra we learned in high school. In other words, given a group G and $a, b \in G$, if $ax = b$, then $x = a^{-1}b$; if $xa = b$, then $x = ba^{-1}$; and so on. Use this methodology in the following exercises.

Exercise 49. Given $a, b \in \mathbb{C}^*$, where $a = 3 - 3i$ and $b = 2 + 12i$; solve for x in each of the following equations.

(a) $ax = b$ (b) $xa = b$ (c) $bx = a$ (d) $xb = a$.

$\Diamond$

Exercise 50. Suppose G is the group defined by the set $S = \mathbb{R} \setminus \{-1\}$ and the binary operation $a * b = a + b + ab$. Solve for x in each of the following equations.

(a) $11 * x = -3$ (b) $x * 11 = -3$ (c) $-3 * x = 11$ (d) $x * (-3) = 11$.

$\Diamond$

Exercise 51. Given $\rho, \mu \in S_8$, where $\rho = (532)(164)$ and $\mu = (18753)(26)$; solve for x in each of the following equations.

(a) $\rho x = \mu$ (b) $x\rho = \mu$ (c) $\mu x = \rho$ (d) $x\mu = \rho$.

$\Diamond$

Exercise 52. Given the group $U(9)$, solve for x in each of the following equations.

(a) $5x = 8$ (b) $x5 = 8$ (c) $8x = 5$ (d) $x8 = 5$.

$\Diamond$

Exercise 53. Given $A, B \in GL_2(\mathbb{R})$, where

$$A = \begin{pmatrix} 6 & 5 \\ 4 & 4 \end{pmatrix} \text{ and } B = \begin{pmatrix} -2 & -1 \\ 7 & 4 \end{pmatrix}$$

Solve for X in each of the following equations.

(a) $AX = B$ (b) $XA = B$ (c) $BX = A$ (d) $XB = A$.

$\Diamond$

Exercise 54.

(a) Given a group G and $a, b \in G$, prove that if G is abelian, then any solution of $ax = b$ is also a solution of $xa = b$ (and vice versa). Given a group G that is *not* abelian, show that it is always possible to find an equation of the form $ax = b$ which has a solution that is *not* a solution to $xa = b$.

$\Diamond$

In our work so far, we've frequently used the ***substitution property***. For instance if $x = y$, then we know also that $a \cdot x = a \cdot y$, regardless of the operation $\cdot$. But suppose I gave you the equation $a \cdot x = a \cdot y$. Is it necessarily true that $x = y$? If $a, x, y \in \mathbb{R}$ and the operation is multiplication, then it's true *as long as* $a \neq 0$. To show this, we may use the method we talked

about in the previous proposition: multiply each side of the equation by a^{-1} (that is, divide by a), and the result is $x = y$. In basic algebra courses this property is often called the ***law of cancellation***. Now this works for real numbers: but suppose a, x, y were elements of some other group. Would the law of cancellation still hold? In fact, using the method shown above, you can prove this property holds for any group G.

Proposition 55. If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

This proposition tells us that the ***right and left cancellation laws*** are true in groups. We leave the proof as an exercise.

Exercise 56.

(a) To prove Proposition 55, we need prove both $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$. Why do these two statements require two different proofs?

(b) Prove Proposition 55.

$\Diamond$

We can use exponential notation for groups just as we do in ordinary algebra:

Definition 57. If G is a group and $g \in G$, then we define $g^0 = e$. For $n \in \mathbb{N}$, we define

$$g^n = \underbrace{g \cdot g \cdots g}_{n \text{ times}}$$

and

$$g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}.$$

$\triangle$

Proposition 58. In a group, the usual laws of exponents hold; that is, for all $g, h \in G$,

1. $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$;

2. $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$;

3. $(gh)^n = (h^{-1}g^{-1})^{-n}$ for all $n \in \mathbb{Z}$. Furthermore, if G is abelian, then $(gh)^n = g^n h^n$.

PROOF. We will prove part (1), and you will do the rest. We can break part (1) into four cases: (a) $m, n \geq 0$; (b) $m, n < 0$; (c) $m \geq 0, n < 0$; (d) $m < 0, n \geq 0$.

Consider first case (a). Using Definition 57, we have

$$g^m g^n = \underbrace{g \cdot g \cdots g}_{m \text{ times}} \underbrace{g \cdot g \cdots g}_{n \text{ times}},$$

and

$$g^{m+n} = \underbrace{g \cdot g \cdots g}_{m+n \text{ times}}.$$

Since the right-hand sides of these expressions are equal, then so are the left-hand sides: so $g^m g^n = g^{m+n}$.

The proof of case (b) is exactly the same, except on the right-hand sides we should replace all g's with g^{-1} and we should also replace 'm times', 'n times', and '$m+n$ times' with '$-m$ times', '$-n$ times', and '$-(m+n)$ times' respectively.

In case (c), we have

$$g^m g^n = \underbrace{g \cdot g \cdots g}_{m \text{ times}} \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-n \text{ times}}.$$

We now have two subcases to consider. First, if $m \geq -n$, then all of the g^{-1} factors cancel and we end up with

$$g^m g^n = \underbrace{g \cdot g \cdots g}_{m+n \text{ times}}.$$

Second, if $m < -n$, then all of the g factors are cancelled and we end up with

$$g^m g^n = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-(m+n) \text{ times}}.$$

In either of these subcases, the right-hand side agrees with the definition of g^{m+n}, so the equality is proved.

Case (d) is just like (c), except we exchange the signs on the$g$'s, m's and n's on the right-hand sides. This completes the proof of part (1).

Exercise 59. Prove parts (2) and (3) of Proposition 58. ◊

□

Notice that $(gh)^n \neq g^n h^n$ in general, since the group may not be abelian.

If the group is $\mathbb{Z}$ or $\mathbb{Z}_n$, we write the group operation additively and the exponential operation multiplicatively; that is, we write ng instead of g^n. The laws of exponents now become

1. $mg + ng = (m + n)g$ for all $m, n \in \mathbb{Z}$;
2. $m(ng) = (mn)g$ for all $m, n \in \mathbb{Z}$;
3. $m(g + h) = mg + mh$ for all $m \in \mathbb{Z}$.

It is important to realize that the last statement can be made only because $\mathbb{Z}$ and $\mathbb{Z}_n$ are abelian groups.

Historical Note

Although the first clear axiomatic definition of a group was not given until the late 1800s, group-theoretic methods had been employed before this time in the development of many areas of mathematics, including geometry and the theory of algebraic equations.

Joseph-Louis Lagrange used group-theoretic methods in a 1770–1771 memoir to study methods of solving polynomial equations. Later, Évariste Galois (1811–1832) succeeded in developing the mathematics necessary to determine exactly which polynomial equations could be solved in terms of the polynomials' coefficients. Galois' primary tool was group theory.

The study of geometry was revolutionized in 1872 when Felix Klein proposed that geometric spaces should be studied by examining those properties that are invariant under a transformation of the space. Sophus Lie, a contemporary of Klein, used group theory to study solutions of partial differential equations. One of the first modern treatments of group theory appeared in William Burnside's *The Theory of Groups of Finite Order* [1], first published in 1897. □

11.4 Subgroups

We first came across subgroups in the Permutations chapter. We saw that S_n, the set of permutations on a set of n elements, is a group under function composition. Yet we also saw that the set of symmetries of an n-sided figure, which is a subset of S_n, is itself a group under function composition. So a subgroup is a subset of a larger group that is itself a group under the same operation as the larger group. Formally then:

Definition 60. A ***subgroup*** H of a group $(G, \circ)$ is a subset H of G such that when the group operation of G is restricted to H, H is a group in its own right. $\triangle$

By definition, all subgroups are subsets: but is the reverse true? If not, what makes a sub*set* a sub*group*? What special properties must subsets possess in order to qualify as subgroups?

The key to answering this question is the observation that any subset $H \subset G$ that is a subgroup of G must also be a group in its own right: and we're already experts at deciding whether a set with a binary operation is a group:

Example 61. Consider the set of even integers $2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$. A more mathematically concise definition is:

$$2\mathbb{Z} = \{x \in \mathbb{Z} | x = 2n \text{ for some } n \in \mathbb{Z}\}$$

$2\mathbb{Z}$ is actually a subgroup of $\mathbb{Z}$, under the operation of addition. To show this, according to the definition of subgroup we need to show:

(a) $(\mathbb{Z}, +)$ is a group;

(b) $2\mathbb{Z} \subset \mathbb{Z}$;

(c) $(2\mathbb{Z}, +)$ is a group.

Items (a) and (b) can be dispatched in short order. From our work in Chapters 1 and 2, we know $\mathbb{Z}$ is a group under addition: this takes care of (a). For item (b), we have that any element $m \in 2\mathbb{Z}$ can be written as $m = 2n$, where $n \in \mathbb{Z}$: hence $m \in \mathbb{Z}$ also.

To show (c), we must verify all the group properties for $2\mathbb{Z}$ under the operation $+$:

- *(Closure)*: Given $x, y \in 2\mathbb{Z}$, it follows $x = 2n$ and $y = 2m$ for some $n, m \in \mathbb{Z}$. Therefore

$$x + y = 2n + 2m = 2(n + m)$$

  Since $\mathbb{Z}$ is closed under $+$, it follows $(n + m) \in \mathbb{Z}$, so $2(n + m) \in 2\mathbb{Z}$. Since x and y were arbitrary, it follows that $2\mathbb{Z}$ is closed under addition.

- *(Associative)*: Suppose $w, x, y \in 2\mathbb{Z}$. Then w, x, y are integers, and $w + (x + y) = (w + x) + y$ by the associativity of $(\mathbb{Z}, +)$. Hence $2\mathbb{Z}$ is associative under addition.

- *(Identity)*: $0 \in 2\mathbb{Z}$, since $2 \cdot 0 = 0$: and for any $x \in 2\mathbb{Z}$,

  $0 + x = x + 0 = x$.

  Hence $2\mathbb{Z}$ has an identity under addition, namely 0.

- *(Inverse)*: Given $x \in 2\mathbb{Z}$, where $x = 2n$,

  $-x = -(2n) = 2(-n)$, [associative and commutative properties of $\mathbb{Z}$ under multiplication]

  and since $-n \in \mathbb{Z}$ (closure of $\mathbb{Z}$ under multiplication) it follows that $-x \in 2\mathbb{Z}$. Now since

  $-x + x = x + (-x) = 0$,

  it follows $\forall x \in 2\mathbb{Z}$, $\exists x^{-1} \in 2\mathbb{Z}$, namely $x^{-1} = -x$.

This completes the proof that $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition. ⧫

Exercise 62. Given any fixed integer m Prove that $m\mathbb{Z} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$, is a subgroup of $\mathbb{Z}$ under the operation of addition. ◊

It's also good to look at some examples that are *not* subgroups:

Exercise 63.

(a) Explain why $(\mathbb{R}, \cdot)$ is *not* a group.

(b) Explain why $\mathbb{C}$ is not a group under complex multiplication.

$\Diamond$

Notice that the operation used in the subgroup must be the *same* operation that's used in the group it's contained in. For example, $\mathbb{R}^*$ is not a subgroup of $\mathbb{R}$, because $(\mathbb{R}^*, +)$ is not a group.

Exercise 64. Prove or disprove:

(a) $GL_2(\mathbb{R})$ is a subgroup of $\mathbb{M}_2(\mathbb{R})$.

(b) $U(n)$ is a subgroup of $\mathbb{Z}_n$.

$\Diamond$

We can make subgroup proofs a little easier. Notice that in Example 61, $2\mathbb{Z}$ was associative simply by virtue of the fact that it's contained in the group $\mathbb{Z}$ (with the same operation): so all of its elements must associate automatically. So we can simplify our list of things to check. This list is formalized in the following proposition (which is essentially proved by the forgoing discussion):

Proposition 65. A subset H of a group G is a subgroup if and only if it satisfies the following conditions.

(a) The identity e of G is in H.

(b) If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.

(c) If $h \in H$, then $h^{-1} \in H$.

Exercise 66. The set $\mathbb{T}$ is defined as the subset of the $\mathbb{C}$ whose elements all have a modulus of 1; that is

$$\mathbb{T} = \{c \in \mathbb{C} : |c| = 1\}$$

(a) Using Proposition 65 above, prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.

(b) What is $|\mathbb{T}|$?

(c) Prove or disprove that $\mathbb{T}$ is commutative.

◊

Exercise 67. Let $H_4 = \{1, -1, i, -i\}$, (these are the fourth roots of unity, which we studied in the Complex Numbers chapter).

(a) Using Proposition 65, prove that H is a subgroup of $\mathbb{T}$. (*Note* you should first verify that H is a subset of $\mathbb{T}$.)

(b) What is $|H_4|$?

(c) Prove or disprove that H is commutative.

◊

Exercise 68. Let's generalize the last exercise. Suppose now that H is the set of n^{th} roots of unity. That is

$$H_n = \{z \in \mathbb{C} : z^n = 1\}$$

(a) Prove that H_n is a subset of $\mathbb{T}$.

(b) Using Proposition 65, prove that H is a subgroup of $\mathbb{T}$.

(c) What is $|H_n|$?

(d) Prove or disprove that H_n is commutative.

◊

Exercise 69. Let $\mathbb{Q}^*$ be defined in the following way:

$$\mathbb{Q}^* = \{p/q : p, q \text{ are nonzero integers } \}$$

In other words $\mathbb{Q}^*$ is the set of non-zero rational numbers ($\mathbb{Q}^* = \mathbb{Q} \setminus 0$).

(a) Using Proposition 65, prove that $\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$.

(b) Prove or disprove that $\mathbb{Q}^*$ is commutative.

$\Diamond$

Exercise 70. We define $SL_2(\mathbb{R})$ to be the set of 2×2 matrices of determinant one; that is, a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $SL_2(\mathbb{R})$ exactly when $ad - bc = 1$. We call this the ***Special Linear Group*** .

(a) Using Proposition 65, prove that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

(b) Prove or disprove that $SL_2(\mathbb{R})$ is commutative.

$\Diamond$

There is an alternative way to prove a subset H of G is a subgroup of G that can save some time. It turns out that the three conditions in Proposition 65 can be combined into a single statement:

Proposition 71. Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.

PROOF. Let H be a nonempty subset of G. Then H contains some element g. So $gg^{-1} = e$ is in H. If $g \in H$, then $eg^{-1} = g^{-1}$ is also in H. Finally, let $g, h \in H$. We must show that their product is also in H. However, $g(h^{-1})^{-1} = gh \in H$. Hence, H is indeed a subgroup of G. Conversely, if g and h are in H, we want to show that $gh^{-1} \in H$. Since h is in H, its inverse h^{-1} must also be in H. Because of the closure of the group operation, $gh^{-1} \in H$. $\square$

Example 72. Using the proposition above, let's reprove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.

PROOF. Based on the proposition, there are four things we need to show:

(a) $\mathbb{C}^*$ is a group;

(b) $\mathbb{T} \neq \emptyset$;

(c) $\mathbb{T} \subset \mathbb{C}^*$;

(d) Given $x, y \in \mathbb{T}$, $xy^{-1} \in \mathbb{T}$.

Items (a), (b), and (c) we have shown before. As to item (d),

$x, y \in \mathbb{T}$
$\Rightarrow |x| = 1$ and $|y| = 1$
$\Rightarrow |xy^{-1}| = |x| \cdot |y^{-1}| = |x|/|y| = 1/1 = 1$
$\Rightarrow |xy^{-1}| \in \mathbb{T}$

□ ♦

Exercise 73. Use Proposition 71 to reprove the following:

(a) $\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$

(b) $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$

◊

11.5 Cyclic groups

In this section we will explore an important property of some groups and subgroups.

11.5.1 Cyclic groups

Example 74. Consider the group $\mathbb{Z}$. Let us try to find the smallest subgroup of $\mathbb{Z}$ that contains the number 1.

(1) We start with the smallest subset possible, $P = \{1\}$.

(2) The subset has to be a group under addition. But so far P does not contain an additive identity. So we need to add 0 to the set, giving us $P = \{0, 1\}$.

(3) Zero is its own inverse under addition, but notice that our set does not include an inverse for 1. So we add -1 to P, giving us $P = \{-1, 0, 1\}$.

(4) Is P closed under addition? Certainly when we add 0 to 1 and -1, we get 1 and -1, respectively. And $-1+1=0$. But what about when we add 1 and 1, or -1 and -1? So we need to add 2 and -2 to the set, giving us $P=\{-2,-1,0,1,2\}$.

(5) Now, what about $1+2$, or $(-1)+(-2)$? So we need 3 and -3, giving us $P=\{-3,-2,-1,0,1,2,3\}$.

(6) And we can see that this process would keep going until we get all the integers. In other words,

$P=\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}=\mathbb{Z}$.

Therefore the smallest subgroup of $\mathbb{Z}$ that contains 1 is $\mathbb{Z}$ itself. ♦

From the last example, we saw that P was generated through repeated additions of 1 and repeated additions of -1 (with 0 thrown in for good measure). Zero in fact can be calculated by adding 1 and -1, and can be thought of as a zero multiple of 1. In addition, the repeated additions of 1 and -1 can be thought of as positive and negative multiples of 1. Therefore we can think of all the elements of P as integer multiples of 1. We denote the set of all integer multiples of 1 as $\langle 1\rangle$; therefore,

$$\langle 1\rangle=\{n\cdot 1 : n\in\mathbb{Z}\}=P.$$

In Example 74 we also saw that P was in fact $\mathbb{Z}$; therefore $\mathbb{Z}=\langle 1\rangle$. We say that $\mathbb{Z}$ is *generated by* 1, as per the following definition:

Let us extend this concept to groups in general:

Definition 75. Given a group G and an element $a\in G$, then ***the set generated by the element*** a is denoted by $\langle a\rangle$, and is defined as the set obtained by repeated operation on the identity e by the group elements a and a^{-1}. Using the notation we introduced right before Proposition 58, we can write this as

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

or

$$\langle a\rangle=\{a^k : k\in\mathbb{Z}\}$$

$\langle a\rangle$ is sometimes called the ***orbit*** of a. △

Remark 76. If we are using the "+" operation, as in the case of the integers above, we write $\langle a \rangle = \{na : n \in \mathbb{Z}\}$. △

Exercise 77. List the set $\langle 3 \rangle$ for $3 \in \mathbb{R}^*$. ◊

We have special terminology for the case where all the elements of a group are generated by a single element:

Definition 78. If a group G contains some element a such that $G = \langle a \rangle$, then G is a ***cyclic group***. In this case a is a ***generator*** of G. △

We have seen above that 1 is a generator of $\mathbb{Z}$, and thus $\mathbb{Z}$ is a cyclic group. A cyclic group may have more than one generator:

Exercise 79. Show that -1 is a generator of $\mathbb{Z}$; that is that $\mathbb{Z} = \langle -1 \rangle$. ◊

Example 80. Consider the group $\mathbb{Z}_6$. $\langle 1 \rangle$ is computed as follows:

- $1 \equiv 1$
- $1 + 1 \equiv 2$
- $1 + 1 + 1 \equiv 3$
- $1 + 1 + 1 + 1 \equiv 4$
- $1 + 1 + 1 + 1 + 1 \equiv 5$
- $1 + 1 + 1 + 1 + 1 + 1 \equiv 0$
- Notice that we've already generated all the elements in $\mathbb{Z}_6$. So we don't have to worry about finding the additive integer multiples of 1^{-1} (Note that $(1^{-1} = 5)$), because these calculations can't produce any new elements.
- So $\langle 1 \rangle = \{1, 2, 3, 4, 5, 0\} = \mathbb{Z}_6$.

Therefore $\mathbb{Z}_6$ is a cyclic group generated by 1. ♦

Exercise 81. Show that $\langle 5 \rangle = \mathbb{Z}_6$. ◊

Exercise 82. Given a group G, suppose that $G = \langle a \rangle$. Prove that $G = \langle a^{-1} \rangle$. ◊

Example 83. The group of units, $U(9)$ is a cyclic group. As a set, $U(9)$ is $\{1, 2, 4, 5, 7, 8\}$. Computing $\langle 2 \rangle$, we get

$$\begin{aligned} \langle 2 \rangle &= \{2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1\} \\ &= \{2, 4, 8, 7, 5, 1\} \\ &= U(9) \end{aligned}$$

So $\langle 2 \rangle = \{2^n \pmod 9 : n \in \mathbb{Z}\} = U(9)$ ♦

Exercise 84. Find any other generators of $U(9)$ if they exist (say so if none others exist). ◊

11.5.2 Cyclic subgroups

In this section we further explore properties of the set $\langle a \rangle$ for arbitrary group elements $a \in G$. We have seen that in some cases, $\langle a \rangle$ is actually a group. We'll see in a minute that in fact $\langle a \rangle$ is *always* a group. Let's look at some examples first.

Example 85. Suppose that we consider $4 \in \mathbb{Z}$.

$$\langle 4 \rangle = \{\ldots, -8, -4, 0, 4, 8, \ldots\}.$$

which happens to be the set $4\mathbb{Z}$.

Exercise 86. Prove that $4\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. ◊

It follows from this exercise that $4\mathbb{Z}$ is the *cyclic subgroup* of $\mathbb{Z}$ generated by 4. ♦

Exercise 87. Let $H = \{2^n : n \in \mathbb{Z}\} = \langle 2 \rangle$ under multiplication.

(a) List the elements in H

(b) Show that $H \subset \mathbb{Q}^*$.

(c) Show that H is closed under multiplication.

(d) Show that H is closed under inverse.

(e) Is H a subgroup of Q^*? *Explain* your answer.

$\Diamond$

It follows from this exercise that H is the *cyclic subgroup* of $\mathbb{Q}^*$ generated by 2.

By now we've seen enough examples so that we're ready to prove the general result.

Proposition 88. Let G be a group and a be any element in G. Then the set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a.

PROOF. The identity is in $\langle a \rangle$ since $a^0 = e$. If g and h are any two elements in $\langle a \rangle$, then by the definition of $\langle a \rangle$ we can write $g = a^m$ and $h = a^n$ for some integers m and n. So $gh = a^m a^n = a^{m+n}$ is again in $\langle a \rangle$. Finally, if $g = a^n$ in $\langle a \rangle$, then the inverse $g^{-1} = a^{-n}$ is also in $\langle a \rangle$. Clearly, any subgroup H of G containing a must contain all the powers of a by closure; hence, H contains $\langle a \rangle$. Therefore, $\langle a \rangle$ is the smallest subgroup of G containing a. $\square$

Definition 89. Given a group G, for each $a \in G$, we call $\langle a \rangle$ the ***cyclic subgroup*** generated by a. $\triangle$

Let us now consider in particular the case of finite groups. Let G be a finite group, and let a be an element of G. Consider the set $A := \{a, a^2, a^3, \ldots\}$. Since $A \subset G$ and G is finite, the set A must also be finite. In particular, the list $\{a, a^2, a^3, \ldots\}$ must contain duplicate elements, since otherwise A would be infinite. We must therefore have $a^k = a^l$ for two different natural numbers k, l. This is the key fact in proving the following exercise:

Exercise 90. Let G be a finite group, and let $a \in G$ where $a \neq e$. Show there exists a natural number $m > 0$ such that $a^m = e$. (*Hint*) $\Diamond$

In view of the preceding exercise, we may make the following definition:

Definition 91. If a is an element of a group G, we define the ***order*** of a to be the smallest positive integer n such that $a^n = e$, and we write $|a| = n$. If there is no such integer n, we say that the order of a is infinite and write $|a| = \infty$ to denote the order of a. [4] △

Example 92. Let us consider the orders of different elements in the infinite group $\mathbb{Z}$.

- First, what is $|0|$? According to Definition 91, we need to find the smallest positive integer such that $n \cdot 0 = 0$ (remember, $\mathbb{Z}$ is an *additive* group. We get $n = 1$, so $|0| = 1$, and the cyclic subgroup generated by 0 is $\langle 0 \rangle = \{0\}$
- What is $|1|$? $1 + 1 = 2$; $1 + 1 + 1 = 3$; ... In fact you'll never get to 0 adding a positive number of ones. So $|1| = \infty$, and as we've seen, $\langle 1 \rangle = \mathbb{Z}$.
- Similarly, $|-1| = \infty$.

♦

Exercise 93.

(a) In the group $\mathbb{Z}_6$, What is $|1|$? What is $|5|$?

(b) Given any group G, If e is the identity element of G then what is $|e|$?

◊

Example 94. The order of $2 \in \mathbb{Z}_6$ is 3, because under repeated modular addition we have

$$2 \oplus 2 = 4; \qquad 2 \oplus 2 \oplus 2 = 0.$$

Therefore the cyclic subgroup generated by 2 is $\langle 2 \rangle = \{0, 2, 4\}$. ♦

[4] Yet another use of the term "order" and the absolute value sign. But you should be used to it by now.

Exercise 95. Find the orders and cyclic subgroups generated by each element of $U(9)$. ♢

Exercise 96. We have defined the order of a (denoted by $|a|$) as the smallest natural number such that $a^n = e$. On the other hand, we have $|\langle a \rangle|$ is equal to the order of the cyclic subgroup generated by a. Which is larger, $|a|$ or $|\langle a \rangle|$? *Explain* your answer. ♢

Exercise 97. Let G be a finite group, and let $a \in G$ such that $|a| = n$ for $n > 0$. Show that there exists a natural number m such that $a^{-1} = a^m$, and express m in terms of n. ♢

Example 98. Not every group is a cyclic group. Consider the symmetry group of an equilateral triangle S_3. S_3 has 6 elements: we saw the Cayley table for S_3 in the Symmetries chapter. You may verify by using the table that no single element generates the entire group. The subgroups of S_3 are shown in Figure 11.1. You may verify that every subgroup is cyclic. ♦

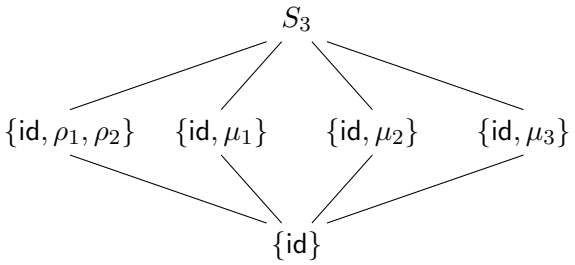


Figure 11.1. Subgroups of S_3

However, we can prove that:

Proposition 99. Every cyclic group is abelian.

PROOF. Let G be a cyclic group and $a \in G$ be a generator for G. If g and h are in G, then they can be written as powers of a, say $g = a^r$ and $h = a^s$. Since

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg,$$

G is abelian. □

11.5.3 Subgroups of cyclic groups

We can ask some interesting questions about cyclic subgroups of a group and subgroups of a cyclic group. If G is a group, which subgroups of G are cyclic? If G is a cyclic group, what type of subgroups does G possess?

Proposition 100. Every subgroup of a cyclic group is cyclic.

PROOF. The main tools used in this proof are the division algorithm and the Principle of Well-Ordering. Let G be a cyclic group generated by a and suppose that H is a subgroup of G. If $H = \{e\}$, then trivially H is cyclic. Suppose that H contains some other element g distinct from the identity. Then g can be written as a^n for some integer n. We can assume that $n > 0$. Let m be the smallest natural number such that $a^m \in H$. Such an m exists by the Principle of Well-Ordering.

We claim that $h = a^m$ is a generator for H. We must show that every $h' \in H$ can be written as a power of h. Since $h' \in H$ and H is a subgroup of G, $h' = a^k$ for some positive integer k. Using the division algorithm, we can find numbers q and r such that $k = mq + r$ where $0 \leq r < m$; hence,

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

So we can solve for a^r: $a^r = h^{-q} a^k$. Since a^k and h^{-q} are in H, a^r must also be in H. However, m was the smallest positive number such that a^m was in H; consequently, $r = 0$ and so $k = mq$. Therefore,

$$h' = a^k = a^{mq} = h^q$$

and H is generated by h. □

Corollary 101. The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

Proposition 102. Let G be a cyclic group of order n and suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.

PROOF. First suppose that $a^k = e$. By the division algorithm, $k = nq + r$ where $0 \leq r < n$; hence,

$$e = a^k = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = e^q a^r = a^r.$$

Since the smallest positive integer m such that $a^m = e$ is n, it follows that r cannot be a positive integer. So $r = 0$ is the only possibility.

Conversely, if n divides k, then $k = ns$ for some integer s. Consequently,

$$a^k = a^{ns} = (a^n)^s = e^s = e.$$

□

Proposition 103. Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.

PROOF. We wish to find the smallest integer m such that $e = b^m = a^{km}$. By Proposition 102, this is the smallest integer m such that n divides km or, equivalently, n/d divides $m(k/d)$. (Note that n/d and k/d are both integers, since d divides both n and k.) Since d is the greatest common divisor of n and k, n/d and k/d are relatively prime. Hence, for n/d to divide $m(k/d)$ it must divide m. The smallest such m is n/d. □

Corollary 104. The generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

Example 105. Let us examine the group $\mathbb{Z}_{16}$. The numbers 1, 3, 5, 7, 9, 11, 13, and 15 are the elements of $\mathbb{Z}_{16}$ that are relatively prime to 16. Each of these elements generates $\mathbb{Z}_{16}$. For example,

$$\begin{array}{lll} 1 \cdot 9 = 9 & 2 \cdot 9 = 2 & 3 \cdot 9 = 11 \\ 4 \cdot 9 = 4 & 5 \cdot 9 = 13 & 6 \cdot 9 = 6 \\ 7 \cdot 9 = 15 & 8 \cdot 9 = 8 & 9 \cdot 9 = 1 \\ 10 \cdot 9 = 10 & 11 \cdot 9 = 3 & 12 \cdot 9 = 12 \\ 13 \cdot 9 = 5 & 14 \cdot 9 = 14 & 15 \cdot 9 = 7. \end{array}$$

♦

11.6 Additional group and subgroup exercises

Note: most of these exercises are taken directly from Tom Judson's book.

1. Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$. How many elements are in each group? Are the groups the same? Why or why not?

2. Describe the symmetries of a rhombus and prove that the set of symmetries forms a group. Give Cayley tables for both the symmetries of a rectangle and the symmetries of a rhombus. Are the symmetries of a rectangle and those of a rhombus the same?

3. Describe the symmetries of a square and prove that the set of symmetries is a group. Give a Cayley table for the symmetries. How many ways can the vertices of a square be permuted? Is each permutation necessarily a symmetry of the square? The symmetry group of the square is denoted by D_4.

4. Give a multiplication table for the group $U(12)$.

5. Give an example of two elements A and B in $GL_2(\mathbb{R})$ with $AB \neq BA$.

6. Prove that the product of two matrices in $SL_2(\mathbb{R})$ is also in $SL_2(\mathbb{R})$.

7. Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

   is a group under matrix multiplication. This group, known as the ***Heisenberg group***, is important in quantum physics.

8. Prove that $\det(AB) = \det(A)\det(B)$ in $GL_2(\mathbb{R})$. Use this result to show that the binary operation in the group $GL_2(\mathbb{R})$ is closed; that is, if A and B are in $GL_2(\mathbb{R})$, then $AB \in GL_2(\mathbb{R})$.

9. Let $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on $\mathbb{Z}_2^n$ by

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

   Prove that $\mathbb{Z}_2^n$ is a group under this operation. This group is important in algebraic coding theory.

10. (a) Recall the discussion of Section 9.6, which explains how two apparently different groups can in fact be essentially the "same" group. Find two groups of order eight that we have studied are not the "same" in this sense, and explain why they can't be considered as examples of the "same" group.

    (b) Using the previous exercise (which introduces $\mathbb{Z}_2^n$), give an example of a third group that is not the "same" as the two groups you found in (a), and explain why it is not the "same".

11. Prove or disprove that every group containing six elements is abelian.

12. Give a specific example of some group G and elements $g, h \in G$ where $(gh)^n \neq g^n h^n$.
13. Let a and b be elements in a group G. Prove that $ab^n a^{-1} = (aba^{-1})^n$.
14. Let $U(n)$ be the group of units in $\mathbb{Z}_n$. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.
15. Prove that the inverse of $g_1 g_2 \cdots g_n$ is $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.
16. Prove the right and left cancellation laws for a group G; that is, show that in the group G, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$ for elements $a, b, c \in G$.
17. Show that if $a^2 = e$ for all $a \in G$, then G must be an abelian group.
18. Show that if G is a finite group of even order, then there is an $a \in G$ such that a is not the identity and $a^2 = e$.
19. Let G be a group and suppose that $(ab)^2 = a^2 b^2$ for all a and b in G. Prove that G is an abelian group.
20. Let $\mathbb{Z}_3 \times \mathbb{Z}_3$ be the set of all pairs (a, b) where $a, b \in \mathbb{Z}_3$, with the following group operation:

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 \cdot a_2, b_1 \cdot b_2),$$

so that multiplication mod 3 is performed separately on the first and second elements in the pairs.

21. Find all the subgroups of the symmetry group of an equilateral triangle.
22. Compute the subgroups of the symmetry group of a square.
23. Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Q}^*$.
24. Let $n = 0, 1, 2, \ldots$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Show that these subgroups are the only subgroups of $\mathbb{Z}$.
25. Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.
26. Let G consist of the 2×2 matrices of the form

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where $\theta \in \mathbb{R}$. Prove that G is a subgroup of $SL_2(\mathbb{R})$.

27. Prove that

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$

is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

28. Let G be the group of 2×2 matrices under addition and

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}.$$

Prove that H is a subgroup of G.

29. Prove or disprove: $SL_2(\mathbb{Z})$, the set of 2×2 matrices with integer entries and determinant one, is a subgroup of $SL_2(\mathbb{R})$.

30. The *quaternion group* (denoted by Q_8) consists of 8 elements: 1, i, j, k, -1, $-i$, $-j$, $-k$. You may find the Cayley table for Q_8 on `wolframalpha.com` or Wikipedia.

    (a) Find the orders of all 8 elements of Q_8.

    (b) Find all the subgroups of Q_8. (*Hint*)

31. Prove that the intersection of two subgroups of a group G is also a subgroup of G.

32. Prove or disprove: If H and K are subgroups of a group G, then $H \cup K$ is a subgroup of G.

33. Prove or disprove: If H and K are subgroups of a group G, then $HK = \{hk : h \in H \text{ and } k \in K\}$ is a subgroup of G. What if G is abelian?

34. Let G be a group. Show that

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$$

is a subgroup of G. This subgroup is called the ***center*** of G.

35. Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

36. Give an example of an infinite group in which every nontrivial subgroup is infinite.

37. Give an example of an infinite group in which every proper subgroup is finite.

38. If $xy = x^{-1}y^{-1}$ for all x and y in $G \setminus e$, prove that G must be abelian. (*Hint*)

39. If $(xy)^2 = xy$ for all x and y in $G \setminus e$, prove that G must be abelian. (*Hint*)

40. Prove or disprove: Every nontrivial subgroup of an non-abelian group is non-abelian.

41. Let H be a subgroup of G and

$$N(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$

Prove $N(H)$ is a subgroup of G. This subgroup is called the ***normalizer*** of H in G.

12

Cosets and Factor Groups

SHREK: For your information, there's a lot more to ogres than people think.

DONKEY: Example?

SHREK: Example... uh... ogres are like onions!

DONKEY: They stink?

SHREK: Yes... No!

DONKEY: Oh, they make you cry?

SHREK: No!

DONKEY: Oh, you leave 'em out in the sun, they get all brown, start sproutin' little white hairs...

SHREK: NO! Layers. Onions have layers. Ogres have layers... You get it? We both have layers.

Source: *Shrek* (movie), 2001.

Groups, like onions and ogres, also have layers. As we've seen, many groups have subgroups inside them. These subgroups can be used to define "layers" which are called *cosets*. And in some cases, the "layers" (cosets) themselves form groups, which are called *factor groups*.

Our examination of cosets will give us deep insight into the nature and structure of groups. We will be leaning heavily on the material from Chapter 4 (which will furnish us with motivating examples), Chapter 8 (which will aid us in our characterization of cosets), and of course Chapter 11. In the course of reading this chapter, you may want to review these chapters. So, here we go![1]

12.1 Definition of cosets

The concept of "coset" brings together two ideas that we've seen before: subgroups and equivalence classes. We'll see how cosets arise from this mix by using a familiar example.

Example 1. *(Modular addition déjà vu All Over Again)*

Back in Chapter 4 we defined modular equivalence (Definition 13), and in Proposition 18 we gave an alternative characterization:

$a \equiv b \pmod{m}$ iff $a - b = k \cdot m$, where k is an integer (that is, $k \in \mathbb{Z}$).

Exercise 2.

(a) Give 4 integers a that satisfy the equation: $a \equiv 0 \pmod{3}$.

(b) Give 4 integers a that satisfy the equation: $a \equiv 2 \pmod{3}$.

$\Diamond$

In Section 8.4 in the Equivalence Relations chapter, we saw that modular equivalence was indeed an *equivalence relation*, and gave rise to *equivalence classes*:

$$[0]_3 = \{\text{All integers equivalent to 0 mod 3}\} = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}.$$
$$[1]_3 = \{\text{All integers equivalent to 1 mod 3}\} = \{\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\}.$$
$$[2]_3 = \{\text{All integers equivalent to 2 mod 3}\} = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}.$$

[1] Thanks to Tom Judson for material used in this chapter.

Then in the Groups chapter we introduced an alternative notation for $[0]_3$, namely $3\mathbb{Z}$. Since every element of $[1]_3$ is $1 +$ an element of $3\mathbb{Z}$ (and similarly for $[2]_3$) it makes sense to introduce the notation:

$[1]_3 = 1 + 3\mathbb{Z}$.

$[2]_3 = 2 + 3\mathbb{Z}$.

Notice the pattern here. Recall that $3\mathbb{Z}$ is a *subgroup* of $\mathbb{Z}$. In order to "create" the equivalence class $1 + 3\mathbb{Z}$, we added a specific group element (namely, 1) to *every* element of the subgroup $3\mathbb{Z}$. The same holds true for $2 + 3\mathbb{Z}$ – in both cases the notation follows the pattern:

(selected group element) (group operation) (Subgroup).

An alternative notation that also makes sense is:

$[1]_3 = 3\mathbb{Z} + 1$

$[2]_3 = 3\mathbb{Z} + 2$,

which follows the pattern:

(Subgroup) (group operation) (selected group element). ⧫

Exercise 3.

(a) Write the 5 equivalence classes (subsets) of $\mathbb{Z}$) which make up $\mathbb{Z}_5$ in using our new notation.

(b) Write all elements of $\mathbb{Z}_7$ using our new notation.

◊

The same pattern that we saw in the preceding example can actually be generalized to any group possessing a subgroup:

Definition 4. Let G be a group and H a subgroup of G. The ***left coset*** of H with ***representative*** $g \in G$ is defined as the following set:

$$gH = \{gh : h \in H\}.$$

Right cosets are defined similarly by

$$Hg = \{hg : h \in H\}.$$

(Note that in the preceding equations, "gh" denotes $g \circ h$ where $\circ$ is the group operation. This is similar to our writing xy to denote $x \cdot y$ in conventional algebra). △

Definition 4 looks a little different from Example 1, e.g. we have gH instead of $3 + \mathbb{Z}$. But in fact the pattern is the same: (group element) (group operation) (Subgroup). If the group operation is $+$, we will typically write left cosets as $g + H$ and right cosets as $H + g$. For all other group operations, we'll use the more compact notation gH and Hg.

Now Definition 4 distinguishes between a *left* and *right* cosets. In Example 1, $1 + 3\mathbb{Z}$ (left coset) and $3\mathbb{Z} + 1$ (right coset) were in fact the same set; and this held for the other two cosets: the left and right cosets were equal. But is this always the case? Interestingly not:

Example 5.

- Let H be the subgroup of S_3 defined by the permutations $\{(1), (123), (132)\}$. (Here we are using (1) to denote the identity permutation id.) The left cosets of H are

$$(1)H = (123)H = (132)H = \{(1), (123), (132)\}$$
$$(12)H = (13)H = (23)H = \{(12), (13), (23)\}.$$

  and the right cosets of H are

$$H(1) = H(123) = H(132) = \{(1), (123), (132)\}$$
$$H(12) = H(13) = H(23) = \{(12), (13), (23)\}.$$

  So in this case again the left cosets and right cosets are the same.

- *But*, let K be the subgroup of S_3 defined by the permutations $\{(1), (12)\}$. Then the left cosets of K are

$$(1)K = (12)K = \{(1), (12)\}$$
$$(13)K = (123)K = \{(13), (123)\}$$
$$(23)K = (132)K = \{(23), (132)\};$$

and the right cosets of K are

$$K(1) = K(12) = \{(1), (12)\}$$
$$K(13) = K(132) = \{(13), (132)\}$$
$$K(23) = K(123) = \{(23), (123)\}.$$

The left and right cosets are *not* the same.

♦

Unequal left and right cosets are actually very common. So let's get some practice determining left and right cosets:

Exercise 6. Let H be the subgroup of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ consisting of the elements 0 and 3. (We are using our simplified notation here: '0' represents $\overline{0}$, etc.) The left cosets are

$$0 + H = 3 + H = \{0, 3\}$$
$$1 + H = 4 + H = \{1, 4\}$$
$$2 + H = 5 + H = \{2, 5\}.$$

What are the right cosets? Are the left and right cosets equal? ◊

Exercise 7. List the left and right cosets of the subgroups in each of the following. Tell whether the left and right cosets are equal.

(Recall that A_n (the alternating group) is the set of even permutations, on n objects; D_4 is the group of symmetries of a square; and $\mathbb{T}$ is the group of complex numbers with modulus 1, under the operation of multiplication.)

(a) $\langle 8 \rangle$ in $\mathbb{Z}_{24}$

(b) $\langle 3 \rangle$ in $U(8)$

(c) $4\mathbb{Z}$ in $\mathbb{Z}$

(d) $H = \{(1), (123), (132)\}$ in S_4

(e) $K = \{(1), (12), (13), (14)\}$ in S_4

(f) A_4 in S_4

(g) A_n in S_n

(h) D_4 in S_4

(i) $\mathbb{T}$ in $\mathbb{C}^*$

◊

Remark 8. From now on, if the left and right cosets coincide, or if it is clear from the context to which type of coset that we are referring, we will use the word *coset* without specifying left or right. △

From the exercises and examples we have seen so far, you might have seen a pattern; you might have started thinking, "hmmmm, I wonder if the group being abelian causes the left and right cosets to be equal?" This makes sense, because abelian means you get the same result whether you compose on the left or on the right. So let's prove it:

Exercise 9. Show that if G is an *abelian* group and H is a subgroup of G, then any left coset gH is equal to the right coset Hg. (*Hint*) ◊

Are abelian groups the only groups in which left cosets are equal to right cosets? The answer is No (see the first case in Example 5. So we still haven't answered the question of what is the most general situation in which left cosets and right cosets are equal. We'll take this issue up again in Section 12.4.

12.2 Cosets and partitions of groups

In Example 1, the cosets that we described were equivalence classes. We saw in Chapter 8 that equivalence classes form a *partition* which divides up the containing set into disjoint subsets. This is actually a general fact that is true for all cosets, and we will prove this below. In the proof, we will need the following proposition, which shows there are several different ways of characterizing when two cosets are equal.

Proposition 10. Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. The following conditions are equivalent.

1. $g_1H = g_2H$;
2. $g_1^{-1}g_2 \in H$.
3. $g_2 \in g_1H$;
4. $g_2H \subset g_1H$; (*Note:* "$\subset$" means equality is also possible)
5. $Hg_1^{-1} = Hg_2^{-1}$;

The proof of this Proposition is laid out in the Exercise 11 below, and you are asked to fill in the details. Parts (a)-(f) of the exercise establish the following steps:

$$(1) \underset{(a)}{\Rightarrow} (2) \underset{(b)}{\Rightarrow} (3) \underset{(c)}{\Rightarrow} (4) \underset{(d)}{\Rightarrow} (1) \qquad \text{and} \qquad (2) \underset{(e,f)}{\Leftrightarrow} (5).$$

Exercise 11.

(a) Show that condition (1) implies condition (2). (*Hint*)

(b) Show that condition (2) implies condition (3). (*Hint*)

(c) Show that condition (3) implies condition (4). (*Hint*)

(d) Show that condition (4) implies condition (1). (*Hint*)

(e) Show that condition (2) implies condition (5). (*Hint*)

(f) Show that condition (5) implies condition (2).

◊

Exercise 12. Proposition 10 deals with *left* cosets. A parallel proposition holds for right cosets. List the five equivalent conditions for *right* cosets that correspond to the five conditions given in Proposition 10. ◊

Now we're ready to prove that the cosets of a subgroup always form a partition of the group that contains it:

Proposition 13. Let H be a subgroup of a group G. Then the left cosets of H in G partition G. That is, the group G is the disjoint union of the left cosets of H in G.

PROOF. Let g_1H and g_2H be two cosets of H in G. We must show that either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose that $g_1H \cap g_2H \neq \emptyset$ and $a \in g_1H \cap g_2H$. Then by the definition of a left coset, $a = g_1h_1 = g_2h_2$ for some elements h_1 and h_2 in H. Hence, $g_1 = g_2h_2h_1^{-1}$ or $g_1 \in g_2H$. By Proposition 10, $g_1H = g_2H$. □

Remark 14. Right cosets also partition G. The partition may not be the same as the partition using the left cosets, since the left and right cosets

aren't necessarily equal, The proof of this fact is exactly the same as the proof for left cosets except that all group multiplications are done on the right side of H. △

Let's consider now the question of how many cosets there are for a particular subgroup within a given group. First, we define some convenient notation:

Definition 15. Let G be a group and H be a subgroup of G. Define the ***index*** of H in G to be the number of left cosets of H in G. We will denote the index by $[G : H]$. △

Example 16. Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then looking back at Exercise 6, we see that $[G : H] = 3$. ♦

Exercise 17. Based on your work in Exercise 6, how many right cosets of $H = \{0, 3\}$ were there in $\mathbb{Z}_6$? ◊

Example 18. Suppose that $G = S_3$, $H = \{(1), (123), (132)\}$, and $K = \{(1), (12)\}$. Then looking back at Example 5, we can see that $[G : H] = 2$ and $[G : K] = 3$. ♦

Exercise 19. How many right cosets of $H = \{(1), (123), (132)\}$ in S_3 were there? How about right cosets of $K = \{(1), (12)\}$ in S_3? ◊

Exercise 20. Using your work from Exercise 7, find:

(a) $[\mathbb{Z}_{24} : \langle 8\rangle]$ and the number of right cosets of $\langle 8\rangle$ in $\mathbb{Z}_{24}$.

(b) $[U(8) : \langle 3\rangle]$ and the number of right cosets of $\langle 3\rangle$ in $U(8)$.

(c) $[\mathbb{Z} : 4\mathbb{Z}]$ and the number of right cosets of $4\mathbb{Z}$ in $\mathbb{Z}$.

(d) $[S_4 : \{(1), (123), (132)\}]$ and the number of the right cosets of $\{(1), (123), (132)\}$ in S_4.

(e) $[S_4 : \{(1), (12), (13), (14)\}]$ and the number of right cosets of $\{(1), (12), (13), (14)\}$ in S_4.

(f) $[S_4 : A_4]$ and the number of right cosets of A_4 in S_4.

(g) $[S_n : A_n]$ and the number of right cosets of A_n in S_n.

(h) $[S_4 : D_4]$ and the number of right cosets of D_4 in S_4.

(i) $[\mathbb{C}^* : \mathbb{T}]$ and the number or right cosets of $\mathbb{T}$ in $\mathbb{C}^*$.

$\Diamond$

As the last several examples and exericses seem to suggest, though the the left and right cosets of a subgroup aren't necessarily equal, it seems the *number* of them is the same. Indeed we can prove this:

Proposition 21. Let H be a subgroup of a group G. The number of left cosets of H in G is the same as the number of right cosets of H in G.

PROOF. Let L and R denote the set of left and right cosets of H in G, respectively. If we can define a bijection $\phi : L \to R$, then the proposition will be proved. If $gH \in L$, let $\phi(gH) = Hg^{-1}$. By Proposition 10, the map ϕ is well-defined; that is, if $g_1H = g_2H$, then $Hg_1^{-1} = Hg_2^{-1}$. To show that ϕ is one-to-one, suppose that

$$Hg_1^{-1} = \phi(g_1H) = \phi(g_2H) = Hg_2^{-1}.$$

Again by Proposition 10, $g_1H = g_2H$. The map ϕ is onto since $\phi(g^{-1}H) = Hg$. $\square$

Exercise 22. Describe the left and right cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$. What is the index of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$? Are the left and right cosets equal? $\Diamond$

Exercise 23. Find the left and right cosets of $\{1, -1, i, -i\}$ in Q_8. What is the index of $\{1, -1, i, -i\}$ in Q_8? Are the left and right cosets equal? [2] $\Diamond$

[2] Q_8 is the *quaternion group*, mentioned in Exercise 30 of Chapter 11. You will need the Cayley table for the quaternions to figure out the left and right cosets, which can be found on Wikipedia or another web source.

12.3 Lagrange's theorem, and some consequences

12.3.1 Lagrange's theorem

At the beginning of the chapter, we compared cosets to layers of an onion. Indeed, as we saw in the last section, this is a good analogy because the cosets of a subgroup partion the group. However, an even better analogy is to slices of a loaf of sandwich bread–because as we'll see in this section, every coset of a particular subgroup within a given group has exactly the same size.

What may we conclude from this? Let us push our analogy with sandwich bread a little farther. Suppose the bread has raisins in it, and each slice has exactly the same number of raisins. Then the number of raisins in the loaf must be equal to the sum of all raisins in all the slices, that is:

$$|\text{raisins in loaf}| = |\text{raisins in each slice}| \cdot |\text{slices}|,$$

where as usual the $|\cdots|$ notation signifies "size" or "number of". Applying this same reasoning to groups and their subgroups leads to a very general result called *Lagrange's theorem*, which will enable us to prove some surprising properties of subgroups, their elements, and even some results in number theory. So let's get started.

Remark 24. In the following discussion, for specificity's sake we will refer to left cosets. However, just lke we saw in the last section (Remark 14), everything we say about left cosets is also true for right cosets. Indeed, to prove the cases for the right cosets, you simply need to take the left coset proofs given below and operate on the right instead of the left. △

As we mentioned in our raisin bread analogy, to prove Lagrange's theorem, we need to prove that every left coset of a subgroup has the exactly the same size. Once we have that though, Lagrange's Theorem comes immediately from it:

Proposition 25. Let H be a subgroup of G with $g \in G$ and define a map $\phi : H \to gH$ by $\phi(h) = gh$. The map ϕ is a bijection; hence, the number of elements in H is the same as the number of elements in gH.

Proof. We first show that the map ϕ is one-to-one. Suppose that $\phi(h_1) = \phi(h_2)$ for elements $h_1, h_2 \in H$. We must show that $h_1 = h_2$, but $\phi(h_1) = gh_1$ and $\phi(h_2) = gh_2$. So $gh_1 = gh_2$, and by left cancellation $h_1 = h_2$. To show

that ϕ is onto is easy. By definition every element of gH is of the form gh for some $h \in H$ and $\phi(h) = gh$. □

Proposition 26.[Lagrange's Theorem] Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.

PROOF. The group G is partitioned into $[G : H]$ distinct left cosets. Each left coset has $|H|$ elements; therefore, $|G| = [G : H]|H|$. □

And there we have it. The number of elements in a subgroup *must* divide evenly into the number of elements in the group; you can't have just any number of elements in a subgroup. This is a very powerful tool to give insight into the structure of groups.

Example 27. Let G be a group with $|G| = 25$. Then since 2 doesn't divide 25 evenly, Lagrange's Theorem implies that G can't possibly have a subgroup with 2 elements. ♦

Exercise 28. Suppose that G is a finite group with an element g of order 5 and an element h of order 7. Why must $|G| \geq 35$? ◊

Exercise 29. Suppose that G is a finite group with 60 elements. What are the possible orders for subgroups of G? ◊

We can take the result in Lagrange's theorem a step farther by considering subgroups of subgroups.

Proposition 30. Let H and K be subgroups of a finite group G such that $G \supset H \supset K$. Then

$$[G : K] = [G : H][H : K].$$

PROOF. Observe that

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K].$$

□

Historical Note

Joseph-Louis Lagrange (1736–1813), born in Turin, Italy, was of French and Italian descent. His talent for mathematics became apparent at an early age. Leonhard Euler recognized Lagrange's abilities when Lagrange, who was only 19, communicated to Euler some work that he had done in the calculus of variations. That year he was also named a professor at the Royal Artillery School in Turin. At the age of 23 he joined the Berlin Academy. Frederick the Great had written to Lagrange proclaiming that the "greatest king in Europe" should have the "greatest mathematician in Europe" at his court. For 20 years Lagrange held the position vacated by his mentor, Euler. His works include contributions to number theory, group theory, physics and mechanics, the calculus of variations, the theory of equations, and differential equations. Along with Laplace and Lavoisier, Lagrange was one of the people responsible for designing the metric system. During his life Lagrange profoundly influenced the development of mathematics, leaving much to the next generation of mathematicians in the form of examples and new problems to be solved.

12.3.2 Orders of elements, Euler's theorem, Fermat's little theorem, and prime order

Now let's really put Lagrange's theorem to work. Note that Lagrange's theorem is an extremely general result–it applies to *any* subgroup of *any* group. So let's consider one particular type of subgroup, namely the cyclic subgroups $\langle g \rangle$ generated by the elements g of a given group G (see Proposition 88 in Section 11.5.2 of the Groups chapter for the definition of $\langle g \rangle$, and the proof that it is indeed a group).

Proposition 31. Suppose that G is a finite group and $g \in G$. Then the order of g must divide the number of elements in G.

PROOF. The order of a group element g, which is denoted as $|g|$, is defined in Definition 91 in Section 11.5.2 of the Groups chapter. We indicated in Exercise 96 in that same section that $|g|$ is equal to $|\langle g \rangle|$, which is the order of the cylic subgroup generated by g. It follows immediately from Lagrange's theorem that $|g|$ must divide $|G|$. □

To show the power of this result, we'll apply it to the group of units $U(n)$ which was introduced in Section 11.2.1 of the Groups chapter.

But before we do this, let's do some exploration. Recall that the elements of $U(n)$ are the positive integers that are less than n and relatively prime to n (we showed in Exercise 30 of Section 11.2.1 that these elements actually form a group. There is a special notation for the number of elements in $U(n)$:

Definition 32. For $n > 1$, define $\phi(n)$ as the number of natural numbers that are less than n and relatively prime to n. Alternatively, we can say that $\phi(n)$ is the

number of natural numbers m where $m < n$ and $\gcd(m, n) = 1$. In order to make ϕ a function on the natural numbers, we also define $\phi(1) = 1$. The function ϕ is called the ***Euler ϕ- function***. △

Exercise 33. Evaluate the following:

(a) $\phi(12)$

(b) $\phi(16)$

(c) $\phi(20)$

(d) $\phi(23)$

(e) $\phi(51)$

(f) $\phi(p)$, where p is prime.

(g) $\phi(p^2)$, where p is prime.

(h) $\phi(p^n)$, where p is prime and $n \in \mathbb{N}$.

(i) $\phi(pq)$, where p and q are primes and $p \neq q$.

(*Hint*) ◊

If we now apply Lagrange's theorem to $U(n)$, we obtain an important result in number theory which was first proved by Leonhard Euler in 1763.

Proposition 34. (*Euler's theorem*) Let a and n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. First, let r be the remainder when a is divided by n. We may consider r as an element of $U(n)$.

As noted above, the order of $U(n)$ is $\phi(n)$. Lagrange's theorem then tells us that $|r|$ divides $\phi(n)$, so we can write: $\phi(n) = k|r|$, where $k \in \mathbb{N}$. Consequently, considering r as an element of $U(n)$, we have $r^{\phi(n)} = r^{k|r|} = (r^{|r|})^k = (1)^k = 1$ (note that the multiplication that is being used here is *modular* multiplication, not regular multiplication).

Finally, we may use the fact that $a \equiv r \pmod{n}$ and apply Exercise 45 in Section 4.4.1 (Modular Arithmetic chapter) to conclude that $a^{\phi(n)} \equiv 1 \pmod{n}$.

□

Exercise 35.

(a) Verify Euler's theorem for $n = 15$ and $a = 4$.

(b) Verify Euler's theorem for $n = 22$ and $a = 3$.

◊

Exercise 36. Evaluate the following, using the results of Exercise 33

(a) mod $(5^{200}, 12)$

(b) mod $(13^{48}, 16)$

(c) mod $(9^{200}, 20)$

(d) mod $(15^{231}, 23)$

(e) mod $(10^{33}, 51)$

(f) mod $\left(\left(\frac{p+1}{2}\right)^p, p\right)$, where p is prime.

(g) mod $((p+1)^{p^2}, p^2)$, where p is prime.

♢

In the following exercise you will prove *Fermat's little theorem*, which may be thought of as a special case of Euler's theorem:

Exercise 37. Suppose that p is a prime number, and a is a natural number which is relatively prime to p. Show that $a^{p-1} \equiv 1 \bmod p$. ♢

We can also apply Proposition 31 to groups of prime order, as in the following exercise.

Exercise 38. Let G be a group such that $|G| = p$, where p is a prime number.

(a) Let a be an element of $G \setminus \{e\}$. What does Proposition 31 tell us about $|a|$?

(b) Prove that G is cyclic.

(c) Describe the set of generators of G (recall that $g \in G$ is a generator of G if $\langle g \rangle = G$.)

♢

The results of the preceding exercise can be summarized as follows:

Proposition 39. Let $|G| = p$ with p a prime number. Then G is cyclic and any $g \in G$ such that $g \neq e$ is a generator.

Later we will use this proposition to show that all groups of prime order p are the "same" in some sense (see Section 15.5.1 of the Isomorphisms chapter).

Finally, we can use Lagrange's theorem to show that groups of prime order have a very simple structure:

Exercise 40. Let G be a group of prime order. Use Lagrange's Theorem to show that the only proper subgroup of G is the trivial subgroup $\{e\}$. ♢

Exercise 40 shows that groups of prime order (such as $\mathbb{Z}_p$) are "simple" in the sense that they don't contain any nontrivial subgroups. In Section 12.5 we will talk more about "simple" groups.

12.4 Factor groups and normal subgroups

We saw in Section 12.1 that if H is a subgroup of a group G, then right cosets of H in G are not always the same as left cosets. The *number* of right cosets and left cosets are always equal, and the number of elements in the left and right cosets match; but the right and left cosets *themselves* may not equal each other (it is not always the case that $gH = Hg$ for all $g \in G$). But as we saw sometimes they do equal each other. The subgroups for which this property holds play a critical role in group theory: they allow for the construction of a new class of groups, called factor or quotient groups.

12.4.1 Normal subgroups

First, let's give a name to these nice subgroups:

Definition 41. A subgroup H of a group G is ***normal*** in G if $gH = Hg$ for all $g \in G$. That is, a normal subgroup of a group G is one in which the right and left cosets are precisely the same. △

Example 42. Think back to Example 5 earlier in the chapter. H was the subgroup of S_3 consisting of elements (1) and (12). Since

$$(123)H = \{(123), (13)\} \quad \text{and} \quad H(123) = \{(123), (23)\},$$

H cannot be a normal subgroup of S_3. However, the subgroup K, consisting of the permutations (1), (123), and (132), is normal since the cosets of N are

$$N = \{(1), (123), (132)\}$$
$$(12)N = N(12) = \{(12), (13), (23)\}.$$

♦

Exercise 43. Looking back at Exercise 7, which of the subgroups were normal? ◊

Exercise 44. Is $SL_2(\mathbb{R})$ a normal subgroup of $GL_2(\mathbb{R})$? Prove or disprove. (*Hint*) ◊

Exercise 45. Is $\{1, -1, i, -i\}$ a normal subgroup of Q_8? ◊

Exercise 46. Prove that any subgroup of an abelian group is normal. (*Hint*) ◊

Now let's see if you can prove some general facts about normal subgroups. Here's an interesting one that's not too hard to prove:

Exercise 47. Prove that for *any* group G, the set $\{e\}$ is a normal subgroup of G (in other words the identity of group is always a normal subgoup). ◊

And here's an alternative way to characterize normal subgroups:

Exercise 48. Show that a subgroup $H \subset G$ is normal iff every left coset of H is also a right coset of H. ◊

The following proposition can be useful when trying to prove that a certain subgroup is normal. It gives several different characterizations of normal subgroups.

Proposition 49. Let G be a group and N be a subgroup of G. Then the following statements are equivalent.

1. The subgroup N is normal in G.
2. For all $g \in G$, $gNg^{-1} \subset N$.
3. For all $g \in G$, $gNg^{-1} = N$.

PROOF. (1) $\Rightarrow$ (2). Since N is normal in G, $gN = Ng$ for all $g \in G$. Hence, for a given $g \in G$ and $n \in N$, there exists an n' in N such that $gn = n'g$. Therefore, $gng^{-1} = n' \in N$ or $gNg^{-1} \subset N$.

(2) $\Rightarrow$ (3). Let $g \in G$. Since $gNg^{-1} \subset N$, we need only show $N \subset gNg^{-1}$. For $n \in N$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Hence, $g^{-1}ng = n'$ for some $n' \in N$. Therefore, $n = gn'g^{-1}$ is in gNg^{-1}.

(3) $\Rightarrow$ (1). Suppose that $gNg^{-1} = N$ for all $g \in G$. Then for any $n \in N$ there exists an $n' \in N$ such that $gng^{-1} = n'$. Consequently, $gn = n'g$ or $gN \subset Ng$. Similarly, $Ng \subset gN$. □

Proposition 49 enables us to formulate an alternative definition for normal subgroups:

Definition 50. Given a group G, a subgroup $H \subset G$ is called a ***normal subgroup*** if for every $g \in G$ and for every $h \in H$, we have that $ghg^{-1} \in H$. (Alternatively, we can write this condition as: $gHg^{-1} = H$.) △

Exercise 51. Prove that Definition 50 is equivalent to Definition 41. (*Hint*) ◊

Exercise 52.

(a) Show that if H is a subgroup of G and $|H| = k$, then for any $g \in G$ it's true that gHg^{-1} is also a subgroup of G and $|gHg^{-1}| = k$.

(b) If a group G has exactly one subgroup H of order k, prove that H is normal in G. (*Hint*)

$\Diamond$

Finally, here's one that will be very useful in a couple of sections.

Exercise 53.

(a) Let $H \subset G$ be a normal subgroup, and let $g \in G, h \in H$. Show that $g^{-1}hg \in H$.

(b) Let $H \subset G$ be a normal subgroup, and let $g \in G, h \in H$. Use part (a) to show that there exists an $h' \in H$ such that $hg = gh'$.

(c) Let $H \subset G$ be a normal subgroup, and suppose $x_1 \in g_1H$ and $x_2 \in g_2H$. Prove that $x_1x_2 \in g_1g_2H$. (*Hint*)

$\Diamond$

12.4.2 Factor groups

So what's the hubbub about these normal subgroups? We've been promising a grand revelation. It turns out that the cosets of normal subgroups have some very special properties.

Example 54. Consider the normal subgroup $3\mathbb{Z}$ of $\mathbb{Z}$ that we started exploring at the beginning of the chapter. The cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ were

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{\ldots, -3, 0, 3, 6, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

Now just for curiosity's sake, let's say we took *every* element in $0 + 3\mathbb{Z}$ and added them to *every* element in $1 + 3\mathbb{Z}$. What would be the resulting set? Try some examples: take an arbitrary element of $0 + 3\mathbb{Z}$, and add to it an arbitrary element of $1 + 3\mathbb{Z}$. You will find that the result is always in $1 + 3\mathbb{Z}$. Let's give a proof of this. First let's give some notation:

Definition 55.(*Set addition*) Let A and B be two sets of real numbers. Then the ***sum*** $A + B$ is defined as the set:

$$A + B := \{a + b, \text{ where } a \in A \text{ and } b \in B\}.$$

△

Notice that we are giving a *new* meaning to the symbol '+', because we are applying it to *sets* rather than *numbers*.

In terms of this new notation, what we're trying to prove is:

$$(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) = 1 + 3\mathbb{Z}.$$

As we've done many times before, we may prove that these two sets are equal by showing that all elements of the left-hand set are contained in the right-hand set, and vice versa. So let's take an arbitrary element of $(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z})$. We may write this element as $(0 + 3m) + (1 + 3n)$, where $m, n \in \mathbb{Z}$. Basic algebra gives us:

$$(0 + 3m) + (1 + 3n) = 1 + 3(m + n),$$

which is in $1 + 3\mathbb{Z}$. This shows that:

$$(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) \subset 1 + 3\mathbb{Z}.$$

On the other hand, we may write an arbitrary element of $1 + 3\mathbb{Z}$ as $1 + 3k$, which is equal to $0 + (1 + 3k)$. Since $0 \in 0 + 3\mathbb{Z}$, we have

$$(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) \supset 1 + 3\mathbb{Z},$$

and the proof is complete.

Let's step back and see what we've done. We've taken one coset of $3\mathbb{Z}$ (i.e. $0 + 3\mathbb{Z}$), and "added" a second coset (i.e. $1 + 3\mathbb{Z}$) to it, to get a third coset of $3\mathbb{Z}$. This sounds like closure. We can do the same thing with all pairs of cosets, and obtain the following "addition" table:

$+$	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$0 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$1 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$
$2 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$

Indeed we have closure. It's beginning to look like we have a group here. Actually, we can see an identity ($0+3\mathbb{Z}$) and an inverse for every coset (for example $[1 + 3\mathbb{Z}]^{-1} = 2 + 3\mathbb{Z}$). It turns that the associative property also holds: this follows from the associativity of ordinary addition. So we got it: the cosets of $3\mathbb{Z}$ *themselves* form a group! (Note the Cayley table for this group looks suspiciously the same as the Cayley table for $\mathbb{Z}_3$; we'll pick up on this in the Isomorphisms chapter.) ♦

So *this* is the grand revelation about normal subgroups: *the cosets of a normal subgroup form a group.* But we shouldn't jump the gun: we've only shown it's true

for a special case. Now we have to get down to the hard work of proving it in general. First we have to generalize Definition 55 to other group operations.

Definition 56.(*Set composition*) Let A and B be two subsets of a group G. Then the ***composition*** $A \circ B$ (or AB) is defined as the set:

$$A \circ B := \{ab, \text{ where } a \in A \text{ and } b \in B\}.$$

△

The reason that normal subgroups are special is that set composition defines an operation on cosets:

Proposition 57. Let N be a normal subgroup of a group G. If $a, b \in G$, then $aN \circ bN = abN$.

PROOF. The proof parallels the argument in Example 54. Let $x \in aN$ and $y \in bN$. Using Exercise 53 part (c), we may conclude that $xy \in abN$. This shows that $aN \circ bN \subset abN$. On the other hand, let $z \in abN$. Then $z = ae \circ bn$ for some $n \in N$, which implies that $z \in aN \circ bN$. This shows that $aN \circ bN \supset abN$, and the proof is finished. □

Proposition 58. Let N be a normal subgroup of a group G. The cosets of N in G form a group under the operation of set composition.

PROOF. We have shown that the set composition operation is well-defined and closed on the set of cosets of N, provided that N is normal. Associativity follows by the associativity of the group operation defined on G. Using Proposition 57 we have that $eN \circ aN = aN \circ eN = aN$, so $eN = N$ is an identity. Proposition 57 also gives us that $g^{-1}N \circ gN = gN \circ g^{-1}N = eN$, so the inverse of gN is $g^{-1}N$. □

Let's define a special notation for our new discovery.

Definition 59. If N is a normal subgroup of a group G, then the group of cosets of N under the operation of set composition is denoted as G/N This group is called the ***factor*** or ***quotient group*** of G and N. △

Note that the order of G/N is $[G : N]$, the number of cosets of N in G.

Remark 60. In Example 54 above, the factor group would have been labeled $\mathbb{Z}/3\mathbb{Z}$. In general, the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is normal. The cosets of the factor group $\mathbb{Z}/n\mathbb{Z}$ then are

$$n\mathbb{Z}; \quad 1 + n\mathbb{Z}; \quad 2 + n\mathbb{Z}; \quad \cdots \quad (n-1) + n\mathbb{Z}.$$

and the sum of the cosets $k+\mathbb{Z}$ and $l+\mathbb{Z}$ is $k+l+\mathbb{Z}$. Notice that we have written our cosets additively, because the group operation is integer addition. △

It is very important to remember that the elements in a factor group are not the elements of the original group, but *sets of elements* in the original group. As well then, the operation for the factor group is not the original operation of the group (which was used to compose elements), but a convenient derivative of it that we use to compose sets together. Both of these facts take a second to get use to, so let's practice:

Example 61. Consider the normal subgroup of S_3, $H = \{(1), (123), (132)\}$ which we started exploring in Example 5. The cosets of H in S_3 were H and $(12)N$. Using the group operation from Defintion 59 to compose these cosets together, the factor group S_3/N then has the following multiplication table.

	N	$(12)N$
N	N	$(12)N$
$(12)N$	$(12)N$	N

Notice that S_3/N is a smaller group than S_3 (2 elements compared to 6 eleemnts). So the factor group then displays a pared down amount of information about S_3. Actually, $N = A_3$, the group of even permutations, and $(12)N = \{(12), (13), (23)\}$ is the set of odd permutations. The information captured in G/N is parity; that is, multiplying two even or two odd permutations results in an even permutation, whereas multiplying an odd permutation by an even permutation yields an odd permutation. This information, as well as the Cayley table above, might suggest to you that the factor group is equivalent to another group we know. Again, we'll pick up on this in the Isomorphisms chapter. ♦

Now it's your turn:

Exercise 62. Give the multiplication tables for the following factor groups:

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

(b) $\mathbb{Z}/6\mathbb{Z}$

(c) $\mathbb{Z}_{24}/\langle 8\rangle$

(d) $\mathbb{Z}_{20}/\langle 4\rangle$

(e) $\mathbb{Z}_6/\{0,3\}$

(f) $\mathbb{Z}_8/\{0,4\}$

(g) $U(8)/\langle 3\rangle$

(h) $U(20)/\langle 3\rangle$

◊

Example 63. Consider the dihedral group D_n that we studied in the Symmetries chapter, which was the group of symmetries (rotations and reflections) of a regular

n sided polygon. We determined in the latter part of that chapter that D_n was actually generated by the two elements r and s, satisfying the relations

$$r^n = id$$
$$s^2 = id$$
$$srs = r^{-1}.$$

The element r generates the cyclic subgroup of rotations, R_n, of D_n. Since $srs^{-1} = srs = r^{-1} \in R_n$, then by Definition 50 the group of rotations is a normal subgroup of D_n; therefore, D_n/R_n is a group. Now there are $2n$ symmetries in D_n and n rotations in R_n; so Lagrange's Theorem tells us the number of cosets, $[D_n : R_n] = \frac{|D_n|}{|R_n|} = \frac{2n}{n} = 2$.

Since R_n, the rotations, are one of the cosets, the reflections must be the other coset. So the group D_n/R_n boils down to to two elements, rotations and reflections, described by a 2×2 multiplication table. ♦

Exercise 64. Construct the multiplication table for D_n/R_n. ◊

12.5 The simplicity of the alternating group

In the previous section we talked about how a normal subgroup enables us to "factor" a group to obtain a group with fewer elements (i.e. the group of cosets.) In some way this is similar to the idea of factoring positive integers as a product of smaller numbers. A natural question then is whether there are groups that can't be "factored": in other words, Are there groups which have no normal subgroups?

Actually, in Exercise 47 you've already answered that question: for any group, the identity $\{e\}$ is a normal subgroup. But factoring by $\{e\}$ doesn't give a group with fewer elements, because the number of cosets of the identity in any group G is (by Lagrange's Theorem)

$$\frac{|G|}{|\{e\}|} = \frac{|G|}{1} = |G|.$$

Thus factoring a group by $\{e\}$ is kind of like dividing an integer by 1: it doesn't change anything. So let's change our question to: Are there groups which have no *nontrivial* subgroups? Such groups would be like prime numbers: they can't be factored any further.

A group with no nontrivial normal subgroups is called a ***simple group***. In a way, simple groups are the "prime numbers" in group theory. Just like any positive integer uniquely factors into a product of prime numbers, it turns out that any

group can be uniquely factored into a series of simple groups. (Unfortunately, proving this is beyond the scope of this course.)

On the other hand, simple groups are somewhat more complicated than prime numbers. There are several classes of simple groups, and it's taken mathematicians hundreds of years to classify them. (Some simple groups defy classification: see the Historical Note at the end of this section.) We've already seen one such class: the groups of prime order. As we noted following Exercise 40, these groups are simple since they have no nontrivial proper subgroups.

We'll take the rest of this section to demonstrate another class of simple groups: we'll show that the alternating groups, A_n, are simple for $n \geq 5$. We will prove this result by looking at properties of 3-cycles. The strategy is to establish the following two facts:

(1) The only normal subgroup of $A_n (n \geq 3)$ that contains a 3-cycle is A_n itself.

(2) Any nontrivial normal subgroup of $A_n (n \geq 5)$ contains a 3-cycle.

Logically, (1) and (2) imply that the only nontrivial normal subgroup of $A_n (n \geq 5)$ is A_n itself.

Before we can prove facts (1) and (2), we need a preliminarly result:

Proposition 65. The alternating group A_n is generated by 3-cycles for $n \geq 3$.

PROOF. To show that the 3-cycles generate A_n, we need only show that any pair of transpositions can be written as the product of 3-cycles. Since $(ab) = (ba)$, every pair of transpositions must be one of the following:

$$\begin{aligned}(ab)(ab) &= id \\ (ab)(cd) &= (acb)(acd) \\ (ab)(ac) &= (acb).\end{aligned}$$

□

Now we're able to prove fact (1).

Proposition 66. Let N be a normal subgroup of A_n, where $n \geq 3$. If N contains a 3-cycle, then $N = A_n$.

PROOF. We will first show that A_n is generated by 3-cycles of the specific form (ijk), where i and j are fixed in $\{1, 2, \ldots, n\}$ and we let k vary. Every 3-cycle is the product of 3-cycles of this form, since

$$\begin{aligned}(iaj) &= (ija)^2 \\ (iab) &= (ijb)(ija)^2 \\ (jab) &= (ijb)^2(ija) \\ (abc) &= (ija)^2(ijc)(ijb)^2(ija).\end{aligned}$$

Now suppose that N is a nontrivial normal subgroup of A_n for $n \geq 3$ such that N contains a 3-cycle of the form (ija). Using the normality of N, we see that

$$[(ij)(ak)](ija)^2[(ij)(ak)]^{-1} = (ijk)$$

is in N. Hence, N must contain all of the 3-cycles (ijk) for $1 \leq k \leq n$. By Proposition 65, these 3-cycles generate A_n; hence, $N = A_n$. □

Let's move on to fact (2):

Proposition 67. For $n \geq 5$, every nontrivial normal subgroup N of A_n contains a 3-cycle.

PROOF. Let σ be an arbitrary element in a normal subgroup N. There are several possible cycle structures for σ.

- σ is a 3-cycle.
- σ is the product of disjoint cycles, $\sigma = \tau(a_1 a_2 \cdots a_r) \in N$, where $r > 3$.
- σ is the product of disjoint cycles, $\sigma = \tau(a_1 a_2 a_3)(a_4 a_5 a_6)$.
- $\sigma = \tau(a_1 a_2 a_3)$, where τ is the product of disjoint 2-cycles.
- $\sigma = \tau(a_1 a_2)(a_3 a_4)$, where τ is the product of an even number of disjoint 2-cycles.

If σ is a 3-cycle, then we are done. If N contains a product of disjoint cycles, σ, and at least one of these cycles has length greater than 3, say $\sigma = \tau(a_1 a_2 \cdots a_r)$, then

$$(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}$$

is in N since N is normal; hence,

$$\sigma^{-1}(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}$$

is also in N. Since

$$\begin{aligned}
&\sigma^{-1}(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1} \\
&= \sigma^{-1}(a_1 a_2 a_3)\sigma(a_1 a_3 a_2) \\
&= (a_1 a_2 \cdots a_r)^{-1}\tau^{-1}(a_1 a_2 a_3)\tau(a_1 a_2 \cdots a_r)(a_1 a_3 a_2) \\
&= (a_1 a_r a_{r-1} \cdots a_2)(a_1 a_2 a_3)(a_1 a_2 \cdots a_r)(a_1 a_3 a_2) \\
&= (a_1 a_3 a_r),
\end{aligned}$$

N must contain a 3-cycle; hence, $N = A_n$.

Now suppose that N contains a disjoint product of the form

$$\sigma = \tau(a_1 a_2 a_3)(a_4 a_5 a_6).$$

Then

$$\sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \in N$$

since

$$(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \in N.$$

So

$$\begin{aligned}
&\sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \\
&= [\tau(a_1a_2a_3)(a_4a_5a_6)]^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_2a_4)^{-1} \\
&= (a_4a_6a_5)(a_1a_3a_2)\tau^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2) \\
&= (a_4a_6a_5)(a_1a_3a_2)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2) \\
&= (a_1a_4a_2a_6a_3).
\end{aligned}$$

So N contains a disjoint cycle of length greater than 3, and we can apply the previous case.

Suppose N contains a disjoint product of the form $\sigma = \tau(a_1a_2a_3)$, where τ is the product of disjoint 2-cycles. Since $\sigma \in N$, $\sigma^2 \in N$, and

$$\begin{aligned}
\sigma^2 &= \tau(a_1a_2a_3)\tau(a_1a_2a_3) \\
&= (a_1a_3a_2).
\end{aligned}$$

So N contains a 3-cycle.

The only remaining possible case is a disjoint product of the form

$$\sigma = \tau(a_1a_2)(a_3a_4),$$

where τ is the product of an even number of disjoint 2-cycles. But

$$\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1}$$

is in N since $(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1}$ is in N; and so

$$\begin{aligned}
&\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \\
&= \tau^{-1}(a_1a_2)(a_3a_4)(a_1a_2a_3)\tau(a_1a_2)(a_3a_4)(a_1a_2a_3)^{-1} \\
&= (a_1a_3)(a_2a_4).
\end{aligned}$$

Since $n \geq 5$, we can find $b \in \{1, 2, \ldots, n\}$ such that $b \neq a_1, a_2, a_3, a_4$. Let $\mu = (a_1a_3b)$. Then

$$\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) \in N$$

and

$$\begin{aligned}
&\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) \\
&= (a_1ba_3)(a_1a_3)(a_2a_4)(a_1a_3b)(a_1a_3)(a_2a_4) \\
&= (a_1a_3b).
\end{aligned}$$

Therefore, N contains a 3-cycle. This completes the proof of the proposition. □

So finally we may summarize the proof that A_n is simple ($n \geq 5$).

Proposition 68. The alternating group, A_n, is simple for $n \geq 5$.

PROOF. Let N be a normal subgroup of A_n. By Proposition 67, N contains a 3-cycle. By Proposition 66, $N = A_n$; therefore, A_n contains no proper nontrivial normal subgroups for $n \geq 5$. □

And there we have it, A_n is a simple group for $n \geq 5$. Simple, right? :)

Historical Note

One of the foremost problems of group theory has been to classify all simple finite groups. This problem is over a century old and has been solved only in the last few years. In a sense, finite simple groups are the building blocks of all finite groups. The first nonabelian simple groups to be discovered were the alternating groups. Galois was the first to prove that A_5 was simple. Later mathematicians, such as C. Jordan and L. E. Dickson, found several infinite families of matrix groups that were simple. Other families of simple groups were discovered in the 1950s. At the turn of the century, William Burnside conjectured that all nonabelian simple groups must have even order. In 1963, W. Feit and J. Thompson proved Burnside's conjecture and published their results in the paper "Solvability of Groups of Odd Order," which appeared in the *Pacific Journal of Mathematics*. Their proof, running over 250 pages, gave impetus to a program in the 1960s and 1970s to classify all finite simple groups. Daniel Gorenstein was the organizer of this remarkable effort. One of the last simple groups was the "Monster," discovered by R. Greiss. The Monster, a 196,833 × 196,833 matrix group, is one of the 26 sporadic, or special, simple groups. These sporadic simple groups are groups that fit into no infinite family of simple groups.

Additional exercises

Note: most of these exercises are taken directly from Tom Judson's book. They tend to be somewhat harder than the in-chapter exercises.

1. Let T be the group of nonsingular upper triangular 2×2 matrices with entries in $\mathbb{R}$; that is, matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

where a, b, $c \in \mathbb{R}$ and $ac \neq 0$. Let U consist of matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

where $x \in \mathbb{R}$.

(a) Show that U is a subgroup of T.

(b) Prove that U is abelian.

(c) Prove that U is normal in T.

(d) Show that T/U is abelian.

(e) Is T normal in $GL_2(\mathbb{R})$?

2. Show that the intersection of two normal subgroups is a normal subgroup.

3. If a group G has exactly one subgroup H of order k, prove that H is normal in G.

4. If G is abelian, prove that G/H must also be abelian.

5. Prove or disprove: If H is a normal subgroup of G such that H and G/H are abelian, then G is abelian.

6. If G is cyclic, prove that G/H must also be cyclic.

7. Prove or disprove: If H and G/H are cyclic, then G is cyclic.

8. Let H be a subgroup of index 2 of a group G. Prove that H must be a normal subgroup of G. Conclude that S_n is not simple for $n \geq 3$.

9. Define the ***centralizer*** of an element g in a group G to be the set

$$C(g) = \{x \in G : xg = gx\}.$$

Show that $C(g)$ is a subgroup of G. If g generates a normal subgroup of G, prove that $C(g)$ is normal in G.

10. Recall that the ***center*** of a group G is the set

$$Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}.$$

(a) Calculate the center of S_3.

(b) Calculate the center of $GL_2(\mathbb{R})$.

(c) Show that the center of any group G is a normal subgroup of G.

(d) If $G/Z(G)$ is cyclic, show that G is abelian.

11. Let G be a group and let $G' = \{aba^{-1}b^{-1}, a, b \in G\}$; that is, G' is the set of all finite products of elements in G of the form $aba^{-1}b^{-1}$.

(a) Show that G' is a subgroup of G. G' is called the ***commutator subgroup*** of G.

(b) Show that G' is a normal subgroup of G.

(c) Let N be a normal subgroup of G. Prove that G/N is abelian if and only if N contains the commutator subgroup of G.

12. Use Fermat's little theorem to show that if $p = 4n + 3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.

13. Show that the integers have infinite index in the additive group of rational numbers.

14. Show that the additive group of real numbers has infinite index in the additive group of the complex numbers.

15. What fails in the proof of Proposition 21 if $\phi : \mathcal{L}_H \to \mathcal{R}_H$ is defined by $\phi(gH) = Hg$?

16. Suppose that $g^n = e$. Show that the order of g divides n.

17. If $|G| = 2n$, prove that the number of elements of order 2 is odd. Use this result to show that G must contain a subgroup of order 2. (*Hint*)

18. Suppose that $[G : H] = 2$. If $a, b \in G \setminus H$, show that $ab \in H$.

19. If $[G : H] = 2$, prove that $gH = Hg$.

20. Let H and K be subgroups of a group G. Prove that $gH \cap gK$ is a coset of $H \cap K$ in G.

21. Let H and K be subgroups of a group G. Define a relation $\sim$ on G by $a \sim b$ if there exists an $h \in H$ and a $k \in K$ such that $hak = b$. Show that this relation is an equivalence relation. The corresponding equivalence classes are called ***double cosets***. In the case where $G = A_4$, compute the double cosets for:

    (a) $H = K = \{(1), (123), (132)\}$.

    (b) $H = \{(1), (123), (132)\}$, $K = \{(1), (124), (142)\}$.

22. If G is a group of order p^n where p is prime, show that G must have a proper subgroup of order p. If $n \geq 3$, is it true that G will have a proper subgroup of order p^2?

23. Let G be a cyclic group of order n. Show that there are exactly $\phi(n)$ generators for G.

24. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the factorization of n into distinct primes. Prove that
$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

25. Show that
$$n = \sum_{d|n} \phi(d)$$
for all positive integers n.

13

Group Actions

We've defined a "group" as as set with an operation defined on it. From this point of view, group elements are "objects" in a set. We have many examples of this: like the integers with addition, the integers mod n, the group of units $U(n)$, groups of matrices, and so on.

Later on we introduced the idea that permutations form a group. Permutations are actually bijections (1-1, onto functions) that map a set of objects to itself. Another way of saying this is that permutations "act on" a set by moving the elements around. Similarly, we saw in Figure 9.5 in Section 9.3 that the symmetries of an equilateral triangle (which are elements of the group S_3) move the vertices of the triangle from one position to another. As a third example, in the group $\mathbb{Q}^*$ of non-zero rational numbers we can think of left multiplying by 2 as "moving" -5 over to -10. Left multiplying again by 2 "moves" -10 to -20: and so on.

The examples in the previous paragraph illustrate a general concept called *group actions*. We will see in this chapter how group actions can give us deeper insight into many of the symmetries that we see in the world around us: for instance, in the geometric solids and in crystals.[1]

13.1 Basic definitions

We'll get to definitions momentarily, but first it's helpful to look at one more example.

Example 1. Consider the 60° counterclockwise rotation of regular hexagon, an element of the group D_6. We've seen this before (see Example 5 in Chapter 9).

[1] This chapter is by Holly Webb (edited by C.T.). Thanks to Tom Judson for material used in this chapter.

Following are the tableau and cycle representations of this rotation.

$$\text{tableau: } r_{60} = \begin{pmatrix} A & B & C & D & E & F \\ B & C & D & E & F & A \end{pmatrix}; \qquad \text{cycle: } r_{60} = (ABCDEF).$$

Both these notations indicate that the rotation acts on the set of vertices (by producing a permutation). In the same way, any symmetry of the hexagon (rotation or reflection) acts on vertices of the hexagon. ♦

Exercise 2. Generalize the previous example to any regular n-gon. Include a tableau in your answer. ◊

Now we're ready to give a general definition of group action.

Definition 3. Let X be a set and G be a group. A ***(left) action*** of G on X is a map $G \times X \to X$ given by $(g, x) \to gx$, where

(1) $ex = x$ for all $x \in X$;

(2) $(g_1 g_2)x = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

The set X on which G acts is called a ***G-set***. △

It is also possible to define right group actions, but in this chapter we'll focus just on left group actions. Following are some more examples of group actions.

Example 4. Let $G = GL_2(\mathbb{R})$ (the group of invertible 2×2 matrices) and $X = \mathbb{R}^2$ Then G acts on X by left multiplication. If $v \in \mathbb{R}^2$ and I is the identity matrix, then $Iv = v$. If A and B are 2×2 invertible matrices, then $(AB)v = A(Bv)$ since matrix multiplication is associative. Therefore, by definition, X is a G-set. ♦

Exercise 5. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}; \quad B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}; \quad v = \begin{bmatrix} x \\ y \end{bmatrix}.$$

Verify the previous example by showing associative property of matrix and vector multiplication. ◊

Exercise 6.

(a) Let $G = 2\mathbb{Z}$ and let $X = \mathbb{Z}$. Show that X is a G-set.

(b) Let $G = \mathbb{Z}$ and let $X = 2\mathbb{Z}$. Is X a G-set? Explain.

(c) Let $G = H_6$ (the complex 6-th roots of unity (see Section 3.4.3 in Chapter 3) and let $X = \mathbb{C}$. Show that X is a G-set.

(d) Let $G = \mathbb{C}$ and let $X = H_8$. Is X a G-set? Explain.

◊

13.2 Group actions on regular polyhedra

We want to apply our new ideas to gain insight about the groups of rotational symmetries of ***regular polyhedra*** In general, a *polyhedron* can be thought of as a collection of faces, edges and vertices: for example, a cube has 6 faces, 12 edges and 8 vertices. A*regular polyhedron* is a polyhedron in which all faces are congruent regular polygons, and the same number of edges meet at every vertex. The group of rotational symmetries of a polyhedron act on the faces, edges and vertices. A rotation will always take faces to faces, edges to edges and vertices to vertices.

In the following discussion we'll be introducing a bunch of new ideas. As usual, we'll illustrate these ideas first on a particular example. So let's begin with the cube, which is perhaps the regular polyhedron which is easiest to understand.

13.2.1 G-equivalence and orbits

Some of the rotational symmetries of the cube are indicated in Figure 13.1. [2] The figure shows three possible rotation axes. We will denote the 90° counterclockwise rotations around the x, y and z axes as r_x, r_y, r_z respectively. We will also denote the faces of the cube as $x_-, x_+, y_-, y_+, z_-, z_+$. For example the rotation $r_x \circ r_x = r_x^2$ will take the bottom face (z_-) to the top face (z_+). *Note*: when we rotate the cube, the axes remain fixed while the cube rotates around them. For example, the z axis is always vertical no matter how the cube is rotated.

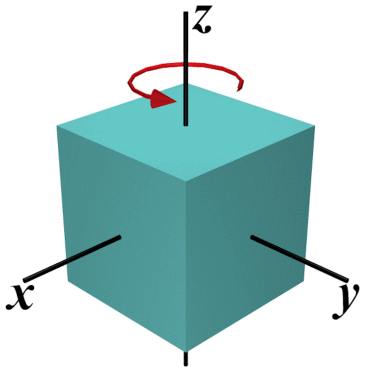


Figure 13.1. Cube with 3 axes of rotation that give symmetries.

Exercise 7.

[2] Note that these are NOT the only rotational symmetries of the cube–we'll discuss the others later (see also the excellent video: www.youtube.com/watch?v=gBg4-lJ19Gg).

(a) Give rotations that take the bottom face (z_-) to each of the faces x_-, x_+, y_-, y_+.

(b) Give rotations that take the face y_- to each of the faces x_-, x_+, y_+, z_-, z_+.

(c) Let's define a notation for the cube's vertices as follows. For example, $+++$ represents the vertex in the first octant ($x > 0, y > 0, z > 0$). The vertex $+--$ will be in the octant where $x > 0, y < 0, z < 0$ (Which is the vertex at lower left in Figure 13.1). Give rotations that take the vertex $+--$ to each of the of the vertices

$$+++,\ -++,\ +-+,\ ++-,\ --+,\ -+-,\ ---.$$

(d) Let's denote the edges of the cube as follows. For example, $\overline{x_+z_-}$ represents the edge where the faces x_+ and z_- meet. The edge $\overline{x_+y_-}$ is where the faces x_+ and y_- meet. (This is the left, front-facing edge of cube in Figure 13.1.)

(i) Using the above notation, list all edges of the cube.

(ii) Give rotations that take the edge $\overline{x_+y_+}$ to each of the other edges.

◊

From the previous exercise it's pretty clear that for any two faces of a cube there is at least one symmetry that takes the first face to the second. In other words, if A and B represent faces then there always exists a symmetry g such that $gA = B$. This example motivates the following definition.

Definition 8. If a group G acts on a set X and $x, y \in X$, then x is said to be ***G-equivalent*** to y if there exists a $g \in G$ such that $gx = y$. We write $x \sim_G y$ or $x \sim y$ if two elements are G-equivalent. △

By this definition we can say that all faces of a cube are G-equivalent to each other under the group of rotational symmetries of a cube. The notation we're using strongly suggests that $\sim_G$ must be an equivalence relation. If fact this is true:

Proposition 9. Let X be a G-set. Then G-equivalence is an equivalence relation on X.

Proof. The relation $\sim$ is reflexive since $ex = x$. Suppose that $x \sim y$ for $x, y \in X$. Then there exists a g such that $gx = y$. In this case $g^{-1}y = x$; hence, $y \sim x$. To show that the relation is transitive, suppose that $x \sim y$ and $y \sim z$. Then, there must exist group elements g and h such that $gx = y$ and $hy = z$. So $z = hy = (hg)x$, and x is equivalent to z. □

Recall from Chapter 8 that every equivalence relation on a set X is associated with a partition of X, where a partition is a collection of disjoint subsets whose union is X. Each set in this partition is called an ***equivalence class***.

Exercise 10. Consider the edge $\overline{y_+z_+}$ of a cube. What is the equivalence class of this edge under G-equivalence, where G is the groups of rotational symmetries of a cube? ◊

In the case of a cube where $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$ The three sets $\{\text{faces}\}, \{\text{edges}\}, \{\text{vertices}\}$ are disjoint equivalence classes whose union is X. We call each of these sets an *orbit* of X under G. In general, we have the following definition.

Definition 11. If X is a G-set, then each set in the partition of X associated with G-equivalence is called an ***orbit*** of X under G. We will denote the orbit that contains an element x of X by $\mathcal{O}_x$. △

The next example shows how these concepts apply to permutation groups as well.

Example 12. Let G be the permutation group defined by

$$G = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$$

and $X = \{1, 2, 3, 4, 5\}$. Then X is a G-set. There are permutations in G that take $1 \to 2$, $1 \to 3$, $2 \to 3$, and vice versa. There are also permutations that take $4 \to 5$ and vice versa. So the orbits are $\{1, 2, 3\}$ and $\{4, 5\}$. ⧫

Exercise 13.

(a) Let $G = \{\mathsf{id}, \mu_1\}$ which is a subgroup of S_3 (the symmetry group of an equilateral triangle) (See Figure 9.5 in Section 9.3.) Let $X = \{A, B, C\}$ be the set of vertices of an equilateral triangle. List the orbits of X under G

(b) Let G be the permutation group defined by

$$\begin{aligned} G = \{&(1), (1358), (1538), (1853), (247), (274), (1358)(247), (1538)(247), \\ &(1853)(247), (1358)(274), (1538)(274), (1853)(274)\} \end{aligned}$$

and $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Then X is a G-set. List the orbits of X under G.

◊

13.2.2 Stabilizers, stabilizer subgroups, and fixed point sets

Let's return to the cube to illustrate another new concept. Every rotation of a cube has an axis of rotation as well as an angle. For rotations which are symmetries we've considered 3 possible axes, passing through opposite pairs of faces. For every pair of opposite faces, all rotational symmetries whose axis passes through those faces leaves them fixed. Note that these rotations form a subgroup. Similar subgroups are obtained when we take the axes through opposite edges, or opposite vertices. These are all examples of *stabilizer subgroups*. The general definition is as follows.

Definition 14. Given that X is a G-set and $x \in X$, let G_x be the set of group elements g that fix x: in other words, $gx = x$. Then G_x is called the ***stabilizer subgroup*** or ***isotropy subgroup*** of x. △

Exercise 15. Given any x in X, prove that the stabilizer subgroup G_x is a subgroup of G. (Recall this involves proving closure under composition and inverse.) ◊

On the other hand, each element of G has an associated subset of X that it leaves unchanged. Recall that the group of rotations of a cube act on the set: $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. Any rotation about the x axis (r_x^n) leaves the faces x_+ and x_- fixed. $\{x_+, x_-\}$is a subset of X. Similarly, $\{y_+ , y_-\}$ and $\{z_+, z_-\}$ are fixed by rotations about the y axis and z axis, respectively. Thus, $\{x_+, x_-\}, \{y_+, y_-\}, \{z_+, z_-\}$, are all examples of *fixed point sets* in X. This leads to another definition:

Definition 16. Let G be a group acting on a set X, and let g be an element of G. The ***fixed point set*** of g in X, denoted by X_g, is the set of all $x \in X$ such that $gx = x$. △

It is important to remember that $X_g \subset X$ and $G_x \subset G$.

Let's use this notation to describe some stabilizer subgroups and fixed point sets for familiar examples of group actions.

Example 17. Let G be the rotational symmetries of a cube and $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$ The fixed point set of id is:

$$X_{\mathsf{id}} = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$$

since the identity rotation leaves the entire cube unchanged. ⧫

Example 18. Let's consider the stabilizer subgroups for the faces of a cube. These contain the elements of the group G of rotations of the cube that leave each face

unchanged. The stabilizer subgroups for the faces are:

$$\begin{aligned} G_{x_+} = G_{x_-} &= \{\mathsf{id}, \mathsf{r_x}, \mathsf{r_x^2}, \mathsf{r_x^3}\} \\ G_{y_+} = G_{y_-} &= \{\mathsf{id}, \mathsf{r_y}, \mathsf{r_y^2}, \mathsf{r_y^3}\} \\ G_{z_+} = G_{z_-} &= \{\mathsf{id}, \mathsf{r_x}, \mathsf{r_x^2}, \mathsf{r_x^3}\} \end{aligned}$$

♦

Example 19. Let $X = \{1, 2, 3, 4, 5, 6\}$ and suppose that G is the permutation group given by the permutations

$$\{(1), (12)(3456), (35)(46), (12)(3654)\}.$$

Then the fixed point sets of X under the action of G for the different group elements are

$$\begin{aligned} X_{(1)} &= X, \\ X_{(35)(46)} &= \{1, 2\}, \\ X_{(12)(3456)} &= X_{(12)(3654)} = \emptyset, \end{aligned}$$

and the stabilizer subgroups for the different elements of X are

$$\begin{aligned} G_1 = G_2 &= \{(1), (35)(46)\}, \\ G_3 = G_4 = G_5 = G_6 &= \{(1)\}. \end{aligned}$$

♦

Exercise 20. Let $G = S_4$ (the permutations of 4 elements), and let $X = \{1, 2, 3, 4\}$. X is a G-set.

(a) Give G_2, G_4, and $G_2 \cap G_4$. Is $G_2 \cap G_4$ a group? *Explain* your answer.

(b) Give $X_{(123)}$, $X_{(234)}$,and $X_{(123)} \cap X_{(234)}$.

(c) Repeat part (a) with $G = A_4$ (the group of even permutations on 4 elements).

(d) Repeat part (b) with $G = A_4$ (the group of even permutations on 4 elements).

◊

As usual, we will denote the number of elements in the fixed point set of an element $g \in G$ by $|X_g|$, the number of elements of the stabilizer subgroup of $x \in X$ as $|G_x|$ and the number of elements in the orbit of $x \in X$ by $|\mathcal{O}_x|$.

Exercise 21. Let $G = S_n$ (the permutations of n elements), and let $X = \{1, 2, \ldots n\}$. X is a G-set.

(a) What is $|G_1|$? What is $|G_2|$? What is $|G_k|$ where $k \in X$? (Recall that $|S_n| = n!$)

(b) If g is a 3-cycle, then what is $|X_g|$? What if g is a 5-cycle? (You may assume that $n \geq 5$).

(c) Give a general formula for X_g, where g is a k-cycle ($2 \leq k \leq n$).

(d) Repeat part (a) with $G = A_n$ (the even permutations of n elements).

(e) Repeat part (b) with $G = A_n$.

(f) Repeat part (c) with $G = A_n$.

◊

13.2.3 Counting formula for the order of polyhedral rotational symmetry groups

It is possible to characterize the size of the rotational symmetry group G for a regular polyhedron in terms of $|\mathcal{O}_x|$and $|G_x|$. We'll show this with an example.

Example 22. Consider our old friend the group of rotational symmetries of a cube acting on $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. We've seen that $G_{x_+} = \{\mathsf{id}, \mathsf{r}_\mathsf{x}, \mathsf{r}_\mathsf{x}^2, \mathsf{r}_\mathsf{x}^3\}$ is the stabilizer subgroup for x_+. Thus there are four rotations that take x_+ to itself. We've also seen that there's at least one rotation that takes x_+ to each of the six faces of the cube: this is the same thing as saying that the orbit of a face is the set of all faces. Each of these rotations can be composed with any of the elements of G_{x_+} for a total of $6 \cdot 4 = 24$ rotational symmetries of a cube. To summarize, we've discovered that

$$|G| = |G_{x_+}| \cdot |\mathcal{O}_{x_+}|.$$

Note that x_+ was an arbitrary choice: we could use this argument with any of the faces and obtain the same result. ♦

In the previous example we used faces to count the rotational symmetries of a cube but we could use edges or vertices as well. In the next exercise we'll consider edges and in the following one we'll consider vertices. A model of a cube might help with these exercises (see Figure 13.2).

Exercise 23.

(a) Find the stabilizer subgroup for the edge $\overline{x_+, z_+}$. (*Hint*)

(b) Find the stabilizer subgroup for the edge $\overline{x_-, y_+}$.

(c) In Example 22 we constructed a formula for $|G|$ in terms of $|G_{x_+}|$ and $|\mathcal{O}_{x_+}|$. Can you do the same thing with $\overline{x_+, z_+}$ using part (a)? Can you do the same thing with $\overline{x_-, y_+}$ using part (b)?

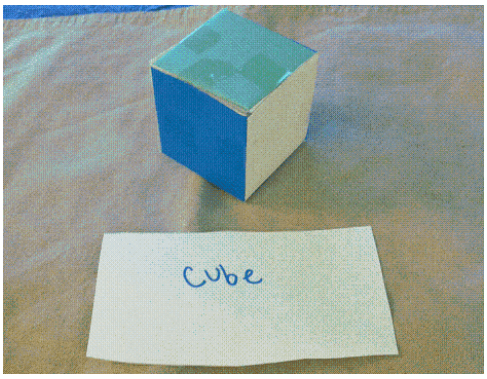


Figure 13.2. A paper cube to print, cut and fold from www.korthalsaltes.com

(d) Find the stabilizer subgroup for the vertex $+,+,+$ (*Hint*)

(e) Find the stabilizer subgroup for the vertex $+,-,+$.

(f) Using parts (d) and (e), construct alternative formulas for $|G|$.

$\Diamond$

From the previous example and exercises, it seems we have a general formula: if G acts on X and $x \in X$, then

$$|G| = |G_x| \cdot |\mathcal{O}_x|.$$

This may remind you of *Lagrange's Theorem*, which we proved in

$$|G| = |H| \cdot [G : H],$$

where H is any subgroup of G. If we replace H with G_x, this becomes

$$|G| = |G_x| \cdot [G : G_x].$$

Comparing with our previous formula, we get

$$|\mathcal{O}_x| = [G : G_x].$$

Let's give a real mathematical proof of this.

Proposition 24.(*Counting formula*): Let G be a group and X a G-set. If $x \in X$, then $|\mathcal{O}_x| = [G : G_x]$.

PROOF. In general, a good way to show that two sets are the same size is to show that there is a *bijection*. (1-1 and onto map) between the two sets. We will define a map ϕ between the orbit $\mathcal{O}_x$ and the set of left cosets of G_x in G as follows. Let $y \in \mathcal{O}_x$. Then there exists a g in G such that $gx = y$. Define ϕ by $\phi(y) = gG_x$. Note that this coset contain an element $ge = g$: so it contains an element that takes $x \to y$.

Before we can show that ϕ is a bijection, we must first show that $\phi(y)$ is well-defined for any y, and does not depend on our selection of g. Suppose that g' is another element in G such that $g'x = y$. Then $gx = g'x$ or $x = g^{-1}g'x$. By the definition of the stabilizer subgroup G_x, $g^{-1}g' \in G_x$. By Proposition 10 in Section 12.2, it follows that $gG_x = g'G_x$. Thus, y gets mapped to the same coset regardless of the choice of group element.

To show that ϕ is one-to-one, we'll assume that $\phi(x_1) = \phi(x_2)$, and show that this means that $x_1 = x_2$. Here we go:

Recall that $\phi(x_1)$ is defined as a coset of G_x that contains an element g_1 that satisfies $g_1x = x_1$. Similarly, $\phi(x_2)$, contains an element g_2 that satisfies $g_2x = x_2$. But we're assuming that $\phi(x_1) = \phi(x_2)$. This means that g_1 and g_2 are in the same coset of G_x.

Now consider the expression $g_1(g_1^{-1}g_2)x$. On the one hand, by the associative law we get:

$$(g_1g_1^{-1})g_2x = g_2x = x_2.$$

On the other hand, by Proposition 10 in the Cosets chapter, it follows that $g_1^{-1}g_2$ is in G_x, so that $g_1^{-1}g_2x = x$. This means that we also have:

$$g_1(g_1^{-1}g_2)x = g_1x = x_1.$$

Therefore $x_1 = x_2$. This completes the proof that ϕ is 1-1.

Finally, we must show that the map ϕ is onto: that is, every coset of G_x is in the range of ϕ. This is much quicker than the proof of 1-1. Let gG_x be any left coset. If $gx = y$, then $\phi(y) = gG_x$. Thus gG_x is in the range of ϕ, and the proof is finished. □

13.2.4 Representing G in terms of stabilizer subgroups

We can approach the structure of the group of rotational symmetries of a cube from another direction. We've talked about stabilizer subgroups, and we can see how these subgroups "fit together" within G. For example, we've seen that for every face there are three rotations (besides the identity) that leaves that face fixed. These rotations correspond to 90, 180, and 270 degree rotations of a square: so they have order 4,2, and 4 respectively.[3] So for each face, there are two rotations

[3]Recall that the "order" of a group element g is the smallest positive integer n such that $g^n = \mathsf{id}$.

of order 4 and one rotation of order 2 in the stabilizer of that face. Since there are 6 faces of a cube, this seems to imply that there must be twelve rotations of order 4 and six rotations of order 2 associated with the stabilizers of the different faces. Unfortunately, this is not quite true. The reason is that any rotation that leaves the front face fixed also leaves the back face fixed. So the stabilizer of the front face is the same as the stabilizer of the back face. In fact, the faces of the cube are stabilized in pairs: front-back, left-right, and top-bottom. Since there are 3 pairs, this means that we only have 6 rotations of order 4 and 3 rotations of order 2. If we add in the identity, this gives a total of 10 rotations. But we've already shown that the group of rotational symmetries of a cube has 24 elements. Where are the other 14? Well, we haven't exhausted the possible stabilizers. Consider for instance the stabilizer of a vertex. We know that 3 faces meet at each vertex. So if I twirl the cube around the vertex, the three faces can rotate into each other. So besides the identity, there are two rotations of order 3. As with the faces, each vertex has a corresponding opposite vertex–so the vertices are stabilized in pairs. Since there are 8 vertices, this means there are 4 pairs, which means there are 8 rotations of order 3. This brings us up to a total of 18 rotations. Where are the other six?

Exercise 25. Consider the edges of a cube.

(a) For each edge, how many rotations (besides the identity) leave that edge fixed?

(b) What are the orders of the rotations that leave an edge fixed?

(c) Do edges come in pairs or not? If so give the pairs, if not, explain why not.

(d) How many additional group elements do we obtain from the stabilizers of the different edges, and what are their orders?

◊

Exercise 26. Complete the following table to characterize the group elements of the rotational symmetries of a cube. [4]

Number of elements	order of the element	Type of set that it stabilizes
1	1	entire cube (identity)
2	4	face
–	–	–
–	–	–
–	–	–

◊

[4] We refer the reader once more to the video: www.youtube.com/watch?v=gBg4-lJ19Gg).

13.3 Examples of other regular polyhedral rotation groups

Let's get to know some other regular polyhedra using orbits and stabilizer subgroups to describe their rotational symmetry groups.

13.3.1 The tetrahedron

Consider a regular tetrahedron, as shown in Figure 13.3 This polyhedron has 4 faces, 6 edges and 4 vertices. Each face is a triangle and each face is opposite a vertex. We will consider the rotations of a tetrahedron around 4 axes. Each axis passes through a vertex and the face opposite that vertex. See Figure 13.3. For example, a rotation of the axis through vertex A will also stabilize face a. We can call this axis $\overleftrightarrow{Aa}$. Similarly, we will call the other axes $\overleftrightarrow{Bb}$, $\overleftrightarrow{Cc}$ and $\overleftrightarrow{Dd}$.

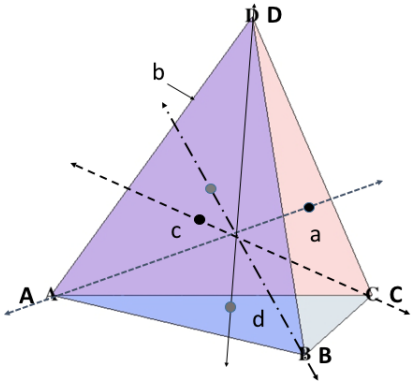


Figure 13.3. Tetrahedron with 4 axes of rotation that give symmetries. Figure modified from - https://inspirehep.net

Note that each of these axes rotates a triangular face. We'll write one counter-clockwise rotation of face a around $\overleftrightarrow{Aa}$ as r_{Aa} (and similarly for the other axes). An animation of the rotations of a tetrahedron is available at:

https://www.youtube.com/watch?v=qAR8BFMS3Bc

You can also make your own tetrahedron like the one in Figure 13.4.

Exercise 27.

(a) How many degrees does r_{Aa} rotate face a?

(b) What is the order of r_{Aa}?

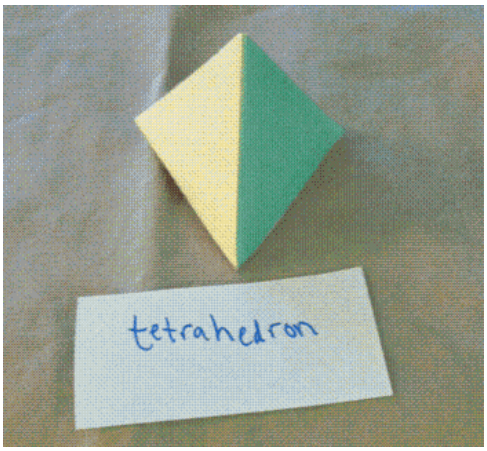


Figure 13.4. Tetrahedron to print, cut and fold from www.korthalsaltes.com

◊

Consider the tetrahedron in Figure 13.3. The rotation r_{Cc} takes vertex D to vertex A and face d to face a.

Exercise 28. We'll find it useful later to represent these rotations as permutations.

(a) Represent each of the rotations r_{Aa}, r_{Bb}, r_{Cc}, r_{Dd} as permutations on the set of vertices.

(b) Represent each of the rotations $r_{Aa}r_{Bb}r_{Cc}r_{Dd}$ as permutations on the set of faces.

◊

Exercise 29.

(a) Give rotations that takes face c to each to each of the other faces a, b, d.

(b) Give rotations that takes vertex D to each of the other vertices.

(c) Consider the edges of the tetrahedron. Denote the edge between the vertices C and D as $\overline{CD}$: and other edges similarly. Use this notation to name each of the edges of the tetrahedron.

(d) Give a rotation that takes edge $\overline{CD}$ to each of the other edges.

◊

Exercise 30. Consider the vertex A of a tetrahedron. What is the equivalence class of this vertex under G-equivalence, where G is the groups of rotational symmetries of a tetrahedron? (Note: This G-equivalence class is the same as orbit of A. which we denote as $\mathcal{O}_A$.) ◊

Just as with the cube, the rotation group G of any polyhedron acts on the set $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. Recall that each group element $g \in G$ has a *fixed point set* $X_g \in X$ that it leaves unchanged: that is, $gx = x$ for any $x \in X_g$. Let's find some fixed point sets for rotations of the tetrahedron.

Exercise 31.

(a) Let G be the rotational symmetries of a tetrahedron what is the fixed point set of r_{Bb}

(b) What is the fixed point set of $r_{Bb} \circ r_{Dd}$? (*Hint*)

(c) What is the fixed point set of $r_{Bb}^{-1} \circ r_{Dd}$?

(d) Give all rotations that fix the set $\{D, d\}$.

◊

Let's consider the stabilizer subgroups for the faces and vertices of a tetrahedron. *hint* R_{Bb}^2 is the 240 degree rotation around the axis $\overleftrightarrow{Bb}$, it will stabilize face b.

Exercise 32. Find the stabilizer subgroups for each of the following: G_A, G_B, G_C, G_D, G_a, G_b, G_c, G_d. Which subgroups are equal? ◊

Let's use the stabilizer subgroups above to determine the total number of rotational symmetries of a tetrahedron.

Exercise 33. Let G be the rotational symmetries of a tetrahedron. As in Example 22 construct a formula for $|G|$ in terms of $|G_A|$ and $|\mathcal{O}_A|$. ◊

So far we've found 4 rotational axes and two rotations around each axis (besides the identity). This gives nine rotations. As we can see there must be more rotational symmetries of a tetrahedron than we've discovered so far. Let's try to find them.

Exercise 34.

(a) Find the stabilizer subgroup for the edge $\overline{CD}$.

(b) Find the stabilizer subgroup for the edge $\overline{AB}$.

(c) How many different group elements (besides the identity) stabilize at least one edge?

(d) Are there any group elements that are not stabilizers of either an edge or a face? Explain your answer.

◊

Exercise 35. In Exercise 33 we constructed a formula for $|G|$ in terms of$|G_A|$ and $|\mathcal{O}_A|$. Can you do the same thing using $|G_{\overline{AB}}|$ and $|\mathcal{O}_{\overline{AB}}|$? ◊

Exercise 36. Complete the following table to characterize the group elements of the rotational symmetries of a tetrahedron. We show two rows, how many more to complete the table?

Number of elements	order of the element	Type of set that it stabilizes
–	–	entire tetrahedron (identity)
–	–	face and vertex

◊

13.3.2 The octahedron

Another regular polyhedron is the octahedron. We will see that in some ways an octahedron is like a cube. When viewed on a vertical z axis the octahedron has no vertical or horizontal faces. See Figure 13.5. We can call a 90 degree counterclockwise rotation around the vertical axis r_z (and similarly for rotations around the x, and y axes). Since each vertex of the octahedron lies on an axis, we can use the x, y, and z axis to label the vertices. For example y_+ is the vertex on the positive y axis. We can also name the edges using this notation for their endpoints. Let's use the axes to label the faces of the octahedron too. Consider Figure 13.5, we'll refer to the the face in the first octant as $\triangle_{+++}$ (the other faces will be labeled similarly).

Exercise 37.

(a) List all the faces of the octahedron using the notation above.

(b) Based on Figure 13.5 how many faces does an octahedron have? How many vertices? How many edges?

◊

A model of an octahedron might help with the following exercises. You can make one like the one in Figure 13.6.

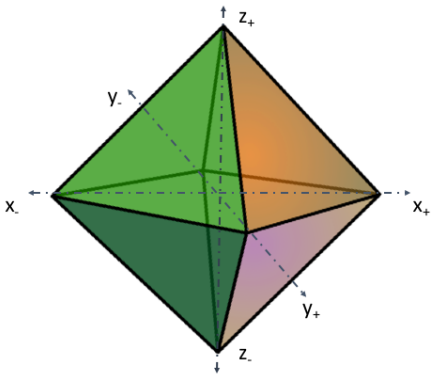


Figure 13.5. Octahedron with 3 axes of rotation that give symmetries. Figure modified from https://en.wikipedia.org/wiki/File:Octahedron.svg

Figure 13.6. A paper octahedron to print, cut and fold (from www.korthalsaltes.com).

Exercise 38. What is the order of r_z? ◊

Exercise 39.

(a) Give rotations that take $\triangle_{+++}$ to each to each of the other faces.

(b) Give rotations that take x_- to each of the other vertices.

(c) Give a rotation that takes edge $\overline{z_+ y_+}$ to each of the other edges.

$\Diamond$

Exercise 40. Consider the edge $\overline{x_- y_+}$ of a octahedron. What is $\mathcal{O}_{\overline{x_- y_+}}$? $\Diamond$

Exercise 41.

(a) Let G be the rotational symmetries of an octahedron what is the fixed point set of $r_y \circ r_z$?

(b) What is the fixed point set of $r_y^2 \circ r_x$?

(c) What is the fixed point set of $r_x^2 \circ r_y$?

$\Diamond$

Let's consider the stabilizer subgroups for the faces and vertices of an octahedron.

Exercise 42. Find the stabilizer subgroups for each of the vertices of the octahedron. (*Hint*) $\Diamond$

Let's find the total number of rotational symmetries for the octahedron.

Exercise 43. Let G be the rotational symmetries of an octahedron. Construct a formula for $|G|$ in terms of $|G_{y_+}|$ and $|\mathcal{O}_{y_+}|$ (see Example 22). $\Diamond$

So far we have discovered 10 rotational symmetries of an octahedron. Three axis of 3 rotations each plus the identity. By the previous exercise, there are still more to discover. Here we go!

Exercise 44.

(a) Find the stabilizer subgroup for the edge $\overline{y_+ \ z_+}$.

(b) Find the stabilizer subgroup for the edge $\overline{y_- \ z_-}$.

(c) How many different group elements (besides the identity) stabilize at least one edge?

$\Diamond$

Exercise 45.

(a) Find the stabilizer subgroup for the face $\triangle_{+++}$.

(b) Find the stabilizer subgroup for the face $\triangle_{-\ -\ -}$.

(c) How many different group elements stabilize at least one face?

◊

Exercise 46. In Exercise 43 we constructed a formula for $|G|$ in terms of $|G_{y_+}|$ and $|\mathcal{O}_{y_+}|$. Can you do the same thing using $|G_{\triangle_{+++}}|$ and $|\mathcal{O}_{\triangle_{+++}}|$? ◊

Exercise 47. Complete the following table to characterize the group elements of the rotational symmetries of an octahedron. We show two rows, how many more to complete the table?

Number of elements	order of the element	Type of set that it stabilizes
—	—	entire octahedron (identity)
—	—	vertices

◊

13.3.3 The dodecahedron

Let's practice finding the elements of the rotation group of another regular polyhedron. Consider the regular dodecahedron in Figure 13.7. A dodecahedron has 12 faces and each face is a regular pentagon. How many edges does this polyhedron have and how many vertices? Well, since each of the twelve faces is a pentagon that seems to give $12 \cdot 5 = 60$ edges. But two faces meet at each edge, so we actually have $(12 \cdot 5)/2 = 30$ edges.

You can also make your own dodecahedron to help you explore its rotational symmetries. See Figure 13.8.

Exercise 48. Determine the number of vertices of a regular dodecahedron. ◊

Let f_1 be one face of the dodecahedron. An axis through the center of f_1 also passes the opposite face which is parallel to f_1. We'll call this opposite face f_1^* and denote a counterclockwise rotation of f_1 about this axis as r_{f_1}.

Exercise 49.

(a) What is the order of r_{f_1}?

(b) Let G be the rotational symmetry group of a dodecahedron. List all rotations in the stabilizer subgroup G_{f_1}. What else do they stabilize?

(c) What is $|G_{f_1}|$?

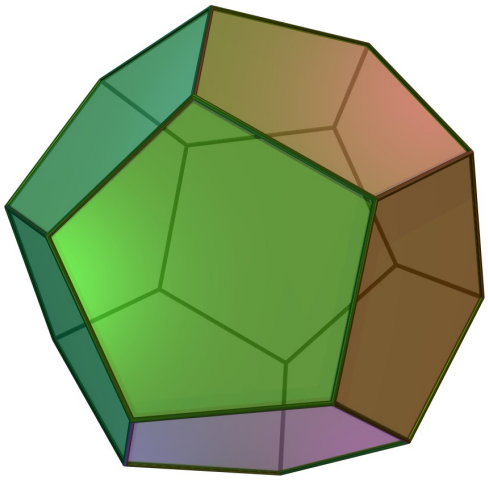


Figure 13.7. Dodecahedron. Source:https://en.wikipedia.org.

(d) How many group elements in G stabilize at least 1 face?

(e) What is $|\mathcal{O}_{f_1}|$?

$\Diamond$

Now we can find the total number of rotational symmetries in G.

Exercise 50. Find $|G|$ in terms of $|G_{f_1}|$ and $|\mathcal{O}_{f_1}|$. $\Diamond$

So far we've found the number of the stabilizers of faces of the dodecahedron. But, as with the cube and tetrahedron, we need axes of symmetry through edges and vertices as well. Let v_1 be one vertex of the dodecahedron. An axis of symmetry through v_1 will also pass through the opposite vertex, which we will call v_1^*. A counterclockwise rotation about this axis is called r_{v_1}.

Exercise 51.

1. Find the order of r_{v_1}.
2. List all rotations in the stabilizer subgroup G_{v_1}. What else do they stabilize?
3. How many group elements in G (besides the identity) stabilize at least 1 vertex?
4. What is $|\mathcal{O}_{v_1}|$?
5. Find $|G|$ in terms of $|G_{v_1}|$ and $|\mathcal{O}_{v_1}|$.

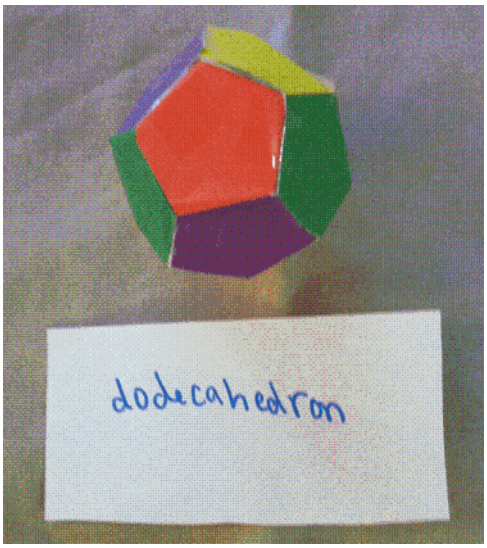


Figure 13.8. A dodecahedron to print, cut and fold (from www.korthalsaltes.com).

◊

Let's consider the edges of the dodecahedron. We've seen already that there are 30 edges. Based on this information and previous exercises, complete the following.

Exercise 52.

(a) Let e_1 be one edge of the dodecahedron. What is $|G_{e_1}|$?

(b) Are the edges of a dodecahedron stabilized in pairs? Explain your answer. (*Hint*)

◊

Exercise 53.

(a) How many group elements of G besides the identity stabilize at least 1 edge?

(b) Complete the following table to characterize the group elements of the rotational symmetries of a dodecahedron. We show two rows, how many more to complete the table?

Number of elements	order of the element	Type of set that it stabilizes
–	–	entire dodecahedron (identity)
–	–	vertices

◊

13.3.4 Soccer ball

All the polyhedra we've studied so far have congruent regular faces. These are also known as ***Platonic solids***. Let's explore the rotation group of a polyhedron whose faces are not all congruent. A familiar example is the football ("soccer ball' in the U.S.), as shown in Figure 13.9. The soccer ball has 32 faces, 12 regular pentagons and 20 hexagons.

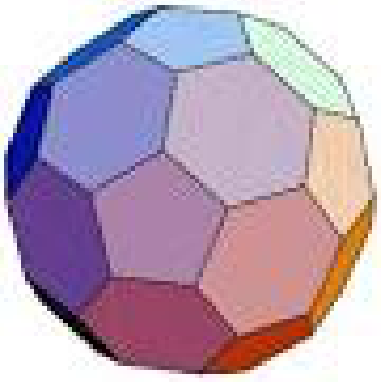


Figure 13.9. A faces of a soccer ball are 12 pentagons and 20 hexagons. Source: http://mathworld.wolfram.com/TruncatedIcosahedron.html.

Exercise 54. With the help of Figure 13.9 determine the number of edges and vertices of the soccer ball. ◊

Let's try to count the rotations of a soccer ball that preserve symmetry. Axes can be placed through the center of pentagonal faces, which are stabilized in pairs. Axes can also be placed through the center of hexagonal faces. However, not all rotations about an axis through a hexagonal face will result in symmetry.

Exercise 55. Let G be the rotation group of a soccer ball.

(a) How many rotations (besides the identity) stabilize at least one pentagonal face?

(b) How many rotations (besides the identity) stabilize at least one hexagonal face?

◊

Axes of rotation also pass through edges that join two hexagonal faces.

Exercise 56. **How many rotations in G (besides the identity) stabilize at least one edge? ◊

Exercise 57.

(a) Find $|G|$ using the counting formula applied to the pentagonal faces.

(b) Find $|G|$ using the counting formula applied to the hexagonal faces.

(c) Find $|G|$ using the counting formula applied to the edges.

◊

13.4 Euler's formula for regular polyhedra

In this section we'll play with counting the order of the rotation group G of a regular polyhedron in different ways. It turns out that this will lead us to an interesting and useful formula relating the number of edges, vertices, and faces in a polyhedron. Let's start by reviewing our previous examples and noticing a pattern.

Exercise 58.

(a) Complete the table and compare $|G|$ to the number of edges of each polyhedron. The number of edges is equal to the order of the orbit of any edge e, denoted as $|\mathcal{O}_e|$.

polyhedron	number of edges ($\lvert\mathcal{O}_e\rvert$)	order of group ($\lvert G\rvert$)
cube	12	24
octahedron	–	–
dodecahedron	–	–

(b) Write an equation for $|G|$ in terms of $\mathcal{O}_e$.

◊

Now in Exercise 26 we showed another way of counting the elements of G. Essentially, we showed that we could express $|G|$ as:

$$|G| = 1 + |\text{stabilizers of faces}| + |\text{stabilizers of vertices}| + |\text{stabilizers of edges}|,$$

where the '1' comes because we need to count the identity. We'll call this the ***stabilizer counting formula***.

Let's apply this formula to a polyhedron with $|\mathcal{O}_f|$ faces, $|\mathcal{O}_v|$ vertices and $|\mathcal{O}_e|$ edges. We'll start with the faces. For any face f we already have a formula for $|G_f|$ using the counting formula in Proposition 24. Dividing this formula by $|\mathcal{O}_f|$ gives: $|G_f| = |G|/|\mathcal{O}_f|$. By substitution we see that $|G_f| = (2 \cdot |\mathcal{O}_e|)/|\mathcal{O}_f|$. But we know that one of the elements of $|G_f|$ is the identity, which has already been counted. Since there are $|\mathcal{O}_f|$ different faces, this *seems to* imply that there are $|\mathcal{O}_f| \cdot (2|\mathcal{O}_e|/|\mathcal{O}_f| - 1) = 2|\mathcal{O}_e| - |\mathcal{O}_f|$ different stabilizers of faces (besides the identity).

By the same method, we can count the number of stabilizers of vertices and edges. This gives us $2|\mathcal{O}_e| - |\mathcal{O}_v|$ and $2|\mathcal{O}_e| - |\mathcal{O}_e|$ stabilizers of vertices and edges, respectively. Putting these numbers into our stabilizer counting formula we *apparently* get

$$\begin{aligned} \text{“}|G| &= 1 + 2|\mathcal{O}_e| - |\mathcal{O}_f| + 2|\mathcal{O}_e| - |\mathcal{O}_v| + |\mathcal{O}_e| \\ &= 1 + 5|\mathcal{O}_e| - |\mathcal{O}_f| - |\mathcal{O}_v|\text{''}. \end{aligned}$$

We've put this equation in quotes for a reason. Let's see if it actually works.

Exercise 59. Let G be the rotational symmetries of a cube. Then $|G| = 24$. Verify whether the above formula accurately calculates $|G|$. ♢

Something is wrong! How come we have too many elements? For all previous examples of polyhedra every element in a rotation group G stabilizes at least two elements of the set $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. For example, In the rotational symmetry group of a cube faces are stabilized in pairs. This means that we've counted every stabilizer twice. So we need to divide by two in our formula:

$$|G| = 1 + 5|\mathcal{O}_e|/2 - |\mathcal{O}_f|/2 - |\mathcal{O}_v|/2.$$

Let's see if the stabilizer counting formula works now.

Exercise 60.

(a) Verify the above equation work for the cube.

(b) Verify it works for the tetrahedron.

(c) Verify that it works for a soccer ball

♢

Let's put this equation together with our expression $|G| = 2 \cdot |\mathcal{O}_e|$ to discover a relationship between the number of faces, vertices, and edges of any regular

polyhedron:

$$2|\mathcal{O}_e| = 1 + 5|\mathcal{O}_e|/2 - |\mathcal{O}_f|/2 - |\mathcal{O}_v|/2 \qquad \text{(by substitution)}$$
$$|\mathcal{O}_f| + |\mathcal{O}_v| - |\mathcal{O}_e| = 2 \qquad \text{(by basic algebra)}$$

This powerful tool is known as ***Euler's formula***. Let's see how it can be used.

Exercise 61. A regular icosahedron has 12 triangular faces and 30 edges. By Euler's formula, how many vertices does an icosahedron have? ◊

We should clarify that what we've shown is only a very special case of Euler's formula which is much more general and has lots of applications in graph theory and topology.

13.5 Closing comments on polyhedral symmetry groups

Finally we mention that the rotational symmetries of the regular solids are not the only possible symmetries. Recall that in the dihedral group, besides rotations there were reflections. Consider for example the hexagon: it had 6 rotations (including the identity) and 6 reflections. It's possible to rotate the hexagon and keep the hexagon in the same plane. However, to reflect the hexagon, you have to "flip" it, which requires three dimensions. It turns out that something similar is true for the regular solids. There are also reflection symmetries for the regular solids: in fact, there are as many reflections as rotations, just as in the dihedral group. Also like the dihedral group, to reflect a solid requires one extra dimension. It is rather mind-blowing to think that if we lived in a world with four physical dimensions, it would be possible to turn a cube inside out just by moving it!

13.6 Group actions on subgroups and cosets

Let's explore some other examples of group action with applications that we may find familiar. It turns out that if the set X is also a group, then it's always possible to define a group action of X on itself.

Example 62. Let $X = Z_5$ and $G = Z_5$. Show that in this case, X is a G-set. In order to show that X is a G-set we must show $1x = x$ for all $x \in \mathbb{Z}_5$; this is true by identity property of multiplication $\mathbb{Z}_5$. Then we need to show: $(g_1g_2)x = g_1(g_2x)$ for all $x, g_1, g_2 \in \mathbb{Z}_5$. This is true by the associative property of multiplication $\mathbb{Z}_5$. Therefore, by definition of G-set, $\mathbb{Z}_5$ is a G-set of itself. ⧫

Exercise 63.

(a) Let $X = \mathbb{Q}^*$ (the nonzero rational numbers) and $G = \mathbb{Q}^*$. Show that in this case, X is a G-set.

(b) Let $X = H_5$ and $G = H_5$ (The complex 5th roots of unity: see Section 3.4.3). Show that in this case, X is a G-set.

(c) Let $X = T$ (the unit circle in the complex numbers: see Figure 3.9 in Section 3.4.3). Find a group G such that X is a G-set, and prove the statement.

$\Diamond$

We can generalize the results of the preceding exercise in the following proposition:

Proposition 64. For any group G, if we let $X = G$ then X is a G-set using the mapping: $(g, x) \to gx$.

Exercise 65.: Prove the above proposition. $\Diamond$

In the previous exercises, we've seen cases where $X = G$ is a group and H is a subgroup of X. In this situation, H will always produce a group action on X.

Exercise 66. Prove the following proposition: If $X = G$ and G is a group, and H is a subgroup of G, then G is a H-set using the mapping: $(h, g) \to hg$. $\Diamond$

Recall our discussion of cosets in Chapter 12 In particular, a left coset consists of a group element g acting on a subgroup H of G. The group element acts on each element of the subgroup to create a coset. In other words, a coset is a subgroup shifted by action of a group element. If G is a group, we can let L be the set of left cosets. We will see in the following examples that we can define a group action on L. That is the set of left cosets, L is a G-set. Let G be the additive group of real numbers. That is, $G = (\mathbb{R}, +)$, and let H be all integer multiples of 2π. That is, $H = \{2k\pi : k \in \mathbb{Z}\}$, or $H = 2\pi\mathbb{Z}$ for short.

Exercise 67. Prove that $2\pi\mathbb{Z}$ is a subgroup of $(\mathbb{R}, +)$. $\Diamond$

Example 68. Let L be the set of left cosets of $2\pi\mathbb{Z}$ in the group $(\mathbb{R}, +)$. Recall from Definition 4 in Chapter 12 that the set of left cosets L is defined as $x+2\pi\mathbb{Z} = \{x+h : h \in 2\pi\mathbb{Z}\}$. For example, the left coset which contains $\pi/3$ is the set $\{\pi/3+2k\pi, k \in \mathbb{Z}\}$, which we could also write as $\{\ldots \pi/3-4\pi, \pi/3-2\pi, \pi/3, \pi/3+2\pi, \pi/3+4\pi, \ldots\}$. It turns out that L is G-set under the action $(g, x + 2\pi\mathbb{Z}) \to g + x + 2\pi\mathbb{Z}$. Let's verify the two axioms (conditions) of a G-set:

(a) For the first axiom note that $e \in G = 0$. Then, $0 + x + 2\pi\mathbb{Z} = x + 2\pi\mathbb{Z}$ for any $x + 2\pi\mathbb{Z} \in L$. So the first axiom is true.

(b) For the second axiom consider two real numbers a, b. Then, by associativity of real number addition, $(a + b) + x + 2\pi\mathbb{Z} = a + (b + x + 2\pi\mathbb{Z})$ for any $x + 2\pi\mathbb{Z}$ in L. So the second axiom is true. L is a G-set of the additive group of real numbers.

This example has a very practical significance. We know that angles on a unit circle are arbitrary up to multiples of 2π. So we can think of each angle as a coset: that is, the angle θ where $0 \leq \theta < 2\pi$ represents the coset $\{\theta + 2k\pi\}$ or $\theta + 2\pi\mathbb{Z}$. Now consider what an arbitrary rotation ϕ does to the angle θ. For instance, consider the case where $\theta = \frac{\pi}{4}$–then $\theta + H = \{\frac{\pi}{4} + 2k\pi\}$. We'll suppose that the rotation angle is $\phi = \frac{15\pi}{2}$. According to the group action, $\phi + \theta + H = \frac{15\pi}{2} + \{\frac{\pi}{4} + 2k\pi\}$ which will result in the new coset $\{\frac{31\pi}{4} + 2k\pi\} = \{\frac{7\pi}{4} + 2k\pi\}$. As we can see, the action of the additive group $(R, +)$ on the cosets $\theta + 2\pi k$ corresponds to rotation by arbitrary angles around the unit circle. If the rotation is more than 2π, the action still works because the cosets take care of any extra factors of 2π. ♦

Let's consider another example of group action on a set of cosets. This example can be thought of as a two-dimensional version of the previous example, and can be envisioned using computer graphics.

Example 69. Let G be the xy plane under addition (that is, $G = (\mathbb{R}^2, +)$). Let $H = \mathbb{Z}\times\mathbb{Z}$, which is a subgroup of G (H is called the ***integer lattice***). A coset of H in G is defined as $x+H = \{(x+m, y+n) : m, n \in \mathbb{Z}\}$ Each coset of the form $x+H$ has a single point inside the unit square. Consider, $g = (0.2, 0), x = (0.9, 0.5)$ and $h = (m, n)$, for $g, x \in G$ and $h \in H$. $g+x+H = (0.2 + .9 + m, 0 + 0.5 + n) : m, n \in Z = (1.1 + m, 0.5 + n) : m, n \in Z$ Using $h = (-1, 0)$ yields $g + x + h = (0.1, 0.5)$, the single point for the coset $g + x + H$ which is inside the unit square. $g + x + H$ is equivalent to the coset $(0.1, 0.5) + H$ Imagine the unit square is your computer screen. The example above can be used to describe the motion of a character on the screen of a wraparound" video game. That is, if he moves off the right edge of the screen, he re-appears on the left edge as shown in Figure 13.10. ♦

Recall that by definition a left coset of the integer lattice $x+H$ means adding the same point $\{x = (a, b)|a, b \in \mathbb{R}\}$ to each point in the integer lattice. a group action simply changes one coset of H in G to a different coset. The three illustrations below show the progression of the group action in the Example 69. You can duplicate this illustration by drawing the coset points on a transparency, placing it over a graph of the integer lattice and moving the transparency 0.2 units to the right.

Exercise 70.

(a) Given $x = (0.8, 0.6)$ and $g = (1.4, 0)$ find a point $h \in \mathbb{Z} \times \mathbb{Z}$ Such that $g + x + h$ is inside the unit square. (In fact, this is the *only* point h for which $g + x + H$ is inside the unit square.)

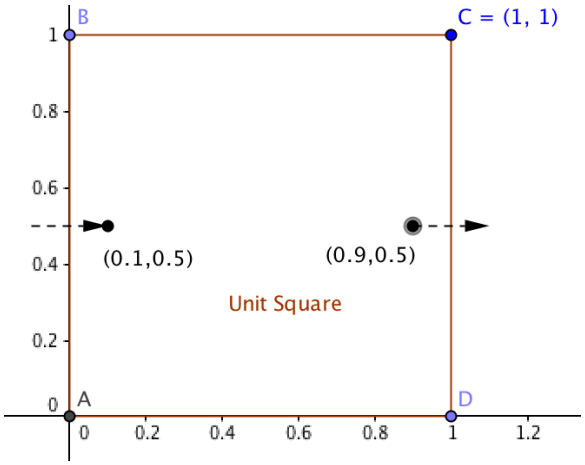


Figure 13.10. Unit square illustrating a left group action of $G = (\mathbb{R}^2, +)$ on the left cosets of $H =$ integer lattice in G

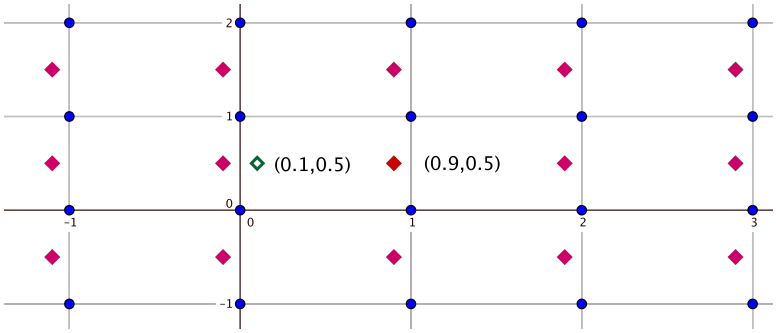


Figure 13.11. Illustrating $x + H$ for $x = (0.9, 0.5)$ Note: this illustration and the two following were created using the software "GeoGebra" (see www.geogebra.org). The rectangles should be thought of as unit squares (the scales on the x and y axes are not equal). These figures illustrate a left group action of $(\mathbb{R}, +)$ on a left coset of integer lattice.

(b) Given $x = (0.8, 0.6)$ and $g = (1.2, 1.3)$ find a point $h \in \mathbb{Z} \times \mathbb{Z}$ Such that $g+x+h$ is inside the unit square.

(c) Given $x = (0.8, 0.6)$ and $g = (0, 3.5)$ find a point $h \in \mathbb{Z} \times \mathbb{Z}$ Such that $g+x+h$ is inside the unit square.

(d) For each g and x above, find g' in the unit square, such that $g' + H = g + x + H$.

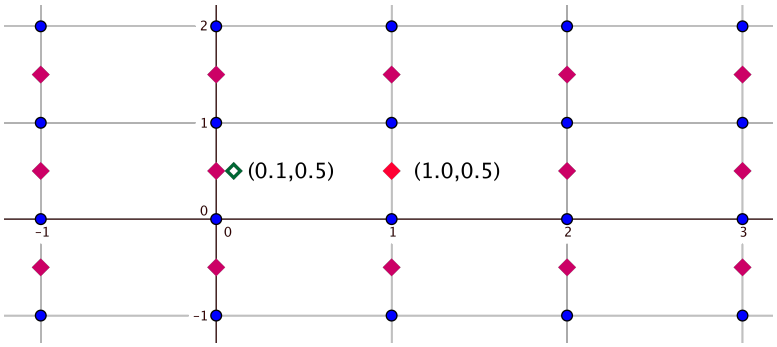


Figure 13.12. Illustrating $g + x + H$ for $g = (0.1, 0)$ and $x = (0.9, 0.5)$

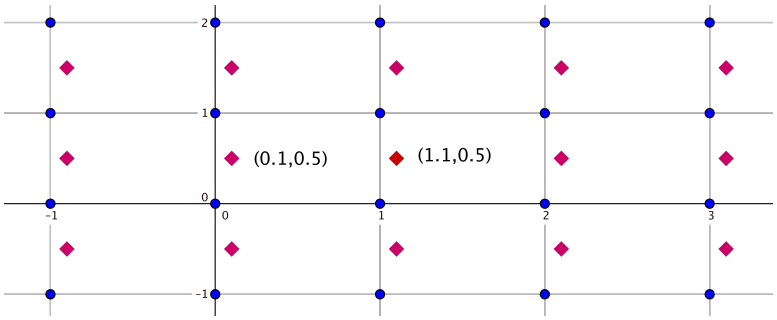


Figure 13.13. Illustrating $g + x + H$ for $g = (0.2, 0)$ and $x = (0.9, 0.5)$

(e) Illustrate part (a) with a graph. Graph the point x. (This is actually the point $x + h'$ for $h' = (0, 0)$). Then graph the point $g + x + h$ using the h you found in part (a). Include ordered pairs to indicate the position of points. Include arrows to indicate "movement" as in the example.

(f) Create a similar graphs illustrating part (b) and (c).

(g) Prove that the above are examples of a group action of G on $x + H$. That is, show that $x + H$ is a G-set.

$\Diamond$

We can think about this example in another way. Suppose we have a *torus*, which is the mathematical word for a donut shape. We could imagine creating a "map" of the surface of the torus by cutting the torus apart as shown in Figure 13.14. If we spread this map out flat, it would look like a square (see Figure 13.15). If we wanted to use the map to chart motion on the surface of the

torus, then any motion that goes off the right edge would reappear at the left edge; and any motion that goes off the top edge would reappear at the bottom. So you see this is exactly what we saw for the previous example. So using cosets of $\mathbb{Z}^2$ in $\mathbb{R}^2$, we've created a mathematical representation for motion on the surface of a torus.

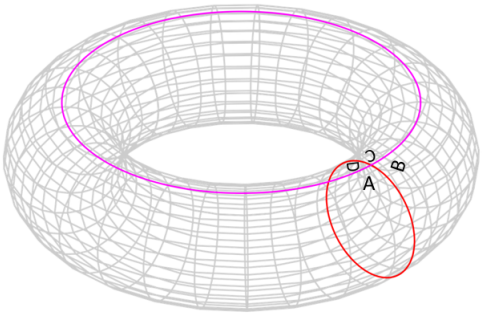


Figure 13.14. Torus, showing two cut lines.

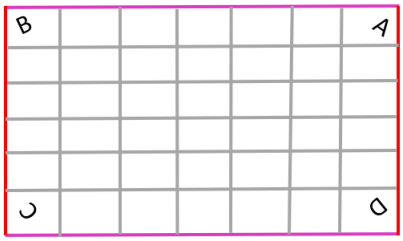


Figure 13.15. The cut torus, flattened out.

We can generalize the two previous examples by considering cosets of a subgroup H in a group G that contains H.

Example 71. Let H be a subgroup of G and L_H the set of left cosets of H. The set L_H is a G-set under the action $(g, xH) \to gxH$. Again, it is easy to see that the first axiom is true. Since $(gg')xH = g(g'xH)$, the second axiom is also true. ♦

So far, we've been looking at group actions on left cosets. What about right cosets? Let's investigate.

Exercise 72. Consider the case where $G = S_3$, $H = \{\mathsf{id}, (12)\}$, and R is the set of right cosets of H. Define a function from $G \times R \to R$ by $(g, R) \to Rg$. Does this function define a group action of G on R? (*Hint*) ◊

The previous exercise shows that we can't always do the same thing with right cosets that we can do with left cosets. Let's look at an alternative:

Exercise 73.

(a) Repeat the previous exercise, but this time use the function $(g, R) \to Rg^{-1}$.

(b) Show that in general the function $(g, R) \to Rg^{-1}$ defines an action of G on the right cosets of H.

◊

13.7 Conjugation

Commutative diagrams and the definition of conjugation

When we talked about permutations, we saw that the objects we were permuting didn't really change the situation. For example, we saw that permuting $\{1, 2, 3, 4\}$ was the "same thing" as permuting $\{A, B, C, D\}$. Now what do we really mean by the "same thing"? Well for example, if we take any permutation of $\{1, 2, 3, 4\}$ and replace 1 with A, 2 with B and so on, then we'll get a permutation of $\{A, B, C, D\}$. To be specific let's take $\sigma = (123)$ and $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ A & B & C & D \end{pmatrix}$. It's possible to represent this situation with diagram in Figure 13.16. This type of diagram is called a ***commutative diagram***.

The commutative diagram illustrates the construction of a conjugation. We can begin in the upper right corner and travel to the upper left, in the opposite direction of the f arrow. That is f^{-1}. Then, from upper left to lower left represents the permutation $\sigma = (123)$. Then, proceed in the direction of the arrow, that is f from lower left to lower right. At the lower right corner, we arrive at the mapping of μ. So the diagram shows $\mu = f\sigma f^{-1}$. (Recall functions are composed from right to left.).

Let's think of this another way. We can follow the path $f\sigma$ or μf. Both take us to the lower right. So we can write $f\sigma = \mu f$. By right multiplying by f^{-1} we discover the algebraic structure of the conjugate of σ, $f\sigma f^{-1} = \mu$. There is a short cut to

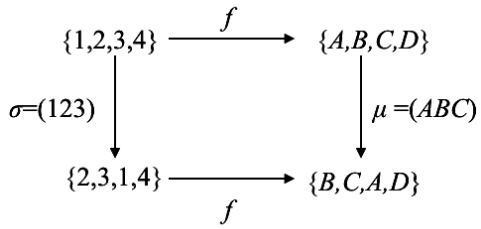


Figure 13.16. Commutative diagram of a conjugate mapping.

arrive at μ. μ is simply σ relabeled according to f. That is, if we take the cycle representation of σ and replace the numbers according to f ($1 \to A, 2 \to B, 3 \to C$), then we end up with μ. We will call this short cut, "the relabeling method".

Exercise 74. For each σ and and f, complete a commutative diagram like the one in Figure 13.16. Find the conjugate mapping in two ways, using conjugation and the relabeling method.

(a) $\sigma = (12)(35)$ and $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ A & B & C & D & E \end{pmatrix}$

(b) $\sigma = (2346)$ and $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ A & B & C & D & E & F \end{pmatrix}$

(c) $\sigma = (147)(2563)$ and $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ A & B & C & D & E & F & G \end{pmatrix}$

$\Diamond$

Now instead of f going between different sets, we can choose f to map $\{1, 2, 3, 4\}$ to itself. In this case, f itself is a permutation. To be more consistent with our earlier notation for permutations, we'll use the symbol τ instead of f in the following discussion. What τ corresponds to is just relabeling the objects that we're permuting. Figure 13.17 shows an example where both τ and σ are permutations on the set $\{1, 2, 3, 4\}$. The diagram shows that if we do a permutation σ on the originally-labeled objects, and compare to the same permutation of the relabeled objects, we find that the relabeled permutation is exactly given by $\tau\sigma\tau^{-1}$. The permutations σ and $\tau\sigma\tau^{-1}$ are called ***conjugate permutations***, and the operation which takes σ to $\tau\sigma\tau^{-1}$ is called ***conjugation***.[5]

[5]Note this is quite different from conjugation of complex numbers. Unfortunately, "conjugation" is a very popular word in mathematics, and is used in many different senses.

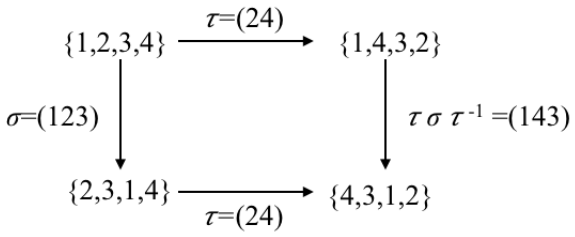


Figure 13.17. Conjugate mapping with τ and σ permuting {1,2,3,4}.

Conjugate permutations and cycle structure

Two permutations that are conjugate are in many ways very similar. We could almost call them the "same" permutation, only they act on a relabeled set of objects. In particular, it's true that two conjugate permutations must have the same cycle structure. For instance, in the example we did earlier in Figure 13.16 we saw that both permutations were three-cycles. This will be true in general because conjugation simply means relabeling the objects that are permuted, without changing anything else.

Example 75. Let $\sigma = (153)(276)$ and $\tau = (427)(165)$. Then

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Relabeling σ according to τ gives the conjugate $(136)(457)$. You can check that computing $\tau\sigma\tau^{-1}$ will give the same result as the relabeling method. ♦

Exercise 76. Given σ and τ use the relabeling method to find the permutation conjugate to σ. Check your work by computing the conjugate with $\tau\sigma\tau^{-1}$

(a) $\sigma = (6247)$ and $\tau = (527)(63)$. σ and τ act on the set $\{1, 2, 3, 4, 5, 6, 7\}$.

(b) $\sigma = (256)(134)$ and $\tau = (21643)$. σ and τ act on the set $\{1, 2, 3, 4, 5, 6\}$.

(c) $\sigma = (14)(27356)$ and $\tau = (463)$. σ and τ act on the set $\{1, 2, 3, 4, 5, 6, 7\}$.

◊

It turns out that it's also true that any two permutations with the same cycle structure are conjugate.

Example 77. Let $\sigma = (12)(3456)(789), \mu = (149)(2658)(37)$. Notice that σ becomes μ if we use the following relabeling:

$$1 \to 3; \quad 2 \to 7; \quad 3 \to 2; \quad 4 \to 6; \quad 5 \to 5; \quad 6 \to 8; \quad 7 \to 1; \quad 8 \to 4; \quad 9 \to 9.$$

We can use this information to write τ in tableau notation:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 2 & 6 & 5 & 8 & 1 & 4 & 9 \end{pmatrix},$$

from which we find, $\tau = (1327)(468)$. Then you may check that σ and μ are conjugate according to: $\mu = \tau\sigma\tau^{-1}$. ♦

Exercise 78. In each of the following find a permutation τ that makes σ and μ conjugate. Check that σ and μ are conjugate according to: $\mu = \tau\sigma\tau^{-1}$.

(a) $\sigma = (135)(792)(468)$, $\mu = (236)(189)(457)$

(b) $\sigma = (2579)(3561)$, $\mu = (2461)(5793)$

(c) $\sigma = (25)(13578)$, $\mu = (36)(28454)$

◊

These examples lead up to the following theorem:

Proposition 79. Given a permutation group G, and two permutations $\sigma, \mu \in G$. Then σ and μ are conjugate if and only if they have exactly the same cycle structure.

Proof. The "only if" part follows from remarks we have made above: the conjugation operation simply re-labels the elements of the permuted set, so two conjugate permutations must have the same cycle structure. For the "only if" part, we may write σ in cycle notation as

$$\sigma = (a_{11}\ a_{12}\ \ldots\ a_{1n_1})(a_{21}\ a_{22}\ \ldots\ a_{2n_2})\ldots(a_{k1}\ a_{k2}\ \ldots\ a_{kn_k}).$$

Suppose that τ has the same cycle structure, which means that τ can be written as

$$\tau = (b_{11}\ b_{12}\ \ldots\ b_{1n_1})(b_{21}\ b_{22}\ \ldots\ b_{2n_2})\ldots(b_{k1}\ b_{k2}\ \ldots\ b_{kn_k}).$$

Then we can define a bijection f by: $f(a_{ij}) = b_{ij}$, for any i and j. Using the above cycle structures, we can show that τ is equal to $f\sigma f^{-1}$. All we have to do is show that this works for any b_{ij}. For example, consider b_{11}: then $f\sigma f^{-1}(b_{11}) = f\sigma(a_{11}) = f(a_{12}) = b_{12}$, which is exactly equal to $\tau(b_{11})$. □

Conjugacy and group action

We will now relate the idea of conjugacy with the notion of group action that was introduced earlier in the chapter.

Example 80. Let G be the dihedral group D_4. Recall that D_4 consists of four rotations and four reflections. In fact we can write $D_4 = \{e, r, r^2, r^3, s, s \circ r, s \circ r^2, s \circ r^3\}$, where r is counterclockwise rotation by 90°, and s is the reflection that leaves vertices labeled 1 and 3 fixed. Let H be the subgroup $\{e, s\}$. We'll define our mapping from $H \times G \to G$ as follows:

$$(h, g) \to hgh^{-1}.$$

For example, consider the case $h = s$ and $g = r$. Then $(s, r) \to s \circ r \circ s^{-1}$. We can simplify this, since s is a reflection, so $s^{-1} = s$. furthermore, by part c of Proposition 42 in Section 9.4, we can show $r \circ s = s \circ r^3$. This gives us

$$s \circ r \circ s^{-1} = s \circ r \circ s = s \circ s \circ r^3 = r^3.$$

♦

Exercise 81. Complete the previous example with $G = D_4$ and $H = \{e, s\}$ by listing all the pairs (h, g) with $h \in H$ and $g \in G$ together with the result of the mapping hgh^{-1}. Simplify your expression for hgh^{-1} as much as possible. ◊

Note something very interesting in the previous exercise. When $h = e$ the all elements of G remain unchanged by the mapping, but when $h = s$ all the rotations map to their inverses. We can generalize Example 80 using the following definition.

Definition 82. Given two group elements g, h in G, then hgh^{-1} is said to a ***conjugate element*** to g. In this case, we would say that h acts on g by conjugation. △

The definition of conjugation gives us a new group action for any subgroup H acting on a group G which contains H:

Proposition 83.. If H is a subgroup of G, then G is an H-set under conjugation. That is, we can define an action $H \times G \to G$, by $(h, g) \to hgh^{-1}$ for $h \in H$ and $g \in G$.

The proof is contained in the following exercise.

Exercise 84. Fill in the blanks to proof the proposition:

First, we have that $\_\_<1>\_\_$ is in H and $(e, g) = \_\_<2>\ g\ <3>\_\_ = g$. So the first axiom for a group action holds.

Also, observing that

$$(h_1h_2, g) = \_\_<4>\ g\ <5>\_\_ = h_1(h_2g\_\_<6>\_\_)\_\_<7>\_\_ = (h_1, (\_\_<8>\_\_, g)),$$

we see that the second condition is also satisfied. ◊

Order of conjugate elements

In order to illustrate some properties of the action of conjugation, we will take a familiar example: the group of rotational symmetries of a cube. What are the conjugate elements? We've seen that the rotations can be classified into:

- Stabilizers of faces;
- Stabilizers of vertices;
- Stabilizers of edges;
- Stabilizers of everything (identity).

Which of these are conjugate?

Consider the conjugates of r_z, which is a 90 degree counterclockwise rotation around the z axis. Supposing that g is an arbitrary rotational symmetry, what does gr_zg^{-1} do? First, the g^{-1} will rotate another pair of faces to the top and bottom positions. Then, r_z will rotate that pair of faces by 90 degrees. Then g will rotate the two rotated faces back to their original places. The net result will always be a 90 degree rotation of an opposite pair of faces of the cube. The question now is, are *all* such 90 degree rotations conjugate to each other? In particular, are 90 degree *counterclockwise* rotations the same as 90 degree *clockwise* rotations? For instance, is r_z conjugate to r_z^{-1}. In fact it is, as we'll see in the next example.

Example 85. Let $g = r_x^2$ then consider $r_x^2 \circ r_z \circ r_x^{-2}$. What will this rotation do? First r_x^{-2} will take the top face to the bottom face and vice versa. Then r_z will rotate the face z_- (which is now on top) 90 degrees counterclockwise and z_+ (which is now on the bottom) 90 degrees clockwise. Then r_x^2 will rotate z_- back to the bottom and z_+ back to the top. So we see $r_x^2 \circ r_z \circ r_x^{-2} = r_z^{-1}$. (This is related to the formula $srs^{-1} = r^{-1}$, which we saw in Chapter 9.) ♦

We have also seen that it's possible to rotate any pair of opposite faces to the top and bottom face. This means that any 90 rotation of any pair of opposite faces of the cube is conjugate to r_z.

Exercise 86.

(a) In view of Exercise 29 of Chapter 9, what's another way to write r_z^{-1} ?

(b) What rotation results from the composition $r_y^2 \circ r_x^3 \circ r_y^{-2}$?

(c) What is the order of each of the following: $r_x^3, r_x, r_z, r_z^{-1}$?

◊

The order of rotations plays an important role in determining which group elements are conjugate:

Exercise 87.

(a) What is the result of the following conjugation? $r_x \circ r_z^2 \circ r_x^{-1}$

(b) Will a rotation conjugate to r_z^2 ever have order 4? Explain your answer.

◊

We've seen that stabilizers of faces are conjugate to each other if they are rotations of the same order. Let's consider stabilizers of vertices.

Example 88. $r_y \circ r_z$ is a 120 degree stabilizer of vertex $+++$. Consider the conjugation of $r_y \circ r_z$ by the group element r_y, that is, $r_y \circ (r_y \circ r_z) \circ r_y^{-1}$. First, r_y^{-1} takes $++-$ to $+++$. Then $r_y \circ r_z$ rotates $++-$ 120 degrees counterclockwise. Then r_y rotates $++-$ back to its original place. The net result is a 120 degree counterclockwise rotation of the vertex $++-$. ♦

Exercise 89.

(a) Which vertex does $r_z \circ r_y$ stabilize? What is the order of this stabilizer?

(b) Consider the conjugate $r_x^2 \circ (r_z \circ r_y) \circ r_x^{-2}$. Which vertex will this stabilize? What is the order of this stabilizer?

(c) What is the order of a conjugate of a stabilizer of a cube's vertex? Is the order always the same? Explain your answer.

◊

Finally, let's consider conjugates of stabilizers of edges.

Example 90. The rotation $r_z^2 \circ r_y^{-1}$ stabilizes the edge $\overline{x_- z_-}$. It's a 180 degree rotation about an axis through this edges $\overline{x_- z_-}$ and $\overline{x_+ z_+}$. Consider the conjugate $r_z^2 \circ (r_z^2 \circ r_y^{-1}) \circ r_z^{-2}$. What does this rotation do? First, r_z^{-2} takes $\overline{x_+ z_-}$ to $\overline{x_- z_-}$. Then $(r_z^2 \circ r_y^{-1})$ rotates about the axis through $\overline{x_+ z_-}$ 180 degrees, switching the

two faces. Then r_z^2 rotates $\overline{x_+z_-}$ back to its original position. The net result is a 180 degree rotation about the axis through $\overline{x_+z_-}$ and $\overline{x_-z_+}$. ♦

Exercise 91.

(a) The rotation $y^2 \circ z$ stabilizes the edge $\overline{x_+y_+}$. One conjugate of this rotation $r_y \circ (y^2 \circ z) \circ r_y^{-1}$ What does the conjugate stabilize?

(b) What is the order of a conjugate of a stabilizer of an edge of a cube? Is the order always the same? Explain your answer.

◊

For all the examples we've seen so far, the order of a conjugate of any stabilizer is the same as the order of the stabilizer itself. Of course, examples are not proof– but in this case they're a strong indication that this may be a general property. In fact, we can show:

Proposition 92. Let G be a group, $g \in G$, and $\tilde{g}$ is conjugate to g. Then $|g| = |\tilde{g}|$: that is, g has the same order as $\tilde{g}$.

PROOF. The proof is outlined in the following exercise.

Exercise 93. Fill in the blanks to complete the proof that a group element and its conjugate always have the same order.

Suppose that $\tilde{g}$ is conjugate to g. This means that there exists an $x \in G$ such that $\tilde{g} = \underline{\quad < 1 > \quad}$. Suppose $|g| = n$. Compute $\tilde{g}^n$ as follows:

$\tilde{g}^n = (\underline{\quad < 2 > \quad}) \dots (\underline{\quad < 4 > \quad})$ $\quad n$ times)

$= xg(\underline{\quad < 5 > \quad})g \dots g(\underline{\quad < 6 > \quad})gx^{-1}$ (associative property)

$= xg(\underline{\quad < 7 > \quad})g...g(\underline{\quad < 8 > \quad})gx^{-1} = x(\underline{\quad < 9 > \quad})x^{-1} = \underline{\quad < 10 > \quad}$ (inverse property)

It follows that $|\tilde{g}| \leq |\underline{\quad < 11 > \quad}|$. On the other hand,

$$(\underline{\quad < 12 > \quad})\tilde{g}(\underline{\quad < 13 > \quad}) = g \quad \text{(inverse property)}.$$

The same proof shows that $|g|\underline{\quad < 14 > \quad}|\tilde{g}|$ Therefore, $|g| = \underline{\quad < 15 > \quad}$ ◊

□

Exercise 94. We've shown that if elements are conjugate they must have the same order.

(a) What is the converse of the above statement?

(b) Prove or disprove the converse using previous examples to help you.

◊

Conjugacy classes and the class equation

We have seen before that g-equivalent elements form an equivalence class. This means that the operation of conjugacy defines an equivalence relation, and every set of conjugate elements is an equivalence classes. These equivalence classes are known as ***conjugacy classes***. The upshot is that we have the group G partitioned into 5 conjugacy classes, consisting of:

- the identity,
- 90 degree stabilizers of faces,
- 180 degree stabilizers of faces,
- stabilizers of vertices,
- stabilizers of edges.

This is exactly the method we used before to count up the number of elements in G. What we've just done for the rotational symmetries of a cube can be done for any group. We have the general formula:

$$|G| = \sum(\text{orders of conjugacy classes}).$$

This is known as the ***class equation***.

Example 95. We can verify that the class equation correctly calculates the order of the group of rotational symmetries of a cube.

$$\begin{aligned}
|G| =& |\text{conjugacy class of 90 degree stabilizers of faces}| \\
&+ |\text{conjugacy class of 180 degree stabilizers of faces}| \\
&+ |\text{conjugacy class of stabilizers of vertices}| \\
&+ |\text{conjugacy class of stabilizers of edges}| \\
&+ |\text{conjugacy class of identity}| \\
=& 6 + 3 + 8 + 6 + 1 \\
=& 24.
\end{aligned}$$

♦

Let's use the class equation to verify $|G|$ for some other familiar groups.

Example 96.

Consider the group S_3. Note this is the same as the dihedral group of an equilateral triangle. Let s be the reflection that leaves the vertex labeled '1' fixed,

and let r be the counterclockwise rotation by 120 degrees. We can find the conjugacy classes of S_3 by creating a table with a column for each of the elements in the group. Each row will represent a conjugacy class.

It's clear that id has its own conjugacy class of one element. For example, $r^2 \circ \mathsf{id} \circ \mathsf{r} = \mathsf{r}^2 \circ \mathsf{r} = \mathsf{id}$. We can verify that id is only conjugate to itself.

We can see that r has two conjugates. For example:

$\mathsf{id} \circ \mathsf{r} \circ \mathsf{id} = \mathsf{r}$

$s \circ r \circ s = s \circ s \circ r^2 = \mathsf{id} \circ \mathsf{r}^2 = \mathsf{r}^2$ by Proposition 42 in Chapter 9.

We don't need a row for r^2 because it belongs to the same conjugacy class as r. Computing the row for s completes the table, since s is conjugate to all the other reflections.

g	id	r	r^2	s	$s \circ r$	$s \circ r^2$
$g \circ \mathsf{id} \circ \mathsf{g}^{-1}$	id	id	id	id	id	id
$g \circ r \circ g^{-1}$	r	r	r	r^2	r^2	r^2
$g \circ s \circ g^{-1}$	s	$s \circ r$	$s \circ r^2$	s	$s \circ r^2$	$s \circ r$

The table shows that S_3 is partitioned into three conjugacy classes: id, rotations and reflections of orders 1, 2, and 3 respectively. The class equation verifies the order of S_3.

$|S_3| = 1 + 2 + 3 = 6$ ♦

Exercise 97.

(a) Complete a conjugacy table like the one in Example 96 for $G = D_4$. As in the example r is a counterclockwise rotation by 90 degrees and s is the reflection that leaves the vertex labeled "1" fixed. Compute and simplify the conjugate expressions as compositions of r and s. We show one row. How many more rows are needed to complete the table?

g	id	r	r^2	r^3	s	$s \circ r$	$s \circ r^2$	$s \circ r^3$
$g \circ \mathsf{id} \circ \mathsf{g}^{-1}$	—	–	–	–	–	–	–	–

Remember, once a group element appears in a row, you don't need to compute a row for that element, because you have already found its conjugacy class.

(b) Verify that the class equation correctly calculates $|D_4|$.

◊

Example 98. We can also create a conjugacy table for using permutation notation. Here is the conjugacy table for S_3 using permutations.

g	(1)	(123)	(132)	(23)	(13)	(12)
$g \circ (1) \circ g^{-1}$	(1)	(1)	(1)	(1)	(1)	(1)
$g \circ (123) \circ g^{-1}$	(123)	(123)	(123)	(132)	(132)	(132)
$g \circ (23) \circ g^{-1}$	(23)	(13)	(12)	(23)	(12)	(13)

Recall the relabeling method in Exercise 76. We recommend using this method to save time when making conjugacy tables.

For instance, to simplify $(12) \circ (23) \circ (12)$ we can relabel (23) according to (12). That is: $2 \to 1$ and $3 \to 3$. So, $(12) \circ (23) \circ (12) = (13)$. ♦

In the next exercise you may practice creating a conjugacy table using both permutation notation and the relabeling method.

Exercise 99.

(a) Create a conjugacy table for A_4 (The subgroup of even permutations in S_4) See Definition 100 of Section 10.6.2. We show one a table with one row. How many rows to complete the conjugacy table? (Use the relabeling method to save time in creating your table.)

x	(1)	(12)(34)	(13)(24)	(14)(23)	(123)	...
$g \circ (1) \circ g^{-1}$	–	–	–	–	–	...

(b) Verify that the class equation correctly calculates $|A_4|$.

◊

Exercise 100. Let G be an abelian group of finite order and $x, g \in G$. Simplify the conjugate expression $x \circ g \circ x^{-1}$. How many conjugacy classes are in the abelian group G? How many elements are in each conjugacy class? ◊

14

Algebraic Coding

Coding theory is an application of algebra that has become increasingly important over the last several decades. When we transmit data, we are concerned about sending a message over a channel that could be affected by "noise." We wish to be able to encode and decode the information in a manner that will allow the detection, and possibly the correction, of errors caused by noise. This situation arises in many areas of communications, including radio, telephone, television, computer communications, and even compact disc player technology. Probability, combinatorics, group theory, linear algebra, and polynomial rings over finite fields all play important roles in coding theory. [1]

14.1 Error-Detecting and Correcting Codes

Let us examine a simple model of a communications system for transmitting and receiving coded messages (Figure 14.1). Uncoded messages consist of a sequence of symbols, such as letters or characters. Typically these symbols are re-expressed in a binary code (such as ASCII), so that the message can be considered as a sequence of binary digits (binary digits are referred to as ***bits***). This sequence is divided up into chunks of m bits apiece: these binary m-tuples are referred to as ***message words*** . Message words are then encoded into ***codewords*** of n bits apiece by a device called an ***encoder***. The Codewords are transmitted over a channel and received by a receiver. Random noise in this transmission process causes some of the bits to be corrupted: and we say that an ***error*** occurs every time a bit is changed from 0 to 1 or vice-versa due to transmission noise. A ***decoding scheme*** is a method that either converts each received n-tuple into a message word or gives an error message for that n-tuple. If the received word is a codeword (one of the special n-tuples allowed to be transmitted), then the decoded message word must be the unique message word that encodes into the codeword. For received words that are not codewords, the decoding scheme will give an error indication, or, if we

[1] Thanks to Tom Judson for material used in this chapter.

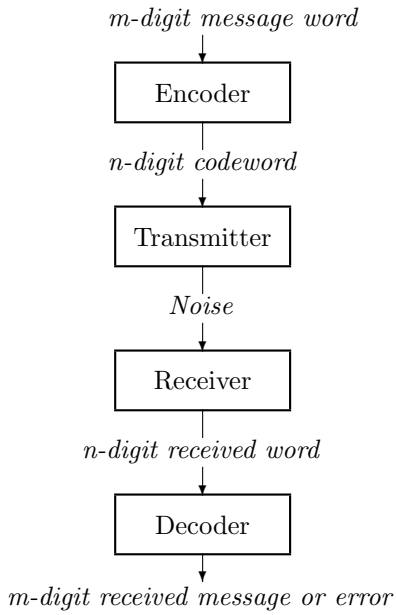


Figure 14.1. Encoding and decoding messages

are more clever, will actually try to correct the error and reconstruct the original message word. Our goal is to transmit error-free messages as cheaply and quickly as possible.

Exercise 1. Why is the following encoding scheme not acceptable?

Information:	0	1	2	3	4	5	6	7	8
Codeword:	000	001	010	011	101	110	111	000	001

◊

Example 2. One possible coding scheme would be to send each message word several times and to compare the received copies with one another. Suppose that the message word to be encoded is a binary m-tuple $(x_1, x_2, \ldots, x_m)$. The message is encoded into a binary $3m$-tuple by simply repeating the message three times:

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_n).$$

To decode the received word, we choose as the ith digit the one that appears in the ith place in at least two of the three transmissions. For example, if the

original message is (0110), then the transmitted message will be (0110 0110 0110). If there is a transmission error in the fifth digit, then the received word will be (0110 1110 0110), which will be correctly decoded as (0110).[2] This triple-repetition method will automatically detect and correct all single errors, but it is slow and inefficient: to send a message word consisting of m bits, $2m$ extra bits are required, and we can only detect and correct single errors. We will see that it is possible to find an error-correcting encoding scheme that will encode a message of m bits into n bits with n much smaller than $3m$. ♦

Example 3. ***Even parity***, a commonly used coding scheme, is much more efficient than the simple repetition scheme. The ASCII (American Standard Code for Information Interchange) coding system uses binary 8-tuples, yielding $2^8 = 256$ possible codewords. However, only seven bits are needed since there are only $2^7 = 128$ ASCII characters. What can or should be done with the extra bit? Using the full eight bits, we can detect single transmission errors. For example, the ASCII codes for A, B, and C are

$$\begin{aligned} \text{A} &= 65_{10} = 01000001_2, \\ \text{B} &= 66_{10} = 01000010_2, \\ \text{C} &= 67_{10} = 01000011_2. \end{aligned}$$

Notice that the leftmost bit is always set to 0; that is, the 128 ASCII characters have codes

$$\begin{aligned} 00000000_2 &= 0_{10}, \\ &\vdots \\ 01111111_2 &= 127_{10}. \end{aligned}$$

The bit can be used for error checking on the other seven bits. It is set to either 0 or 1 so that the total number of 1 bits in the representation of a character is even. Using even parity, the codes for A, B, and C now become

$$\begin{aligned} \text{A} &= 01000001_2, \\ \text{B} &= 01000010_2, \\ \text{C} &= 11000011_2. \end{aligned}$$

Suppose an A is sent and a transmission error in the sixth bit is caused by noise over the communication channel so that (01000101) is received. We know an error has occurred since the received word has an odd number of 1's, and we can now request that the codeword be transmitted again. When used for error checking, the leftmost bit is called a ***parity check bit***.

By far the most common error-detecting codes used in computers are based on the addition of a parity bit. Typically, a computer stores information in binary

[2] We will adopt the convention that bits are numbered left to right in binary n-tuples.

words consisting of 8, 16, or 32 bits: a ***byte*** for example is a 8-bit binary word. One bit in each binary word is set aside as the parity check bit, and is not used to store information. This bit is set to either 0 or 1, so as to make the total number of 1's to be even.

Adding a parity check bit allows the detection of all single errors because changing a single bit either increases or decreases the number of 1's by one, and in either case the parity has been changed from even to odd, so the new word is not a codeword. (We could also construct an error detection scheme based on ***odd parity***; that is, we could set the parity check bit so that a codeword always has an odd number of 1's.) ♦

The even parity system is easy to implement, but has two drawbacks. First, multiple errors are not detectable. Suppose an A is sent and the first and seventh bits are changed from 0 to 1. The received word is a codeword, but will be decoded into a C instead of an A. Second, we do not have the ability to correct errors. If the 8-tuple (10011000) is received, we know that an error has occurred, but we have no idea which bit has been changed. We will now investigate a coding scheme that will not only allow us to detect transmission errors but will actually correct the errors.

		Received Word							
		000	001	010	011	100	101	110	111
Transmitted	000	0	1	1	2	1	2	2	3
Codeword	111	3	2	2	1	2	1	1	0

Table 14.1: A repetition code

Example 4. Suppose that our original message is either a 0 or a 1, and that 0 encodes to (000) and 1 encodes to (111). If only a single error occurs during transmission, we can detect and correct the error. For example, if a 101 is received, then the second bit must have been changed from a 1 to a 0. The originally transmitted codeword must have been (111). This method will detect and correct all single errors.

In Table 14.1, we present all possible words that might be received for the transmitted codewords (000) and (111). Table 14.1 also shows the number of bits by which each received 3-tuple differs from each original codeword. ♦

14.1.1 Maximum-Likelihood Decoding

This section requires a knowledge of probability, It can be skipped without loss of continuity.

The coding scheme presented in Example 4 is not a complete solution to the problem because it does not account for the possibility of multiple errors. For example, either a (000) or a (111) could be sent and a (001) received. We have no means of deciding from the received word whether there was a single error in the third bit or two errors, one in the first bit and one in the second. No matter what coding scheme is used, an incorrect message could be received: we could transmit a (000), have errors in all three bits, and receive the codeword (111). It is important to make explicit assumptions about the likelihood and distribution of transmission errors so that, in a particular application, it will be known whether a given error detection scheme is appropriate. We will assume that transmission errors are rare, and, that when they do occur, they occur independently in each bit; that is, if p is the probability of an error in one bit and q is the probability of an error in a different bit, then the probability of errors occurring in both of these bits at the same time is pq. We will also assume that a received n-tuple is decoded into a codeword that is closest to it; that is, we assume that the receiver uses ***maximum-likelihood decoding***.

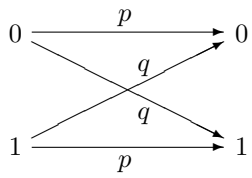


Figure 14.2. Binary symmetric channel

A ***binary symmetric channel*** is a model that consists of a transmitter capable of sending a binary signal, either a 0 or a 1, together with a receiver. Let p be the probability that the signal is correctly received. Then $q = 1 - p$ is the probability of an incorrect reception. If a 1 is sent, then the probability that a 1 is received is p and the probability that a 0 is received is q (Figure 14.2). The probability that no errors occur during the transmission of a binary codeword of length n is p^n. For example, if $p = 0.999$ and a message consisting of 10,000 bits is sent, then the probability of a perfect transmission is

$$(0.999)^{10,000} \approx 0.00005.$$

Proposition 5. If a binary n-tuple $(x_1, \ldots, x_n)$ is transmitted across a binary symmetric channel with probability p that no error will occur in each coordinate, then the probability that there are errors in exactly k coordinates is

$$\binom{n}{k} q^k p^{n-k}.$$

PROOF. Fix k different coordinates. We first compute the probability that an error has occurred in this fixed set of coordinates. The probability of an error occurring in a particular one of these k coordinates is q; the probability that an error will not occur in any of the remaining $n-k$ coordinates is p. The probability of each of these n independent events is $q^k p^{n-k}$. The number of possible error patterns with exactly k errors occurring is equal to

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!},$$

the number of combinations of n things taken k at a time. Each of these error patterns has probability $q^k p^{n-k}$ of occurring; hence, the probability of all of these error patterns is

$$\left(\begin{array}{c} n \\ k \end{array} \right) q^k p^{n-k}.$$

□

Example 6. Suppose that $p = 0.995$ and a 500-bit message is sent. The probability that the message was sent error-free is

$$p^n = (0.995)^{500} \approx 0.082.$$

The probability of exactly one error occurring is

$$\left(\begin{array}{c} n \\ 1 \end{array} \right) qp^{n-1} = 500(0.005)(0.995)^{499} \approx 0.204.$$

The probability of exactly two errors is

$$\left(\begin{array}{c} n \\ 2 \end{array} \right) q^2 p^{n-2} = \frac{500 \cdot 499}{2}(0.005)^2(0.995)^{498} \approx 0.257.$$

The probability of more than two errors is approximately

$$1 - 0.082 - 0.204 - 0.257 = 0.457.$$

♦

Exercise 7.

(a) In a binary symmetric channel where the error probability of any bit is 0.05, then whats the probability that a 3-bit message is transmitted with no errors? Whats the probability its transmitted with 1 error?

(b) Same as (a), except this time the message is 30 bits.

(c) Same as (a), except this time the error probability is 0.005.

(d) Same as (b), except this time the error probability is 0.005.

♢

Exercise 8. Suppose that a 1000-bit binary message is transmitted. Assume that the probability of a single error is p and that the errors occurring in different bits are independent of one another. If $p = 0.01$, what is the probability of more than one error occurring? What is the probability of exactly two errors occurring? Repeat this problem for $p = 0.0001$. ♢

14.1.2 Block Codes

In Figure 14.1 we illustrated the case where m-digit message words are encoded into n-digit codewords. This is certainly not the only scheme possible. For instance, we could encode different message words with codewords of differing sizes. Alternatively, we could use some kind of scheme which doesn't break the message into words at all. Such coding schemes have extremely important practical uses. Nonetheless, we will focus on the simple case where message words all have equal size, and all codewords also have equal size. We shall see shortly that group theory can be used in this case to design codes with "good" properties.

We begin as usual with a definition.

Definition 9. a (n, m) ***block code*** is a code that divides information into m-bit message words, and encodes each message word as a n-bit codeword. In order to accomplish this, the specification of an (n, m)-block code must include a *one-to-one* ***encoding function***

$$E : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$$

and an *onto* ***decoding function***

$$D : \mathbb{Z}_2^n \to \mathbb{Z}_2^m.$$

A ***codeword*** is any element in the range of E. △

In the above definition, the encoding function E for a block code is required to be one-to-one so each codeword will correspond to a *unique*. On the other hand, the decoding function D is required to be onto so that any encoded message can be decoded (although the decoded message may have errors).

Exercise 10. Given the above definition, is it possible to have a (n, m) block code where $n > m$? Is $m > n$ possible? *Explain* your answer. ♢

Example 11. The even-parity coding system developed to detect single errors in ASCII characters is an $(8, 7)$-block code. The encoding function is

$$E(x_7, x_6, \ldots, x_1) = (x_8, x_7, \ldots, x_1),$$

where $x_8 = x_7 + x_6 + \cdots + x_1$ with addition in $\mathbb{Z}_2$. ♦

Exercise 12. What is the decoding function for the code in Example 11? ◊

Exercise 13. Given an even-parity coding system in which codewords have n bits. Is the code a block code? If so, what are the parameters n and m? What is the encoding function? What is the decoding function? ◊

In order to characterize error detection and correction properties of codes, we need to quantify the degree of "similarity" between code words, since two code words that are similar are liable to be mistaken for each other. This leads naturally to the idea of "distance" between code words, defined as follows.

Definition 14. Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ be binary n-tuples. The ***Hamming distance*** or ***distance***, $d(\mathbf{x}, \mathbf{y})$, between $\mathbf{x}$ and $\mathbf{y}$ is the number of bit positions where $\mathbf{x}$ and $\mathbf{y}$ differ. The distance between two codewords is the minimum number of transmission errors required to change one codeword into the other. The ***minimum distance*** for a code, $d_{\min}$, is the minimum of all distances $d(\mathbf{x}, \mathbf{y})$, where $\mathbf{x}$ and $\mathbf{y}$ are distinct codewords. The ***weight***, $w(\mathbf{x})$, of a binary codeword $\mathbf{x}$ is the number of 1's in $\mathbf{x}$. It follows that $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, where $\mathbf{0} = (00 \cdots 0)$, since $\mathbf{x}$ differs from $\mathbf{0}$ in exactly its '1' bits. △

Example 15. Let $\mathbf{x} = (10101)$, $\mathbf{y} = (11010)$, and $\mathbf{z} = (00011)$ be all of the codewords in some code C. Then we have the following Hamming distances:

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) &= 4, \\ d(\mathbf{x}, \mathbf{z}) &= 3, \\ d(\mathbf{y}, \mathbf{z}) &= 3. \end{aligned}$$

The minimum distance for this code is 3. We also have the following weights:

$$\begin{aligned} w(\mathbf{x}) &= 3, \\ w(\mathbf{y}) &= 3, \\ w(\mathbf{z}) &= 2. \end{aligned}$$

♦

Exercise 16. Compute the Hamming distances between the following pairs of n-tuples.

(a) $(011010), (011100)$ **(b)** $(11110101), (01010100)$ ◊

(c) $(00110), (01111)$ **(d)** $(1001), (0111)$

Exercise 17. Compute the weights of the following n-tuples.

(a) (011010) **(b)** (11110101)

(c) (01111) **(d)** (1011)

◊

Exercise 18. What is the minimum distance for each of the following block codes?

1. (011010) (011100) (110111) (110000)
2. (011100) (011011) (111011) (100011)
   (000000) (010101) (110100) (110011)
3. (000000) (011100) (110101) (110001)
4. (0110110) (0111100) (1110000) (1111111)
   (1001001) (1000011) (0001111) (0000000)

◊

The weights in a particular block code are usually much easier to compute than the Hamming distances between all codewords in the code. As we shall see later, if a code is set up carefully then we can use this fact to our advantage.

In order to prove statements about Hamming distance and weight, it is useful to have a concrete formula for the distance between two codewords. Such a formula is given in the following proposition.

Proposition 19. Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ be binary n-tuples. Then the Hamming distance $d(\mathbf{x}, \mathbf{y})$ may be computed by the following formula:

$$d(\mathbf{x}, \mathbf{y}) = (x_1 \oplus y_1) + \ldots (x_n \oplus y_n)),$$

where "$\oplus$" denotes addition mod 2 and "$+$" denotes ordinary addition. Using summation notation, the formula can also be written

$$d(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} x_j \oplus y_j.$$

x_j	y_j	$x_j \oplus y_j$
0	0	0
0	1	1
1	0	1
1	1	0

Table 14.2: Bit sums (mod 2)

PROOF. For each j, we have the 4 possibilities for x_j and y_j shown in Table 14.2. The table shows that $x_j \oplus y_j = 0$ when $x_j = y_j$, and $x_j \oplus y_j = 1$ when $x_j \neq y_j$. So if we sum these terms for all j, we obtain the number of bit positions where $\mathbf{x}$ and $\mathbf{y}$ differ, which by definition is $d(\mathbf{x}, \mathbf{y})$. □

We have been referring to $d(\mathbf{x}, \mathbf{y})$ as "Hamming distance". To justify this terminology, we will prove that the function $d(\ldots)$ does indeed possess the properties that we usually associate with a notion of "distance":

Proposition 20. Let $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ be binary n-tuples. Then

(a) $d(\mathbf{x}, \mathbf{y}) \geq 0$, and $d(\mathbf{x}, \mathbf{y}) = 0$ exactly when $\mathbf{x} = \mathbf{y}$;

(b) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;

(c) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

In higher mathematics, any function that satisfies the properties listed in Proposition 20 is called a ***metric***.

Exercise 21. Using the formula in Proposition 19, prove the statements in Proposition 20. ◊

In order to see how distance relates to error correction, consider the case where $\mathbf{x} = (1101)$ and $\mathbf{y} = (1100)$ are codewords in some code. If we transmit (1101) and an error occurs in the rightmost bit, then (1100) will be received. Since (1100) is a codeword, the decoder will decode (1100) as the transmitted message. This code is clearly not very appropriate for error detection. The problem is that $d(\mathbf{x}, \mathbf{y}) = 1$, so a single-bit error can change one codeword into a different codeword.

On the other hand, given the two codewords $\mathbf{x} = (1100)$ and $\mathbf{y} = (1010)$ then $d(\mathbf{x}, \mathbf{y}) = 2$. If $\mathbf{x}$ is transmitted and a single error occurs, then no matter which bit is in error it's still impossible for $\mathbf{y}$ to be received. If for example the third bit is mistransmitted and received word is (1110), then we can tell something is wrong – that is, we can detect that an error has taken place. The same will hold true

whenever the distance between codewords is greater than or equal to 2: a single-bit error will be detectable.

Example 22. Consider the $(4, 3)$ code in which the first three bits carry information and the fourth is an even parity check bit. Table 14.3 gives the distances between all codewords in this code. We can see that the minimum distance here is 2; hence, the code is suitable as a single error-detecting code.

	0000	0011	0101	0110	1001	1010	1100	1111
0000	0	2	2	2	2	2	2	4
0011	2	0	2	2	2	2	4	2
0101	2	2	0	2	2	4	2	2
0110	2	2	2	0	4	2	2	2
1001	2	2	2	4	0	2	2	2
1010	2	2	4	2	2	0	2	2
1100	2	4	2	2	2	2	0	2
1111	4	2	2	2	2	2	2	0

Table 14.3: Distances between 4-bit codewords

♦

Let us generalize and extend this discussion. Given codewords $\mathbf{x}$ and $\mathbf{y}$:

- If $d(\mathbf{x}, \mathbf{y}) = 1$ and an error occurs where $\mathbf{x}$ and $\mathbf{y}$ differ, then $\mathbf{x}$ is changed to $\mathbf{y}$. The received codeword is $\mathbf{y}$ and no error message is given.
- If $d(\mathbf{x}, \mathbf{y}) = 2$, then a single error cannot change $\mathbf{x}$ to $\mathbf{y}$. Therefore, if $d_{\min} = 2$, we have the ability to detect single errors. However, suppose that $d(\mathbf{x}, \mathbf{y}) = 2$, $\mathbf{y}$ is sent, and a noncodeword $\mathbf{z}$ is received such that

  $$d(\mathbf{x}, \mathbf{z}) = d(\mathbf{y}, \mathbf{z}) = 1.$$

  Then the decoder cannot decide between $\mathbf{x}$ and $\mathbf{y}$. Even though we are aware that an error has occurred, we do not know what the error is.
- If $d_{\min} \geq 3$, then using the same reasoning it folows that we can detect errors of up to two bits.

  Furthermore, the maximum-likelihood decoding scheme *corrects* all single errors. Starting with a codeword $\mathbf{x}$, an error in the transmission of a single bit gives $\mathbf{y}$ with $d(\mathbf{x}, \mathbf{y}) = 1$, but $d(\mathbf{z}, \mathbf{y}) \geq 2$ for any other codeword $\mathbf{z} \neq \mathbf{x}$. Hence the correct codeword is the closest, and will be selected by the decoding scheme.

This line of reasoning leads us to the following general proposition.

Proposition 23. Let C be a code with $d_{\min} = 2n + 1$. Then C can correct any n or fewer errors. Furthermore, any $2n$ or fewer errors can be detected in C.

PROOF. Suppose that a codeword $\mathbf{x}$ is sent and the word $\mathbf{y}$ is received with at most n errors. Then $d(\mathbf{x}, \mathbf{y}) \leq n$. If $\mathbf{z}$ is any codeword other than $\mathbf{x}$, then

$$2n + 1 \leq d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \leq n + d(\mathbf{y}, \mathbf{z}).$$

Hence, $d(\mathbf{y}, \mathbf{z}) \geq n + 1$ and $\mathbf{y}$ will be correctly decoded as $\mathbf{x}$. Now suppose that $\mathbf{x}$ is transmitted and $\mathbf{y}$ is received and that at least one error has occurred, but not more than $2n$ errors. Then $1 \leq d(\mathbf{x}, \mathbf{y}) \leq 2n$. Since the minimum distance between codewords is $2n + 1$, $\mathbf{y}$ cannot be a codeword. Consequently, the code can detect between 1 and $2n$ errors. □

Example 24. In Table 14.4, the codewords $\mathbf{c}_1 = (00000)$, $\mathbf{c}_2 = (00111)$, $\mathbf{c}_3 = (11100)$, and $\mathbf{c}_4 = (11011)$ determine a single error-correcting code. ♦

	00000	00111	11100	11011
00000	0	3	3	4
00111	3	0	4	3
11100	3	4	0	3
11011	4	3	3	0

Table 14.4: Hamming distances for an error-correcting code

Exercise 25. What are the error detection and correction capabilities for the codes given in Exercise 18? ◊

Exercise 26. Suppose that a block code C has a minimum weight of 7. What are the error-detection and error-correction capabilities of C? ◊

Exercise 27. Construct a $(5, 2)$-block code. Discuss the error-detection and error-correction capabilities of your code. ◊

14.2 Group codes and linear codes

So far in this book, we have tried to relate everything we've talked about to groups. Codes are no exception to this rule! In fact, we know that all codewords of length n are elements of $\mathbb{Z}_2^n$, which in fact turns out to be a group. To show this, we must first define a group operation:

Definition 28. The group $\mathbb{Z}_2^n$ consists of the set of all binary n-tuples, together with an operation "+" defined as follows:

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

where "$\oplus$" means addition mod 2. △

Remark 29. Please note that in the following, if $\mathbf{x}$ and $\mathbf{y}$ are binary n-tuples then the expression $\mathbf{x} + \mathbf{y}$ *always* refers to the operation "+" defined in Definition 28 rather than ordinary addition. This is just one more example of the fact that in mathematics, the meaning of symbols is determined by the context. △

Now we need to put our money where our mouth is, and verify that $\mathbb{Z}_2^n$ is indeed a group.

Exercise 30.

(a) Show that if $\mathbf{x}$ and $\mathbf{y}$ are in $\mathbb{Z}_2^n$, then $\mathbf{x} + \mathbf{y}$ is also in $\mathbb{Z}_2^n$.

(b) What is the identity of $\mathbb{Z}_2^n$ under the + operation?

(c) In $\mathbb{Z}_2^9$, what is $(11000101) + (11000101)$?

(d) If $\mathbf{x} \in \mathbb{Z}_2^n$, then what is $\mathbf{x} + \mathbf{x}$?

(e) Explain why the above results show that $\mathbb{Z}_2^n$ is a group under the operation $+$.

(f) Is the group abelian? *Prove* your answer.

◊

Exercise 31. We may define a subtraction operation on $\mathbb{Z}_2^n$ as we usually do on additive groups: namely, $\mathbf{x} - \mathbf{y}$ is defined as $\mathbf{x} + \mathbf{y}'$, where $\mathbf{y}'$ is the additive inverse of $\mathbf{y}$. Based on the previous exercise, what can you conclude about the difference between $\mathbf{x} - \mathbf{y}$ and $\mathbf{x} + \mathbf{y}$? ◊

It turns out that weight and Hamming distance are in some sense "compatible" with the operation + defined on $\mathbb{Z}_2^n$, as shown in the following proposition.

Proposition 32. Let $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ be binary n-tuples. Then

(a) $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$

(b) $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$

(c) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} + \mathbf{z}, \mathbf{y} + \mathbf{z})$

We have already shown (a) in the definition of weight (Definition 14). Parts (b) and (c) are for you to prove:

Exercise 33.

(a) Prove part (b) of Proposition 32 by using part (a) of Proposition 32 and the formula in Proposition 19.

(b) Prove part (c) (*Hint*)

◊

The codes we discussed in Section 14.1 were all subsets of $\mathbb{Z}_2^n$, for some positive integer n. We shall now see that codes that are also *subgroups* have special properties that enable efficient encoding and decoding. Accordingly, we define:

Definition 34. A ***group code*** is a set of codewords that is also a subgroup of $\mathbb{Z}_2^n$. △

Note that at this point we are simply thinking of a group code as a set of codewords with certain properties. Of course, practical codes also require encoding and decoding functions: we'll talk about these later.

To check that a set of codewords is a group code, we need only verify closure under addition. It turns out that identity and inverse are guaranteed by closure:

Exercise 35.

(a) Show that a set of codewords in $\mathbb{Z}_2^n$ which is closed under the operation $+$ must also contain $\mathbf{0}$

(b) Show that any set of codewords always includes the inverses of those codewords.

(c) Prove that any set of codewords of length n that is closed under $+$ is a subgroup of $\mathbb{Z}_2^n$.

◊

Exercise 36. Without doing any addition, explain why the following set of 4-tuples in $\mathbb{Z}_2^4$ cannot be a group code.

(0110) (1001) (1010) (1100)

♢

Example 37. Suppose that we have a code that consists of the following 7-tuples:

(0000000)	(0001111)	(0010101)	(0011010)
(0100110)	(0101001)	(0110011)	(0111100)
(1000011)	(1001100)	(1010110)	(1011001)
(1100101)	(1101010)	(1110000)	(1111111).

It's possible to verify directly (for instance, by computing the Cayley table) that this code is a group code (later we will show there are much, much quicker ways to do this). To find the minimum distance, one may compute the distances between all pairs of codewords. The result is $d_{\min} = 3$, so the code can detect 2 errors and correct 1 error. ♦

From the previous example, it seems like finding the error detection/correction capabilities of a code is a long and tedious process. However, for group codes there is a far simpler way:

Proposition 38. Let $d_{\min}$ be the minimum distance for a group code C. Then $d_{\min}$ is the minimum weight of all nonzero codewords in C. That is,

$$d_{\min} = \min\{w(\mathbf{x}) : \mathbf{x} \neq \mathbf{0}\}.$$

Proof. Observe that

$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y}\} \\ &= \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} + \mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{x} + \mathbf{y}) : \mathbf{x} + \mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{z}) : \mathbf{z} \neq \mathbf{0}\}. \end{aligned}$$

□

Warning Proposition 38 *only* applies to *group codes*, and not to codes in general.

♢

14.3 Linear Block Codes

Using Proposition 38, it is now a simple matter to find the error detection and correction capabilities of a group code. However, so far we don't have a good method for creating group codes. In this section, we will use some techniques

from linear algebra to give one such method. This method is widely used in digital information processing: for instance, in CD's DVD's and satellite communications.[3]

Definition 39. The ***inner product*** of two binary n-tuples is

$$(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) \equiv x_1y_1 + \cdots + x_ny_n \pmod 2.$$

For example, $(011001) \cdot (110101) = 0 + 1 + 0 + 0 + 0 + 1 \equiv 0 \pmod 2$.

(The astute reader will recognize this definition from our discussion of UPC codes in Section 4.3). △

Note the difference between inner product and weight. When computing the weight of a codeword, the entries are added using ordinary addition. However, when computing the inner product in $\mathbb{Z}_2^n$, the terms are added with mod 2 addition.

We can also look at an inner product as the matrix product of a row vector with a column vector. To do so, we will need to re-envision our codewords as *column vectors*: so for example the binary $n-$tuple (011001) should be considered as the 6×1 column vector $(0, 1, 1, 0, 0, 1)^{\mathrm{T}}$, where "T" denotes transpose. Hence in our new vector picture, the codewords $\mathbf{x}$ and $\mathbf{y}$ are envisioned as column vectors: $\mathbf{x} = (x_1, x_2, \ldots, x_n)^{\mathrm{T}}$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)^{\mathrm{T}}$. Then we have

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= \mathbf{x}^{\mathrm{T}}\mathbf{y} \\ &= \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &= x_1y_1 + x_2y_2 + \cdots + x_ny_n. \end{aligned}$$

Again, we emphasize the addition here is mod 2 addition.

Example 40. Suppose that the words to be encoded consist of all binary 3-tuples and that our encoding scheme is even-parity. To encode an arbitrary 3-tuple, we add a fourth bit to obtain an even number of 1's. Notice that an arbitrary n-tuple $\mathbf{x} = (x_1, x_2, \ldots, x_n)^{\mathrm{T}}$ has an even number of 1's exactly when $x_1 + x_2 + \cdots + x_n = 0$; hence, a 4-tuple $\mathbf{x} = (x_1, x_2, x_3, x_4)^{\mathrm{T}}$ has an even number of 1's if $x_1 + x_2 + x_3 + x_4 = 0$, or

$$\mathbf{1} \cdot \mathbf{x} = \mathbf{1}^{\mathrm{T}}\mathbf{x} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0.$$

[3] To understand this section, readers should familiar with basic notions of linear algebra such as vectors, linear combination, matrix multiplication, and transpose. Readers may find a brief refresher on matrix multiplication in Chapter 17.

♦

Example 50 shows that an even-parity codeword can be verified by an inner product, which is a special case of a matrix multiplication. We will now show that codewords in other types of group codes can also be verified by matrix multiplication. But first, as usual, a definition:

Definition 41. Let $\mathbb{M}_{k\times n}(\mathbb{Z}_2)$ denote the set of all $k\times n$ matrices with entries in $\mathbb{Z}_2$. We do matrix operations as usual except that all our addition and multiplication operations occur in $\mathbb{Z}_2$. Define the ***null space*** of a matrix $H \in \mathbb{M}_{k\times n}(\mathbb{Z}_2)$ to be the set of all binary n-tuples $\mathbf{x}$ such that $H\mathbf{x} = \mathbf{0}$. We denote the null space of a matrix H by Null(H). △

Example 42. Suppose that

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

For a 5-tuple $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5)^{\mathrm{T}}$ to be in the null space of H, $H\mathbf{x} = \mathbf{0}$. Equivalently, the following system of equations must be satisfied (note that "+" is binary addition):

$$\begin{aligned} x_2 + x_4 &= 0 \\ x_1 + x_2 + x_3 + x_4 &= 0 \\ x_3 + x_4 + x_5 &= 0. \end{aligned}$$

This set of equations may be solved using conventional methods such as elimination (the only difference of course is that we're using binary arithmetic). Since there are more variables than equations, there is more than one solution. The set of all solutions is

$$(x_1, x_2, x_3, x_4, x_5) = \{(0,0,0,0,0), (1,1,1,1,0), (1,0,1,0,1), (0,1,0,1,1)\}.$$

This code is easily determined to be a group code. ♦

Exercise 43. Compute the null space of each of the following matrices. In cases (a) and (b), show that the result is a group code.

(a) $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$ **(b)** $\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ **(d)** $\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$

◊

Example 42 shows a case where the null space of a matrix with entries in $\mathbb{Z}_2$ turns out to be a group code. In fact, the nulll space of such a matrix is *always* a group code:

Proposition 44. Let H be in $\mathbb{M}_{k\times n}(\mathbb{Z}_2)$. Then the null space of H is a group code.

PROOF. As mentioned previously, to show that Null(H) is a group code we just need to show that it's closed under the group operation $+$. Let $\mathbf{x}, \mathbf{y} \in \text{Null}(H)$ for some matrix H in $\mathbb{M}_{k\times n}(\mathbb{Z}_2)$. Then $H\mathbf{x} = \mathbf{0}$ and $H\mathbf{y} = \mathbf{0}$. So

$$H(\mathbf{x}+\mathbf{y}) = H(\mathbf{x}+\mathbf{y}) = H\mathbf{x} + H\mathbf{y} = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

Hence, $\mathbf{x}+\mathbf{y}$ is in the null space of H and therefore must be a codeword.
□

We give a special name to group codes that are obtained as null spaces:

Definition 45. A code is a ***linear code*** if it is determined by the null space of some matrix $H \in \mathbb{M}_{k\times n}(\mathbb{Z}_2)$. △

Note that at this point, all we know is that linear codes are group codes – we haven't yet proven that all group codes in $\mathbb{Z}_2^n$ are linear codes (although this turns out to be true also!)

Example 46. Let C be the code given by the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Suppose that the 7-tuple $\mathbf{x} = (0,1,0,0,1,1)^{\mathrm{T}}$ is received. It is a simple matter of matrix multiplication to determine whether or not $\mathbf{x}$ is a codeword. Since

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

the received word is not a codeword. We must either attempt to correct the word or request that it be transmitted again. ⧫

Exercise 47. Which of the following are codewords for the code in Example 46?

(a) $(1,1,1,1,1,0)^{\mathrm{T}}$

(b) $(1,0,0,0,1,1)^{\mathrm{T}}$

(c) $(1,0,1,0,1,0)^{\mathrm{T}}$

$\Diamond$

14.4 Code words and encoding in block linear codes

We have shown how to define a set of codewords for a block linear code. But so far we don't understand too well what code words look like, and we haven't considered encoding and decoding. One of the great advantages of linear codes is that they enable very efficient methods of encoding and decoding. It's easiest to see how this works in the case where H has a special form, which we will now define.

14.4.1 Canonical Parity-check matrices

Definition 48. Suppose that H is an $k \times n$ matrix with entries in $\mathbb{Z}_2$ and $n > k$. If the last k columns of the matrix form the $k \times k$ identity matrix, I_k, then the matrix is called a ***canonical parity-check matrix***. More specifically, $H = (A \mid I_k)$, where A is the $k \times (n-k)$ matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-k} \\ a_{21} & a_{22} & \cdots & a_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{k,n-k} \end{pmatrix}$$

and I_k is the $k \times k$ identity matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

$\triangle$

Exercise 49. Only one of the matrices in Exercise 43 is a canonical parity-check matrix. Which one is it? $\Diamond$

Readers who have had a class in linear algebra may notice the similarity between canonical parity-check matrices and reduced row-echelon form. The only difference

is that reduced row-echelon matrices have the identity submatrix on the left, while the canonical parity-check matrix has it on the right.

In the following example, we will explore the relation between the canonical parity-check matrix H and the structure of the codewords.

Example 50. Suppose the matrix A is given by

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

then the associated canonical parity-check matrix is

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

Observe that the rows in H represent the parity checks on certain bit positions in a 6-tuple. The 1's in the identity matrix serve as parity checks for the 1's in the same row. If $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5, x_6)$, then

$$\mathbf{0} = H\mathbf{x} = \begin{pmatrix} x_2 + x_3 + x_4 \\ x_1 + x_2 + x_5 \\ x_1 + x_3 + x_6 \end{pmatrix},$$

which yields a system of equations:

$$\begin{aligned} x_2 + x_3 + x_4 &= 0 \\ x_1 + x_2 + x_5 &= 0 \\ x_1 + x_3 + x_6 &= 0 \end{aligned}$$

(remember that all of these equations are using binary arithmetic!) Here x_4 serves as a check bit for x_2 and x_3; x_5 is a check bit for x_1 and x_2; and x_6 is a check bit for x_1 and x_3. The identity matrix keeps x_4, x_5, and x_6 from having to check on each other. Hence, x_1, x_2, and x_3 can be arbitrary but x_4, x_5, and x_6 must be chosen to ensure parity. By following this method, we find that the vectors in $\text{Null}(H)$ are

$$\begin{array}{cccc} (000000)^{\mathrm{T}} & (001101)^{\mathrm{T}} & (010110)^{\mathrm{T}} & (011011)^{\mathrm{T}} \\ (100011)^{\mathrm{T}} & (101110)^{\mathrm{T}} & (110101)^{\mathrm{T}} & (111000)^{\mathrm{T}}. \end{array}$$

♦

The following proposition generalizes some of our findings from Example 50.

Proposition 51. Let $H \in \mathbb{M}_{k\times n}(\mathbb{Z}_2)$ be a canonical parity-check matrix. Then $\text{Null}(H)$ consists of all $\mathbf{x} \in \mathbb{Z}_2^n$ whose first $n-k$ bits are arbitrary but whose last

k bits are determined by $H\mathbf{x} = \mathbf{0}$. Each of the last k bits serves as an even parity check bit for some of the first $n-k$ bits. Hence, H gives rise to an $(n, n-k)$-block code .

The proof of Proposition 51 simply follows the same steps as in Example 50, except that instead of 3 equations in 6 unknowns we have k equations in n unknowns. Readers who've had linear algebra may recognize that this is exactly the same as the method for solving linear equations using row-echelon form: the k equations in n unknowns give rise to $n-k$ free variables, that determine the other variables in the solution.

Proposition 51 motivates the following definitions.

Definition 52. Let H be a canonical parity-check matrix, and let $\mathbf{x}$ be a codeword in Null(H). Then the first $n-k$ bits of $\mathbf{x}$ are called ***information bits*** and the last k bits are called ***check bits***. △

In Example 50, the first three bits are the information bits and the last three are the check bits.

Exercise 53.

(a) Find the canonical parity-check matrix that gives the even parity check code with three information bits. How many check bits are there?

(b) Same as (a), except with seven information bits.

(c) It is possible to implement the odd parity-check code using a parity-check matrix? *Explain* your answer.

◊

14.4.2 Standard Generator Matrices

We now have a relatively straightforward way to generate the codewords in Null(H), if H is a canonical parity-check matrix. But there's an even easier way – and one that gives us an encoding function in the bargain. But first, another definition:

Definition 54. With each $k \times n$ canonical parity-check matrix $H = (A \mid I_k)$ we can associate an $n \times (n-k)$ ***standard generator matrix*** G, given by

$$G = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix}$$

△

In order to explore the connection between parity-check and generator matrices, we continue our previous example of a particular 3×3 matrix A.

Example 55. (*Example 50 continued*) For the matrix A used in Example 50, you may check that the associated generator matrix is:

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

By comparing G with the list of vectors in Null(H), we find that all the columns of G "just happen" to be contained in Null(H) (this is no accident, as we shall see!). In fact, any linear combination of the columns of G will also be in Null(H). To see this, denote the columns of G by $\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3$, and let $x_1, x_2, x_3 \in \mathbb{Z}_2$. Then we have (by ordinary matrix multiplication, except all operations are binary)

$$H(x_1\mathbf{g}_1 + x_2\mathbf{g}_2 + x_3\mathbf{g}_3) = x_1H\mathbf{g}_1 + x_2H\mathbf{g}_2 + x_3H\mathbf{g}_3 = x_1\mathbf{0} + x_2\mathbf{0} + x_3\mathbf{0} = \mathbf{0}.$$

The linear combination of columns of G can in fact be represented more simply using matrix-vector multiplication:

$$x_1\mathbf{g}_1 + x_2\mathbf{g}_2 + x_3\mathbf{g}_3 = G\mathbf{x}$$

This gives us another way to generate codewords that are in Null(H): we just take any element in $\mathbb{Z}_2^3$, and multiply it by G. In fact, this gives us our long-sought encoding function! For any message word in $\mathbb{Z}_2^3$ we multiply on the left by G and voilà! The result is a codeword. Table 14.5 shows the results of this procedure. From the table, we find that this method of generating codewords gives us all of the vectors in Null(H). Furthermore, each different message word produces a different codeword, as a proper encoding function should.

♦

Exercise 56. For each of the following canonical parity-check matrices, find the corresponding standard generator matrix. Use the standard generator matrix to compute codewords (make a table similar to Table 14.5), and verify that the codewords are in the null space of the canonical parity-check matrix.

Message Word $\mathbf{x}$	Codeword $G\mathbf{x}$
000	000000
001	001101
010	010110
011	011011
100	100011
101	101110
110	110101
111	111000

Table 14.5: A matrix-generated code

(a) $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$ **(b)** $\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$ ♢

(c) $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ **(d)** $\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

The following proposition generalizes what we found in the previous example.

Proposition 57. Suppose that G is an $n \times k$ standard generator matrix. Then $C = \{\mathbf{y} : G\mathbf{x} = \mathbf{y} \text{ for } \mathbf{x} \in \mathbb{Z}_2^k\}$ is an (n, k)-block code. More specifically, C is a group code.

PROOF. Let $G\mathbf{x}_1 = \mathbf{y}_1$ and $G\mathbf{x}_2 = \mathbf{y}_2$ be two codewords. Then $\mathbf{y}_1 + \mathbf{y}_2$ is in C since

$$G(\mathbf{x}_1 + \mathbf{x}_2) = G\mathbf{x}_1 + G\mathbf{x}_2 = \mathbf{y}_1 + \mathbf{y}_2.$$

We must also show that two message blocks cannot be encoded into the same codeword. That is, we must show that if $G\mathbf{x} = G\mathbf{y}$, then $\mathbf{x} = \mathbf{y}$. Suppose that $G\mathbf{x} = G\mathbf{y}$. Then

$$G\mathbf{x} - G\mathbf{y} = G(\mathbf{x} - \mathbf{y}) = \mathbf{0}.$$

However, the first k coordinates in $G(\mathbf{x} - \mathbf{y})$ are exactly $x_1 - y_1, \ldots, x_k - y_k$, since they are determined by the identity matrix, I_k, part of G. Hence, $G(\mathbf{x} - \mathbf{y}) = \mathbf{0}$ exactly when $\mathbf{x} = \mathbf{y}$. □

In order to complete the link between canonical parity-check matrices and standard generating matrices, we first need the following useful result.

Proposition 58. Let $H = (A \mid I_k)$ be an $k \times n$ canonical parity-check matrix and $G = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix}$ be the corresponding $n \times (n-k)$ standard generator matrix. Then $HG = \mathbf{0}$, where $\mathbf{0}$ denotes the $k \times n-k$ matrix of all 0's.

PROOF. It is possible to prove this by writing out the matrix product HG using summation notation (see Chapter 17). This is however somewhat long-winded. A much easier way is to multiply H and G as *block matrices*.[4] Since the block sizes are compatible, we have

$$HG = (A \mid I_k) \begin{pmatrix} I_{n-k} \\ A \end{pmatrix} = (A + A),$$

but since we are adding in binary, it follows that $A + A$ is the $k \times n-k$ matrix of all 0's. □

We now administer the coup-de grâce, and establish equality between Null(H) and the code generated by G.

Proposition 59. Let $H = (A \mid I_k)$ be an $k \times n$ canonical parity-check matrix and let $G = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix}$ be the $n \times (n-k)$ standard generator matrix associated with H. Let C be the code generated by G. Then $\mathbf{y}$ is in C if and only if $H\mathbf{y} = \mathbf{0}$. In particular, C is a linear code with canonical parity-check matrix H.

PROOF. First suppose that $\mathbf{y} \in C$. Then $G\mathbf{x} = \mathbf{y}$ for some $\mathbf{x} \in \mathbb{Z}_2^{n-k}$. By Proposition 58, $H\mathbf{y} = HG\mathbf{x} = \mathbf{0}$.

Conversely, suppose that $\mathbf{y} = (y_1, \ldots, y_n)^{\mathrm{T}}$ is in the null space of H. We can split $\mathbf{y}$ into two parts as follows:

$$\mathbf{y} = \begin{pmatrix} \mathbf{y}_a \\ \mathbf{y}_b \end{pmatrix} \quad \text{where } \mathbf{y}_a := (y_1, \ldots, y_{n-k})^{\mathrm{T}} \text{ and } \mathbf{y}_b := (y_{n-k+1}, \ldots, y_n)^{\mathrm{T}}.$$

Since $\mathbf{y}$ is in the null space of H we have $H\mathbf{y} = \mathbf{0}$, which we can also write as (using partitioned matrix multiplication)

$$H\mathbf{y} = (A \mid I_m) \begin{pmatrix} \mathbf{y}_a \\ \mathbf{y}_b \end{pmatrix} = A\mathbf{y}_a + \mathbf{y}_b = \mathbf{0}.$$

Since we are adding in binary, it follows that $A\mathbf{y}_a = \mathbf{y}_b$, so that we may write

$$\mathbf{y} = \begin{pmatrix} \mathbf{y}_a \\ \mathbf{y}_b \end{pmatrix} = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix} \mathbf{y}_a,$$

so that $\mathbf{y}$ is in C. □

[4] see for example mathworld.wolfram.com/BlockMatrix.html.

14.4.3 Error detection and correction

In this section, we will show how to obtain the error correction and detection properties of a code directly from its matrix H. First, we will look at detection and correction of single errors.

Suppose that a codeword $\mathbf{x}$ is transmitted with a single error. Then the resulting transmitted word can be written as $\mathbf{x} + \mathbf{e}_j$, where $\mathbf{e}_j$ has a nonzero entry only in the j'th position:

$$\begin{aligned} \mathbf{e}_1 &= (100\cdots00)^{\mathrm{T}} \\ \mathbf{e}_2 &= (010\cdots00)^{\mathrm{T}} \\ &\vdots \\ \mathbf{e}_n &= (000\cdots01)^{\mathrm{T}} \end{aligned}$$

In this case, when we apply the parity check matrix to the transmitted codeword we obtain

$$H(\mathbf{x} + \mathbf{e}_j) = H\mathbf{x} + H\mathbf{e}_j = \mathbf{0} + H\mathbf{e}_j = H\mathbf{e}_j.$$

It appears that $H\mathbf{e}_j$ plays an important role in determining the error detection and correction properties of the code.

Exercise 60. Let H be the parity-check matrix given by

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

1. Compute $H\mathbf{e}_j$ for $j = 1, 2, 3, 4, 5$.
2. What is the relationship between your answers in (a) and the columns of H?

$\Diamond$

We generalize our findings in this exercise as follows:

Proposition 61. Let $\mathbf{e}_i$ be the binary n-tuple with a 1 in the ith coordinate and 0's elsewhere and suppose that $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Then $H\mathbf{e}_i$ is the ith column of the matrix H.

Proposition 61 is a well-known fact in linear algebra, so we refer the reader to a linear algebra textbook for proof.[5]

[5] See for example: David C. Lay, "Linear Algebra and its Applications" (Third Edition), Section 1.4.

This result leads immediately to a simple rule for single error detection.

Proposition 62. Let H be an $m \times n$ binary matrix. Then the null space of H is a single error-detecting code if and only if no column of H consists entirely of zeros.

PROOF. Suppose that Null(H) is a single error-detecting code. Then the minimum distance of the code must be at least 2. Since the null space is a group code, it is sufficient to require that the code contain no codewords of less than weight 2 other than the zero codeword. That is, $\mathbf{e}_i$ must not be a codeword for $i = 1, \ldots, n$. Since $H\mathbf{e}_i$ is the ith column of H, the only way in which $\mathbf{e}_i$ could be in the null space of H would be if the ith column were all zeros, which is impossible; hence, the code must have the capability to detect at least single errors.

Conversely, suppose that no column of H is the zero column. By Proposition 61, $H\mathbf{e}_i \neq \mathbf{0}$. □

Exercise 63. Which of the following parity-check matrices determine single error-detecting codes? *Explain* your answer.

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad ; \quad H_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

◊

Using similar reasoning, we can also come up with a method for determining single error-correction from the parity-check matrix.

Example 64. Consider the parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

The corresponding code is single error-correcting if all nonzero codewords have weight greater than two. Since there are no zero columns, Proposition 62 tells us that no codewords have weight 1. So we only need to check that Null(H) does not contain any 4-tuples of weight 2, so that $(1100)^{\mathrm{T}}$, $(1010)^{\mathrm{T}}$, $(1001)^{\mathrm{T}}$, $(0110)^{\mathrm{T}}$, $(0101)^{\mathrm{T}}$, and $(0011)^{\mathrm{T}}$ must not be in Null(H). ♦

Exercise 65. Does the code in Example 64 correct single errors? *Explain* your answer. ◊

For larger codewords, the task of checking all tuples of weight 2 can be tedious. Fortunately, there is a much easier way that avoids exhausting checking:

Proposition 66. Let H be a binary matrix. The null space of H is a single error-correcting code if and only if H does not contain any zero columns and no two columns of H are identical.

PROOF. The n-tuple $\mathbf{e}_i + \mathbf{e}_j$ has 1's in the ith and jth entries and 0's elsewhere, and $w(\mathbf{e}_i + \mathbf{e}_j) = 2$ for $i \neq j$. Since

$$\mathbf{0} = H(\mathbf{e}_i + \mathbf{e}_j) = H\mathbf{e}_i + H\mathbf{e}_j$$

can only occur if the ith and jth columns are identical, the null space of H is a single error-correcting code. □

Exercise 67. Which of the parity-check matrices in Exercise 56 produce codes that can correct single errors? ♢

Suppose now that we have a canonical parity-check matrix H with three rows. Then we might ask how many more columns we can add to the matrix and still have a null space that is a single error-detecting and single error-correcting code. Since each column has three entries, there are $2^3 = 8$ possible distinct columns. We cannot add the columns

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

So we can add as many as four columns and still maintain a minimum distance of 3.

In general, if H is an $k \times n$ canonical parity-check matrix, then there are $n - k$ information bits in each codeword. Each column has k bits, so there are 2^k possible distinct columns. It is necessary that the columns $\mathbf{0}, \mathbf{e}_1, \ldots, \mathbf{e}_n$ be excluded, leaving $2^k - (1+n)$ remaining columns for information if we are still to maintain the ability not only to detect but also to correct single errors.

Exercise 68. Suppose we want to design a code that encodes each of the 128 ASCII characters as a single codeword, such that the code also can detect and/or correct single-bit errors. We also want codewords to be as short as possible to speed up transmission.

(a) How many information bits are in each codeword?

(b) In order to *detect* single-bit errors, what is the smallest possible codeword size?

(c) In order to *correct* single-bit errors, what is the smallest possible codeword size? (*Hint*)

(d) Redo parts (a), (b), (c) if we want instead to encode the extended ASCII character set of 256 characters.

◊

Exercise 69.

(a) What is the smallest possible codeword size for a single error-correcting code with 20 information bits per codeword?

(b) What is the smallest possible codeword size for a single error-correcting code with 32 information bits per codeword?

◊

14.5 Efficient Decoding

We are now at the stage where we are able to generate linear codes that detect and correct errors fairly easily. However, we haven't yet seen a good way to decode a received n-tuple that has some errors. The only thing we can do so far is compare the received n-tuple, to each possible codeword, and find the closest one. If the code is large, this may be very time-consuming.

In the following subsections, we will explore two different decoding methods which are much efficient and practical.

14.5.1 Decoding using syndromes

The following example introduces the notion of *syndrome*.

Example 70. Given the binary matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and the 5-tuples $\mathbf{x} = (11011)^{\mathrm{T}}$ and $\mathbf{y} = (01011)^{\mathrm{T}}$, we can compute

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

and

$$H\mathbf{y} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Hence, $\mathbf{x}$ is a codeword and $\mathbf{y}$ is not, since $\mathbf{x}$ is in the null space and $\mathbf{y}$ is not. Notice that $H\mathbf{x}$ is identical to the first column of H. In fact, this is where the error occurred. If we flip the first bit in $\mathbf{y}$ from 0 to 1, then we obtain $\mathbf{x}$. ♦

It appears from this example that the vector $H\mathbf{x}$ has special importance, so we create a special term for it:

Definition 71. If H is an $k \times n$ matrix and $\mathbf{x} \in \mathbb{Z}_2^n$, then $H\mathbf{x}$ is called the ***syndrome*** of $\mathbf{x}$ △

The following proposition allows the quick detection and correction of errors.

Proposition 72. Let the $k \times n$ binary matrix H determine a linear code and let $\mathbf{x}$ be the received n-tuple. Write $\mathbf{x}$ as $\mathbf{x} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c}$ is the transmitted codeword and $\mathbf{e}$ is the transmission error. Then the syndrome $H\mathbf{x}$ of the received codeword $\mathbf{x}$ is also the syndrome of the error $\mathbf{e}$.

PROOF. $H\mathbf{x} = H(\mathbf{c} + \mathbf{e}) = H\mathbf{c} + H\mathbf{e} = \mathbf{0} + H\mathbf{e} = H\mathbf{e}$. □

This proposition tells us that the syndrome of a received word depends solely on the error and not on the transmitted codeword. The proof of the following proposition follows immediately from Proposition 72 and from the fact that $H\mathbf{e}_j$ is the jth column of the matrix H.

Proposition 73. Let $H \in \mathbb{M}_{k\times n}(\mathbb{Z}_2)$ and suppose that the linear code corresponding to H is single error-correcting. Let $\mathbf{r}$ be a received n-tuple that was transmitted with at most one error. If the syndrome of $\mathbf{r}$ is $\mathbf{0}$, then no error has occurred; otherwise, if the syndrome of $\mathbf{r}$ is equal to some column of H, say the ith column, then the error has occurred in the ith bit.

Example 74. Consider the matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

and suppose that the 6-tuples $\mathbf{x} = (111110)$, $\mathbf{y} = (111111)$, and $\mathbf{z} = (010111)$ have been received (technically these are column vectors, but we write them as row vectors for convenience). Then

$$H\mathbf{x} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, H\mathbf{y} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, H\mathbf{z} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Hence, $\mathbf{x}$ has an error in the third bit and $\mathbf{z}$ has an error in the fourth bit. The transmitted codewords for $\mathbf{x}$ and $\mathbf{z}$ must have been (110110) and (010011), respectively. The syndrome of $\mathbf{y}$ does not occur in any of the columns of the matrix H, so multiple errors must have occurred to produce $\mathbf{y}$. ♦

Exercise 75. Let

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Compute the syndrome caused by each of the following transmission errors.

1. An error in the first bit.
2. An error in the third bit.
3. An error in the last bit.
4. Errors in the third and fourth bits.

◊

Exercise 76. Let C be the code obtained from the null space of the matrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Decode the message

$$11101 \quad 11011 \quad 10101 \quad 01101$$

if possible. ◊

Exercise 77. List all possible syndromes for the codes associated with each the parity matrices in Exercise 56. ◊

14.5.2 Coset Decoding

We can use group theory to obtain another way of decoding messages that makes use of *cosets*. (If you've forgotten what cosets are, you may look back at Chapter 12 to refresh your memory.)

Since the linear code C is a subgroup of $\mathbb{Z}_2^n$, it follows that $\mathbb{Z}_2^n$ may be partitioned into cosets of C. In particular, if C is an (n, m)-linear code, then a coset of C in $\mathbb{Z}_2^n$ is written in the form $\mathbf{x} + C$, where $\mathbf{x} \in \mathbb{Z}_2^n$. By Lagrange's Theorem, there are

	Cosets
C	(00000) (01101) (10011) (11110)
(10000) + C	(10000) (11101) (00011) (01110)
(01000) + C	(01000) (00101) (11011) (10110)
(00100) + C	(00100) (01001) (10111) (11010)
(00010) + C	(00010) (01111) (10001) (11100)
(00001) + C	(00001) (01100) (10010) (11111)
(10100) + C	(00111) (01010) (10100) (11001)
(00110) + C	(00110) (01011) (10101) (11000)

Table 14.6: Cosets of C

2^{n-m} distinct cosets of C in $\mathbb{Z}_2^n$. The following example shows how this works in a particular case:

Example 78. Let C be the $(5,3)$-linear code given by the parity-check matrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

The code consists of the codewords

$$(00000) \quad (01101) \quad (10011) \quad (11110),$$

There are $2^{5-2} = 2^3$ cosets of C in $\mathbb{Z}_2^5$, each with order $2^2 = 4$. These cosets are listed in Table 14.6. ♦

Let's see how knowing the cosets helps us to decode a message. Suppose that $\mathbf{x}$ was the original codeword sent and that $\mathbf{r}$ is the n-tuple received. If $\mathbf{e}$ is the transmission error, then $\mathbf{r} = \mathbf{e} + \mathbf{x}$ or, equivalently, $\mathbf{x} = \mathbf{e} + \mathbf{r}$. However, this is exactly the statement that $\mathbf{r}$ is an element in the coset $\mathbf{e}+C$. In maximum-likelihood decoding we expect the error $\mathbf{e}$ to be as small as possible; that is, $\mathbf{e}$ will have the least weight. An n-tuple of least weight in a coset is called a ***coset leader***. Once we have determined a coset leader for each coset, the decoding process becomes a task of calculating $\mathbf{r} + \mathbf{e}$ to obtain $\mathbf{x}$.

Example 79. In Table 14.6, notice that we have chosen a representative of the least possible weight for each coset. These representatives are coset leaders. Now suppose that $\mathbf{r} = (01111)$ is the received word. To decode $\mathbf{r}$, we find that it is in the coset $(00010) + C$; hence, the originally transmitted codeword must have been $(01101) = (01111) + (00010)$. ♦

A potential problem with this method of decoding is that we might have to examine every coset for the received codeword. The following proposition shows us

that we can avoid this because the syndrome that we calculate from the received codeword points to exactly one coset:

Proposition 80. Let C be an (n, k)-linear code given by the matrix H and suppose that $\mathbf{x}$ and $\mathbf{y}$ are in $\mathbb{Z}_2^n$. Then $\mathbf{x}$ and $\mathbf{y}$ are in the same coset of C if and only if $H\mathbf{x} = H\mathbf{y}$. That is, two n-tuples are in the same coset if and only if their syndromes are the same.

PROOF. Two n-tuples $\mathbf{x}$ and $\mathbf{y}$ are in the same coset of C exactly when $\mathbf{x} - \mathbf{y} \in C$; however, this is equivalent to $H(\mathbf{x} - \mathbf{y}) = 0$ or $H\mathbf{x} = H\mathbf{y}$. □

This proposition gives us a three-step process for finding decoding:

(a) Compute the syndrome for the received codeword;

(b) Find the coset leader of the coset associated with this syndrome;

(c) Subtract the coset leader from the received codeword to find the most likely transmitted codeword.

To facilitate step (b) of this process, we may make a lookup table that displays the coset leader associated with each syndrome. Such a table is called a ***decoding table***.

Example 81. Table 14.7 is a decoding table for the code C given in Example 78. If $\mathbf{x} = (01111)$ is received, then its syndrome can be computed to be

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Examining the decoding table, we determine that the coset leader is (00010). It is now easy to decode the received codeword. ♦

Given an (n, k)-block code, the question arises of whether or not coset decoding is a manageable scheme. A decoding table requires a list of cosets and syndromes, one for each of the 2^{n-k} cosets of C. Suppose that we have a $(32, 24)$-block code. We have a huge number of codewords, 2^{24}, yet there are only $2^{32-24} = 2^8 = 256$ cosets.

Exercise 82. Let C be the group code in $\mathbb{Z}_2^3$ defined by the codewords (000) and (111). Compute the cosets of H in $\mathbb{Z}_2^3$. Why was there no need to specify right or left cosets? Give the single transmission error, if any, to which each coset corresponds. ◊

Exercise 83. For each of the following matrices, find the cosets of the corresponding code C. Give a decoding table for each code if possible.

Syndrome	Coset Leader
(000)	(00000)
(001)	(00001)
(010)	(00010)
(011)	(10000)
(100)	(00100)
(101)	(01000)
(110)	(00110)
(111)	(10100)

Table 14.7: Syndromes for each coset

(a) $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$ **(b)** $\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ **(d)** $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$

◊

14.6 Additional algebraic coding exercises

Exercise 84. Let C be a linear code. Show that either the ith coordinates in the codewords of C are all zeros or exactly half of them are zeros. (*Hint*) ◊

Exercise 85. Show that the codewords of even weight in a linear code C are also a linear code. (*Hint*) ◊

Exercise 86. Let C be a linear code. Show that either every codeword has even weight or exactly half of the codewords have even weight. (*Hint*) ◊

Exercise 87. Let C be an (n, k)-linear code. Define the ***dual*** or ***Orthogonal code*** of C to be

$$C^{\perp} = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in C\}.$$

(a) Find the dual code of the linear code C where C is given by the matrix

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

(b) Show that $C^\perp$ is an $(n, n-k)$-linear code.

(c) Find the standard generator and parity-check matrices of C and $C^\perp$. What happens in general? Prove your conjecture.

$\Diamond$

Exercise 88. Let H be an $m \times n$ matrix over $\mathbb{Z}_2$, where the ith column is the number i written in binary with m bits. The null space of such a matrix is called a ***Hamming code***.

(a) Show that the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

generates a Hamming code. What are the error-correcting properties of a Hamming code?

(b) The column corresponding to the syndrome also marks the bit that was in error; that is, the ith column of the matrix is i written as a binary number, and the syndrome immediately tells us which bit is in error. If the received word is (101011), compute the syndrome. In which bit did the error occur in this case, and what codeword was originally transmitted?

(c) Give a binary matrix H for the Hamming code with six information positions and four check positions. What are the check positions and what are the information positions? Encode the messages (101101) and (001001). Decode the received words (0010000101) and (0000101100). What are the possible syndromes for this code?

(d) What is the number of check bits and the number of information bits in an (m, n)-block Hamming code? Give both an upper and a lower bound on the number of information bits in terms of the number of check bits. Hamming codes having the maximum possible number of information bits with k check bits are called ***perfect***. Every possible syndrome except **0** occurs as a column. If the number of information bits is less than the maximum, then the code is called ***shortened***. In this case, give an example showing that some syndromes can represent multiple errors.

♢

Exercise 89. Write a program to implement a $(16, 12)$-linear code. Your program should be able to encode and decode messages using coset decoding. Once your program is written, write a program to simulate a binary symmetric channel with transmission noise. Compare the results of your simulation with the theoretically predicted error probability. ♢

Historical Note

Modern coding theory began in 1948 with C. Shannon's paper, "A Mathematical Theory of Information" [7]. This paper offered an example of an algebraic code, and Shannon's Theorem proclaimed exactly how good codes could be expected to be. Richard Hamming began working with linear codes at Bell Labs in the late 1940s and early 1950s after becoming frustrated because the programs that he was running could not recover from simple errors generated by noise. Coding theory has grown tremendously in the past several years. *The Theory of Error-Correcting Codes*, by MacWilliams and Sloane [5], published in 1977, already contained over 1500 references. Linear codes (Reed-Muller $(32, 6)$-block codes) were used on NASA's Mariner space probes. More recent space probes such as Voyager have used what are called convolution codes. Currently, very active research is being done with Goppa codes, which are heavily dependent on algebraic geometry.

14.7 References and Suggested Readings

[1] Blake, I. F. "Codes and Designs," *Mathematics Magazine* **52** (1979), 81–95.

[2] Hill, R. *A First Course in Coding Theory*. Oxford University Press, Oxford, 1986.

[3] Levinson, N. "Coding Theory: A Counterexample to G. H. Hardy's Conception of Applied Mathematics," *American Mathematical Monthly* **77** (1970), 249–58.

[4] Lidl, R. and Pilz, G. *Applied Abstract Algebra*. Springer-Verlag, New York, 1984.

[5] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.

[6] Roman, S. *Coding and Information Theory*. Springer-Verlag, New York, 1992.

[7] Shannon, C. E. "A Mathematical Theory of Communication," *Bell System Technical Journal* **27** (1948), 379–423, 623–56.

[**8**] Thompson, T. M. *From Error-Correcting Codes through Sphere Packing to Simple Groups*. Carus Monograph Series, No. 21. Mathematical Association of America, Washington, DC, 1983.

[**9**] van Lint, J. H. *Introduction to Coding Theory*. Springer-Verlag, New York, 1982.

15

Isomorphisms of Groups

15.1 Preliminary examples

Several times in the book so far we have run into the idea of isomorphic groups.[1] For instance:

Example 1. In Chapter 1 we pointed out that $\mathbb{C}$ under complex addition and $\mathbb{R} \times \mathbb{R}$ under pairwise addition act exactly the same. In order to introduce the new concepts of this chapter, let's go over this again.

If $z = a + bi$ and $w = c + di$ are complex numbers, we can identify them as real ordered pairs according to the following "translation":

$$a + bi \longrightarrow (a, b).$$

If we add two complex numbers and "translate" the result to an ordered pair, we find:

$$z + w = (a + bi) + (c + di) \longrightarrow (a + b, c + d).$$

On the other hand, if we map z and w separately we get:

$$z = a + bi \longrightarrow (a, b); \qquad w = c + di \longrightarrow (c, d),$$

and then if we add the resulting coordinate pairs, we obtain

$$(a, b) + (c, d) = (a + c, b + d).$$

which is the same as before. So we get the same result whether we add the complex numbers or their corresponding ordered pairs.

What we've shown is illustrated in Figure 15.1. If we start with the complex numbers z, w, we get the same result whether we follow first the arrow to the right

[1] Thanks to Tom Judson for material used in this chapter.

("translation" to $\mathbb{R}\times\mathbb{R}$) and then go down (addition in $\mathbb{R}\times\mathbb{R}$), or whether we follow first the down arrow (addition in $\mathbb{C}$) and then go right ("translation" to $\mathbb{R}\times\mathbb{R}$).[2] The "translation map" we are using is the function

$$f : \mathbb{C} \longrightarrow \mathbb{R}\times\mathbb{R} \text{ such that } f(a+bi) = (a,b).$$

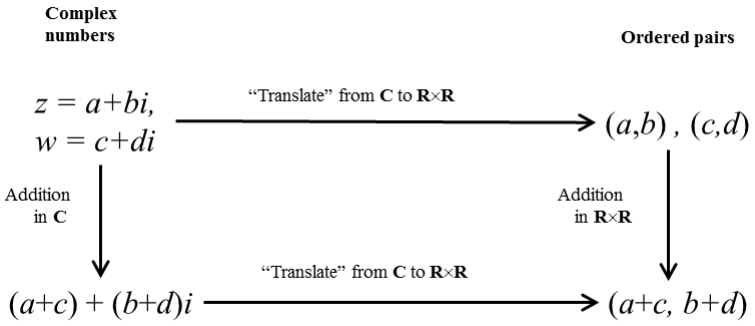


Figure 15.1. Addition is the "same" for complex numbers and real ordered pairs.

♦

Exercise 2. Let f be the function used in Example 1 to rename complex numbers as ordered pairs. Recall that $r\,\mathrm{cis}\,\theta$ is the polar form of a complex number. How would you write $f(r\,\mathrm{cis}\,\theta)$? ◊

Previously when we talked informally about two groups being isomorphic, we emphasized that the two groups are "equivalent" in some sense. So for instance, in the case of Example 1 it should be possiible to exchange the roles of $\mathbb{C}$ and $\mathbb{R}\times\mathbb{R}$ and get the same result. For this to work, there should be a function from $\mathbb{R}\times\mathbb{R}$ to $\mathbb{C}$ that shows how to replace ordered pairs with complex numbers without "changing anything". What would that function be? A prime suspect is the inverse of f:

$$f^{-1} : \mathbb{R}\times\mathbb{R} \longrightarrow \mathbb{C} \text{ such that } f^{-1}(a,b) = (a+bi)$$

But for this to work, what does that mean about f? What type of function does it have to be in order to have an inverse? You guessed it–a bijection.

Exercise 3. Prove that the function in Example 1 is a bijection. ◊

[2]This type of diagram is called a *commutative diagram*, and is widely used in abstract algebra.

Exercise 4. Draw a diagram similar to Figure 15.1 for the function $g : \mathbb{C} \to \mathbb{R} \times \mathbb{R}$ defined by $g(a + bi) = (3a, 3b)$. Show that the same "arrow-following" property holds: that is, you can follow the arrows from the upper left to lower right in either order, and still end up with the same result. ◊

Exercise 5. Prove that the function $h(a+bi) = (a+2, b+2)$ is **not** an isomorphism from $\mathbb{C}$ to $\mathbb{R} \times \mathbb{R}$. (*Hint*) ◊

Example 6. In the Symmetries chapter we also saw some examples of isomorphic groups. In particular, we saw that $\mathbb{Z}_4$, the 4^{th} roots of unity, and the rotations of a square act exactly the same under modular addition, modular multiplication, and function composition respectively. Let's remind ourselves why. The following are the Cayley tables for $\mathbb{Z}_4$, the 4^{th} roots of unity (which we'll denote by $\langle i \rangle$), and the rotations of a square (R_4):

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 15.1: Cayley table for $\mathbb{Z}_4$

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
-i	$-i$	1	i	-1

Table 15.2: Cayley table for $\langle i \rangle$

$\circ$	id	r_{90}	r_{180}	r_{270}
id	id	r_{90}	r_{180}	r_{270}
r_{90}	r_{90}	r_{180}	r_{270}	id
r_{180}	r_{180}	r_{270}	id	r_{90}
r_{270}	r_{270}	id	r_{90}	r_{180}

Table 15.3: Cayley table for R_4

(1) Comparing $\mathbb{Z}_4$ and $\langle i \rangle$, notice that if we identify

$$0 \leftrightarrow 1 \qquad 1 \leftrightarrow i \qquad 2 \leftrightarrow -1 \qquad 3 \leftrightarrow -i,$$

then the two Cayley tables match each other exactly. This means that if you add any two elements in $\mathbb{Z}_4$ (say 1 and 2), and then multiply their corresponding elements in $\langle i \rangle$ (i and -1), your results from each of these actions are in fact the same (3 and $-i$).

Hence the function $f : \mathbb{Z}_4 \longrightarrow \langle i \rangle$ that takes

$$0 \longrightarrow 1, \quad 1 \longrightarrow i, \quad 2 \longrightarrow -1, \quad 3 \longrightarrow -i$$

is an isomorphism from $\mathbb{Z}_4$ to the 4^{th} roots of unity, and these groups are isomorphic to each other.

(2) Now if we compare $\langle i \rangle$ and R_4, using the function $g : \langle i \rangle \longrightarrow R_4$ defined by

$$1 \longrightarrow \mathsf{id}, \quad \mathsf{i} \longrightarrow \mathsf{r}_{90}, \quad -1 \longrightarrow \mathsf{r}_{180}, \quad -\mathsf{i} \longrightarrow \mathsf{r}_{270},$$

we see that their Cayley tables are in fact exactly the same. Hence the 4^{th} roots of unity and the rotations of a square are isomorphic to each other, and g is an isomorphism between them.

(3) Finally, using the function $h : \mathbb{Z}_4 \longrightarrow R_4$ that takes

$$0 \longrightarrow \mathsf{id}, \quad 1 \longrightarrow \mathsf{r}_{90}, \quad 2 \longrightarrow \mathsf{r}_{180}, \quad 3 \longrightarrow \mathsf{r}_{270},$$

we see that the Cayley tables for $\mathbb{Z}_4$ and R_4 are exactly the same. Hence $\mathbb{Z}_4$ and the rotations of a square are isomorphic to each other, and h is an isomorphism between them.

So $\mathbb{Z}_4$, R_4, and $\langle i \rangle$ are all isomorphic to each other. Mathematically we state this as follows:

$$\mathbb{Z}_4 \cong R_4 \cong \langle i \rangle$$

♦

Exercise 7. Determine whether each of the following functions are isomorphisms between the groups in Example 6. Justify your answers.

(a) $f : \mathbb{Z}_4 \longrightarrow \langle i \rangle$ defined by

$$f(0) = 1, \quad f(1) = -1, \quad f(2) = i, \quad f(3) = -i.$$

(b) $g : \mathbb{Z}_4 \longrightarrow R_4$ defined by

$$g(0) = \mathsf{id}, \quad \mathsf{g}(1) = \mathsf{r}_{270}, \quad \mathsf{g}(2) = \mathsf{r}_{90}, \quad \mathsf{g}(3) = \mathsf{r}_{180}.$$

(c) $h : \langle i \rangle \longrightarrow R_4$ defined by

$$h(1) = \mathsf{id}, \quad \mathsf{h}(\mathsf{i}) = \mathsf{r}_{270}, \quad \mathsf{h}(-1) = \mathsf{r}_{180}, \quad \mathsf{h}(-\mathsf{i}) = \mathsf{r}_{90}.$$

$\Diamond$

Exercise 8. Come up with a *different* isomorphism for each pairing of groups in Example 6. For instance, find a function different from f that maps $\mathbb{Z}_4 \longrightarrow \langle i \rangle$ that matches the the two Cayley tables. Do the same thing with g and h. $\Diamond$

15.2 Formal definition and basic properties of isomorphisms

So let's buckle down and get mathematical. We start with a rigorous definition of isomorphism:

Definition 9. Two groups $(G, \cdot)$ and $(H, \circ)$ are ***isomorphic*** if there exists a bijection $\phi : G \to H$ such that the group operation is preserved; that is,

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

for all a and b in G. If G is isomorphic to H, we write $G \cong H$. The function ϕ is called an ***isomorphism***. $\triangle$

Remark 10. We'll often use greek letters (ϕ ('phi'), γ ('gamma'), ψ('psi'), etc.) to denote isomorphisms–partially because 'phi' is reminiscent of isomor'phi'sm, and partially because we don't want to confuse isomorphisms with group elements (which are denoted by g, h, and so on.) $\triangle$

Exercise 11. Let a be a real number, and consider the function $\phi_a : \mathbb{R} \to \mathbb{R}$ defined by: $\phi_a(x) = ax$. Use Definition 9 to show that ϕ_a defines an isomorphism. What are the two isomorphic groups involved? $\Diamond$

Some important properties of isomorphisms follow directly from the above definition. First we have:

Proposition 12. Given that $\phi : G \to H$ is an isomorphism, then ϕ takes the identity to the identity: that is, if e is the identity of G, then $\phi(e)$ is the identity of H.

Exercise 13. Fill in the blanks in the following proof of Proposition 12:

Given that e is the identity of $\_\_ < 1 > \_\_$ and h is an arbitrary element of $\_\_ < 2 > \_\_$. Since ϕ is a bijection, then there exists $g \in \_\_ < 3 > \_\_$ such that $\phi(\_\_ < 4 > \_\_) = h$. Then we have:

$$\begin{aligned} \phi(e) \circ h &= \phi(e) \circ \phi(\_\_ < 5 > \_\_) && \text{(substitution)} \\ &= \phi(e \cdot \_\_ < 6 > \_\_) && \text{(definition of } \_\_ < 7 > \_\_) \\ &= \phi(\_\_ < 8 > \_\_) && \text{(definition of } \_\_ < 9 > \_\_) \\ &= h && \text{(substitution)} \end{aligned}$$

Following the same steps, we can also show

$$h \circ \phi(e) = \_\_ < 10 > \_\_.$$

It follows from the definition of identity that $\_\_ < 11 > \_\_$ is the identity of the group $\_\_ < 12 > \_\_$. ◊

Another important property of isomorphisms is:

Proposition 14. Given that $\phi : G \to H$ is an isomorphism, then ϕ preserves the operation of inverse: that is, for any $g \in G$ we have

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

Exercise 15. Fill in the blanks in the following proof of Proposition 14:

Let e and f be the identities of G and H, respectively. Given that $g \in \_\_ < 1 > \_\_$, we have:

$$\begin{aligned} \phi(g) \circ \phi(g^{-1}) &= \phi(g \cdot g^{-1}) && \text{(definition of } \_\_ < 2 > \_\_) \\ &= \phi(e) && \text{(definition of } \_\_ < 3 > \_\_) \\ &= f && \text{(Proposition } \_\_ < 4 > \_\_). \end{aligned}$$

Using the same steps, we can also show

$$\phi(g^{-1}) \circ \phi(g) = \_\_ < 5 > \_\_.$$

By the definition of inverse, it follows that

$$(\phi(g))^{-1} = \_\_ < 6 > \_\_.$$

◊

It's possible to use isomorphisms to create other isomorphisms:

Exercise 16.

(a) Given that $\phi : G \to H$ is an isomorphism, show that that $\phi^{-1} : H \to G$ is also an isomorphism. (*Hint*)

(b) Given that $\phi : G \to H$ and $\psi : H \to K$ is an isomorphism, show that that $\psi \circ \phi : G \to K$ is also an isomorphism. (*Hint*)

$\Diamond$

We said in the previous section that isomorphic groups are "equivalent" in some sense. This fact has a formal mathematical statement as well:

Proposition 17. Isomorphism is an equivalence relation on groups.

Exercise 18. Prove Proposition 17. (*Hint*) $\Diamond$

15.3 More Examples

Now that we have a formal definition of what it means for two groups to be isomorphic, let's look at some more examples, in order to get a good feel for identifying groups that are isomorphic and those that aren't.

From high school and college algebra we are well familiar with the fact that when you multiply exponentials (with the same bases), the result of this operation is the same as if you had just kept the base and added the exponents. This equivalence of operations is a telltale sign for identifying possible isomorphic groups. The next two examples illustrate this observation.

For our first example, we denote the set of integer powers of 2 as $2^{\mathbb{Z}}$, that is:

$$2^{\mathbb{Z}} \equiv \{\ldots, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, \ldots\}.$$

Exercise 19. Show that $2^{\mathbb{Z}}$ with the operation of multiplication is a subgroup of $\mathbb{Q}^*$. $\Diamond$

Example 20. When elements of $2^{\mathbb{Z}}$ are multiplied together, their exponents add: we know this from basic algebra. This suggests there should be an isomorphism between $\mathbb{Z}$ and $2^{\mathbb{Z}}$. In fact, we may define the function $\phi : \mathbb{Z} \to 2^{\mathbb{Z}}$ by $\phi(n) = 2^n$. To show that this is indeed an isomorphism, by our definition we must show two things: (a) that the function preserves the operations of the respective groups; and (b) that the function is a bijection:

(a) We may compute

$$\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n).$$

(b) By definition the function ϕ is onto the subset $\{2^n : n \in \mathbb{Z}\}$ of $\mathbb{Q}^*$. To show that the map is injective, assume that $m \neq n$. If we can show that $\phi(m) \neq \phi(n)$, then we are done. Suppose that $m > n$ and assume that $\phi(m) = \phi(n)$. Then $2^m = 2^n$ or $2^{m-n} = 1$, which is impossible since $m - n > 0$.

This completes the proof that $\mathbb{Z} \cong 2^{\mathbb{Z}}$. ♦

Example 21. As in the previous example, the real powers of e under multiplication acts exactly like addition of those real exponents. This suggests that the function $\psi(x) = e^x$ is an isomorphism between an additive group and a multiplicative group. The reader will complete this proof of this fact as an exercise. ♦

Exercise 22.

(a) What is the domain and range of ψ?

(b) Prove that $\psi(x)$ is a bijection.

(c) Prove that $\psi(x)$ preserves the operations of the two groups; that $\psi(x + y) = \psi(x)\psi(y)$.

(d) Now that we know $\psi(x)$ is an isomorphism, what can we conclude about $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$?

◊

Exercise 23.

(a) What is the domain and range of the natural logarithm function $\ln(x)$?

(b) Using the results of the previous exercise and a result from an earlier exercise in this chapter, show that the natural logarithm function is an isomorphism. What are the two isomorphic groups?

(c) * Using the fact that $\log_{10}(x) = \ln(x)/\ln(10)$, show that the base 10 logarithm function is also an isomorphism. What are the two isomorphic groups?

(d) * Explain how the fact that $\log_{10}(x)$ is an isomorphism enables us to find the product of any two positive real numbers using addition and a base-10 logarithm table.

◊

Exercise 24. Prove that $\mathbb{Z} \cong n\mathbb{Z}$ for $n \neq 0$. ◊

Exercise 25. Prove that $\mathbb{C}^*$ is isomorphic to the subgroup of $GL_2(\mathbb{R})$ consisting of matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

$\Diamond$

In some cases, it is easy to show that two groups are *not* isomorphic to each other.

Example 26. Consider the groups $\mathbb{Z}_8$ and $\mathbb{Z}_{12}$. Can you tell right away that there can't be an isomorphism between them? Remember, an isomorphism is a one-to-one and onto function: but since $|\mathbb{Z}_{12}| > |\mathbb{Z}_8|$ there is no onto function from $\mathbb{Z}_8$ to $\mathbb{Z}_{12}$, and so they can not be isomorphic to each other. Similarly it can be shown that any two finite groups that have differing numbers of elements cannot be isomorphic to each other. $\blacklozenge$

Example 27. Let us look now at the group of units of $\mathbb{Z}_8$ and the group of units of $\mathbb{Z}_{12}$; i.e. $U(8)$ and $U(12)$. We have seen that these consist of the elements in $\mathbb{Z}_8$ and $\mathbb{Z}_{12}$, that are relatively prime to 8 and 12, respectively, so

$$U(8) = \{1, 3, 5, 7\}$$
$$U(12) = \{1, 5, 7, 11\}.$$

Exercise 28. Give the Cayley tables for $U(8)$ and $U(12)$. $\Diamond$

An isomorphism $\phi : U(8) \to U(12)$ is then given by

$$1 \mapsto 1$$
$$3 \mapsto 5$$
$$5 \mapsto 7$$
$$7 \mapsto 11.$$

ϕ is one-to-one and onto by observation, and we can verify visually that ϕ preserves the operations of $U(8)$ and $U(12)$ by the Cayley tables you gave. Hence $U(8) \cong U(12)$. $\blacklozenge$

Exercise 29. The function ϕ is not the only possible isomorphism between $U(8)$ and $U(12)$. Define another isomorphism between $U(8)$ and $U(12)$. $\Diamond$

Exercise 30. Prove that both $U(8)$ and $U(12)$ are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (recall $Z_2 \times Z_2$ is the set of all pairs (a, b) with $a, b \in Z_2$, where the group operation is addition mod 2 on each element in the pair). ◊

Exercise 31. Prove that $U(8)$ is isomorphic to the group of matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

◊

Exercise 32. Show that the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

form a group. Find an isomorphism of G with a more familiar group of order 6. ◊

Example 33. In Example 61 of the Cosets chapter, we looked at the normal subgroup $N = \{(1), (123), (132)\}$ of S_3. The cosets of N in S_3 were N and $(12)N$; and the factor group S_3/N had the following multiplication table.

	N	$(12)N$
N	N	$(12)N$
$(12)N$	$(12)N$	N

As we mentioned there,$N = A_3$, the group of even permutations, and $(12)N = \{(12), (13), (23)\}$ is the set of odd permutations. The information captured in S_3/N is parity; that is, multiplying two even or two odd permutations results in an even permutation, whereas multiplying an odd permutation by an even permutation yields an odd permutation. This suggests a possible isomorphism to $\mathbb{Z}_2$. ♦

Exercise 34. Prove then that the factor group $S_3/A_3 \cong \mathbb{Z}_2$. ◊

In Section 12.4.2 of the Cosets chapter we hinted at several examples of possible isomorphisms, which we'll have you prove now:

Exercise 35. Prove the following:

(a) $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$

(b) $D_n/R_n \cong \mathbb{Z}_2$

$\Diamond$

Exercise 36. And based on your work in Exercise 62 of that section, you can prove the following :)

(a) $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$

(b) $\mathbb{Z}_{24}/\langle 8 \rangle \cong \mathbb{Z}_8$

(c) $U(20)/\langle 3 \rangle \cong \mathbb{Z}_2$

$\Diamond$

We have now seen several examples where Cayley tables made it easy to show that two groups are isomorphic. (Of course, this works best if the groups are not too large, and it certainly doesn't work if the groups are infinite!) Let us now consider whether it is possible to use Cayley tables to show when groups are *not* isomorphic to each other:

Example 37. The following are the Cayley tables for $\mathbb{Z}_4$ and $U(5)$.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 15.4: Cayley table for $\mathbb{Z}_4$

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Table 15.5: Cayley table for $U(5)$

Notice that the main diagonals (left to right) of the Cayley tables seem to have a different pattern. The main diagonal for $\mathbb{Z}_4$ is the alternating sequence,

$0, 2, 0, 2$, while the main diagonal of $U(5)$ is the non-alternating sequence $1, 4, 4, 1$. It appears at first sight that these two groups must be non-isomorphic. However, we may rearrange the row and column labels in Table 15.5 to obtain Table 15.6. From the rearranged table we may read off the isomorphism: $0 \to 1, 1 \to 2, 2 \to 4, 3 \to 3$.

$\odot$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Table 15.6: Rearranged Cayley table for $U(5)$

Note the important point that when we rearranged the table, we used the *same* ordering $(1, 2, 4, 3)$ for both rows and columns. You don't want to use one ordering for rows, and a different ordering for columns. ♦

We conclude that it is more difficult to use Cayley tables to prove non-isomorphism, because we have to consider all possible rearrangements of the table. However, in some cases we can still use this method.

Exercise 38.

(a) Give the Cayley table for $U(12)$. What do you notice about the diagonal entries?

(b) If you rearranged the rows and columns of this Cayley table (always using the same ordering for the rows as for columns) then what happens to the diagonal entries?

(c) Explain why we can use this result to conclude that $\mathbb{Z}_4 \ncong U(12)$.

◊

Exercise 39. Prove or disprove: $U(8) \cong \mathbb{Z}_4$. ◊

Exercise 40. Let σ be the permutation (12), and let τ be the permutation (34). Let G be the set $\{\mathsf{id}, \sigma, \tau, \sigma\tau\}$ together with the operation of composition.

(a) Give the Cayley table for the group G.

(b) Prove or disprove: $G \cong \mathbb{Z}_4$.

(c) Prove or disprove: $G \cong U(12)$.

$\Diamond$

Example 41. Even though D_3 and $\mathbb{Z}_6$ possess the same number of elements, we might suspect that they are not isomorphic, because $\mathbb{Z}_6$ is abelian and D_3 is non-abelian. Let's see if the Cayley tables can help us here:

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Table 15.7: Cayley table for D_3

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table 15.8: Cayley table for $\mathbb{Z}_6$

Note that the Cayley table for $\mathbb{Z}_6$ is symmetric across the main diagonal while the Cayley table for D_3 is not. Furthermore, no matter how we rearrange the row and column headings for the Cayley table for $\mathbb{Z}_6$, the table will always be symmetric. It follows that there is no way to to match up the two groups' Cayley tables: so $D_3 \ncong \mathbb{Z}_6$.

This argument via Cayley table works in the case where the two groups being compared are both small, but if the groups are large then it's far too time-consuming (especially if the groups are infinite!). So let us take a different approach, and fall back on our time-tested strategy of proof by contradiction. In the case at hand, this means that we first suppose that $D_3 \cong \mathbb{Z}_6$, and then find a contradiction based on that supposition.

So, suppose that the two groups are isomorphic, which means there exists an isomorphism $\phi : \mathbb{Z}_6 \to D_3$. Let $a, b \in D_3$ be two elements such that $a \circ b \neq b \circ a$. Since ϕ is an isomorphism, there exist elements m and n in $\mathbb{Z}_6$ such that

$$\phi(m) = a \quad \text{and} \quad \phi(n) = b.$$

However,

$$a \circ b = \phi(m) \circ \phi(n) = \phi(m \oplus n) = \phi(n \oplus m) = \phi(n) \circ \phi(m) = b \circ a,$$

which contradicts the fact that a and b do not commute. ♦

Although we have only proven the non-isomorphicity of abelian and non-abelian groups for one particular case, the same method of proof can be used to prove the following general result.

Proposition 42. If G is an abelian group and H is a non-abelian group, then $G \ncong H$.

Exercise 43. Prove Proposition 42 by imitating the proof in Example 41. ◊

Exercise 44. Prove $D_4 \ncong \mathbb{Z}_8$. ◊

Exercise 45. Prove $\mathbb{Z}/6\mathbb{Z} \ncong S_3$. ◊

Finally, let's look at $\mathbb{Z}$ and $\mathbb{R}$. We know $\mathbb{Z}$ is a cyclic group with 1 as the generator, while $\mathbb{R}$ is not cyclic. (Do you remember why?) We might suspect that $\mathbb{Z} \ncong \mathbb{R}$, since one group is cyclic and the other isn't. This is in fact true, and we'll prove it. Since $\mathbb{Z}$ and $\mathbb{R}$ are infinite groups though, we can't use Cayley tables, so we have to use another method (three guessess as to what it is):

Proposition 46. $\mathbb{Z}$ is not isomorphic to $\mathbb{R}$.

PROOF. We will use a proof by contradiction. Suppose that there exists an isomorphism $\phi : \mathbb{Z} \to \mathbb{R}$. Choose any $x \in \mathbb{R}$, and let $m \in \mathbb{Z}$ be the pre-image of x, that is $\phi(m) = x$. It follows that:

$$x = \phi(m) = \phi(\underbrace{1 + \ldots + 1}_{m \text{ times}}) = \underbrace{\phi(1) + \ldots + \phi(1)}_{m \text{ times}}.$$

Thus $x \in \langle \phi(1) \rangle$. But since this is true for *any* $x \in \mathbb{R}$, this means that $\phi(1)$ is a generator of $\mathbb{R}$, which means that $\mathbb{R}$ is cyclic. But we've already seen that $\mathbb{R}$ is *not* cyclic. This contradiction shows that our original supposition must be false: namely, there *cannot* exist an isomorphism $\phi : \mathbb{Z} \to \mathbb{R}$. This completes the proof. □

Again we can generalize this proof to prove that a cyclic group cannot be isomorphic to a non-cyclic group. The contrapositive of this statement is:

Proposition 47. If G is cyclic and $G \cong H$, then H is also cyclic.

Exercise 48. Prove Proposition 47. (*Hint*) ◊

Exercise 49.

(a) Prove that $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$.

(b) Prove that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not isomorphic to $\mathbb{Z}_9$.

(c) Prove that $D_4 \ncong \mathbb{Z}_{24}/\langle 8 \rangle$

◊

15.4 More properties of isomorphisms

In the last two sections we proved several properties of isomorphic groups and their corresponding isomorphisms. We collect these properties (and add a few more) in the following proposition:

Proposition 50. Let $\phi : G \to H$ be an isomorphism of two groups. Then the following statements are true.

(1) $|G| = |H|$.

(2) $\phi^{-1} : H \to G$ is an isomorphism.

(3) G is abelian if and only if H is abelian.

(4) G is cyclic if and only if H is cyclic.

(5) If $g \in G$ is an element of order n (that is, $|\langle g \rangle| = n$), then $\phi(g) \in H$ is also an element of order n.

(6) If G' is a subgroup of G, then $\phi(G')$ is a subgroup of H and $G' \cong \phi(G')$ (Recall that $\phi(G') = \{\phi(g), g \in G'\}$.)

Proof. Assertion (1) follows from the fact that ϕ is a bijection. The proofs of (2)–(6) are indicated in the following exercises.

Exercise 51.

(a) Show part (2) of Proposition 50. (*Hint*)

(b) Show part (3) of Proposition 50. (*Hint*)

(c) Show part (4) of Proposition 50. (*Hint*)

◊

Exercise 52. Suppose, G, H, ϕ are as given in Proposition 50, and suppose $g \in G$ is an element of order n, where $n > 1$. Show that $\phi(g)^k \neq \mathsf{id}_H$ for $k = 1, \ldots n-1$, where id_H is the identity of H. Use your result to prove part (5) of Proposition 50. ◊

We will complete the proof of part (6) in two steps:

Step (I): $\phi(G')$ is a subgroup of H;

Step (II): $\phi(G')$ is isomorphic to G'.

Exercise 53. Fill in the blanks of the following proof of Step (I) (that is, $\phi(G')$ is a subgroup of H):

Let us suppose that G' is a subgroup of G. We claim that $\phi(G')$ is actually a subgroup of $\underline{\quad < 1 > \quad}$. To show this, by Proposition 71 it's enough to show that if h_1 and h_2 are elements of $\phi(G')$, then $h_1 h_2^{-1}$ is also an element of $\underline{\quad < 2 > \quad}$.

Now given that $h_1, h_2 \in \phi(G')$, by the definition of $\phi(G')$ it must be true that there exist $g_1, g_2 \in \underline{\quad < 3 > \quad}$ such that $\phi(g_1) = h_1, \phi(g_2) = h_2$. But then we have

$$\begin{aligned} h_1 h_2^{-1} &= \phi(g_1)\phi(g_2)^{-1} && \text{(by substitution)} \\ &= \phi(g_1)\phi(g_2^{-1}) && \text{(by Proposition } \underline{\quad < 4 > \quad}\text{)} \\ &= \phi(g_1 g_2^{-1}) && \text{(by the definition of } \underline{\quad < 5 > \quad}\text{).} \end{aligned}$$

Since $g_1 g_2^{-1}$ is an element of G', it follows that $h_1 h_2^{-1} \in \underline{\quad < 6 > \quad}$. This completes the proof of Step (I). ◊

Exercise 54. Complete the following proof of Step (II) (that is, G' and $\phi(G')$ are isomorphic).

Consider the function ϕ restricted to the set G': that is, $\phi : G' \to \phi(G')$. To prove this gives an isomorphism from G' to $\phi(G')$, we need to show (i) $\phi : G' \to \phi(G')$ is a bijection; and (ii) $\phi : G' \to \phi(G')$ has the operation-preserving property.

To show (i), we note that by the definition of $\phi(G')$, for every $h \in \phi(G')$ there exists a $g \in \underline{\quad < 1 > \quad}$ such that $\phi(\underline{\quad < 2 > \quad}) = h$. It follows that ϕ maps G' onto $\underline{\quad < 3 > \quad}$. Also, if $g_1, g_2 \in G'$ and $\phi(g_1) = \phi(g_2)$, then since ϕ is a one-to-one

function on G it follows that $g_1 = \underline{\quad < 4 > \quad}$. From this it follows that ϕ is also a one-to-one function on $\underline{\quad < 5 > \quad}$. We conclude that $\underline{\quad < 6 > \quad}$ is a bijection.

To show (ii), given $g_1, g_2 \in \underline{\quad < 7 > \quad}$ we have that $\phi(g_1 g_2) = \underline{\quad < 8 > \quad}$ since by assumption ϕ is an isomorphism from $\underline{\quad < 9 > \quad}$ to $\underline{\quad < 10 > \quad}$. This implies that ϕ also has the operation-preserving property when it's considered as a function from $\underline{\quad < 11 > \quad}$ to $\underline{\quad < 12 > \quad}$. This completes the proof of Step (II). ♢

□

Exercise 55. Prove S_4 is not isomorphic to D_{12}. ♢

Exercise 56. Prove A_4 is not isomorphic to D_6. (Recall that A_4 is the alternating group (group of even permutations) on 4 letters.) ♢

Exercise 57. The *quaternion group* (denoted by Q_8) consists of 8 elements: 1, i, j, k, -1, $-i$, $-j$, $-k$. You may find the Cayley table for Q_8 on wolframalpha.com or Wikipedia. Show that the quaternion group is not isomorphic to D_4. ♢

15.5 Classification up to isomorphism

We have been emphasizing that two groups that are isomorphic are the "same" as far as all group properties are concerned. So if we can characterize a class of groups as isomorphic to a well-understood set of groups, then all of the properties of the well-understood groups carry over to the entire class of groups. We will see two examples of this in the following subsections.

15.5.1 Classifying cyclic groups

Our first classification result concerns cyclic groups.

Proposition 58. If G is a cyclic group of infinite order, then G is isomorphic to $\mathbb{Z}$.

PROOF. Let G be a cyclic group with infinite order and suppose that a is a generator of G. Define a map $\phi : \mathbb{Z} \to G$ by $\phi : n \mapsto a^n$. Then

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n).$$

To show that ϕ is one-to-one, suppose that m and n are two elements in $\mathbb{Z}$, where $m \neq n$. We can assume that $m > n$. We must show that $a^m \neq a^n$. Let us suppose

the contrary; that is, $a^m = a^n$. In this case $a^{m-n} = e$, where $m - n > 0$, which contradicts the fact that a has infinite order. Our map is onto since any element in G can be written as a^n for some integer n and $\phi(n) = a^n$. □

Exercise 59. Using Proposition 58, prove again that $\{2^n | n \in \mathbb{Z}\} \cong \mathbb{Z}$. ♢

Exercise 60. Prove again that $n\mathbb{Z} \cong \mathbb{Z}$ for $n \neq 0$. ♢

Proposition 61. If G is a cyclic group of order n, then G is isomorphic to $\mathbb{Z}_n$.

PROOF. Let G be a cyclic group of order n generated by a and define a map $\phi : \mathbb{Z}_n \to G$ by $\phi : k \mapsto a^k$, where $0 \leq k < n$. The proof that ϕ is an isomorphism is left as the next exercise. □

Exercise 62. Prove that ϕ defined in Proposition 61 is an isomorphism. ♢

Exercise 63.

(a) In fact, the *converse* of Proposition 61 is true: that is, If G is isomorphic to $\mathbb{Z}_n$ then G is a cyclic group of order n. How do we know this?

(b) Is the converse of Proposition 61 also true? *Justify* your answer.

♢

Exercise 64. Show that the multiplicative group of the complex nth roots of unity is isomorphic to $\mathbb{Z}_n$. ♢

Proposition 65. If G is a group of order p, where p is a prime number, then G is isomorphic to $\mathbb{Z}_p$.

PROOF. This is a direct result of Proposition 39 in the Cosets chapter. □

15.5.2 Characterizing all finite groups: Cayley's theorem

In the previous section, we saw that any cyclic group is "equivalent" (in the sense of isomorphism) to one of the groups $\mathbb{Z}_n$. This enables us to easily conceptualize any cyclic group in terms of a standardized set of groups that we're very familiar with.

Now, can we do something similar with *all* groups? In other words, can we find a standardized set of groups so that any group can be characterized as equivalent (up to isomorphism) to one of these standard groups?.

In a way we already have a standardized characterization of finite groups, because we have seen that every finite group can be represented with a Cayley table. But this is not really satisfactory, because there are many Cayley tables which do not correspond to any group.

Exercise 66. Give examples of Cayley tables for binary operations that meet each of the following criteria. (You can make your row and column labels be the set of integers $\{1, 2, ..n\}$, for an appropriate value of n.

1. The binary operation has no identity.
2. The binary operation has an identity, but not inverses for every element
3. *The binary operation has an identity and inverses, but the associative law fails.

$\Diamond$

Although Cayley tables are not adequate for our purpose, it turns out that they provide the key to the characterization we're seeking. Consider first the following simple example.

Example 67. The Cayley table for $\mathbb{Z}_3$ is

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The addition table of $\mathbb{Z}_3$ suggests that it is the isomorphic to the permutation group $\{\mathsf{id}, (012), (021)\}$. One possible isomorphism is

$$0 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = \mathsf{id}$$

$$1 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (012)$$

$$2 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (021).$$

Notice the interesting "coincidence" that the rows of the Cayley table ((0 1 2), (1 2 0) and 2 1 0) respectively) "just happen" to agree exactly with the second rows of the three tableaus!

Of course, this "coincidence" is no accident. For example, the second row of the Cayley table is obtained as $(1 \oplus 0 \quad 1 \oplus 1 \quad 1 \oplus 2)$, and the permutation $\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$ that is the isomorphic image of 1 is actually the function from $\mathbb{Z}_3 \to \mathbb{Z}_3$ that takes n to $1 \oplus n$. The following proposition is basically a generalization of this simple observation.

♦

Proposition 68. (*Cayley's theorem*) Every group is isomorphic to a group of permutations.

PROOF. Let G be a group with $|G|$ elements. We seek a group of permutations $P \subset S_{|G|}$ that is isomorphic to G. For any $g \in G$ we may define a function $\phi_g : G \to G$ by

$$\phi_g(a) := ga.$$

We claim that ϕ_g is a permutation on G: you will show this in Exercise 69 below. Let us define the set $P \subset S_{|G|}$ as

$$P = \{\phi_g : g \in G\}.$$

Let us now define a function $\Phi : G \to P$ just as we did in Example 67:

$$\Phi(g) := \phi_g.$$

Let's pause for a minute here, to make sure that you understand what's going on. According to the definition, Φ is a function whose domain is the group G and whose range is a subset of the permutation group on $|G|$ letters. Now permutations are functions in their own right: so Φ is a function (from G to P), and for each $g \in G$, $\Phi(g)$ is *also* a function (from G to G). We could say that Φ is a function-valued function. (This can be quite unnerving the first time you see it – but such constructions are common in higher mathematics, so it's best to get used to them!) In this case, you should understand that $\Phi(g)$ is a permutation, and $\Phi(g)(a)$ is the permutation $\Phi(g)$ applied to the group element a. According to the definition of $\Phi(g)$, $\Phi(g)(a)$ is equal to $\phi_g(a)$, which by the definition of ϕ_g is equal to ga.

OK, now let's get back to the argument. To show that Φ is an isomorphism, we must show that Φ is one-to-one, onto, and preserves the group operation. You will show that Φ is one-to-one and onto in Exercise 69 below. To show that Φ preserves the group operation, we need to show that $\Phi(gh) = \Phi(g) \circ \Phi(h)$ for any elements $g, h \in G$. We may show this element-by-element: that is, we show that

$\Phi(gh)(a) = (\Phi(g) \circ \Phi(h))(a)$ for an arbitrary $a \in G$ as follows:

$$\begin{aligned} \Phi(gh)(a) &= (gh)a && \text{[definition of } \Phi(gh)\text{]} \\ &= g(ha) && \text{[associativity of } G\text{]} \\ &= g(\Phi(h)(a)) && \text{[definition of } \Phi(h)\text{]} \\ &= \Phi(g) \circ \Phi(h)(a). && \text{[definition of } \Phi(g)\text{]} \end{aligned}$$

□

Exercise 69.

(a) Show that $\phi_g : G \to G$ defined in the above proof is a permutation on G. (It is enough to show that ϕ_g is one-to-one and onto.)

(b) Complete the proof of Proposition 68 by showing that $\Phi : G \to P$ is one-to-one and onto.

◊

The isomorphism $\Phi : G \to S_{|G|}$ defined in the proof is known as the ***left regular representation*** of G. This is not the only possible isomorphism. Another isomorphism is presented in the following exercise.

Exercise 70. The ***right regular representation*** $\tilde{\Phi} : G \to S_{|G|}$ is defined as follows. For any $g \in G$ define the function $\tilde{\phi}_g : G \to G$ by

$$\tilde{\sigma}_g(a) := ag^{-1}.$$

Define the set $\tilde{P}$ as

$$\tilde{P} = \{\tilde{\phi}_g : g \in G\},$$

and define the function $\tilde{\Phi} : G \to P$ as

$$\tilde{\Phi}(g) := \tilde{\phi}_g.$$

(a) Show that $\tilde{\phi}_g : G \to G$ defined in the above proof is a permutation on G. (It follows that the set $\tilde{P}$ is a subset of $S_{|G|}$.)

(b) Show that $\tilde{\Phi} : G \to \tilde{P}$ is one-to-one and onto.

(c) Complete the proof that $G \cong \tilde{P}$ by showing that $\tilde{\Phi}$ preserves the group operation, that is: $\tilde{\Phi}(gh) = \tilde{\Phi}(g) \circ \tilde{\Phi}(h)$ for any elements $g, h \in G$.

(d) Give the isomorphism $\tilde{\Phi}$ for the group $\mathbb{Z}_3$. Is this isomorphism different from Φ defined on the same group?

◊

Historical Note

Arthur Cayley was born in England in 1821, though he spent much of the first part of his life in Russia, where his father was a merchant. Cayley was educated at Cambridge, where he took the first Smith's Prize in mathematics. A lawyer for much of his adult life, he wrote several papers in his early twenties before entering the legal profession at the age of 25. While practicing law he continued his mathematical research, writing more than 300 papers during this period of his life. These included some of his best work. In 1863 he left law to become a professor at Cambridge. Cayley wrote more than 900 papers in fields such as group theory, geometry, and linear algebra. His legal knowledge was very valuable to Cambridge; he participated in the writing of many of the university's statutes. Cayley was also one of the people responsible for the admission of women to Cambridge.

15.6 Direct Products

Given two groups G and H, it is possible to construct a new group from the Cartesian product of G and H, $G \times H$. Conversely, given a large group, it is sometimes possible to decompose the group; that is, a group is sometimes isomorphic to the direct product of two smaller groups. In this case, all of the properties of the large group can be derived from the properties of the smaller groups, which can lead to tremendous simplification.

15.6.1 External Direct Products

If $(G, \cdot)$ and $(H, \circ)$ are groups, then we can make the Cartesian product of G and H into a new group. As a set, our group is just the ordered pairs $(g, h) \in G \times H$ where $g \in G$ and $h \in H$. We can define a binary operation on $G \times H$ by

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2);$$

that is, we just multiply elements in the first coordinate as we do in G and elements in the second coordinate as we do in H. We have specified the particular operations $\cdot$ and $\circ$ in each group here for the sake of clarity; we usually just write $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Proposition 71. Let G and H be groups. The set $G \times H$ is a group under the operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ where $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

The proof is outlined in the following exercise.

Exercise 72. (*Hint*)

1. Show that the set $G \times H$ is closed under the binary operation defined in Proposition 71.
2. Show that (e_G, e_H) is the identity of $G \times H$, where e_G and e_H are the identities of the groups G and H respectively.
3. Show that the inverse of $(g, h) \in G \times H$ is (g^{-1}, h^{-1}).
4. Show that the operation defined in Proposition 71 is associative.

$\Diamond$

Example 73. Let $\mathbb{R}$ be the group of real numbers under addition. The Cartesian product of $\mathbb{R}$ with itself, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, is also a group, in which the group operation is just addition in each coordinate; that is, $(a, b) + (c, d) = (a + c, b + d)$. The identity is $(0, 0)$ and the inverse of (a, b) is $(-a, -b)$. $\blacklozenge$

Example 74. Consider

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

Although $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ both contain four elements, they are not isomorphic. We can prove this by noting that $\mathbb{Z}_4$ is cyclic, while every element (a, b) in $\mathbb{Z}_2 \times \mathbb{Z}$ has order 2 (verify this). $\blacklozenge$

The group $G \times H$ is called the ***external direct product*** of G and H. Notice the difference between 'Cartesian product' and 'external direct product': the external direct product is a group whose underlying set is a Cartesian product; but in addition, the external direct product has a group operation, which generic off-the-shelf Cartesian products don't ordinarily have.

In the previous example, we used two groups to build a new group. But there's no reason to stop with two! The direct product

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$$

of the groups $G_1, G_2, \ldots, G_n$ may be defined in a similar way.

Exercise 75. How would you write an element in $\prod_{i=1}^{n} G_i$? Write two different elements of $\prod_{i=1}^{n} G_i$, and show how you would define the group operation in terms of these two elements. (You may denote the group operation on each group G_i by the symbol '$\cdot$'. $\Diamond$

If $G = G_1 = G_2 = \cdots = G_n$, we often write G^n instead of $G_1 \times G_2 \times \cdots \times G_n$.

Example 76. The group $\mathbb{Z}_2^n$, considered as a set, is just the set of all binary n-tuples. The group operation is the "exclusive or" of two binary n-tuples. For example,

$$(01011101) + (01001011) = (00010110).$$

This group is important in coding theory, in cryptography, and in many areas of computer science. ♦

What is the difference between $G \times H$ and $H \times G$? Not much, as the following exercise shows:

Exercise 77. Show that for any groups G and H, $G \times H \cong H \times G$. (*Hint*) ◊

By extending this same idea, we find that we can rearrange the groups in a direct product arbitrarily and still end up with the "same" group:

Proposition 78. Let $G_1, G_2, \ldots G_n$ be arbitrary groups, and let $\sigma \in S_n$ be any permutation on $\{1, 2, \ldots n\}$. Then

$$G_1 \times G_2 \times \ldots \times G_n \cong G_{\sigma(1)} \times G_{\sigma(2)} \times \ldots \times G_{\sigma(n)}.$$

Exercise 79. What isomorphism would you need to define in order to prove Proposition 78? (We won't ask you to give a complete proof of the proposition, but you can if you want to!) ◊

Suppose you start out with groups that are isomorphic, and take direct products of them. Are the direct products also isomorphic? It just so happens that they are:

Proposition 80. Suppose that $G_1 \cong H_1, G_2 \cong H_2, \ldots, G_n \cong H_n$. Then $G_1 \times \ldots \times G_n \cong H_1 \times \ldots \times H_n$.

We won't give the full proof, but you can get the idea of how it goes by doing the following exercise.

Exercise 81. Prove Proposition 80 for the case where $n = 2$. (Remember that the default method for proving that groups are isomorphic is to define a suitable function and prove that it's an isomorphism.) ◊

15.6.2 Classifying abelian groups by factorization

We have used isomorphisms to classify cyclic groups (Proposition 58) and general groups (Cayley's theorem, Proposition 68). In this section, we will make use of direct products to prove a classification of abelian groups up to isomorphism. The bottom line is that every abelian group is isomorphic to a direct product of cyclic groups. To get to the bottom line, we'll have to establish some more properties of direct products, especially in relation to cyclic groups. The following proposition characterizes the order of the elements in a direct product.

Proposition 82. Let $(g, h) \in G \times H$. If g and h have finite orders r and s respectively, then the order of (g, h) in $G \times H$ is the least common multiple of r and s.

PROOF. Suppose that m is the least common multiple of r and s and let $n = |(g, h)|$. Then

$$(g, h)^m = (g^m, h^m) = (e_G, e_H)$$
$$(g^n, h^n) = (g, h)^n = (e_G, e_H).$$

Hence, n must divide m, and $n \leq m$. However, by the second equation, both r and s must divide n; therefore, n is a common multiple of r and s. Since m is the *least common multiple* of r and s, $m \leq n$. Consequently, m must be equal to n. □

By applying Proposition 82 inductively, it is possible to prove an analogous result for direct products of more than two groups. We'll leave it to you to fill in the details of the proof.

Corollary 83. Let $(g_1, \ldots, g_n) \in \prod G_i$. If g_i has finite order r_i in G_i, then the order of $(g_1, \ldots, g_n)$ in $\prod G_i$ is the least common multiple of $r_1, \ldots, r_n$.

For the rest of the section, we will be dealing with direct products of $\mathbb{Z}_n$ (we know that any cyclic group is isomorphic to $\mathbb{Z}_n$ for some n).

Example 84. Let $(8, 56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$. Since $\gcd(8, 12) = 4$, the order of 8 is $12/4 = 3$ in $\mathbb{Z}_{12}$. Similarly, the order of 56 in $\mathbb{Z}_{60}$ is 15. The least common multiple of 3 and 15 is 15; hence, $(8, 56)$ has order 15 in $\mathbb{Z}_{12} \times \mathbb{Z}_{60}$. ♦

Example 85. The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ consists of the pairs

$$(0, 0), \quad (0, 1), \quad (0, 2), \quad (1, 0), \quad (1, 1), \quad (1, 2).$$

In this case, unlike that of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, it is true that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. We need only show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. It is easy to see that $(1, 1)$ is a generator for $\mathbb{Z}_2 \times \mathbb{Z}_3$. ♦

Exercise 86. Find the order of each of the following elements.

1. $(3, 4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$
2. $(6, 15, 4)$ in $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$
3. $(5, 10, 15)$ in $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$
4. $(8, 8, 8)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$

$\Diamond$

Exercise 87.

(a) Show that $\mathbb{Z}_4 \times \mathbb{Z}_9$ is cyclic, and find 6 different generators for the group.

(b) Show that $\mathbb{Z}_3 \times \mathbb{Z}_5$ is cyclic. How many different generators does it have?

$\Diamond$

The next proposition tells us exactly when the direct product of two cyclic groups is cyclic.

Proposition 88. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

PROOF. Assume first that if $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, then $\gcd(m, n) = 1$. To show this, we will prove the contrapositive; that is, we will show that if $\gcd(m, n) = d > 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic. Notice that mn/d is divisible by both m and n; hence, for any element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\underbrace{(a, b) + (a, b) + \cdots + (a, b)}_{mn/d \text{ times}} = (0, 0).$$

Therefore, no (a, b) can generate all of $\mathbb{Z}_m \times \mathbb{Z}_n$.

The converse follows directly from Proposition 82 since $\operatorname{lcm}(m, n) = mn$ if and only if $\gcd(m, n) = 1$. □

This idea extends directly to arbitrary direct products: a product of cyclic groups is cyclic if and only if the orders of the groups in the product are all relatively prime.

Proposition 89. Let $n_1, \ldots, n_k$ be positive integers. Then

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

if and only if $\text{lcm}(n_1, \ldots, n_k) = \prod_{i=1}^{k} n_i$ (in other words, $n_1, \ldots, n_k$ are all relatively prime).

PROOF. Use the argument in Proposition 88 first with n_1 and n_2, then with $n_1 n_2$ and n_3, then with $n_1 n_2 n_3$ and n_4, and so on. (The best way to do this proof is using induction.) □

Exercise 90. Prove Proposition 89 using induction. ♢

A special case of this proposition is:

Corollary 91. If

$$m = p_1^{e_1} \cdots p_k^{e_k},$$

where the p_i's are distinct primes, then

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

PROOF. Since $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$ for $i \neq j$, the proof follows from Corollary 89. □

Exercise 92. Find three non-isomorphic abelian groups of order 8, and show that they are not isomophic. ♢

Remember that in the Permutations chapter we showed that every permutation can be "factored" as the product of disjoint cycles. (At that time, we compared this to the factorization of integers into prime factors). It turns out that abelian groups can also be "factored". This beautiful and general result is summarized in the following proposition. We will not give a complete proof of the proposition (which uses induction), but we hope that it makes sense to you in light of the foregoing discussion.[3]

Proposition 93. ***(Factorization of abelian groups)*** If G is an abelian group, then there exist prime numbers $p_1 \ldots p_k$ and exponents $e_1 \ldots e_k$ such that

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$$

Note that the prime numbers $p_1, \ldots, p_k$ may not necessarily be distinct.

Exercise 94. Show that the primes $p_1 \ldots p_k$ and exponents $e_1 \ldots e_k$ in Proposition 93 must satisfy $|G| = p_1^{e_1} \cdots p_k^{e_k}$. ♢

Exercise 95.

[3] Many proofs can be found on the web: search for "structure of finite abelian groups".

(a) Prove or disprove: There is an abelian group of order 22 that is *not* cyclic.

(b) Prove or disprove: There is an abelian group of order 24 that is *not* cyclic.

(c) Prove or disprove: There is an abelian group of order 30 that is *not* cyclic.

◊

Exercise 96.

1. Show that $\mathbb{Z}_{3^n}$ contains an element of order 3, for any positive integer n.
2. Show that every abelian group of order divisible by 3 contains an element of order 3.
3. Show that every abelian group of order divisible by 9 contains a subgroup of order 9. (*Hint*)
4. Prove or disprove: for any prime p, every abelian group of order divisible by p^2 contains a subgroup of order p^2.

◊

15.6.3 Internal Direct Products

The external direct product of two groups builds a large group out of two smaller groups. We would like to be able to reverse this process and conveniently break down a group into its direct product components; that is, we would like to be able to say when a group is isomorphic to the direct product of two of its subgroups.

Definition 97. Let G be a group with subgroups H and K satisfying the following conditions.

- $G = HK = \{hk : h \in H, k \in K\}$;
- $H \cap K = \{e\}$;
- $hk = kh$ for all $k \in K$ and $h \in H$.

Then G is the ***internal direct product*** of H and K. △

Example 98. The group $U(8)$ is the internal direct product of

$$H = \{1, 3\} \quad \text{and} \quad K = \{1, 5\}.$$

⧫

Example 99. The dihedral group D_6 is an internal direct product of its two subgroups

$$H = \{\mathsf{id}, \mathsf{r}^3\} \quad \text{and} \quad \mathsf{K} = \{\mathsf{id}, \mathsf{r}^2, \mathsf{r}^4, \mathsf{s}, \mathsf{r}^2\mathsf{s}, \mathsf{r}^4\mathsf{s}\}.$$

It can be shown that $K \cong S_3$; consequently, $D_6 \cong \mathbb{Z}_2 \times S_3$. ♦

Example 100. Not every group can be written as the internal direct product of two of its proper subgroups. If the group S_3 were an internal direct product of its proper subgroups H and K, then one of the subgroups, say H, would have to have order 3. In this case H is the subgroup $\{(1), (123), (132)\}$. The subgroup K must have order 2, but no matter which subgroup we choose for K, the condition that $hk = kh$ will never be satisfied for $h \in H$ and $k \in K$. ♦

Proposition 101. Let G be the internal direct product of subgroups H and K. Then G is isomorphic to $H \times K$.

Proof. Since G is an internal direct product, we can write any element $g \in G$ as $g = hk$ for some $h \in H$ and some $k \in K$. Define a map $\phi : G \to H \times K$ by $\phi(g) = (h, k)$.

The first problem that we must face is to show that ϕ is a well-defined map; that is, we must show that h and k are uniquely determined by g. Suppose that $g = hk = h'k'$. Then $h^{-1}h' = k(k')^{-1}$ is in both H and K, so it must be the identity. Therefore, $h = h'$ and $k = k'$, which proves that ϕ is, indeed, well-defined.

To show that ϕ preserves the group operation, let $g_1 = h_1k_1$ and $g_2 = h_2k_2$ and observe that

$$\begin{aligned}
\phi(g_1g_2) &= \phi(h_1k_1h_2k_2) \\
&= \phi(h_1h_2k_1k_2) \\
&= (h_1h_2, k_1k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= \phi(g_1)\phi(g_2).
\end{aligned}$$

We will leave the proof that ϕ is a bijection as an exercise:

Exercise 102. Prove that ϕ defined in the proof of Proposition 101 is a bijection, thus completing the proof of the proposition. ♢

□

Example 103. The group $\mathbb{Z}_6$ is an internal direct product isomorphic to $\{0, 2, 4\} \times \{0, 3\}$. ♦

Exercise 104. Prove that the subgroup of $\mathbb{Q}^*$ consisting of elements of the form $2^m 3^n$ for $m, n \in \mathbb{Z}$ is an internal direct product isomorphic to $\mathbb{Z} \times \mathbb{Z}$. ◊

Exercise 105. In this problem, we define $G \subset S_2 \times S_n$ by:

$G = (\mathsf{id}, A_n) \cup ((12), (S_n \setminus A_n))$.

(a) Show that $S_2 \times S_n$ is isomorphic to a subgroup of S_{n+2}.

(b) Show that G is a subgroup of $S_2 \times S_n$.

(c) Show that G is isomorphic to a subgroup of A_{n+2}.

(d) Show that G is isomorphic to S_n .

(e) Show that S_n is isomorphic to a subgroup of A_{n+2}.

◊

A (sort of) converse of Proposition 101 is also true:

Proposition 106. Let H and K be subgroups of G, and define the map $\phi : H \times K \to G$ by $\phi(\,(h,k)\,) = hk$. Suppose that ϕ is an isomorphism. Then G is the internal direct product of H and K. .

Exercise 107. Prove Proposition 106. ◊

Exercise 108. Let G be a group of order 20. If G has subgroups H and K of orders 4 and 5 respectively such that $hk = kh$ for all $h \in H$ and $k \in K$, prove that G is the internal direct product of H and K. ◊

Exercise 109. Prove the following: Let G, H, and K be groups such that $G \times K \cong H \times K$. Then is is also true that $G \cong H$. (*Hint*) ◊

We can extend the definition of an internal direct product of G to a collection of subgroups $H_1, H_2, \ldots, H_n$ of G, by requiring that

- $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_i \in H_i\}$;
- $H_i \cap \langle \cup_{j \neq i} H_j \rangle = \{e\}$;
- $h_i h_j = h_j h_i$ for all $h_i \in H_i$ and $h_j \in H_j$.

We will leave the proof of the following proposition as an exercise.

Proposition 110. Let G be the internal direct product of subgroups H_i, where $i = 1, 2, \ldots, n$. Then G is isomorphic to $\prod_i H_i$.

Exercise 111. Prove Proposition 110. ◊

Additional exercises

(1) Let $\omega = \text{cis}(2\pi/n)$. Show that $\omega^n = 1$, and prove that the matrices

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

generate a multiplicative group isomorphic to D_n.

(2) Show that the set of all matrices of the form

$$B = \begin{pmatrix} \pm 1 & n \\ 0 & 1 \end{pmatrix},$$

where $n \in \mathbb{Z}_n$, is a group isomorphic to D_n.

(3) Let $G = \mathbb{R} \setminus \{-1\}$ and define a binary operation on G by

$$a * b = a + b + ab.$$

Prove that G is a group under this operation. Show that $(G, *)$ is isomorphic to the multiplicative group of nonzero real numbers.

(4) Find all the subgroups of D_4. Which subgroups are normal? What are all the factor groups of D_4 up to isomorphism?

(5) Prove that D_4 cannot be the internal direct product of two of its proper subgroups.

(6) * Prove that $S_3 \times \mathbb{Z}_2$ is isomorphic to D_6. Can you make a conjecture about D_{2n}? Prove your conjecture. (*Hint*)

(7) The ***quaternion group*** is a well-known group of order 8. (You may find the Cayley table of the quaternion group by doing a web search.) Prove or disprove: The quaternion group is isomorphic to $D4$.

(8) Find all the subgroups of the quaternion group, Q_8. Which subgroups are normal? What are all the factor groups of Q_8 up to isomorphism?

(9) Prove $U(5) \cong \mathbb{Z}_4$. Can you generalize this result to show that $U(p) \cong \mathbb{Z}_{p-1}$?

(10) Write out the permutations associated with each element of S_3 in the proof of Cayley's Theorem.

(11) Prove that $A \times B$ is abelian if and only if A and B are abelian.

(12) Let H_1 and H_2 be subgroups of G_1 and G_2, respectively. Prove that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$.

(13) Let $m, n \in \mathbb{Z}$, so that $(m, n) \in \mathbb{Z} \times \mathbb{Z}$. Prove that $\langle (m, n) \rangle \cong \langle d \rangle$ if and only if $d = \gcd(m, n)$.

(14) Let $m, n \in \mathbb{Z}$. Prove that $\langle m \rangle \cap \langle n \rangle \cong \langle l \rangle$ if and only if $d = \text{lcm}(m, n)$.

The following exercises will require this definition:

Definition 112. An ***automorphism*** of a group G is an isomorphism with itself. △

(15) Prove that complex conjugation is an automorphism of the additive group of complex numbers; that is, show that the map $\phi(a + bi) = a - bi$ is an isomorphism from $\mathbb{C}$ to $\mathbb{C}$.

(16) Prove that $a + ib \mapsto a - ib$ is an automorphism of $\mathbb{C}^*$.

(17) Prove that $A \mapsto B^{-1}AB$ is an automorphism of $SL_2(\mathbb{R})$ for all B in $GL_2(\mathbb{R})$.

(18) We will denote the set of all automorphisms of G by $Aut(G)$. Prove that $Aut(G)$ is a subgroup of S_G, the group of permutations of G.

(19) Find $Aut(\mathbb{Z}_6)$.

(20) Find $Aut(\mathbb{Z})$.

(21) Find two nonisomorphic groups G and H such that $Aut(G) \cong Aut(H)$.

(22) (a) Let G be a group and $g \in G$. Define a map $i_g : G \to G$ by $i_g(x) = gxg^{-1}$. Prove that i_g defines an automorphism of G. Such an automorphism is called an ***inner automorphism***.

(b) The set of all inner automorphisms is denoted by $Inn(G)$. Prove that $Inn(G)$ is a subgroup of $Aut(G)$.

(c) What are the inner automorphisms of the quaternion group Q_8? Is $Inn(G) = Aut(G)$ in this case?

(23) Let G be a group and $g \in G$. Define maps $\sigma_g : G \to G$ and $\tau_g : G \to G$ by $\sigma_g(x) = gx$ and $\tau_g(x) = xg^{-1}$. Show that $i_g := \tau_g \circ \sigma_g$ is an automorphism of G.

16

Homomorphisms of Groups

In this chapter we will introduce homomorphisms, which are a powerful tool in the study of the structure of abstract groups. Our brief treatment only gives the reader a taste of this important topic, and the reader wanting to go deeper is encouraged to look at other algebra texts.[1]

16.1 Preliminary examples

In the previous chapter we talked about isomorphisms, which are bijections between two groups that also preserve the group operation. We've seen that isomorphic groups are essentially the "same" group (thinking groupwise).

For instance, we saw that the integers mod 4 and the 4^{th} roots of unity were isomporphic ($\mathbb{Z}_4 \cong \langle i \rangle$) by the following bijection (isomorphism):

$$0 \to 1, \quad 1 \to i, \quad 2 \to -1, \quad 3 \to -i.$$

The group operation is preserved by this bijection: for instance, $1 \oplus 2 = 3$ maps to $i \cdot -1 = -i$. In general, for $a, b \in \mathbb{Z}_4$ we have

$$f(a \oplus b) = f(a) \cdot f(b).$$

Now let us think about the groups $\mathbb{Z}_8$ and $\langle i \rangle$. Do they have the same relationship? Are they isomorphic?

Well, there is *one* immediate problem that comes up: $|\mathbb{Z}_8| \neq |\langle i \rangle|$. And as we saw in the Isomorphism chapter, there's no way then to create a bijection from $\mathbb{Z}_8$ to $\langle i \rangle$: specifically, there is just no way to create a one-to-one function from a

[1] Thanks to Tom Judson for material used in this chapter.

domain of 8 elements to a codomain of 4 elements; the number of elements have to match. But, let's look at their Cayley tables:

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Table 16.1: Addition table for $\mathbb{Z}_8$

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Table 16.2: Cayley table for $\langle i \rangle$

While we can't say that $\mathbb{Z}_8$ and $\langle i \rangle$ are isomorphic, there are some similarities in the patterns of their Cayley tables. Notice for instance the pattern of 2's in the upper left portion of the $\mathbb{Z}_8$ table. This matches exactly with the pattern of -1's in the $\langle i \rangle$ table. In fact, we can see that in both tables the entries in each "anti-diagonal" are all the same. This similarity in structure suggests a similarity in the behavior of the group operations. So although we can't create a bijection, could we possibly create another function that preserves the group operations?

Example 1. Let's try to create a function from $\mathbb{Z}_8$ to $\langle i \rangle$ which preserves group operations. Since there are twice as many elements in $\mathbb{Z}_8$ as in $\langle i \rangle$, it seems natural that 2 elements from $\mathbb{Z}_8$ should each go to one element in $\langle i \rangle$. The question then is, Which two? Because of the nature of modular addition, it makes some sense to pick elements of $\mathbb{Z}_8$ that are spaced evenly thoughout $\mathbb{Z}_8$ if we want them to correspond to the same action in $\langle i \rangle$. So let's look at the function $g : \mathbb{Z}_8 \to \langle i \rangle$ that takes

$$0, 4 \xrightarrow{g} 1, \quad 1, 5 \xrightarrow{g} i, \quad 2, 6 \xrightarrow{g} -1, \quad 3, 7 \xrightarrow{g} -i,$$

as shown in Figure 16.1.

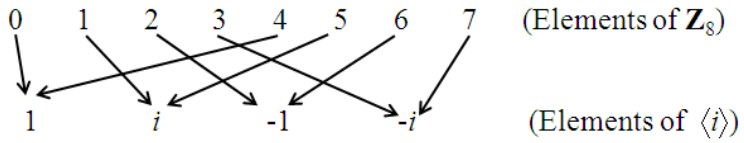


Figure 16.1. Function g between $\mathbb{Z}_8$ and $\langle i \rangle$.

Let's take the $\mathbb{Z}_8$ table then and start transforming it according to g. First we replace all the elements of $\mathbb{Z}_8$ with their counterparts in $\langle i \rangle$:

$\oplus$	1	i	-1	$-i$	1	i	-1	$-i$
1	1	i	-1	$-i$	1	i	-1	$-i$
i	i	-1	$-i$	1	i	-1	$-i$	1
-1	-1	$-i$	1	i	-1	$-i$	1	i
$-i$	$-i$	1	i	-1	$-i$	1	i	-1
1	1	i	-1	$-i$	1	i	-1	$-i$
i	i	-1	$-i$	1	i	-1	$-i$	1
-1	-1	$-i$	1	i	-1	$-i$	1	i
$-i$	$-i$	1	i	-1	$-i$	1	i	-1

Table 16.3: First Transformation of $\mathbb{Z}_8$ into $\langle i \rangle$.

Then we remove redundant rows/columns and change the group operation, and voila:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Table 16.4: Second Transformation of $\mathbb{Z}_8$ into $\langle i \rangle$.

This is exactly the Cayley table for $\langle i \rangle$ (see Table 16.2). So g does it! It preserves the group operations: if we take any two elements of $\mathbb{Z}_8$ and add them (say $3 \oplus 5 = 0$), the result is the same as taking their corresponding elements in $\langle i \rangle$ and multiplying them ($-i \cdot i = 1$). In other words, for all $a, b \in \mathbb{Z}_8$,

$$g(a \oplus b) = g(a) \cdot g(b).$$

A bijection that preserved group operations was called an isomorphism. So what do we call g? We say that g is a *homomorphism* from $\mathbb{Z}_8$ to $\langle i \rangle$, and that $\mathbb{Z}_8$ is *homomorphic* to $\langle i \rangle$. ♦

Remark 2. Notice a couple of things about Example 1:

(1) The identity of $\langle i \rangle$ is 1, and the elements in $\mathbb{Z}_8$ that map to 1 are 0 and 4. The set $\{0, 4\}$ is a subgroup of $\mathbb{Z}_8$, as is $\{1\}$ in $\langle i \rangle$.

Exercise 3.

(a) Show that the sets $\{0, 4\}$ and $\{1\}$ are subgroups of $\mathbb{Z}_8$ and $\langle i \rangle$, respectively.

(b) On the other hand, show that the sets $\{1, 5\}, \{2, 6\}$, and $\{3, 7\}$ are not subgroups of $\mathbb{Z}_8$.

◊

(2) However, $\{1, 5\}, \{2, 6\}$, and $\{3, 7\}$ are in fact the cosets of $\{0, 4\}$ in $\mathbb{Z}_8$, and $\{0, 4\}$ is actually a normal subgroup of $\mathbb{Z}_8$.

Exercise 4. Show that the left and right cosets of $\{0, 4\}$ in $\mathbb{Z}_8$ are in fact equal (and so now $\{0, 4\}$ is a *normal* subgroup of $\mathbb{Z}_8$). ◊

(3) So here's the good part: according to the Cosets chapter, since$\{0, 4\}$ is a normal subgroup, the set of its cosets is *itself* a group, namely the factor group $\mathbb{Z}_8/\{0, 4\}$. Let's look at the Cayley table for $\mathbb{Z}_8/\{0, 4\}$:

$\oplus$	$\{0,4\}$	$\{1,5\}$	$\{2,6\}$	$\{3,7\}$
$\{0,4\}$	$\{0,4\}$	$\{1,5\}$	$\{2,6\}$	$\{3,7\}$
$\{1,5\}$	$\{1,5\}$	$\{2,6\}$	$\{3,7\}$	$\{0,4\}$
$\{2,6\}$	$\{2,6\}$	$\{3,7\}$	$\{0,4\}$	$\{1,5\}$
$\{3,7\}$	$\{3,7\}$	$\{0,4\}$	$\{1,5\}$	$\{2,6\}$

Table 16.5: Cayley table for $\mathbb{Z}_8/\{0, 4\}$

Exercise 5. Verify all the calculations of the Cayley table for $\mathbb{Z}_8/\{0, 4\}$. ◊

Notice that Table 16.5 looks *eerily* similar to the Cayley Table for $\langle i \rangle$, reprinted below:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Table 16.6: Cayley table for $\langle i \rangle$

In fact:

Exercise 6. Show that the function $h : \mathbb{Z}_8/\{0,4\} \longrightarrow \langle i \rangle$ is an isomorphism, where

$$\{0,4\} \xrightarrow{h} 1, \quad \{1,5\} \xrightarrow{h} i, \quad \{2,6\} \xrightarrow{h} -1, \quad \{3,7\} \xrightarrow{h} -i.$$

$\Diamond$

So $\mathbb{Z}_8/\{0,4\} \cong \langle i \rangle$! (See Figure 16.2.)

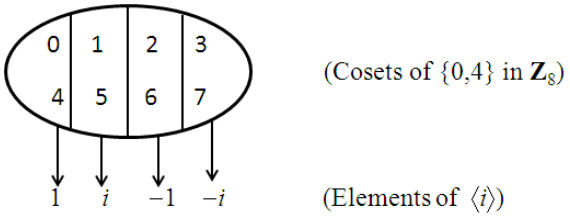


Figure 16.2. Isomorphism h between $\mathbb{Z}_8/\{0,4\}$ and $\langle i \rangle$.

$\triangle$

Remark 2 lists a number of interesting properties of Example 1. But these properties may or may not be true for *all* homomorphisms. To determine which properties are in fact general, we should look at some more examples. In the following sections we will then formalize our observations and provide proofs.

Example 7. The function g which we constructed in Example 1 was not one-to-one, but it was onto. Is "onto" necessary? Or could we possibly find a function from $\mathbb{Z}_8$ to $\langle i \rangle$ that still preserves the group operation, whose range is not all of $\langle i \rangle$?

Let's consider the function $q : \mathbb{Z}_8 \longrightarrow \langle i \rangle$ defined by:

$$0, 2, 4, 6 \xrightarrow{q} 1, \quad 1, 3, 5, 7 \xrightarrow{q} -1.$$

Exercise 8. Prove that $\{1, -1\}$ is a subgroup of $\langle i \rangle$. ◊

If we relabel the Cayley table for $\mathbb{Z}_8$ according to 1, we get the following:

·	1	-1	1	-1	1	-1	1	-1
1	1	-1	1	-1	1	-1	1	-1
-1	-1	1	-1	1	-1	1	-1	1
1	1	-1	1	-1	1	-1	1	-1
-1	-1	1	-1	1	-1	1	-1	1
1	1	-1	1	-1	1	-1	1	-1
-1	-1	1	-1	1	-1	1	-1	1
1	1	-1	1	-1	1	-1	1	-1
-1	-1	1	-1	1	-1	1	-1	1

Table 16.7: First Transformation of $\mathbb{Z}_8$ into $\{1, -1\}$.

And then if we remove the redundant rows and columns, we get:

·	1	-1
1	1	-1
-1	-1	1

Table 16.8: Second Transformation of $\mathbb{Z}_8$ into $\{1, -1\}$.

Now this isn't the *whole* Cayley table for $\langle i \rangle$ (Table 16.6), but it *is* the part of the Cayley table that corresponds to the elements 1 and -1 (remove rows 2 and 4 as well as columns 2 and 4). So q preserves the operations between $\mathbb{Z}_8$ and $\langle i \rangle$, since for all $a, b \in \mathbb{Z}_8$ whe have

$$q(a \oplus b) = q(a) \cdot q(b).$$

In other words, q is a homomorphism. ♦

Remark 9. Notice that as in Remark 2 we still have:

(1) The set $\{0, 2, 4, 6\} \subset \mathbb{Z}_8$ which maps to the identity of $\langle i \rangle$ is a subgroup of $\mathbb{Z}_8$. On the other hand, the set $\{1, 3, 5, 7\}$ which maps to -1 is not a subgroup.

(2) However, $\{1, 3, 5, 7\}$ is a coset of $\{0, 2, 4, 6\}$ in $\mathbb{Z}_8$, and $\{0, 2, 4, 6\}$ is a normal subgroup of $\mathbb{Z}_8$.

(3) Finally, as in Point (3) of Remark 2 we may use q to construct an isomorphism, as you will show in the following exercise.

Exercise 10.

(a) Create the Cayley Table for the Factor Group $\mathbb{Z}_8/\{0,2,4,6\}$.

(b) Show that the function from $\mathbb{Z}_8/\{0,2,4,6\}$ to $\langle i \rangle$ which maps

$$0,2,4,6 \longrightarrow 1, \quad 1,3,5,7 \longrightarrow -1$$

is an isomorphism from $\mathbb{Z}_8/\{0,2,4,6\}$ to the subgroup $\{1,-1\}$ of $\langle i \rangle$.

$\Diamond$

$\triangle$

16.2 Definition and several more examples

In the previous section we saw that homomorphisms give us a way of finding structural similarity between groups, even when those groups are not isomorphic. A homomorphism only needs to map elements from one group to another in such a way that it preserves the operations between the two groups. That's it. Unlike isomorphisms, it doesn't have to be one-to-one or onto.

Let's now formally state the definition:

Definition 11. A ***homomorphism*** between groups $(G,\cdot)$ and $(H,\circ)$ is a function $f : G \to H$ such that

$$f(g_1 \cdot g_2) = f(g_1) \circ f(g_2)$$

for all $g_1, g_2 \in G$. The range of f in H is called the ***homomorphic image*** of f. [2]

$\triangle$

Exercise 12.

(a) For the homomorphism g from $\mathbb{Z}_8$ to $\langle i \rangle$ in Example 1, what is the homomorphic image of g?

(b) For the homomorphism q from $\mathbb{Z}_8$ to $\langle i \rangle$ in Example 7, what is the homomorphic image of q?

[2] You may have noticed that in the Isomorphisms chapter we used greek letters (ϕ etc.) for isomorphisms, whereas here we're using regular letters for homomorphisms. There is no special reason for this (actually, it's because two different people wrote the two chapters). You should be comfortable either way.

♢

All of our examples so far have been with finite groups; let's look at infinite groups instead. As we saw in the Isomorphisms chapter, with finite groups we can use Cayley tables to verify the equality of the group operations, but with infinite groups we don't have Cayley tables, so we need to use the definition of a homomorphism.

Example 13. Recall that the circle group $\mathbb{T}$ consists of all complex numbers z such that $|z| = 1$. So geometrically, the circle group consists of the complex numbers that trace out a circle of radius 1 about the orgin in the complex plane (hence the name), as shown in the figure below:

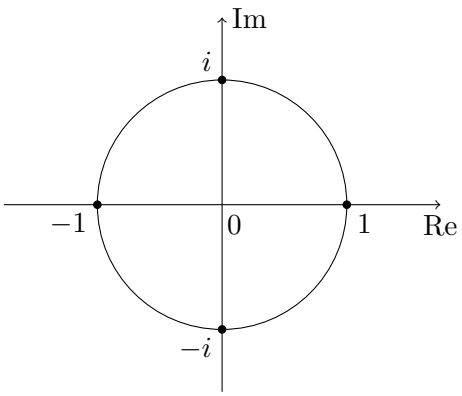


Figure 16.3. Circle group $\mathbb{T}$ in complex plane

Now imagine wrapping the real number line around this circle like it was a tape measure, with 0 on the real number line corresponding to 1 on the unit circle. Then we would have a correspondence between each real number and a complex number in $\mathbb{T}$. Every 2π units the real numbers start around the circle again, so that an infinite set of real numbers corresponds to each complex number z in $\mathbb{T}$. For instance not only 0, but $2\pi, 4\pi, 6\pi$, etc. would correspond to 1. Evidently for a given complex number z, any real number α that corresponds to z is an *argument* for z (see Figure 3.4), so that $z = \operatorname{cis}\alpha$. From this point of view, we may conceive of cis as a function from $\mathbb{R}$ to $\mathbb{T}$. Does cis preserve the operations between $\mathbb{R}$ and $\mathbb{T}$? We've shown this before in Proposition 53 in the Complex Numbers chapter,

but it won't hurt to see it again:

$$\begin{aligned}\operatorname{cis}(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta)\\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)\\ &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)\\ &= \operatorname{cis}(\alpha)\operatorname{cis}(\beta).\end{aligned}$$

So we have it; cis is a homomorphism from the additive group of real numbers to the circle group. This means that in some sense, complex multiplication on the unit circle is like addition of real numbers. ♦

In the following exercise, we relate the previous example to the properties listed in Remarks 2 and 9 in the previous section.

Exercise 14. As we mentioned above, cis maps $0, 2\pi, 4\pi$, etc to 1, the identity, in $\mathbb{T}$. In other words,

$$\operatorname{cis}(\{\ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \ldots\}) = 1$$

or

$$\operatorname{cis}^{-1}(1) = \{\ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \ldots\}.$$

(a) Prove that $\{\ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \ldots\}$ is a subgroup of $\mathbb{R}$

(b) What are the cosets of $\{\ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \ldots\}$ in $\mathbb{R}$?

(c) Which of these cosets are subgroups in $\mathbb{R}$?

(d) Prove then that $\{\ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \ldots\}$ $(2\pi\mathbb{R})$ is a normal subgroup of $\mathbb{R}$.

(e) Prove then that the factor group $\mathbb{R}/2\pi\mathbb{R}$ is isomorphic to $\mathbb{T}$.

(f) What is the homomorphic image of cis?

◊

Example 15. The circle group $\mathbb{T}$ also gives us a completely different way of constructing a homomorphism between complex and real numbers. Every complex number in $\mathbb{T}$ has modulus 1; i.e. they lie all on a circle of radius 1 in the complex plane. If we increase radius of the circle to 2, all of those complex numbers have the same modulus 2. In fact if you keep increasing or decreasing the radius of the circle, you can catch all the complex numbers in the plane with the concentric circles you've created. So every complex number (except 0) corresponds to a positive real number by its modulus. Since we can represent any complex number as $r\operatorname{cis}\theta$, we can define a function $f : \mathbb{C}^* \mapsto \mathbb{R}^*$ by

$$f(r \operatorname{cis} \theta) = r.$$

Let's see whether f is a homomorphism. If $r_1 \operatorname{cis} \theta_1$ and $r_2 \operatorname{cis} \theta_2$ are arbitrary nonzero complex numbers, we have:

$$\begin{aligned} f((r_1 \operatorname{cis} \theta_1) \cdot (r_2 \operatorname{cis} \theta_2)) &= f(r_1 \operatorname{cis} \theta_1 r_2 \operatorname{cis} \theta_2) \\ &= f((r_1 r_2) \operatorname{cis}(\theta_1 + \theta_2)) \\ &= r_1 r_2 \\ &= f((r_1 \operatorname{cis} \theta_1) \cdot f(r_2 \operatorname{cis} \theta_2)). \end{aligned}$$

So f is indeed a homomorphism from $\mathbb{C}^*$ to $\mathbb{R}^*$. ♦

Once again, we may compare this example to the remarks of the previous section.

Exercise 16.

(a) What is the homomorphic image of f?

(b) Find all the elements in $\mathbb{C}^*$ that map to the identity in $\mathbb{R}^*$; that is, find all $r \operatorname{cis} \theta \in \mathbb{C}^*$ such that $f(r \operatorname{cis} \theta) = 1$.

(c) Is the set from part (b) a subgroup of $\mathbb{C}^*$? Prove or disprove.

(d) What are the cosets in $\mathbb{C}^*$ of the set in part (b)?

(e) Which of the cosets from part (d) are subgroups of $\mathbb{C}^*$?

(f) Show the set in part (b) is a normal subgroup in $\mathbb{C}^*$.

(g) Define the factor group created by the normal subgroup in (f), and prove that it's isomorphic to $\mathbb{R}^*$.

◊

Now it's your turn. In the following exercises, you'll have a chance to verify some homomorphisms for yourself.

Exercise 17. Consider the group $GL_2(\mathbb{R})$ (that is, the group of invertible 2×2 matrices under matrix multiplication). If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $GL_2(\mathbb{R})$, then the determinant is nonzero; that is, $\det(A) = ad - bc \neq 0$.

(a) Prove that $\det(AB) = \det(A) \det(B)$ for $A, B \in GL_2(\mathbb{R})$. This shows that the function det is a homomorphism from $GL_2(\mathbb{R})$ to $\mathbb{R}^*$.

(b) What is the homomorphic image of det?

(c) In the Groups chapter we defined $SL_2(\mathbb{R})$ as the set of 2×2 real matrices whose determinant is 1. It follows that $SL_2(\mathbb{R})$ is the subset of $GL_2(\mathbb{R})$ which maps under det to the identity of $\mathbb{R}^*$. Prove that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

(d) Describe the cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$.

(e) Prove that $SL_2(\mathbb{R})$ is a normal subgroup of $GL_2(\mathbb{R})$. (*Hint*)

(f) Prove that the factor group $GL_2(\mathbb{R})/SL_2(\mathbb{R})$ is isomorphic to $\mathbb{R}^*$.

$\Diamond$

Remark 18. This last exercise wasn't as easy to visualize as the previous ones. So we had to rely on *properties* rather than intuition. This is typically what happens in mathematics: you start with visualizable examples, and use these as a springboard to leap into higher abstractions. $\triangle$

Exercise 19. Define a function $g : \mathbb{R} \to GL_2(\mathbb{R}$ as follows:

$$g(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}.$$

Prove that g is a homomorphism. $\Diamond$

Exercise 20. Remember that $\mathbb{M}_2(\mathbb{R})$ is the group of real-valued 2×2 matrices under addition. Define and prove a homomorphism from $\mathbb{M}_2(\mathbb{R})$ to $\mathbb{R}$. $\Diamond$

Now lets deal with homomorphisms in a more general context, to prepare us for the task of proving properties of homomorphisms in general (which we'll get to in the next section).

Example 21. Let G be a group and $g \in G$. In the Groups chapter we saw that the set of all integer powers (positive, negative, and zero) of g form a group, which is called the *cyclic subgroup* generated by g and is denoted by $\langle g \rangle$. Since each integer corresponds to a power of g, we may define a map $f : \mathbb{Z} \to G$ by $f(n) = g^n$. Then f is a group homomorphism, since

$$f(m+n) = g^{m+n} = g^m g^n = f(m)f(n).$$

This homomorphism maps $\mathbb{Z}$ onto $\langle g \rangle$. $\blacklozenge$

Exercise 22. If G is an abelian group and $n \in \mathbb{N}$, show that $\phi : G \to G$ defined by $\phi(g) = g^n$ is a group homomorphism. $\Diamond$

Finally, let's look at one more pattern for the homomorphisms we've developed so far before we go proving these patterns/properties hold for homomorphisms of groups in general:

Exercise 23.

(a) In $\mathbb{Z}_8$, $3^{-1} = 5$. Using the homomorphism g from Example 1, what is $g(3^{-1})$? What is $[g(3)]^{-1}$? Do the inverses match?

(b) In $\mathbb{Z}_8$, $2^{-1} = 6$. Using the homomorphism q from Example 7, what is $q(2^{-1})$? What is $[q(2)]^{-1}$? Do the inverses match?

(c) In $\mathbb{C}^*$, $(r\,\mathrm{cis}\,\theta)^{-1} = \frac{1}{r}\,\mathrm{cis}(2\pi - \theta)$. Using f from Example 15, does $f\left((r\,\mathrm{cis}\,\theta)^{-1}\right) = [f(r\,\mathrm{cis}\,\theta)]^{-1}$? Verify it if it's true, and give a counterexample if it's false.

(d) In $GL_2(\mathbb{R})$, what is the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$? Using f from Exercise 17, does $f\left(\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)^{-1}\right) = [f(\begin{pmatrix} a & b \\ c & d \end{pmatrix})]^{-1}$? Verify or give a counterexample.

(e) What general property of homomorphisms can you infer from these examples? (You don't need to give a proof if you don't want to.)

$\Diamond$

16.3 Proofs of homomorphism properties

So it seems there are several properties of homomorphisms that have consistently held true in our examples so far. For any homomorphism f with domain G and the codomain H, it seems that:

- The elements in G that map under f to the identity of H are in fact a normal subgroup of G.
- The factor group created by that normal subgroup is then isomorphic to the image of the homomorphism.
- If f maps g to h, then f also maps g^{-1} to h^{-1}.

These properties are indeed true for all homomorphisms, and we'll take the next two sections to prove these as well as other properties of homomorphisms. We begin with

Proposition 24. Let $f : G \to H$ be a homomorphism of groups. Then

1. If e is the identity of G, then $f(e)$ is the identity of H;

2. For any element $g \in G$, $f(g^{-1}) = [f(g)]^{-1}$;
3. If S is a subgroup of G, then $f(S)$ is a subgroup of H;
4. If T is a subgroup of H, then $f^{-1}(T) = \{g \in G : f(g) \in T\}$ is a subgroup of G. Furthermore, if T is normal in H, then $f^{-1}(T)$ is normal in G.

PROOF.

(1) Suppose that e and e' are the identities of G and H, respectively. Then

$$e'f(e) = f(e) = f(ee) = f(e)f(e).$$

By cancellation, $f(e) = e'$.

(2) This statement follows from the fact that

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

(3) The set $f(S)$ is nonempty since the identity of T is in $f(S)$. Suppose that S is a subgroup of G and let x and y be in $f(S)$. There exist elements $a, b \in S$ such that $f(a) = x$ and $f(b) = y$. Since

$$xy = f(a)f(b) = f(ab) \in f(S),$$

and

$$x^{-1} = f(a)^{-1} = f(a^{-1}) \in f(S),$$

it follows that $f(S)$ is a subgroup of H (since it is closed under the group operation and inverse).

(4) Let T be a subgroup of H and define S to be $f^{-1}(T)$; that is, S is the set of all $g \in G$ such that $f(g) \in T$. The identity is in S since $f(e) = e$. If a and b are in S, then $f(ab^{-1}) = f(a)[f(b)]^{-1}$ is in T since T is a subgroup of H. Therefore, $ab^{-1} \in S$ and S is a subgroup of G. If T is normal in H, we must show that $g^{-1}hg \in S$ for $h \in S$ and $g \in G_1$. But

$$f(g^{-1}hg) = [f(g)]^{-1}f(h)f(g) \in T,$$

since T is a normal subgroup of H. Therefore, $g^{-1}hg \in S$. □

Now that we have these properties down, we can use them to prove some other properties of homomorphisms. We know that homomorphisms preserve group operations, which suggests that homomorphisms may preserve other group properties as well. We'll look at two group properties in the next exercise.

Exercise 25. Prove the following:

(a) If $f : G \to H$ is a group homomorphism and G is abelian, prove that $f(G)$ is also abelian.

(b) If $f : G \to H$ is a group homomorphism and G is cyclic, prove that $f(G)$ is also cyclic.

$\Diamond$

One of the patterns we saw in our examples that we haven't verified yet was that the elements in G that map to the identity of H formed a normal subgroup in G. We can now prove this in general, but first a definition:

Definition 26. Let $f : G \to H$ be a homomorphism and suppose that e' is the identity of H. The set $f^{-1}(\{e\})$ is called the ***kernel*** of f, and will be denoted by $\ker f$. $\triangle$

Proposition 27. Let $f : G \to H$ be a group homomorphism. Then the kernel of f is a normal subgroup of G.

Exercise 28. Prove Proposition 27. (*Hint*) $\Diamond$

Exercise 29. What were the kernels of the homomorphisms in:

(a) Example 1

(b) Example 7

(c) Example 13

(d) Example 15

(e) Exercise 17

$\Diamond$

Exercise 30. Which of the following functions are homomorphisms? If the map is a homomorphism, what is the kernel?

1. $f : \mathbb{R} \to GL_2(\mathbb{R})$ defined by
$$f(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$
2. $f : GL_2(\mathbb{R}) \to \mathbb{R}$ defined by
$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d$$

3. $f : \mathbb{M}_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = b,$$

where $\mathbb{M}_2(\mathbb{R})$ is the additive group of 2×2 matrices with entries in $\mathbb{R}$.

$\Diamond$

Exercise 31. Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(n) = 7n$. Prove that f is a group homomorphism. Find the kernel and the image of f. $\Diamond$

Example 32. Suppose that we wish to determine all possible homomorphisms f from $\mathbb{Z}_7$ to $\mathbb{Z}_{12}$. Since the kernel of f must be a subgroup of $\mathbb{Z}_7$, there are only two possible kernels, $\{0\}$ and all of $\mathbb{Z}_7$. The image of a subgroup of $\mathbb{Z}_7$ must be a subgroup of $\mathbb{Z}_{12}$. Hence, there is no injective homomorphism; otherwise, $\mathbb{Z}_{12}$ would have a subgroup of order 7, which is impossible. Consequently, the only possible homomorphism from $\mathbb{Z}_7$ to $\mathbb{Z}_{12}$ is the one mapping all elements to zero. $\blacklozenge$

Exercise 33. Describe all of the homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$. $\Diamond$

Exercise 34. Describe all of the homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_{12}$. $\Diamond$

Exercise 35. Find all of the homomorphisms $f : \mathbb{Z} \to \mathbb{Z}$. Which of these are isomorphisms? (*Hint*) $\Diamond$

16.4 The First Isomorphism Theorem

There's one property that we observed in earlier sections of this chapter that we haven't proven so far, namely, the factor group created by the kernel of a homomorphism is isomorphic to the image of the homomorphism. In order to do this, we'll need a clearer idea of how homomorphisms actually work. Figure 16.4 gives a schematic diagram of a general homomorphism f with kernel K.

The figure shows the cosets of K, which form a partition of G as we showed in the Cosets chapter. These cosets can be thought of as elements of the factor group G/K.

The arrangement of arrows in the figure indicate that any two points in the same coset gK map to the same element of H. This is true because

$$f(gk) = f(g)f(k) = f(g)e' = f(g) \qquad \text{(given that } g \in G, k \in K\text{)}.$$

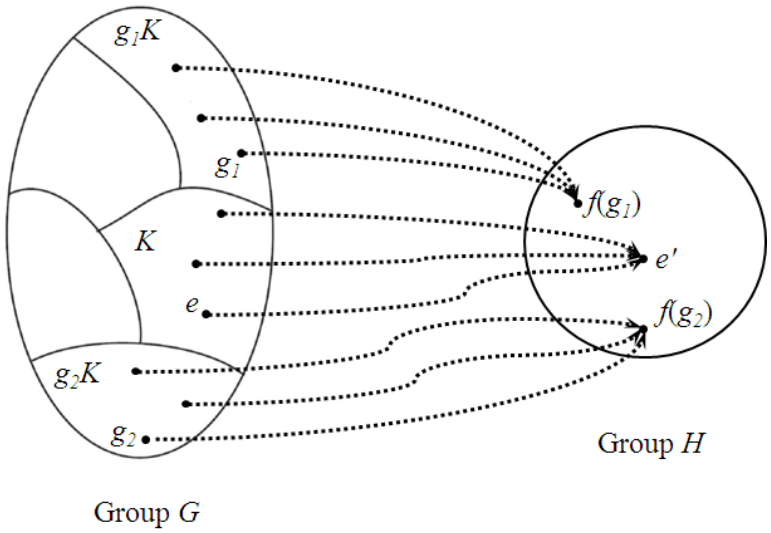


Figure 16.4. Homomorphism $f : G \to H$ with kernel K.

This implies that we can actually define a function F from G/K to H as follows:

$$F(gK) = f(g).$$

The function is well-defined because if $g'K = gK$ then $F(g'K) = f(g') = f(g) = F(gK)$.

So what's the point? It turns out that this function F is exactly the isomorphism that we're looking for. We've already shown that it's well-defined: all that's left is to show that it's one-to-one and onto, and that it preserves the operation. We state these results as a proposition.

Proposition 36. (*First Isomorphism Theorem* If $f : G \to H$ is a homomorphism with $K = \ker f$. Let the function $F : G/K \to f(G)$ be defined according to $F(gK) = f(g)$. Then F is an isomorphism.

PROOF. As mentioned above, we only need to show that F is 1-1, onto, and preserves the operation.

- 1-1: Suppose that $F(g_1K) = F(g_2K)$. Then according to the definition of F, this means that $f(g_1) = f(g_2)$. From this we obtain (using the homomorphism property of f):

  $$f(g_1^{-1}g_2)) = f(g_1^{-1})f(g_2) = f(g_1)^{-1}f(g_2) = f(g_1)^{-1}f(g_1) = e' \Rightarrow g_1^{-1}g_2 \in K.$$

  By Proposition 10 in the Cosets chapter (parts (1) and (2)), this implies that $g_1K = g_2K$.

- Onto: Let h be an arbitrary element of $f(G)$. Then there exists $g \in G$ such that $f(g) = h$. By the definition of F, we have also that $F(gK) = h$.
- Preserves operations: Using properties of normal subgroups, we have:

$$F(g_1Kg_2K) = F(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = F(g_1K)F(g_2K).$$

□

Example 37. Let G be a cyclic group with generator g. Define a map $f : \mathbb{Z} \to G$ by $n \mapsto g^n$. This map is a surjective homomorphism since

$$f(m+n) = g^{m+n} = g^m g^n = f(m)f(n).$$

Clearly f is onto. If $|g| = m$, then $g^m = e$. Hence, $\ker f = m\mathbb{Z}$ and $\mathbb{Z}/\ker f = \mathbb{Z}/m\mathbb{Z} \cong G$. On the other hand, if the order of g is infinite, then $\ker f = 0$ and ϕ is an isomorphism of G and $\mathbb{Z}$. Hence, two cyclic groups are isomorphic exactly when they have the same order. Up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}_n$. ♦

Additional Exercises

1. Let $f : G \to H$ be a homomorphism. Show that f is one-to-one if and only if $f^{-1}(e') = \{e\}$, where e and e' are the identities of G and H, respectively.
2. For $k \in \mathbb{Z}_n$, define a map $f_k : \mathbb{Z}_n \to \mathbb{Z}_n$ by $a \mapsto ka$. Prove that f_k is a homomorphism.
3. Show that a homomorphism defined on a cyclic group is completely determined by its action on the generator of the group. (*Hint*)
4. Prove or disprove: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$. (*Hint*)
5. Let G and H be groups, and let M and N be normal subgroups of G and H respectively. Let $f : G \to H$ be a homomorphism which satisfies $f(M) \subset N$. Show that f can be used to define a homomorphism $F : G/M \to H/N$.
6. Let $f : G \to H$ be a homomorphism that is onto. Let M be a normal subgroup of G and suppose that $f(M) = N$. Prove that $G/M \cong H/N$.

17

Sigma Notation

We are about to start looking at polynomials, which means we will be working with sums of terms – sometimes many terms. Such sums are often written using *Sigma notation*. It's possible that you are already a master of Sigma notation. If not, you can brush up with the material in this section. (At very least, you should try some of the exercises to make sure that you haven't gotten rusty!)[1]

17.1 Lots of examples

It's unavoidable that in mathematics, one often encounters sums. Sometimes these sums have very few terms, but occasionally the sums can reach hundreds, thousands or even an infinite number of terms. In these cases, rather than listing each and every term or listing the first several terms and assuming the pattern is obvious, one can represent a sum using *summation notation*, often referred to as *Sigma notation*.

Sigma notation has four main parts: the *index variable*, the *starting value*, the *final value* and the *formula*. These parts are illustrated in the following example.

Example 1. Consider:

$$\sum_{i=1}^{10}(i+2)$$

In this case, the Σ symbol lets us know that this is a sum. The $i = 1$ serves two functions. It tells us that the index variable is i, and that i has a starting value of 1. The 10 is the final value, and the $(i + 2)$ to the right of the Σ is the formula. The i in the formula, takes each integer value from the starting value (1) to the final value (10). Therefore we have:

$$\sum_{i=1}^{10}(i+2) = 3+4+5+6+7+8+9+10+11+12 = 75.$$

[1] This chapter was written by David Weathers and Johnny Watts (edited by CT).

♦

This notation has a lot of flexibility. For example, the sum's formula can be a constant value:

$$\sum_{i=1}^{10} 5 = 5+5+5+5+5+5+5+5+5+5 = 50.$$

Or we could have the index as an exponent: operator value

$$\sum_{i=1}^{10} (2^i) = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10}$$

Now all the examples so far have a numerical value that can be calculated. However, summation notation can also be used to express functions of variables such as:

$$\sum_{i=1}^{10} (x^i) = x^1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10}$$

Note that any variables in the formula that do not match the index are left as variables (such as x in the previous example). While we do not know what the sum value is other than in terms of x, we can much more concisely state the sum in Sigma notation.

Another typical use for the index in the formula is to denote an index in a coefficient. Consider the polynomial:

$$ax^2 + bx + c.$$

Instead of using a different letter, we can use a subscript to denote a different value but use the same letter:

$$a_2x^2 + a_1x + a_0.$$

And when we use subscripts, we can use the index in the formula to denote that subscript.

$$\sum_{i=0}^{2} a_i x^i$$

Changing the starting and/or final values does not affect the pattern of the formula, but it does change the number of terms and any index values used in that formula. Take one of the previous examples:

$$\sum_{i=1}^{10} i = 1+2+3+4+5+6+7+8+9+10$$

If we were to change the $i = 1$ to $i = 4$ then the sum would lose terms 1,2,3:

$$\sum_{i=4}^{10} i = 4 + 5 + 6 + 7 + 8 + 9 + 10$$

Likewise, if we were to also change the 10 to 6, it would lose the terms 10,9,8 and 7;

$$\sum_{i=4}^{6} i = 4 + 5 + 6.$$

Exercise 2. Evaluate the following:

(1) $\sum_{i=0}^{400} 2$

(2) $\sum_{j=17}^{20} \left(2j^2 - j\right)$

(3) $\sum_{k=0}^{4}(x^{2k} - k)$ (Your answer should be in terms of x).

(4) $\sum_{k=0}^{7}(-1)^k \frac{x^k}{(k+1)(k+2)}$ (Your answer should be in terms of x).

$\Diamond$

17.2 Sigma notation properties

As with any algebraic notation, there are rules that allow us to do algebraic manipulations with expressions that involve Sigma. Take for example:

$$\sum_{i=0}^{5} 2i$$

We know this is the Sigma notation for $2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + 2 \cdot 4 + 2 \cdot 5$. Using the distributive property of addition and multiplication of integers, we know this sum is the same as $2 \cdot (1 + 2 + 3 + 4 + 5)$. Now we convert the sum in the parenthesis to Sigma notation to yield

$$2 \cdot \sum_{i=0}^{5} i.$$

The same argument could be used for any sum multiplied by any constant. We can write this rule as:

$$\sum_{i=a}^{b} c \cdot d_i = c \cdot \sum_{i=a}^{b} d_i,$$

where c denotes an arbitrary constant and d_i represents the term of the sum corresponding to index i. Some additional sum rules:

$$\sum_{i=0}^{n}(x_i + y_i) = \sum_{i=0}^{n} x_i + \sum_{i=0}^{n} y_i$$

$$\sum_{i=0}^{n}(c \cdot x_i + d \cdot y_i) = c \cdot \sum_{i=0}^{n} x_i + d \cdot \sum_{i=0}^{n} y_i$$

It is also possible to shift the starting and final values without changing the value of the formula. Take the following sum:

$$\sum_{i=2}^{7}(i-1)$$

In this case, the sum is $1+2+3+4+5+6$, which can be represented as:

$$\sum_{i=1}^{6} i$$

A similar example is:

$$\sum_{i=2}^{4}(i+1)(i+2) = (2+1)(2+2) + (3+1)(3+2) + (4+1)(4+2) = 62$$

$$(3+0)(3+1) + (4+0)(4+1) + (5+0)(5+1) = \sum_{j=3}^{5} j(j+1).$$

Changing the starting and final values in this way can be thought of as a change of variable. For instance, in the previous example we had

$$\sum_{i=2}^{i=4}(i+1)(i+2).$$

Let $j = i+1$, and solve for i: $i = j-1$. We then replace all i's in the formula with $j-1$ to obtain

$$\sum_{(j-1)=2}^{(j-1)=4}((j-1)+1)((j-1)+2),$$

and after algebraic simplification we get

$$\sum_{j=3}^{5}(j)(j+1),$$

as before.

Occasionally, it may be necessary to add or remove a single term from the sum. This can be done by changing the start value or end condition. For example,

$$\sum_{i=1}^{10} i = 1 + \sum_{i=2}^{10} i = \sum_{i=1}^{9} i.$$

When removing a term from the middle, it may be necessary to split the sum into two separate sums.

$$\sum_{i=1}^{10} i = \sum_{i=1}^{3} i + 4 + \sum_{i=5}^{10} i.$$

Exercise 3. Take the following Sigma notation examples and change the formula and final value so that the starting value becomes 0 and the sum maintains the same value. Calculate the value of both the listed sum and the resulting sum to show that the value is the same.

(a) $\sum_{i=3}^{46} 2i$

(b) $\sum_{j=7}^{20} \cos(j\pi)$

(c) $\sum_{j=20}^{40} j - 20$

◊

Exercise 4. We have shown that a "sum rule" holds for sigma notation. Is there a corresponding "product rule"? That is: is it true that

$$\sum_{i=0}^{n} (x_i + y_i) \stackrel{?}{=} \sum_{i=0}^{n} x_i + \sum_{i=0}^{n} y_i$$

If true then prove it; if not, give a counterexample. ◊

17.3 Nested Sigmas

Since any pattern of sum can be replaced with Sigma notation, it is quite possible for one Sigma to end up inside another:

$$\sum_{i=0}^{3} \left(\sum_{j=0}^{2} (1) \right)$$

This means that for each value of the index of the outside Sigma, the entire sum of the inside Sigma must be calculated. In this case, $\sum_{j=0}^{2}(1) = 3$, so we have

$$\sum_{i=0}^{3}\left(\sum_{j=0}^{2}(1)\right) = \sum_{i=0}^{3}(3) = 3+3+3+3 = 12.$$

The situation becomes more interesting when the sum inside depends on the the index variable of the outside Sigma:

$$\sum_{i=0}^{3}\left(\sum_{j=0}^{i}(1)\right)$$

Unlike the previous case, the inside sum will change depending on what i is. When $i = 0$ then $\sum_{j=0}^{i}(1) = \sum_{j=0}^{0}(1) = 1$ so 1 would be the first term in the outside sum. When $i = 1$ then $\sum_{j=0}^{i}(1) = \sum_{j=0}^{1}(1) = 1+1 = 2$ so 2 would be the next term. With each successive term, the inside sum increases by 1, so the result is $1+2+3+4 = 10$.

Note that the index of the outer sum may appear in any or all parts of the inner sum. Here are some examples:

$$\sum_{i=0}^{3}\left(\sum_{j=i}^{10}(1)\right); \qquad \sum_{i=0}^{3}\left(\sum_{j=1}^{10}(i)\right); \qquad \sum_{i=0}^{3}\left(\sum_{j=i}^{2i}(3i+x^j)\right).$$

When using nested sums, it is possible to rearrange the order of summation. Take for example:

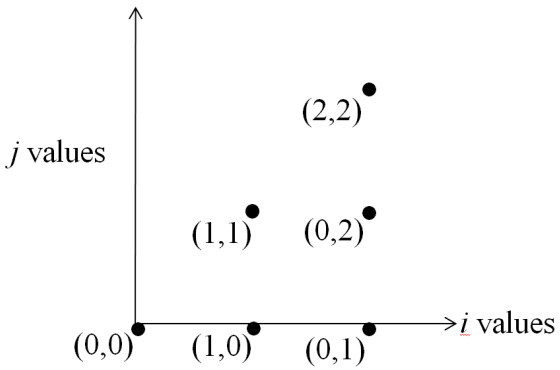
$$\sum_{i=0}^{2}\left(\sum_{j=0}^{i}(1)\right)$$

The first term has $i = 0$ and $j = 0$: we write this as $(i, j) = (0, 0)$. When $i = 1$, then we have two terms: $j = 0$ and $j = 1$. Finally, when $i = 2$, we have $j = 0, 1$, or 2. Altogether we have the index pairs: $(0,0), (1,0), (1,1), (2,0), (2,1), (2,2)$. These index pairs may be displayed on a grid, as shown in Figure 17.3.

Alternatively, we can arrange these index pairs by j coordinate. When j is 0, i takes the values (0,1,2), when j is 1, i takes the values of (1,2) and when j is 2 i takes the value 2. This can be expressed as the sum:

$$\sum_{j=0}^{2}(\sum_{i=j}^{2}(i))$$

So far our examples have only two Sigmas, but it's quite possible to have an unlimited number of nested Sigmas. Regardless of how many Sigmas, the process



of calculation is the same as above: start with the outermost sum, pick the starting value and work your way inward.

Exercise 5. For each of the following nested sums, swap the sum indices and change the start value and end condition so the nested sum maintains the same value.

(1) $\sum_{i=0}^{4}(\sum_{j=0}^{8}(i))$

(2) $\sum_{j=0}^{2}(\sum_{i=j}^{2j}(i+j))$

(3) $\sum_{k=0}^{17}(\sum_{i=0}^{2k}(2i+1))$

◊

17.4 Common Sums

There are several sums, even a few infinite sums, that the total value is known. One very basic example is:

$$\sum_{i=1}^{k} 1$$

The answer is NOT 1. (What is it?) Make sure you don't get tripped up by this one.

Another very useful example is:

$$\sum_{i=1}^{k} i = 1 + 2 + 3 \cdots + (k-1) + k$$

If one were to take the first term 1 and add it to the last term k, we get $k+1$. If we take the second term 2 and add to the second-to-last term $k-1$ again we get $k+1$. This is true for all terms in between. In the case of an even number of terms (such as $1+2+3+4$), the terms split evenly. In the case of an odd number of terms (such as $1+2+3+4+5+6+7$) we have 3 pairs that add to 8 but an additional term in the middle. In either case, we take the first term add to the last term and multiply that quantity by $1/2$ the number of terms. The formula is thus:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}.$$

We can use the same reasoning to arrive at the following formula.

$$\sum_{i=a}^{k} i = a + (a+1) + (a+2) \cdots + (k-1) + k = (k+a) * (k-a)/2,$$

where a and k are integers and $a < k$

Exercise 6.

(a) Write the sum of odd integers from $2a+1$ to $2k+1$ in Sigma notation.

(b) Give a formula for the sum that you wrote in (a). (Use the same reasoning that we used to find sums of consecutive integers.)

(c) Write the sum of even integers from $2a$ to $2k$ in Sigma notation.

(d) Give a formula for the sum that you wrote in (c).

(e) Write the sum of every 5^{th} integer from a to $a+5k$ in Sigma notation.

(f) Give a formula for the sum that you wrote in (e).

$\Diamond$

One infinite sum called the *geometric series*, and is defined as the sum of integer powers of a common base. For example, here is the geometric series when the base is $1/2$:

$$\sum_{i=0}^{\infty} (\frac{1}{2})^i = (\frac{1}{2})^0 + (\frac{1}{2})^1 + (\frac{1}{2})^2 \cdots = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} \cdots$$

As we add the terms of the sum together it becomes apparent that the total sum gets closer to 2, but never quite gets there. However if we add all the terms together, the sum approaches:

$$\frac{1}{1-\frac{1}{2}}.$$

More generally for any value $-1 < x < 1$ the series:

$$\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$$

We can easily prove this using some fairly simple algebra. Let S be the value of this sum. We can solve for S by writing:

$$S = 1 + x + x^2 + x^3 + \cdots$$

$$xS = x + x^2 + x^3 + x^4 + \cdots$$

Subtracting these two equations gives $S - xS = 1$, and solving for S gives:

$$s = \frac{1}{1-x}.$$

This same technique can be used to prove the formula for a geometric series with a finite number of terms:

$$\sum_{i=0}^{n-1} ar^i = a\frac{1-r^n}{1-r}$$

As before, we let S be the value of this sum. We then compute $S - rS$ (most terms in the sums cancel) and solve for S. See if you can do this for yourself. (It may be on the test!)

Other sums with known values include:

$$\sum_{i=0}^{\infty} \frac{x^i}{i!} = 1 + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} \cdots = e^x$$

$$\sum_{i=0}^{\infty} \frac{(-1)^i x^{2i+1}}{(2i+1)!} = \frac{x^1}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} \cdots = \sin(x)$$

There are also sums which *diverge*, that is, they can be shown to approach positive or negative infinity. Examples include:

$$\text{The harmonic series: } \sum_{i=0}^{\infty} \left(\frac{1}{i}\right)$$

$$\text{The geometric series when } |x| \geq 1: \quad \sum_{i=0}^{\infty} x^i.$$

17.5 Sigma notation in linear algebra

17.5.1 Applications to matrices

In the following discussions, we will assume that all matrices have real entries. However, all of the results that we will prove also apply (in some cases, with slight modifications) for matrices with *complex* entries, or even matrices with entries in $\mathbb{Z}_p$.

Matrix multiplication

It should come as no surprise that summation notation commonly shows up when working with matrices. In the following discussion, we will follow the common practice of denoting a matrix with a capital letter in italics, and the entries of the matrix with the same letter in lowercase. Thus for example, $a_{2,4}$ denotes the entry of matrix A in row 2, column 4.

Consider the example of multiplying the 3×3 matrix A and the 3×2 matrix B.

$$AB = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \\ b_{3,1} & b_{3,2} \end{pmatrix}$$

$$= \begin{pmatrix} a_{1,1}b_{1,1} + a_{1,2}b_{2,1} + a_{1,3}b_{3,1} & a_{1,1}b_{1,2} + a_{1,2}b_{2,2} + a_{1,3}b_{3,2} \\ a_{2,1}b_{1,1} + a_{2,2}b_{2,1} + a_{2,3}b_{3,1} & a_{2,1}b_{1,2} + a_{2,2}b_{2,2} + a_{2,3}b_{3,2} \\ a_{3,1}b_{1,1} + a_{3,2}b_{2,1} + a_{3,3}b_{3,1} & a_{3,1}b_{1,2} + a_{3,2}b_{2,2} + a_{3,3}b_{3,2} \end{pmatrix}$$

How great would it be if we shorten that mess? Fortunately we can! Let the matrix C be the product AB, where A is an $m \times n$ matrix and B is an $n \times p$ matrix [2], which implies that the dimensions of C will be $m \times p$. If the row number is given by the first index (in this case i), and the column number is given by the second index (in this case j), we can write the entries of C as:

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}$$

(what do you think the restrictions on i and j are?)

This may look a little confusing at first, but once you do a few examples it will start to make sense. Suppose A is a 3×3 matrix and B is a 3×2 matrix as in our previous example, then the result of the product AB is a 3×2 matrix we can call C. Now suppose we want to find the entry on the third row in the second column of C, then we would compute:

[2] Remember the requirement for multiplying any two matrices is that the number of columns of the first must match the number of rows of the second.

$$\begin{aligned} c_{3,2} =& \sum_{k=1}^{3} a_{3,k} b_{k,2} \\ =& a_{3,1} b_{1,2} + a_{3,2} b_{2,2} + a_{3,3} b_{3,2}. \end{aligned}$$

Sure enough, when we look at the long version we wrote earlier for the product AB our result matches the entry on the second row, third column.

Exercise 7. Given three matrices A, B, C with sizes $m \times n, n \times p, p \times q$ respectively.

(a) Let $D = BC$. Write a formula for the entries $d_{i,j}$ of D in terms of the entries of B and C ($b_{i,k}$ and $c_{k,j}$, respectively).

(b) Let $G = AD$. Write a formula for the entries $g_{\ell,j}$ of G in terms of the entries of A, B and C.

(c) Let $H = (AB)$, and let $M = HC$. Write a formula for the entries $m_{\ell,j}$ of M in terms of the entries of A, B and C.

(d) Show that matrix multiplication is *associative*.

$\Diamond$

The ***identity matrix*** I often comes up when working with matrices. You may remember that an identity matrix looks like:

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

There is a summation notation counterpart, called the ***Kronecker delta***.[3] The Kronecker delta is written as $\delta_{i,j}$, and it takes the following values:

$$\delta_{ij} = \begin{cases} 1 \text{ if } i = j, \\ 0 \text{ if } i \neq j. \end{cases}$$

Exercise 8.

[3] after Leopold Kronecker (1823-1891), a prominent German mathematician who made many contributions to abstract algebra and number theory. But outside of those areas, he is most famous for his strong opposition to the theory of infinite sets first proposed by Georg Cantor (1845-1918). Most mathematicians today would say that Cantor was right, and Kronecker was wrong. This is an interesting topic that you can read about.

(a) What is the relationship between δ_{ij} the entries of the identity matrix I?

(b) We know that if a matrix B is the inverse of the $n \times n$ matrix A then we have the equations: $BA = I$ and $AB = I$. Rewrite these matrix equations in summation notation, making use of the Kronecker delta δ_{ij}.

$\Diamond$

Exercise 9. Show that:

$$\sum_k \delta_{ik}\delta_{kj} = \delta_{ij}$$

$\Diamond$

Exercise 10. The Kronecker delta can also be use to write a compact, summation notation version of the definition for dot product. Guess what this formula is, and use it to find the dot product of the vectors $\mathbf{a} = [5 \ 1 \ -2]$ and $\mathbf{b} = [3 \ 2 \ -6]$. (*Hint*) $\Diamond$

Matrix transpose

Transpose is another operation on matrices that lends itself to summation notation. Recall that the transpose of a matrix changes the rows to columns,so that the first row becomes the first column, the second row becomes the second column, and so on. Using indices and recalling that first index is the row and the second is the column, we can state this as:

$$\left[A^{\mathrm{T}}\right]_{i,j} = a_{j,i}.$$

Now let's demonstrate the power of our new notation to prove one of the properties of transpose:

$$(AB)^{\mathrm{T}} = B^{\mathrm{T}}A^{\mathrm{T}}.$$

We'll prove this by expressing the (i, j) entry of the left-hand side in summation notation, doing some algebraic hocus-pocus, and showing that it agrees with the (i, j) entry of the right side. First we make things clear by specifying that A has n columns and B has n rows (these dimensions have to agree, or the product is not defined). This gives us

$$[AB]_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j}.$$

so the (i, j) entry of the left-hand side is:

$$\left[(AB)^T\right]_{i,j} = [AB]_{j,i} = \sum_{k=1}^{n} a_{j,k} b_{k,i}.$$

At this point we can introduce A and B transpose because the j, k entry of any matrix is the k, j entry of its transpose:

$$\sum_{k=1}^{n} a_{j,k} b_{k,i} = \sum_{k=1}^{n} \left[A^{\mathrm{T}}\right]_{k,j} \left[B^{\mathrm{T}}\right]_{i,k.}$$

Since the terms of A and B are being expressed as a summation, they commute (i.e. order doesn't matter), which allows us to say (using our definition of matrix product):

$$\sum_{k=1}^{n} \left[A^{\mathrm{T}}\right]_{k,j} \left[B^{\mathrm{T}}\right]_{i,k} = \sum_{k=1}^{n} \left[B^{\mathrm{T}}\right]_{i,k} \left[A^{\mathrm{T}}\right]_{k,j} = \left[B^{\mathrm{T}} A^{\mathrm{T}}\right]_{i,j},$$

Voila, we have the (i, j) entry of the right-hand side, and the proof is complete.

Exercise 11. Give a formula for $(ABC)^T$, and prove your formula using summation notation. ◊

Exercise 12. We know that the transpose of a $n \times n$ matrix is a $n \times n$ matrix. So we can consider transpose as a function from $GL_n(\mathbb{R})$ to $GL_n(\mathbb{R})$, where (as before) $GL_n(\mathbb{R})$ is the multiplicative group of $n \times n$ real invertible matrices. Prove or disprove the following:

(a) Transpose defines an invertible function from $GL_n(\mathbb{R})$ to $GL_n(\mathbb{R})$.

(b) Transpose defines an isomorphism from $GL_n(\mathbb{R})$ to $GL_n(\mathbb{R})$.

◊

Matrix traces

Another cool application of summation notation with matrices is to prove things about the ***trace*** of a matrix. The trace only applies to square matrices (equal number of rows and columns) and is the sum of all the entries on the diagonal – that is, the sum of all entries with the same column and row number. In summation notation, the trace of an $n \times n$ matrix as:

$$\mathrm{Tr}\,(A) = a_{1,1} + a_{2,2} + \ldots + a_{n,n} = \sum_{i=1}^{n} a_{i,i}$$

This time we are using the index i for both the row position and the column position, so its the position of the index that denotes row and column. The formula for the product used two different letters for the indices because they were not always equal, but for trace the row and column number will always be equal, so we only need one letter.

The next exercise covers some basic properties of traces:

Exercise 13.

(a) Prove that if A and B are square matrices of the same size, then $\mathrm{Tr}\,(A+B) = \mathrm{Tr}\,(A) + \mathrm{Tr}\,(B)$.

(b) Prove that if $A$is a square matrix with real entries and k is a real number, then $\mathrm{Tr}\,(kA) = k\mathrm{Tr}\,(A)$.

(c) Prove or disprove: trace defines an isomorphism between $\mathbb{M}_2$ (the additive group of 2×2 matrices with real entries) and $\mathbb{R}$.

(d) Prove or disprove: trace defines a homomorphsim from $\mathbb{M}_2$ to $\mathbb{R}$.

(e) Prove or disprove: trace defines a homomorphsim from $GL_2(\mathbb{R})$ (invertible 2×2 matrices under multiplication) to $\mathbb{R}$.

$\Diamond$

In the above exercise, we have considered the trace of the sum of two matrices. Now we consider the trace of the *product* of two matrices. To this end, let A and B be a $n \times n$ matrices. So first we have:

$$\mathrm{Tr}\,(AB) = \sum_{i=1}^{n} [AB]_{i,i} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{i,k}b_{k,i}.$$

All we've done here is take the matrix product formula, and set the second index of the second matrix entry equal to first index of the first matrix entry. Now to make things interesting, let's find the trace for the reverse order:

$$\mathrm{Tr}\,(BA) = \sum_{i=1}^{n} [BA]_{i,i} = \sum_{i=1}^{n}\sum_{k=1}^{n} b_{ik}a_{k,i}.$$

Let's play with this last equation a bit. Since the matrix entries commute, and also we can change the order of the summations without changing the result, it follows that we can do the following rearrangment:

$$\mathrm{Tr}\,(BA) = \sum_{i=1}^{n}\sum_{k=1}^{n} b_{ik}a_{k,i} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{k,i}b_{i,k} = \sum_{k=1}^{n}\sum_{i=1}^{n} a_{k,i}b_{i,k}.$$

Finally, we rename the indices by changing k to i and i to k. (Remember, it's the positions of the indices that are important, not the letters we call them by!) After renaming, we get:

$$\sum_{i=1}^{n}\sum_{k=1}^{n} a_{i,k}b_{k,i}$$

Which is exactly the same as the trace of AB.

Exercise 14. In the above proof that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, we assumed that both A and B were square matrices. Show that the formula is still true when A is a $m \times n$ matrix and B is a $n \times m$ matrix. (Notice that AB and BA are both square matrices, so that $\mathrm{Tr}\,(AB)$ and $\mathrm{Tr}\,(BA)$ are both well-defined.) ◊

Exercise 15. Show that $\mathrm{Tr}(ABC) = \mathrm{Tr}(CAB)$, as long as the dimensions of A, B, C are such that the products are well-defined. (*Hint*) ◊

Exercise 16. Show that

$$\mathrm{Tr}(ABCD) = \mathrm{Tr}(DABC) = \mathrm{Tr}(CDAB) = \mathrm{Tr}(BCDA),$$

as long as the matrices have dimensions so that all of these products are defined. Notice that all of these arrangements of the matrices A, B, C, D are *cyclic permutations* of each other. ◊

Exercise 17. In linear algebra, given two $n \times n$ matrices A and B we say that A is ***similar*** to B if there exists an invertible matrix S such that $B = S^{-1}AS$.

(a) Prove that if A is similar to B, then B is similar to A.

(b) Prove that if A is similar to B, then $\mathrm{Tr}(A) = \mathrm{Tr}(B)$. (*Hint*)

◊

Exercise 18. Let A be a $n \times n$ diagonal matrix with positive entries, so that the entries of A are given by: $[A]_{ij} = a_i\delta_{ij}$ where $a_i > 0, i = 1, \ldots, n$. Define the matrix $\log A$ as follows: $[\log A]_{ij} = \log(a_i)\delta_{ij}$, where log refers to natural logarithm. Show that:

$$\mathrm{Tr}(\log A) = \log(\det A).$$

(This formula is actually quite general, and applies to many non-diagonal matrices as well, as long as $\log A$ is properly defined.)[4]

$\Diamond$

17.5.2 Levi-Civita symbols

Definition

When dealing with vectors and matrices in physics, one often finds lurking the Levi-Civita symbol,[5] which is written as an epsilon (the Greek letter ϵ) with various numbers of subscripts. The possible values it can take are 1, -1, or 0, depending on the values of the subscripts (we refer to these subscripts as "indices"). This might not seem too useful since it can only take three different values, but you will see that it does a great job of simplifying expressions that ordinarily would be much more complicated.

For an epsilon with two indices (written as ϵ_{ij}), each index can be either 1 or 2. The different values that ϵ_{ij} can take are:

$$\epsilon_{ij} = \begin{cases} 1 \text{ if } i = 1, j = 2, \\ -1 \text{ if } i = 2, j = 1, \\ 0 \text{ if } i = j. \end{cases}$$

For an epsilon with three indices, each index can be either 1,2,or 3. The values of ϵ_{ijk} are:

$$\epsilon_{ijk} = \begin{cases} 1 \text{ where } (i,j,k) = (1,2,3), (2,3,1), \text{ or } (3,1,2), \\ -1 \text{ where } (i,j,k) = (2,1,3), (1,3,2), \text{ or } (3,2,1), \\ 0 \text{ where } i = j, i = k, \text{ or } j = k, \text{ i.e., if any index is repeated.} \end{cases}$$

What is the rule behind this definition? Every *permutation* of $(1,2,3)$. corresponds to one possible rearrangement of the indices. For instance the permutation $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ corresponds to the rearrangement $(2,3,1)$. Whenever this permutation $\left(\begin{smallmatrix} 1 & 2 & 3 \\ i & j & k \end{smallmatrix}\right)$ is *even* (that is, it can be written as the product of an even number of transpositions), then the corresponding value of ϵ_{ijk} is 1. Whenever this permutation

[4] In some cases, the formula can be used to estimate the determinants of very large matrices: see http://arxiv.org/pdf/hep-lat/9707001.

[5] Levi-Civita actually refers to one person, not two: the Italian mathematician Tullio Levi-Civita, (1873-1941), who worked on mathematical physics (including relativity).

$\left(\begin{smallmatrix}1&2&3\\i&j&k\end{smallmatrix}\right)$ is *odd* , then the corresponding value of ϵ_{ijk} is -1. Whenever any of the indices i, j, k are repeated, then $\left(\begin{smallmatrix}1&2&3\\i&j&k\end{smallmatrix}\right)$ does not correspond to a permutation, and the value of ϵ_{ijk} is 0.

This observation motivates the following general definition of the ***Levi-Civita symbol*** with n indices as:

$$\epsilon_{i_1 i_2 i_3 i_n} = \begin{cases} 1 \text{ if } (i_1, i_2, i_3, i_n) \text{ is an even permutation of } (1, 2, 3, \ldots n) \\ -1 \text{ if } (i_1, i_2, i_3, i_n) \text{ is an odd permutation of } (1, 2, 3, \ldots n) \\ 0 \text{ for any repeated index} \end{cases}$$

The symbol with n indices is sometimes called an n-dimensional Levi-Civita symbol: for instance, ϵ_{ijk} is a 3-dimensional Levi-Civita symbol. The reason for this is that most often they are used with vector spaces that have the same dimension as the number of indices in the symbol. So the Levi-Civita symbol with three indices, ϵ_{ijk} is most useful in three dimensions, as we'll see shortly.

Exercise 19. Using what you now know about the Kronecker delta and the Levi-Civita symbol, show that:

$$\sum_{i,j} \epsilon_{ij} \delta_{ij} = 0$$

(*Hint*) ◊

In the Set Theory chapter you saw the formula:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

This means that you may count all the elements contained in set A or set B by counting the elements in A and B separately, then subtracting their intersection. You have to subtract the intersection because the overlap between A and B gets counted twice in the separate counts of A and B. (Think of a set diagram, where A and B are represented by intersecting circles.) When we split up summations depending on whether indices are equal or unequal, we have to add and subtract in a similar way. We can prove this using Levi-Civita symbols.

Exercise 20.

(a) Show that $1 = |\epsilon_{ijk}| + \delta_{ij} + \delta_{jk} + \delta_{ik} - 2\delta_{ij}\delta_{ik}$ (*Hint*)

(b) Show that

$$\sum_{i,j,k} a_{ijk} = \sum_{i,j,k \text{ all unequal}} a_{ijk} + \sum_{i,k} a_{iik} + \sum_{i,j} a_{ijj} + \sum_{j,k} a_{kjk} - 2\sum_{i} a_{iii}.$$

(*Hint*)

◊

Levi-Civita symbols and determinants

Now that we have defined what the Levi-Civita symbol is, we can actually use if for something! The first application we'll look at is determinants. Suppose you have a 2×2 matrix A:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

Then the determinant is:

$$\det(A) = \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$$

We can write this using the Levi-Civita symbol as:

$$\det A = \sum_{i=1}^{2}\sum_{j=1}^{2} \epsilon_{ij} a_{1,i} a_{2,j}$$

Let's check this by evaluating the nested sum:

$$\begin{aligned} \det A =& \sum_{i=1}^{2}\sum_{j=1}^{2} \epsilon_{ij} a_{1,i} a_{2,j} && (17.1) \\ =& \sum_{i=1}^{2} \left(\epsilon_{i,1} a_{1,i} a_{2,1} + \epsilon_{i,2} a_{1,i} a_{2,2}\right) && (17.2) \\ =& \epsilon_{1,1}a_{1,1}a_{2,1} + \epsilon_{1,2}a_{1,1}a_{2,2} + \epsilon_{2,1}a_{1,2}a_{2,1} + \epsilon_{2,2}a_{1,2}a_{2,2} && (17.3) \end{aligned}$$

Looking at the definition, we know that $\epsilon_{1,1}$ and $\epsilon_{2,2}$ equals zero, so the leftmost and rightmost terms go to zero. For the remaining terms we have $\epsilon_{1,2}$ which equals 1, and $\epsilon_{2,1}$ which equals -1. Therefore, we are left with:

$$\det A = a_{1,1}a_{2,2} - a_{1,2}a_{2,1},$$

which is exactly the definition you learned in linear algebra.

The natural generalization to a 3×3 matrix as:

$$\det A = \sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{k=1}^{3} \epsilon_{ijk} a_{1,i} a_{2,j} a_{3,k}$$

Exercise 21. Show that the above formula using ϵ_{ijk} does agree with the determinant formula that you obtain from row expansion. $\Diamond$

Exercise 22. There is a formula for the determinant of a 4×4 matrix in terms of a 4-index Levi-Civita symbol. Write down what you think the formula is? (You don't need to prove the formula.) ◊

Exercise 23. Suppose σ is a permutation in S_4. We can define a 4×4 matrix P_σ using index notation as follows:

$$[P_\sigma]_{ij} = \begin{cases} 1 & \text{if } j = \sigma(i), \\ 0 & \text{if } j \neq \sigma(i). \end{cases}$$

(Here i and j can take any values from 1 to 4.)

(a) Write down the matrix P_σ when: (i) $\sigma = (13)$; (ii) $\sigma = (132)$; (iii) $\sigma = (12)(34)$; (iv) $\sigma = (1234)$.

(b) Show that when you multiply the 4×1 row vector [1 2 3 4] times the matrix P_σ, you obtain the second row of the tableau for σ. In other words, the matrix P_σ "performs" the permutation σ on row vector entries.

(c) Using the formula that you guessed in the previous problem, evaluate $\det P_\sigma$ when: (i) $\sigma = (24)$; (ii) $\sigma = (143)$; (iii) $\sigma = (14)(23)$; (iv) $\sigma = (1423)$.

(d) In the Permutations chapter we talked about —empheven and *odd* permutations. How is the value of $\det P_\sigma$ related to the evenness or oddness of σ?

◊

Exercise 24. Use the Levi-Civita form of the determinant to prove that the determinant of any square matrix A is equal to the determinant of its transpose. That is, $\det A = \det A^T$. ◊

An important concept to keep in mind when dealing with these Levi-Civita symbols is what they mean based on when indicies are equal or unequal, and how that relates to permutations. To see how this works, let's look at a proof to show that if any two rows in a 3x3 matrix are equal, the determinant is 0. Based on our definition we start out with:

$$\det A = \sum_{i,j,k} \epsilon_{ijk} a_{1i} a_{2j} a_{3k}$$

We want to show what happens when any two rows are equal, so lets do one case where row one equals row 2. In that case $a_{2j} = a_{1j}$. That means we can rewrite our determinant as:

$$\det A = \sum_{i,j,k} \epsilon_{ijk} a_{1i} a_{1j} a_{3k}$$

Notice what happens when we switch a_{1i} and a_{1j}; it also means that we must change ϵ_{ijk} to ϵ_{jik} because it is the position of the indicies that count (i.e. if we change the order of two indicies we must change the order for the rest). Switching a_{1i} and a_{1j} doesn't change our final product since they are communatative, so we end up with the expression:

$$\det A = \sum_{j,i,k} \epsilon_{jik} a_{1j} a_{1i} a_{3k}$$

Now remember what we discused earlier, if you interchange two indices (that is, an odd permutation) of ϵ_{ijk}, you get its negative, so $\epsilon_{jik} = -\epsilon_{ijk}$. This gives us the equality:

$$\sum_{j,i,k} \epsilon_{jik} a_{1j} a_{1i} a_{3k} = \sum_{j,i,k} -\epsilon_{ijk} a_{1i} a_{1j} a_{3k}$$

First of all, lets not lose sight that both the left hand side and the right hand side represent the same determinant. So what we see is that the determinant (a real number value) is equal to its negative. There is only one real number that is equal to its negative and that is zero! So to recap, if the first row is the same as the second row in a 3x3 matrix, the determinant is always zero.

Exercise 25. We showed that if the first and second row of a 3x3 matrix is the same, the determinant is zero. Now finish the proof that the determinant of a 3x3 is always zero if *any* two rows are the same; that is, prove it for the remaining cases. ♢

We can take the notion of equal and unequal indices as step farther by proving that the determinant of a product of two matricies is equal to the product of their determinants. Lets start with a simple 2x2 matrix. If matrices A and B are both 2x2, we want to prove that $\det(AB) = \det A$
$, textdet B$. We can write $\det(AB)$ as:

$$\det(AB) = \sum_{x,y} \epsilon_{xy} [AB]_{1x} [AB]_{2y}$$

Based on what we learned on how to represent products in terms of summation symbols, we can expand this as:

$$\begin{aligned} \det(AB) &= \sum_{x,y} \epsilon_{xy} \left[\sum_i a_{1i} b_{ix} \sum_j a_{2j} b_{jy} \right] \\ &= \sum_{x,y} \epsilon_{xy} \left[\sum_{i,j} a_{1i} a_{2j} b_{ix} b_{jy} \right] \end{aligned}$$

At this point we can now consider the product of two possibilities for our indices, one where $i = j$ and another where $i \neq j$:

$$\sum_{x,y} \epsilon_{xy} \left[\sum_{i=j} (\ldots) + \sum_{i \neq j} (\ldots) \right].$$

Of the two sums in the square brackets, the first makes zero contribution:

Exercise 26. Given that $i = j$ show that $\sum_{x,y} \epsilon_{xy} b_{ix} b_{jy}$ is equal to 0. Use this to show that the first summation in the square brackets makes zero contribution. $\Diamond$

Since we can ignore the case where $i = j$, let us look at the case where $i \neq j$. There are actually two cases: $i = 1, j = 2$ and $i = 2, j = 1$. Notice that:

$$\epsilon_{xy} b_{ix} b_{jy} = \epsilon_{xy} b_{1x} b_{2y} \text{ when } i = 1, j = 2;$$
$$\epsilon_{xy} b_{ix} b_{jy} = -\epsilon_{xy} b_{1x} b_{2y} \text{ when } i = 2, j = 1.$$

These two cases can be summarized as:

$$\epsilon_{xy} b_{ix} b_{jy} = \epsilon_{xy} \epsilon_{ij} b_{1x} b_{2y}.$$

This gives us:

$$\begin{aligned} \sum_{x,y} \epsilon_{xy} \left[\sum_{i,j} a_{1i} a_{2j} b_{ix} b_{jy} \right] &= \sum_{x,y} \sum_{i,j} \epsilon_{xy} \epsilon_{ij} a_{1i} a_{2j} b_{1x} b_{2y} \\ &= \left(\sum_{i,j} \epsilon_{ij} a_{1i} a_{2j} \right) \left(\sum_{x,y} \epsilon_{xy} b_{1x} b_{2y} \right), \end{aligned}$$

where in the second line we have noticed that the terms with x, y in the RHS of the first line can be separated from the terms with i, j. At this point we are just about done, since:

$$\det A = \sum_{i,j} \epsilon_{ij} a_{1i} a_{2j},$$
$$\det B = \sum_{x,y} \epsilon_{xy} b_{1x} b_{2y},$$

and therefore:

$$\begin{aligned} \det(AB) &= \sum_{x,y} \epsilon_{xy} \left[\sum_{i} a_{1i} b_{ix} \sum_{j} a_{2j} b_{jy} \right] \\ &= \left(\sum_{i,j} \epsilon_{ij} a_{1i} a_{2j} \right) \left(\sum_{x,y} \epsilon_{xy} b_{1x} b_{2y} \right) \\ &= \det A \det B. \end{aligned}$$

Levi-Civita symbols and cross products

Since we can define determinants using the Levi-Civita symbol, we can also define cross products of vectors, but before going any further it is important to know that in this section we are writing vectors in a very particular way. For vectors, we are labeling the components using numbered subscripts. For example, the vector $\mathbf{a}$ is written out as $\mathbf{a} = (a_1, a_2, a_3)$, and intuitively you can think of a_1 as the $x-$component of vector $\mathbf{a}$, a_2 as the $y-$component, and a_3 as the $z-$component. The reason for doing it this way is that having indices refer to natural numbers (such as the indices of the Levi-Civita symbol) makes the rest of the notation much easier to work with, especially if we want to make it more general .

If you think back to vector calculus (or for some of you college physics), the cross product of two vectors $\mathbf{a}$ and $\mathbf{b}$, where the components of each vector are $\mathbf{a} = (a_1, a_2, a_3)$ and $\mathbf{b} = (b_1, b_2, b_3)$ with a basis [6] of $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ (intuitively you can think of these basis components as labels for the x, y and z components, respectively), is given by the determinant of a matrix:

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix},$$

(Note that the absolute value brackets $|\cdots|$ indicate that this is a determinant, and not a matrix.) For example, suppose we have the vectors:

$$\mathbf{a} = [2\ 2\ 4] \qquad \text{and} \qquad \mathbf{b} = [-1\ 2\ -3].$$

Then the cross product $\mathbf{a} \times \mathbf{b}$ is given by the determinant:

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ 2 & 2 & 4 \\ -1 & 2 & -3 \end{vmatrix}.$$

Therefore:

$$\begin{aligned} \mathbf{a} \times \mathbf{b} =& \mathbf{e}_1 \begin{vmatrix} 2 & 4 \\ 2 & -3 \end{vmatrix} - \mathbf{e}_2 \begin{vmatrix} 2 & 4 \\ -1 & -3 \end{vmatrix} + \mathbf{e}_3 \begin{vmatrix} 2 & 2 \\ 1 & 2 \end{vmatrix} \\ =& -14\mathbf{e}_1 + 2\mathbf{e}_2 + 6\mathbf{e}_3. \end{aligned} \tag{17.4}$$

Or we can write the last line in a more familiar fashion:

$$[-14\ 2\ 6].$$

So all we have to do to define a cross product using the Levi-Civita symbol is to simply plug these terms into the formula for the 3×3 determinant from earlier:

$$\mathbf{a} \times \mathbf{b} = \det A = \sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} \epsilon_{ijk} \mathbf{e}_i a_j b_k$$

[6] Sometimes the basis is written as $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$, not to be confused with the indices i, j, k.

Notice that we have dropped the first index on each term. The reason is that the $\mathbf{e}$ terms will always be on the first row, a on the second, and b on the third. We can actually shorten this up a little bit more, by rewriting the formula to find the i^{th} component of $\mathbf{a} \times \mathbf{b}$. In other words, we don't want the summation of all three $\mathbf{e}_i$ terms, just one particular $\mathbf{e}_i$ term. That means we remove the summation over i, which leaves us with:

$$(\mathbf{a} \times \mathbf{b})_i = \sum_{j=1}^{3} \sum_{k=1}^{3} \epsilon_{ijk} a_j b_k$$

So for example, the first component (intuitively the x component, or as we would say, the $\mathbf{e}_1$ component) is:

$$(\mathbf{a} \times \mathbf{b})_1 = a_2 b_3 - a_3 b_2$$

Now see if you can find the equations for the second and third components. For those of you who are familiar enough with cyclic permutations, this is a relatively easy exercise.

Exercise 27. Use the Levi-Civita symbol to find the cross product of the vectors $\mathbf{a} = [2 \ -3 \ 2]$ and $\mathbf{b} = [1 \ 4 \ -3]$. ♢

Exercise 28. Use the Levi-Civita symbol–based equation for the cross product to show $\mathbf{a} \times \mathbf{b} = -\mathbf{b} \times \mathbf{a}$. ♢

In the following discussion, we will be writing many multiple sums involving the indices i, j and k, where each of these indices runs from 1 to 3. It is convenient to simplify the notation by representing the multiple sum as a single sum over multiple indices. For instance, with this simplified notation we may rewrite our expression for $\mathbf{a} \times \mathbf{b}$ as

$$\mathbf{a} \times \mathbf{b} = \sum_{i,j,k} \epsilon_{ijk} \mathbf{e}_i a_j b_k,$$

and we may rewrite the expression for $(\mathbf{a} \times \mathbf{b})_i$ as

$$(\mathbf{a} \times \mathbf{b})_i = \sum_{j,k} \epsilon_{ijk} a_j b_k.$$

Note that we do not bother to indicate that the indices i, j, k run from 1 to 3: this is understood by the nature of ϵ_{ijk}.

BAC-CAB Rule

As a final example, suppose we want to prove what is known as the $BAC - CAB$ rule, which states:

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = \mathbf{b} (\mathbf{a} \cdot \mathbf{c}) - \mathbf{c} (\mathbf{a} \cdot \mathbf{b}).$$

To prove this we can go two different routes: the brute-force method or the symmetry method. Let's start with the brute force method.

We can rewrite this using Levi-Civita symbols by using our definition of cross product. First we find the cross product of $\mathbf{b}$ and $\mathbf{c}$:

$$(\mathbf{b} \times \mathbf{c})_i = \sum_{j,k} \epsilon_{ijk} b_j c_k.$$

The tricky part is taking the cross product of that result with $\mathbf{a}$. Let us call the resulting vector of $\mathbf{b} \times \mathbf{c}$, $\mathbf{d}$. Then the first component of the resulting vector $\mathbf{d}$ is:

$$d_1 = (\mathbf{b} \times \mathbf{c})_1 = b_2 c_3 - b_3 c_2.$$

We can find the other components by noting that the indices are cyclic permutations. Recal that ϵ_{123} is equivalent to ϵ_{231} because the cycles (123) and (231) are equivalent. So to go from d_1 to d_2, we need an equivalent cycle that replaces the 1 in the i position (the first position) with a 2. Now the j position, the second position, would have to be 3, because in this cycle 2 goes to 3, and similarly for the last position it will become a 1. So 1 becomes 2, 2 becomes 3, and 3 becomes 1. Using this replacement we get d_2:

$$d_2 = (\mathbf{b} \times \mathbf{c})_2 = b_3 c_1 - b_1 c_3.$$

Tthe same strategy gives us d_3:

$$d_3 = (\mathbf{b} \times \mathbf{c})_3 = b_1 c_2 - b_2 c_1.$$

By substitution (and some algebraic rearranging) we can find $\mathbf{a} \times \mathbf{d}$, which is the same as $\mathbf{a} \times (\mathbf{b} \times \mathbf{c})$:

$$\begin{aligned}(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_1 = (\mathbf{a} \times \mathbf{d})_1 = a_2 d_3 - a_3 d_2 =& a_2 (b_1 c_2 - b_2 c_1) - a_3 (b_3 c_1 - b_1 c_3) \\ =& b_1 (a_2 c_2 + a_3 c_3) - c_1 (a_2 b_2 + a_3 b_3).\end{aligned}$$

Again, we can use the strategy of cyclically permuting the indices to easily find b_2 and b_3:

$$\begin{aligned}(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_2 = (\mathbf{a} \times \mathbf{d})_2 = a_3 d_1 - a_1 d_3 =& a_3 (b_2 c_3 - b_3 c_2) - a_1 (b_1 c_2 - b_2 c_1) \\ =& b_2 (a_3 c_3 + a_1 c_1) - c_2 (a_1 b_1 + a_3 b_3),\end{aligned}$$

$$\begin{aligned}(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_3 = (\mathbf{a} \times \mathbf{d})_3 = a_1 d_2 - a_2 d_1 =& a_1 (b_3 c_1 - b_1 c_3) - a_2 (b_2 c_3 - b_3 c_2) \\ =& b_3 (a_1 c_1 + a_2 c_2) - c_3 (a_1 b_1 + a_2 b_2).\end{aligned}$$

Recall the definition of dot product in three dimensions:

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + a_2 b_2 + a_3 b_3.$$

This means we're very close; we're just missing a few terms. It turns out that we can add them in without changing anything. For example, let us see what happens when we add the terms a_1c_1 and a_1b_1 to the first component of $\mathbf{a}\times(\mathbf{b}\times\mathbf{c})$ we found earlier:

$$\begin{aligned}
&b_1\left(a_1c_1+a_2c_2+a_3c_3\right)-c_1\left(a_1b_1+a_2b_2+a_3b_3\right)\\
&\quad=b_1a_1c_1+b_1a_2c_2+b_1a_3c_3-c_1a_1b_1-c_1a_2b_2-c_1a_3b_3\\
&\quad=\left(b_1a_1c_1-c_1a_1b_1\right)+b_1\left(a_2c_2+a_3c_3\right)-c_1\left(a_2b_2+a_3b_3\right)\\
&\quad=b_1\left(a_2c_2+a_3c_3\right)-c_1\left(a_2b_2+a_3b_3\right).
\end{aligned}$$

The same steps can be used to justify adding missing terms in the other two components as well. So now we can say that:

$$\begin{aligned}
\left(\mathbf{a}\times(\mathbf{b}\times\mathbf{c})\right)_1&=b_1\left(\mathbf{a}\cdot\mathbf{c}\right)-c_1\left(\mathbf{a}\cdot\mathbf{b}\right),\\
\left(\mathbf{a}\times(\mathbf{b}\times\mathbf{c})\right)_2&=b_2\left(\mathbf{a}\cdot\mathbf{c}\right)-c_2\left(\mathbf{a}\cdot\mathbf{b}\right),\\
\left(\mathbf{a}\times(\mathbf{b}\times\mathbf{c})\right)_3&=b_3\left(\mathbf{a}\cdot\mathbf{c}\right)-c_3\left(\mathbf{a}\cdot\mathbf{b}\right).
\end{aligned}$$

Since we have all three components of the vectors represented and multiplied by the same thing we can shorten this to:

$$\mathbf{a}\times(\mathbf{b}\times\mathbf{c})=\mathbf{b}\left(\mathbf{a}\cdot\mathbf{c}\right)-\mathbf{c}\left(\mathbf{a}\cdot\mathbf{b}\right).$$

Done!

The other way of proving the BAC-CAB rule requires a bit more finesse than our previous brute force approach. This time around we are going make more use of the symmetries of ϵ, so that we do not have to write out every single term. First let us write the BAC-CAB rule in a way that allows us to more easily ask what happens for every possible value our indices can take, so that we may organize them and get rid of any zero terms.

We begin by writing the i'th component of $A\times(B\times C)$ using Levi-Civita symbols as

$$\left(A\times(B\times C)\right)_i=\sum_{j,k,m,n}\left[\epsilon_{ijk}A_j(\epsilon_{kmn}B_mC_n)\right].$$

You can rewrite this as:

$$\left(A\times(B\times C)\right)_i=\sum_{j,m,n}\left[\sum_k\epsilon_{ijk}\epsilon_{kmn}\right]A_jB_mC_n.$$

Let's define the quantity inside the $[\dots]$ as S_{ijmn}:

$$S_{ijmn}:=\left[\sum_k\epsilon_{ijk}\epsilon_{kmn}\right].$$

Then we will be able to simplify our expression for $(A \times (B \times C))_i$ if we can find a simpler expression for S_{ijmn}. This quantity will have a different value for each choice of i, j, m, n.

Let's focus on the indices i and j. First, if $i = j$ then $\epsilon_{ijk} = \epsilon_{iik} = 0$, so $S_{iimn} = 0$. On the other hand, if $i \neq j$, there is only one value of k that makes ϵ_{ijk} nonzero (because we must have $k \neq i, j$). We must also have $m, n \neq k$ in order for $\epsilon_{kmn} \neq 0$. It follows that there are two possibilities for which $S_{ijmn} \neq 0$:

(A) $i \neq j$, $m = i$ and $n = j$;

(B) $i \neq j$, $m = j$ and $n = i$.

In case (A) we have:

$$S_{ijij} = \left[\sum_k \epsilon_{ijk}\epsilon_{kij}\right] = \left[\sum_k \epsilon_{ijk}^2\right] = 1.$$

In case (B) we have:

$$S_{ijji} = \left[\sum_k \epsilon_{ijk}\epsilon_{kji}\right] = \left[\sum_k -\left[\epsilon_{ijk}^2\right]\right] = -1.$$

In summary we have:

$$\begin{aligned} S_{ijmn} &= 1 \text{ if } m = i,\ n = j,\ \text{and } i \neq j; \\ S_{ijmn} &= -1 \text{ if } n = i,\ m = j,\ \text{and } i \neq j; \\ S_{ijmn} &= 0 \text{ otherwise.} \end{aligned}$$

Let's plug this back into our expression for $(A \times (B \times C))_i$. We can then separate the terms where $m = i$, $n = j$ from the terms where $n = i$, $m = j$. Notice that there is no longer a sum over 3 indices but only one index, since m and n are determined by i and j:

$$\underbrace{\sum_{j,j\neq i} A_j B_i C_j}_{(\text{terms for } m = i,\ n = j)} \quad - \quad \underbrace{\sum_{j,j\neq i} A_j B_j C_i}_{(\text{terms for } m = j,\ n = i)}$$

Now if we add $A_i B_i C_i$ to the first set of terms, and subtract $A_i B_i C_i$ to the second set of terms, then the overall sum doesn't change but the two expressions simplify:

$$\sum_j A_j B_i C_j - \sum_j A_j B_j C_i$$

This is the same as:

$$B_i(A \cdot C) - C_i(A \cdot B),$$

which is the $BAC - CAB$ rule. In this example the brute force method wasn't much harder than the symmetry method, but for more complicated expressions it is far easier to use the symmetries of ϵ to prove a statement rather than do it term by term.

Exercise 29. Using some facts from the discussion above, show that S_{ijmn} can also be written in terms of Kronecker deltas as follows:

$$S_{ijmn} = \delta_{im}\delta_{jn} - \delta_{in}\delta_{jm}.$$

$\Diamond$

17.6 Summation by parts

Those of you who have studied integrals in calculus are probably familiar with integration by parts, where you use it to find the integral of the product of two terms. It turns out that there is a discrete version, called summation by parts:

$$\sum_{k=m}^{n} a_k \left(b_{k+1} - b_k\right) = \left[a_{n+1}b_{n+1} - a_m b_m\right] - \sum_{k=m}^{n} b_{k+1} \left(a_{k+1} - a_k\right)$$

There are other ways of rewriting this to make it a little bit shorter. Suppose our sum starts at 0, and furthermore, suppose we define the following term:

$$B_n = \sum_{k=0}^{n} b_k \text{ for every } n > 0$$

Then we have:

$$\sum_{n=0}^{N} a_n b_n = a_N B_N - \sum_{n=0}^{N-1} B_n \left(a_{n+1} - a_n\right)$$

In this form, summation by parts is relatively easy to prove. Notice that:

$$b_n = B_n - B_{n-1}$$

Then we can say:

$$\begin{aligned}\sum_{n=0}^{N} a_n b_n =& a_0 b_0 + \sum_{n=1}^{N} a_n \left(B_n - B_{n-1}\right) \\ =& a_0 b_0 - a_1 B_0 + a_N B_N + \sum_{n=1}^{N-1} B_n \left(a_n - a_{n+1}\right) \\ =& a_N B_N - \sum_{n=0}^{N-1} B_n \left(a_{n+1} - a_n\right)\end{aligned}$$

To make some sense of this, let's try an example. Suppose we want to prove the following:

$$\sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}$$

We could use induction to prove this. But we can also prove it directly using the summation by parts formula we wrote earlier:

$$\sum_{k=m}^{n} a_k \left(b_{k+1} - b_k\right) = \left[a_{n+1} b_{n+1} - a_m b_m\right] - \sum_{k=m}^{n} b_{k+1} \left(a_{k+1} - a_k\right)$$

Just as is the case with integration by parts, deciding what the terms will be will determine if we have an easy or difficult (sometimes impossible) time. In this case, a good choice is to let $a_k = k^2$ and $b_k = k$. Notice that with this choice, we have:

$$\sum_{k=1}^{n} a_k \left(b_{k+1} - b_k\right) = \sum_{k=1}^{n} k^2 \left((k+1) - k\right) = \sum_{k=1}^{n} k^2$$

So our choice of terms does indeed give us k^2. Now that we have our two sequences $\{a_k\}$ and $\{b_k\}$, let's plug them in to the summation by parts formula and see what we get:

$$\begin{aligned}\sum_{k=1}^{n} k^2 = \sum_{k=1}^{n} k^2 \left((k+1) - k\right) =& \left((n+1)^2 (n+1) - 1\right) - \sum_{k=1}^{n} \left((k+1)^2 - k^2\right)(k+1) \\ =& (n+1)^3 - 1 - \sum_{k=1}^{n} (k+1)^3 - \left(k^3 + k^2\right) \\ =& n^3 + 3n^2 + 3n - \sum_{k=1}^{n} k^3 + 3k^2 + 3k + 1 - k^3 - k^2 \\ =& n^3 + 3n^2 + 3n - \sum_{k=1}^{n} \left(2k^2 + 3k + 1\right) \\ =& n^3 + nk^2 + nk - \sum_{k=1}^{n} 2k^2 - \sum_{k=1}^{n} 3k - \sum_{k=1}^{n} 1\end{aligned}$$

Notice that we have the summation of k^2 on the right, and one of the summation terms on the left is $-2k^2$. We can combine these on the left to get:

$$3\sum_{k=1}^{n} k^2 = n^3 + 3n^2 + 3n - 3\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1$$

The remaining sums on the right are common sums that we can easily find:

$$\begin{aligned} 3\sum_{k=1}^{n} k^2 =& n^3 + 3n^2 + 3n - 3\frac{n(n+1)}{2} - n \\ =& n^3 + \frac{3n^2}{2} + \frac{n}{2} \end{aligned}$$

And finally dividing by three gives us our final result:

$$\sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}$$

Exercise 30. Prove the following equation using summation by parts:

$$\sum_{k=1}^{n} k^3 = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}$$

◊

Exercise 31. Evaluate the sum:

$$\sum_{k=1}^{n} k \cdot 2^k.$$

(*Hint*) ◊

18

Polynomials

18.1 Polynomials of various stripes

In high school we learn how to do algebraic operations on polynomials.[1] For instance, if we have

$$\begin{aligned} p(x) &= x^3 - 3x + 2 \\ q(x) &= 3x^2 - 6x + 5, \end{aligned}$$

then we can compute

$$\begin{aligned} p(x) + q(x) &= (x^3 - 3x + 2) + (3x^2 - 6x + 5) \\ &= x^3 + 3x^2 - 3x - 6x + 5 + 2 \\ &= x^3 + 3x^2 - 9x + 7 \end{aligned}$$

Notice that we have grouped together terms which have the same power of our variable x, which is not only pretty but also very useful later on.

Multiplication of polynomials is a bit more involved, so let us start with polynomials of single terms (monomials) and then move up from there. Suppose we have,

$$p(x) = 5x^3 \text{ and } q(x) = 3x^2.$$

Then their product is

$$\begin{aligned} p(x)q(x) &= 5x^3 3x^2 \\ &= (5 \cdot 3)x^{(3+2)}, \\ &= 15x^5 \end{aligned}$$

[1] This chapter contains contributions from David Weathers, Johnny Watts, and Semi Harrison (edited by C.T.). Thanks to Tom Judson for material used in this chapter.

where we combined the coefficients and the exponents (remember your exponent rules!).

Let's extend ourselves and multiply a polynomial of two terms by a monomial:

$$p(x) = 5x^3 + 2x \text{ and } q(x) = 3x^2.$$

According to the distributive law, we multiply each term in the first polynomial with the second polynomial:

$$\begin{aligned} p(x)q(x) &= (5x^3 + 2x)3x^2 \\ &= 5x^3 3x^2 + 2x3x^2 \\ &= (5 \cdot 3)x^{(3+2)} + (2 \cdot 3)x^{(1+2)} \\ &= 15x^5 + 6x^3. \end{aligned}$$

In order to multiply a two term polynomial by another two term polynomial, e.g.

$$p(x) = 5x^3 + 2x \text{ and } q(x) = 3x^2 - 6x,$$

we extend the distributive law even further. Like before, each term in the first polynomial is being multiplied by every term in the second polynomial, Then their product is

$$\begin{aligned} p(x)q(x) &= (5x^3 + 2x)(3x^2 - 6x) \\ &= 5x^3(3x^2 - 6x) + 2x(3x^2 - 6x) \end{aligned}$$

At this point we just have the sum of two monomials times a two term polynomial, which we now know can be calculated using the distributive property,

$$\begin{aligned} &= 5x^3(3x^2 - 6x) + 2x(3x^2 - 6x) \\ &= (15x^5 - 30x^4) + (6x^3 - 12x^2) \\ &= 15x^5 - 30x^4 + 6x^3 - 12x^2 \end{aligned}$$

This is just the same result as the FOIL method you learned in high school, but thinking in terms of the distributive property has the advantage of being applicable to polynomials that have more than just two terms each. For instance, with

$$p(x) = 5x^3 + 4x^2 - 2x \text{ and } q(x) = 3x^2 - 6x,$$

we obtain

$$\begin{aligned} p(x)q(x) &= 5x^3(3x^2 - 6x) + 4x^2(3x^2 - 6x) - 2x(3x^2 - 6x) \\ &= (15x^5 - 30x^4) + (12x^4 - 24x^3) + (-6x^3 + 12x^2) \\ &= 15x^5 - 30x^4 + 12x^4 - 24x^3 - 6x^3 + 12x^2 \\ &= 15x^5 + (-30 + 12)x^4 + (-24 - 6)x^3 + 12x^2 \\ &= 15x^5 - 18x^4 - 30x^3 + 12x^2. \end{aligned}$$

Again notice that we are grouping like terms by exponent. Later, when we give a more general way of multiplying polynomials, this method of distributing is what you need to have in mind.

Similar rules apply if we perform algebraic operations on polynomials with integer, rational, real, or complex coefficents. We may identify different sets of polynomials according to the type of coefficient used. For instance we may define:

- $\mathbb{Z}[x]$ is the set of polynomials in the variable x with integer coefficients;
- $\mathbb{R}[x]$ is the set of polynomials in the variable x with real coefficients.

Similarly we may define $\mathbb{N}[x], \mathbb{Q}[x], \mathbb{C}[x]$, and so on. We may even define $\mathbb{Z}_n[x]$ for the integers mod n. For example, two polynomials $p(x)$ and $q(x)$ in $\mathbb{Z}_4[x]$ are

$$\begin{aligned} p(x) &= x^3 + 3x + 1 \\ q(x) &= 3x^3 + 3x^2 + 2x + 2. \end{aligned}$$

We may add them as follows:

$$\begin{aligned} p(x) + q(x) &= (1 \oplus 3)x^3 + (0 \oplus 3)x^2 + (3 \oplus 2)x + (1 \oplus 2) \\ &= 3x^2 + x + 3, \end{aligned}$$

and multiply as folows:

$$\begin{aligned} p(x)q(x) &= (1 \odot 3)x^6 + (1 \odot 3)x^5 + (2 \oplus 3 \odot 3)x^4 + (1 \odot 2 \oplus 3 \odot 3 \oplus 1 \odot 3)x^3 \\ &\quad + (3 \odot 2 \oplus 1 \odot 3)x^2 + (3 \odot 2) + 1 \odot 2)x + 1 \odot 2 \\ &= 3x^6 + 3x^5 + 3x^4 + 2x^3 + 1x^2 + 2. \end{aligned}$$

Notice that arithmetic mod 4 is used on the *coefficients* of each term, but the regular '+' sign is used to add terms themselves.

It turns out that $\mathbb{Z}_2[x]$ is of great practical usefulness (in polynomial codes), so we include an exercise to get you warmed up.

Exercise 1. Compute the sum and product of $p(x)$ and $q(x)$, where both polynomials are in $\mathbb{Z}_2[x]$.

(a) $p(x) = x^2 + x + 1$, $q(x) = x^3 + x^2 + x + 1$

(b) $p(x) = x^4 + x^2 + 1$, $q(x) = x^4 + x^3 + x^2$.

(c) $p(x) = x^4 + x^3 + x^2 + x + 1$, $q(x) = p(x)$.

$\Diamond$

Are these sets of polynomials ($\mathbb{Z}[x], \mathbb{R}[x]$ and so on) also groups? I'm glad you asked! See if you can figure it out:

Exercise 2. For each of the following parts, *explain* your answer.

(a) Which of the following are groups under addition: $\mathbb{N}[x], \mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_5[x]$,$\mathbb{Z}_6[x]$?

(b) Which of the following are groups under multiplication: $\mathbb{N}[x]$, $\mathbb{Z}[x]$,$\mathbb{Q}[x]$,$\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_5[x]$,$\mathbb{Z}_6[x]$?

$\Diamond$

Exercise 3. Compute the sum and product of $p(x)$ and $q(x)$.

(a) $p(x) = 2x^2 + x + 1$, $q(x) = x^3 + 3x^2$,where both polynomials are in $\mathbb{Z}_5[x]$.

(b) $p(x) = 2x^4 + 3x^3 + 4x^2 + 1$, $q(x) = x^3 + 2x^2 + 5$, where both polynomials are in $\mathbb{Z}_6[x]$.

$\Diamond$

In some sense, polynomials are more complicated than groups because they have two operations, while groups have only one. It turns out that polynomial sets are important examples of a second type of mathematical object called a *ring*. Later in this chapter we will define rings in general; but for now, we will look at polynomials in particular (and generalize our results later).

18.2 Polynomial rings

We have noted above that polynomials can have different types of coefficients. In this section we will impose some properties on the coefficients that, although quite general, will enable us to prove several interesting properties. But first, let's relate polynomials to the summation notation that we discussed in the previous chapter:

Definition 4. (*Polynomial notation*) A polynomial may be written as

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = \sum_{i=0}^{n} a_ix^i,$$

Where $\{a_i, i = 1, 2, \ldots n\}$ are called the ***coefficients*** of $\{x^i\}$. It is possible for $a_i = 0$, in which case we usually omit the corresponding x^i term (for instance, we write $x^2 - 7$ rather than $x^2 + 0x - 7$). When we write a polynomial as a sum in this way we will *assume* that $a_n \neq 0$ (here a_n is called the ***leading coefficient***. Thus the largest power of x that appears in the polynomial is x^n: this largest power is called the ***degree*** of the polynomial. $\triangle$

Exercise 5. Re-express the following polynomials in summation notation, and give the degree of each polynomial.

(a) $1 + 0x + 3x^2 + 0x^3 + 5x^4 + 0x^5 + 7x^6 + 0x^7 + 9x^8$

(b) $1 + 0x + \text{cis}(\pi/2)x^2 + 0x^3 + \text{cis}(\pi)x^4 + 0x^5 + \text{cis}(3\pi/2)x^6 + 0x^7$

(c) $1 + 2x + 4x^2 + 8x^3 + 16x^4 + 32x^5$

(d) $1 + 4x + 11x^2 + 30x^3 + 85x^4$ (*Hint*)

(e) $1 - \frac{1}{3}x + \frac{1}{5}x^2 - \frac{1}{7}x^3 + \frac{1}{9}x^4 - \frac{1}{11}^5$

$\Diamond$

Definition 6. (*Polynomial rings*) A set of polynomials is called a ***polynomial ring*** if two operations (which we denote as $+$ and $\cdot$) are defined on the set of coefficients and

- The coefficients form an abelian group under $+$, with identity element 0;
- The nonzero coefficients form an abelian group under $\cdot$, with identity element 1.
- The operations $+$ and $\cdot$ on the set of coefficients satisfy the distributive property: for any three coefficients a, b, c, we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

$\triangle$

Remark 7.

- Many other references define polynomial rings differently (for instance, they may not require that the nonzero coefficients form a group under multiplication). Our definition is more restrictive than most.
- In the following, whenever we refer to 'polynomials" without specifically mentioning what type of coefficients it has, we are presuming that the polynomials are elements of a polynomial ring.

$\triangle$

Exercise 8.

(a) According to Definition 6,is $\mathbb{Z}_6[x]$ a polynomial ring? *Explain* your answer.

(b) According to Definition 6,is $\mathbb{Z}_{11}[x]$ a polynomial ring? *Explain* your answer.

(c) What are the conditions on n such that $\mathbb{Z}_n[x]$ is a polynomial ring?

◊

We see from the previous exercise that $F[x]$ fails to be a polynomial ring when F^* is not an abelian group. Why do we require this? It turns out that if we don't, then the polynomials have some nasty properties that we don't want.

Exercise 9.

(a) Find two nonzero polynomials in $\mathbb{Z}_4[x]$ of degree 1 and 3 respectively whose product is 0.

(b) Is it possible to find two nonzero polynomials $\mathbb{Z}_5[x]$ whose product is 0? *Explain* your answer.

(c) Suppose $n = p \cdot q$, where p and q are positive integers. Show that there exist two nonzero polynomials in $\mathbb{Z}_n[x]$ whose product is 0.

◊

In the previous section, we showed properties of polynomials in the familiar case where the coefficients are real numbers. Now let's do the same thing, but this time for arbitrary polynomial rings.

Definition 10. Two polynomials are said to be ***equal*** if and only if their corresponding coefficients are equal. That is, if we let

$$p(x) = \sum_{i=0}^{n} a_i x^i; \qquad q(x) = \sum_{i=0}^{m} b_i x^i,$$

then $p(x) = q(x)$ if and only if $n = m$ and $a_i = b_i$ for all $0 \leq i \leq n$. △

Definition 11. We define the ***sum of two polynomials*** as follows. Let

$$p(x) = \sum_{i=0}^{n} a_i x^i; \qquad q(x) = \sum_{i=0}^{m} b_i x^i,$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i.$$

(If a_i or b_i is not specified for some power $i \leq \max(m, n)$, then it is assumed to be 0.)

△

Notice that we have taken the upper limit of the sum to $\max(n, m)$ in order to make sure to include all nonzero terms from both polynomials.

Throughout this book, we have encountered various mathematical structures and shown that in many cases they possess group properties. Let's now give polynomials that same treatment. Since we have two operations, addition and multiplication, it is possible that polynomials are groups under either or both of these operations. Of course, it's possible that polynomials may have have different properties depending on what type of coefficients they have, so all of the following proofs will depend *only* on the coefficient properties listed in Definition 5.

First let us take a look at the commutativity and associativity of addition. While commutativity is not a necessary property for groups, we include the following proof because it uses techniques that are useful in many polynomial proofs.

Proposition 12. Polynomial addition is both commutative:

$$p(x) + q(x) = q(x) + p(x),$$

and associative:

$$(p(x) + q(x)) + r(x) = p(x) + (q(x) + r(x)).$$

PROOF. First, we show commutativity: Given polynomials,

$$p(x) = \sum_{i=0}^{n} a_i x^i; \qquad q(x) = \sum_{i=0}^{m} b_i x^i,$$

then

$$p(x) + q(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i,$$

and

$$p(x) + q(x) = \sum_{i=0}^{\max(m,n)} (b_i + a_i) x^i.$$

Since the coefficients are abelian under $+$, we have $a_i + b_i = b_i + a_i$ for all i. It follows that all coefficents of $p(x)+q(x)$ are equal to the corresponding coefficients of $q(x)+p(x)$. By the definition of polynomial equality, this means that $p(x)+q(x) = q(x)+p(x)$. Note that the condition that the coefficients be commutative is satisfied for all of the polynomials we have been considering so far, including $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, and so on.

□

Exercise 13. Using the definition of polynomial equality and polynomial addition, complete Proposition 12 by proving the associativity of polynomial addition. ◊

It is also true that polynomials under addition have an identity and an inverse.

Proposition 14. Polynomials have an additive identity.

Exercise 15. Show that polynomials have an additive identity by specifying the identity polynomial, and showing that it satisfies the identity property. ◊

Proposition 16. Every polynomial has an additive inverse. (In the following, we will write the additive inverse of $p(x)$ as $-p(x)$).

Exercise 17. Given any polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$, show that an additive inverse to that polynomial exists by (a) specifying the inverse and (b) showing that it satisfies the inverse property. ◊

Proposition 18. Polynomials under addition form a group. The group is abelian if the additive group of coefficients is abelian.

Exercise 19. Prove Proposition 18. ◊

If we have a formula for adding polynomials, we must surely have a formula for multiplying polynomials, and sure enough we do. The easy part is knowing what degree (the value of the highest exponent) of polynomial the result will be, because that is just the sum of the degrees of polynomials being multiplied. For example, a first degree polynomial like $2x + 1$ times a second degree polynomial like $4x^2$ gives us $8x^3 + 4x^2$, which is a third degree polynomial. By looking at similar examples, you may convince yourself that for *any* two polynomials, if $p(x)$ is a polynomial of degree m and $q(x)$ is a polynomial of degree n, then their product will produce a polynomial with a degree of $m + n$:

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k.$$

If a power doesn't show up in the result, it just means the coefficient is zero. For instance, our earlier result of $8x^3 + 4x^2$ could also have been written as $8x^3 + 4x^2 + 0x^1 + 0x^0$. So we have a general formula that gives the correct exponents for our variable, in this case x, but we still don't know what the coefficients c are.

To find a general expression for those coefficients we need to use the same techniques as we did earlier when multiplying polynomials, except this time look at it in a general way. So instead of giving you an example with specific numbers,

let us define two general polynomials and see what we get when we multiply them. As with addition, we use

$$p(x) = \sum_{i=0}^{n} a_i x^i; \qquad q(x) = \sum_{i=0}^{m} b_i x^i.$$

Remember from basic algebra that when you multiply polynomials you multiply the first term of the first polynomial by each term in the second polynomial. You then add that result to multiplying the second term of the first polynomial by each term in the second polynomial, and do the same for the other terms. Going by that rule, the product of our two polynomials is:

$$p(x)q(x) = a_0 x^0 \Big(\sum_{k=0}^{n} b_k x^k \Big) + a_1 x^1 \Big(\sum_{k=0}^{n} b_k x^k \Big) + \ldots + a_m x^m \Big(\sum_{k=0}^{n} b_k x^k \Big).$$

We can also write this in summation notation, which will be useful later on when we try to prove that multiplication of polynomials is associative.

$$p(x)q(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j}$$

Let us get back to finding a formula for those coefficients. Given the expanded form of the product $p(x)q(x)$, we can collect some common terms, we will call them R_t (the index t tells us what exponent is associated with the variable x), and see what we come up with, where we define common terms as the sum of all values of x that share the same exponent. Let us start with the terms associated with x^0, in our case the term labeled R_0, where there is only one possible combination that results in x^0:

$$R_0 = a_0 x^0 b_0 x^0 = a_0 b_0 (x^0 \cdot x^0) = a_0 b_0 (x^0)$$

Thus the coefficient c_0 is:

$$c_0 = a_0 b_0.$$

How about R_1 and R_2, where we collect every possible combination that will result in x having an exponent of 1 and 2, respectively:

$$R_1 = a_0 x^0 b_1 x^1 + a_1 x^1 b_0 x^0 = (a_0 b_1 + a_1 b_0) x^1 \Rightarrow c_1 = a_0 b_1 + a_1 b_0$$

$$R_2 = a_0 x^0 b_2 x^2 + a_1 x^1 b_1 x^1 + a_2 x^2 b_0 x^0 = (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 \Rightarrow c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

Looking at the indices of the coefficients, especially once we get to the third coefficient,you can see the pattern:

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i},$$

which we can combine with what we already know about the exponents to give a general formua:

Definition 20.

The *product* of polynomials $p(x)$ and $q(x)$ is:

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k,$$

where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

for each i. Notice that in each case some of the coefficients may be zero. △

If you are still not convinced the formula given in the definion works, look at the fourth coefficient. The formula in the definition gives:

$$c_3 = \sum_{i=0}^{3} a_i b_{3-i} = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0.$$

If you go about it the long way, that is to write out the polynomial and then pick out and add together every single combination that results in x^3, you will get the exact same thing. Having established that the definition works, we can actually use it with confidence. Suppose we have two polynomials, $p(x)$ and $q(x)$ we want to multiply, and let us call the result $f(x)$:

$$f(x) = (1 + x^2 - 2x^3)(x + 4x^3)$$

So $p(x)$ and $q(x)$ are:

$$p(x) = 1x^0 + 0x^1 + 1x^2 + (-2)x^3$$

$$q(x) = 0x^0 + 1x^1 + 0x^2 + 4x^3$$

The highest exponent on both of these is 3, so going by the formula given in the definition we have $m = 3$ and $n = 3$:

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k = \sum_{k=0}^{6} c_k x^k.$$

Now all we have to do is find the values of the seven coefficients $c_0, \ldots, c_6$, some of which may be zero. Let us start with c_0:

$$c_0 = \sum_{i=0}^{0} a_i b_{0-i} = a_0 b_0 = 0 \cdot 1 = 0.$$

Already we've found a term that is zero. Six more coefficients to find–how about we look at the fifth coefficient:

$$c_4 = \sum_{i=0}^{4} a_i b_{4-i} = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0.$$

Notice that $a_4 = b_4 = 0$ since $p(x)$ and $q(x)$ both have degree 3, so the first and last terms are both 0. Altogether we have

$$c_4 = 0 + 0 \cdot 4 + 1 \cdot 0 + (-2) \cdot 1 + 0 = -2.$$

Doing the same for the other coefficients gives us:

$$0x^0 + 1x^1 + 0x^2 + 5x^3 + (-2)x^4 + 4x^5 + (-8)x^6$$

Getting rid of the zero terms and dealing with the negatives gives us the simplified version:

$$x + 5x^3 - 2x^4 + 4x^5 - 8x^6.$$

Exercise 21. Perform the following polynomial multiplications in two ways: first, by distributing and collecting terms; and second, by using the coefficent formula in Definition 20 directly. Verify that the two methods agree.

(a) $(x - 5)(x^2 + 3x)$

(b) $(x - \sqrt{3})(5x^3 + 2\sqrt{3})$

(c) $(4x^2 - 3x + 7/2)(x^3 + 2)$

(d) $(8x^5 + 4x^3 - 7x^2)(10x^2 - 5x + 3)$

$\Diamond$

Exercise 22. Use the coefficent formula in Definition 20 to evaluate the following products.

(a) $p(x)^2$, where $p(x) = \sum_{i=0}^{3} x^i$

(b) $p(x) \cdot q(x)$, where $p(x) = \sum_{i=1}^{3} (i-1)x^i$ and $q(x) = \sum_{j=0}^{2} (3-j)x^j$

(c) $p(x) \cdot q(x)$, where $p(x) = \sum_{i=0}^{4} (i-3)x^i$ and $q(x) = \sum_{j=0}^{4} (j-2)x^j$

(d) $p(x) \cdot q(x)$, where $p(x) = \sum_{i=0}^{4} (2i-6)x^i$ and $q(x) = \sum_{j=0}^{4} (3j-6)x^j$ (*Hint*)

◊

Polynomials also have *some* group properties under multiplication.

Exercise 23. Show that the polynomial $p(x) = 1x^0$ is a multiplicative identity for the set of polynomials $\mathbb{C}[x]$. ◊

Polynomials in general do not have multiplicative inverses *that are polynomials*. Of course, in high-school algebra you defined $1/p(x)$ as the multiplicative inverse of the polynomial $p(x)$, but $1/p(x)$ is not a polynomial so it doesn't count!

Exercise 24.

(a) Consider the polynomial $p(x) = 1x$ as an element of $\mathbb{R}[x]$. Show there is no polynomial in $\mathbb{R}[x]$ that is a multiplicative inverse of $p(x)$.

(b) Prove or disprove: polynomial rings are also commutative groups over multiplication.

◊

Another useful fact to keep in mind is that polynomial multiplication is associative. First, let's see this in an example.

Exercise 25. Show that the multiplication of two linear terms and one quadratic term is associative. ◊

Now we'd like to prove associativity in general. Here's where summation notation comes in really handy. To show associativity, we need to show that $(p(x)q(x))r(x) = (p(x)q(x))r(x)$. As we stated before, the product of two polynomials $p(x)$ and $q(x)$ written in summation notation is:

$$p(x)q(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j}$$

So let's introduce a third polynomial, $r(x)$, with degree l and coefficients $\{c_i, i = 1 \dots l$, and calculate its product with $(p(x)q(x))$:

$$\begin{aligned}(p(x)q(x))r(x) =& \Big(\sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j}\Big)\Big(\sum_{k=0}^{l} c_k x^k\Big) \\ =& \sum_{i=0}^{m}\sum_{j=0}^{n}\Big(a_i b_j x^{i+j}\Big(\sum_{k=0}^{l} c_k x^k\Big)\Big) \\ =& \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{k=0}^{l} a_i b_j x^{i+j}\cdot c_k x^k \\ =& \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{k=0}^{l} a_i b_j c_k x^{i+j+k}.\end{aligned}$$

Here we used our summation and exponent rules that you know and love so well. Now let's see if we get the same result for $p(x)(q(x)r(x))$. Following similar steps, we get:

$$\begin{aligned}p(x)(q(x)r(x)) =& \Big(\sum_{i=0}^{m} a_i x^i\Big)\Big(\sum_{j=0}^{n}\sum_{k=0}^{l} b_j x^j c_k x^k\Big) \\ =& \sum_{i=0}^{m}\left(a_i x^i\Big(\sum_{j=0}^{n}\sum_{k=0}^{l} b_j c_k x^{j+k}\Big)\right) \\ =& \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{k=0}^{l} a_i x^i \cdot b_j c_k x^{j+k} \\ =& \sum_{i=0}^{m}\sum_{j=0}^{n}\sum_{k=0}^{l} a_i b_j c_k x^{i+j+k}.\end{aligned}$$

This is indeed the exact same expression as before, so it is true that $(p(x)q(x))r(x) = p(x)(q(x)r(x))$; therefore, multiplication of polynomials is associative.

Exercise 26. Using summation notation, prove the following properties of polynomial multiplication:

(1) Commutativity: $p(x)q(x) = q(x)p(x)$;

(2) Distributivity across addition: $p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x)$.

$\Diamond$

18.3 The Division Algorithm for Polynomials

In the chapter on modular arithmetic, we used the following fact about integers: for any two integers a and b with $b > 0$, then there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$. This fact was known to the ancient Greeks, who proved it using what's known as the *division algorithm*.[2] It turns out that a similar division algorithm exists for polynomials. In this section we'll give the proof. But first, as usual, some examples.

Example 27. Dividing polynomials is very similar to long division of real numbers. For example, suppose that we divide $x^3 - x^2 + 2x - 3$ by $x - 2$.

$$\begin{array}{rl|lllllll} & & x^2 & + & x & + & 4 & & \\ \cline{3-8} x-2 & \big| & x^3 & - & x^2 & + & 2x & - & 3 \\ & & x^3 & - & 2x^2 & & & & \\ \cline{3-8} & & & & x^2 & + & 2x & - & 3 \\ & & & & x^2 & - & 2x & & \\ \cline{5-8} & & & & & & 4x & - & 3 \\ & & & & & & 4x & - & 8 \\ \cline{6-8} & & & & & & & & 5 \end{array}$$

In the example, we need to take the leading power term of x in the divisor and multiply by something that will make it equal to the the leading power term in the dividend. In this case it is x^2. This gives $x^2 \cdot (x-2) = x^3 - 2x^2$ Subtract from the dividend to yield a remainder of $x^2 + 2x - 3$ and repeat until the remainder is of a degree less than the divisor.

Hence, $x^3 - x^2 + 2x - 3 = (x-2)(x^2 + x + 4) + 5$. And simply multiplying out the right side will show that these are indeed equal. ♦

Example 28. Divide $(2x^3 + 3x^2 + x + 4)$ by $(x + 2)$ where both polynomials are in $\mathbb{Z}_5$.

$$\begin{array}{rl|lllllll} & & 2x^2 & + & 4x & + & 3 & & \\ \cline{3-8} x+2 & \big| & 2x^3 & + & 3x^2 & + & x & + & 4 \\ & & 2x^3 & + & 4x^2 & & & & \\ \cline{3-8} & & & & 4x^2 & + & x & + & 4 \\ & & & & 4x^2 & + & 3x & & \\ \cline{5-8} & & & & & & 3x & + & 4 \\ & & & & & & 3x & + & 1 \\ \cline{6-8} & & & & & & & & 3 \end{array}$$

[2] As we said before, you may find a proof in any book on number theory. Or, take a look at: http://2000clicks.com/mathhelp/NumberTh09EuclidsAlgorithm.aspx.

♦

Exercise 29. Find $q(x)$ and $r(x)$ in the following equations.

(a) $x^2 + 3x + 27 = (x - 2)q(x) + r(x)$

(b) $15x^3 + 13x - 27 = (x - 5)q(x) + r(x)$

(c) $10x^3 - x^2 + 3x + 27 = (2x^2 - 4)q(x) + r(x)$

◊

Exercise 30.

(a) Divide $(3x^6 + x^5 + 4x^4 + 2)$ by $(x + 3)$ where both polynomials are in $\mathbb{Z}_5$.

(b) Divide $(x^7 + x^5 + x^3 + x)$ by $(x + 1)$ where both polynomials are in $\mathbb{Z}_2$.

◊

And now for the proof.

Proposition 31. Let $f(x)$ and $g(x)$ be nonzero polynomials where the degree of $g(x)$ is greater than 0. Then there exists unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

where the degree of $r(x)$ is less than the degree of $g(x)$.

Remark 32. This proposition is true for *any* polynomial ring (according to our definition). You may check the following proof works for any polynomial ring, and not just real polynomials. △

Proof. We will first prove the existence of $q(x)$ and $r(x)$. We define a set S as follows:

$$S = \{f(x) - g(x)h(x), \text{ for all } h(x) \in P(x)\}.$$

This set is nonempty since $f(x) \in S$. Let $r(x)$ be a polynomial of smallest degree in S.[3] This means that there must exist a $q(x)$ such that

$$r(x) = f(x) - g(x)q(x).$$

[3] At this point we can't assume that there's only one such polynomial, so we have to say "a polynomial" rather than "the polynomial".

We need to show that the degree of $r(x)$ is less than the degree of $g(x)$. Let's prove this by contradiction. So we assume the contrary, namely that $\deg g(x) \leq \deg r(x)$. Let n, m be the degree of $g(x), r(x)$ respectively, where $n \leq m$. Then we may write

$$g(x) = a_0 + a_1 x + \cdots + a_n x^n$$

and

$$r(x) = b_0 + b_1 x + \cdots + b_m x^m,$$

where $a_n \neq 0$ and $b_m \neq 0$. Taking a cue from the process of long division, we define a new polynomial $r'(x)$ by

$$r'(x) := r(x) - b_m(a_n^{-1})x^{m-n}g(x)$$

It's tedious to write out all the terms of $r'(x)$. Fortunately, it's not really necessary. We only need to remark that the degree of $r'(x)$ is less than the degree of $r(x)$, since the leading-order terms of $r(x)$ and $b_m(a_n^{-1})x^{m-n}g(x)$ are both $b_m x^m$, so they cancel. We may plug in $r(x) = f(x) - g(x)q(x)$ to obtain

$$\begin{aligned} r'(x) &:= f(x) - g(x)q(x) - b_m(a_n^{-1})x^{m-n}g(x) \\ &= f(x) - g(x)\left(q(x) - b_m(a_n^{-1})x^{m-n}\right). \end{aligned}$$

This shows that $r'(x)$ is also in S (look back at the definition and see!). But $\deg r'(x) < \deg r(x)$, which contradicts our condition that $r(x)$ is an element of S with smallest degree. The rules of proof by contradiction allow us to conclude that our assumption is false: namely, it must be true that $\deg g(x) > \deg r(x)$. This finishes the proof of existence.

To show that $q(x)$ and $r(x)$ are unique, suppose that polynomials $q'(x)$ and $r'(x)$ satisfy $f(x) = g(x)q'(x) + r'(x)$, so that

$$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x).$$

This implies

$$g(x)[q(x) - q'(x)] = r'(x) - r(x).$$

If g is not the zero polynomial, then

$$\deg(g(x)[q(x) - q'(x)]) = \deg(r'(x) - r(x)) \geq \deg g(x).$$

However, the degrees of both $r(x)$ and $r'(x)$ are strictly less than the degree of $g(x)$; therefore, $r(x) = r'(x)$ and $q(x) = q'(x)$. □

18.4 Polynomial roots

The Fundamental Theorem of Algebra (discussed in Section 3.5) asserts that a real polynomial of degree n has at most n roots. You may have learned this before from

previous math classes, but you've probably never seen it proved. Seek no more: the proof is at hand. Not only that–our results will apply to *any* polynomial ring, including $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Q}[x]$, and $\mathbb{Z}_p[x]$.

The following proposition gives us a way to relate polynomial values to polynomial remainders.

Proposition 33. When dividing $f(x)$ by $x - a$, the remainder is $f(a)$.

PROOF. By the division algorithm above, if we divide $f(x)$ by $x-a$, it will produce two unique polynomials $q(x)$ and $r(x)$ such that $f(x) = (x - a)q(x) + r(x)$. Since the degree of $x - a$ is 1, then according to the division algorithm, the degree of $r(x)$ must be less than 1. Therefore $r(x)$ has to be a constant. We will show this replacing $r(x)$ with r where r is an real number. This yields:

$$f(x) = (x - a)q(x) + r.$$

If we set $x = a$ then we get:

$$f(a) = (a - a)q(x) + r \Rightarrow f(a) = 0 \cdot q(x) + r \Rightarrow f(a) = r.$$

□

This proposition can save us a lot of time when finding remainders under division by monomials.

Exercise 34.

(a) Find the remainder when $\sum_{k=1}^{100} kx^{k-1}$ is divided by $x - 1$ and $x + 1$.

(b) Find the remainders when $\sum_{k=0}^{100} \left(\frac{1}{2}\right)^k x^k$ is divided by $x - 1/2$ and $x + 1/2$.

(c) Find the remainders when $\sum_{k=0}^{100} 3^k x^k$ is divided by $x + 1/9$ and $x - 1/9$.

♢

The following proposition in an important special case of Proposition 36.

Proposition 35. a is a root of $f(x)$ if and only if $x - a$ divides $f(x)$.

PROOF. From Proposition 36 $f(x) = (x - a) \cdot q(x) + f(a)$, so $f(a) = 0$ if and only if $f(x) = (x - a) \cdot q(x)$ which is true if and only if $x - a$ divides $f(x)$. □

We will need one more fact in order to prove the Fundamental Theorem of Algebra. From basic algebra, we know that if $ab = 0$ then either $a = 0$ or $b = 0$

(see also Proposition 30 of Chapter 3). It turns out that the same is true for polynomials, as we now show.

Proposition 36. Suppose $F(x)$ is a polynomial ring, and suppose $p(x), q(x) \in F(x)$. Then $p(x)q(x) = 0$ iff either $p(x) = 0$ or $q(x) = 0$.

PROOF. Since this is a "iff" proof, we must actually prove two things:

First we prove the "if" part. It is clear from the formula for multiplication of polynomials that if either $p(x) = 0$ or $q(x) = 0$, then the product $p(x)q(x)$ must also be 0. That was easy!

The "only if" part is harder. We will prove the contrapositive, namely that $p(x) \neq 0$ and $q(x) \neq 0$ implies that $p(x)q(x) \neq 0$. Let

$$p(x) = \sum_{i=0}^{m} a_i x^i \quad \text{and} \quad q(x) = \sum_{j=0}^{n} b_j x^j,$$

where $a_m \neq 0$ and $b_n \neq 0$. We can then write

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k, \quad \text{where} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Consider the coefficient c_{m+n}, which may be expanded out as

$$c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + \ldots + a_m b_n + \cdots + a_{n+m-1} b_1 + a_{n+m} b_0.$$

Take a look at these terms for a moment. Which of them are nonzero? Notice how we've separated out the term $a_m b_n$ in the middle of the expansion. Since $a_m \neq 0$ and $b_n \neq 0$, this term is nonzero. Now, are there any other nonzero terms? All terms have the form $a_i b_j$, and for every other term in the series (besides $a_m b_n$) we have either $i > m$ or $j > n$. If $i > m$ then $a_i = 0$, since the degree of $p(x)$ is m and all coefficients of terms of higher degree are 0. For the same reason, if $j > n$ then $b_j = 0$. It follows that except for the term $a_m b_n$, all other terms $a_i b_j$ are 0, which implies that $c_{m+n} = a_m b_n \neq 0$. But this means that $p(x)q(x)$ has a nonzero term, namely $c_{m+n} x^{m+n}$, so $p(x)q(x) \neq 0$. The proof is completed. □

And here's the result we've been waiting for. Now that we've prepared the ground, it's not so difficult to prove.

Proposition 37. In any polynomial ring, the equation $x^m - c = 0$ has at most m solutions.

PROOF. Suppose a_1 is a solution to $x^m - c = 0$. Then by Proposition 35 it follows that $x - a_1$ divides $x^n - c$. Therefore $x^n - c = (x - a_1) g_{n-1}(x)$ where the degree of $g_{n-1}(x) = n - 1$.

Now if $a_2 \neq a_1$ is another solution then using our above result we have

$$a_2{}^n - c = (a_2 - a_1)g_{n-1}(a_2) = 0.$$

Since $a_2 - a_1 \neq 0$, it follows that $g_{n-1}(a_2) = 0$. So we can write $g_{n-1}(x) = (x - a_2)g_{n-2}(x)$ where the degree of $g_2(x) = n - 2$.

Continuing in the same way, if there are distinct roots $a_1, a_2, ..., a_n$ then

$$x^n - c = (x - a_1)(x - a_2)...(x - a_n)g_0,$$

where the degree of g_0 is 0 (in other words, g_0 is a constant.). So there can't be any more solutions, a_{n+1}, because $(x - a_{n+1})$ doesn't divide g_0. □

18.5 Proof that $U(p)$ is cyclic

Mathematics has many mysterious and wonderful connections. Surprisingly, we can use Proposition 37 to prove something about group theory. Recall that $U(n)$ is the group of units in $\mathbb{Z}_n$, where a "unit" is an element with a multiplicative inverse. If p is a prime, then $U(p)$ is the set of all nonzero elements of $\mathbb{Z}_p$.

Proposition 38. $U(p)$ is cyclic for every prime p.

PROOF. First, notice that Proposition 37 says that there are at most m solutions to the equation $x^m = 1$ in $\mathbb{Z}_p$. Since 0 is not a solution, it follow that all of these solutions are also in $U(p)$.

Also, according to the factorization of Abelian groups (Proposition 93), there exists an isomorphism ϕ:

$$\phi : U(p) \to \mathbb{Z}_{{p_1}^{e_1}} \times \mathbb{Z}_{{p_2}^{e_2}} \times ... \times \mathbb{Z}_{{p_k}^{e_k}},$$

where $p_1, p_2, \ldots, p_k$ are all primes. It's not necessarily true a priori that all of the p_j's are distinct: but if they are, then Proposition 89 tells us that $U(p)$ must be cyclic.

So it LL comes down to proving that all of the p_j's are distinct. We will prove this by contradiction. Thus, we may suppose that $p_i = p_j$ for some $i \neq j$. Now consider the following two elements of the direct product:

$$g_i = (0, \ldots, \underbrace{p_i^{e_i - 1}}_{i'\text{th place}}, \ldots, 0) \quad \text{and} \quad g_j = (0, \ldots, \underbrace{p_j^{e_j - 1}}_{j'\text{th place}}, \ldots, 0).$$

It is then possible to prove that (recall that "$|g|$ " is the order of the group element g)

$$|g_i| = p_i \quad \text{and} \quad |g_j| = p_j.$$

Exercise 39. Given the above definitions of g_i and g_j, show that $|g_i| = p_i$ and $|g_j| = p_j$. (*Hint*) ◊

As a result of the above exercise, Proposition 39 of the Cosets chapter enables us to conclude that

$$|g_i^n| = p_i \quad \text{and} \quad |g_j^n| = p_j \quad \text{for} \quad (n = 1, ..., p_j - 1).$$

Since $p_i = p_j$, we have at least $2(p_i - 1)$ elements in $\mathbb{Z}_{{p_1}^{e_1}} \times \mathbb{Z}_{{p_2}^{e_2}} \times ... \times \mathbb{Z}_{{p_k}^{e_k}}$ of order p_i. By Proposition 50 of the Isomorphisms chapter, this means there are $2(p_i - 1)$ elements of $U(p)$ which have order p_i, and all of these elements are solutions of the equation $x^{p_i} - 1 = 0$ (Why?). But at the beginning of this proof, we demonstrated that there can only be at most p_i solutions. This contradiction shows us our supposition is false, so all of the p_i's in the direct product must be unequal. □

19

Appendix: Induction proofs–patterns and examples

19.1 Basic examples of induction proofs

Below is a complete proof of the formula for the sum of the first n integers, that can serve as a model for proofs of similar sum/product formulas. [1]

Proposition 1. For all $n \in \mathbb{N}$, it is true that

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \qquad (P(n))$$

PROOF. *(By induction)*:

Base case: When $n = 1$, the left side of $P(n)$ is 1, and the right side is $1(1+1)/2 = 1$, so both sides are equal and $(*)$ holds for $n = 1$.

[1] This entire section was ripped off (with permission!) from A. J. Hildebrand's excellent notes on induction (reformatted and minor edits by C.T.).

Induction step: Let $k \in \mathbb{N}$ be given and suppose formula $P(n)$ holds for $n = k$. Then

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \quad \text{(by definition of } \textstyle\sum \text{ notation)} \\ &= \frac{k(k+1)}{2} + (k+1) \quad \text{(by induction hypothesis)} \\ &= \frac{k(k+1) + 2(k+1)}{2} \quad \text{(by algebra)} \\ &= \frac{(k+1)((k+1)+1)}{2} \quad \text{(by algebra).}\end{aligned}$$

Thus, $P(n)$ holds for $n = k + 1$, and the proof of the induction step is complete.

Conclusion: By the principle of induction, we have proved that $P(n)$ holds for all $n \in \mathbb{N}$. □

19.2 Advice on writing up induction proofs

Here are four things to keep in mind as you write up induction proofs.

#1: Begin any induction proof by stating precisely, and prominently, the statement you plan to prove. This statement typically involves an equation (or assertion) in the variable n, and we're trying to prove this equation (or assertion) for all natural numbers n bigger than a certain value. A good idea is to write out the statement and label it as "$P(n)$", so that it's easy to spot, and easy to reference; see the sample proofs for examples.

#2: Be sure to properly begin and end the induction step. From a logical point of view, an induction step is a proof of a statement of the form, "for all $k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$". To prove such a statement, you need to start out by asserting,"let $k \in \mathbb{N}$ be given"), then assume $P(k)$ is true ("Suppose $P(n)$ is true for $n = k$"), and, after a sequence of logical deductions, derive $P(k+1)$ ("Therefore $P(n)$ is true for $n = k + 1$").

#3: Use different letters for the general variable appearing in the statement you seek to prove (n in the above example) and the variable used for the induction step (k in the above example). The reason for this distinction is that in the induction step you want to be able to say something like the following: "Let $k \in \mathbb{N}$ be given, and suppose $P(k)$ .... [Proof of induction step goes here] ... Therefore $P(k+1)$ is true." Without introducing a second variable k, such a statement wouldn't make sense.

#4: Always clearly state, at the appropriate place in the induction step, when the induction hypothesis is being used. E.g., say "By the induction hypthesis we have ...", or use a parenthetical note "(by induction hypothesis)" in

a chain of equations as in the above example. The induction hypothesis is the case $n = k$ of the statement we seek to prove (i.e., the statement "$P(k)$" and it is what you assume at the start of the induction step. The place where this hypothesis is used is the most crucial step in an induction argument, and you must get this hypothesis into play at some point during the proof of the induction step—if not, you are doing something wrong.

19.3 Induction proof patterns & practice problems

Induction proofs, type I: Sum/product formulas

The most common, and the easiest, application of induction is to prove formulas for sums or products of n terms. All of these proofs follow the same pattern.

Examples:

1. $\sum_{i=0}^{n} r^i = \frac{1-r^{n+1}}{1-r}$ $(r \neq 1)$ (sum of finite geometric series)
2. $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$
3. $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ (sum of powers of 2)
4. $\sum_{i=0}^{n} i!i = (n+1)! - 1$.

We will give outlines for parts (a) and (d). Fill in the blanks for (a), and supply the items for (d). Parts (b) and (c) are up to you!

Proof of (a): We seek to show that, for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}. \qquad (\ P(n))$$

Base case: When $n = 1$, the left side of $P(1)$ is equal to ___, and the right side is equal to _____, so both sides are equal and $P(1)$ is true.

Induction step: Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true. Then

$$\begin{aligned}\sum_{i=1}^{k+1} i(i+1) &= \sum_{i=1}^{k} i(i+1) + \_\_\_\_\_ \\ &= \frac{k(k+1)(k+2)}{3} + \_\_\_\_\_ \quad \text{(by induction hypothesis)} \\ &= \frac{(k+1)(k+2)(k+3)}{3}.\end{aligned}$$

Thus, $P(\_\_$ holds, and the proof of the induction step is complete.

Conclusion: By the principle of induction, it follows that ___ is true for all $n \in \mathbb{N}$. □

Proof of (d):

(i) What is the equation that must be shown for all $n \in \mathbb{N}$? (Call this equation "$P(n)$").

(ii) Identify the base case, and show that equation $P(n)$ holds for the base case.

(iii) Write the left-hand side of $P(k+1)$.

(iv) Separate off the last term in the sum, so that you have a sum from 1 to k plus an additional term.

(v) Use the induction hypothesis to replace the sum from 1 to k with a simpler expression.

(vi) Use algebra to obtain $P(k+1)$, which completes the proof of the induction step.

Conclusion: By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$.

□

Induction proofs, type II: Inequalities

A second general type of application of induction is to prove inequalities involving a natural number n. These proofs also tend to be on the routine side; in fact, the algebra required is usually very minimal, in contrast to some of the summation formulas.

In some cases the inequalities don't "kick in" until n is large enough. By checking the first few values of n one can usually quickly determine the first n-value, say n_0, for which the inequality holds. Induction with $n = n_0$ as base case

Examples:

1. $2^n > n$
2. $2^n \geq n^2$ $(n \geq 4)$
3. $n! > 2^n$ $(n \geq 4)$
4. $(1-x)^n \geq 1 - nx$ $(0 < x < 1)$
5. $(1+x)^n \geq 1 + nx$ $(x > 0)$

We will give outlines for (c) and (d). The other inequalities can be proved similarly.

Proof of (c): A direct check of the inequality for the first few values of n shows that the inequality fails for $n = 1, 2, 3$. But this doesn't matter, because we only have to show that it works for for all n from 4 onwards.

We are trying to show that

$$n! > 2^n \qquad (P(n))$$

holds for all $n \geq 4$.

Base case: For $n = 4$, the left and right sides of $P(4)$ are equal to __ and ___, respectively, so $P(4)$ is true.

Induction step: Let $k \geq 4$ be given and suppose ____ is true. Then

$$\begin{aligned}(k+1)! &= k! \cdot (k+1) \\ &> 2^k \cdot \_\_\_ \quad (\text{by } \_\_\_\_\_) \\ &\geq 2^k \cdot 2 \quad (\text{since } k \geq 4 \text{ and so } k+1 \geq 2)) \\ &= \_\_\_\_.\end{aligned}$$

Thus, ___ holds, and the proof of the induction step is complete.

Conclusion: By the principle of induction, it follows that $P(n)$ is true for all $n \geq 4$. □

Proof of (d):

(i) What statement do you need to prove for every real number $0 < x < 1$ and any $n \in \mathbb{N}$? Call this statement "$P(n)$".

(ii) **Base case:** Show that the left and right sides of $P(n)$ are equal in the base case.

(iii) **Induction step:** Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true for any real number $0 < x < 1$. What do we seek to show?

(iv) Rewrite $(1-x)^{k+1}$ as $(1-x)^k \cdot (1-x)$. Then use $(*)$ for $n = k$ to obtain an inequality. Using basic algebra, simplify the right-hand side until you obtain a quantity that is greater than $1 - (k+1)x$.

(v) What may you conclude about $P(k+1)$?

Conclusion: By the principle of induction, it follows that $P(n)$ holds for all $n \in \mathbb{N}$. □

Induction proofs, type III: Extension of theorems from 2 variables to n variables

Another very common and usually routine application of induction is to extend general results that have been proved for the case of 2 variables to the case of n variables. Below are some examples. In proving these results, use the case $n = 2$ as base case. To see how to carry out the general induction step (from the case $n = k$ to $n = k+1$), it may be helpful to first try to see how get from the base case $n = 2$ to the next case $n = 3$.

Examples:

1. Show that if $x_1, \ldots, x_n$ are odd, then $x_1 x_2 \ldots x_n$ is odd. (Use the fact (proved earlier) that the product of two odd numbers is odd, as starting point, and use induction to extend this result to the product of n odd numbers.)

2. Show that if a_i and b_i $(i = 1, 2, \ldots, n)$ are real numbers such that $a_i \leq b_i$ for all i, then
$$\sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} b_i.$$
(Use the fact (from Chapter 1) that $a \leq b$ and $c \leq d$ implies $a + c \leq b + d$.)

3. Show that if $x_1, \ldots, x_n$ are real numbers, then
$$\left| \sin\left(\sum_{i=1}^{n} x_i \right) \right| \leq \sum_{i=1}^{n} |\sin x_i| .$$
(Use the trig identity for $\sin(\alpha + \beta)$.)

4. Show that if $A_1, \ldots, A_n$ are sets, then
$$(A_1 \cup \cdots \cup A_n)^c = A_1^c \cap \cdots \cap A_n^c.$$
(This is a generalization of De Morgan's Law to unions of n sets. Use De Morgan's Law for two sets ($(A \cup B)^c = A^c \cap B^c$) and induction to prove this result.)

We'll give outlines of the proofs of (a) and (b):

Proof of (a): We will prove by induction on n the following statement:

If $x_1, \ldots, x_n$ are odd numbers, then $x_1 x_2 \ldots x_n$ is odd. $(P(n))$

We will use the following fact (proved earlier):

If x and y are odd, then xy is odd. $(**)$

Base case: For $n = 1$, the product $x_1 \dots x_n$ reduces to ___, which is odd whenever x_1 is odd. Hence $P(n)$ is true for $n = 1$.

Induction step.

- Let $k \geq 1$, and suppose $(*)$ is true for $n = k$, i.e., suppose that any product of __ odd numbers is again odd.
- We seek to show that ___ is true, i.e., that any product of __ odd numbers is odd.
- Let $x_1, \dots, x_{k+1}$ be odd numbers.
- Applying the induction hypothesis to $x_1, \dots, x_k$, we obtain that the product ____ is odd.
- Since x_{k+1} is __ and, by $(**)$, the product of two odd numbers is again odd, it follows that $x_1 x_2 \dots x_{k+1} = (x_1 \dots x_k)x_{k+1}$ is odd.
- As $x_1, \dots, x_{k+1}$ were arbitrary odd numbers, we have proved ___, so the induction step is complete.

Conclusion: By the principle of induction, it follows that $(*)$ is true for all $n \in \mathbb{N}$. □

Proof of (b):

(i) What statement do we want to prove for all natural numbers n and for all real numbers a_i and b_i $(i = 1, \dots, n)$ such that $a_i \leq b_i$? Call this statement "P(n)". (Note that the condition "for all real numbers a_i and b_i" must be part of the induction statement we seek to prove.)

(ii) **Base case:** Show that $P(1)$ is true.

(iii) **Induction step:** Let $k \geq 1$. Write $P(k)$.

(iv) What do you seek to prove?

(v) (Fill in the blanks) Let $a_1, \dots, a_{k+1}$ and $b_1, \dots, b_{k+1}$ be given real numbers such that ___ for each i.

(vi) Then

$$\sum_{i=1}^{k+1} a_i = \_\_\_ + a_{k+1}.$$

(vii) Use basic algebra to show that $P(k+1)$ and the given numbers $a_1, \dots, a_{k+1}$ and $b_1, \dots, b_{k+1}$.

(viii) What may we conclude?

Conclusion: By the principle of induction, it follows that $P(n)$ is true for all $n \in \mathbb{N}$. □

19.4 Strong Induction, with applications

One of the most common applications of induction is to problems involving recurrence sequences such as the Fibonacci numbers, and to representation problems such as the representation of integers as a product of primes (Fundamental Theorem of Arithmetic), sums of powers of 2 (binary representation), and sums of stamp denominations (postage stamp problem).

In applications of this type, the case $n = k$ in the induction step is not enough to deduce the case $n = k+1$; one usually needs additional predecessors predecessors to get the induction step to work, e.g., the two preceding cases $n = k$ and $n = k-1$, or *all* preceding cases $n = k, k-1, \ldots, 1$. This variation of the induction method is called **strong induction**. The induction principle remains valid in this modified form.

Strong induction and recurrences

In the induction proofs we've looked at so far, we first had to prove a base case, and then used a preceding case ($n = k$) to prove the case $n = k+1$ in the induction step. But when we aply induction to two-term recurrence sequences like the Fibonacci numbers, we'll need *two* preceding cases, $n = k$ and $n = k - 1$, in the induction step, and *two* base cases (e.g., $n = 1$ and $n = 2$) to get the induction going. The logical structure of such a proof is of the following form:

Base step: $P(n)$ is true for $n = 1, 2$.

Induction step: Let $k \in \mathbb{N}$ with $k \geq 2$ be given and assume $P(n)$ holds for $n = k$ and $n = k - 1$.

[... Work goes here ...]

Therefore $P(n)$ holds for $n = k + 1$.

Conclusion: By the principle of strong induction, $P(n)$ holds for all $n \in \mathbb{N}$.

Note that in the induction step, one could also say "Assume $P(n)$ holds for " $n = 1, 2, \ldots, k$"; this is a bit redundant as only the last two of the cases $n = 1, 2, \ldots, k$ are needed, though logically correct.

Here is a worked-out example of a proof by strong induction.

Proposition 2. Let a_n be the sequence defined by $a_1 = 1$, $a_2 = 8$, and $a_n = a_{n-1} + 2a_{n-2}$ for $n \geq 3$. Then $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ for all $n \in \mathbb{N}$.

PROOF. We'll prove by strong induction that, for all $n \in \mathbb{N}$,

$$a_n = 3 \cdot 2^{n-1} + 2(-1)^n. \qquad (P(n))$$

Base case: When $n = 1$, the left side of $P(1)$ is $a_1 = 1$, and the right side is $3 \cdot 2^0 + 2 \cdot (-1)^1 = 1$, so both sides are equal and $P(1)$ is true.

When $n = 2$, the left and right sides of $P(2)$ are $a_2 = 8$ and $3 \cdot 2^1 + 2 \cdot (-1)^2 = 8$, so $P(2)$ also holds.

Induction step: Let $k \in \mathbb{N}$ with $k \geq 2$ be given and suppose $P(n)$ is true for $n = 1, 2, \ldots, k$. Then

$$\begin{aligned} a_{k+1} &= a_k + 2a_{k-1} \quad \text{(by recurrence for } a_n\text{)} \\ &= 3 \cdot 2^{k-1} + 2 \cdot (-1)^k + 2\left(3 \cdot 2^{k-2} + 2 \cdot (-1)^{k-1}\right) \quad \text{(by } P(k) \text{ and } P(k-1)\text{)} \\ &= 3 \cdot \left(2^{k-1} + 2^{k-1}\right) + 2\left((-1)^k + 2(-1)^{k-1}\right) \quad \text{(by algebra)} \\ &= 3 \cdot 2^k + 2(-1)^{k+1} \quad \text{(more algebra).} \end{aligned}$$

Thus, $P(k+1))$ holds, and the proof of the induction step is complete.

Conclusion: By the strong induction principle, it follows that $P(n)$ is true for all $n \in \mathbb{N}$. □

Strong Induction and representation problems

For applications to representation problems one typically requires the induction hypothesis in its strongest possible form, where one assumes *all* preceding cases (i.e., for $n = 1, 2, \ldots, k$) instead of just the immediate predecessor (as in simple induction) or two predecessors (as in strong induction applied to two-term recurrences).

Below is a classic example of this type, a proof that every integer ≥ 2 can be written as a product of prime numbers. This is the existence part of what is called the Fundamental Theorem of Arithmetic; the other part guarantees uniquess of the representation, which we will not be concerned with here.

The precise definitions of "prime" and "composite" are as follows: An integer $n \geq 2$ is called **composite** if it can be written as $n = ab$ with integers a, b satisfying $2 \leq a, b < n$. An integer $n \geq 2$ is called **prime** if it cannot be factored in this way. (Only integers ≥ 2 are classified in this way. In particular, the number 1 is neither prime nor composite.)

Using these definitions, we may now state and prove:

Proposition 3. *(Fundamental Theorem of Arithmetic: existence)*

Any integer $n \geq 2$ is either a prime or can be represented as a product of (not necessarily distinct) primes, i.e., in the form $n = p_1 p_2 \ldots p_r$, where the p_i are primes.

PROOF. We will prove by strong induction that the following statement holds for all integers $n \geq 2$.

$$n \text{ can be represented as a product of one or more primes.} \qquad (P(n))$$

Base case: The integer $n = 2$ is a prime since it cannot be written as a product ab, with integers $a, b \geq 2$, so $P(n)$ holds for $n = 2$.

Induction step:

- Let $k \geq 2$ be given and suppose $P(n)$ is true for all integers $2 \leq n \leq k$, i.e., suppose that all such n can be represented as a product of one or more primes.
- We seek to show that $k + 1$ also has a representation of this form.
- If $k + 1$ itself is prime, then $P(n)$ holds for $n = k + 1$, and we are done.
- Now consider the case when $k + 1$ is composite.
- By definition, this means that $k + 1$ can be written in the form $k + 1 = ab$, where a and b are integers satisfying $2 \leq a, b < k + 1$, i.e., $2 \leq a, b \leq k$.
- Since $2 \leq a, b \leq k$, the induction hypothesis can be applied to a and b and shows that a and b can be represented as products of one or more primes.
- Multiplying these two representations gives a representation of $k + 1$ as a product of primes.
- Hence $k + 1$ has a representation of the desired form, so $P(n)$ holds for $n = k + 1$, and the induction step is complete.

Conclusion: By the strong induction principle, it follows that $P(n)$ is true for all $n \geq 2$, i.e., every integer $n \geq 2$ is either a prime or can be represented as a product of primes. □

19.5 More advice on induction and strong induction proofs

Should I use ordinary induction or strong induction? With some standard types of problems (e.g., sum formulas) it is clear ahead of time what type of induction is *likely* to be required, but usually this question answers itself during the exploratory/scratch phase of the argument. In the induction step you will need to reach the $k + 1$ case, and you should ask yourself which of the previous cases you need to get there. If all you need to prove the $k + 1$ case is the case k of the statement, then ordinary induction is appropriate. If two preceding cases, $k - 1$ and k, are necessary to get to $k+1$, then (a weak form of) strong induction is appropriate. If one needs the full range of preceding cases (i.e., all cases $n = 1, 2, \ldots, k$), then the full force of strong induction is needed.

How many base cases are needed? The number of base cases to be checked depends on how far back one needs to "look" in the induction step. In standard induction proofs (e.g., for summation formulas) the induction step requires only the

immediately preceding case (i.e., the case $n = k$), so a single base case is enough to start the induction.

- For Fibonacci-type problems, the induction step usually requires the result for the two preceding cases, $n = k$ and $n = k - 1$. To get the induction started, one therefore needs to know the result for two consecutive cases, e.g., $n = 1$ and $n = 2$.
- In postage stamp type problems, getting the result for $n = k + 1$ might require knowing the result for $n = k - 2$ and $n = k - 6$, say. This amounts to "looking back" 7 steps (namely $n = k, k - 1, \ldots, k - 6$), so 7 consecutive cases are needed to get the induction started.
- On the other hand, in problems involving the full strength of the strong induction hypothesis (i.e., if in the induction step one needs to assume the result for *all* preceding cases $n = k, k - 1, \ldots, 1$), a single base case may be sufficient. An example is the Fundamental Theorem of Arithmetic.

How do I write the induction step? As in the case of ordinary induction, at the beginning of the induction step *state precisely what you are assuming, including any constraints on the induction variable k*. Without an explicitly stated assumption, the argument is incomplete. The appropriate induction hypothesis depends on the nature of the problem and the type of induction used. Here are some common ways to start out an induction step:

- "Let $k \in \mathbb{N}$ be given and assume $P(k)$ is true." (typical form for standard induction proofs)
- "Let $k \geq 2$ be given and assume $P(n)$ holds for $n = k - 1$ and $n = k$." (typical form for induction involving recurrences)
- "Let $k \in \mathbb{N}$ be given and assume $P(n)$ holds for $n = 1, 2, \ldots, k$." (typical form for representation problems)

19.6 Common mistakes

The following examples illustrate some common mistakes in setting up base case(s) and the induction step.

Example 1.

- **Base step:** $n = 3$.
- **Induction step:** Let $k \in \mathbb{N}$ with $k \geq 3$ be given and assume $(*)$ is true for $n = k$ and $n = k - 1$.

- **Comment: BAD:** When $k = 3$ (the first case of the induction step), the induction step requires the cases 3 and 2, but only 2 is covered in the base step.
  FIX: Add the case $n = 2$ to the base step.

Example 2.

- **Base step:** $n = 1$ and $n = 2$.
- **Induction step:** Let $k \in \mathbb{N}$ with $k > 2$ be given and assume $P(n)$ is true for $n = k$ and $n = k - 1$.
- **Comment: BAD.** Gap between base case and the first case of the induction step: The first case $k = 3$ of the induction step requires the cases 3 and 2, but the base step only gives the cases 1 and 2.
  FIX: Start induction step at $k = 2$ rather than $k = 3$: "Let $k \in \mathbb{N}$ with $k \geq 2$ be given ..."

Example 3.

- **Base step:** $n = 1$ and $n = 2$.
- **Induction step:** Assume $P(n)$ is true for $n = k$ and $n = k - 1$. Then ...
- **Comment: BAD.** The variable k in the induction step is not quantified.
  FIX: Add "Let $k \in \mathbb{N}$ with $k \geq 2$ be given."

Example 4.

- **Base step:** $n = 1$ and $n = 2$.
- **Induction step:** Let $k \in \mathbb{N}$ be given and assume $P(n)$ is true for $n = k$ and $n = k - 1$.
- **Comment: BAD.** Here the first case induction step is $k = 1$, with the induction hypothesis being the cases $n = k$ and $n = k - 1$. But when $k = 1$, the second of these cases, $n = k - 1 = 0$, is out of range.
  FIX: Add the restriction $k \geq 2$ to the induction step: "Let $k \in \mathbb{N}$ with $k \geq 2$ be given."

19.7 Strong induction practice problems

1. **Recurrences:** The first few problems deal with properties of the Fibonacci sequence and related recurrence sequences. The Fibonacci sequence is defined by $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Its first few terms are $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$.

   In the following problems, use an appropriate form of induction (standard induction or strong induction) to establish the desired properties and formulas. (Note that some of these problems require only ordinary induction.)

(a) **Fibonacci sums:** Prove that $\sum_{i=1}^{n} F_i = F_{n+2} - 1$ for all $n \in \mathbb{N}$.

(b) **Fibonacci matrix:** Show that, for all $n \in \mathbb{N}$,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}. \qquad (P(n))$$

(c) **Odd/even Fibonacci numbers:** Prove that the Fibonacci numbers follow the pattern odd,odd,even: that is, show that for any positive integer m, F_{3m-2} and F_{3m-1} are odd and F_{3m} is even.

(d) **Inequalities for recurrence sequences:** Let the sequence T_n ("Tribonacci sequence") be defined by $T_1 = T_2 = T_3 = 1$ and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 4$. Prove that

$$T_n < 2^n \qquad (P(n))$$

holds for all $n \in \mathbb{N}$.

We'll give an outline for the proof of (d).

We will prove $P(n)$ by strong induction.

Base step: For $n = 1, 2, 3$, T_n is equal to __, whereas the right-hand side of $P(n)$ is equal to $2^1 = 2$, $2^2 = 4$, and $2^3 = 8$, respectively. Thus, $P(n)$ holds for $n = 1, 2, 3$.

Induction step: Let $k \geq 3$ be given and suppose $P(n)$ is true for all $n = 1, 2, \ldots, k$. Then

$$\begin{aligned} T_{k+1} &= T_k + T_{k-1} + \_\_ \quad \text{(by recurrence for } T_n\text{)} \\ &< 2^k + 2^{k-1} + \_\_ \quad \text{(strong ind. hyp. \& } (P(k), P(k-1), P(k-2))\text{)} \\ &= 2^{k+1}\left(\frac{1}{2} + \frac{1}{4} + \_\_\right) \\ &= 2^{k+1} \cdot \_\_ < 2^{k+1}. \end{aligned}$$

Thus, ____ holds, and the proof of the induction step is complete.

Conclusion: By the strong induction principle, it follows that $P(n)$ is true for all $n \in \mathbb{N}$.

2. **Representation problems.** One of the main applications of strong induction is to prove the existence of representations of integers of various types. In these applications, strong induction is usually needed in its full force, i.e., in the induction step, one needs to assume that all predecessor cases $n = 1, 2, \ldots, k$.

(a) **The postage stamp problem:** Determine which postage amounts can be created using the stamps of 3 and 7 cents. In other words, determine the exact set of positive integers n that can be written in the form $n = 3x + 7y$ with x and y nonnegative integers. (*Hint*: Check the

first few values of n directly, then use strong induction to show that, from a certain point n_0 onwards, all numbers n have such a representation.)

(b) **Binary representation:** Using strong induction prove that every positive integer n can be represented as a sum of *distinct* powers of 2, i.e., in the form $n = 2^{i_1} + \cdots + 2^{i_h}$ with integers $0 \leq i_1 < \cdots < i_h$. (*Hint*: To ensure distinctness, use the *largest* power of 2 as the first "building block" in the induction step.)

(c) **Factorial representation.** Show that any integer $n \geq 1$ has a represention in the form $n = d_1 1! + d_2 2! + \cdots + d_r r!$ with "digits" d_i in the range $d_i \in \{0, 1, \ldots, i\}$. (*Hint*: Use again the "greedy" trick (pick the largest factorial that "fits" as your first building block), and use the fact (established in an earlier problem) that $\sum_{i=1}^{k} i!i = (k+1)! - 1$.)

19.8 Non-formula induction proofs.

Below is a sample proof of the statement that any n-element set (i.e., any set with n elements) has 2^n subsets. This illustrates a case where the result we seek to prove is not a formula, but a statement that must be expressed verbally, and where the induction step requires some verbal explanation, and not just a chain of equalities. Additional practice problems follow below.

Proposition 4. For all $n \in \mathbb{N}$, the following holds:

$$\text{Any } n\text{-element set has } 2^n \text{ subsets.} \qquad (P(n))$$

PROOF.(*By induction*):

Base case: Since any 1-element set has 2 subsets, namely the empty set and the set itself, and $2^1 = 2$, the statement $P(n)$ is true for $n = 1$.

Induction step:

- Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true, i.e., that any k-element set has 2^k subsets. We seek to show that $P(k+1)$ is true as well, i.e., that any $(k+1)$-element set has 2^{k+1} subsets.
- Let A be a set with $k+1$ elements.
- Let a be an element of A, and let $A' = A - \{a\}$ (so that A' is a set with k elements).
- We classify the subsets of A into two types: (I) subsets that do *not* contain a, and (II) subsets that do contain a.

- The subsets of type (I) are exactly the subsets of the set A'. Since A' has k elements, the induction hypothesis can be applied to this set and we conclude that there are 2^k subsets of type (I).
- The subsets of type (II) are exactly the sets of the form $B = B' \cup \{a\}$, where B' is a subset of A'. By the induction hypothesis there are 2^k such sets B', and hence 2^k subsets of type (II).
- Since there are 2^k subsets of each of the two types, the total number of subsets of A is $2^k + 2^k = 2^{k+1}$.
- Since A was an arbitrary $(k+1)$-element set, we have proved that any $(k+1)$-element set has 2^{k+1} subsets. Thus $P(k+1)$ is true, completing the induction step.

Conclusion: By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

19.9 Practice problems for non-formula induction

1. **Number of subsets with an even (or odd) number of elements:** Using induction, prove that an n-element set has 2^{n-1} subsets with an even number of elements and 2^{n-1} subsets with an odd number of elements.
2. **Number of regions created by n lines:** How many regions are created by n lines in the plane such that no two lines are parallel and no three lines intersect at the same point? Guess the answer from the first few cases, then use induction to prove your guess.
3. **Sum of angles in a polygon:** The sum of the interior angles in a triangle is 180 degrees, or π. Using this result and induction, prove that for any $n \geq 3$, the sum of the interior angles in an n-sided polygon is $(n-2)\pi$.
4. **Pie-throwing problem:** Here is a harder, but fun problem. Consider a group of n fraternity members standing in a yard, such that their mutual distances are all distinct. Suppose each of throws a pie at his nearest neighbor. Show that if n is odd, then there is one person in the group who does not get hit by a pie. (*Hint*: Let $n = 2m + 1$ with $m \in \mathbb{N}$, and use m as the induction variable. Consider first some small cases, e.g., $n = 3$ and $n = 5$.)

19.10 Fallacies and pitfalls

By now, induction proofs should feel routine to you, to the point that you could almost do them in your sleep. However, it is important not to become complacent and careless, for example, by skipping seemingly minor details in the write-up, omitting quantifiers, or neglecting to check conditions and hypotheses.

Below are some examples of false induction proofs that illustrate what can happen when some minor details are left out. In each case, the statement claimed is clearly nonsensical (e.g., that all numbers are equal), but the induction argument sounds perfectly fine, and in some cases the errors are quite subtle and hard to spot. Try to find them!

Example 5. Let us "prove" that for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{1}{2}(n + \frac{1}{2})^2 \qquad (P(n))$$

Proof: We prove the claim by induction.

Base step: When $n = 1$, $P(n)$ holds.

Induction step: Let $k \in \mathbb{N}$ and suppose $(*)$ holds for $n = k$. Then

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\
&= \frac{1}{2}\left(k + \frac{1}{2}\right)^2 + (k+1) \quad \text{(by ind. hypothesis)} \\
&= \frac{1}{2}\left(k^2 + k + \frac{1}{4} + 2k + 2\right) \quad \text{(by algebra)} \\
&= \frac{1}{2}\left(\left(k + 1 + \frac{1}{2}\right)^2 - 3k - \frac{9}{4} + k + \frac{1}{4} + 2k + 2\right) \quad \text{(more algebra)} \\
&= \frac{1}{2}\left((k+1) + \frac{1}{2}\right)^2 \quad \text{(simplifying).}
\end{aligned}$$

Thus, $P(n)$ holds for $n = k + 1$, so the induction step is complete.

Conclusion: By the principle of induction, $P(n)$ holds for all $n \in \mathbb{N}$. ♦

Example 6. Now we will "prove" that all real numbers are equal. To prove the claim, we will prove by induction that, for all $n \in \mathbb{N}$, the following statement holds:

For any real numbers $a_1, a_2, \ldots, a_n$, we have $a_1 = a_2 = \cdots = a_n$. $\qquad (P(n))$

Base step: When $n = 1$, the statement is trivially true, so $P(1)$ holds.

Induction step: Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true, i.e., that any k real numbers must be equal. We seek to show that $P(k + 1)$ is true as well, i.e., that any $k + 1$ real numbers must also be equal.

Let $a_1, a_2, \ldots, a_{k+1}$ be given real numbers. Applying the induction hypothesis to the first k of these numbers, $a_1, a_2, \ldots, a_k$, we obtain

$$a_1 = a_2 = \cdots = a_k. \tag{1}$$

Similarly, applying the induction hypothesis to the last k of these numbers, $a_2, a_3, \ldots, a_k, a_{k+1}$, we get

$$a_2 = a_3 = \cdots = a_k = a_{k+1}. \tag{2}$$

Combining (1) and (2) gives

$$a_1 = a_2 = \cdots = a_k = a_{k+1}, \tag{3}$$

so the numbers $a_1, a_2, \ldots, a_{k+1}$ are equal. Thus, we have proved $P(k+1)$, and the induction step is complete.

Conclusion: By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. Thus, any n real numbers must be equal. ♦

Example 7. Here is a "proof" that for every nonnegative integer n,

$$5n = 0. \qquad (P(n))$$

Proof: We prove that $P(n)$ holds for all $n = 0, 1, 2, \ldots$, using strong induction with the case $n = 0$ as base case.

Base step: When $n = 0$, $5n = 5 \cdot 0 = 0$, so $(*)$ holds in this case.

Induction step: Suppose $P(n)$ is true for all integers n in the range $0 \leq n \leq k$, i.e., that for all integers in this range $5n = 0$. We will show that $P(k+1)$ also holds, so that

$$5(k+1) = 0. \qquad (P(k+1))$$

Write $k + 1 = i + j$ with integers i, j satisfying $0 \leq i, j \leq k$. Applying the induction hypothesis to i and j, we get $5i = 0$ and $5j = 0$. Then

$$5(k+1) = 5(i+j) = 5i + 5j = 0 + 0 = 0,$$

proving $P(k+1)$. Hence the induction step is complete.

Conclusion: By the principle of strong induction, $P(n)$ holds for all nonnegative integers n. ♦

Example 8. Let's "prove" that for every nonnegative integer n,

$$2^n = 1 \qquad (P(n))$$

Proof: We prove that $(*)$ holds for all $n = 0, 1, 2, \ldots$, using strong induction with the case $n = 0$ as base case.

Base step: When $n = 0$, $2^0 = 1$, so $P(0)$ holds. (Note: it is perfectly OK to begin with a base case of $n = 0$.)

Induction step: Suppose $P(n)$ is true for all integers n in the range $0 \leq n \leq k$, i.e., assume that for all integers in this range $2^n = 1$. We will show that $P(k+1)$ also holds, i.e.,

$$2^n = 1 \qquad (P(k+1))$$

We have

$$\begin{aligned} 2^{k+1} &= \frac{2^{2k}}{2^{k-1}} && \text{(by algebra)} \\ &= \frac{2^k \cdot 2^k}{2^{k-1}} && \text{(by algebra)} \\ &= \frac{1 \cdot 1}{1} && \text{(by strong ind. hypothesis applied to each term)} \\ &= 1 && \text{(simplifying),} \end{aligned}$$

proving $P(k+1)$. Hence the induction step is complete.

Conclusion: By the principle of strong induction, $P(n)$ holds for all nonnegative integers n. ♦

Example 9. We will "prove" that all positive integers are equal. To prove this claim, we will prove by induction that, for all $n \in \mathbb{N}$, the following statement holds:

$$\text{For any } x, y \in \mathbb{N}, \text{ if } \max(x, y) = n, \text{ then } x = y. \qquad (P(n))$$

(Here $\max(x, y)$ denotes the larger of the two numbers x and y, or the common value if both are equal.)

Base step: When $n = 1$, the condition in $P(1)$ becomes $\max(x, y) = 1$. But this forces $x = 1$ and $y = 1$, and hence $x = y$.

Induction step: Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true. We seek to show that $P(k+1)$ is true as well.

Let $x, y \in \mathbb{N}$ such that $\max(x, y) = k+1$. Then $\max(x-1, y-1) = \max(x, y) - 1 = (k+1) - 1 = k$. By the induction hypothesis, it follows that $x - 1 = y - 1$, and therefore $x = y$. This proves $P(k+1)$, so the induction step is complete.

Conclusion: By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. In particular, since $\max(1, n) = n$ for any positive integer n, it follows that $1 = n$ for any positive integer n. Thus, all positive integers must be equal to 1 ♦

20

Hints

20.1 Hints for "Complex Numbers" exercises

Exercise 8(b) Start your proof this way: "Given that m is an integer and m^2 is even. Suppose that m is odd. Then ..." (complete the proof by obtaining a contradiction. You should make use of part (a) in your proof.

Exercise 8(c) The proof is similar to that in (b). What modifications do you need to make?

Exercise 17(a) Start out your proof this way: "Let x be the cube root of 2. Then x satisfies the equation $x^3 = 2$." For the rest of the proof, follow closely the proof of Proposition 9. (Or use the statement−reason format, if you prefer.

Exercise 11 Since $3|n$, it follows that $n = 3j$ for some integer j. Obtain a similar equation from $4|m$, and multiply your equations together.

Exercise 12 Since $n|4m$, it follows that $4m = n \cdot j$ for some integer j. Since $12|n$, then what can you substitute for n?

Exercise 18 Try using contradiction. If n is even, then $n = 2k$ for some integer k.

Exercise 26 To show $zz^{-1} = 1$, rewrite z^{-1} as $(a - bi) \cdot \frac{1}{a^2+b^2}$. This is justified by the distributive law. Remember also that showing $z^{-1}z = 1$ requires its own proof.

Exercise 27(i) In the answer $x + yi$, x and y both turn out to be integers!

Exercise 27(n) Yes, you can do it! Find the first few powers of i, and see the pattern.

Exercise 27(o) It's easiest to compute $(1 + i)^2 \cdot (1 + i)^2$.

Exercise 28 If you have trouble with this one, do some examples.

Exercise 41(f) Use part (e).

Exercise 41(g) and (h) See Exercise 26.

Exercise 43 Use part (b) of the previous exercise, plus some of the results from Exercise 41.

Exercise 44(a) Use the formula $|w|^2 = w \cdot \overline{w}$. (d) This one requires calculus.

Exercise 63 Just make minor changes to the previous exercise.

Exercise 68(b) Use a basic identity involving cosine and sine.

Exercise 74(b) What left shifts will change a cosine curve into a sine curve?

Exercise 75 Use Proposition 53 to evaluate $\operatorname{cis}\theta \cdot \operatorname{cis}(t)$, and recall that $\operatorname{cis}(\alpha)$ means the same as as $\cos(\alpha) + i\sin(\alpha)$.

Exercise 84(a) We have already shown in Proposition 30 that the product of two nonzero complex numbers is never equal to 0. Use this to show that the product of four nonzero complex numbers is never equal to 0.

Exercise 84(b) Multiply out the inequality that you proved in (a).

Exercise 85(a) It's easier to multiply the numbers in polar form, you don't have to convert to Cartesian. Note that $\operatorname{cis}\left(\frac{4\pi}{3}\right)$ is the complex conjugate of $\operatorname{cis}\left(\frac{2\pi}{3}\right)$.

Exercise 94(c) Note that $OA = |z|, OC = |w|.$ and $AC = |z - w|$.

Exercise 95(c) Use your answer to part (b).

Exercise 97(c) To find the polar form of this number, try squaring it.

Exercise 100(b) If r is a solution to the above equation, then $z - r$ divides $z^4 + a_3z^3 + a_2z^2 + a_1z + a_0$.

Exercise 101 Let M be the number of distinct solutions with positive imaginary part. Then how many distinct solutions are there with negative imaginary part? And how many non-real solutions are there altogether?

20.2 Hints for "Modular Arithmetic" exercises

Exercise 20: Use the alternative definition of modular equivalence in Proposition 18.

Exercise 29(f): Prove by contradiction: suppose the codes $d_1, d_2, \ldots d_{10}$ and $e_1, e_2, \ldots e_{10}$ are both valid, and suppose that all digits are equal except for the n'th digit (so $d_n \neq e_n$). There are two cases: (a) n is even; (b) n is odd. In case (a), show that this implies $e_n - d_n \equiv 0 \pmod{10}$, and derive a contradiction. Prove case (b) similarly.

Exercise 30(d): Use the fact that $10 \equiv -1 \pmod{11}$.

Exercise 30(i): Prove by contradiction: Suppose the codes $d_1, d_2, \ldots d_{10}$ and $e_1, e_2, \ldots e_{10}$ are both valid, and suppose that all digits are equal except for the n'th digit (so $d_n \neq e_n$). Show that $d_n - e_n$ satisfies $(d_n - e_n)n \equiv 0 \pmod{11}$, and show that the only solution is $d_n - e_n = 0$.

Exercise 30(j): Suppose the code $d_1, d_2, \ldots d_{10}$ is valid, and suppose the code is still valid when the digits d_n and d_{n+1} are exchanged. Write down two modular equations, and take the difference between the two modular equations. Use this to find an equation involving d_n and d_{n+1}.

Exercise 40(c): Find a *negative* number that is equivalent to 856 (mod 123).

Exercise 46(a): You will need to use Proposition 43 twice.

Exercise 52: Use the definitions of $\oplus$ and $\odot$.

Exercise 53: Be careful about 0!

Exercise 58(b)(i): Use the fact that $0 < a < n$.

Exercise 64(a): What is the inverse of 0?

Exercise 78(a): The left-hand side is always even, no matter what m and n are.

Exercise 80: Use Proposition 72.

Exercise 84: Use Proposition 79.

Exercise 86(a): Use Proposition 79. (b): p must divide the left-hand side of the multiplied equation (explain why). (c): Consider two cases (I) a is relatively prime to p; (II) a is not relatively prime to p.

Exercise 93: Use Proposition 83.

Exercise 94: Use the previous exercise.

Exercise 96(c): Follow the method used in the Chinese Remainder Theorem, and for each modular equivalence obtained show that a solution exists.

20.3 Hints for "Introducction to Cryptography" exercises

Exercise 23: Prove by contradiction. If A has an inverse, then there exists a matrix B such that $AB = I$. Take the determinant of this equation, and show that it produces a contradiction to the fact that $(a \odot d) \ominus (b \odot c)$ has no inverse.

Exercise 34: It is possible to list all of the numbers between 1 and pq which are *not* relatively prime to pq.

Exercise 35(c): Remember your exponent rules!

Exercise 41: Consider the case where n is the product of two *equal* factors: $n = a \cdot a$. Then how large must a be? Compare this with the general case where n is the product of two unequal factors: $n = xy$. Show that the *smaller* of these two factors must be smaller than a.

Exercise 43: Suppose $n = ab$. Choose a to be the smaller factor. Write $a = x - y$ and $b = x + y$, and solve for x and y. To finish the proof, you need to prove that x and y must both be integers.

Exercise 44: Solve for x. What value of y makes x as small as possible?

Exercise 45(a): Prove by contradiction. (b): Write $m = 2k + 1$. (d): Use part (c), part (b), and the distributive law. (e): This is similar to part(b).

20.4 Hints for "Set Theory" exercises

Exercise 31(d): Guess the pattern from the previous parts of this exercise.

20.5 Hints for "Functions: basic concepts" exercises

Exercise 15(e): There is a formula of the form $f(x) = ax^2 + bx + c$

Exercise 45: Can there be any elements in the codomain that are not in the range?.

Exercise 67(a): Consider the values $f(1, i)$ for $i = 1, 2, 3, \ldots$. (b): Consider the values $f(2, j)$ and $f(1, i)$.

Exercise 68(a): Given any element (i, j) of $\mathbb{Z} \times \mathbb{Z}$, set $i = m + n$ and $j = m + 2n$ and solve for m and n in terms of i and j.

Exercise 68(b): Suppose that $g(m, n) = g(p, q)$. It follows that $(m + n, m + 2n) = (p + q, p + 2q)$.

Exercise 84(a): You just need to show that $g \circ f$ is both one-to-one and onto. Use the previous exercises.

20.6 Hints for "Equivalence Relations and Equivalence Classes" exercises

Exercise 7(a): There are two. (b): There are four. (c): There are four. (d): There are sixteen. (e): The answer is *bigger* than 500!

Exercise 14(c): There are 9.

Exercise 17(a): $\leq$ is *not* symmetric – you may show this by giving a counterexample.

Exercise 19(a): Give a specific example where $a \sim b$ and $b \sim c$ but $a \not\sim c$. In other words, (a, b) and (b, c) are elements of $R_\sim$, but (a, c) is not in $R_\sim$. It is not necessary for a, b, and c to be distinct.

Exercise 19(b): Explain why it is impossible to find a counterexample.

Exercise 29(b): You may assume (without proof) that the negative of any integer is an integer, and that the sum of any two integers is an integer. For transitivity, notice that $x - z = (x - y) + (y - z)$.

Exercise 29(c): This is similar to the proof in Example 28, but with multiplication in place of addition.

Exercise 67(a): What is the equation of a circle? (d): Use (b) and (c).

20.7 Hints for "Symmetries of Plane Figures" exercises

Exercise 4: The rearrangement that doesn't move anything is still considered to be a symmetry: for obvious reasons, it is called the ***identity***).

Exercise 24: The proof is very similar to part (ii) of the same proposition.

Exercise 33: The proof is very similar to the previous proof.

Exercise 36: Look at Figure 9.8 for some ideas.

Exercise 37(a): Look at Figure 9.9 for some ideas.

Exercise 38(a): Look at Figure 9.9 for some ideas.

Exercise 41(b): If μ is a reflection, then what is $\mu \circ \mu$?

Exercise 47(a): One of them is $\{5, 10, 15, \ldots 5 \cdot k, \ldots\}$.

20.8 Hints for "Permutations" exercises

Exercise 64: The first blank should be replaced by k

Exercise 85(c): Take advantage of the previous part.

Exercise 96: Use the cycle structures you found in Exercise 52

Exercise 97: Think equivalence classes.

Exercise 98(b): If you write σ as the product of transpositions $\tau_1 \cdots \tau_n$, then what is σ^{-1}?

Exercise 98(c): If $\sigma = \tau_1 \cdots \tau_n$ and $\mu = \lambda_1 \cdots \lambda_m$, then what about $\sigma\mu$?

Exercise 103(a): If σ is even, then what about $(12) \circ \sigma$?

Exercise 103(b): If μ is odd, then what about $(12) \circ \mu$? Also, what is $f((12) \circ \mu)$?

Exercise 103(c): If $(12)\sigma_1 = (12)\sigma_2$, then what can you conclude about σ_1 and σ_2? Why are you able to conclude this?

Additional exercises:

Exercise 1: Consider the cycle structure.

Exercise 6: We know that σ can be written as the product of disjoint cycles. So let $\sigma_1, \sigma_2, \ldots \sigma_m$ be disjoint cycles such that $\sigma = \sigma_1\sigma_2 \ldots \sigma_m$, and let ℓ_j be the length of the cycle σ_j. How many transpositions does it take to construct each of these disjoint cycles? And what is the largest possible value of the sum of ℓ_j?

Exercise 7: Use the notation of the previous problem, and write a formula (in terms of $\ell_1 \ldots \ell_m$ and m) for the number of transpositions it takes to construct σ.

Exercise 8: Let ℓ be the length of σ: then what is the order of σ? On the other hand, let k be the order of σ^2: then what do you know about σ^{2k}?

20.9 Hints for "Abstract Groups: Definitions and Basic Properties" exercises

Exercise 22: For the "if" part, assume that $g \circ h = h$, and use this to show that $g = e$. Multiply both sides of the assumed equation by g^{-1}. You will need to use associativity and properties of inverses and the identity to obtain the result. For the "only if" part, assume that $g = e$ and use this fact to show that $g \circ h = g$.

Exercise 23: Prove by contradiction. Suppose that for row "g", the entries in columns "h" and "h'" are the same, where $h \neq h'$. Then what equation must be true? Show this equation leads to a contradiction.

Exercise 30(b): Refer to Section 4.5.5.

Exercise 90: Use the fact that $a^k = a^l$ for $k \neq l$. You may assume that $k < l$ in your proof.

Additional exercises:

Exercise 30b: From part (a), you may obtain 4 different subgroups (why?) To look for more subgroups, suppose for instance there is a subgroup that contains both i and j. What other elements must it contain? Do the same for i and k, j and k, etc.

Exercise 38: Consider Exercise 17 above.

Exercise 39: In fact, such a group can have at most two elements. Why?

20.10 Hints for "Cosets" exercises

Exercise 9: (*Hint*: You're trying to show that the two sets gH and Hg are equal. One way to do this is to show every element of gH is an element of Hg, and vice versa.)

Exercise 11(a): The hypothesis $g_1H = g_2H$ implies that there exists $h \in H$ such that $g_1h = g_2e$, where e is the group identity.

Exercise 11(b): $g_1^{-1}g_2 \in H$ means that $g_1^{-1}g_2 = h$ for some $h \in H$.

Exercise 11(c): You need to show that $g_2H \subset g_1H$. From (3), deduce that $g_2 = g_1h$ for some $h \in H$. Then, show that any element of the form g_2h' for $h' \in H$ can be expressed as g_1h'' where $h'' \in H$. You should be able to express h'' in terms of h and h'.

Exercise 11(d): You need to show that (4) implies $g_1H \subset g_2H$. It's enough to show that for any $h \in H$, $g_1h \in g_2H$. To do this, express g_1 in terms of g_2.

Exercise 11(e): Condition (2) implies that $g_1^{-1}g_2 = h$ for some $h \in H$.

Exercise 33: For part (g), use the fact that the numbers less than p^2 that are *not* relatively prime to p^2 are $p, 2p, 3p, \ldots (p-1)p$: how many numbers remain? For parts (h) and (i) use a similar logic.

Exercise 44: Look back at your work on Exercise 22.

Exercise 46: Use Exercise 9 earlier in this chapter.

Exercise 51: Let H be a subgroup of the group G that satisfies the property that for any $g \in G$ and any $h \in H$, then ghg^{-1} is also in H. Show that every right coset of H in G is also a left coset, and vice versa (and hence H is a normal subgroup of G.

Exercise 52: Use part (a) and Definition 50.

Exercise 53(c): We may write $x_1 = g_1h_1$ and $x_2 = g_2h_2$, so that $x_1x_2 = g_1h_1g_2h_2$. Use part (b) with $h = h_1$, $g = g_2$.

Additional exercises

Exercise 17: Define an equivalence relation on G as follows: $g_1 \sim g_2$ if and only if either $g_1 = g_2$ or $g_1 = g_2^{-1}$. Prove that this is indeed an equivalence relation; and show that the equivalence class of g has an odd number of elements if and only if $g = g^{-1}$. Use the partition of G to show that there must be an even number of equivalence classes with an odd number of elements (including the equivalence class of the identity).

20.11 Hints for "Group Actions" exercises

Exercise 23(a): There are two elements. (d): There are three elements.

Exercise 31(b): It may be helpful to calculate the rotation using cycle notation.

Exercise 42: How many group elements (rotations) are in G_{x_+}? What else do they stabilize?

Exercise 52(b): What is $|G|$ according to the counting formula? How many stabilizers have we found so far?

Exercise 72: H itself is a coset, and take $g_1 = (123)$ and $g_2 = (23)$. Is it true that acting on H by g_1 followed by g_2 is the same as acting on H by g_2g_1?

20.12 Hints for "Algebraic Coding" exercises

Exercise 33(c): Apply part (b) to both sides of the equation, and show they are equal.

Exercise 35(a): Add any codeword to itself.

Exercise 68(c): Use the paragraph just above this exercise.

Exercise 84: Show that the codewords in C that have i'th coordinate equal to 0 form a subgroup of C, and consider the cosets of this subgroup in C.

Exercise 85: What row should you add to the parity check matrix?

Exercise 86: Use the previous exercise to show the codewords of even weight in C form a subgroup. Then consider the cosets of this subgroup in C.

20.13 Hints for "Isomorphisms" exercises

Exercise 5: Show a counterexample where the sum of two complex numbers is not the same as the sum of their corresponding ordered pairs.

Exercise 16(a): According to Definition 9, this involves proving two things about ϕ^{-1}. What are they?

Exercise 16(b): You need to prove the same two things as in part (a). Use results from the Functions chapter.

Exercise 18: Recall that this involves proving the three properties: reflexive, symmetric, and transitive. You may find that Exercise 16 is useful.

Exercise 48: Follow Proposition 46.

Exercise 51(a): Use Exercise 16. (b): Use Proposition 42. (c): Use Proposition 47.

Exercise 72: For each group property to be proved, use the corresponding group property for G and H.

Exercise 77: Define a function $\phi : G \times H \to H \times G$ by: $\phi(g, h) =$ ___ (you fill in the blank). Show that this function is in fact an isomorphism.

Exercise 96(c): Consider 2 cases: (i) 9 divides one of the factors $p_i^{e_i}$ in Proposition 93; (ii) 9 does not divide any of the factors.

Exercise 109: Show that $G \times \mathsf{id}_K$ is a subgroup of $G \times K$, and that $G \times \mathsf{id}_K \cong G$; and similarly for H.

Additional exercises

Exercise 6: If you take every other vertex in a hexagon, you get an equilateral triangle. Also note that 180-degree rotation is an element of order 2.

20.14 Hints for "Homomorphism" exercises

Exercise 17(d): Use Definition 50 from the Cosets chapter, and the multiplicative property of determinants.

Exercise 28: Use Part (d) of Proposition 24, using $T = \{e\}$.

Exercise 35: The function f is completely determined by the value of $f(1)$. For instance, if $f(1) = 2$, then the operation-preserving property implies that $f(n) = 2n$ for any integer n (Why?).

Additional exercises:

Exercise 3: Use the operation-preserving property.

Exercise 4: What is the order of $0.5 + \mathbb{Z}$?

20.15 Hints for "Sigma Notation" exercises

Exercise 10: You will have two summation symbols.

Exercise 15: Notice that the product AB is in both terms.

Exercise 17(b): Use one of the previous exercises.

Exercise 19: There are two possibilities to consider, $i = j$ and $i \neq j$.

Exercise 20(a): Hint: Make a table for all possible values of i, j, k.

Exercise 20(b): Multiply the equation you found in (a) by a_{ijk} and sum over all i, j, k.

Exercise 31: First show that: $\sum_{k=1}^{n} 2^k = 2^{n+1} - 2$.

20.16 Hints for "Polynomial Rings" exercises

Exercise 5(d): Note $4 = 3 + 1$ and $11 = 3^2 + 2$.

Exercise 22(d): Are there any common factors you can take outside the summations before multiplying?

Exercise 39: Consider $g_i, g_i^2, g_i^3, \ldots, g_i^{p_i - 1}$ and use exponent rules to show that they are not equal to e. Similarly, show that $g_i^{p_i} = e$.

Index