Proofs, Sets, Functions, and More: Fundamentals of Mathematical Reasoning, with Engaging Examples from Algebra, Number Theory, and Analysis

Mike Krebs

James Pommersheim

Anthony Shaheen

For the instructor to read

We should put a section in the front of the book that organizes the organization of the book. It would be the instructor section that would have:

– flow chart that shows which sections are prereqs for what sections. We can start making this now so we don't have to remember the flow later.

– main organization and objects in each chapter

– What a Cfu is and how to use it

– Why we have the proofcomment formatting and what it is.

– Applications sections and what they are

– Other things that need to be pointed out.

IDEA: Seperate each of the above into subsections that are labeled for ease of reading but not shown in the table of contents in the front of the book.

———————— main organization examples: ————————

In a course such as this, the student comes in contact with many abstract concepts, such as that of a set, a function, and an equivalence class of an equivalence relation. What is the best way to learn this material. We have come up with several rules that we want to follow in this book.

Themes of the book:

1. The book has a few central mathematical objects that are used throughout the book. 2. Each central mathematical object from theme #1 must be a fundamental object in mathematics that appears in many areas of mathematics and its applications. 3. When definitions of abstract objects such as functions and equivalence relations come up the book focuses on the central examples. 4. Add more... 5. Add more...

We chose two central themes for the book: number theory / abstract algebra, and analysis / topology.

For number theory and abstract algebra, the main examples are the integers modulo n, properties of the prime numbers, etc. Some applications sections include sections on generating the pythagorean triples, the group of primitive pythagorean triples, the Guassian integers with an application to sums of squares.

For analysis / topology, we study the real line and real plane. Fill this part in .... distance function? open sets/closed sets?

See the flow chart in Figure ...

The chapter contents are layed out as follows.

Ch. 1 -

Ch. 2 -

Ch. 3 - This is really where the nuts and bolts of the course start. We go through the kinds of proofs that one encounters in math texts, such as direct proof, contradiction, etc. We discuss the divisibility properties of the integers and focus on congruence modulo n. Prime numbers, irrational numbers, and the greatest common divisor are are introduced in this chapter and are used throughout the text. Powerful theorems about prime numbers, such as Theorem and Theorem on page and page , are proven in this chapter. Their first application appears in the proof that $\sqrt{3}$ is irrational.

Ch. 4 - We introduce the methods of induction. We prove two big theorems from number theory: There are an infinite number of primes, and every integer can be factored uniquely into a product of primes.

Ch. 5 - sets

Ch. 6 - relations. We focus on equivalence relations and equivalence classes because it is the most important topic in the chapter. One main example that is used throughout the remainder of the book is the integers modulo n. We especially use the integers modulo n in the functions chapter.

Ch. 7 - functions. Functions are one of the most important objects in mathematics. In illustrating concepts such as one-to-one, onto, image, and inverse image we use examples from our central objects: integers modulo n, integers, whatever else we add in this chapter. There are several examples of functions between the integers modulo n that are used in group theory and number theory. Put what the real number ones will be if we add more or replace some of the number theory.

... ...

Here are several ways to navigate through the book:

Way 1: Put a sequence of sections here.

Way 2: Put a sequence of sections here.

Contents

Chapter 1

Introduction

1.1. Welcome to mathematics!

We expect that most people reading this book will be students taking a transitional "proofs" course; that most such students are math majors; and that this is the first course exclusively for, or at least dominated by, math majors. So we feel that this is a great opportunity to welcome and introduce you to the wide and wonderful world of mathematics.

As you have probably heard, lower-division math courses such as Calculus tend to be heavily computational, whereas upper-division math courses are usually more theoretical and abstract. The primary purpose of this text is to help you make that transition.

In this first section, though, we'd like you to tell you about some fun and useful pieces of information that together comprise a significant portion of "math culture." Your professors probably know most of this, plus lots more that we overlooked, but as an early-career math major, chances are that you have not yet been clued in.

Though many of the items below apply throughout the globe, some pertain only to the United States, where the authors of this book reside. Moreover, the longer it's been since this section was written, the more likely it is to be obsolete. An internet search should provide information that is up-to-date and relevant to countries outside the US. But now you'll know some things you can look for!

Jobs in math: Math majors are often not aware of job opportunities outside of teaching that make use of their academic training. Such career paths abound, however. Moreover, they are not just jobs; they are

highly desirable jobs. In the year 2014, CareerCast.com rated "mathematician" as the very best in a ranking of two hundred different jobs. Criteria included work environment, income, stress level, etc. Many other highly rated jobs were math-related, such as actuary and statistician, both of which were in the top five.

Math-intensive vocations include, but are by no means limited to, the following: actuary, cryptologist, economist, environmental mathematician, geodesist, inventory strategist, operations research analyst, staff systems air traffic control analyst, and statistician.

For more information, you may want to visit the Mathematical Association of America's Career Profiles website at:

`www.maa.org/careers/career-profiles`

Teaching math: Teaching, of course, remains a way to make use of a degree in mathematics. One can teach math at the middle school, high school, two-year college, or four-year college level. Generally speaking, these different levels have different minimum requirements for employment.

Each state sets its own minimum requirements for becoming a public middle school or public high school mathematics teacher. Typical requirements include obtaining a bachelor's degree in mathematics, passing a basic skills test, and successfully completing an approved teacher education program. To do internet searches to find out specific requirements for your state, try the search terms "teaching credential" or "teaching certificate." The Math Department professors and/or your school's career center may be able to guide you here as well. The requirements to teach math at a private middle school or high school vary; often, a teaching credential is not required.

Obtaining a full-time position teaching math at a two-year (community) college often requires, as a minimum, a master's degree in mathematics, though some schools require only a bachelor's degree. Many two-year colleges specifically require a master's degree in mathematics as opposed to mathematics education. Some graduate programs in mathematics do not offer anything higher than a master's degree, and these programs are often designed primarily for students who intend to become math professors at two-year colleges. In contrast, other graduate programs in mathematics, usually at top research schools, award PhDs as their main function but also give master's degrees to students who successfully complete part but not all of the PhD program. The job market for full-time faculty positions in math at two-year colleges varies over time and from region to region but generally speaking is quite competitive.

Becoming a full-time professor of mathematics at a four-year college or university requires a PhD in the field, at a minimum. Tenure-track faculty positions in mathematics are highly sought-after and extremely competitive, especially at top research universities. Frequently, to be offered such a job, one must first have completed one or more temporary postdoctoral positions in order to have built up a sufficient track record in teaching and research.

At both two-year and four-year colleges, full-time professors can get tenure (and the job security that comes with it). Adjunct faculty, however, are assigned classes from term to term on an as-needed basis and cannot receive tenure.

Graduate school: Generally speaking, there are two types of graduate programs in mathematics: those that offer only master's degrees, and those that grant PhDs.

Many students who enroll in masters' programs in mathematics do so to qualify to teach math at a two-year college. Sometimes students do so to prepare for work in business, industry, or government, or to prepare more thoroughly for a PhD program. Typically, it takes about two years to complete a master's program in mathematics. Requirements generally focus on completion of coursework that is similar to upper-division undergraduate coursework. Many masters' programs have both thesis and non-thesis options.

PhD programs in mathematics generally cater to students who wish to become full-time professors at four-year colleges and universities, though some students there intend to go on to work in business, industry, or government. Obtaining a PhD in math typically takes five to six years. Often, the student receives a teaching assistantship and/or stipend during that time so that there is little to no tuition cost. The first two years usually focus on coursework, after which one must pass qualifying exams. From that point on, one works with an adviser to do original research, culminating in a dissertation. Some students enter PhD programs with a set idea of the area of math they want to do research in, but many do not. When selecting PhD programs to apply to (or to attend, if accepted), one may want to ask some of the following questions. What percentage of students pass the qualifying exams? What percentage of students graduate? Of those who have graduated recently, where are they now? Which faculty members are potential dissertation advisers? We cannot overemphasize the importance of selecting a good adviser. We recommend looking for someone who has tenure, who meets regularly with his or her students, who is well-regarded in the field, who gets along well with students, who

makes an effort to help his or her students find employment after graduation, and who does not plan to retire within the next five years. Most schools require applicants to take both the GRE General Test and the GRE Subject Test. The GRE Subject Test in mathematics is quite difficult, and we encourage anyone who plans to take it to budget a considerable amount of time well in advance to study for it. The website `www.phds.org` contains a great deal of useful information about PhD programs.

The two main branches of mathematics are applied math (in which the one uses math to solve problems that emanate from the real world) and pure math (in which one engages in problem-solving for its own sake). At some schools, applied math and pure math are housed in different departments. In that case, one must decide which department to apply to, or whether to apply to both. Statistics, too, is often an independent department.

For all types of graduate programs, the AMS website on applying to grad school contains a large amount of practical information and advice:

`www.ams.org/profession/career-info/grad-school/grad-school`

Branches of math: One public misconception about math is that it consists entirely of a fixed collection of established techniques. In fact, new discoveries in math are being made every day. To push the boundaries of human knowledge a little further, researchers must specialize in a particular field, or, less commonly, lay the foundations for a new one. So mathematics, like most mature areas of study, branches out into sub-disciplines, and sub-sub-disciplines, and so on. Your upper-division electives begin to hint at the breathtaking diversity of topics.

The first main division occurs when mathematics bifurcates into pure mathematics and applied mathematics. The line between pure math and applied math is fuzzy at best, but roughly speaking, pure math includes logic, set theory, combinatorics, graph theory, algebra, number theory, algebraic geometry, analysis, complex analysis, harmonic analysis, differential geometry, algebraic topology, and many other fields, while applied math includes probability theory, numerical analysis, operations research, game theory, systems control theory, and many other fields. Other related areas include math history, philosophy of mathematics, and math education. One widely used organizational scheme is the Mathematics Subject Classification (MSC); it lists sixty-four different disciplines within mathematics, each with various sub-disciplines. There is active ongoing research in all of these fields!

Undergraduate research: A few years ago, a math major wrote on an online forum, "I have not met any other students doing undergraduate math research and my current feeling is that many or all the problems in math are far beyond my ability to research them." Not true! While advanced research does indeed require specialized training, there are plenty of unsolved questions an undergraduate math major can tackle. College students routinely prove new theorems, publish their results in peer-reviewed journals, and present their findings at conferences.

What's more, there are plenty of programs, usually in the summer, to guide undergraduates through the process of doing original research in math. Many of these programs go by the name Research Experience for Undergraduates (REU). Visit

`www.ams.org/programs/students/undergrad/emp-reu`

for a listing of these programs. As of May 2014, there were over one hundred REU programs at universities throughout the United States. The National Science Foundation, which funds REU sites, describes a typical REU experience as follows. "An REU Site consists of a group of ten or so undergraduates who work in the research programs of the host institution. Each student is associated with a specific research project, where he/she works closely with the faculty and other researchers. Students are granted stipends and, in many cases, assistance with housing and travel." Application deadlines for REUs usually occur in February or March. There are many other programs out there that are similar to REUs; you can find them by doing an internet search for "undergraduate math research."

Some professors do research with undergraduate students during the academic year. If you're interested, ask your favorite math professors about how to get started with your own project.

Competitions: There are several math competitions for undergraduate college students. The William Lowell Putnam Mathematical Competition, commonly known as the Putnam Exam, is a well-known national contest. Students taking the Putnam Exam spend six hours trying to solve twelve extremely difficult math problems. Another contest is the Mathematical Contest in Modeling (MCM), whose website states that it "challenges teams of students to clarify, analyze, and propose solutions to open-ended problems."

Honorary societies: Undergraduate math majors may be eligible for one of the national honorary societies that seek to promote mathematics. These include Pi Mu Epsilon (PME) and Kappa Mu Epsilon

(KME). Both groups publish journals and host events. PME's annual conference is held in conjunction with MathFest.

Organizations: Many organizations in the United States and throughout the world support the mathematical community in various ways. The American Mathematical Society (AMS) focuses on research and scholarship. The Mathematical Association of America (MAA) states that its mission is "to advance the mathematical sciences, especially at the collegiate level." The Society for Industrial and Applied Mathematics (SIAM) seeks to promote cooperation between mathematicians and those in science and industry. The National Council of Teachers of Mathematics (NCTM) describes itself as "the public voice of mathematics education." Several societies strive to achieve equal opportunity for underrepresented groups in the mathematical sciences. These include the Association for Women in Mathematics (AWM), the National Association of Mathematicians (NAM), the Benjamin Banneker Association (BBA), and TODOS: Mathematics for ALL.

Conferences: We strongly encourage you to attend a conference at some point; it's a great way to meet other people who share your passion for mathematics and to find out about new discoveries being made. Most of the organizations listed above host periodic conferences. The largest one is the Joint Mathematics Meetings (JMM), hosted annually by both the AMS and MAA (hence the name) in early January. The location varies. JMM features an extraordinarily large number and vast range of talks, from fun and engaging general audience presentations to highly technical sessions on specialized topics. Undergraduate students, graduate students, and faculty alike all present there. Other activities of interest include a Mathematical Art Exhibit and a Graduate Student Fair. The MAA also hosts another annual conference in the summer called MathFest; in accordance with the MAA's mission, it focuses primarily on undergraduate mathematics. Like JMM, MathFest is held in a different city every year. Both the AMS and the MAA have regional sections throughout the United States that hold regular meetings. In addition, the MAA sponsors several regional conferences specifically for undergraduates; for more informtion, see:

`www.maa.org/programs/maa-grants/RUMC`

These are just a handful of the countless math conferences that take place every year. With an internet search for "mathematics conferences," you will find many more.

Funding to cover the costs of attending a conference (registration, travel, lodging, etc.) is often available, through the organization hosting the conference or through your school. Frequently, grants are open only to students presenting research results. Deadlines typically occur many months in advance, so plan ahead.

Journals, articles, and databases: When a mathematician proves a significant result, he or she then usually attempts to publish it in a peer-reviewed journal. By publishing an article, the journal in effect puts its stamp of approval on it, verifying that the content is significant, well-written, and apparently correct. There are quite a few journals dedicated to mathematics; in the year 2010, the Australian Research Council ranked over 20,000 of them. Some, such as *Ergodic Theory and Dynamical Systems* and the *Journal of Combinatorial Optimization* focus on specific fields; others, such as *Acta Mathematica* and *Annals of Mathematics* (two of the oldest and most highly respected journals), cover all fields of mathematics. Some journals publish only articles by undergraduate authors or with student co-authors; these include *Involve*, the *Rose-Hulman Institute of Technology Undergraduate Mathematics Journal*, and *SIAM Undergraduate Research Online*. A few publications contain articles of general interest that do not require advanced training in a specific subfield. The *American Mathematical Monthly*, *Notices*, *College Mathematics Journal*, and others all fall into this category. In these journals, some articles detail new findings, whereas some are expository articles that seek to more clearly explain established results, or to put them in a new light.

With so many journals, how do you find the articles that are relevant to your research topic? The best way is to search a journal database. By far, the most widely used database in mathematics is MathSciNet, located online at ⟨`www.ams.org/mathscinet`⟩. You need a subscription to access MathSciNet. Your school library may well have a subscription, so ask a librarian about this.

It is by no means unusual for a delay of several years to occur between the time an article is first written and submitted to a journal, and the time it finally appears in print. Such an article—one that is written but not yet published in a journal—is called a "preprint." Authors sometimes post preprints online, either on their own website, or on a preprint server such as arXiv ⟨`www.arxiv.org`⟩. If you want to get a sense of how much new mathematics is being done all the time, click the link for "new" under the heading "Mathematics" on arXiv. On the day this sentence was written (Tuesday, May 20, 2014), 331 articles had been posted. How many were posted today?

Producing mathematical symbols: There are various ways to use a computer to write mathematical expressions. Microsoft Word, for example, has a user-friendly feature called Equation Editor for this purpose. For a professional-quality end product, mathematicians generally use a document preparation system such as LaTeX. The TeX Users Group ⟨`tug.org`⟩ provides information on using and getting started with LaTeX. Moreover, it is available for free online. However, it takes an initial investment of time to learn LaTeX, because it uses special commands much like a programming language. To produce $\int_0^\infty \frac{\log x}{x^2+1}\,dx$, for example, one enters `\(\int_0^{\infty}\frac{\log x}{x^2+1}\;dx\)`.

Online resources: In the internet age, one can routinely find answers to the most abstruse questions with just a few keystrokes. We list here several websites that we've found useful. Mathematics Stack Exchange ⟨`math.stackexchange.com`⟩ describes itself as "a question and answer site for people studying math at any level and professionals in related fields." MathWorld ⟨`mathworld.wolfram.com`⟩ is a Wikipedia-like online encyclopedia dedicated exclusively to mathematics. Ask a Topologist ⟨`at.yorku.ca/cgi-bin/bbqa`⟩, another question-and-answer site, contains forums concentrating on calculus, algebra, analysis, topology, and algebraic topology. The On-Line Encyclopedia of Integer Sequences ⟨`at.yorku.ca/cgi-bin/bbqa`⟩ allows users to search for sequences of integers, given a portion of the sequence; if you have the terms $1, 3, 4, 7, 6, 12$ and want to know what comes next, this is the place to go.

Computational software: Many mathematicians, especially in applied fields, make use of software that can perform tedious calculations with astonishing speed and accuracy. Examples include Mathematica, Maple, and Matlab. Many of these packages can do quite a bit more than a scientific calculator; they can compute integrals, find inverses of matrices, graph in three dimensions, and much more. If you ask Mathematica to compute the infinite sum $\sum_{n=1}^{\infty} \frac{1}{n^2}$, for example, it will not give you a numerical approximation; rather, it will find the exact answer, which is $\pi^2/6$. The mathematical software system Sage, available at ⟨`www.sagemath.org`⟩, is free and open-source.

For more information: The American Mathematical Society hosts a website full of the sort of information we've presented in this section. The page is entitled "Undergraduate Mathematics Majors" and can be found at:

`www.ams.org/programs/students/undergrad/undergrad`

1.2. What are proofs, and why do we do them?

Consider the following classic logic puzzle. Three contestants compete for prizes on a game show. The emcee shows them five hats, three of them black, the other two white. He tells them that he will put one of those hats on each of their heads and discard the remaining two. Each contestant's task will be to determine what color hat he or she is wearing. The emcee then seats the three players in three chairs arranged one behind the other, blindfolds each contestant, puts one hat on each player, moves the other two hats out of sight, and removes the blindfolds. The first contestant, seated at the rear, can see the hats on the heads of the other two. The emcee asks Contestant #1 what color hat she is wearing, but she says, "I don't know." Now the emcee puts the same question to the player seated in the middle, who can see only the hat directly in front of him. This contestant, too, states that he is unable to determine his own hat color. At that point, the third and final contestant, who is unable to see *any* hat whatsoever, exclaims, "I know what color my hat is!" What color is Contestant #3's hat, and how did she figure it out?

If you want to work the solution out for yourself—as any self-respecting math person should want to do—then close this book now and don't look at the next paragraph until you've got it.

OK, here's how she did it. Imagine that the first contestant looked up and saw two white hats. She would then have been able to deduce that she herself was wearing a black hat. But she did not do so. The other two players now know that at least one of them is wearing a black hat. So had Contestant #2 seen a white hat, he would have known that he must have been the one wearing a black hat. However, he, too, could not say with certitude whether his hat was black or white. Now the final player knows that she is not wearing a white hat, and she therefore correctly declares that she has a black hat atop her head, whereupon she wins, let's say, a trillion dollars.

The argument in the preceding paragraph is a mathematical proof. We began with a set of premises (how many hats of each color, who can see which hats, etc.). From there, we constructed an unbroken chain of logical steps that culminated in a final conclusion, namely, that the third player's hat was black. So long as the premises and the logic were correct, we can be certain that the conclusion is correct, too.

Very few mathematicians study hat color theory. Every mathematician, however, writes proofs. In this book, we will introduce you to the basic objects that mathematicians do use in their research, as

well as techniques for proving statements about them. From Calculus and other classes, you already have some familiarity with many of these objects, such as functions and sets. Now, we will go back to square one and revisit them, this time with absolute precision and with a completely new focus: not on performing computations, but on correctly writing true statements and making logical inferences.

When you put the last piece of a jigsaw puzzle into its proper place, you may experience a feeling of great satisfaction. You may feel similarly satisfied by the proof that the third player's hat is black, particularly if you figured it out yourself. Every part of the logic meshes just so with every other part, with no parts left over, and together they eliminate all doubt that the conclusion is correct. To varying degrees, every mathematical proof produces this feeling of satisfaction. When a sequence of logical steps reaches a conclusion with surprising efficiency, mathematicians call it "elegant" or "beautiful." Public perception to the contrary, tedious computations are not what mathematics is all about. Rather, putting logical pieces together to form a beautiful, elegant proof is the heart and soul of the subject.

If the scenario described in the hat puzzle took place on an actual game show, the third contestant could not have been completely convinced of her answer. The second contestant, for example, might have seen a white hat but been unable to reason his way to the solution. The first contestant may have been blinded by the television studio's lights and thus unable to see the other two players' hats. The same issue affects any application of mathematics to the real world. A chemist may use math to draw conclusions in a scientific inquiry but cannot be certain that her lab is free from all contaminants. A social psychologist may use a mathematical theorem when analyzing data from an experiment but may worry that some small difference in conditions may have subtly affected the subjects' responses. A team of Wall Street analysts may solve differential equations to predict market behavior but can never be sure that their underlying assumptions are valid. The great physicist Albert Einstein put it this way: "As far as the laws of mathematics refer to reality, they are not certain; and as far as they are certain, they do not refer to reality." Those who employ math in science, business, industry, and government must expend time and effort mitigating the inherent tentativeness of the non-mathematical aspects of their work. But the validity of math itself causes no such anxiety. So there is a practical as well as an aesthetic value to the sureness that mathematics provides.

One time, two of the authors of this book were talking with a well-known marine biologist about open problems in mathematics, i.e.,

things we still don't know. We gave the example of Goldbach's conjecture, which surmises that every even number greater than 2 is a sum of two prime numbers. (When mathematicians suspect but cannot prove that a statement is true, we call it a "conjecture." Goldbach is the last name of the person who made this conjecture.) For example, the even number 106 equals 47 plus 59, both of which are prime. Though this problem has been around since the year 1742, no one has yet been able to prove or disprove it. We told the biologist that the conjecture has been verified by computer for all even numbers up to four quintillion, that is, $4 \times 10^{18} = 4,000,000,000,000,000,000$. He replied, "Isn't that good enough?" In science, experimental evidence that backs up a hypothesis four quintillion times over is more than good enough. How many whales of a particular species does a biologist need to observe, after all, before drawing general conclusions about the behavior of that species? But in math, we deal with the infinite. Yes, Goldbach's conjecture is true for the first several quintillion even numbers. But think about this: How many even numbers are there that we have *not* checked yet? What *percentage* of all even numbers have we looked at so far? For all we know, the smallest counterexample may be on the order of a googol (10^{100}) or a googolplex (10^{googol}) or Graham's number (look it up—it's *much* bigger than those other two). Computing examples one at a time, no matter how many, will never convince us that Goldbach's conjecture holds for *all* even numbers. If the conjecture is indeed true, then to be certain of it, we will need a proof.

Indeed, mathematicians have oftentimes made conjectures backed by substantial numerical evidence that turned out later to be false. One famous case is that of Euler's sum-of-powers conjecture. The great mathematician Leonhard Euler speculated in the year 1769 that a kth power of an integer cannot be written as a sum of more than one but fewer than k positive integers, each of which is a kth power. In the year 1988, the smallest counterexample for $k = 4$ was found:

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

By contrast, it is impossible to find positive integers a, b, c such that $a^3 + b^3 = c^3$. How can we be so sure? As we just pointed out, checking lots of examples will not persuade us. But we know for a fact that no such a, b, c exist because in the year 1770, Euler gave a *proof*.

So proofs provide certainty. But they serve another purpose as well. For one does not always have a conjecture to work with. In the hat puzzle, Contestant #3's thought process did not begin with the notion that she was wearing a black hat, followed by an attempt to prove that fact. Not at all! Instead, she simply made a sequence of logical

inferences, based on the available information, that led to the correct conclusion. The process of proving led to the solution. This situation is common in mathematics. So deductive reasoning not only verifies true statements, it also sometimes helps us discover them.

In math, you cannot determine whether a statement is true unless it is written with the utmost precision and a total lack of ambiguity. For example, consider the sequence $1/n$, whose terms are $1, 1/2, 1/3, \ldots$. In Calculus, you learned that the limit of this sequence is 0. You may have been told that that's because the terms "get closer and closer" to 0. Isn't it also true that the terms get closer and closer to -1? So maybe -1 is also the limit of this sequence? No, -1 is not the limit; the limit is 0. The problem is that the phrase "getting closer and closer" is not sufficiently precise. (We learned about this example from a talk given by math education expert Guershon Harel.) A big part of this course will be learning to write mathematical statements in such a way that anyone who reads them will interpret them exactly as you intended.

Rigorous proof first developed mainly in ancient Greece. The so-called "axiomatic method" we use today, where we begin with clearly spelled-out assumptions (axioms) from which we make logical deductions, was introduced by Euclid around 300 BCE. This way of thinking has been extraordinarily influential throughout history, and not just in mathematics. The structure of the Declaration of Independence, for example, from the premises that begin with "We hold these truths to be self-evident . . ." to the conclusion introduced with the word "therefore," is modelled after a Euclidean-style proof.

In the fifth century BCE, the rebuilding of the Persian Royal Road significantly reduced travel time across the empire. A few centuries later, according to a legend, King Ptolemy I attempted to learn geometry from Euclid's treatise *Elements* but gave up because he found it too difficult. Ptolemy summoned Euclid and asked him if there was an easier way to learn the material. Referring to the great streamlined Persian superhighway, Euclid replied, "Sire, there is no Royal Road to geometry."

Over the next few months, you will feel the king's pain. (His Royal Pain, you might say.) Many students make their way through algebra, trigonometry, and calculus by finding and mimicking examples from the textbook. *That approach will not work in this class.* You will need to learn a new way to learn mathematics. Rather than follow a recipe, you will need to forge your own path, given only a starting point and a desired ending place, all the while scrupulously following the rigid rules of the game. It's not easy. There is no royal road. Frequently, despite

your best efforts, you will have no idea how to proceed, and this can be excruciatingly aggravating. It's also a completely normal part of learning. One of our professors used to say, "If you're not frustrated, then you're not working hard enough." Athletes and musicians must first do endless drills in order to learn to play well. Likewise, you will need to complete a giant pile of exercises to learn this material. Each one will be a struggle. For athletes, the hard work pays off when they make spectacular plays in the game. For musicians, creating wonderful music makes worthwhile the vexation of a thousand hours of rehearsal. For you, we hope that the reward comes in the form of immense fulfillment when you write your very own exquisitely crafted, elegant, beautiful proofs.

Part 1

Basics

Chapter 2

Basics of sets

In mathematics we use sets to construct or organize mathematical objects. For example, suppose you had the three numbers 2, 3, and 5 and you wanted to put them together into a collection because they had a property that you wanted to study—in this case, these three numbers are the first three prime numbers. You would do this with a set. The set containing 2, 3, and 5 is notated as $\{2, 3, 5\}$.

Virtually every mathematical object that you know can be constructed using a set: numbers, functions, etc. For example, you can build the function $y = x^2$ using sets. (See the discussion in ?????????? if you are interested.) Even the numbers 3 and say $1,000$ can be made out of sets. See ????? for more details on this topic.

Before we begin to learn about logic and proofs we first need some basic ideas about sets. We give a brief introduction to sets in this chapter. In Chapter 6 we study them in more detail.

2.1. Beginning to work with sets

Informal Definition 2.1. *A* **set** *is a collection of objects. The objects in a set are called the* **elements***, or* **members***, of the set. If S is a set and x is an element of S, then we write $x \in S$. If x is not an element of S, then we write $x \notin S$. Two sets are equal if they contain the same elements.*

Example 2.2. One way to specify a set is to list its elements and put curly braces around them. For example, let $S = \{1, 15, 0\}$. Then S is the set with the three elements 1, 15, and 0. We write $1 \in S$,

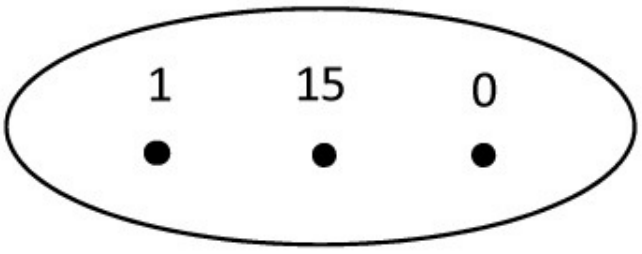


FIGURE 1. A picture of the set $\{1, 15, 0\}$ from Example 2.2

$15 \in S$, and $0 \in S$. Note that $-1 \notin S$ because -1 is not listed as an element of S. One way to visualize a set as a closed curve with dots (elements) inside it, as in Figure 1.

TOO MUCH INFORMATION 2.3. We often say "x is in S" or "S contains x" to mean "$x \in S$." For example, in Example 2.2 we can say that "15 is in S." We can also say "S contains 0."

TOO MUCH INFORMATION 2.4. Notice that we defined a set as a "collection of objects". What is a "collection of objects" ? What does that mean? We have a sense of what it means. You take a bunch of "objects" and group them together. When you want to define a new mathematical object you have to start somewhere. You either (a) define it in terms of some other mathematical object that you already know or (b) create a new object. How do you create a new object? In the end you have to start with some assumption or given that is "understood." This is called an axiom or assumption in mathematics. In this book we are taking the concept of a set as a starting point. One can go further and define more formally what a set is, but this is unnecessary at this level.

We would like to point out that our definition of a set actually gets you into trouble. It is too general, and allows you to create "collections of objects" that bring up logical contradictions such as Russell's paradox. See ????? for more information on Russell's paradox. However, we will never see any of these contradictions in this book because we won't construct any wacky sets like the one from Russell's paradox.

TOO MUCH INFORMATION 2.5. There are two facts about sets that are important to understand.

- Sets cannot have duplicate elements. For example, $\{1, 1, 2\}$ is not a set. When someone writes this set they really mean $\{1, 2\}$.
- Order doesn't matter in a set. For example, $\{1, 10, -3\}$, $\{10, -3, 1\}$, and $\{-3, 10, 1\}$ are all the same set.

INFORMAL DEFINITION 2.6. *The set of* **natural numbers** *is the set whose elements are all the positive whole numbers. We denote the set of natural numbers by* $\mathbb{N}$. *Thus*

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}.$$

We use the dots "..." to indicate that the set keeps going forever.

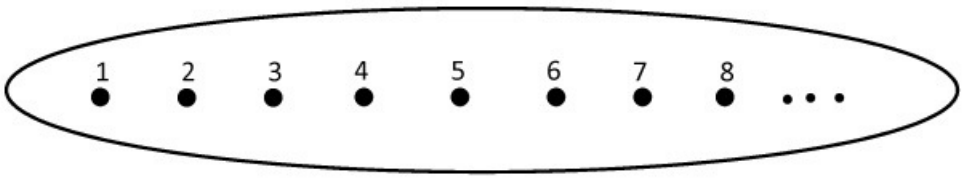


FIGURE 2. A picture of $\mathbb{N}$, the set of natural numbers

TOO MUCH INFORMATION 2.7. Again we encounter the unknown term "positive whole number." You are probably so used to what a number is that you would never think that it needs a definition. Here we have a mental idea what a whole number is because we can think

about, say for example, the number 2 as representing two of something. And we live in a world where we can put two things in front of us. But what is the mathematical object 2? What does $2 + 7$ mean? How do you add these "positive whole numbers?" Here we take the positive whole numbers as a starting point. We assume for now that they exist, we know how to add and multiply them, and that the basic properties about them also hold. We will discuss this again in ?????????????.

What is amazing is that you *can* construct the natural numbers using only set theory. And it turns out that you can define how to "add" two natural numbers using a method called induction. We will learn the technique of induction in Chapter ?????.

EXAMPLE 2.8. The numbers 1000 and $12,325,111,432$ are examples of natural numbers. The numbers -10, $\frac{1}{2}$, and $\pi \approx 3.14159265$ are not natural numbers.

INFORMAL DEFINITION 2.9. *The set of* **integers** *is the set whose elements are zero, the positive whole numbers, and the negative whole numbers. We denote the set of integers by* $\mathbb{Z}$*. Thus*

$$\mathbb{Z} = \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}.$$

As in Informal Def. 2.6, we use the dots "..." to indicate that the set extends infinitely in both directions.

TOO MUCH INFORMATION 2.10. As with the natural numbers, our definition of the integers is an informal definition. What is a negative whole number and what is zero? In this book we will take the integers and their basic properties as givens.

As we discussed in Remark 2.6 about the natural numbers, one can also construct the integers out of sets and how to add and multiply them. Then one can derive all of their usual properties.

EXAMPLE 2.11. The numbers 101 and $-1,223,546$ and $6,789$ are all integers. Notice that all of the natural numbers are integers. But, not every integer is a natural number. For example, -10 is an integer. But -10 is not a natural number because it is not positive.

So far the only examples of sets that we have are finite sets, such as $\{1, 15, 0\}$, where one can list all of the elements of the set; and infinite sets such as $\mathbb{N} = \{1, 2, 3, \ldots\}$ whose elements follow a simple pattern that is understood once a few of the elements of the set are listed. We

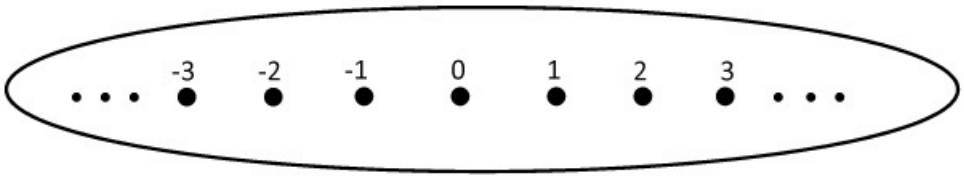


FIGURE 3. A picture of $\mathbb{Z}$, the set of integers

now describe another way to construct a set which allows for sets that do not fit the above descriptions.

NOTATION 2.12. We now describe **set builder notation**. Consider the following expression

$$\{x \in S \mid P(x)\}.$$

This stands for the set of all x from the set S where $P(x)$ is true. This is a common way to construct a set. Sometimes we leave out the S and just write x when S is understood. Another common notation is $\{x \in S \ : \ P(x)\}$.

EXAMPLE 2.13. Let $S = \{1, 6, -5, 3\}$ and let $X = \{x \in S \mid x^2 < 12\}$. The set X consists of the elements x from S that satisfy the equation $x^2 < 12$. Let's check each element of S and see which ones are in X. We see that

$$\begin{array}{rcccl} 1^2 & = & 1 & < & 12 \\ 6^2 & = & 36 & \not< & 12 \\ (-5)^2 & = & 25 & \not< & 12 \\ 3^2 & = & 9 & < & 12 \end{array}$$

Thus, 1 and 3 are elements of X because they satisfy the equation $x^2 < 12$, but 6 and -5 are not elements of X. So $X = \{1, 3\}$.

EXAMPLE 2.14. Consider the set $S = \{1, 7, -2, 3, 15, 22, -49, 13\}$. Let $X = \{x \in S \mid 5 \leq x < 22\}$. The set X consists of the elements x from S that satisfy the equation $5 \leq x < 22$. Thus, $X = \{7, 15\}$.

NOTATION 2.15. There is a more general way to do set-builder notation. The most general form is as follows:

$$\{\text{description of elements} \mid \text{condition imposed on elements}\}$$

EXAMPLE 2.16. Let $T = \{7, -2, 14, 3\}$. Let $Y = \{x^2 \mid x \in T\}$. In this case, the set Y consists of all the elements of the form x^2 where x is an element of T. Thus, $Y = \{(7)^2, (-2)^2, (14)^2, (3)^2\} = \{49, 4, 196, 9\}$.

EXAMPLE 2.17. Let $X = \{3x \mid x \in \mathbb{Z}\}$. What are the elements of X? We see that the set X consists of the elements of the form $3x$ where x is an integer. For example, $6 = 3(2)$ is in X. The number $-15 = 3(-5)$ is also in X. We see that

$$\begin{array}{rcl} X & = & \{\ldots, 3(-3), 3(-2), 3(-1), 3(0), 3(1), 3(2), 3(3), \ldots\} \\ & = & \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}. \end{array}$$

That is, the set X consists of the multiples of 3.

EXAMPLE 2.18. Let $A = \{10, -5\}$ and $B = \{0, 1\}$. Consider the set

$$X = \{5a - 2b \mid a \in A, b \in B\}.$$

What does this mean? The notation "$a \in A, b \in B$" means that a is an element of A and b is an element of B. When we write this we mean that a and b range over all of the values of A and B. Thus, the set X consists of the elements of the form $5a - 2b$ where a is an element of A and b is an element of B. These elements are

$$\begin{array}{rcrl} 5(10) - 2(0) & = & 50 & \text{(this is when a = 10 and b = 0)} \\ 5(10) - 2(1) & = & 48 & \text{(this is when a = 10 and b = 1)} \\ 5(-5) - 2(0) & = & -25 & \text{(this is when a = -5 and b = 0)} \\ 5(-5) - 2(1) & = & -27 & \text{(this is when a = -5 and b = 1)} \end{array}$$

So $X = \{50, 48, -25, -27\}$.

CHECK FOR UNDERSTANDING 2.19.

(1) Let $S = \{-10, 4, 16, 77, 13, 2, 6, -155\}$ and $T = \{x \in S \mid 2x - 1 < 50\}$. List the elements of T.
(2) Let $S = \{-5, 10, 4\}$ and $X = \{x^3 - 1 \mid x \in S\}$. List the elements of X.
(3) Let $A = \{1, 2\}$ and $B = \{5, -4, 100\}$. Let $Y = \{a + b \mid a \in A, b \in B\}$. List the elements of Y.

INFORMAL DEFINITION 2.20. *The set of* **rational numbers** *is denoted by* $\mathbb{Q}$ *and is defined as follows*

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

EXAMPLE 2.21. The numbers $1 = \frac{1}{1}$, $-100 = \frac{-100}{1}$, $\frac{-1}{10}$, and $\frac{52}{13}$ are rational numbers. Later, in Theorem 4.53, we will see that the number $\sqrt{2} \approx 1.414213562$ is not a rational number; that is, there is no way to write $\sqrt{2}$ in the form $\frac{a}{b}$ where a and b are integers.

INFORMAL DEFINITION 2.22. *The set of* **real numbers** *is denoted by* $\mathbb{R}$ *and is defined as follows*

$$\mathbb{R} = \{x \mid x \text{ is a number with a decimal expansion}\}.$$

EXAMPLE 2.23. A real number is any number with a decimal expansion. The numbers $\sqrt{2} \approx 1.414213562$, $\pi \approx 3.14159$, $\frac{1}{2} = 0.5$, $-10 = -10.0$, and $5 = 5.0$ are all real numbers. Notice that natural numbers, integers, and rational numbers are all real numbers.

One can picture the real numbers as a line that goes infinitely in both directions. At each point on the line we have a real number given by its decimal expansion. We call this line the **real number line**. See Figure 4.

TOO MUCH INFORMATION 2.24. Note again that the definition of the rational numbers and real numbers is informal. What is a fraction? What is a decimal expansion? Does it even make sense to make a number that way? Yes, it does. If you want to get more formal and construct these number systems, then you can do so. Again, as with the integers and natural numbers, one can construct the set of rational numbers and the set of real numbers using set theory. Although, one requires limits to do so. For now we assume that the rational and real numbers exist and they satisfy their usual properties. More about this in ??????????????.

There is one other set that we need to define that is used quite a bit in mathematics. It is the set that contains nothing.

DEFINITION 2.25. The set with no elements is called the **empty set** and is denoted by $\emptyset$ or $\{\}$.

EXAMPLE 2.26. Consider the set $S = \{1, 2, 3\}$. Let $X = \{x \in S \mid 5 < x\}$. Thus X consists of all the elements x from S that satisfy the equation $5 < x$. Since no elements from S satisfy $5 < x$ we have that $X = \emptyset$. That is, X is the empty set. Notice that the empty set came in handy in this example. For without it, what would X be?

2.2. Exercises

(1) Find all the elements from the set $\{n \in \mathbb{Z} \mid 1 \leq n^2 \leq 100\}$.

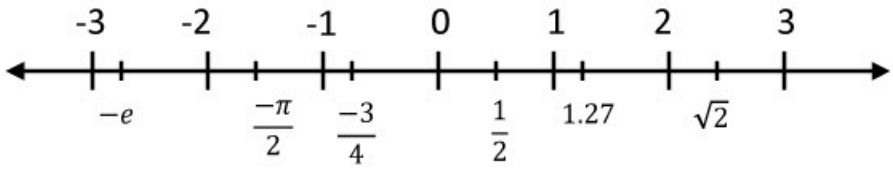


FIGURE 4. A picture of $\mathbb{R}$, viewed as the real number line

(2) Let $X = \{x \in \mathbb{R} \mid x^2 + 1 = 0\}$. What set is X equal to?
(3) List 10 elements from the set $\{x \in \mathbb{R} \mid x^2 \geq 1\}$. Does this set have a smallest element? Explain.
(4) Find all the elements in the set $\{x \in \mathbb{N} \mid x^2 \leq 9\}$.

(5) Let $S = \{1, 5, 7\}$ and $T = \{-1, 0, 10, 5\}$. Find all the elements in the set $\{a + b \mid a \in S, b \in T\}$.
(6) Let $S = \{1, 5, 7\}$ and $T = \{-1, 0, 10, 5\}$. Find all the elements in the set $\{a^2 \mid a \in S\}$.
(7) List 10 elements from the set $\{2x \mid x \in \mathbb{Z}\}$.
(8) List 10 elements from the set $\{x^2 \mid x \in \mathbb{Z}\}$.
(9) List 10 elements from the set $\{2x - 5y \mid x, y \in \mathbb{Z}\}$.
(10) Suppose that k is some fixed integer. List 10 elements from the set $\{xk \mid x \in \mathbb{Z}\}$.
(11) Suppose that r and s are two fixed integers. List 10 elements from the set $\{xr + ys \mid x, y \in \mathbb{Z}\}$.
(12) Use set-builder notation to write the set $\{-3, -2, -1, 0, 1, 2, 3, 4\}$ without listing each of its elements individually.
(13) Use set-builder notation to write the set $\{1, 2, 3, 4, \ldots, 100\}$ without listing each of its elements individually. By using set-builder notation, you are avoiding the use of "..." and are being more precise.
(14) Use set-builder notation to write the set of all positive odd numbers.
(15) Suppose that Γ is some set, where every element of Γ is a real number. Let $\Lambda = \{\beta^2 \mid \beta \in \Gamma\}$. Given that $2x-1 \in \Gamma$ for some real number x, what real number must then be an element of Λ?
(16) Logic puzzle: Let Γ and Λ be as in Exercise (15). Tony says, "I know an element of Λ." Mike says, "What is it?" Tony says, "I'm not going to tell you—then you would know a real number which must be in Γ." Mike says, "Now I know what number it is." What number is it?
(17) Suppose that $xy \in \{\gamma^2 \mid \gamma \in \mathbb{Z}\}$ and $y \neq 0$. What can you conclude about x?

Chapter 3

Logic

> Pure mathematics is, in its way, the poetry of logical ideas.
>
> Albert Einstein

In this chapter we introduce the basic ideas of logic. We need logic to study mathematics. We need to know what we mean by the statement "3 is odd and $5 < 7$" and the statement "If $x > 2$, then $x^2 > 4$." That is, we need to define when statements like "P and Q" and "If P, then Q" are true or false. We will do this in this chapter. We also introduce an important idea in mathematics: quantifiers. Quantifiers appear in mathematical statements such as "For every integer x, either $x \leq 5$ or $x > 5$" or "There exists an integer x where $2^x = 8$." Words like "for every" and "there exists" are quantifiers. We will study these in detail.

We would like to point out that although we use formal logical symbols such as $\wedge$, $\vee$, and $\Rightarrow$ in this chapter, we will discontinue their use in later chapters. Each symbol has an english version that goes with it and most mathematicians use the english version instead of the formal symbol. However, it is good to know what the logical symbols are and what they mean, so we have included them in this chapter.

3.1. Rules of logic

DEFINITION 3.1. A **proposition** is a mathematical sentence that is either true or false.

EXAMPLE 3.2. The expression

$$1 + 1 = 2$$

is a proposition because it is true. The expression

$$-10 > 5$$

is a proposition because it is false. The expression

$$15 > x$$

is not a proposition because it is neither true or false. It depends on what x is.

Given two propositions P and Q, sometimes we want to define a new proposition, say R, out of them. For example, we may want to define what "P and Q" means. One way to do this is with a **truth table**. In the left-most columns we list all the possible truth values of P and Q. In the next column we give the truth values of R as it depends on P and Q. The general form is as follows.

P	Q	some other proposition R
T	T	the truth value of R when P is true and Q is true
T	F	the truth value of R when P is true and Q is false
F	T	the truth value of R when P is false and Q is true
F	F	the truth value of R when P is false and Q is false

DEFINITION 3.3. Let P and Q be propositions. The **conjuction** of P and Q is written $P \wedge Q$ or "P and Q". It is defined to be true exactly when both P and Q are true. If either of P or Q are false, then $P \wedge Q$ is false. The truth table of $P \wedge Q$ is given by

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

EXAMPLE 3.4. The conjunction

$$(13 > 2) \wedge (|-2| = 2)$$

is true because $13 > 2$ is true and $|-2| = 2$ is true. The conjunction

$$(1 + 1 = 2) \text{ and } (-10 > 5)$$

is false because $1 + 1 = 2$ is true and $-10 > 5$ is false. The conjunction

$$(7 < 2) \wedge (2^3 = 8)$$

is false because $7 < 2$ is false and $2^3 = 8$ is true. The conjunction

$$(3 \text{ is an even number}) \text{ and } (15 \leq 14)$$

is false because "3 is an even number" is false and $15 \leq 14$ is false.

DEFINITION 3.5. Let P and Q be propositions. The **disjunction** of P and Q is written $P \vee Q$ or "P or Q". It is true when either P or Q are true. If both P and Q are false, then $P \vee Q$ is false. The truth table of $P \vee Q$ is given by

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

EXAMPLE 3.6. The disjunction

$$(5 > -3) \vee (10^2 = 1)$$

is true because $5 > -3$ is true. The disjunction

$$(100 \text{ is an odd number}) \text{ or } (10^2 = 100)$$

is true because $10^2 = 100$ is true. The disjunction

$$(3 < 10) \vee (15 = 15)$$

is true because both $3 < 10$ and $15 = 15$ are true. The disjunction

$$(10 < -20) \text{ or } (2 = 3)$$

is false because both $10 < -20$ and $2 = 3$ are false.

CHECK FOR UNDERSTANDING 3.7. Check if the following propositions are true or false.

(1) $(5 < 10)$ and $(-15 \geq -1000)$
(2) $(-5 > 10) \vee (-1 \geq -10)$
(3) (5 is even) $\wedge$ $(-1 \geq -10)$
(4) $(2! = 4)$ or $(1 > -1)$

DEFINITION 3.8. Let P be a proposition. The **negation**, or **denial**, of P is written $\neg P$ or "not P". It is true when P is false. It is false, when P is true. The truth table of $\neg P$ is given by

P	$\neg P$
T	F
F	T

TOO MUCH INFORMATION 3.9. Some books use $\sim P$ instead of $\neg P$ for the negation of P.

EXAMPLE 3.10. The proposition

$$\neg(5 > 10)$$

is true because $5 > 10$ is false. The proposition

$$\neg(2^2 = 4)$$

if false because $2^2 = 4$ is true. Consider the proposition

$$-5 \text{ is not a natural number.}$$

One can write this as $\neg(-5$ is a natural number.) This proposition is true because "-5 is a natural number" is false.

EXAMPLE 3.11. Let P be the proposition $5 > 10$. In this example we find the negation of P and simplify it. The negation of P is the proposition "It is not the case that $5 > 10$." This simplifies to the proposition $5 \leq 10$. Notice that $5 > 10$ is false while $5 \leq 10$ is true; that is, notice that P and $\neg P$ have opposite true values.

CHECK FOR UNDERSTANDING 3.12. Answer the following questions.

(1) Is the proposition $\neg(5 \geq 3)$ true or false?
(2) Is the proposition "7 is not a prime number" true or false?
(3) Find the negation of the proposition "10 is an even number."

DEFINITION 3.13. Let P and Q be propositions. The **implication** of P and Q is written $P \Rightarrow Q$ or "If P, then Q" or "P implies Q". It is false precisely when P is true and Q is false. Otherwise, it is true. The truth table of $P \Rightarrow Q$ is given by

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

EXAMPLE 3.14. The proposition

$$(5 > 3) \Rightarrow (2 = 2)$$

is true because $5 > 3$ is true and $2 = 2$ is true. The proposition

$$\text{If } 5 > 3, \text{ then } -1 = 5$$

is false because $5 > 3$ is true and $-1 = 5$ is false. The proposition

$$7 = 3 \text{ implies that } 7 > 2$$

is true because $7 = 3$ is false and $7 > 2$ is true. The proposition

$$\text{If } 17^2 = -10, \text{ then } 6^3 < 2$$

is true because $17^2 = -10$ is false and $6^3 < 2$ is false.

TOO MUCH INFORMATION 3.15. We know that Definition 3.13 and Example 3.14 are confusing. The reason is because there is no connection between P and Q in the "If P, then Q" examples that we gave in Example 3.14. The definition of implication will make more sense when we introduce quantifiers. This will allow us to use variables. See Example 3.34.

DEFINITION 3.16. Let P and Q be propositions. The **biconditional** of P and Q is written $P \Leftrightarrow Q$ or "P if and only if Q" or "P iff Q". It is true when either both P and Q are true, or both P and Q are false. Otherwise it is false. The truth table of $P \Leftrightarrow Q$ is given by

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

EXAMPLE 3.17. The proposition

$$(5 = 5) \Leftrightarrow (7 > 2)$$

is true because both $5 = 5$ and $7 > 2$ are true. The proposition

$$10 = 2 \text{ if and only if } (-3)^2 = 8$$

is true because both $10 = 2$ and $(-3)^2 = 8$ are false. The proposition

$$3 > 1 \text{ iff } 2 = 5$$

is false because $3 > 1$ is true and $2 = 5$ is false. The proposition

$$(10 \neq 10) \Leftrightarrow (100^2 \geq 7)$$

is false because $10 \neq 10$ is false and $100^2 \geq 7$ is true.

TOO MUCH INFORMATION 3.18. We know that Definition 3.16 and Example 3.17 are confusing. Again, as with implications, the definition of biconditionals will be made clear once we reach quantifiers and variables.

CHECK FOR UNDERSTANDING 3.19. Are the following propositions true or false?

(1) If $5 \leq 10$, then 7 is an even number.
(2) $9 + 2 \leq 15$ if and only if $(-10)^2 = 100$.
(3) If $1 + 2 + 3 = 6$, then 16 is an integer.
(4) 9 is a real number if and only if $10 > 123$.
(5) If 6 is an odd number, then $5 + 10 = 16$.

DEFINITION 3.20. A **propositional form** is a well-formed expression that consists of logical connectives, parentheses, and letters representing propositions.

EXAMPLE 3.21. $\neg P$, $(P \vee Q) \wedge P$, and $P \Leftrightarrow (P \vee Q)$ are propositional forms.

TOO MUCH INFORMATION 3.22. Notice that we have defined a propositional form as a "well-formed" expression. Without going into all the details, this just means that the expression must make sense. For example, $\Rightarrow QQ\wedge$ is not a propositional form because it is pure nonsense.

Too Much Information 3.23. Propositional forms differ from propositions. For example, $(5 > 3) \vee (2 = 7)$ is a proposition. It has a truth value—it is true. On the other hand, $P \vee Q$ is a propositional form—it has no truth value until propositions are plugged into P and Q.

Definition 3.24. Two propositional forms are **logically equivalent** if and only if they have the same truth tables.

Example 3.25. Consider the statements "P iff Q" and "(If P, then Q) and (If Q, then P)." Are these propositional forms logically equivalent? Yes. We can check it with a truth table. In the truth table below we use the logic versions of each statement to save space.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Notice that the columns under $P \Leftrightarrow Q$ and $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ are the same. Thus, $P \Leftrightarrow Q$ and $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ are logically equivalent. How does this help us? It tells us that "P iff Q" is true if and only if both "If P, then Q" and "If Q, then P" are true.

Example 3.26 (de Morgan's rules). Let P and Q be propositions. Then

(1) $\neg(P \vee Q)$ and $(\neg P) \wedge (\neg Q)$ are logically equivalent.
(2) $\neg(P \wedge Q)$ and $(\neg P) \vee (\neg Q)$ are logically equivalent.

The above facts are known as de Morgan's rules. We show part (1) and leave part (2) as an exercise. The following truth table shows that part (1) is true.

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$(\neg P) \wedge (\neg Q)$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

Example 3.27. de Morgan's rules allow us to negate statements of the form "P and Q" and "P or Q." Consider the statement

$$(5 > 7) \text{ and } (107 \in \mathbb{N}).$$

By de Morgan's rules, the negation of this statement is

$$\neg(5 > 7) \text{ or } \neg(107 \in \mathbb{N})$$

which simplifies to

$$(5 \leq 7) \text{ or } (107 \notin \mathbb{N}).$$

CHECK FOR UNDERSTANDING 3.28. Negate the following propositions.

(1) $(7.32 \notin \mathbb{N})$ and $(|-10| = 5)$
(2) $(2^{-2} = 4)$ or (5 is odd)

3.2. Quantifiers

DEFINITION 3.29. Let S be a set. Suppose that x is a variable whose value comes from S. An expression $P(x)$ involving the variable x such that whenever x is replaced by a value from S becomes a proposition, is called a **predicate**. S is called the **universe** of $P(x)$.

EXAMPLE 3.30. Let S be the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$. Let $P(n)$ be the expression $2^n < n!$. The expression $P(1)$ is $2^1 < 1! = 1$ which is false. The expression $P(2)$ is $2^2 < 2! = 2$ which is false. The expression $P(3)$ is $2^3 < 3! = 6$ which is false. The expression $P(4)$ is $2^4 < 4! = 24$ which is true. We see that once we plug in a natural number for n into $P(n)$ then we get a proposition that is either true or false. Hence, $P(n)$ is a predicate.

EXAMPLE 3.31. Let $S = \mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Consider the predicate $P(x)$ given by

$$(x > 5) \Rightarrow (x > 10).$$

Then $P(12)$ is the proposition

$$(12 > 5) \Rightarrow (12 > 10)$$

which is true; $P(6)$ is the proposition

$$(6 > 5) \Rightarrow (6 > 10)$$

which is false; and $P(-12)$ is the proposition

$$(-12 > 5) \Rightarrow (-12 > 10)$$

which is true.

DEFINITION 3.32. Let $P(x)$ be a predicate where x takes values from some set S. That is, S is the universe for $P(x)$.

(1) The proposition $(\exists x \in S)P(x)$ is read "there exists an x in S such that $P(x)$" or "for some x in S, $P(x)$" and is true precisely when there is at least one element x of S such that $P(x)$ is true.
(2) The proposition $(\forall x \in S)P(x)$ is read "for all x in S, $P(x)''$ and is true precisely when $P(x)$ is true for every x in S.

EXAMPLE 3.33. Let $S = \mathbb{Z}$ and $P(x)$ be the predicate

$$(x > 5) \text{ and } (x^2 = 81).$$

Notice that $P(9)$ is the proposition $(9 > 5)$ and $(9^2 = 81)$ which is true. Hence there exists an x in S where $P(x)$ is true. Thus,

$$(\exists x \in \mathbb{Z})((x > 5) \text{ and } (x^2 = 81))$$

is true. Notice that $P(6)$ is the proposition $(6 > 5)$ and $(6^2 = 81)$ which is false. Since $P(x)$ is not true for every integer x we see that

$$(\forall x \in \mathbb{Z})((x > 5) \text{ and } (x^2 = 81))$$

is false.

EXAMPLE 3.34. This is an example of why $P \Rightarrow Q$ is defined the way it is.

Let $S(x)$ be the predicate

$$\text{If } x > 3, \text{ then } x^2 > 9.$$

Then $S(4)$ is the proposition

$$\text{If } 4 > 3, \text{ then } 4^2 > 9$$

which is true. $S(0)$ is the proposition

$$\text{If } 0 > 3, \text{ then } 0 > 9$$

which is true. $S(-4)$ is the proposition

$$\text{If } -4 > 3, \text{ then } (-4)^2 > 9$$

which is true.

Note that if x is an integer and $x > 3$, then by squaring both sides of the inequality we have that $x^2 > 9$. Thus, whenever $x > 3$ is true, $x^2 > 9$ is true. Note that if $x > 3$ is false, then $S(x)$ is true by the definition of $P \Rightarrow Q$—this is because if P is false, then $P \Rightarrow Q$ is

always true. This shows that $(\forall x \in \mathbb{Z})S(x)$ is true since $S(x)$ is true for all integers x.

NOTATION 3.35. In math we don't always write the quantifiers. For example, suppose you are reading a math book and you run into the following:

"Let x be an integer. If x is even, then $x+1$ is odd."

or

"If x is an even integer, then $x+1$ is odd."

What do these statements mean? If you translate them into the format of this chapter, then they are saying the following:

"For every integer x, if x is even, then $x+1$ is odd."

or in logic

$$(\forall x \in \mathbb{Z})(x \text{ is even } \Rightarrow x+1 \text{ is odd. })$$

Consider the predicate

"There exists an integer x such that $2^x = 8$."

If we translate this into the logical format of this chapter we get

$$(\exists x \in \mathbb{Z})(2^x = 8).$$

Consider the expression $(\forall x \in S)P(x)$. When is $(\forall x \in S)P(x)$ false? It is false when there exists an x in S that makes $P(x)$ true. When is $(\forall x \in S)P(x)$ true? When every x in S makes $P(x)$ true. Thus, $\neg((\forall x \in S)P(x))$ is true when there exists some x from S that makes $P(x)$ false. And $\neg((\forall x \in S)P(x))$ is false when every element x in S makes $P(x)$ true. This is precisely when $(\exists x \in S)(\neg P(x))$ is true or false. This argument gives us the first part of Theorem 3.36. A similar argument shows that the second part is true.

THEOREM 3.36. *Let $P(x)$ be a predicate where x takes values from some set S. Then*

(1) $\neg((\forall x \in S)P(x)$ *is logically equivalent to* $(\exists x \in S)(\neg P(x))$
(2) $\neg((\exists x \in S)P(x)$ *is logically equivalent to* $(\forall x \in S)(\neg P(x))$

EXAMPLE 3.37. The negation of the proposition

There exists an integer x such that $2^x = 10$

is

$$\text{For every integer } x \text{ we have that } 2^x \neq 10.$$

EXAMPLE 3.38. The negation of the proposition

$$\text{For every integer } x \text{ we have that } x \text{ is even or } x \text{ is prime}$$

is

There exists an integer x such that x is odd and x is not prime.

Sometimes we need two quantifiers in a predicate. This is called nested quantifiers.

EXAMPLE 3.39. Consider the following sentence "For every natural number x, there exists a natual number y where $x \leq y$." In logic we write this as follows:

$$(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x \leq y)$$

What does this mean? What does it take to make the above sentence true? We would need that no matter what natural number x you pick there must be another natural number y where $x \leq y$. For example, for the natural number $x = 5$ one can let $y = 6$ and we have $x \leq y$. In general, given a natural number x we may set $y = x + 1$ and we have $x \leq y$. Thus the above sentence is true.

EXAMPLE 3.40. Consider the following sentence "There exists a natural number x, such that for all natural numbers y, we have that $x \leq y$." In logic we write this as follows:

$$(\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(x \leq y)$$

What does this mean? What does it take to make the above sentence true? Here we must produce a natural number x where $x \leq y$ no matter what natural number y we pick. For example, suppose we pick $x = 4$. This x will not make the above sentence true because if you choose $y = 2$ then $x \not\leq y$. However, if instead we choose $x = 1$ then $x \leq y$ for all natural numbers y because 1 is the smallest natural number. Hence the above sentence is true.

3.3. Exercises

Here are some definitions for this exercise set.

Let $n \in \mathbb{N}$ with $n > 1$. We say that n is a **prime** number if its only divisors are 1 and n. For example, 4 is not prime because 2 divides 4

and 2 is not equal to 1 or 4. The number 5 is prime, because the only divisors of 5 are 1 and 5.

Let $n \in \mathbb{N}$. A **proper divisor of** n is a divisor of n other than n itself. n is called a **perfect number** if n equals the sum of its proper divisors. For example, the proper divisors of the nuber 6 are 1, 2, and 3. And $6 = 1 + 2 + 3$. So 6 is a perfect number. The proper divisors of 4 are 1 and 2. Since $1 + 2 \neq 4$, we know that 4 is not a perfect number.

(1) Which of the following are true? Explain why or why not. Don't just write down true or false.
   (a) $(5 = |-5|) \wedge (3 > -2)$
   (b) $(2^3 = -8) \vee (13 < 0)$
   (c) $(2^3 = 8) \vee (1 < 10)$
   (d) $(1000 \text{ is prime }) \wedge (1 \geq 1)$
   (e) If 7 is prime, then $19 = 3 + 6$.
   (f) $(19 > 10) \Rightarrow (|-16| = 16)$
   (g) $(f(x) = |x| \text{ is differentiable at } 0) \wedge (7 \text{ is a perfect number})$
   (h) $\neg \left(\dfrac{x^3}{3} \text{ is an antiderivative of } x^2 \right)$
   (i) $\neg(\neg(3 \text{ is an odd number}))$

(2) Which of the following are true? Explain why or why not. Don't just write down true or false.
   (a) $(\exists\, x \in \mathbb{N})(x^2 = 4)$
   (b) $(\forall\, x \in \mathbb{Z})((x > 10) \vee (x < 10))$
   (c) There exists an $x \in \mathbb{Z}$ where $x^2 = 2$.
   (d) $(\forall\, x \in \mathbb{Z})((x > 2) \Rightarrow (x^2 > 1))$
   (e) Let x be in $\mathbb{Z}$. If $x > 2$, then $-x < -10$.
   (f) $(\exists\, x \in \mathbb{Z})((-1 \leq x < 10) \Rightarrow (x^2 = 9))$
   (g) Let $x \in \mathbb{Z}$. If $-1 \leq x < 10$, then $x^2 = 9$.
   (h) Let $x \in \mathbb{Z}$. We have that $x > 2$ if and only if $x^2 \geq 4$.
   (i) $(\exists\, x \in \mathbb{Z})((x > 2) \Leftrightarrow (x^2 \geq 4))$
   (j) $(\exists x \in \mathbb{Z})((x^2 = 1) \wedge (x > 2))$
   (k) $(\forall x \in \mathbb{Z})((x > 100) \vee (x < 101))$
   (l) $(\forall x \in \mathbb{Z})((1 \leq x \leq 3) \Rightarrow (x > -1))$
   (m) $(\forall x \in \mathbb{Z})((x^3 = 8) \Leftrightarrow (x \geq -2))$

(3) Are the two given propositions logically equivalent? Use a truth table to check.
   (a) $\neg\,(P \wedge Q)$ and $(\neg\, P) \vee (\neg\, Q)$.
   (b) $P \Rightarrow Q$ and $(\neg\, Q) \Rightarrow (\neg\, P)$.
   (c) $P \wedge (\neg\, Q)$ and $(P \vee Q) \Leftrightarrow P$.
   (d) $P \wedge Q$ and $P \vee (P \Rightarrow Q)$

(4) Find the negation of the following expresions.
   (a) $x \in A$ and $x \in B$
   (b) $x \in A$ or $x \notin B$
   (c) x is an integer and $x \geq 0$
   (d) $(\forall\, x \in \mathbb{Z})((x > 10) \vee (x < 10))$
   (e) There exists and odd perfect number.
   (f) $(\exists\, x \in \mathbb{N})(2^x = 5)$
   (g) Let $x \in \mathbb{Z}$. Then $1/x$ is not an integer.
   (h) $x \in \mathbb{Z}$ and x is odd.

3.4. Fun math facts

The first four perfect numbers are 6, 28, 496, and 8128. Notice that they are all even. A famous conjecture of number theory is that there are no odd perfect numbers. (A conjecture is a statement that someone thinks is true, but no one knows whether or not it is true.) No one has ever found an odd perfect number.

Notice that $2^1(2^2-1) = 2\cdot 3 = 6$, $2^2(2^3-1) = 4\cdot 7 = 28$, $2^4(2^5-1) = 16 \cdot 31 = 496$, and $2^6(2^7-1) = 64 \cdot 127 = 8128$. Here is an interesting fact: If n is an even perfect number, then n can be written in the form $n = 2^{m-1}(2^m - 1)$ where $2^m - 1$ is prime. Furthermore, if $2^m - 1$ is prime, then $n = 2^{m-1}(2^m - 1)$ is perfect.

It is unknown whether or not there are an infinite number of even perfect numbers. According to the article "Perfect Numbers : An Elementary Introduction" by John Voight, as of the year 1998, the largest even perfect number found is $2^{3021376}(2^{3021377}-1)$. It has 1819050 digits.

Part 2

Main Stuff

Chapter 4

Proof techniques

EPIGRAPH.

PERSON

In mathematics—unlike any other field of study—to accept something as true, we require *absolute* certainty. If you make a claim, then we mathematicians will insist that you demonstrate its correctness with an unbroken chain of logical steps. In other words, you must write a proof.

This textbook was designed as a transition from lower-level math courses, which tend to be more heavily computational in nature, to upper-level math courses, which tend to be more theoretical. So, in your later math courses, many of the homework and test questions will consist of writing proofs. For success in this course as well as your later math courses, this chapter is therefore critical.

4.1. Our starting assumptions

A few sections from now, we will prove that $\sqrt{2}$ is an irrational number. This is not an obvious fact, so to convince you that it is true, we should be very careful in our reasoning. Along the way, we will make use of the fact that every fraction can be written in lowest terms. Is that an obvious fact? Can we use it in a proof? Perhaps it is obvious to you, but not so obvious to someone else. Part of the power of mathematics comes from its complete lack of ambiguity, and so we refuse to tolerate this level of subjectivity. To remedy the situation, we create a list of facts about numbers that we all agree to accept and that we all agree can be used as a step in a proof.

We now state these main assumptions that will serve as our starting point for proofs. The first of these spells out the fundamental properties of equality.

ASSUMPTION 4.1.

(1) *If a is any element of any set, then $a = a$. (reflexive property of equality)*
(2) *If $a = b$ and $P(a)$ is true, then $P(b)$ is true. (substitution property of equality)*

Item (1) is fairly straightforward; it says that everything equals itself. Item (2) is extraordinarily general; it says that if two things are equal, then you're allowed to substitute one for the other. The two things can be any type of object: numbers, sets, functions, whatever.

EXAMPLE 4.2. Suppose we know that $z^2 - 1 = (z + 1)(z - 1)$ and that $y > z^2 - 1$. Apply the substitution property of equality.

Answer: Substituting $(z + 1)(z - 1)$ for $z^2 - 1$, we get $y > (z + 1)(z - 1)$.

⟨In Item (2) of Assumption 4.1, $z^2 - 1$ takes the place of a, and $(z+1)(z-1)$ takes the place of b. The predicate $P(x)$ is "$y > x$." We are given that $P(z^2-1)$ is true. So (2) then tells us that $P((z+1)(z-1))$ is also true.⟩

TOO MUCH INFORMATION 4.3. You may be familiar with the symmetric and transitive properties of equality. Both of those follow from Assumption 4.1.

Our next assumption deals with the real numbers. Note that the last item, property (17), involves some vocabulary we will not encounter until Chapter 11.

ASSUMPTION 4.4. *We assume that there exists a set $\mathbb{R}$ such that there are two elements $0, 1 \in \mathbb{R}$ as well as two binary operations $+$ and $\cdot$ on $\mathbb{R}$ and a relation $<$ on $\mathbb{R}$ such that the following statements are true.*

(1) *$\forall a, b \in \mathbb{R}$, we have that $a + b \in \mathbb{R}$. ("$\mathbb{R}$ is closed under addition.")*
(2) *$\forall a \in \mathbb{R}$, we have that $a + 0 = a$. ("0 is an additive identity for $\mathbb{R}$.")*
(3) *$\forall a \in \mathbb{R}$, we have that $\exists b \in \mathbb{R}$ such that $a + b = 0$. ("Every element a of $\mathbb{R}$ has an additive inverse.")*
(4) *$\forall a, b, c \in \mathbb{R}$, we have that $(a + b) + c = a + (b + c)$. ("$\mathbb{R}$ is associative under addition.")*

(5) $\forall a, b \in \mathbb{R}$, *we have that* $a + b = b + a$. *("$\mathbb{R}$ is commutative under addition.")*
(6) $\forall a, b \in \mathbb{R}$, *we have that* $a \cdot b \in \mathbb{R}$. *("$\mathbb{R}$ is closed under multiplication.")*
(7) $\forall a \in \mathbb{R}$, *we have that* $a \cdot 1 = a$. *("1 is a multiplicative identity for $\mathbb{R}$.")*
(8) $\forall a \in \mathbb{R}$ *such that* $a \neq 0$, *we have that* $\exists b \in \mathbb{R}$ *such that* $a \cdot b = 1$. *("Every nonzero element a of $\mathbb{R}$ has a multiplicative inverse.")*
(9) $\forall a, b, c \in \mathbb{R}$, *we have that* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. *("$\mathbb{R}$ is associative under multiplication.")*
(10) $\forall a, b \in \mathbb{R}$, *we have that* $a \cdot b = b \cdot a$. *("$\mathbb{R}$ is commutative under multiplication.")*
(11) $\forall a, b, c \in \mathbb{R}$, *we have that* $a \cdot (b + c) = a \cdot b + a \cdot c$. *("$\mathbb{R}$ satisfies the distributive property.")*
(12) $0 \neq 1$. *("Zero is not equal to one.")*
(13) $\forall a, b \in \mathbb{R}$, *if* $a > 0$ *and* $b > 0$, *then* $a + b > 0$. *("The set of positive real numbers is closed under addition.")*
(14) $\forall a, b \in \mathbb{R}$, *if* $a > 0$ *and* $b > 0$, *then* $ab > 0$. *("The set of positive real numbers is closed under multiplication.")*
(15) $\forall a, b, c \in \mathbb{R}$, *if* $a > b$, *then* $a + c > b + c$. *("Addition by a real number preserves inequalities.")*
(16) $\forall a \in \mathbb{R}$, *we have that* $0 > a$ *or* $a = 0$ *or* $a > 0$. *("$\mathbb{R}$ satisfies the Law of Trichotomy.")*
(17) *Every nonempty bounded subset of* $\mathbb{R}$ *has a least upper bound. ("$\mathbb{R}$ is complete.")*

Each item in Assumption 4.4 is called an **axiom** (that is, a defining assumption) for the real numbers.

Too Much Information 4.5. You are already familiar with Axioms 1–16. We know that. That's the point. Because you already accept them as true, it is reasonable to use them as a starting point that we can all agree on. And so we can also accept as true any facts that follow logically from them, including some spectacular and non-obvious results. In Chapter 11, we will study Axiom 17 in detail; as you become familiar with it, it will come to seem as natural as the other axioms.

Too Much Information 4.6. Axioms 1–4 say that $\mathbb{R}$ is a "group" under addition. In contrast, the natural numbers do not form a group under addition, because they do not contain the additive identity element. Axioms 1–5 say that $\mathbb{R}$ is a "commutative" (or "abelian") group under addition. Similarly, the corresponding axioms for multiplication, that is, Axioms 6–9, say that the set of nonzero elements of $\mathbb{R}$ forms a

group under multiplication; adding Axiom 10 to these says that that group is commutative as well.

Axioms 1–10, together with Axiom 11, say that $\mathbb{R}$ is a "ring." (Some authors, though, omit Axiom 7 from the list of ring axioms.) Because $\mathbb{R}$ is a ring that also satisfies Axiom 10, we say that $\mathbb{R}$ is a "commutative ring." The integers also form a ring. And because $\mathbb{R}$ is a commutative ring that also satisfies Axioms 8 and 12, we say that $\mathbb{R}$ is a "field." The rational numbers and complex numbers give us two other examples of fields. The integers do not form a field, because not every nonzero integer has a multiplicative inverse in the integers. You will learn more about groups, rings, and fields in a course on Abstract Algebra.

From your Linear Algebra course, you may remember that the field axioms encompass the axioms for a "vector space"; hence every field is a vector space over itself.

Being a field that also satisfies Axioms 13–16, $\mathbb{R}$ is an "ordered field." The rational numbers also form an ordered field, whereas the complex numbers do not. The complete list of axioms in Assumption 4.4 asserts that $\mathbb{R}$ is a "complete ordered field." These axioms were not chosen haphazardly. In fact, it can be shown in a precise way that $\mathbb{R}$ is completely determined by them. That is, any other complete ordered field must be essentially the same as (more precisely: "isomorphic to") $\mathbb{R}$. (To put it in technical terms, we can prove that Assumption 4.4 is "categorical.") One typically does just that as part of an Analysis course. Even your professor may be surprised to know, though, that we have more axioms here than we really need. For example, we do not need to have the commutative property of addition on this list, because we can prove that fact from the other axioms—see the exercises at the end of Chapter 11. However, for our first few proofs, we would like to have the commutative property of addition at our disposal, and so we choose include it in our starting assumptions, even though it's overkill.

Too Much Information 4.7. Note that there are many true statements about the real numbers not listed in Assumption 4.4. For example, it is true that $\forall a \in \mathbb{R}$, we have that $0 \cdot a = 0$. However, this property is not one of our starting assumptions. In fact, we can use Assumption 4.4 to prove that $\forall a \in \mathbb{R}$, we have that $0 \cdot a = 0$. We try to begin with as few starting assumptions as possible, then prove what we can from there.

Similarly, we try to begin with as few symbols as possible, then define others from there. So we assume the existence of addition and multiplication, but then we can define subtraction and division in terms

of them. (See Section 4.) Also notice we do not use the symbols $\leq$, $\geq$, or $>$ in the axioms, because those can all be defined in terms of $<$.

DEFINITION 4.8. We define $a \geq b$ to mean that $a > b$ or $a = b$. We define $a < b$ to mean that $b > a$. And we define $a \leq b$ to mean that $a = b$ or $a < b$.

We frequently combine inequalities into *compound inequalities* such as "$4 \leq x < y \leq 7$," which means "$4 \leq x$ and $x < y$ and $y \leq 7$."

We now state our axioms for the integers.

ASSUMPTION 4.9. *We assume that there exists a set $\mathbb{Z}$ such that:*

(1) *If $n \in \mathbb{Z}$, then $n \in \mathbb{R}$. ("Every integer is a real number.")*
(2) *$0, 1 \in \mathbb{Z}$. ("0 and 1 are integers.")*
(3) *$\forall a, b \in \mathbb{Z}$, we have that $a + b \in \mathbb{Z}$. ("$\mathbb{Z}$ is closed under addition.")*
(4) *$\forall a \in \mathbb{Z}$, we have that $-a \in \mathbb{Z}$. ("The additive inverse of an integer is an integer.")*
(5) *$\forall a, b \in \mathbb{Z}$, we have that $a \cdot b \in \mathbb{Z}$. ("$\mathbb{Z}$ is closed under multiplication.")*
(6) *Suppose S is a set such that $1 \in S$ and such that if $x \in S$, then $x \in \mathbb{R}$ and $x + 1 \in S$. It follows that if $n \in \mathbb{Z}$ and $n > 0$, then $n \in S$. ("The set of positive integers obeys the principle of mathematical induction.")*

TOO MUCH INFORMATION 4.10. You may have noticed that item (6) is a bit involved. Indeed, we have an entire chapter (Chapter 5) devoted to that axiom, which formalizes the principle of mathematical induction.

TOO MUCH INFORMATION 4.11. Notice that the statement "The multiplicative inverse of a nonzero integer is an integer." is not on this list. And for good reason: It is not true. Counterexample: $2 \in \mathbb{Z}$, but $1/2 \notin \mathbb{Z}$.

Now that we have introduced $\mathbb{Z}$ more formally, we can define $\mathbb{N}$ more rigorously.

DEFINITION 4.12. We define $\mathbb{N} := \{n \in \mathbb{Z} \mid n > 0\}$. Elements of $\mathbb{N}$ are called **natural numbers**.

Too Much Information 4.13. You might recall that earlier, we had an informal definition of natural numbers, namely, Informal Definition 2.6, which gave us some intuition about what natural numbers are but is too "fuzzy" to use in proofs. In contrast, Definition 4.48 is a precise mathematical definition that we can use in rigorous proofs.

4.2. Proofs from Axioms – put as optional at end

Before getting started with any proof, it is a good idea to identify the following information: What statements are given? What statement are we trying to prove? (In other words, what do we *know*, and what do we want to *show*?) Also, what definitions, axioms, and previously proven statements seem relevant?

NOTE TO OURSELVES: SOMETHING TO EMPHASIZE: AT EVERY STEP, ASK YOURSELF, IS IT SOMETHING WE *KNOW* OR SOMETHING WE WANT TO *SHOW*?

MORE NOTES TO OURSELVES:

SO MAYBE WE SHOULD HAVE EXERCISES AND EXAMPLES WHERE STUDENTS HAVE TO DO SOME BABY STEPS, SUCH AS: IDENTIFY THE GIVEN INFORMATION; IDENTIFY THE STATEMENT WE'RE TRYING TO PROVE; IDENTIFY DEFINITIONS, AXIOMS, AND THEOREMS THAT SEEM RELEVANT.

Immediate consequences of the assumptions

Example 4.14. Suppose a problem says: "Let $x, y, z \in \mathbb{R}$. Prove that if $x + y = x + z$, then $y = z$." What statements are given? What statement are we trying to prove?

Answer. Given information (what we *know*): $x, y, z \in \mathbb{R}$. $x + y = x + z$.

We are trying to prove (what we want to *show*): $y = z$.

(For a problem that says, "Prove that if ____, then ____," the "if" part is always part of the given information, and the "then" part is what we want to show.)

CHECK WE SAY SOMEWHERE THAT IN $x, y, z \in \mathbb{R}$ THE COMMAS MEAN AND.

Example 4.15. Let $x, y, z \in \mathbb{R}$. Prove in minute detail that if $x + y = x + z$, then $y = z$.

Proof. We know that $x + y = x + z$.
By Axiom (3) of Assumption 4.4, because $x \in \mathbb{R}$, we know that there exists $\exists b \in \mathbb{R}$ such that $x + b = 0$.
So $b + (x + y) = b + (x + z)$.

So $(b + x) + y = (b + x) + z$, by the associative property of addition.
So $(x + b) + y = (x + b) + z$, by the commutative property of addition.
So $0 + y = 0 + z$, by substitution.
Therefore $y = z$, by Axiom (2) of Assumption 4.4. ■

Our next example illustrates how we can use a previously proven statement to go from one step to the next in a proof.

EXAMPLE 4.16. Let $x, y \in \mathbb{R}$. Prove in minute detail that if $x + y = x$, then $y = 0$.

PROOF. We are given that $x + y = x$.
So $x + y = x + 0$, by Axiom (2) of Assumption 4.4 and substitution.
So $y = 0$, by the statement we proved in Example 4.15.⟨*Note that* 0 *takes the place of* z.⟩ ■

TOO MUCH INFORMATION 4.17. Here is another proof of the statement in Example 4.16.

PROOF. We know that $x + y = x$.
By Axiom (3) of Assumption 4.4, because $x \in \mathbb{R}$, we know that there exists $\exists b \in \mathbb{R}$ such that $x + b = 0$.
So $b + (x + y) = b + x$.
So $(b + x) + y = b + x$, by the associative property of addition.
So $(x + b) + y = (x + b) + z$, by the commutative property of addition.
So $0 + y = 0$, by substitution.
Therefore $y = 0$, by Axiom (2) of Assumption 4.4. ■

Both proofs are correct. Which proof do you like better? Most mathematicians would prefer our first proof, because it's shorter. After all, we already did all that work in the first place to prove the statement in Example 4.15. Why do all that work all over again? See Remark 4.26 for another take on this.

EXAMPLE 4.18. Suppose a problem says: "Prove that if $y \in \mathbb{R}$, then $0 \cdot y = 0$." Which axioms, definitions, and previously proven statements seem relevant?

Possible answer. Axiom (2) of Assumption 4.4 seems relevant, because it is the most important property of the number 0.

EXAMPLE 4.19. Prove in minute detail that if $y \in \mathbb{R}$, then $0 \cdot y = 0$.

PROOF. Let $y \in \mathbb{R}$.
By Axiom 2 of Assumption 4.4, we know that $0 + x = x$ for all $x \in \mathbb{R}$.
In particular, taking $x = 0$, we get $0 + 0 = 0$.

So

$$\begin{aligned} 0 \cdot y &= (0+0) \cdot y && \text{(by substitution)} \\ &= 0 \cdot y + 0 \cdot y && \text{(by the distributive property)} \end{aligned}$$

Let $z = 0 \cdot y$.
Then $z = z + z$, by substitution.
So $z = 0$, by the statement we proved in Example 4.16.⟨*Note that z takes the place of both x and y.*⟩
Therefore $0 \cdot y = 0$, by substitution. ■

TOO MUCH INFORMATION 4.20. A few comments on Example 4.19. We use the word "Let" to introduce a variable for the first time. So once we write "Let $y \in \mathbb{R}$," then y is a fixed (that is, unchanging) real number that we can work with.

Believe it or not, we're not being as picky as we could be in these proofs. For instance, in one step in Example 4.19, we applied the statement from Example 4.16. Technically, to apply that statement, first we should have established that $z \in \mathbb{R}$. We could have argued that $z \in \mathbb{R}$ because $0 \in \mathbb{R}$ and $y \in \mathbb{R}$ and $\mathbb{R}$ is closed under multiplication. Even in these "minute detail" proofs, we're willing to allow a very small amount of "hand waving" like that. It's a judgment call as to when it's OK to skip steps—ask your professor for guidance.

Finally, you may wonder why we didn't just add $-z$ to both sides of the equation $z = z + z$. The reason is that we do not yet know that each real number has a unique additive inverse, and in these early, nitpicky proofs, we don't want to refer to $-z$ until we know that there's just one $-z$.

EXAMPLE 4.21. Suppose a problem says: "Let x, y, z be real numbers such that $x > y$ and $y > z$. Prove that $x > z$." Which axioms, definitions, and previously proven statements seem relevant?

Possible answer. We do not have any definitions or previously proven statements involving inequalities. So we will certainly need to use some or all of Axioms (13)–(16).

EXAMPLE 4.22. Let x, y, z be real numbers such that $x > y$ and $y > z$. Prove in minute detail that $x > z$.

PROOF. We know that $x > y$ and $y > z$.
By Axiom (3) of Assumption 4.4, $\exists b \in \mathbb{R}$ such that $y + b = 0$.
Similarly, by Axiom (3) of Assumption 4.4, $\exists c \in \mathbb{R}$ such that $z + c = 0$.
By Axiom (15) of Assumption 4.4, we get that $x + b > y + b$ and $y + c > z + c$.
So $x + b > 0$ and $y + c > 0$, by substitution.

So $(x + b) + (y + c) > 0$, by Axiom (13) of Assumption 4.4.
So $x + (b + (y + c)) > 0$, by the associative property of addition.
⟨*Here we are treating $y+c$ as a single real number, which is OK, because the real numbers are closed under addition.*⟩
So $x + ((b + y) + c) > 0$, by the associative property of addition.
So $x + ((y + b) + c) > 0$, by the commutative property of addition.
So $x + (0 + c) > 0$, by substitution.
So $x + c > 0$, by Axiom (2) of Assumption 4.4.
So $(x + c) + z > 0 + z$, by Axiom (15) of Assumption 4.4.
So $(x + c) + z > z$, by Axiom (2) of Assumption 4.4.
So $x + (c + z) > z$, by the associative property of addition.
So $x + (z + c) > z$, by the commutative property of addition.
So $x + 0 > z$, by substitution (using an equation we *know* from earlier, namely $z + c = 0$).
Therefore $x > z$, by Axiom (2) of Assumption 4.4.
⟨*Whew! It certainly takes more work than you might think to prove a statement in such gory detail. Rest assured, soon we will be skipping a lot of these steps.*⟩ ■

Too Much Information 4.23. If you sat down and tried to do Example 4.22 as a homework problem, it's pretty unlikely that you would just sit down, start writing, and this proof would just flow right out. More likely, you need to do a bunch of scratch work first. Think of writing a proof as more similar to writing an essay than to doing, say, a Calculus problem. You should expect to have to write a few drafts before you get to your final version. Here, for example, is some of the scratch work / thought process we might have done before coming up with the solution in Example 4.22:

MAYBE PUT THIS IN A THOUGHT BUBBLE COMING OUT OF A PERSON'S HEAD?

Let's try to use the axiom which tells us that the sum of two positive numbers is positive.

But we don't have any positive numbers yet, so we can't use that yet. All we have is $x > y$ and $y > z$.

But we do know $x - y$ is positive and $y - z$ is positive.

So what if we add those . . . ?

Example 4.24. Prove in minute detail that if $a = b$ and $b = c$, then $a = c$. (Side note: This is known as the transitive property of equality.)

Proof. Use the substitution property of equality. Specifically, substitute a for b in the equation $b = c$ to get $a = c$. ■

EXAMPLE 4.25. Prove in minute detail that if $a, b, c \in \mathbb{Z}$, then $ab + ac \in \mathbb{Z}$.

PROOF. Let $a, b, c \in \mathbb{Z}$.
Then $a, b, c \in \mathbb{R}$, by axiom (1) of Assumption 4.9.
Then $a(b + c) = ab + ac$, by the distributive property. ⟨*Small technicality: Before using the distributive property, we first established that* $a, b, c \in \mathbb{R}$*, because Assumption 4.4 applies only to real numbers.*⟩
We know $b + c \in \mathbb{Z}$, because $\mathbb{Z}$ is closed under addition and $b, c \in \mathbb{Z}$.
So $a(b+c) \in \mathbb{Z}$, because $\mathbb{Z}$ is closed under multiplication, and $a, b+c \in \mathbb{Z}$.
So $ab + ac \in \mathbb{Z}$, by substitution. ■

TOO MUCH INFORMATION 4.26. In our proof in Example 4.25, we took one of many possible paths. Alternatively, we could have first used closure under multiplication to show that $ab, ac \in \mathbb{Z}$, then used closure under addition to show that $ab + ac \in \mathbb{Z}$. It is typical to have many different ways to prove a statement. As long as every step in these proofs is valid, they are all correct—no valid proof is "more correct" than another. (Contrast that to science, philosophy, or even everyday life, where we often find certain pieces of evidence or lines of reasoning more convincing than others.)

That doesn't mean we *like* all proofs equally. We prefer proofs that are as short as possible, with no wasted steps. It's a bit like driving a car from one place to another. We have a starting point (the given information) and a destination (the statement we're trying to prove). There are many different routes we can take to get from where we are to where we want to go. Any route will will get us there, so long as we follow the rules of the road, but we prefer routes that get us there as quickly as possible.

CHECK FOR UNDERSTANDING 4.27. Fill in the blanks in this proof of this statement:
Let $x, y \in \mathbb{R}$. Prove in minute detail that if $x > 0 > y$, then $0 > xy$.

PROOF. We know $x > 0$ and $0 > y$.
By ____, $\exists b \in \mathbb{R}$ such that $y + b = 0$.
So $0 + b > y + b$, by ____.
So $0 + b > 0$, by ____.
So $b > 0$, by ____.
So $xb > 0$, by ____.
So $xb + xy > xy$, by ____.
So $x(b + y) > xy$, by ____.
So $x(y + b) > xy$, by ____.
So $x \cdot 0 > xy$, by ____.
So $0 \cdot x > xy$, by ____.
So $0 > xy$, by ____.
■

From this point on, we will skip many of these steps when doing proofs. For example, in the future we may go directly from "$2n - 4 = 3n+7$" to "$-11 = n$" without spelling out all the axioms used. (In case you're curious, they're the ones involving additive inverses, additive identity, associative property, distributive property, and multiplicative identity.) The homework problems where we ask you to write out all these steps are the ones that say, "Prove in minute detail . . ."

4.3. Direct Proofs

In the next several sections, we will discuss several different proof techniques. We begin with the most straightforward one, namely the "direct proof."

Suppose we want to prove that $P \Rightarrow Q$ is true. One way to do this is with a direct proof. The method involves the following steps.

Direct proof of $P \Rightarrow Q$

- **Step 1.** Assume that P is true.
- **Step 2.** String together other statements and theorems that you know are true with the fact that P is true. In this step, to get from one line to the next, we may use only:
  - The given information (that is, P)
  - Definitions

  - Assumptions (for example, Assumption 4.4)
  - Previously proven statements (including previous theorems, previous lines in a proof, homework problems—anything that's been proven before)
- **Step 3.** Repeat Step 2 until you arrive at the fact that Q is true.
- **Step 4.** Because starting with the fact that P is true leads to the fact that Q is true, we conclude that the statement $P \Rightarrow Q$ is true.

DEFINITION 4.28. Let x be an integer. We say that x is **even** if there exists an integer k where $x = 2k$. We say that x is **odd** if there exists an integer k where $x = 2k + 1$.

EXAMPLE 4.29. The integer 5 is odd since $5 = 2(2)+1$. The integer 100 is even since $100 = 2(50)$. The integer 0 is even since $0 = 2(0)$. The integer -15 is odd since $-15 = 2(-8) + 1$.

THEOREM 4.30. *If x and y are even integers, then $x + y$ is even.*

PROOF. Suppose that x and y are even integers. Then there exist integers a and b where $x = 2a$ and $y = 2b$. So $x+y = 2a+2b = 2(a+b)$. Since $a + b$ is an integer, we see that $x + y$ is even. ■

DEFINITION 4.31. Let x and y be integers with $x \neq 0$. We say that x **divides** y if there exists an integer k where $xk = y$. If x divides y, then we say that x is a **divisor** of y and we write $x|y$. If x does not divide y, then we write $x \nmid y$.

EXAMPLE 4.32. Since $5(2) = 10$, we see that 5 divides 10. So we write $5|10$. Since $(-6)(-2) = 12$, we see that -6 divides 12. So we write $-6|12$.

Note that there is no integer k with $3k = 2$ (we would need $k = \frac{2}{3}$ which isn't an integer). Therefore 3 does not divide 2 and we write $3 \nmid 2$.

THEOREM 4.33. *Suppose that x, y, and z are integers where $x|y$ and $x|z$. Then $x|(y+z)$*

PROOF. Since $x|y$, there is an integer k with $xk = y$. Since $x|z$, there is an integer m with $xm = z$. Thus $y+z = xk+xm = x(k+m)$. Since $k+m$ is an integer, we see that x divides $y+z$. ■

EXAMPLE 4.34 (Common Mistake). The following attempt at a proof contains a common mistake that we've seen many times. Find the error. "Suppose that x, y, and z are integers where $x|y$ and $x|z$. Prove that $x|(y+z)$. *Proof.* We know there exists an integer k with $xk = y$, by def. of divides. Also, we know there exists an integer k with $xk = z$, by def. of divides. So $y+z = xk+xk = x(2k)$. Since $2k$ is an integer, therefore $x|y+z$, by def. of divides."

The error is that the variable k is overused. The variable k was introduced in the line "We know there exists an integer k with $xk = y$ . . ." *Once a variable has been introduced, it cannot be introduced again.* So in the next sentence, we should use a different variable instead of k. That's why, in Thm. 4.33, we used an m.

The reason for this rule becomes clear when you plug in numbers. Imagine, for example, that $x = 5$, $y = 15$, $z = 20$. You can't have the same k for both x and y.

EXAMPLE 4.35 (Common Mistake). The following attempt at a proof contains a common mistake that we've seen many times. Find the error. "Prove that if $x \in \mathbb{Z}$, then $x|x^2$.*Proof* First, $x|x^2$ means $xk = x^2$ for some $k \in \mathbb{Z}$. Solve for k to get $k = x$, which is an integer."

The error is that in the first line, we do not *know* that $x|x^2$—that's something we're trying to *show*. The logic is completely backwards. The "proof" above is really scratch work we might do in order to get the idea of how to prove it. See the next example for a correct proof.

EXAMPLE 4.36. Prove that if $x \in \mathbb{Z}$, then $x|x^2$.

PROOF. We know $x^2 = x \cdot x$, and $x \in \mathbb{Z}$.
So $x|x^2$, by def. of "divides." ■

TOO MUCH INFORMATION 4.37. Notice that superficially, the correct proof in Example 4.36 *looks* a lot like the incorrect proof in Example 4.35. They use the same definition, and a lot of the same words. But there is a world of difference between them. Correct proofs flow in a logical order: We *start* with what we *know*. At each step, we rely

only on facts that we *know* up to that point. Then we *end* with what we're trying to *show*.

We now introduce the idea of congruence modulo an integer. This is an important tool in number theory. (Indeed, it is used in all branches of mathematics.)

DEFINITION 4.38. Let n be an integer with $n \geq 2$. Let x and y be integers. If n divides $x - y$ then we say that x is **congruent** to y modulo n and write $x \equiv y (\text{mod } n)$. If n does not divide $x - y$ then we say that x is not **congruent** to y modulo n and we write $x \not\equiv y (\text{mod } n)$.

EXAMPLE 4.39. Note that $32 \equiv 7 (\text{mod } 5)$ because $32 - 7 = 25$ and 5 divides 25. Note that $10 \not\equiv 26 (\text{mod } 7)$ because $10 - 26 = -16$ and 7 does not divide -16. Note that $1 \equiv -5 (\text{mod } 3)$ because $1 - (-5) = 6$ and 3 divides 6.

The main fact to notice about congruence is the following: Two integers are congruent modulo n if they differ by a multiple of n. For example, $100 - 4 = 96 = 3(32)$. We see that 100 and 4 differ by a multiple of 3, so $100 \equiv 4 (\text{mod } 3)$.

EXAMPLE 4.40. Can one add equations modulo n? Yes. Before we delve into the theoretical formulation of this idea, let's see an example first. Let $n = 3$. Notice that $5 \equiv 17 (\text{mod } 3)$ because $5 - 17 = -12$ which is divisible by 3 since $-12 = 3(-4)$. Notice also that $-12 \equiv 6 (\text{mod } 3)$ because $-12 - 6 = -18$ which is divisible by 3 since $-18 = 3(-6)$. So we have two equations modulo three: $5 \equiv 17 (\text{mod } 3)$ and $-12 \equiv 6 (\text{mod } 3)$. Without thinking if we are doing something that makes sense, let's add the two equations and see if it works. Adding we get that $-7 \equiv 23 (\text{mod } 3)$. Notice that we added 5 and 12 to get -7 and we added 17 and 6 to get 23, but we did not add the 3's. Let's check if what we did works. Notice that $-7 - 23 = -30$ which is divisible by 3 since $-30 = 3(-10)$. So $-7 \equiv 23 (\text{mod } 3)$ is correct. The theorem below formalizes this procedure.

THEOREM 4.41. *Let a, b, c, d, n be integers with $n \geq 2$. If $a \equiv b (\text{mod } n)$ and $c \equiv d (\text{mod } n)$, then $(a + c) \equiv (b + d) (\text{mod } n)$.*

PROOF. Since $a \equiv b (\text{mod } n)$ we know that n divides $a - b$. Thus, $a - b = nk$ for some integer k. Since $c \equiv d (\text{mod } n)$ we know that n

divides $c - d$. Thus, $c - d = nm$ for some integer m. Therefore,

$$(a + c) - (b + d) = (a - b) + (c - d) = nk + nm = n(k + m).$$

Thus, n divides $(a+c)-(b+d)$. Therefore, $(a+c) \equiv (b+d) \pmod{n}$. ■

Examples from the real line and plane

Track 2 stuff goes here. Track 2 stuff goes here. Track 2 stuff goes here. Track 2 stuff goes here.

4.4. Proofs by cases

Suppose that you want to prove $P \Rightarrow Q$. You begin by assuming that P is true. What if there are a variety of ways that P can be true? What do you do? You can do a proof by cases. This involves a case for each way that P can be true. For each case you prove that Q is true. When you have exhasted all the cases, then you are done.

Proof of $P \Rightarrow Q$ by cases

- **Step 1.** Assume that P is true.
- **Step 2.** For each way that P can be true, derive a distinct proof that Q is true.
- **Step 4.** Since no matter how P is true we have that Q is true we know that $P \Rightarrow Q$ is true.

Examples from number theory

We begin with a fact about even and odd integers.

THEOREM 4.42. *Let x be an integer. Then $x(x + 1)$ is even.*

PROOF. Let x be an integer. There are two cases: x is even or x is odd. We assume each individually.

Case 1: First assume that x is even. Then $x = 2k$ for some integer k. Thus,

$$x(x + 1) = 2k(2k + 1) = 4k^2 + 2k = 2(2k^2 + 1).$$

Since $2k^2 + 1$ is an integer, we see that $x(x + 1)$ is even.

Case 2: Now assume that x is odd. Then $x = 2n + 1$ for some integer n. Thus,

$$x(x + 1) = (2n + 1)(2n + 1 + 1) = 4n^2 + 6n + 2 = 2(n^2 + 3n + 1).$$

Since $n^2 + 3n + 1$ is an integer, we see that $x(x + 1)$ is even.

In either case $x(x + 1)$ is even. Hence, we have completed the proof. ■

Sometimes the theorem you are trying to prove has an "or" in it. You can deal with this with a proof by cases.

THEOREM 4.43. *Let n be an integer. If $n \equiv 0 (mod\ 3)$ or $n \equiv 1 (mod\ 3)$, then $n^2 \equiv n (mod\ 3)$.*

PROOF. We begin by supposing that n is an integer with $n \equiv 0 (\text{mod } 3)$ or $n \equiv 1 (\text{mod } 3)$. We break the proof into two cases.

Case 1: Suppose that $n \equiv 0 (\text{mod } 3)$. Then 3 divides $n - 0$. Therefore, 3 divides n. This gives us that $n = 3a$ for some integer a. Therefore,

$$n^2 - n = (3a)^2 - 3a = 9a^2 - 3a = 3(3a^2 - a).$$

Since $3a^2 - a$ is an integer this tells us that 3 divides $n^2 - n$. Hence $n^2 \equiv n (\text{mod } 3)$.

Case 2: Suppose that $n \equiv 1 (\text{mod } 3)$. Then 3 divides $n - 1$. This gives us that $n - 1 = 3b$ for some integer b. So $n = 3b + 1$. Therefore,

$$n^2 - n = (3b+1)^2 - (3b+1) = 9b^2 + 6b + 1 - 3b - 1 = 9b^2 + 3b = 3(3b^2 + b).$$

Since $3b^2 + b$ is an integer this tells us that 3 divides $n^2 - n$. Hence $n^2 \equiv n (\text{mod } 3)$. ■

Examples from the real line and plane

PROVE $x^2 \geq 0$ FOR ALL x.

PROVE IF $ab = 0$ THEN $a = 0$ OR $b = 0$.

4.5. Existence and Uniqueness Proofs

Prove uniqueness of inverses, then define these:

DEFINITION 4.44. Let $a \in \mathbb{R}$. A real number b such that $a + b = 0$ is called an **additive inverse of** a. Later in this chapter, we will prove that any $a \in \mathbb{R}$ has a unique additive inverse, which we denote $-a$.

DEFINITION 4.45. We define **subtraction** by $a - b := a + (-b)$ for all real numbers a and b.

Note that the symbol ":=" means "is defined to be equal to."

DEFINITION 4.46. Let $a \in \mathbb{R}$. A real number b such that $ab = 1$ is called a **multiplicative inverse of** a. Later in this chapter, we will prove that if $a \in \mathbb{R}$ and $a \neq 0$, then a has a unique multiplicative inverse, which we denote a^{-1}.

DEFINITION 4.47. We define **division** by $a/b := a \cdot b^{-1}$ for all real numbers a and b such that $b \neq 0$.

Now that we have defined division, we can define $\mathbb{Q}$ more rigorously.

DEFINITION 4.48. We define $\mathbb{Q} := \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$. Elements of $\mathbb{Q}$ are called **rational numbers**.

MAYBE A SECTION ON Existence and Uniqueness Proofs???

4.6. Contraposition

Suppose you want to prove that $P \Rightarrow Q$ is true, but you cannot figure out how to prove it with a direct proof. Instead you can try to prove it by contraposition. Take a look at the following truth table.

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$(\neg Q) \Rightarrow (\neg P)$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Notice that $P \Rightarrow Q$ is logically equivalent to $(\neg Q) \Rightarrow (\neg P)$. Hence we get the following.

Proof of $P \Rightarrow Q$ by contraposition

- **Step 1.** Write down $(\neg Q) \Rightarrow (\neg P)$ and prove that it is true.
- **Step 2.** Since $(\neg Q) \Rightarrow (\neg P)$ is logically equivalent to $P \Rightarrow Q$, we know that $P \Rightarrow Q$ is true.

Examples from number theory

We now give some examples of proofs by contraposition.

THEOREM 4.49. *If x^2 is an even integer, then x is an even integer.*

PROOF. We will prove this by contraposition. Here we have the proposition $P \Rightarrow Q$ where P is "x^2 is an even integer" and Q is "x is an even integer. Notice that $\neg P$ is "x^2 is an odd integer" and $\neg Q$ is "x is an odd integer." Thus, $(\neg Q) \Rightarrow (\neg P)$ is the proposition "If x is an odd integer, then x^2 is an odd integer." We prove this instead.

Suppose that x is an odd integer. Then there exists an integer k where $x = 2k+1$. Thus $x^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$. Since $2k^2+2k$ is an integer, this shows that x^2 is an odd integer, which completes our proof by contraposition. ■

THEOREM 4.50. *Let x and y be integers. If $xy \not\equiv 0 (mod\ 3)$, then $x \not\equiv 0 (mod\ 3)$ and $y \not\equiv 0 (mod\ 3)$.*

PROOF. We will prove this by contraposition. By DeMorgan's rules the negation of

$$x \not\equiv 0 (\text{mod } 3) \text{ and } y \not\equiv 0 (\text{mod } 3)$$

is

$$x \equiv 0 (\text{mod } 3) \text{ or } y \equiv 0 (\text{mod } 3).$$

Hence we will prove the statement "If $x \equiv 0 (\text{mod } 3)$ or $y \equiv 0 (\text{mod } 3)$, then $xy \equiv 0 (\text{mod } 3)$. We prove this by cases.

Case 1: Suppose that $x \equiv 0 (\text{mod } 3)$. Then 3 divides $x - 0 = x$. Hence $x = 3k$ for some integer k. Thus $xy = 3ky$ is divisible by 3. So $xy \equiv 0 (\text{mod } 3$.

Case 2: Suppose that $y \equiv 0 (\text{mod } 3)$. Then 3 divides $y - 0 = y$. Hence $y = 3m$ for some integer m. Thus $xy = 3xm$ is divisible by 3. So $xy \equiv 0 (\text{mod } 3$. ■

Examples from the real line and plane

Track 2 stuff goes here. Track 2 stuff goes here. Track 2 stuff goes here. Track 2 stuff goes here.

4.7. Contradiction

There are two common ways to prove a statement by contradiction. Sometimes you want to prove that P is true. In that case you do the following.

Proof of P by contradiction

- **Step 1.** Assume that P is false.
- **Step 2.** Use definitions, previous theorems, and the fact that P is false to show that some statement R is both true and false at the same time. This is called a contradition. Note that a statement cannot be both true and false at the same time.
- **Step 3.** Since we have a contradiction if P is false, we must have that P is true.

Sometimes you want to prove that $P \Rightarrow Q$ is true. You do this as follows.

Proof of $P \Rightarrow Q$ by contradiction

- **Step 1.** Assume that P is true.
- **Step 2.** To show that $P \Rightarrow Q$ is true, you must show that Q is true. So assume that Q is false.
- **Step 2.** Use definitions, previous theorems, and the fact that P is true and Q is false to show that some statement R is both true and false at the same time. This is a contradiction since a statement cannot be both true and false at the same time.
- **Step 3.** Hence, if P is true, then we must have that Q is true. So $P \Rightarrow Q$ is true.

Examples from number theory

Let's prove some stuff via contradiction.

DEFINITION 4.51. We say that a real number x is **irrational** if x is not a rational number.

TOO MUCH INFORMATION 4.52. In our next example, we will prove that $\sqrt{2}$ is irrational. First, we have to deal with a small problem: We don't have any axioms, theorems, or definitions about square roots. How can we get started when we don't have anything to work with? For now, then, let's assume that for all real numbers a and b with $a > 0$, there exists a positive real number a^b. Moreover, let's assume that the following properties hold:

(1) $\forall a \in \mathbb{R}$, we have that $a^1 = a$.
(2) $\forall a, b, c \in \mathbb{R}$, we have that $a^b a^c = a^{b+c}$.
(3) $\forall a, b, c \in \mathbb{R}$, we have that $(a^b)^c = a^{bc}$.
(4) $\forall a, b, c \in \mathbb{R}$, we have that $(ab)^c = a^c b^c$.

If n is a natural number, then we denote $a^{1/n}$ by $\sqrt[n]{a}$. We denote $a^{1/2}$ by $\sqrt{a}$.

In Chapter **??**, we'll give a precise definition of a^b, and we'll then be able to prove these laws of exponents for real numbers.

THEOREM 4.53. *$\sqrt{2}$ is an irrational number.*

PROOF. We prove this by contradiction. Suppose that $\sqrt{2}$ is a rational number. Then $\sqrt{2} = \frac{m}{n}$ where m and n are integers and $n \neq 0$. By canceling common factors, we may assume that m and n have no common factors greater than one. By squaring both sides of $\sqrt{2} = \frac{m}{n}$ and then multiplying both sides by n^2 we see that $2n^2 = m^2$. Thus m^2 is an even integer. By Theorem 4.49, this implies that m is an even integer. So there exists an integer k where $m = 2k$. Hence $2n^2 = m^2 = (2k)^2 = 4k^2$. Therefore $n^2 = 2k^2$. Again, by Theorem 4.49, this implies that n is even. But this implies that both m and n are even. Therefore m and n have the integer 2 as a common divisor. This contradicts that assumption that we initially made. Hence, $\sqrt{2}$ cannot be a rational number. Therefore $\sqrt{2}$ is irrational. ■

THEOREM 4.54. *Suppose that a and b are integers. If $a-b$ is odd, then $a+b$ is odd.*

PROOF. We prove this by contradiction. Suppose that $a-b$ is odd. Further assume that $a+b$ is even. We will show that this implies a contradiction. Since $a-b$ is odd, $a-b=2k+1$ for some integer k. Since $a+b$ is even, $a+b=2m$ for some integer m. Adding both equations gives that $2a=(a+b)+(a-b)=2m+2k-1=2(m+k-1)+1$. Wait a minute! This is saying that the even integer $2a$ equals an odd integer $2(m+k-1)+1$. This is a contradiction. Therefore, if $a-b$ is odd, then there is no way that $a+b$ is even. Thus, we must have that $a+b$ is odd if $a-b$ is odd. ■

Examples from the real line and plane

4.8. If and only if proofs

Suppose that you want to prove $P \Leftrightarrow Q$. That is, you want to prove that P is true if and only if Q is true. By the definition of $P \Leftrightarrow Q$ you must show that both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true.

Proof of P if and only if Q

- **Step 1.** Give a proof that $P \Rightarrow Q$ is true.
- **Step 2.** Give a seperate proof that $Q \Rightarrow P$ is true.

Let us give an example to illustrate this.

EXAMPLE 4.55. Suppose that we want to prove that the following statement is true: "Let n and N be integers. We have that $n \geq N$ if and only if $\frac{5}{n}+1 \leq \frac{5}{N}+1$." Recall from ??? that $P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \vee (Q \Rightarrow P)$. Therefore, we must prove that the following two statements are both true.

(1) Let n and N be integers. If $n \geq N$ then $\frac{5}{n}+1 \leq \frac{5}{N}+1$.

(2) Let n and N be integers. If $\frac{5}{n}+1 \leq \frac{5}{N}+1$, then $n \geq N$.

We first prove (1). Suppose that n and N are integers and that $n \geq N$. Therefore, we have that $\frac{1}{n} \leq \frac{1}{N}$. Multiplying by 5 and then adding one, we see that $\dfrac{5}{n} + 1 \leq \dfrac{5}{N} + 1$.

Now we prove (2). This is a totally new proof and is independent of the one given above. Suppose that $\dfrac{5}{n} + 1 \leq \dfrac{5}{N} + 1$. Subtract one from both sides and then divide by 5 to get that $\frac{1}{n} \leq \frac{1}{N}$. Cross multiply and get that $N \leq n$, which is what we want.

Examples from number theory

Let's prove some iff proofs.

THEOREM 4.56. *Let a and b be non-zero integers. We have that $a|b$ and $b|a$ if and only if $a = b$ or $a = -b$.*

PROOF. We first show that if $a|b$ and $b|a$, then $a = b$ or $a = -b$. Assume that $a|b$ and $b|a$. By definition this implies that there exist integers k and m where $ak = b$ and $bm = a$. Thus $akm = bm = a$. Dividing both sides by a gives that $km = 1$. Since k and m are integers, this implies that either $k = m = 1$ or $k = m = -1$. If $k = m = 1$, then $a = b$. If $k = m = -1$, then $a = -b$.

Now we show that if $a = b$ or $a = -b$, then $a|b$ and $b|a$. Assume that $a = b$ or $a = -b$. If $a = b$, then $a(1) = b$ and $b(1) = a$. Thus, $a|b$ and $b|a$. If $a = -b$, then $a(-1) = b$ and $b(-1) = a$. Thus $a|b$ and $b|a$. ■

Examples from the real line and plane

Track 2 stuff goes here. Track 2 stuff goes here. Track 2 stuff goes here.

4.9. Proofs involving nested quantifiers

MAYBE A SECTION ON Proofs involving nested quantifiers

4.10. Application: Number Theory

In this section we use all of the previous proof techniques...blah blah blah blah.

Examples from number theory

THEOREM 4.57. *Let a and b be integers with $a \geq 0$. There exist integers q and r with $b = aq + r$ and $0 \leq r < a$.*

PROOF. Put a proof here. ■

EXAMPLE 4.58. Put some examples here.

DEFINITION 4.59. Let a and b be integers, not both zero. We say that d is a **common divisor** of a and b if d divides a and d divides b. The **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is the largest common divisor of a and b.

EXAMPLE 4.60. Let's calculate $\gcd(36, 48)$. The divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. The divisors of 48 are $1, 2, 3, 4, 6, 8, 12, 16, 24, 48$. The common divisors of 36 and 48 are $1, 2, 3, 4, 6, 12$. The greatest common divisor is $\gcd(36, 48) = 12$.

EXAMPLE 4.61. Let's calculate $\gcd(6, 0)$. The divisors of 6 are $1, 2, 3, 4, 6$. Every integer divides 0. For example, 4 divides 0 because $4(0) = 0$. Therefore, the common divisors of 6 and 0 are $1, 2, 3, 4, 6$. The greatest common divisor is $\gcd(6, 0) = 6$.

EXAMPLE 4.62. Let's calculate $\gcd(42, 72)$. The divisors of 42 are $1, 2, 3, 6, 7, 14, 21, 42$. The divisors of 72 are $1, 2, 3, 4, 6, 8, 9, 12, 18, 36, 72$. The common divisors of 42 and 72 are $1, 2, 3, 6$. The greatest common divisor is $\gcd(42, 72) = 6$. Notice also that $6 = 72(3) + 42(-5)$. That is, we can write $6 = 72x_0 + 42y_0$ where $x_0 = 3$ and $y_0 = -5$. The next theorem shows that we can do this in general.

THEOREM 4.63. *Let a and b be integers, not both zero. Then there exist integers x_0 and y_0 where $ax_0 + by_0 = \gcd(a, b)$.*

PROOF. Consider the set $S = \{ax + by \mid x, y \in \mathbb{Z}\}$. Note that a, $-a$, b, and $-b$ are in S because $a = a(1) + b(0)$, $-a = a(-1) + b(0)$, $b = a(0) + b(1)$, and $b = a(0) + b(-1)$. Since a and b are not both zero, this implies that there exists some positive integer in S. Let d be the smallest positive integer in S. Since d is in S we know that $d = ax_0 + by_0$ for some integers x_0 and y_0. We now show that d is the greatest common divisor of a and b. This will complete the proof.

First we show that d is a common divisor of a and b. By Theorem 4.57, there exist integers q and r where $a = dq + r$ and $0 \leq r < d$. We want to show that $r = 0$. That will imply that $a = dq$, which shows that d divides a. Notice that

$$r = a - dq = a - ax_0q - by_0q = (1 - qx_0)a + (-y_0q)b.$$

Thus r is in S. Since $0 \leq r < d$ and d is the smallest positive integer in S, we must have that $r = 0$. As stated above, this implies that d divides a. A similar argument shows that d divides b. Hence d is a common divisor of a and b.

We now show that d is the greatest common divisor of a and b. Suppose that d' is another positive common divisor of a and b. Thus d' divides a and d' divides b. So there exist integers k and m where $d'k = a$ and $d'm = b$. Therefore

$$d = ax_0 + by_0 = d'kx_0 + d'my_0 = d'(kx_0 + my_0).$$

Thus d' divides d. Since d and d' are both positive integers, this implies that $d' \leq d$. Hence d is the greatest common divisor of a and b. ■

TOO MUCH INFORMATION 4.64. The above theorem is an existence proof. It shows that x_0 and y_0 exist, but it doesn't tell us how to find them. There is an algorithm to find x_0 and y_0, but we do not discuss it in this book. It is called the Euclidean algorithm. You can find it in PUT A REFERENCE HERE.

DEFINITION 4.65. A integer p is a **prime** if $p \geq 2$ and the only divisors of p are 1 and p.

EXAMPLE 4.66. 5 is a prime because the only divisors of 5 are 1 and 5. The integer 4 is not prime because 2 is a divisor of 4.

The primes between 2 and 100 are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,$$
$$59, 61, 67, 71, 73, 79, 83, 89, 97.$$

THEOREM 4.67. *Let a, b, and p be integers. If p is a prime and $p|ab$, then $p|a$ or $p|b$.*

PROOF. If $p|a$ then we are done. Suppose that $p \not| a$. Since the only divisors of p are 1 and p, and p is not a divisor of a, we must have that $\gcd(p, a) = 1$. By Theorem 4.63, we have that $1 = px_0 + ay_0$ for some integers x_0 and y_0. Therefore, $b = px_0b + ay_0b$. Since $p|ab$, there exists an integer k where $ab = pk$. Thus $b = px_0b + y_0pk$. So $p(x_0b + y_0k) = b$. Therefore, $p|b$. ■

THEOREM 4.68. *$\sqrt{3}$ is irrational.*

PROOF. We prove this theorem by contradiction. Temporarily assume that $\sqrt{3}$ is rational. Then $\sqrt{3} = \frac{a}{b}$ where we may assume that a and b have no common divisors. Squaring both sides of this equation and multiplying by b^2 gives us that $3b^2 = a^2$. Hence 3 divides $a^2 = a \cdot a$. Since 3 is a prime, we know by Theorem 4.67 that 3 divides a. This implies that there exists an integer k where $3k = a$. Plugging $3k = a$ into $3b^2 = a^2$ gives $3b^2 = 9k^2$. Thus $b^2 = 3k^2$. So 3 divides b^2. As above, since 3 is a prime, this implies that 3 divides b. We have shown that 3 is a common divisor of a and b, which is a contradiction. Therefore $\sqrt{3}$ is not rational. ■

TOO MUCH INFORMATION 4.69. We now turn our attention to logarithms. Like exponents, it takes some work to define them for all real numbers—we'll do that later in Chapter **??**. For now, we will make the following assumption:

For all positive real numbers a and b, there exists a unique real number x such that $b^x = a$.

We use the notation $\log_b a$ for this unique real number x.

EXAMPLE 4.70. Prove that $\log_2(5)$ is irrational.

PROOF. kjljklkj ■

Examples from the real line and plane

Track 2 stuff goes here. Track 2 stuff goes here. Track 2 stuff goes here. Track 2 stuff goes here.

4.11. Exercises

4.11.1. Direct Proofs.

(1) Let x and y be integers. Prove that if x and y are odd, then $x + y$ is even.
(2) Let x and y be integers. Prove that if x and y are odd, then xy is odd.
(3) Let x and y be integers. Prove that if x is even and y is odd, then $3x + 7y$ is odd.
(4) Let x and y be integers. Prove that if x is odd then, $2x^2+3x+4$ is odd.
(5) Let x, y, and z be integers with $x \neq 0$ and $y \neq 0$. Prove that if $x|y$ and $y|z$, then $x|z$.
(6) Let x, y, m, and n be integers with $x \neq 0$ and $m \neq 0$. Prove that if $x|y$ and $m|n$, then $xm|yn$.
(7) Let x, y, and z be integers with $x \neq 0$ and $y \neq 0$. Prove that if $xy|z$, then $x|z$.
(8) Let x, y, z, and n be integers with $n \neq 0$. Prove that if $n|(x - y)$ and $n|(y - z)$, then $n|(x - z)$.
(9) Let a, b, c, x, and y be integers with $a \neq 0$. Prove that if $a|b$ and $a|c$, then $a|(bx + cy)$.
(10) Given a, b, and n state whether $a \equiv b (\text{mod } n)$ or $a \not\equiv b (\text{mod } n)$.
   (a) $a = 5, b = 3, n = 2$
   (b) $a = 17, b = 210, n = 3$
   (c) $a = -13, b = 21, n = 7$
   (d) $a = 10, b = 7, n = 4$
   (e) $a = -30, b = 15, n = 5$
(11) Let
$$A = \{x \in \mathbb{Z} \mid x \equiv 3 (\text{mod } 5)\}.$$
List 5 positive and 5 negative elements in A.
(12) Let
$$A = \{x \in \mathbb{Z} \mid x \equiv -6 (\text{mod } 7)\}.$$
List 5 positive and 5 negative elements in A.
(13) Let a, b, c, and n be integers with $n \geq 2$. Prove the following:
   (a) $a \equiv a (\text{mod } n)$.
   (b) If $a \equiv b (\text{mod } n)$ then $b \equiv a (\text{mod } n)$.
   (c) If $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$, then $a \equiv c (\text{mod } n)$.

(14) Let a, b, and n be integers and $n \geq 2$. Prove: If $a \equiv 0 (\text{mod } n)$, then $b + a \equiv b (\text{mod } n)$
(15) Let a, b, c, d, and n be integers and $n \geq 2$. Prove: If $a \equiv b (\text{mod } n)$ and $c \equiv d (\text{mod } n)$, then $a + c \equiv b + d (\text{mod } n)$ and $ac \equiv bd (\text{mod } n)$.

4.11.2. Contraposition.

(1) Let x and y be integers. Prove that if xy is even, then either x or y is even.
(2) Let x and y be integers. Prove that if $x^2 + 1$ is odd, then x is even.
(3) Let x and y be integers. Prove that if $x^2y + 3$ is even, then x is odd or y is even.

4.11.3. Contradiction.

(1) Suppose that x is a real number. Prove that if x is irrational and $x \neq 0$, then $\frac{1}{x}$ is irrational.
(2) Suppose that x and y are real numbers. Prove that if x is rational and y is irrational, then $x + y$ is irrational.
(3) Suppose that x and y are real numbers. Prove that if x is rational and y is rational, then $x + y$ is rational and xy is rational.
(4) Prove that $\sqrt[3]{2}$ is irrational.
(5) Prove that $\sqrt{\frac{2}{3}}$ is irrational.
(6) Prove that $\log_2(3)$ is irrational.
(7) Let x and y be integers. Prove by contradiction: If xy is even, then either x or y is even. (This same problem is in the section on Contraposition. How does the proof differ when you use contradiction vs. contraposition?)
(8) Let x and y be integers. Prove by contradiction: If $x^2 + 1$ is odd, then x is even. (This same problem is in the section on Contraposition. How does the proof differ when you use contradiction vs. contraposition?)
(9) Let x and y be integers. Prove by contradiction: If $x^2y + 3$ is even, then x is odd or y is even. (This same problem is in the section on Contraposition. How does the proof differ when you use contradiction vs. contraposition?)

4.11.4. Iff proofs.

(1) Let x, y, z be integers. Prove the following: $xz|yz$ if and only if $x|y$.

4.11.5. Application: Number Theory.

(1) Warm up: Let k and x be integers. If $2k = x^2$, then 2 divides x.
(2) Warm up: Let k be an integer. If $27 = 3k^3$, then 3 divides k.
(3) Warm up: Let $g = \gcd(a, b)$. If $d|a$ and $d|b$, then d divides g. [Hint: Look at Theorem 4.63.]
(4) Let a and b be integers, not both zero. Prove that $\gcd(a, b) = \gcd(b, a)$.
(5) Let a be a non-zero integer. Prove that $\gcd(a, 0) = a$.
(6) Let a be a non-zero integer and p be a prime. Prove that $\gcd(p, a) = 1$ if and only if p does not divide a.
(7) Let x be an integer. Prove that if x^2 is even, then 4 divides x^2.
(8) Prove that $\sqrt{5}$ is irrational.
(9) Prove that if p is a prime, then $\sqrt{p}$ is irrational.
(10) Prove that $\log_3(5)$ is irrational.
(11) Calculate the following:
    (a) $\gcd(12, 24)$
    (b) $\gcd(16, 36)$
    (c) $\gcd(5, 18)$
    (d) $\gcd(0, 3)$
(12) Let a and b be integers, not both zero, and $d = \gcd(a, b)$. Prove that $a|b$ if and only if $d = a$.
(13) Suppose that a, b, x, y are integers. Prove that $\gcd(a, b)$ divides $ax + by$.
(14) Prove that no integers x and y exist such that $x - y = 200$ and $\gcd(x, y) = 3$.
(15) Prove that there exist integers x and y where $3x + 18y = 9$.
(16) Prove that there are no integers solutions x and y to the equation $6x - 3y = 7$.
(17) Suppose that x, y, z are integers. Prove that $x|yz$ if and only if $\left.\dfrac{x}{\gcd(x, y)}\right| z$.
(18) This is a four part exercise. The last part needs the previous parts.
    (a) Suppose that a and b are integers, not both zero. Suppose that there exist integers x and y with $ax + by = 1$. Prove that $\gcd(a, b) = 1$.
    (b) Suppose that a and b are integers, not both zero. Let $d = \gcd(a, b)$. Prove that $\gcd\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

(c) Suppose that a and b are integers, not both zero. Prove that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

(d) Suppose that x and y are integers, not both zero. Let z be another integer. Prove that if $x|yz$, then $\dfrac{x}{\gcd(x, y)}$ divides z.

(19) Write down a true statement about the integers or real numbers. Then prove it. (Of course, your statement should not be an axiom or definition or statement that you've proven already.)

4.12. Fun math facts

A number is called **algebraic** if it is the root (zero) of an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

where $a_n, a_{n-1}, \ldots, a_1, a_0$ are integers. If a number is not algebraic, then it is said to be **transcendental**.

For example, the number $\sqrt{2}$ is algebraic because it is the root of the equation $x^2 - 2 = 0$. The complex number i is algebraic because it is the root of the equation $x^2 + 1 = 0$. $1/2$ is algebraic because it is the root of the equation $2x - 1 = 0$. It is true that any rational number is algebraic. Can you prove it?

It is not even clear that transcendental numbers exist. In 1844, Liouville gave the first proof that transcendental numbers do indeed exist. Later, in 1851, he gave examples of transcendental numbers. One of his examples was the following number:

$$\sum_{n=1}^{\infty} 10^{-n!} = 0.11000100000000000000000001000\ldots$$

There is a proof of this fact on page 418 in the 5th edition of the book "An Introduction to the theory of numbers" by Niven, Zuckerman, and Montgomery. It uses techniques from calculus. It is known that π and e are transcendental numbers. This means that there is no polynomial equation with integer coefficients that π is a root of. It is not easy to prove this. According to Wikipedia, it is not known whether the following numbers are transcendental or not: $\pi + e$, $\pi - e$, πe, π/e, π^π, e^e, π^e.

Note: Since any rational number is algebraic, this shows that a real number that is transcendental must be irrational. Why?

TOO MUCH INFORMATION 4.71. You may be interested to know that computers can prove theorems. A computer can treat "=" and "+" and ">" and so forth as meaningless symbols. Some mathematicians have programmed computers to start with axioms as strings of such symbols, follow rigid rules of logic to manipulate these symbols, and thereby obtain mathematical truths! (No deep theorems have yet been proven this way, however, so humans still have the advantage here. For now.)

Although human beings are not computers, by making both the axioms and rules of logic as strict and rigid as possible, we then have a system without any ambiguity: if you claim to have proven a new theorem, any two mathematicians in the world ought to be able to agree, eventually, on whether your proof is correct. This absolute clarity was a major reason for the development of the axiomatic method.

HOW ABOUT A LITTLE ON THE HISTORY OF HOW IT GOT TO BE THAT PROOFS BECAME SO IMPORTANT FOR MATHEMATICIANS?

Chapter 5

Induction

5.1. Proofs by induction

We begin with an example that illustrates the technique of induction.

EXAMPLE 5.1. Given a positive integer n, let $S(n)$ be the statement $2^n < 3^n$. How do we prove that this statement is true? Is it even true? Let's try a few cases. When $n = 1$, then $S(1)$ is the statement $2^1 < 3^1$, which is true. When $n = 2$, then $S(2)$ is the statement $2^2 < 3^2$, which is true. When $n = 10,000$, then $S(n)$ is the statement $2^{10000} < 3^{10000}$. Is this true? It turns out that it is true. But how would you check it? These numbers are huge! Try typing them into a computer algebra system like Mathematica.

Suppose that we want to prove that $S(n)$ is true for all integers $n \geq 1$. To do this we can use induction. Here is how it works. First we check the first case, which is $n = 1$ in this problem. We did this above and saw that $S(1)$ is true since $2^1 < 3^1$. Now we do the following "ladder" part of induction: We show that whenever $S(k)$ is true for some integer $k \geq 1$, then we must have that $S(k + 1)$ is also true. Suppose that k is some integer with $k \geq 1$. Assume that $S(k)$ is true. That is assume that $2^k < 3^k$. (Note that we are making an assumption that $S(k)$ is true—we haven't proven it.) Now if we multiply the equation $2^k < 3^k$ on both sides by 2, then we get $2 \cdot 2^k < 2 \cdot 3^k$. So $2^{k+1} < 2 \cdot 3^k$. Because $2 < 3$ we see that $2 \cdot 3^k < 3 \cdot 3^k$. Putting this all together we get that

$$2^{k+1} < 2 \cdot 3^k < 3 \cdot 3^k = 3^{k+1}.$$

Hence $2^{k+1} < 3^{k+1}$. So $S(k + 1)$ is true.

What have we done? We proved two things:

(1) $S(1)$ is true. That is $2^1 < 3^1$.
(2) If $S(k)$ is true for some integer $k \geq 1$, then $S(k+1)$ is true.

Now look at what we have. We know that $S(1)$ is true. By (2) using $k = 1$, this implies that $S(k+1) = S(2)$ is true; that is, $2^2 < 3^2$. Now we apply (2) again using $k = 2$. This gives us that $S(k+1) = S(3)$ is true; that is $2^3 < 3^3$. Now we apply (2) again using $k = 3$. This gives us that $S(k+1) = S(4)$ is true; that is $2^4 < 3^4$. You can keep using (2) forever and ever! What happens is that you get that $S(n)$ is true for all $n \geq 1$. Induction is powerful!

DEFINITION 5.2 (The principle of induction). Let $S(n)$ be a statement where n is an integer. Suppose that

(1) $S(n_0)$ is true for some fixed integer n_0.
(2) The following statement is true: For each $k \geq n_0$, if $S(k)$ is true, then $S(k+1)$ is true.

Then $S(n)$ is true for all $n \geq n_0$.

EXAMPLE 5.3. Let x be a real number with $x \neq 1$. We now show by induction that

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}$$

for every positive integer n with $n \geq 0$.

PROOF. Let $S(n)$ be the statement

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

When $n = 0$, the statement $S(0)$ is the statement

$$1 = \frac{x^{0+1} - 1}{x - 1}$$

which is true.

Let k be an integer with $k \geq 0$ and assume that $S(k)$ is true. That is assume that

$$1 + x + x^2 + \cdots + x^k = \frac{x^{k+1} - 1}{x - 1}. \tag{1}$$

Adding x^{k+1} to both sides of equation (1) gives

$$1 + x + x^2 + \cdots + x^k + x^{k+1} = \frac{x^{k+1} - 1}{x - 1} + x^{k+1},$$

which simplifies to

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

Hence $S(k+1)$ is true.
By the principle of mathematical induction, we have that $S(n)$ is true for all $n \geq 0$. ■

5.2. Complete induction

DEFINITION 5.4 (Principle of complete induction). Let $S(n)$ be a statement where n is an integer. Suppose that

(1) $S(n_0)$ is true for some fixed integer n_0.
(2) The following statement is true: Given $k \geq n_0$, if $S(n_0), S(n_0+1), S(n_0+2), \ldots, S(k-2), S(k-1)$ are all true, then $S(k)$ is true.

Then $S(n)$ is true for all $n \geq n_0$.

Consider an integer, say $n = 120$. Notice that we can keep factoring 120 into smaller and smaller pieces. First we break it into

$$120 = 2 \cdot 60.$$

We can't break the two any further, but we can break the 60 into $60 = 2 \cdot 30$ which gives

$$120 = 2 \cdot 2 \cdot 30.$$

We can factor 120 by breaking 30 into $3 \cdot 15$. This gives

$$120 = 2 \cdot 2 \cdot 3 \cdot 10.$$

If we keep doing this we get

$$\begin{aligned} 120 &= 2 \cdot 2 \cdot 3 \cdot 2 \cdot 5 \\ &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \\ &= 2^3 \cdot 3 \cdot 5. \end{aligned}$$

We can't factor 120 any further because each of the numbers in $2{\cdot}2{\cdot}2{\cdot}3{\cdot}5$ is a prime and can't be factored any further. Is there another way to factor n into primes? Maybe if we break it up differently. Let's try it another way:

$$\begin{aligned} 120 &= 5 \cdot 24 \\ &= 5 \cdot 2 \cdot 12 \\ &= 5 \cdot 2 \cdot 3 \cdot 4 \\ &= 5 \cdot 2 \cdot 3 \cdot 2 \cdot 2 \\ &= 2^3 \cdot 3 \cdot 5. \end{aligned}$$

Given any integer n, can we factor n into a product of primes? Furthermore, is this factorization unique? That is, can we do it in another way?

We answer the first question below in Proposition . That is, yes, every integer n can be factored into a product of primes. We leave the question of uniqueness until Theorem 5.8 on page 5.8.

PROPOSITION 5.5. *Let n be an integer and $n \geq 2$. Then n can be expressed as a product of one or more primes.*

PROOF. We prove this result by the principle of complete induction. Let $S(n)$ be the statement

"n can be expressed as a product of one or more primes."

We see that $S(2)$ is true since 2 is the product of one prime.
Let $k > 2$.
Assume that each of $S(2), S(3), \ldots, S(k-1)$ is true.
⟨*We just assumed that any integer smaller than k can be written as a product of one or more primes. We now want to use this information to show that k can be written as a product of one or more primes. We break the proof into two cases: when k is a prime and when k is not a prime.*⟩
Case 1: Suppose that k is prime.
Then k is the product of one prime.
Hence $S(k)$ is true.
Case 2: Suppose that k is not prime.
Thus $k = a \cdot b$ where a and b are integers with $2 \leq a \leq k-1$ and $2 \leq a \leq k-1$.
By assumption $S(a)$ and $S(b)$ are true.
Since $S(a)$ is true we have that $a = p_1 p_2 \ldots p_r$ where $p_1, p_2, \ldots, p_r$ are

primes.
Since $S(b)$ is true we have that $b = q_1 q_2 \dots q_s$ where $q_1, q_2, \dots, q_s$ are primes.
Then $k = ab = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$ is a product of primes.
Hence $S(k)$ is true.
$\langle$*In either case, $S(k)$ is true. Since we have dealt with the only two cases that can occur, this concludes the proof of this proposition.*$\rangle$ ■

5.3. Applications to number theory

In this section we give proofs of two famous theorems in mathematics: Euclid's proof showing that there are an infinite number of primes, and a proof of the fundamental theorem of arithmetic.

We begin with the primes. The following is a list of the first 100 primes:

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541

Here is a question: How many primes are there? Are there ten million primes? Are there a billion primes? Or do the primes never end, that is, are there an infinite number of primes? The answer is that there are an infinite number of primes. The first person to prove this fact was Euclid.

THEOREM 5.6 (Euclid). *There are infinitely many primes.*

PROOF. We prove the theorem by contradiction.
Suppose that there are only finitely many primes.
Suppose that they are $p_1, p_2, \dots, p_m$ are all the primes.
Set $N = p_1 p_2 \cdots p_m + 1$.
By Proposition 5.5, N must factor into a product of primes.
Hence there must be a prime that divides N.
The only primes are $p_1, p_2, \dots, p_m$.

Hence p_k must divide N for some $1 \leq k \leq m$.
For notational simplicity, let us assume that p_1 is a divisor of N. (The same proof will work for other k.)
Thus $p_1 x = N$ for some integer x.
But then $p_1 x = p_1 p_2 \cdots p_m + 1$.
So, $p_1(x - p_2 \cdots p_m) = 1$.
Thus p_1 divides 1.
Since p_1 is a positive integer we must have that $p_1 = 1$. Since p_1 is a prime, $p_1 \neq 1$.
This gives a contradiction.
Therefore, there are infinitely many primes. ■

We now give a proof of the fundamental theorem of arithmetic. Consider the integer $n = 504$. We saw in Prop 5.5 that n must factor into primes. Note that $n = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$. Is there some other way to factor n into primes? How about $n = 3 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 2$? We see that the above two factorizations of n are the same. We have just changed the ordering of the primes. It turns out that there is no other way to factor n into primes except for just rearranging the above primes. This is a fact for any positive integer greater than or equal to 2. We will prove this fact in Theorem 5.8. But first we need a lemma.

LEMMA 5.7. *Suppose that p is prime and $a_1, a_2, \ldots, a_n$ are positive integers greater than one. If $p | a_1 \cdot a_2 \cdots a_n$, then p divides a_i for some i with $1 \leq i \leq n$.*

PROOF. Let p be a prime.
⟨*The prime p is fixed throughout this proof and does not change. We give a proof using induction on n.*⟩
Let $S(n)$ be the statement

> If $p | a_1 \cdot a_2 \cdots a_n$ where $a_1, a_2, \ldots, a_n$ are positive integers, then p divides a_i for some i with $1 \leq i \leq n$."

We first deal with the case where $n = 2$.
Suppose that $p | a_1 a_2$.
Then Theorem 4.67 shows that $p | a_1$ or $p | a_2$.
Hence $S(2)$ is true.
Let k be an integer with $k \geq 2$.
Assume that $S(k)$ is true.
Suppose that $p | a_1 a_2 \cdots a_k a_{k+1}$ where $a_1, a_2, \cdots a_k, a_{k+1}$ are positive integers.

By Theorem 4.67 $p|a_1a_2\cdots a_k$ or $p|a_{k+1}$.
If $p|a_{k+1}$, then $S(k+1)$ is true.
If $p|a_1a_2\cdots a_k$, then since $S(k)$ is true we have that $p|a_i$ for some integer i with $1 \leq i \leq k$.
Hence $S(k+1)$ is true.
Therefore, by induction $S(n)$ is true for all n with $n \geq 2$. ■

THEOREM 5.8 (Fundamental theorem of arithmetic). *Let n be an integer with $n \geq 2$. Then n factors into a product of primes. Moreover, the factorization is unique apart from the ordering of the prime factors.*

PROOF. By Proposition 5.5 we have that n factors into a product of primes.
Suppose that n factors into two different prime factorizations.
By dividing off the comman factors we may assume that

$$n = p_1p_2\cdots p_k = q_1q_2\cdots q_m$$

where $p_1, p_2, \ldots p_k, q_1, q_2, \ldots, q_m$ are primes and $p_i \neq q_j$ for all $1 \leq i \leq k$ and $1 \leq j \leq m$.
Since $p_1p_2\cdots p_k = q_1q_2\cdots q_m$ we see that p_1 divides $q_1q_2\cdots q_m$.
By Lemma 5.7 we have that $p_1|q_i$ for some i with $1 \leq i \leq m$.
Since q_i is prime, the only positive divisors of q_i are 1 and q_i.
Since p_1 is not equal to 1 we must have that $p_1 = q_i$.
But this contradicts the fact that $p_i \neq q_j$ for all $1 \leq i \leq k$ and $1 \leq j \leq m$.
Hence n factors uniquely (up to rearrangement) into a product of primes. ■

5.4. Exercises

5.4.1. Exercises for section 5.1.

(1) Prove the following by inducton:
   (a) $1 + 3 + 5 + \cdots + (2n-1) = n^2$, for $n \geq 1$.
   (b) $3^n < 4^n$, for $n \geq 1$.
   (c) $5 + 8 + 11 + \cdots + (3n+2) = \dfrac{3n^2+7n}{2}$, for $n \geq 1$.
   (d) $n^2 < 2^n$ for $n \geq 5$.
   (e) $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \dfrac{1}{3\cdot 4} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$, for $n \geq 1$.
   (f) $n! > 3^n$, for $n \geq 7$.

(g) 3 divides $4^n - 1$, for $n \geq 1$.
(h) 6 divides $n^3 + 5n$, for $n \geq 1$.
(i) $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$, for $n \geq 1$.
(j) $\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} = \frac{n}{2n+1}$, for $n \geq 1$.
(k) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, for $n \geq 1$.

(2) Let n and m be integers. Suppose that $n \geq 2$. Suppose that $a \equiv b (\text{mod } n)$. Prove the following by induction on m:

$$a^m \equiv b^m (\text{mod } n) \text{ for all } m \geq 1.$$

[Hint: Notice that $a^{k+1} - b^{k+1} = a \cdot a^k - a \cdot b^k + a \cdot b^k - b \cdot b^k$.]

5.4.2. Exercises for section 5.2. PUT SOME EXERCISES IN HERE.

5.4.3. Exercises for section 5.3. PUT SOME EXERCISES IN HERE.

5.5. Fun math facts

Recall that in Theorem 5.6 we proved that there are infinitely many primes. A question one could ask is "how are the primes distributed amongst the natural numbers?" We give one way to think about this question. Let $\pi(x)$ be the number of primes p that satisfy the bound $1 \leq p \leq x$. For example, suppose that $x = 31$. Below we have listed all the numbers between 1 and 31. The primes are circled.

$$\textcircled{2}\,\textcircled{3}, 4, \textcircled{5}, 6, \textcircled{7}, 8, 9, 10, \textcircled{11}, 12, \textcircled{13}, 14, 15, 16, \textcircled{17}, 18, \textcircled{19}, 20,$$
$$21, 22, \textcircled{23}, 24, 25, 26, 27, 28, \textcircled{29}, 30, \textcircled{31}, \ldots$$

We see that $\pi(31) = 11$.

Look at how the primes are distributed in the above list. Do you think there is any pattern to $\pi(x)$? What happens as x gets larger and larger? How many primes are there between 1 and x? What is amazing is that people have given formulas that estimate the answer to this problem. For example, a famous theorem called the prime number theorem states that as x goes to infinity $\pi(x)$ is estimated by $x/\ln(x)$. This is amazing that such a simple function can approximate such complex behavior that exists in how the primes are distributed throughout the numbers. Look at table 1. Look at how well $x/\ln(x)$ approximates $\pi(x)$.

x	$\pi(x)$	$x/\ln(x)$
31	11	9.03
100	25	21.71
10000	1229	1085.74
1000000	78498	72382.4
1000000000	50847534	48254942

TABLE 1. Values of $\pi(x)$

Chapter 6

Sets

Quote or pun (Sets and the City?)

UNION IS STRENGTH—AESOP???

Brief intro paragraph on sets. Refer back to Basic Set Theory chapter.

FOR THE BASIC SET THEORY SECTION: NOTE THAT COMMA MEANS "AND" IN STATEMENTS LIKE $x, y \in A$.

6.1. Subsets

DEFINITION 6.1. Let A and B be sets. We say that A is a **subset** of B if every element of A is an element of B. We denote that A is a subset of B by writing $A \subseteq B$.

In other words, the statement "$A \subseteq B$" means the same thing as the statement "If $x \in A$, then $x \in B$."

TOO MUCH INFORMATION 6.2. Some books use the notation $A \subset B$ instead of $A \subseteq B$.

TOO MUCH INFORMATION 6.3. If $A \subseteq B$, we occasionally say that B is a **superset** of A and write $B \supseteq A$.

MEDIOCRE PUN 6.4. We can visualize a "superset" as a set wearing a cape and flying around saving people.

EXAMPLE 6.5. Let $A = \{a, b, c\}$ and $B = \{a, b, c, d\}$. Then $A \subseteq B$ by Def. 6.1, because every element of A is an element of B. Specifically, $a \in B$, $b \in B$, and $c \in B$, and a, b, and c are all of the elements of A. However, B is not a subset of A, because $d \in B$, but $d \notin A$.

PICTURE: VENN DIAGRAM TO GO WITH THIS EXAMPLE.

EXAMPLE 6.6. We have that $\mathbb{Z} \subseteq \mathbb{Q}$ by Def. 6.1, because every element of $\mathbb{Z}$ is an element of $\mathbb{Q}$. In other words, $\mathbb{Z} \subseteq \mathbb{Q}$ because every integer is a rational number. Note that we cannot check one element at a time, as we did in Example 6.5, because $\mathbb{Z}$ has infinitely many elements.

Also note that $\mathbb{Q}$ is not a subset of $\mathbb{Z}$, because $\frac{1}{2} \in \mathbb{Q}$, but $\frac{1}{2} \notin \mathbb{Z}$.

CHECK FOR UNDERSTANDING 6.7.

(1) Let $\Theta = \{a, b, c\}$, $\Upsilon = \{a, b, c, d\}$, $\Phi = \{a, b, d\}$. Which of the following statements are true: $\Theta \subseteq \Upsilon$? $\Upsilon \subseteq \Theta$? $\Upsilon \subseteq \Phi$? $\Phi \subseteq \Upsilon$? $\Phi \subseteq \Theta$? $\Theta \subseteq \Phi$?

(2) Which of the following statements are true: $\mathbb{N} \subseteq \mathbb{Z}$? $\mathbb{Z} \subseteq \mathbb{N}$?

(3) Is the set of all negative real numbers a subset of $\mathbb{Q}$?

(4) Given that $x \in B$ and $B \subseteq H$, does Def. 6.1 apply? If so, what conclusion can you make?

(5) Given that $x \in H$ and $B \subseteq H$, does Def. 6.1 apply? If so, what conclusion can you make?

(6) Given that $\alpha \in \Delta$, what additional information would you need in order for Def. 6.1 to imply that $\alpha \in \Gamma$?

TOO MUCH INFORMATION 6.8. It will happen *very frequently* in your later math courses that you will be asked to prove that one set is a subset of another. The approach in Example **??** is *extremely* typical. That is, we have:

One common way to show $A \subseteq B$: First let $x \in A$. Then show $x \in B$.

THEOREM 6.9. *If A, B, and C are sets such that $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

PROOF. We will show that if $x \in A$, then $x \in C$.
Let $x \in A$. (Note: See Remark 6.12.)
Then $x \in B$, by definition of "subset," because we know that $x \in A$ and $A \subseteq B$.
Then $x \in C$, by definition of "subset," because we know that $x \in B$ and $B \subseteq C$.
Therefore the statement "If $x \in A$, then $x \in C$." is true.
Therefore $A \subseteq C$, by definition of "subset." ■

EXAMPLE 6.10 (Common Mistake). Here's a student mistake we've seen many times. Can you find the error(s)?

Show that if A, B, and C are sets such that $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

PROOF. We will show that $x \in A$ and $x \in C$.
$x \in A$ and $x \in B$, because $A \subseteq B$.
$x \in B$ and $x \in C$, because $B \subseteq C$.
Therefore $A \subseteq C$, by definition of "subset." ■

There are two mistakes here. One is that the variable x was never introduced. Remember to introduce all variables. (IT WOULD BE NICE TO HAVE A "COMMON MISTAKES" SECTION OR SOMETHING LIKE THAT TO REFER BACK TO HERE.) The other problem is that the student seems to think that the definition of $A \subseteq C$ is "$x \in A$ and $x \in C$." Read Def. 6.1 again. The correct definition of $A \subseteq C$ is "*If* $x \in A$, *then* $x \in C$." The point is that *starting* from the information that $x \in A$, we must *end* with the information that $x \in C$. That's what "if-then" means. The statement "$x \in A$ and $x \in C$" means that we know both "$x \in A$" and "$x \in C$" simultaneously. Remember that $P \Rightarrow Q$ is not the same as P and Q. (IT WOULD BE NICE TO HAVE A "COMMON MISTAKES" SECTION OR SOMETHING LIKE THAT TO REFER BACK TO HERE.)

TOO MUCH INFORMATION 6.11. Note that the empty set is a subset of every other set. For by Def. 6.1, we have that $\emptyset \subseteq B$ is equivalent to the statement "If $x \in \emptyset$, then $x \in B$." This statement is vacuously true, because the empty set does not contain any elements.

TOO MUCH INFORMATION 6.12. ACTUALLY THIS TECHNICALITY HAPPENS IN EVERY SINGLE "FOR ALL" PROOF. SO WE SHOULD MENTION THIS IN THE PROOFS CHAPTER.

There is a small technicality in Example **??**. At one point in the proof, we wrote "Let $x \in A$." But what if A is the empty set? Then we cannot write "Let $x \in A$," because A does not have any elements.

So it might be slightly more precise to split into cases here, as in: "Case 1: $A = \emptyset$. Then $A \subseteq C$ is vacuously true—see Remark 6.11. Case 2: $A \neq \emptyset$. Let $x \in A \ldots$" In practice, though, mathematicians never do this. Because Case 1 here is *always* vacuously true, we always proceed directly to Case 2—we never bother splitting into cases in this situation. But we think it's worth pointing out, because in general you should never write a sentence like "Let $x \in A$" without first asking yourself, "But what if $A = \emptyset$?"

MAYBE WE CAN INSERT A YELLOW "CAUTION" ROAD SIGN HERE?

Too Much Information 6.13. When $A \subseteq B$, mathematicians sometimes say that "B contains A." Careful! When $x \in B$, mathematicians also sometimes say that "B contains x." The word "contains" means two very different things in these two sentences. In the first sentence, it means, "A is a *subset* of B." In the second sentence, it means, "x is an *element* of B." This is *not* the same thing! We'll have more to say about this later on.

Assumption 6.14. *Two sets are equal iff each is a subset of the other. That is, $A = B$ iff $A \subseteq B$ and $B \subseteq A$.*

Assumption 6.14 essentially tells us what it means for two sets to be equal, namely, that they contain exactly the same elements.

Too Much Information 6.15. Some books refer to Assumption 6.14 as the definition of set equality. In set theory, Assumption 6.14 is sometimes called the Axiom of Extensionality.

Example 6.16. Prove that if $A \subseteq B$ and $B \subseteq C$ and $C \subseteq D$ and $D \subseteq A$, then $A = C$.

Proof. Let A, B, C, D be sets such that $A \subseteq B$ and $B \subseteq C$ and $C \subseteq D$ and $D \subseteq A$.
We will show that $A = C$.
To do so, we will show that $A \subseteq C$ and $C \subseteq A$.
We know that $A \subseteq B$ and $B \subseteq C$, so by Theorem 6.9, it follows that $A \subseteq C$.
Also, we know that $C \subseteq D$ and $D \subseteq A$, so by Theorem 6.9, it follows that $C \subseteq A$. Therefore $A \subseteq C$ and $C \subseteq A$.
So by Assumption 6.14, $A = C$. ■

Too Much Information 6.17. It will happen *very frequently* in your later math courses that you will be asked to prove that two sets are equal. The approach in Example 6.16 is *extremely* typical. That is, we have:

One common way to show $A = B$, where A and B are sets:
First show $A \subseteq B$. Then show $B \subseteq A$.

There's one special case that's worth mentioning. Namely, when you're trying to show that a set equals the empty set, it's often best to use contradiction. Begin by temporarily assuming that the set is not empty—that is, that it contains at least one element.

One common way to show $A = \emptyset$:
Temporarily there exists $x \in A$. Then derive a contradiction.

Example 6.18. Let $\Delta = \{x \in \mathbb{R} \mid x + 1 = x + 2\}$. Prove that $\Delta = \emptyset$.

Proof. Temporarily assume that there exists $x \in \Delta$.
Then $x + 1 = x + 2$, by definition of Δ.
So $1 = 2$, by subtracting x from both sides.
Contradiction.
So there does not exist $x \in \Delta$.
Therefore $\Delta = \emptyset$. ■

Too Much Information 6.19. If you really wanted to, you could use Assumption 6.14 in Example 6.18. The statements "If $x \in \Delta$, then $x \in \emptyset$" and "If $x \in \emptyset$, then $x \in \Delta$" are both vacuously true. So Δ and $\emptyset$ are each subsets of each other, hence equal.

Definition 6.20. Let A and B be sets. We say that A is a **proper subset** of B if $A \subseteq B$ and $A \neq B$. We denote that A is a proper subset of B by writing $A \subset B$.

Example 6.21. The set $\{a, b, c\}$ is a proper subset of $\{a, b, c, d\}$.

WARNING SYMBOL, YELLOW CAUTION SIGN, WHATEVER

Too Much Information 6.22. Recall Remark 6.2—so the notation $A \subset B$ is ambiguous! Depending what book you're reading, it can either mean "A is a subset of B" or "A is a proper subset of B."

Books that use the alternative notation $A \subset B$ for "A is a subset of B" also sometimes use the notation $A \subsetneq B$ for "A is a proper subset of B."

MEDIOCRE PUN 6.23. We can visualize a "proper" subset as a subset with elegant table manners.

Examples from number theory

EXAMPLE 6.24. Let $\Sigma = \{n \in \mathbb{Z} \mid n \text{ is even}\}$. Let $\Delta = \{n \in \mathbb{Z} \mid 4 \text{ divides } n\}$. Show that $\Delta \subseteq \Sigma$.

PROOF. We'll show that if $n \in \Delta$, then $n \in \Sigma$. Let $n \in \Delta$. We'll show that $n \in \Sigma$.
We know that $n \in \mathbb{Z}$ and $4|n$, by definition of Δ.
So $n = 4k$ for some $k \in \mathbb{Z}$, by definition of "divides."
Then $n = 2(2k)$.
We know $2k \in \mathbb{Z}$, because $2, k \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under multiplication.
So n is even, by definition of "even."
Because $n \in \mathbb{Z}$ and n is even, therefore $n \in \Sigma$, by definition of Σ.
Therefore the statement "If $n \in \Delta$, then $n \in \Sigma$" is true.
Therefore $\Delta \subseteq \Sigma$, by definition of "subset." ■

Let's take a step back and think about what we just did. We showed that every multiple of 4 is even. That's what the statement $\Delta \subseteq \Sigma$ was saying.

Examples from the real line and plane

WHERE DO WE INTRODUCE INTERVAL NOTATION? BASIC SET THEORY?

EXAMPLE 6.25. Let $a, b, c, d \in \mathbb{R}$ such that $a < b$ and $c < d$. Show $[c, d] \subseteq (a, b)$ iff $a < c < d < b$.

PROOF. First we will show that if $[c, d] \subseteq (a, b)$ then $a < c < d < b$.
Let $a, b, c, d \in \mathbb{R}$ such that $a < b$ and $c < d$ and $[c, d] \subseteq (a, b)$.
We will show that $a < c < d < b$.
We know that $c, d \in [c, d]$ by definition of "closed interval," because $c \leq c \leq d$ and $c \leq d \leq d$.
So $c, d \in (a, b)$ by definition of "subset."
So $a < c < b$ and $a < d < b$, by definition of "open interval."
So $a < c < d < b$, because we are given that $c < d$.

Now we will show that if $a < c < d < b$, then $[c, d] \subseteq (a, b)$.
Let $a, b, c, d \in \mathbb{R}$ such that $a < b$ and $c < d$ and $a < c < d < b$.
We will show that $[c, d] \subseteq (a, b)$.
Let $x \in [c, d]$. We will show that $x \in (a, b)$.

We know that $c \leq x \leq d$, by definition of "closed interval."
Therefore $a < x$, because $a < c$ and $c \leq x$.
Also, $x < b$, because $x \leq d$ and $d < b$.
Therefore $x \in (a, b)$ by definition of "open interval," because $a < x < b$.
So $[c, d] \subseteq (a, b)$ by definition of "subset," because the statement "If $x \in [c, d]$, then $x \in (a, b)$" is true.

Therefore $[c, d] \subseteq (a, b)$ iff $a < c < d < b$, because the statements "if $[c, d] \subseteq (a, b)$ then $a < c < d < b$" and "if $a < c < d < b$, then $[c, d] \subseteq (a, b)$" are both true. ■

FORMATTING: I THINK THIS WOULD LOOK BETTER WITH SPACE BETWEEN PARAGRAPHS AND NO INDENTING.

DEFINITION 6.26. Let $A \subseteq \mathbb{R}$. We say that A is an **open** subset of $\mathbb{R}$ if for all $x \in A$, there exist $c, d \in \mathbb{R}$ such that $c < x < d$ and $(c, d) \subset A$.

EXAMPLE 6.27. Let $P = \{x \in \mathbb{R} \mid x > 0\}$. Prove that P is an open subset of $\mathbb{R}$.

PROOF. We will show that for all $x \in P$, there exist $c, d \in \mathbb{R}$ such that $c < x < d$ and $(c, d) \subset P$.
Let $x \in P$. We will show that there exist $c, d \in \mathbb{R}$ such that $c < x < d$ and $(c, d) \subset P$.
Let $c = \frac{x}{2}$ and $d = 2x$.
We know $x > 0$, by definition of P.
So $c < x < d$, because $x > 0$.
Now we will show that $(c, d) \subset P$.
Let $y \in (c, d)$. We will show that $y \in P$.
We know that $c < y$, by definition of "open interval."
We know $0 < c$, because $c = \frac{x}{2}$ and $x > 0$.
So $y > 0$, because $c < y$ and $0 < c$.
Therefore $y \in P$, by definition of P.
So the statement "If $y \in (c, d)$, then $y \in P$" is true.
So $(c, d) \subset P$, by definition of subset.
So the statement "For all $x \in P$, there exist $c, d \in \mathbb{R}$ such that $c < x < d$ and $(c, d) \subset P$" is true.
Therefore P is an open subset of $\mathbb{R}$, by definition of "open." ■

Figure **??** illustrates this proof.

Figure showing the open interval $(\frac{x}{2}, 2x)$ on the real line, with x in the middle.

Too Much Information 6.28. You will see open sets a *lot* if you take a course in Analysis or Topology.

6.2. Unions, intersections, and complements

In this section, we will learn about ways to make new sets from old ones.

Definition 6.29. Let A, B be sets. We define the **union** of A and B, denoted $A \cup B$, by

$$A \cup B := \{x \mid x \in A \text{ or } x \in B\}.$$

HAVE WE MENTIONED ":=" BEFORE?

Figure **??** shows a Venn diagram for the union of A and B.

Definition 6.30. Let A, B be sets. We define the **intersection** of A and B, denoted $A \cap B$, by

$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}.$$

Figure **??** shows a Venn diagram for the intersection of A and B.

Example 6.31. Let $\Gamma = \{3, 7, 9, 47\}$ and $\Psi = \{7, 8, 9, 10\}$. Then $\Gamma \cup \Psi = \{3, 7, 8, 9, 10, 47\}$ and $\Gamma \cap \Psi = \{7, 9\}$. Let $\Lambda = \{22, -6, 3\}$. Then $\Lambda \cap \Psi = \emptyset$ and $(\Lambda \cap \Gamma) \cup \Psi = \{3, 7, 8, 9, 10\}$.

Example 6.32. Let $\Theta = \{x \in \mathbb{R} \mid x > 0\}$. Then $\Theta \cap \mathbb{Z} = \mathbb{N}$. HAVE WE DECIDED IF N CONTAINS 0?

Example 6.33. Suppose $a \in (X \cup Y) \cap Z$. What can we conclude about a? By definition of intersection, a is in both $X \cup Y$ and Z. By definition of union, a is in X or a is in Y. So a is either in both X and Z, or a is in both Y and Z.

Check for Understanding 6.34.

(1) Let $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$. Describe $\{3\}$ and $\{1, 2, 3, 4, 5\}$ in terms of A and B.

(2) What is $\mathbb{Z} \cap (-4, 5]$?

(3) Suppose $a \in (X \cap Y) \cup Z$. What can we conclude about a?

EXAMPLE 6.35. Let A and B be sets. Show that $A \subseteq A \cup B$.

PROOF. Let $x \in A$.
Then the statement "$x \in A$ or $x \in B$" is true.
Therefore $x \in A \cup B$, by definition of "union." ■

EXAMPLE 6.36. Let A, B, and C be sets. Show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

PROOF. First, we will show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
Let $x \in A \cap (B \cup C)$.
Then $x \in A$ and $x \in B \cup C$, by definition of "intersection."
So $x \in B$ or $x \in C$, by definition of "union."
Case 1: $x \in B$
Then $x \in A \cap B$, by definition of "intersection."
So $x \in (A \cap B) \cup (A \cap C)$, by definition of "union."
Case 2: $x \in C$
Then $x \in A \cap C$, by definition of "intersection."
So $x \in (A \cap B) \cup (A \cap C)$, by definition of "union."
In either case, we have $x \in (A \cap B) \cup (A \cap C)$.
So the statement "If $x \in A \cap (B \cup C)$, then $x \in (A \cap B) \cup (A \cap C)$." is true.
Therefore $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$, by definition of "subset."
Next, we will show that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
Let $x \in (A \cap B) \cup (A \cap C)$.
Then $x \in A \cap B$ or $x \in A \cap C$, by definition of "union."
Case 1: $x \in A \cap B$
Then $x \in A$ and $x \in B$, by definition of "intersection."
Then $x \in B \cup C$, by definition of "union."
So $x \in A \cap (B \cup C)$, by definition of intersection.
Case 2: $x \in A \cap C$
Then $x \in A$ and $x \in C$, by definition of "intersection."
Then $x \in B \cup C$, by definition of "union."
So $x \in A \cap (B \cup C)$, by definition of intersection.
In either case, we have $x \in A \cap (B \cup C)$.
So the statement "If $x \in (A \cap B) \cup (A \cap C)$, then $x \in A \cap (B \cup C)$." is true.
Therefore $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, by definition of "subset." ■

Hence the two sets $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ are subsets of each other.
Therefore, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Definition 6.37. Let A, B be sets. We define the **difference** of A and B, denoted $A \setminus B$, by

$$A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}.$$

Figure **??** shows a Venn diagram for the intersection of A and B.
VENN DIAGRAM OF A MINUS B

Too Much Information 6.38. Some books write $A - B$ instead of $A \setminus B$.

Too Much Information 6.39. The difference of A and B is sometimes called the **relative complement** of A with respect to B.

Example 6.40. Let $\Omega = \{2, 4, 6, 8\}$ and $\Sigma = \{1, 2, 3, 4\}$. Then $\Omega \setminus \Sigma = \{6, 8\}$ and $\Sigma \setminus \Omega = \{1, 3\}$. Notice that $\Omega \setminus \Sigma \neq \Sigma \setminus \Omega$.

Example 6.41. Let $A = (-2, 5]$ and $B = [4, 5]$. Then $A \setminus B = (-2, 4)$ and $B \setminus A = \emptyset$.

Sometimes, we have a "universal set" or "universe" which contains all of the elements that we wish to consider. For example, in number theory, the universe is often $\mathbb{Z}$. In an analysis course, the universe is sometimes the real line or plane. When we know what the universal set is, we can talk about the "complement" of a set.

Definition 6.42. Let A be set, where U is a universal set. The **complement** of A, denoted A^c, is the set $A^c := U \setminus A$. In other words,

$$A^c = \{x \notin A\}.$$

In other words, the complement of A is the set of all elements not in A. Figure **??** shows a Venn diagram representing the complement of a set A.
VENN DIAGRAM FOR COMPLEMENT—PUT GALAXIES IN THE UNIVERSE

Mediocre Pun 6.43. In Figure **??**, notice the galaxies swirling about the universe.

Too Much Information 6.44. Notice in Def. 6.56 that we do *not* need to write $A^c = \{x \in U \mid x \notin A\}$, because all elements are assumed to be in the universe.

TOO MUCH INFORMATION 6.45. Why do we need to have a universe in Def. 6.56? The reason is that if we are not careful, then we will run into serious technical difficulties—logical paradoxes that at one time threatened to undermine the foundations of mathematics. See the "Fun Math Facts" at the end of this chapter for more on this.

TOO MUCH INFORMATION 6.46. Books vary wildly in their notations for the complement of a set. Some other notations for the complement of A are $\overline{A}$, A', or A^*. CAUTION! All of these alternate notations have other meanings in analysis and in topology.

EXAMPLE 6.47. Suppose the universe U is $\{1, 2, 3, 4, 5\}$ and $A = \{1, 3, 4\}$. Then $A^c = \{2, 5\}$.

Now suppose the universe U is $\{1, 2, 3, 4, 5, 6\}$ and $A = \{1, 3, 4\}$. Then $A^c = \{2, 5, 6\}$.

Notice that to know what the complement of a set is, you must know what the universe is.

EXAMPLE 6.48. Suppose the universe is $\mathbb{Z}$. Let $\Pi = \{x \in \mathbb{Z} \mid x \text{ is even }\}$. Then $\Pi^c = \{x \in \mathbb{Z} \mid x \text{ is odd }\}$.

EXAMPLE 6.49. Suppose the universe is $\mathbb{R}$. Then $(-1, 2)^c = (-\infty, -1] \cup [2, \infty)$, as shown in Figure **??**. FIGURE OF THIS ON A NUMBER LINE.

EXAMPLE 6.50. Let A be a set. Prove that $(A^c)^c = A$.

PROOF. First we will show that $(A^c)^c \subseteq A$.
Let $x \in (A^c)^c$.
Then $x \notin A^c$, by definition of "complement."
So $x \in A$, by definition of "complement."
Therefore $(A^c)^c \subseteq A$, by definition of "subset."

Now we will show that $A \subseteq (A^c)^c$.
Let $x \in A$.
Then $x \notin A^c$, by definition of "complement."
So $x \in (A^c)^c$, by definition of "complement."
Therefore $A \subseteq (A^c)^c$, by definition of "subset."

Hence $(A^c)^c = A$. ■

CHECK FOR UNDERSTANDING 6.51. Apply the result in Example 6.50 to fill in the blank: $((A^c \cap B^c)^c)^c =$ ____.

TOO MUCH INFORMATION 6.52. Here's a quick one-line proof for Example 6.50: $x \in A$ iff $x \notin A^c$ iff $x \in (A^c)^c$.

We've seen de Morgan's laws previously, in the logic chapter. The following two theorems are the set theory versions of de Morgan's laws.

THEOREM 6.53 (de Morgan's laws). *Let A and B be sets. Then*
(1) $(A \cap B)^c = A^c \cup B^c$, *and*

(2) $(A \cup B)^c = A^c \cap B^c$.

PROOF. (1) First we will show that $(A \cap B)^c \subseteq A^c \cup B^c$.
Let $x \in (A \cap B)^c$.
Then $x \notin A \cap B$, by definition of "complement."
In other words, the statement "$x \in A \cap B$" is false.
So the statement "$x \in A$ and $x \in B$" is false, by definition of "intersection."
So $x \notin A$ or $x \notin B$, by de Morgan's laws for logic.
So $x \in A^c$ or $x \in B^c$, by definition of "complement."
So $x \in A^c \cup B^c$, by definition of "union."
Therefore, $(A \cap B)^c \subseteq A^c \cup B^c$, by definition of "subset."

Now we will show that $A^c \cup B^c \subseteq (A \cap B)^c$.
⟨*This proof is similar to the reverse direction, so as a check for understanding, we'll leave some blanks for you to fill in.*⟩
Let $x \in A^c \cup B^c$.
Then $x \in A^c$ or $x \in B^c$, by definition of "____."
So $x \notin A$ or $x \notin B$, by definition of "____."
So the statement "$x \in A$ and $x \in B$" is false, by ____.
So $x \notin A \cap B$, by definition of "____."
So $x \in (A \cap B)^c$, by definition of "____." Therefore $A^c \cup B^c \subseteq (A \cap B)^c$, by definition of "____."

Therefore, $(A \cap B)^c = A^c \cup B^c$.

(2) ⟨*We could do a proof similar to (1) here, but let's take the opportunity to show off and do a slick proof.*⟩
We get $(A^c \cap B^c)^c = (A^c)^c \cup (B^c)^c$ by substituting A^c for A and B^c for B in Thm. 6.53 (1).
So $(A^c \cap B^c)^c = A \cup B$, by the result in Example 6.50.
So $A^c \cap B^c = (A \cup B)^c$, by taking complements of both sides and again applying the result in Example 6.50. ■

TOO MUCH INFORMATION 6.54. Wait a minute—in the proof of (2), did we just use Thm. 6.53 to prove Thm. 6.53? Isn't that circular reasoning? No, it's not circular reasoning. Our proof is fine.

Here's why. First we proved (1). Once we did that, then (1) became a previously proven statement, so we were allowed to use it to prove (2).

Too Much Information 6.55. Take the time to translate de Morgan's laws into English and to see why they're pretty much common sense when you stop and think about them. For example, Thm. 6.53 (1) says, "It's not true that x is in both A and B if and only if either x is not in A or x is not in B."

Definition 6.56. Let A and B be sets. We say that A and B are **disjoint** if $A \cap B = \emptyset$.

Example 6.57. The sets $\mathbb{N}$ and $(-3, -1.5)$ are disjoint.

Example 6.58. Let A be a set, and let U be the universe. Prove that A and A^c are disjoint.

Proof. We will show that $A \cap A^c = \emptyset$.
Temporarily assume that there exists $x \in A \cap A^c$.
Then $x \in A$ and $x \in A^c$, by definition of "intersection."
So $x \in U \setminus A$, by definition of "complement."
So $x \notin A$, by definition of "difference."
Contradiction ($x \in A$ but $x \notin A$).
So there does not exist $x \in A \cap A^c$.
So $A \cap A^c = \emptyset$.
So A and A^c are disjoint, by definition of "disjoint." ■

Examples from number theory

Example 6.59. For any integer n, we define the set $\langle n \rangle := \{x \mid x \in \mathbb{Z} \text{ and } n \text{ divides } x\}$. In other words, $\langle n \rangle$ is the set of all multiples of n. Let $a, b \in \mathbb{Z}$, and let $d = \text{lcm}(a, b)$. HAVE WE DEFINED LCM??? Prove that $\langle a \rangle \cap \langle b \rangle = \langle d \rangle$.

Proof. First we will show that $\langle a \rangle \cap \langle b \rangle \subseteq \langle d \rangle$.
Let $x \in \langle a \rangle \cap \langle b \rangle$.
Then $x \in \langle a \rangle$ and $x \in \langle b \rangle$, by definition of "intersection."
Then $a|x$ and $b|x$, by definition of $\langle n \rangle$.
So $d|x$, by NEED A REFERENCE.
So $x \in \langle d \rangle$, by definition of $\langle n \rangle$.
So $\langle a \rangle \cap \langle b \rangle \subseteq \langle d \rangle$, by definition of subset.
Conversely, $\langle d \rangle \subseteq \langle a \rangle \cap \langle b \rangle$, because every multiple of d is both a multiple of a and a multiple of b.

⟨*We combined several steps into one in that last line—as an exercise, you might try spelling it out step-by-step, the way we did in the first half of the proof.*⟩
Therefore, $\langle a \rangle \cap \langle b \rangle = \langle d \rangle$. ■

You will see the sets $\langle n \rangle$ again if you take a course (or courses) in Abstract Algebra—they are important examples of *subgroups* in group theory and *ideals* in ring theory.

Examples from the real line and plane

EXAMPLE 6.60. Let I_1 and I_2 be open intervals. Prove that I_1 and I_2 are disjoint, or $I_1 \cap I_2$ is an open interval.

PROOF. By definition of "open interval," there exist $a, b, c, d \in \mathbb{R}$ with $a < b$ and $c < d$ such that $I_1 = (a, b)$ and $I_2 = (c, d)$.
Without loss of generality, assume that $a \leq c$.
⟨*If it is not true that $a \leq c$, then reverse the roles of I_1 and I_2. It's okay to do that, because the statement "I_1 and I_2 are disjoint, or $I_1 \cap I_2$ is an open interval." is true iff the statement "I_2 and I_1 are disjoint, or $I_2 \cap I_1$ is an open interval." is true.*⟩
Case 1: $d \leq b$.
By Exercise 7, we have $I_1 \cap I_2 = (c, d)$, which is an open interval.
Case 2: $c < b < d$.
By Exercise 8, we have $I_1 \cap I_2 = (c, b)$, which is an open interval.
Case 3: $b \leq c$.
In this case, no real number is both less than b and greater than c.
So $I_1 \cap I_2 = \emptyset$.
So I_1 and I_2 are disjoint, by definition of "disjoint."
Therefore I_1 and I_2 are disjoint, or $I_1 \cap I_2$ is an open interval, because this statement holds in every case. ■

Figure **??** illustrates the three different cases in this proof.

WE NEED SOME DISCUSSION OF "WLOG," WITH EXAMPLES, EXERCISES, ETC. IN THE PROOFS CHAPTER? MAYBE IN THE "CASES" SECTION OF THE PROOFS CHAPTER? SAMPLE EXERCISE: SHORTEN SUCH-AND-SUCH A PROOF WITH WLOG. FOR EXAMPLE, LET x AND y BE DISTINCT REAL NUMBERS. PROVE THERE IS A REAL BETWEEN x AND y. (GOTTA DEFINE "BETWEEN."—MAYBE THIS ISN'T THE BEST EXAMPLE.)

CHECK FOR UNDERSTANDING 6.61. Express the complement of an arbitrary open interval as a union of two rays.

DEFINITION 6.62. Let $X \subseteq \mathbb{R}$. We say X is **disconnected** if there exist disjoint nonempty open sets $U, V \subseteq \mathbb{R}$ such that $X \subseteq U \cup V$. We say X is **connected** if it is not disconnected.

TOO MUCH INFORMATION 6.63. Intuitively, a set is connected if it is "all in one piece," and it is disconnected if it can be separated into different pieces with a little "room" between them. The open sets in Definition 6.62 make this notion precise.

EXAMPLE 6.64. Prove that $\mathbb{Z}$ is disconnected.

PROOF. Let $U = (1/2, \infty)$ and $V = (-\infty, 1/2)$.
By Exercise 3, U and V are open subsets of $\mathbb{R}$.
Also, U and V are disjoint, because no real number can be both greater than $1/2$ and less than $1/2$.
Also, $\mathbb{Z} \subseteq U \cup V$, because every integer is either greater than $1/2$ or less than $1/2$.
Therefore $\mathbb{Z}$ is disconnected, by definition of "disconnected." ■

TOO MUCH INFORMATION 6.65. Connectedness is an important topological property. If you take a Topology class, you will learn a great deal more about it. You will prove, for example, that $\mathbb{R}$ is connected, something that is intuitively obvious but takes some work to demonstrate.

6.3. Cartesian products

INFORMAL DEFINITION 6.66. *An **ordered pair** is an expression of the form (a, b), where a and b are any two objects. We say a is the **first coordinate** of (a, b) and b is the **second coordinate** of (a, b). The most important fact about ordered pairs is the following:*

Let (a, b) and (c, d) be two ordered pairs. Then $(a, b) = (c, d)$ iff $a = c$ and $b = d$.

In other words, two ordered pairs are equal iff their first coordinates are equal and their second coordinates are equal.

EXAMPLE 6.67. True or false: $(2, -3) = (-3, 2)$?

The answer is "false," because $2 \neq -3$, so the two ordered pairs do not have the same first coordinate.

This is why ordered pairs have that name—because order matters. In contrast, $\{2, -3\} = \{-3, 2\}$ because those two sets have the same elements. With sets, order doesn't matter.

EXAMPLE 6.68. Let $x, y \in \mathbb{R}$ such that $(x, 6) = (2y, x)$. Determine x and y.

We know $x = 2y$ (from the first coordinates) and $6 = x$ (from the second coordinates). So $6 = 2y$ by substitution. So $y = 3$.

TOO MUCH INFORMATION 6.69. If we want to be completely precise, then we define the ordered pair $(a, b) := \{a, \{a, b\}\}$. You can check that $\{a, \{a, b\}\} = \{c, \{c, d\}\}$ iff $a = c$ and $b = d$, so this definition has the desired property. The only point here is that it's possible to define ordered pairs in terms of sets. In practice, though, mathematicians almost never think of them that way.

TOO MUCH INFORMATION 6.70. Unfortunately, the notation (a, b) is ambiguous. If a and b are real numbers, then (a, b) could be an ordered pair, or it could be an open interval. You have to figure out from context which it is. Sorry about that. But, hey, don't blame us—*we* didn't make this stuff up.

DEFINITION 6.71. Let A and B be sets. The **Cartesian product** (or **cross product**) of A and B is denoted $A \times B$ (read: "A cross B") and is defined to be the set

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

EXAMPLE 6.72. Let $\Theta = \{1, 2, 3\}$ and $\Gamma = \{\alpha, \beta\}$. Then $\Theta \times \Gamma = \{(1, \alpha), (2, \alpha), (3, \alpha), (1, \beta), (2, \beta), (3, \beta)\}$. Notice that $\Theta \times \Gamma \neq \Gamma \times \Theta$, because $(1, \alpha) \in \Theta \times \Gamma$ but $(1, \alpha) \notin \Gamma \times \Theta$.

We can visualize $\Theta \times \Gamma$ as in Figure **??**.

CHECK FOR UNDERSTANDING 6.73. Draw a picture to represent $\{-1, 2\} \times [-3, 4.5)$, and name five elements of this set.

TOO MUCH INFORMATION 6.74. Note that if A and B are finite sets, where A contains n elements and B contains m elements, then $A \times B$ contains nm elements.

In general, you can visualize Cartesian products by putting the first coordinates along a horizontal axis and the second coordinates along a vertical axis. You've been doing this since you started graphing lines

in high school algebra. Notice that we're avoiding saying "x-axis" and "y-axis," because sometimes we use different variables.

EXAMPLE 6.75. Let Γ, Δ, Θ be sets. Prove that if Γ and Δ are disjoint, then $\Gamma \times \Theta$ and $\Delta \times \Theta$ are disjoint.

PROOF. ⟨*Our goal is to show that* $\Gamma \times \Theta$ *and* $\Delta \times \Theta$ *do NOT have any elements in common. The word "not" tips us off that proof by contradiction is probably the way to go.*⟩
Temporarily assume that $\Gamma \times \Theta$ and $\Delta \times \Theta$ are not disjoint.
Then $(\Gamma \times \Theta) \cap (\Delta \times \Theta) \neq \emptyset$, by definition of "disjoint."
So there exists $(a, b) \in (\Gamma \times \Theta) \cap (\Delta \times \Theta)$.
So $(a, b) \in \Gamma \times \Theta$ and $(a, b) \in \Delta \times \Theta$, by definition of "intersection."
So $a \in \Gamma$ and $a \in \Delta$, by definition of "Cartesian product."
So $a \in \Gamma \cap \Delta$, by definition of "intersection."
So $\Gamma \cap \Delta \neq \emptyset$.
But $\Gamma \cap \Delta = \emptyset$, by definition of "disjoint."
Contradiction.
Therefore $\Gamma \times \Theta$ and $\Delta \times \Theta$ are disjoint. ■

EXAMPLE 6.76. Let A, B, and C be sets. Prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

PROOF. First we will show that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.
Let $(x, y) \in A \times (B \cup C)$.
⟨*Note that* $A \times (B \cup C)$ *is a Cartesian product, so an arbitrary element of* $A \times (B \cup C)$ *is an ordered pair.*⟩
So $x \in A$ and $y \in B \cup C$, by definition of "Cartesian product."
So $y \in B$ or $y \in C$, by definition of "union."
Case 1: $y \in B$.
Then $y \in A$ and $y \in B$, so $(x, y) \in A \times B$, by definition of "Cartesian product."
Then $(x, y) \in (A \times B) \cup (A \times C)$, by definition of "union."
Case 2: $y \in C$.
Then $x \in A$ and $y \in C$, so $(x, y) \in A \times C$, by definition of "Cartesian product."
Then $(x, y) \in (A \times B) \cup (A \times C)$, by definition of "union."
In either case, we have $(x, y) \in (A \times B) \cup (A \times C)$.
So we have shown that every element of $A \times (B \cup C)$ is an element of $(A \times B) \cup (A \times C)$.
Therefore $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, by definition of "subset."

Now we will show that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.
⟨*This proof is similar to the reverse direction, so as a check for understanding, we'll leave some blanks for you to fill in.*⟩

Let $(x, y) \in$ ____.
Then $(x, y) \in$ ____ or $(x, y) \in$ ____, by definition of "union."
Case 1: $(x, y) \in A \times B$
Then $x \in A$ and $y \in B$, by definition of ____.
So $y \in B \cup C$, by definition of ____.
So $(x, y) \in A \times (B \cup C)$, by definition of ____.
Case 2: ____
Then $x \in A$ and $y \in C$, by definition of Cartesian product.
So $y \in$ ____, by definition of "union."
So $(x, y) \in A \times (B \cup C)$, by definition of ____.
In either case, we have ____.
So every element of ____ is an element of ____.
Therefore $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$, by definition of ____. ■

Here's a one-line summary of our proof: $(x, y) \in A \times (B \cup C)$ iff $x \in A$ and ($y \in B$ or $y \in C$) iff $(x, y) \in (A \times B) \cup (A \times C)$.

Figure **??** shows one way to visualize the statement in this theorem. THREE GRAPHS: ONE WITH $A \times B$, ONE WITH $A \times C$, AND ONE WITH $A \times (B \cup C)$. HAVE B AND C OVERLAP A LITTLE.

CHECK FOR UNDERSTANDING 6.77. Let A, B, and C be sets. Draw a picture that represents $A \times (B \cap C)$. Fill in the blank to make a true statement, along the lines of Example 6.76: $A \times (B \cap C) =$ ____. In Exercise 2, you will be asked to prove that your answer is correct.

EXAMPLE 6.78. I DON'T KNOW IF I LIKE THIS EXAMPLE. Suppose $x \in A$ and $y \in B$. Prove that there exists a unique ordered pair (a, b) such that $(a, b) \in (\{x\} \times B) \cap (A \times \{y\})$.

PROOF. First we will show existence.
We will show that $(x, y) \in (\{x\} \times B) \cap (A \times \{y\})$.
We know $(x, y) \in \{x\} \times B$, by definition of "Cartesian product," because $x \in \{x\}$ and $y \in B$.
Also, $(x, y) \in A \times \{y\}$, by definition of "Cartesian product," because $x \in A$ and $y \in \{y\}$.
So $(x, y) \in (\{x\} \times B) \cap (A \times \{y\})$, by definition of "intersection."
Now we will show uniqueness. In other words, we will show that if $(c, d) \in (\{x\} \times B) \cap (A \times \{y\})$ and $(r, s) \in (\{x\} \times B) \cap (A \times \{y\})$, then $(c, d) = (r, s)$.
We know $(c, d) \in \{x\} \times B$ and $A \times \{y\}$, by definition of "intersection."
So $c \in \{x\}$, by definition of "Cartesian product," because $(c, d) \in \{x\} \times B$.
So $c = x$.

⟨*This also tells us that* $d \in B$*, but we won't be using that fact, so we'll leave it out of the proof.*⟩
Also $d \in \{y\}$, by definition of "Cartesian product," because $(c, d) \in A \times \{y\}$.
So $d = y$.
So $(c, d) = (x, y)$, because $c = x$ and $d = y$.
A similar argument, using (r, s) in place of (x, y), shows that $(r, s) = (x, y)$.
So $(c, d) = (x, y)$.
Therefore there exists a unique ordered pair (a, b) such that $(a, b) \in (\{x\} \times B) \cap (A \times \{y\})$. ■

Figure **??** is a "proof without words" for this example.

HAVE FINITE PRODUCTS, n-TUPLES HERE OR IN FAMILIES SECTION? PROBABLY HERE.

Examples from number theory

An element of $\mathbb{Z} \times \mathbb{Z}$ is called a **lattice point**. We can visualize the set $\mathbb{Z} \times \mathbb{Z}$ as in Fig. **??**.

FIGURE OF LATTICE POINTS

EXAMPLE 6.79. Let (a, b) be a lattice point with $a > 0$ and $b > 0$. Prove that there exists $t \in \mathbb{R}$ such that $0 < t < 1$ and (ta, tb) is a lattice point iff a and b are not relatively prime.

PROOF. First, we will show that if there exists $t \in \mathbb{R}$ such that $0 < t < 1$ and (ta, tb) is a lattice point, then a and b are not relatively prime.
Let $t \in \mathbb{R}$ such that $0 < t < 1$ and (ta, tb) is a lattice point.
Then $(ta, tb) \in \mathbb{Z} \times \mathbb{Z}$, by definition of "lattice point."
So $ta, tb \in \mathbb{Z}$, by definition of "Cartesian product."
Then $t = ta/a$, so $t \in \mathbb{Q}$, by definition of $\mathbb{Q}$.
Let r, s be positive integers such that $t = r/s$ and the fraction r/s is in lowest terms, that is, so that r and s are relatively prime.
Note that $s > 1$, because $t < 1$.
Then $ra/s \in \mathbb{Z}$, by substitution.
So $s|ra$, using the definition of "divides."
Therefore $s|a$, by Lemma **??**.
A similar argument shows that $s|b$.
Therefore a and b are not relatively prime, because they have a common factor greater than 1.

Next, we will show that if a and b are not relatively prime, then there exists $t \in \mathbb{R}$ such that $0 < t < 1$ and (ta, tb) is a lattice point.
Let $d = \gcd(a, b)$.

Then $d > 1$, by definition of "relatively prime."
Let $t = 1/d$.
Note that $0 < t < 1$.
Also, $d|a$ and $d|b$, by definition of "gcd."
So $ta, tb \in \mathbb{Z}$, using the definition of "divides."
So $(ta, tb) \in \mathbb{Z} \times \mathbb{Z}$, by definition of "Cartesian product."
So (ta, tb) is a lattice point, by definition of "lattice point." ■

Visually, the statement in this example is saying that the line segment between (a, b) and the origin contains a lattice point other than the two endpoints iff a and b have a common factor greater than 1. See Figure **??**. FIGURE SHOULD SHOW BOTH CASES—ONE WHERE THEY ARE COPRIME AND ONE WHERE THEY ARE NOT.

Examples from the real line and plane

We visualize the set $\mathbb{R}$ as a straight line. Indeed, sometimes we call $\mathbb{R}$ the "real line." We can visualize the set $\mathbb{R} \times \mathbb{R}$ as a flat plane, sometimes called the "Cartesian plane." We often write $\mathbb{R}^2$ instead of $\mathbb{R} \times \mathbb{R}$.

DEFINITION 6.80. Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. The **distance from** (x_1, y_1) **to** (x_2, y_2), denoted $\text{dist}((x_1, y_1), (x_2, y_2))$, is defined by:

$$\text{dist}((x_1, y_1), (x_2, y_2)) := \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

TOO MUCH INFORMATION 6.81. This "distance" is sometimes called "Euclidean distance" or "straight-line distance." As you will learn if you take an Analysis class, there are other notions of distances in the plane (as well as in other sets).

TOO MUCH INFORMATION 6.82. MAYBE MAKE THIS A "COMPLETELY IGNORABLE SIDE COMMENT" WITHIN A "COMPLETELY IGNORABLE SIDE COMMENT" ENVIRONMENT??? Of course you'll recognize the equation in Def. 6.80 as the familiar distance formula. In high school algebra, you derive this formula from the Pythagorean theorem. In order to do so, you must first make some assumptions about distances in the plane. Here, we've taken a subtly different approach, where we don't make any assumptions at all about distance—instead, we simply define the word "distance."

EXAMPLE 6.83. Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$. Prove that $\text{dist}(\mathbf{x}, \mathbf{y}) = 0$ iff $\mathbf{x} = \mathbf{y}$.

PROOF. First we will show that if $\text{dist}(\mathbf{x}, \mathbf{y}) = 0$, then $\mathbf{x} = \mathbf{y}$.
We know $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$, so we know $\mathbf{x} = (a, b)$ and $\mathbf{y} = (c, d)$ for some

$a, b, c, d \in \mathbb{R}$, by definition of "Cartesian product."
Then $\sqrt{(a-c)^2 + (b-d)^2} = 0$, by definition of "distance."
Squaring both sides, we get $(a-c)^2 + (b-d)^2 = 0$.
Now, we must have $(a-c)^2 = 0$ and $(b-d)^2 = 0$, because $(a-c)^2 \geq 0$ and $(b-d)^2 \geq 0$.
So $a - c = 0$ and $b - d = 0$.
So $a = c$ and $b = d$.
Therefore $\mathbf{x} = (a, c) = (b, d) = \mathbf{y}$.
Now we will show that if $\mathbf{x} = \mathbf{y}$, then $\text{dist}(\mathbf{x}, \mathbf{y}) = 0$.
Again, take $\mathbf{x} = (a, b)$ and $\mathbf{y} = (c, d)$.
So $a = c$ and $b = d$, because $\mathbf{x} = \mathbf{y}$.
So $\text{dist}(\mathbf{x}, \mathbf{y}) = \sqrt{(a-c)^2 + (b-d)^2} = 0$, by definition of "distance." ■

DEFINITION 6.84. Let $\mathbf{x} \in \mathbb{R}^2$ and $\epsilon \in \mathbb{R}$. The **open disc of radius ϵ centered at $\mathbf{x}$**, denoted $B(\mathbf{x}, \epsilon)$, is defined by:

$$B(\mathbf{x}, \epsilon) := \{\mathbf{y} \in \mathbb{R}^2 \mid \text{dist}(\mathbf{x}, \mathbf{y}) < \epsilon\}.$$

Figure **??** shows a picture of an open disc.

TOO MUCH INFORMATION 6.85. At some point, you may call an open disc a "circle." Wrong! Wrong! Wrong again, we say! In math, a circle consists only of the "edge" surrounding the open disc. The open disc is the inside. The circle is the skin, the open disc is the guts and all the other internal organs. The circle is the wrapper, the open disc is the candy. The circle is the orange peel, the open disc is the orange fruit. We realize we're going completely overboard here, but we can't seem to help ourselves.

CHECK FOR UNDERSTANDING 6.86. Let $\mathbf{x} \in \mathbb{R}^2$ and $r, s \in \mathbb{R}$. Suppose that $r < s$. Consider the two sets $B(\mathbf{x}, r)$ and $B(\mathbf{x}, s)$. Which one must be a subset of the other? Prove that your answer is correct.

DEFINITION 6.87. Let $U \subset \mathbb{R}^2$. We say U is **open** if for all $\mathbf{x} \in U$, there exists $\epsilon > 0$ such that $B(\mathbf{x}, \epsilon) \subseteq U$.

TOO MUCH INFORMATION 6.88. Recall that we've seen open subsets of the real line before in Def. 6.26. Open subsets of the plane

are of fundamental importance in real analysis, topology, and complex analysis.

EXAMPLE 6.89. Let $U = \{(a, b) \in \mathbb{R}^2 \mid b > 0\}$. (The set U is called the *upper half-plane*. It plays an important role in complex analysis.) Show that U is open.

PROOF. We will show that $\mathbf{x} \in U$, there exists $\epsilon > 0$ such that $B(\mathbf{x}, \epsilon) \subseteq U$.
Let $(a, b) \in U$.
We will show that $B((a, b), b) \subseteq U$.
Let $(c, d) \in B((a, b), b)$.
Then $\text{dist}((a, b), (c, d)) < b$, by definition of "open disc."
So $\sqrt{(a-c)^2 + (b-d)^2} < b$, by definition of "distance."
Note that $(a-c)^2 \geq 0$, so $(b-d)^2 \leq (a-c)^2 + (b-d)^2$.
Therefore $b - d \leq |b-d| = \sqrt{(b-d)^2} \leq \sqrt{(a-c)^2 + (b-d)^2} < b$.
So $d > 0$.
So $(c, d) \in U$, by definition of U.
Therefore $B((a, b), b) \subseteq U$, by definition of "subset."
Therefore U is open, by definition of "open." ■

Figure **??** shows a picture to illustrate this proof.

Any concept in $\mathbb{R}$ that is formulated in terms of open sets carries over to $\mathbb{R}^2$. For example:

DEFINITION 6.90. Let $X \subseteq \mathbb{R}^2$. We say X is **disconnected** if there exist disjoint nonempty open sets $U, V \subseteq \mathbb{R}^2$ such that $X \subseteq U \cup V$. We say X is **connected** if it is not disconnected.

EXAMPLE 6.91. Let $X = \{(x, 1/x) \ : \ x \in \mathbb{R}, x \neq 0\}$. (You'll recognize X as a hyperbola, more specifically the graph of the function $y = 1/x$.) Prove that X is a disconnected subset of $\mathbb{R}^2$.

PROOF. Let $U = \{(a, b) \in \mathbb{R}^2 \mid b > 0\}$ and $V = \{(a, b) \in \mathbb{R}^2 \mid b < 0\}$.
By Example 6.89 and Exercise 5, U and V are open subsets of $\mathbb{R}^2$.
Also, U and V are disjoint, because there is no ordered pair (a, b) with both $b > 0$ and $b < 0$.
We will show that $X \subseteq U \cup V$.
Let $(x, 1/x) \in X$.
Then $x > 0$ or $x < 0$, by definition of X.
So $1/x < 0$ or $1/x > 0$.

So $(x, 1/x) \in U$ or $(x, 1/x) \in V$.
So $(x, 1/x) \in U \cup V$, by definition of "union."
So $X \subseteq U \cup V$, by definition of "subset."
Therefore X is disconnected, by definition of "disconnected." ■

Note that the fact that X is disconnected matches our intuition, which says that the graph of X can be decomposed into two "pieces."

LINEAR INDEPENDENCE???

6.4. Power sets, and sets as elements

A set, as you know, is a collection of elements. One thing that causes no end of confusion to the budding math major is the fact that the elements themselves can be sets.

CAN WE MENTION THE SETS-AS-BOXES SOFTWARE?

EXAMPLE 6.92. Let $V = \{a, b, c, d\}$ and $E = \{\{a, b\}, \{a, c\}, \{b, d\}, \{c, d\}\}$. In other words, the elements of V are a, b, c, and d. The elements of E are all sets, namely the sets $\{a, b\}, \{a, c\}, \{b, d\}$, and $\{c, d\}$. For each of the following statements, is it true or false?

$a, c \in V$? True, because a and c are elements of V.

$\{a, c\} \subseteq V$? True, because every element of $\{a, c\}$ is an element of V. Specifically, $a \in V$ and $c \in V$, and a and c are the only elements we have to check, because they are the only elements of $\{a, c\}$.

$a, c \subseteq V$? False, because a is not a subset of V. (To be *really* nitpicky and technical, we should more precisely say, "Not necessarily true, because we do not know whether a is a subset of V.")

$a \in E$? False, because a is not an element of E.

$\{a, c\} \in E$? True, because $\{a, c\}$ is an element of E.

$\{a, c\} \subseteq E$? False, because not every element of of $\{a, c\}$ is an element of E. To give a specific counterexample, a is an element of $\{a, c\}$, but $a \notin E$.

$\{\{a, c\}\} \subseteq E$? True, because every element of $\{\{a, c\}\}$ is an element of E. Specifically, $\{a, c\} \in E$, and $\{a, c\}$ is the only element we have to check, because it is the only element of $\{\{a, c\}\}$.

TOO MUCH INFORMATION 6.93. Example 6.92 comes from graph theory, a diverse and active area of mathematics with oodles of real-world applications. In Figure **??**, the set V is the set of *vertices* (dots), and E is the set of *edges* (line segments).

EXAMPLE 6.94. Let $A = \{\{n, n+1\} \ : \ n \in \mathbb{Z}\}$. For each of the following statements, is it true or false?

$\{-3, -2\} \in A$? True. (Take $n = -3$.)

$-3 \in A$? False.

$\{-3, -2\} \subseteq A$? False, because $-3 \in \{-3, -2\}$, but $-3 \notin A$.

$\{-3, -1\} \in A$? False, because there does not exist $n \in \mathbb{Z}$ such that $\{-3, -1\} = \{n, n + 1\}$. (Sketch of proof: Temporarily assume there exists such an n. Then $n = -3$ or $n = -1$. In either case, we get a contradiction.)

$\{\{-3, -2\}, \{-2, -1\}\} \subseteq A$? True, because every element of $\{\{-3, -2\}, \{-2, -1\}\}$ is an element of A. Specficially, $\{-3, -2\} \in A$ and $\{-2, -1\} \in A$.

CHECK FOR UNDERSTANDING 6.95. Let $\Phi = \{2, \{2, -2\}\}$, and let $\Psi = \{\{n \in \mathbb{Z} \mid n^2 = k\} \ : \ k \in \{0, 1, 4, 9, 16\}\}$. For each of the following statements, is it true or false?

(1) $2 \in \Phi$?
(2) $\{2\} \in \Phi$?
(3) $\{2\} \subseteq \Phi$?
(4) $-2 \in \Phi$?
(5) $\{-2\} \in \Phi$?
(6) $\{-2\} \subseteq \Phi$?
(7) $2, -2 \in \Phi$?
(8) $\{2, -2\} \in \Phi$?
(9) $0 \in \Psi$?
(10) $\{0\} \in \Psi$?
(11) $\{2, -2\} \in \Psi$?
(12) $\Phi \subseteq \Psi$?
(13) $\Phi \subseteq \Psi \cup \mathbb{N}$?

EXAMPLE 6.96. Here's one that really throws students for a loop. True or false: $\{\emptyset\}$ is the empty set? The answer is false, because $\{\emptyset\}$ contains an element. Specifically, $\emptyset \in \{\emptyset\}$.

DEFINITION 6.97. Let A be a set. We define the **power set of** A, denoted $\mathcal{P}(A)$, by

$$\mathcal{P}(A) := \{B \mid B \subseteq A\}.$$

In other words, the power set of A is the collection of all subsets of A.

EXAMPLE 6.98. Let $B = \{1, 2, 3\}$. Then $\mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, B\}$.

EXAMPLE 6.99. Can the power set of a set A ever be empty? The answer is no, because $\emptyset \subseteq A$ for any set A. Hence $\emptyset \in \mathcal{P}(A)$. Hence $\mathcal{P}(A) \neq \emptyset$.

EXAMPLE 6.100. We have $\mathbb{N} \in \mathcal{P}(\mathbb{Z})$, because $\mathbb{N} \subseteq \mathbb{Z}$. However, the statement "$\mathbb{N} \subseteq \mathcal{P}(\mathbb{Z})$" is false, because there is at least one element of $\mathbb{N}$ which is not an element of $\mathcal{P}(\mathbb{Z})$. For example, $1 \in \mathbb{N}$, but $1 \notin \mathcal{P}(\mathbb{Z})$, because 1 is not a subset of the integers.

CHECK FOR UNDERSTANDING 6.101. Let $\Omega = \{\emptyset, \{\emptyset\}\}$. Find $\mathcal{P}(\Omega)$.

TOO MUCH INFORMATION 6.102. Now recall Example 6.98. Observe that B has 3 elements, and $\mathcal{P}(B)$ has 8 elements. After all, to make a subset of B, we can go through the elements of B one at a time. For each element, we have two choices: either we put it in our subset, or we don't. So in total, we have $2 \cdot 2 \cdot 2 = 8$ possible subsets of B.

In general, let A be a finite set with n elements. The same line of reasoning shows us that $\mathcal{P}(A)$ has 2^n elements.

EXAMPLE 6.103. Prove that $A = B$ iff $\mathcal{P}(A) = \mathcal{P}(B)$.

PROOF. The statement "If $A = B$, then $\mathcal{P}(A) = \mathcal{P}(B)$." follows by substituting B for A.
Now we will show that if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$.
To do so, we will first show that $A \subseteq B$.
We know $A \subseteq A$.
So $A \in \mathcal{P}(A)$, by definition of "power set."
So $A \in \mathcal{P}(B)$, because $\mathcal{P}(A) = \mathcal{P}(B)$.
So $A \subseteq B$, by definition of "power set."
The same argument, reversing the roles of A and B, shows that $B \subseteq A$.
Therefore $A = B$. ■

TOO MUCH INFORMATION 6.104. Here's an alternate proof of the fact that if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$. Let $x \in A$. Then $\{x\} \in \mathcal{P}(A)$. So $\{x\} \in \mathcal{P}(B)$. So $x \in B$. Therefore $A \subseteq B$. The same argument, reversing the roles of A and B, shows that $B \subseteq A$. Therefore $A = B$.

6.5. Families of sets

In advanced math courses, we sometimes need to take unions, intersections, or products of infinitely many sets all at once, not just finitely many. In this section, we discuss these "infinite" set operations.

Warning! Our experience has been that students have a hard time with the material in this section. So go slow, and take the time to master it.

INFORMAL DEFINITION 6.105. *When every element of a set $\mathcal{A}$ is itself a set, then we often call $\mathcal{A}$ a* family *or a* collection *of sets.*

TOO MUCH INFORMATION 6.106. We often use script letters for families of sets.

DEFINITION 6.107. Let $\mathcal{A}$ be a nonempty family of sets. We define the **union over** $\mathcal{A}$, denoted $\bigcap_{A\in\mathcal{A}} A$, by

$$\bigcap_{A\in\mathcal{A}} A := \{x \mid x \in A \text{ for some } A \in \mathcal{A}\}.$$

We define the **intersection over** $\mathcal{A}$, denoted $\bigcup_{A\in\mathcal{A}} A$, by

$$\bigcup_{A\in\mathcal{A}} A := \{x \mid x \in A \text{ for all } A \in \mathcal{A}\}.$$

Figure **??** shows Venn diagrams that illustrate the union and intersection of a family of sets.

TOO MUCH INFORMATION 6.108. When $\mathcal{A}$ is empty, the convention is that $\bigcap_{A\in\mathcal{A}} A = \emptyset$, because the statement "There exists $A \in \mathcal{A}$ such that $x \in A$." is false for all x. Also, if $\mathcal{A}$, then $\bigcup_{A\in\mathcal{A}} A$ is the universe, because the statement "For all $A \in \mathcal{A}$, $x \in A$." is vacuously true for all x.

TOO MUCH INFORMATION 6.109. Note that the ordinary union of two sets C and D is a special case of Def. 6.107. To see this, let $\mathcal{A} = \{C, D\}$. Then $C \cup D$ is the set of all x such that $x \in C$ or $x \in D$. In other words, $C \cup D$ is the set of all x such that $x \in A$ for some $A \in \mathcal{A}$. That is, $C \cup D = \bigcup_{A\in\mathcal{A}} A$.

Similarly, $C \cap D$ can be expressed as an intersection over a family of sets. We can play the same game for a union of three sets, or an intersection of five sets, or in general, any union or intersection of finitely many sets. More precisely,

$$A_1 \cup \cdots \cup A_n = \bigcup_{A\in\mathcal{A}} A$$

and

$$A_1 \cap \cdots \cap A_n = \bigcap_{A \in \mathcal{A}} A.$$

EXAMPLE 6.110. Let $\mathcal{B} = \{\{n \in \mathbb{Z} \ : \ |n| \leq k\} \ | k \in \mathbb{N}\}$. For example, the set $\{-3, -2, -1, 0, 1, 2, 3\}$ is an element of $\mathcal{B}$, corresponding to $k = 3$. Similarly, $\{-1, 0, 1\}$ is an element of $\mathcal{B}$, corresponding to $k = 1$. Then

$$\bigcup_{R \in \mathcal{B}} R = \mathbb{Z},$$

because every integer is contained in some element of $\mathcal{B}$. Also,

$$\bigcap_{R \in \mathcal{B}} R = \{-1, 0, 1\},$$

because $-1, 0$, and 1 are the only integers contained in every element of $\mathcal{B}$.

In Example 6.110, notice that every set in $\mathcal{B}$ has a corresponding number k. It happens frequently with families of sets that each of them have a "label," and it often helps to make the labels explicit. This leads us to our next definition.

DEFINITION 6.111. Let Δ be a nonempty set. Suppose that for all $\alpha \in \Delta$, there is a corresponding set A_α. The family $\{A_\alpha \mid \alpha \in \Delta\}$ is called an **indexed family of sets**. The set Δ is called the **index set**. If $\alpha \in \Delta$, then α is called the **index** of the set A_α.

THIS NEXT REMARK—LET'S MAKE IT A "PUBLIC SERVICE ANNOUNCEMENT" ENVIRONMENT.

TOO MUCH INFORMATION 6.112. The plural of *index* is *indices*, pronounced "IN-duh-SEES." We've heard "IN-duh-SEE" instead of *index*, but neither "IN-duh-SEE" nor *indice* is a word. While we're on the subject, note the similarity to *vertex* (plural: *vertices*, pronounced "VER-tuh-SEES") and *matrix* (plural: *matrices*, pronounced "MAY-truh-SEES"). Just so you know:

"MAY-truh-SEE" is not a word—that is, *matrice* is not a word.

"VER-tuh-SEE" is not a word—that is, *vertice* is not a word.

Please put a quarter in a swear jar every time you utter one of these horrendous vulgarisms. And then when it's full, please mail the swear jar to us! (For the record: Just kidding.)

EXAMPLE 6.113. Let's continue Example 6.110. For each $k \in \mathbb{N}$, let $R_k = \{n \in \mathbb{Z} \ : \ |n| \leq k\}$. So $R_3 = \{-3, -2, -1, 0, 1, 2, 3\}$, for example. The number 3 is the index for the set R_3. (The number 3 is kind of like a "label" attached to the set R_3—think of a runner in a race with the number 3 pinned to the shirt. The point is that it's convenient to have the label to refer to.) Notice that $\mathcal{B} = \{R_k \mid k \in \mathbb{N}$. So $\mathcal{B}$ is an indexed family of sets. The index set here is $\mathbb{N}$.

DEFINITION 6.114. Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be an indexed family of sets. We define

$$\bigcup_{\alpha \in \Delta} A_\alpha := \bigcup A \in \mathcal{A} A \text{ and } \bigcap_{\alpha \in \Delta} A_\alpha := \bigcap A \in \mathcal{A} A.$$

Note the very slight difference in notation between Def. 6.107 and Def. 6.114. In one, the family of sets itself goes under the union or intersection symbol, whereas the other uses the index set instead.

EXAMPLE 6.115. We have $\bigcup_{k \in \mathbb{Z}} (k, k+1) = \mathbb{R} \setminus \mathbb{Z}$, as shown in Figure **??**.

EXAMPLE 6.116. Let Ω be the set of nonnegative integers. For each $\omega \in \Omega$, let

$$A_\omega = \{\frac{x}{2^\omega} \mid x \in \mathbb{Z}\}.$$

Find $\bigcap_{\omega \in \Omega} A_\omega$ and $\bigcup_{\omega \in \Omega} A_\omega$.

A good first step is to think about what each of the individual sets A_ω looks like. We have that A_3, for example, is the of all rational numbers of the form $x/8$. Note that $3/4 \in A_3$, because $3/4 = 6/8$ and $6 \in \mathbb{Z}$. So another way to put it is that A_3 is the set of all rational numbers which in lowest terms are either integers or else have denominator 2, 4, or 8. In general, A_ω is the set of all rational numbers which in lowest terms are either integers or else have denominator $2, 4, \ldots, 2^\omega$. In particular, $A_0 = \mathbb{Z}$.

Now, $\bigcap_{\omega \in \Omega} A_\omega$ is the set of all elements which are in A_ω for *all* ω. The only elements that belong to every single set A_ω are the integers. So $\bigcap_{\omega \in \Omega} A_\omega = \mathbb{Z}$.

The set $\bigcup_{\omega \in \Omega} A_\omega$ is the set of all elements which are in A_ω for *some* ω. So any rational number of the form $x/2^y$, where x is any integer and y is any nonnegative integer, is in $\bigcup_{\omega \in \Omega} A_\omega$. So

$$\bigcup_{\omega \in \Omega} A_\omega = \{\frac{x}{2^y} \mid x \in \mathbb{Z}, y \in \Omega\}.$$

(You may be interested to know that the set $\{\frac{x}{2^y} \mid x \in \mathbb{Z}, y \in \Omega\}$ has a name—it's called the set of *dyadic rationals*.)

EXAMPLE 6.117. Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be an indexed family of sets. Let $\alpha_0 \in \Delta$. Prove that

$$A_{\alpha_0} \subseteq \bigcup_{\alpha \in \Delta} A_\alpha.$$

PROOF. Let $x \in A_{\alpha_0}$.
Then $x \in \bigcup_{\alpha\in\Delta} A_\alpha$, by definition of "union."
Therefore $A_{\alpha_0} \subseteq \bigcup_{\alpha\in\Delta} A_\alpha$, by definition of "subset." ■

CHECK FOR UNDERSTANDING 6.118. With notation as in Example 6.117, prove that $\bigcap_{\alpha\in\Delta} A_\alpha \subseteq A_{\alpha_0}$.

THEOREM 6.119 (de Morgan's laws). *Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be an indexed family of sets. Then*

(1) $\left(\bigcap_{\alpha\in\Delta} A_\alpha\right)^c = \bigcup_{\alpha\in\Delta}(A_\alpha^c)$, *and*
(2) $\left(\bigcup_{\alpha\in\Delta} A_\alpha\right)^c = \bigcap_{\alpha\in\Delta}(A_\alpha^c)$.

PROOF. (1)We have that $x \in \left(\bigcap_{\alpha\in\Delta} A_\alpha\right)^c$ iff
$x \notin \bigcap_{\alpha\in\Delta} A_\alpha$ iff
it is not true that for all $\alpha \in \Delta$, x is in A_α, which holds iff
$x \notin A_{\alpha_0}$ for some $\alpha_0 \in \Delta$ iff
$x \in A_{\alpha_0}^c$ for some $\alpha_0 \in \Delta$ iff
$x \in \bigcup_{\alpha\in\Delta}(A_\alpha^c)$.
(2) The proof is similar, so we leave it as an exercise. ■

ALSO PRODUCTS OF FAMILIES??? SEE WHAT THE OTHER BOOKS DO.

Examples from number theory

EXAMPLE 6.120. Recall the notation $\langle n\rangle = \{x \mid x \in \mathbb{Z} \text{ and } n \text{ divides } x\}$ from Example 6.59. Let S be a nonempty subset of $\mathbb{Z}$, and let $\mathcal{C} = \{\langle n\rangle \mid n \in S\}$. Then $\mathcal{C}$ is an indexed family of sets with index set S. (a) Prove that $\bigcap_{n\in S}\langle n\rangle \neq \emptyset$. (b) Prove that if $a, b \in \bigcap_{n\in S}\langle n\rangle$, then $a - b \in \bigcap_{n\in S}\langle n\rangle$.

PROOF. (a) We know that $n|0$ for all $n \in S$, by definition of "divides."
So $0 \in \langle n\rangle$ for all $n \in S$, by definition of $\langle n\rangle$.

So $0 \in \bigcap_{n\in S}\langle n\rangle$, by definition of "intersection."
So $\bigcap_{n\in S}\langle n\rangle \neq \emptyset$.
(b) Let $n \in S$.
We will show that $a - b \in \langle n\rangle$.
We know that $a, b \in \langle n\rangle$, by definition of "intersection" and the fact that $a, b \in \bigcap_{n\in S}\langle n\rangle$.
So $n|a$ and $n|b$, by definition of $\langle n\rangle$.
So $n|a - b$, by NEED A REFERENCE HERE.
So $a - b \in \langle n\rangle$, by definition of $\langle n\rangle$.
Because n was an arbitrary element of S, we have shown that $a-b \in \langle n\rangle$ for all $n \in S$.
So $a - b \in \bigcap_{n\in S}\langle n\rangle$, by definition of "intersection." ■

If you take a class on group theory, you will learn that what we just did in this example is a special case of a much more general result, that an arbitrary intersection of subgroups is a subgroup.

CHECK FOR UNDERSTANDING 6.121. Use notation as in Example 6.120. Let $\Delta = \{\beta \in \mathbb{N} \mid \beta \geq 2\}$. Find $\bigcap_{\beta\in\Delta}\langle\beta\rangle$ and $\bigcup_{\beta\in\Delta}\langle\beta\rangle$.

Examples from the real line and plane

EXAMPLE 6.122. We have $\bigcap_{k\in\mathbb{N}}(-1, 1/k) = (-1, 0]$, as in Figure ??.

CHECK FOR UNDERSTANDING 6.123. Find $\bigcap_{k\in\mathbb{N}}(0, 1/k)$.

EXAMPLE 6.124. Recall Definition 6.26. Let $\{U_\alpha \mid \alpha \in \Delta\}$ be an indexed family of sets such that for all $\alpha \in \Delta$, we have that U_α is an open subset of $\mathbb{R}$. Prove that $\bigcup_{\alpha\in\Delta} U_\alpha$ is open.

PROOF. Let $x \in \bigcup_{\alpha\in\Delta} U_\alpha$.
We will show that there exists an open interval I such that $x \in I$ and $I \subseteq \bigcup_{\alpha\in\Delta} U_\alpha$.
We know $x \in U_{\alpha_0}$ for some $\alpha_0 \in \Delta$, by definition of "union".
By definition of "open," we know there exists open interval I such that $x \in I$ and $I \subseteq U_{\alpha_0}$.
By Example 6.117, it follows that $I \subseteq \bigcup_{\alpha\in\Delta} U_\alpha$.
Therefore $\bigcup_{\alpha\in\Delta} U_\alpha$, by definition of "open." ■

EXAMPLE 6.125. Recall Definition 6.87. Let $\{U_\alpha \mid \alpha \in \Delta\}$ be an indexed family of sets such that for all $\alpha \in \Delta$, we have that U_α is an open subset of $\mathbb{R}^2$. Prove that $\bigcup_{\alpha\in\Delta} U_\alpha$ is open.

PROOF. The proof is identical to the proof in Example 6.124, once you replace the word "interval" with the word "disc." ■

TOO MUCH INFORMATION 6.126. If you take a Topology class, you will learn that this property—the fact that an arbitrary union of open sets is open—is one of the defining properties of "openness."

TOO MUCH INFORMATION 6.127. After Examples 6.124 and 6.125, you might wonder about intersections of open sets. It turns out that an intersection of finitely many open sets in $\mathbb{R}$ or $\mathbb{R}^2$ is open. An intersection of infinitely many open sets is not necessarily open, as Example 6.123 shows. For each of the sets $(-1, 1/k)$ is open in $\mathbb{R}$, but the intersection is $(-1, 0]$, which is not open in $\mathbb{R}$.

ANSWERS TO CHECKs FOR UNDERSTANDING

- 6.7(1) Only $\Theta \subseteq \Upsilon$ and $\Phi \subseteq \Upsilon$.
- 6.7(2) Only $\mathbb{N} \subseteq \mathbb{Z}$.
- 6.7(3) No, because there are negative real numbers that are not rational. (For example, $-\sqrt{2}$.)
- 6.7(4) Yes, it applies, and we conclude that $x \in H$.
- 6.7(5) No, it does not apply.
- 6.7(6) We would also need to know that $\Delta \subseteq \Gamma$.
- 6.34(1) We have $\{3\} = A \cap B$ and $\{1, 2, 3, 4, 5\} = A \cup B$.
- 6.34(2) We get $\{-3, -2, -1, 0, 1, 2, 3, 4, 5\}$
- 6.34(3) We can conclude that a is either in both X and Y, or in Z.
- 6.61 We have $(a, b)^c = (-\infty, a] \cup [b, \infty)$.
- 6.51 We get $A^c \cap B^c$.
- 6.73 PICTURE. $(-1, -3), (-1, 0), (-1, 4), (2, -3), (2, 1)$ are five elements of this set.
  6.77 PICTURE. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
- 6.86 $B(\mathbf{x}, r)$ must be a subset of $B(\mathbf{x}, s)$.

  PROOF. Let $\mathbf{y} \in B(\mathbf{x}, r)$.
  Then $\text{dist}(\mathbf{x}, \mathbf{y}) < r$, by definition of "open disc."
  So $\text{dist}(\mathbf{x}, \mathbf{y}) < s$, because $r < s$.
  So $\mathbf{y} \in B(\mathbf{x}, s)$, by definition of "open disc."
  Therefore $B(\mathbf{x}, r) \subseteq B(\mathbf{x}, s)$, by definition of "subset." ■

- 6.118

  PROOF. Let $x \in \bigcap_{\alpha\in\Delta} A_\alpha$.
  Then $x \in A_{\alpha_0}$, by definition of "intersection."
  So $\bigcap_{\alpha\in\Delta} A_\alpha \subseteq A_{\alpha_0}$, by definition of "subset." ■

- 6.121 We have $\bigcap_{\beta\in\Delta}\langle\beta\rangle = \{0\}$ and $\bigcup_{\beta\in\Delta}\langle\beta\rangle = \mathbb{Z} \setminus \{1, -1\}$.

6.6. Exercises

THEOREMS IN EGGEN LIKE $A \subseteq A$, etc.

(1) Fill in the blank to make a true statement: "Let $a, b, c, d \in \mathbb{R}$. Then $(c, d) \subseteq [a, b]$ iff ____." Then prove that your statement is correct. (See Example 6.25 to get an idea of how you might fill in the blank.)
(2) Fill in the blank in Check for Understanding 6.77 to make a true statement, and then prove that your answer is correct.
(3) Let A be an open ray. Prove that A is an open subset of $\mathbb{R}$.
(4) Prove that $\mathbb{Q}$ is a disconnected subset of $\mathbb{R}$.
(5) Let $L = \{(a, b) \in \mathbb{R}^2 \mid b < 0\}$. (The set L is called the *lower half-plane.*) Show that L is open.

In the next few exercises, recall the notation $\langle n\rangle = \{x \mid x \in \mathbb{Z} \text{ and } n \text{ divides } x\}$ from Example 6.59, let $S \subseteq \mathbb{Z}$, and let $\mathcal{C} = \{\langle n\rangle \mid n \in S\}$.

(6) Prove that if $a \in \bigcap_{n\in S}\langle n\rangle$ and $r \in \mathbb{Z}$, then $ra \in \bigcap_{n\in S}\langle n\rangle$.
(7) Suppose $a, b, c, d \in \mathbb{R}$ with $a \le c < d \le b$. Prove that $(a, b) \cap (c, d) = (c, d)$.
(8) Suppose $a, b, c, d \in \mathbb{R}$ with $a < b$ and $a \le c \le b < d$. Prove that $(a, b) \cap (c, d) = (c, b)$.
(9) Let $A = \{1, 5, -12, 100, 1/3, \pi\}$, $B = \{5, 1, -12, 18, -1/3\}$, $C = \{10, -1, 0\}$, $D = \{1, 2\}$, and $E = \{1, -1\}$. Calculate the following:
   (a) $A \cup B$
   (b) $A \cap B$
   (c) $A \cap C$
   (d) $A \cap \emptyset$
   (e) $B \cup \emptyset$
   (f) $D \times E$
   (g) $(D \cap A) \times (E \cup D)$
   (h) $C \times D$
   (i) $A - B$
   (j) $C - A$
   (k) $A - \emptyset$

(10) Let $A = \{2k \mid k \in \mathbb{Z}\}$ and $B = \{3n \mid n \in \mathbb{Z}\}$. Prove that $A \cap B = \{6m \mid m \in \mathbb{Z}\}$.

(11) Let A, B, and C be sets. Prove that if $A \subseteq B$, then $A - C \subseteq B - C$.

(12) Let A and B be sets. Prove that $A \subseteq B$ if and only if $A - B = \emptyset$.

(13) Let A, B, and C be sets. Prove that if $A \subseteq B$, then $A \cup C \subseteq B \cup C$.

(14) Let A, B, and C be sets. Prove that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(15) Let A, B, and C be sets. Prove or disprove: If $A \cap B \neq \emptyset$ and $B \cap C \neq \emptyset$, then $A \cap C \neq \emptyset$.

(16) Let n be an integer with $n \geq 2$. Prove that

$$\{x \in \mathbb{Z} \mid x \equiv a (\mathrm{mod}\, n)\} = \{a + qn \mid q \in \mathbb{Z}\}.$$

(17) Suppose that a, b and n are integers with $n \geq 2$. Suppose that $a \not\equiv b (\mathrm{mod}\, n)$. Let

$$A = \{x \in \mathbb{Z} \mid x \equiv a (\mathrm{mod}\, n)\} \text{ and } B = \{x \in \mathbb{Z} \mid x \equiv b (\mathrm{mod}\, n)\}.$$

Prove that $A \cap B = \emptyset$.

(18) Suppose that a, b and n are integers with $n \geq 2$. Suppose that $a \equiv b (\mathrm{mod}\, n)$. Let

$$A = \{x \in \mathbb{Z} \mid x \equiv a (\mathrm{mod}\, n)\} \text{ and } B = \{x \in \mathbb{Z} \mid x \equiv b (\mathrm{mod}\, n)\}.$$

Prove that $A = B$.

(19) Let n be an integer with $n \geq 2$. Let

$$A = \{x \in \mathbb{Z} \mid x \equiv 0 (\mathrm{mod}\, 3)\} \text{ and } B = \{x \in \mathbb{Z} \mid x \equiv 0 (\mathrm{mod}\, 6)\}.$$

Prove that $B \subseteq A$. In general the following is true: If $n|m$, then

$$\{x \in \mathbb{Z} \mid x \equiv 0 (\mathrm{mod}\, m)\} \subseteq \{x \in \mathbb{Z} \mid x \equiv 0 (\mathrm{mod}\, n)\}.$$

Can you prove it?

(20) Define the set P_n to be the set of primes between 1 and n. In mathematical notation, we have that

$$P_n = \{m \in \mathbb{Z} \mid 1 < m \leq n \text{ and } m \text{ is prime.}\}.$$

For example, $P_4 = \{2, 3\}$ and $P_{13} = \{2, 3, 5, 7, 11, 13\}$. Write out the elements of P_5, P_6, P_{16} and P_{21}. Then describe the elements in the sets

$$\bigcup_{n=2}^{\infty} P_n \text{ and } \bigcap_{n=2}^{\infty} P_n.$$

(21) Let $A_n = \{x \in \mathbb{Z} \mid -n \leq x \leq n\}$. List the elements in the sets A_1, A_2, A_3, and A_4. Then calculate the following sets $\bigcap_{i=2}^{\infty} A_n$ and $\bigcup_{i=5}^{\infty} A_n$.

(22) Calculate the following intersections and unions.
   (a) Calculate $\bigcup_{n=1}^{\infty} A_n$ and $\bigcap_{n=1}^{\infty} A_n$ where $A_n = (-n, n)$.
   (b) Calculate $\bigcup_{n=2}^{\infty} A_n$ and $\bigcap_{n=2}^{\infty} A_n$ where $A_n = (1/n, 1)$.
   (c) Calculate $\bigcup_{n=1}^{\infty} A_n$ and $\bigcap_{n=1}^{\infty} A_n$ where $A_n = (2+1/n, n)$.

(23) Let A, B, and C be sets. Prove that $A \cap (B \cap C) = (A \cap B) \cap C$.

(24) Let A, B, and C be sets. Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(25) Let $A = \{1, x, 5\}$. List the elements of the power set $\mathcal{P}(A)$.

(26) Let A and B be sets.
   (a) Prove that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
   (b) Prove that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
   (c) Give an example where $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

(27) Let A and B be sets. Prove that $A \setminus B$ and B are disjoint.

(28) Let A, B, C, and D be sets. Prove that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

OPEN DISCS ARE CONVEX—CONVEXITY IMPORTANT IN OPTIMIZATION

Challenge question: Is the converse of the statement in Exercise 6.75 true? Either prove that it is true, or else find a counterexample. WARNING: This is a trick question. Be careful of a trap we have set for you.

6.7. Fun math facts

History and significance of Descartes' coming up with the plane
Pick's theorem?
Gauss' circle problem?
Interior, exterior, boundary, Jordan Curve Theorem

Chapter 7

Relations

7.1. Relations

Consider the set of integers $\mathbb{Z}$. Given two integers a and b we can compare (or relate) them using the less-than relation $<$. For example, we can write $2 < 5$. Or we can write $7 \not< 2$. In this section, we give a general definition for a relation on a set. We first construct relations using Cartesian products. However, mathematicians usually define relations without constructing them from Cartesian products. Hence we will quickly stop constructing them that way.

Definition 7.1. A **relation** $\sim$ on a set S is a subset of $S \times S$. If (x, y) is an element of $\sim$ then we say that x **is related to** y and write $x \sim y$. If (x, y) is not an element of $\sim$ then we write $x \not\sim y$.

Example 7.2. Let $S = \{-15, 2, 0\}$. Let

$$\sim \; = \; \{(0, 0), (-15, 2), (0, 2)\}.$$

We say that $0 \sim 0$, $-15 \sim 2$, and $0 \sim 2$. However, $-15 \not\sim 0$ because $(-15, 0)$ is not in $\sim$. Also notice that $2 \not\sim -15$ because $(2, -15)$ is not in $\sim$. Order matters in a relation.

Example 7.3. Here we give the more common way of defining a relation; that is, without listing a set of ordered pairs. Consider the set of integers $\mathbb{Z}$. Consider the relation $\sim$ on $\mathbb{Z}$ where $a \sim b$ iff $a < b$. In this case we have $3 \sim 10$ because $3 < 10$. We have that $42 \not\sim 7$ because $42 \not< 7$. To conform with Definition 7.1 we can think of $\sim$ as

the following set

$$\begin{aligned} \sim &= \{\ldots,(-1,0),(-1,1),(-1,2),(-1,3),(-1,4),\ldots \\ &= \{\ldots,(0,1),(0,2),(0,3),(0,4),(0,5),\ldots \\ &= \{\ldots,(1,2),(1,3),(1,4),(1,5),(1,6),\ldots\} \end{aligned}$$

We put "..." because there are infinitely many more ordered pairs in $\sim$ that we didn't give in the above list.

CHECK FOR UNDERSTANDING 7.4. (1) Let $S = \{5, \pi, 3, 10\}$ and

$$\sim = \{(5,3),(3,5),(\pi,10),(3,3)\}.$$

Is $5 \sim 3$? Is $10 \sim \pi$? Is $5 \not\sim 5$?

(2) Consider the relation $\sim$ on $\mathbb{R}$ where $x \sim y$ iff $y - x \in \mathbb{Z}$.
   (a) Is $5.13 \sim 17.13$? Is $5 \sim 100$? Is $\pi \sim 3.14$?
   (b) Find all x such that $x \sim 5$.
   (c) If $x \sim y$ is true, is $y \sim x$ necessarily true?

7.2. Equivalence Relations

DEFINITION 7.5. Let S be a set and $\sim$ be a relation on S. We say that $\sim$ is an **equivalence relation** on S if the following are true:

- (Reflexive) For every $x \in S$ we have that $x \sim x$.
- (Symmetric) For every $x, y \in S$, if $x \sim y$, then $y \sim x$.
- (Transitive) For every $x, y, z \in S$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

EXAMPLE 7.6. Let $S = \{-15, 2, 0\}$. Define the relation

$$\sim = \{(0,0),(0,2),(2,0),(-15,2)\}.$$

Notice that $\sim$ is not reflexive because $-15 \not\sim -15$ and $2 \not\sim 2$.

Notice that $\sim$ is not symmetric because $-15 \sim 2$ but $2 \not\sim -15$. If $(2,-15)$ was an element of $\sim$ then $\sim$ would be symmetric.

Checking transitivity must be done by brute force. That is, one must find all combinations where $x \sim y$ and $y \sim z$ and check to make sure that $x \sim z$. Let's check them all:

(1) We have that $0 \sim 0$ and $0 \sim 2$. And $0 \sim 2$.
(2) We have that $0 \sim 2$ and $2 \sim 0$. And $0 \sim 0$.
(3) We have that $2 \sim 0$ and $0 \sim 0$. And $0 \sim 2$.
(4) We have that $-15 \sim 2$ and $2 \sim 0$, but $-15 \not\sim 0$.

By (4) we see that $\sim$ is not transitive.

EXAMPLE 7.7. Let $A = \{1, 2, 3\}$. Define the relation

$$\sim \; = \; \{(1,1), (2,2), (3,3), (1,3), (3,1)\}$$

on A.

We see that $\sim$ is reflexive because $1 \sim 1$, $2 \sim 2$, and $3 \sim 3$.

Scanning through $\sim$ we see that $\sim$ is symmetric because for every $x \sim y$ we have that $y \sim x$. As an example, notice that $1 \sim 3$. Therefore we need $3 \sim 1$, which is true.

We now check transitivity by brute force.

(1) We have that $1 \sim 1$ and $1 \sim 1$. And $1 \sim 1$.
(2) We have that $1 \sim 1$ and $1 \sim 3$. And $1 \sim 3$.
(3) We have that $3 \sim 3$ and $3 \sim 1$. And $3 \sim 1$.
(4) We have that $1 \sim 3$ and $3 \sim 3$. And $1 \sim 3$.
(5) We have that $1 \sim 3$ and $3 \sim 1$. And $1 \sim 1$.
(6) We have that $3 \sim 1$ and $1 \sim 1$. And $3 \sim 1$.
(7) We have that $3 \sim 1$ and $1 \sim 3$. And $3 \sim 3$.

We see that every combination works; that is, whenever we have $x \sim y$ and $y \sim z$, we also have $x \sim z$. So $\sim$ is transitive.

We have shown that $\sim$ is an equivalence relation on A.

EXAMPLE 7.8. Consider the less-than relation $<$ on the set of integers $\mathbb{Z}$. Note that $<$ is not reflexive, because for example, $3 \not< 3$. Also, $<$ is not symmetric because $1 < 2$ but $2 \not< 1$. However, $<$ is transitive: Let $x, y, z \in \mathbb{Z}$. If $x < y$ and $y < z$, then $x < z$.

CHECK FOR UNDERSTANDING 7.9. (1) Let $S = \{1, 2, 3\}$ and

$$\sim = \{(1,1), (1,2), (2,3), (3,2), (2,1)\}.$$

(a) Is $\sim$ reflexive?
(b) Is $\sim$ symmetric?
(c) Is $\sim$ transitive?

(2) Let $\sim$ be the relation on $\mathbb{R}$ where $x \sim y$ iff $y - x \in \mathbb{Z}$, as in Check for understanding 7.4. Prove that $\sim$ is reflexive, symmetric, and transitive.

DEFINITION 7.10. Let $\sim$ be an equivalence relation on a set S. Let $x \in S$. The **equivalence class** of x is defined to be

$$\overline{x} = \{y \in S \mid x \sim y\}.$$

That is, $\overline{x}$ consists of all the elements y from S that are related to x.

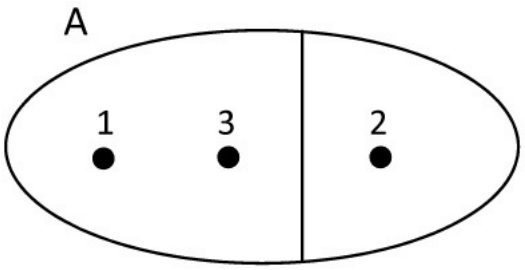


FIGURE 1. A picture showing how A is broken up into equivalence classes

EXAMPLE 7.11. Let $A = \{1, 2, 3\}$. Define the relation

$$\sim \; = \; \{(1,1), (2,2), (3,3), (1,3), (3,1)\}$$

on A. We saw in Example 7.7 that $\sim$ is an equivalence relation on S. Note that $1 \sim 1$ and $1 \sim 3$. Therefore,

$$\overline{1} = \{y \in A \mid 1 \sim y\} = \{1, 3\}.$$

Note that $2 \sim 2$. Thus

$$\overline{2} = \{y \in A \mid 2 \sim y\} = \{2\}.$$

Note that $3 \sim 3$ and $3 \sim 1$. Hence

$$\overline{3} = \{y \in A \mid 3 \sim y\} = \{1, 3\}.$$

Therefore $\sim$ gives rise to two distinct equivalence classes:

$$\begin{aligned} \overline{1} &= \{1, 3\} = \overline{3} \\ \overline{2} &= \{2\} \end{aligned}$$

See Figure 1 for a picture showing how A is broken up into equivalence classes. Notice that either two equivalence classes are equal, for example $\overline{1} = \overline{3}$, or they do not intersect at all, for example $\overline{1} \cap \overline{2} = \emptyset$. Proposition 7.15 will show that this is always the case.

DEFINITION 7.12. Let S be a set and $\sim$ be an equivalence relation on S. We denote the set of equivalence classes of S as $S/\sim$.

EXAMPLE 7.13. Let A and $\sim$ be as in Example 7.11. We saw that $A/\sim = \{\overline{1}, \overline{2}\}$.

CHECK FOR UNDERSTANDING 7.14. (1) Let $\sim$ be the relation on $\mathbb{R}$ where $x \sim y$ iff $y - x \in \mathbb{Z}$, as in Check for understanding 7.4 and 7.9. Recall that $\sim$ is an equivalence relation.
(a) Describe the elements of the set $\overline{0}$.
(b) Prove that if $a \in \mathbb{Z}$ then $\overline{a} = \overline{0}$.
(c) Let $x \in \mathbb{R}$. Describe the elements of $\overline{x}$. Draw a picture of the real line and label several points in $\overline{x}$.

PROPOSITION 7.15. *Let $\sim$ be an equivalence relation on a set S. Let $x, y \in S$. Then*
(1) $x \in \overline{x}$.
(2) $\overline{x} = \overline{y}$ *if and only if* $x \in \overline{y}$.
(3) $\overline{x} = \overline{y}$ *if and only if* $x \sim y$.
(4) $\overline{x} \cap \overline{y} = \emptyset$ *if and only if* $x \not\sim y$.

PROOF. Let $x, y \in S$.

(1) We have that $x \sim x$ since $\sim$ is an equivalence relation and therefore reflexive.
Therefore $x \in \overline{x}$ by the definition of $\overline{x}$.

(2). Suppose that $\overline{x} = \overline{y}$.
We know that $x \in \overline{x}$ by part (1) of this proposition.
Therefore $x \in \overline{y}$ since $\overline{x} = \overline{y}$.

Conversely suppose that $x \in \overline{y}$.
Therefore $y \sim x$ by the definition of $\overline{y}$.
Let $z \in \overline{x}$. Then $x \sim z$ by the definition of $\overline{x}$.
Since $y \sim x$ and $x \sim z$ we have that $y \sim z$ by the transitivity of $\sim$.
Hence $\overline{x} \subseteq \overline{y}$.
Let $w \in \overline{y}$. Then $y \sim w$ by the definition of $\overline{y}$.
Note that $x \sim y$ because $y \sim x$ and $\sim$ is symmetric.
Since $x \sim y$ and $y \sim w$ we have that $x \sim w$ by the transitivity of $\sim$.
Thus $x \in \overline{w}$ by the definition of $\overline{w}$.
Hence $\overline{y} \subseteq \overline{x}$.
Therefore $\overline{x} = \overline{y}$.

(3) Suppose that $\overline{x} = \overline{y}$.
Hence $x \in \overline{y}$ by part (2) of this proposition.
Thus $y \sim x$ by the definition of $\overline{y}$.
Therefore $x \sim y$ since $\sim$ is symmetric.

Conversely suppose that $x \sim y$.
Thus $y \sim x$ since $\sim$ is symmetric.
Hence $x \in \overline{y}$ by the definition of $\overline{y}$.
Hence $\overline{x} = \overline{y}$ by part (2) of this proposition.

(4). Suppose that $\overline{x} \cap \overline{y} = \emptyset$.
Note that $\overline{x} \neq \emptyset$ by part (1) of this proposition.
We have that $\overline{x} \neq \overline{y}$ since $\overline{x} \cap \overline{y} = \emptyset$.
Thus $x \not\sim y$ by part (3) of this proposition.

$\langle$*For the converse direction of part (4) we need to prove that if* $x \not\sim y$, *then* $\overline{x} \cap \overline{y} = \emptyset$. *Instead we prove the contrapositive which says that if* $\overline{x} \cap \overline{y} \neq \emptyset$ *then* $x \sim y$.$\rangle$
Assume that $\overline{x} \cap \overline{y} \neq \emptyset$.
Then there exists some $z \in S$ with $z \in \overline{x} \cap \overline{y}$.
Hence $x \sim z$ and $y \sim z$ since $z \in \overline{x}$ and $z \in \overline{y}$.
Thus $z \sim y$ since $\sim$ is symmetric.
Therefore $x \sim y$ because $x \sim z$ and $z \sim y$ and $\sim$ is transitive. ■

7.3. Integers modulo n

Recall the definition of congruence (Definition ??????).

EXAMPLE 7.16. Let n be an integer with $n \geq 2$. Then congruence modulo n is an equivalence relation.

PROOF. We begin by showing that congruence modulo n is reflexive.
Let $x \in \mathbb{Z}$.
Notice that $x - x = 0 = n \cdot 0$.
Therefore $x \equiv x (\text{mod } n)$ because n divides $x - x$.
Hence congruence modulo n is reflexive because $x \equiv x (\text{mod } n)$ for every $x \in \mathbb{Z}$.

We now show that congruence modulo n is symmetric.
Let $x, y \in \mathbb{Z}$. Suppose that $x \equiv y (\text{mod } n)$.
Then $x - y = nk$ for some integer k.
Thus $y - x = n(-k)$.
Therefore $y \equiv x (\text{mod } n)$ because n divides $y - x$.
Hence congruence modulo n is symmetric because $x \equiv y (\text{mod } n)$ implies that $y \equiv x (\text{mod } n)$ for every $x, y \in \mathbb{Z}$.

We finish by showing that congruence modulo n is transitive.
Let $x, y, z \in \mathbb{Z}$. Suppose that $x \equiv y (\text{mod } n)$ and $y \equiv z (\text{mod } n)$.
Then $nk = x - y$ and $nm = y - z$ for some integers k and m.
Therefore $x - z = x - y + y - z = nk + nm = n(k + m)$.
Hence $x \equiv z (\text{mod } n)$ because n divides $x - z$.
Thus congruence modulo n is transitive because $x \equiv y (\text{mod } n)$ and $y \equiv x (\text{mod } n)$ implies that $x \equiv z (\text{mod } n)$ for every $x, y, z \in \mathbb{Z}$. ■

EXAMPLE 7.17. Let $n = 3$. In this example we compute the equivalence classes for congruence modulo 3 on the integers. See Figure 2 for a picture illustrating the following computations. Consider the integer 0. Then

$$\overline{0} = \{x \in \mathbb{Z} \mid x \equiv 0 (\text{mod } 3)\}.$$

That is, $x \in \overline{0}$ iff 3 divides x. Therefore,

$$\overline{0} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}.$$

By Proposition 7.15 part (2) we see that

$$\cdots = \overline{-12} = \overline{-9} = \overline{-6} = \overline{-3} = \overline{0} = \overline{3} = \overline{6} = \overline{9} = \overline{12} = \cdots$$

Therefore, there is no need to calculate the equivalence classes of the above integers because they are all equal. Another way to see that $\overline{6} = \overline{0}$ is to note that $6 \equiv 0 (\text{mod } 3)$ and use Proposition 7.15 part (3).

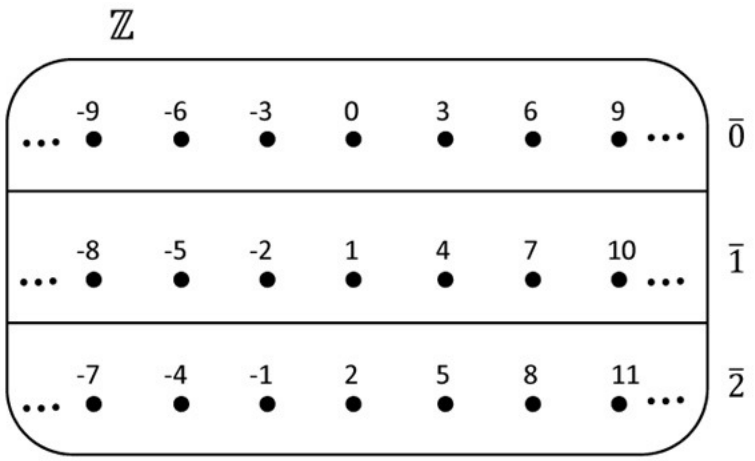


FIGURE 2. A picture showing how $\mathbb{Z}$ is broken up into equivalence classes modulo 3

Looking above we see that there are many integers whose equivalence class we have not yet computed; for example, we have not computed $\overline{1}$. We see that

$$\overline{1} = \{x \in \mathbb{Z} \mid x \equiv 1 (\text{mod } 3)\}.$$

That is, $x \in \overline{1}$ iff 3 divides $x - 1$. Or equivalently, $x \in \overline{1}$ iff $x = 1 + 3k$ for some integer k. To list out elements of $\overline{1}$ one starts at 1 and adds or subtracts multiples of 3 (as k can be positive or negative). That is,

$$\overline{1} = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}.$$

Again, by Proposition 7.15 part (2) we see that

$$\cdots = \overline{-11} = \overline{-8} = \overline{-5} = \overline{-2} = \overline{1} = \overline{4} = \overline{7} = \overline{10} = \overline{13} = \cdots$$

Again, we could have used Proposition 7.15 part (3) to show that $\overline{10} = \overline{1}$ because $10 \equiv 1 (\text{mod } 3)$.

We have still not computed all the equivalence classes modulo 3. For example, we have not computed $\overline{2}$. We see that

$$\overline{2} = \{x \in \mathbb{Z} \mid x \equiv 2 (\text{mod } 3)\}.$$

That is, $x \in \overline{2}$ iff 3 divides $x - 2$. Or equivalently, $x \in \overline{2}$ iff $x = 2 + 3k$ for some integer k. As above, to list out elements of $\overline{2}$ one starts at 2 and adds or subtracts multiples of 3. That is,

$$\overline{2} = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}.$$

Again, by Proposition 7.15 part (2) we see that

$$\cdots = \overline{-10} = \overline{-7} = \overline{-4} = \overline{-1} = \overline{2} = \overline{5} = \overline{8} = \overline{11} = \overline{14} = \cdots$$

We claim that we have computed all of the distinct equivalence classes modulo 3. They are $\overline{0}$, $\overline{1}$, and $\overline{2}$. Any other equivalence class is equal to one of these. We make this precise in Proposition 7.21.

Before we leave this example we want to impress upon the reader the importance of Proposition 7.15 part (3). For example, is $\overline{136} = \overline{1}$? Yes, because $136 \equiv 1 (\text{mod } 3$ since $136 - 1 = 135 = 3 \cdot 45$ is divisible by 3. However, $\overline{-15} \neq \overline{13}$. This is because $-15 \not\equiv 13 (\text{mod } 3$ since $-15 - 13 = -28$ is not divisible by 3.

CHECK FOR UNDERSTANDING 7.18. (1) Let $n = 6$. In this problem we consider the relation on $\mathbb{Z}$ given by $x \sim y$ iff $x \equiv y (\text{mod } 6)$.

(a) List 10 elements in $\overline{2}$.
(b) List 10 elements in $\overline{5}$.
(c) Is $\overline{0} = \overline{6}$?
(d) Is $\overline{1} = \overline{-2}$?
(e) Is $\overline{2} = \overline{3}$?
(f) Is $\overline{-10} = \overline{5}$?
(g) Is $\overline{3} = \overline{21}$?

DEFINITION 7.19. Let n be an integer with $n \geq 2$. We define $\mathbb{Z}_n$ to be the set of equivalence classes modulo n.

EXAMPLE 7.20. In Example 7.17 we showed that $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

PROPOSITION 7.21. *Let n be an integer with $n \geq 2$. Then*

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

Furthermore, the above elements of $\mathbb{Z}_n$ are distinct. That is, if $0 \leq x \leq y \leq n-1$ and $\overline{x} = \overline{y}$, then $x = y$.

PROOF. Let $S = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.
⟨*The proof strategy is as follows. Given an integer x we begin by showing that $\overline{x}$ lies in the set S. This shows that every equivalence class lives in S. We then show that each element of S is distinct.*⟩
Let $x \in \mathbb{Z}$.
By the division algorithm (Theorem 4.57) there exist integers q and r with $x = nq + r$ and $0 \leq r < n$.
Hence n divides $x - r$ and so $x \equiv r(\text{mod n})$.
Therefore $\overline{x} = \overline{r}$ by the definition of equivalence class.
Hence $\overline{x} \in S$ because $0 \leq r < n$.
⟨*We now show that the elements of S are distinct.*⟩
Suppose that $0 \leq x \leq y \leq n-1$ and $\overline{x} = \overline{y}$.
Therefore, $0 \leq y - x < n$.
Notice that $y \equiv x(\text{mod } n)$ since $\overline{x} = \overline{y}$.
This implies that $nk = y - x$ for some positive integer k.
We must have that $k = 0$ because $0 \leq y - x < n$.
Therefore $x = y$.
Hence the elements of $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ are distinct. ■

7.4. Well-defined operations

Recall that the set of rational numbers $\mathbb{Q}$ consists of all fractions of the form a/b where a and b are integers and $b \neq 0$. Suppose that we define the following operation on the rational numbers

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}.$$

Here we have used the symbol $\oplus$ for our new operation so as not to confuse it with the usual $+$ operation on fractions. As an example computation we have that $1/2 \oplus 5/3 = (1+5)/(2+3) = 6/5$. Fantastic! We have a new operation on the rational numbers that we can study. No, it isn't fantastic. The operation $\oplus$ is nonsense. Why? Notice the following: The fraction $1/2$ equals the fraction $2/4$. The fraction $5/3$ equals the fraction $15/9$. If the operation $\oplus$ makes sense then we should have that $1/2 \oplus 5/3 = 2/4 \oplus 15/9$. However, $2/4 \oplus 15/9 =$

$(2+15)/(4+9) = 17/13$. And we saw above that $1/2 \oplus 5/3 = 6/5$. And $17/13 \neq 6/5$. In mathematics, we say that $\oplus$ is not well-defined. Let us now show that the usual operation of addition of fractions is well-defined.

HOW TO 7.22. **Show that an operation is well-defined.**

Let S be a set. Suppose you want to define an operation $\oplus$ on S. To show that $\oplus$ is well-defined one must check the following.

Step 1. For every $x, y \in S$, we have that $x \oplus y \in S$. This is called "showing that S is **closed** under $\oplus$."

Step 2. If some or all of the elements of S can be expressed in more than one way, then one must also show the following: For every $a, b, c, d \in S$, if $a = b$ and $c = d$, then $a \oplus c = b \oplus d$.

EXAMPLE 7.23. Consider the set of rational numbers $\mathbb{Q}$. Define the addition operation $+$ on $\mathbb{Q}$ as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

Then $+$ is well-defined on $\mathbb{Q}$.

PROOF. ⟨*We follow the steps given in How To 7.22. We begin with step one.*⟩
Suppose that a/b and c/d are rational numbers where a, b, c, d are integers with $b \neq 0$ and $d \neq 0$.
By the properties of the integers, $ad + bc$ and bd are integers.
Furthermore, $bd \neq 0$ since $b \neq 0$ and $d \neq 0$.
Hence $a/b + c/d = (ad + bc)/bd$ is a rational number.
⟨*We now complete step two of How To 7.22.*⟩
Suppose that a, b, s, t, c, d, x, y are integers with b, t, d, y not zero and $a/b = s/t$ and $c/d = x/y$.
We have that $a/b + c/d = (ad + cb)/bd$ and $s/t + x/y = (sy + xt)/ty$ by definition of $+$.
Since $a/b = s/t$ we have that $at = sb$.
Since $c/d = x/y$ we have that $cy = xd$.
Note that

$$\begin{aligned}(ad+cb)(ty) - (sy+xt)(bd) &= adty + cbty - sybd - xtbd \\ &= sbdy + xdbt - sybd - xtbd \\ &= 0\end{aligned}$$

because $at = sb$ and $cy = xd$.
Therefore, $(ad + cb)(ty) = (sy + xt)(bd)$.
Hence $a/b + c/d = s/t + x/y$. ■

We now define an addition and multiplication operation on $\mathbb{Z}_n$. This is done in Definition 7.24. We then compute some examples using $\mathbb{Z}_5$ in Example 7.25. In Proposition 7.27 we prove that the operations defined in Definition 7.24 are well-defined.

DEFINITION 7.24. Let n be an integer with $n \geq 2$. Given $\overline{a}, \overline{b} \in \mathbb{Z}_n$ define

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} \cdot \overline{b} &= \overline{ab}. \end{aligned}$$

EXAMPLE 7.25. Let $n = 5$. Then $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Suppose that we define addition and multiplication as in Definition 7.24. For example, we would have that

$$\begin{aligned} \overline{1} + \overline{3} &= \overline{1+3} = \overline{4}, \\ \overline{4} + \overline{3} &= \overline{4+3} = \overline{7} = \overline{2}, \\ \overline{4} \cdot \overline{3} &= \overline{12} = \overline{2}, \\ \text{and} & \\ \overline{2} \cdot \overline{4} &= \overline{8} = \overline{3}. \end{aligned}$$

Are these two operations well-defined on $\mathbb{Z}_5$? According to How To 7.22 we must do two steps. We will not do this thouroughly right now, instead we compute a few examples to illustrate what would need to be done. The "real proof" comes in Proposition 7.27.

The first step of How To 7.22 is to check that $\mathbb{Z}_5$ is closed under the addition and multiplication defined in Definition 7.24. For example, $\overline{2} + \overline{5} = \overline{7} = \overline{2} \in \mathbb{Z}_5$. That is, when we take two elements from $\mathbb{Z}_5$, in this case $\overline{2}$ and $\overline{5}$, and we add them together we should get another element in $\mathbb{Z}_5$. In this case we do, it is the element $\overline{2}$. This always happens, as we will see in Proposition 7.27. The same idea must be verified for multiplication: That is, if $\overline{x}, \overline{y} \in \mathbb{Z}_5$, then $\overline{x} \cdot \overline{y}$ is in $\mathbb{Z}_5$.

The second step of How To 7.22 is different. Each element of $\mathbb{Z}_5$ can be expressed in an infinite number of ways. For example, the element $\overline{3}$ can also be expressed as $\overline{8}$ because $\overline{3} = \overline{8}$. The element $\overline{1}$ can also be expressed as $\overline{11}$ since $\overline{1} = \overline{11}$. In order to check step two of How To 7.22 we must make sure for example that $\overline{3} + \overline{1} = \overline{8} + \overline{11}$. We must make sure that this is true because we know that $\overline{3} = \overline{8}$ and $\overline{1} = \overline{11}$.

Let's check it. Note that $\overline{3}+\overline{1}=\overline{4}$ and $\overline{8}+\overline{11}=\overline{19}=\overline{4}$. In this case they are equal. The same idea must be checked for multiplication. We do all of this in general in Proposition 7.27.

CHECK FOR UNDERSTANDING 7.26. In $\mathbb{Z}_5=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$ calculate the following. As in Example 7.25, reduce your answer $\overline{x}$ so that $0\leq x\leq 4$.

(1) $\overline{4}+\overline{4}$
(2) $\overline{4}\cdot\overline{4}$
(3) $\overline{2}+\overline{-10}$
(4) $\overline{-3}+\overline{2}$
(5) $\overline{3}\cdot\overline{3}$
(6) Show that $\overline{0}=\overline{10}$ and $\overline{2}=\overline{-3}$. Check that $\overline{0}+\overline{2}=\overline{10}+\overline{-3}$ and $\overline{0}\cdot\overline{2}=\overline{10}\cdot\overline{-3}$.

PROPOSITION 7.27. *Let n be an integer with $n\geq 2$. Let $\overline{a},\overline{b}\in\mathbb{Z}_n$. The operations*

$$\begin{aligned}\overline{a}+\overline{b} &= \overline{a+b}\\ \overline{a}\cdot\overline{b} &= \overline{ab}.\end{aligned}$$

are well-defined on $\mathbb{Z}_n$.

PROOF. ⟨*We begin with step one of How To 7.22.*⟩
Let $\overline{x},\overline{y}\in\mathbb{Z}_n$ where $x,y\in\mathbb{Z}$.
By the properties of the integers, both $x+y$ and xy are integers.
Hence $\overline{x}+\overline{y}=\overline{x+y}$ is in $\mathbb{Z}_n$.
And $\overline{x}\cdot\overline{y}=\overline{xy}$ is in $\mathbb{Z}_n$.

⟨*We now verify the second step of How To 7.22.*⟩
Let $\overline{a},\overline{b},\overline{c},\overline{d}\in\mathbb{Z}_n$ with $\overline{a}=\overline{c}$ and $\overline{b}=\overline{d}$.
We must show that

$$\overline{a}+\overline{b} = \overline{c}+\overline{d} \tag{2}$$

$$\overline{a}\cdot\overline{b} = \overline{c}\cdot\overline{d}. \tag{3}$$

⟨*Before verifying equations (2) and (3) we begin with some general remarks.*⟩
Since $\overline{a}=\overline{c}$ and $\overline{b}=\overline{d}$ we have that $a\equiv c(\text{mod } n)$ and $b\equiv d(\text{mod } n)$.
Therefore $n|(a-c)$ and $n|(b-d)$ by the definition of "congruence modulo n."

Hence $a - c = nk$ and $b - d = nm$ for some integers k and m.

We now give a proof of equation (2). Note that

$$(a + b) - (c + d) = (a - c) + (b - d) = nk + nm = n(k + m).$$

Since $k+m$ is an integer the above equation shows that $n|(a+b)-(c+d)$. Therefore $(a+b) \equiv (c+d) (\text{mod } n)$ by definition of "congruence modulo n."
Thus $\overline{a + b} = \overline{c + d}$.
Thus $\overline{a} + \overline{b} = \overline{c} + \overline{d}$ by Definition 7.24.

We now give a proof of equation (3). Note that

$$ab-cd = ab-bc+bc-cd = b(a-c)+c(b-d) = bnk+cnm = n(bk+cm).$$

Since $bk + cm$ is an integer the above equation shows that $n|(ab - cd)$. Therefore $ab \equiv cd (\text{mod } n)$ by definition of "congruence modulo n."
Thus $\overline{ab} = \overline{cd}$.
Thus $\overline{a} \cdot \overline{b} = \overline{c} \cdot \overline{d}$ by Definition 7.24.

■

CHECK FOR UNDERSTANDING 7.28. In $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ calculate the following. As in Example 7.25, reduce your answer $\overline{x}$ so that $0 \leq x \leq 3$.

(1) $\overline{3} + \overline{-10}$
(2) $(\overline{2} \cdot \overline{2}) \cdot \overline{2}$
(3) $(\overline{3} + \overline{-100}) + \overline{54}$
(4) $(\overline{3} \cdot \overline{2}) \cdot \overline{3} + \overline{293}$.

7.5. Partitions

Put stuff here.

7.6. Partial Orders

Put stuff here.

7.7. Exercises

7.7.1. Exercises for section 7.1.

(1) Put some exercises in here.

7.7.2. Exercises for section 7.2.

(1) A set S and a relation $\sim$ on S is given. For each example, check if $\sim$ is (i) reflexive, (ii) symmetric, and/or (iii) transitive. If $\sim$ satisfies the property that you are checking, then prove it. If $\sim$ does not satisfy the property that you are checking, then give an example to show it.
   (a) $S = \mathbb{R}$ where $a \sim b$ if and only if $a \leq b$.
   (b) $S = \mathbb{R}$ where $a \sim b$ if and only if $|a| = |b|$.
   (c) $S = \mathbb{Z}$ where $a \sim b$ if and only if $a|b$.
   (d) S is the set of subsets of $\mathbb{N}$ where $A \sim B$ if and only if $A \subseteq B$. Some examples of elements of S are $\{1, 10, 199\}$, $\{2, 7, 10\}$, and $\{2, 10, 3, 7\}$. Note that $\{2, 7, 10\} \sim \{2, 10, 3, 7\}$

(2) Consider the set $S = \mathbb{R} \times \mathbb{R}$. Define the relation $\sim$ on S where $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 = c^2 + d^2$.
   (a) Find a pairs of points (a, b) and (c, d) that are related in S. Repeat this exercise five more times. Each time you do this, draw a picture.
   (b) Prove that $\sim$ is an equivalence relation on S.
   (c) Draw a picture of the equivalence class of $(1, 0)$. Repeat this exercise for $(0, 0)$, $(1, 1)$, $(0, 2)$, and $(1, 0)$.
   (d) Describe the elements of $S/\sim$. Draw a picture of several equivalence classes.

(3) Consider the set $S = \mathbb{R}$ where $x \sim y$ if and only if $x^2 = y^2$.
   (a) Find all the numbers that are related to $x = 1$. Repeat this exercise for $x = \sqrt{2}$ and $x = 0$.
   (b) Prove that $\sim$ is an equivalence relation on S.
   (c) Draw a number line. Draw a picture of the equivalence class of 1. Repeat this for $x = 0$, $x = \sqrt{6}$, $x = -3$.
   (d) Describe the elements of $S/\sim$. Draw a picture of several equivalence classes.

(4) Consider the set $S = \mathbb{Z}$ where $x \sim y$ if and only if $2|(x + y)$.
   (a) List six numbers that are related to $x = 2$.
   (b) Prove that $\sim$ is an equivalence relation on S.
   (c) Draw a picture of the set of integers. Next, circle the numbers that are in the equivalence class of -3.
   (d) Describe the elements of $S/\sim$. Draw a picture of several equivalence classes.

7.7.3. Exercises for section 7.3.

(1) Let $n = 4$. Consider the equivalence relation given by congruence modulo 4. Compute ten elements from each of the following equivalence classes: $\overline{0}$, $\overline{-3}$, $\overline{2}$, $\overline{5}$.

(2) Answer the following questions where the elements are from $\mathbb{Z}_4$.
   (a) Is $\overline{0} = \overline{8}$?
   (b) Is $\overline{-10} = \overline{-2}$?
   (c) Is $\overline{1} = \overline{13}$?
   (d) Is $\overline{2} = \overline{52}$?
   (e) Is $\overline{-5} = \overline{19}$?

(3) Answer the following questions where the elements are from $\mathbb{Z}_8$.
   (a) Is $\overline{0} = \overline{12}$?
   (b) Is $\overline{-2} = \overline{14}$?
   (c) Is $\overline{-51} = \overline{-109}$?
   (d) Is $\overline{3} = \overline{43}$?

7.7.4. Exercises for section 7.4.

(1) Consider $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. Calculate the following. For each answer $\overline{x}$ that you calculate, reduce it so that $0 \leq x \leq 6$.
   (a) $\overline{2} + \overline{6}$
   (b) $\overline{3} + \overline{4}$
   (c) $\overline{3} \cdot \overline{5}$
   (d) $\overline{2} \cdot \overline{3} + \overline{4} \cdot \overline{6}$
   (e) $\overline{5} \cdot \overline{2} + \overline{1} + \overline{2} \cdot \overline{4} \cdot \overline{6}$

(2) Consider $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Calculate the following. For each answer $\overline{x}$ that you calculate, reduce it so that $0 \leq x \leq 3$.
   (a) $\overline{2} + \overline{3}$
   (b) $\overline{1} + \overline{3}$
   (c) $\overline{3} \cdot \overline{2}$
   (d) $\overline{2} \cdot \overline{2} + \overline{3} \cdot \overline{3}$
   (e) $\overline{3} \cdot \overline{2} + \overline{1} + \overline{2} + \overline{2} \cdot \overline{2} \cdot \overline{2}$

(3) Let n be an integer with $n \geq 2$. Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$. Prove the following. (You will need to use the corresponding properties of the integers given in ??????????????????.)
   (a) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$.
   (b) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.
   (c) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.
   (d) $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.
   (e) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.

(4) Show that the operation $\overline{a} \oplus \overline{b} = \overline{a}^2 + \overline{b}^2$ is a well-defined operation for $\mathbb{Z}_n$. Here $\overline{a}^2$ means $\overline{a} \cdot \overline{a}$. For example, in $\mathbb{Z}_4$ we have that

$$\overline{2} \oplus \overline{3} = \overline{2} \cdot \overline{2} + \overline{3} \cdot \overline{3} = \overline{4} + \overline{9} = \overline{1}.$$

(5) Given two integers a and b, let $\min(a, b)$ denote the minimum (smaller) of a and b. Let n be an integer with $n \geq 2$. Is the operation $\overline{a} \oplus \overline{b} = \overline{\min(a, b)}$ a well-defined operation on $\mathbb{Z}_n$?

(6) Show that the operation $\dfrac{a}{b} \oplus \dfrac{c}{d} = \dfrac{ad}{bc}$ is not a well-defined operation on $\mathbb{Q}$. Is the operation well-defined on $\mathbb{Q} \setminus \{0\}$?

(7) Is the operation $\overline{a} \oplus \overline{b} = \overline{a^b}$ a well-defined operation on $\mathbb{Z}_n$?

(8) Let $S = \mathbb{N} \times \mathbb{N}$. Define the relation $\sim$ on S where $(a, b) \sim (c, d)$ if and only if $a + d = b + c$.
   (a) Is $(3, 6) \sim (7, 10)$?
   (b) Is $(1, 1) \sim (3, 5)$?
   (c) Prove that $\sim$ is an equivalence relation.
   (d) List five elements from each of the following equivalence classes: $\overline{(1, 1)}$, $\overline{(1, 2)}$, $\overline{(5, 12)}$.
   (e) Define the operation $\overline{(a, b)} \oplus \overline{(c, d)} = \overline{(a + c, b + d)}$. Prove that $\oplus$ is well-defined.

(9) Let $S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Define the relation $\sim$ on S where $(a, b) \sim (c, d)$ if and only if $ad = bc$.
   (a) Is $(1, 5) \sim (-3, -15)$?
   (b) Is $(-1, 1) \sim (2, 3)$?
   (c) Prove that $\sim$ is an equivalence relation.
   (d) List five elements from each of the following equivalence classes: $\overline{(1, 1)}$, $\overline{(0, 2)}$, $\overline{(2, 3)}$.
   (e) Define the operation $\overline{(a, b)} \oplus \overline{(c, d)} = \overline{(ad + bc, bd)}$. Prove that $\oplus$ is well-defined.
   (f) Define the operation $\overline{(a, b)} \odot \overline{(c, d)} = \overline{(ac, bd)}$. Prove that $\odot$ is well-defined.

7.7.5. Exercises for section 7.5. Put exercises here.

7.7.6. Exercises for section 7.6. Put exercises here.

Chapter 8

Functions

8.1. Functions

Consider the function f given by the formula $f(x) = x^2$. Here we are assuming that x can be any real number. This function is a common example from algebra and calculus. What *is* the function f? Is there a way to build f using sets? One way to think about f is to draw a picture that represents f. See Figure 1.

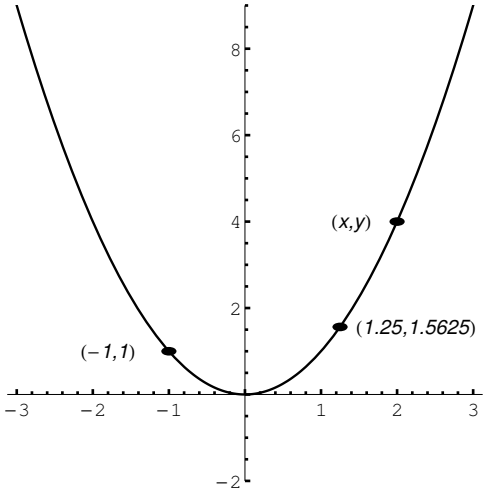


FIGURE 1. A picture of the graph of $y = x^2$ with several points labeled.

Is there a way to think of f as a set instead of as a picture? Yes. The graph of f given in Figure 1 gives us the answer. First of all, the

graph of f lives inside of the set

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

We can think of f as the set of all the points (x, y) from $\mathbb{R} \times \mathbb{R}$ that satisfy the equation $y = x^2$. That is, we can think of the function f as the set

$$f = \{(x, x^2) \mid x \in \mathbb{R}\}.$$

Some examples of points in f are $(-1, 1)$ since $(-1, 1) = (-1, (-1)^2)$, and $(1.25, 1.5625)$ since $(1.25, 1.5625) = (1.25, (1.25)^2)$. Note that $y = x^2$ if and only if $(x, y) \in f$.

We now give a technical definition for a general function. In everyday work, mathematicians do not usually think of as function as a set. However, it is important to see how to build a function out of sets since it shows us that functions can be constructed out of previously known objects in mathematics.

DEFINITION 8.1. Let A and B be sets. Let f be a subset of $A \times B$. We say that f is a **function from A to B** if

(1) For every $a \in A$, there exists a $b \in B$ where $(a, b) \in f$.
(2) If (a, b_1) and (a, b_2) are in f, then $b_1 = b_2$.

If this is the case, then we write $f : A \to B$ to mean that f is a function from A to B.

- The set A is called the **domain** of f.
- The set B is called the **codomain** of f.
- The set

$$\{b \in B \mid \text{there exists } a \in A \text{ with } f(a) = b\}$$

  is called the **range** of f.

If $(a, b) \in f$ then we write $b = f(a)$. If $(a, b) \notin f$ then we write $b \neq f(a)$.

TOO MUCH INFORMATION 8.2. See Figure 2. In Definition 8.1, think of A as the set of inputs to f and the set B as the set of possible outputs from f. That is, you plug $a \in A$ into f and out pops $f(a) = b$ which is in B. A tuple $(a, b) \in f$ means that $f(a) = b$.

As we move along we will phase out the notation $(a, b) \in f$ given in Definition 8.1 with the more familiar notation $b = f(a)$.

TOO MUCH INFORMATION 8.3. There are two conditions given for a function in Definition 8.1. Condition (1) says that for every element $a \in A$ there is an element $b \in B$ with $f(a) = b$. That is, condition (1)

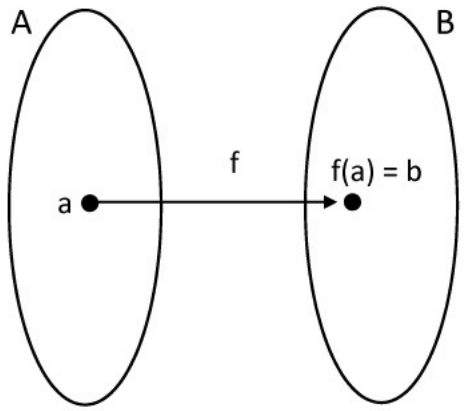


FIGURE 2. A diagram representing a function $f : A \to B$

ensures that one can plug any a from A into the function f. Pictorially, this says that in a picture for f there is always at least one arrow starting at each and every $a \in A$.

Condition (2) says that one cannot have $f(a) = b_1$ and $f(a) = b_2$ if $b_1 \neq b_2$. That is, a function has only one output for each input. Pictorially, this says that in a picture for f there can be only *one* arrow starting from each $a \in A$.

See Example 8.6 for an example where these two conditions fail.

TOO MUCH INFORMATION 8.4. Pictorially, in a picture of a function f from A to B, the range of f consists of all the $b \in B$ with arrows pointing to them.

EXAMPLE 8.5. Let $A = \{-1, 100, 3, 7.2\}$ and $B = \{\pi, -12, -1, 1/2, 17, 14\}$. Define the function

$$f = \{(-1, -1), (100, \pi), (3, 17), (7.2, -1)\}.$$

In this example, A is the domain of f and B is the codomain. We see that $f(-1) = -1$ since $(-1, -1) \in f$, $f(100) = \pi$ since $(\pi, 100) \in f$, $f(3) = 17$ since $(3, 17) \in f$, and $f(7.2) = -1$ since $(7.2, -1) \in f$. One can draw a picture of f as in Figure 3. Note that conditions (1) and (2) from Definition 8.1 are satisfied. (See Remark 8.3.)

What is the range of f? As an example, π is in the range of f because the number 100 is in A and $f(100) = \pi$. Also, $f(-1) = -1$ and $f(3) = 17$. Therefore, we see that the range of f is $C = \{\pi, -1, 17\}$. The range of f is circled in Figure 3 and labeled as C.

EXAMPLE 8.6. Suppose we change Example 8.5 slightly. Let $A = \{-1, 100, 3, 7.2\}$ and $B = \{\pi, -12, -1, 1/2, 17, 14\}$. Define the relation

$$g = \{(100, \pi), (3, 17), (7.2, -1), (100, -12)\}.$$

Is g a function? No. The relation g does not satisfy either condition from Definition 8.1. See Figure 4. Condition (1) is not satisfied because -1 is in A, but $(-1, b)$ does not appear in the definition of g. Because of this $g(-1)$ does not make sense. In pictorial terms, there is no arrow coming out of -1 in the picture of g. Condition (2) is not satisfied because $(100, \pi) \in g$ and $(100, -12) \in g$. If g were a function then $g(100) = \pi$ and $g(100) = -12$ which is nonsense. In pictorial terms, the figure for g has two arrows coming out of 100. Where does 100 go when one plugs it into g? To π or -12? A function has exactly one output for every input.

NOTATION 8.7. From now on we will usually introduce functions as follows: "Let $f : A \to B$ be defined by the formula f(a) = some formula." Or we will define the function f using a picture. In either case, you can think of f as being construced as a subset of $A \times B$. However, we will generally never use this fact or think of f this way.

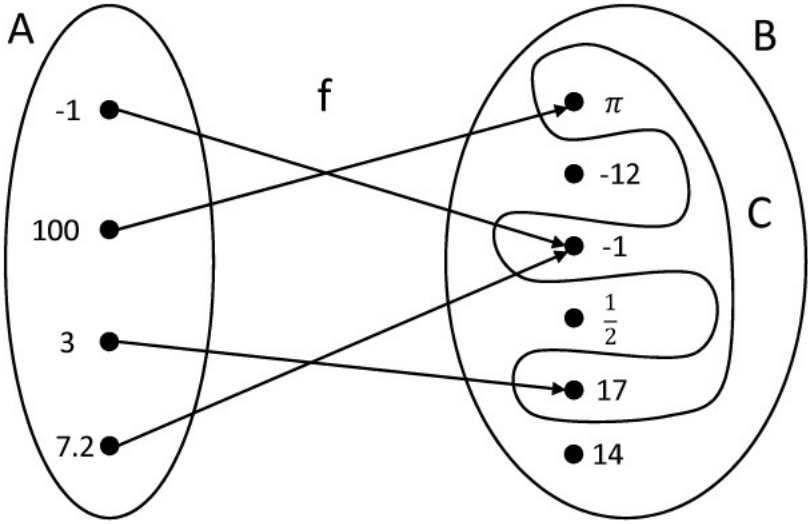


FIGURE 3. A picture of the function f from Example 8.5

CHECK FOR UNDERSTANDING 8.8. Let $A = \{10, -5, 4, 3\}$ and $B = \{-110, \pi, 1.4, 100, 14, 13, -1\}$.

(1) Suppose that $h : A \to B$ is a function. Let $a \in A$. What set does $h(a)$ live in?
(2) Define $f = \{(10, 1.4), (4, \pi), (-5, 1.4)\}$. Is f a function from A to B? If so, draw a picture of f and state the range of f? If f is not a function, explain why not.
(3) Define $g = \{(3, 14), (10, -110), (4, 100), (-5, 14)\}$. Is g a function from A to B? If so, draw a picture of g and state the range of g? If g is not a function, explain why not.

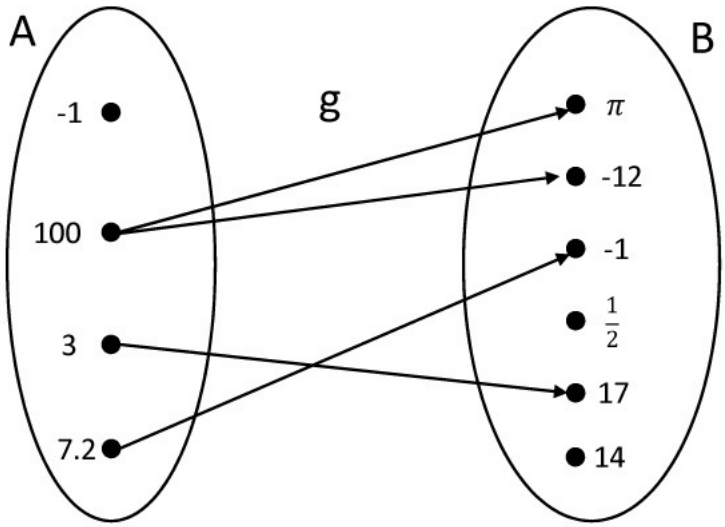


FIGURE 4.
A picture of g from Example 8.6. g is not a function.

DEFINITION 8.9. Let A be a set. Define the function $i_A : A \to A$ by the formula $i_A(a) = a$ for every $a \in A$. The function i_A is called the **identity function on A**.

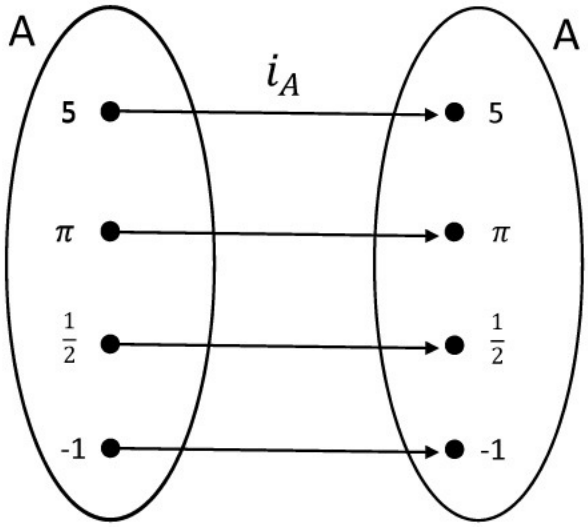


FIGURE 5. The identity function on the set $A = \{5, \pi, 1/2, -1\}$.

EXAMPLE 8.10. Let $A = \{5, \pi, 1/2, -1\}$. The identity function on A is given in Figure 5.

EXAMPLE 8.11. Let n be an integer with $n \geq 2$. Consider the function $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ given by the formula

$$\pi_n(x) = \overline{x}.$$

That is, π_n sends x to the equivalence class of x modulo n. The map π_n is called the **reduction modulo n map**.

For example, consider $n = 3$. Then $\pi_3 : \mathbb{Z} \to \mathbb{Z}_3$ is a function from $\mathbb{Z}$ to $\mathbb{Z}_3$. See Figure 6 for a partial picture of π_3. (We cannot draw the

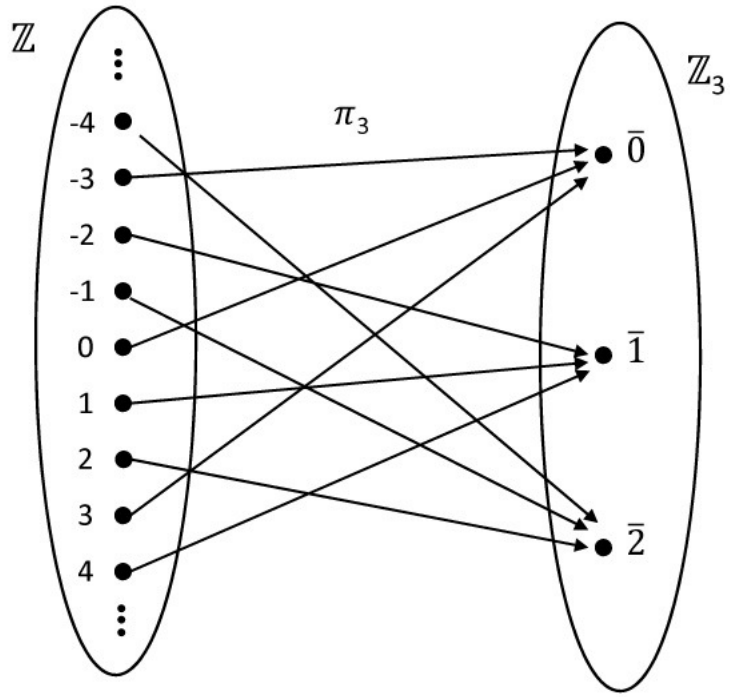


FIGURE 6. A picture of the function π_3 from Example 8.11

entire picture for π_3 because $\mathbb{Z}$ is infinite.) Then,
$\pi_3(0) = \overline{0}$,
$\pi_3(1) = \overline{1}$,
$\pi_3(2) = \overline{2}$,
$\pi_3(3) = \overline{3} = \overline{0}$ because $3 \equiv 0 (\text{mod } 3)$,
$\pi_3(4) = \overline{4} = \overline{1}$ because $4 \equiv 1 (\text{mod } 3)$,
$\pi_3(-1) = \overline{-1} = \overline{2}$ because $-1 \equiv 2 (\text{mod } 3)$,
$\pi_3(-2) = \overline{-2} = \overline{1}$ because $-2 \equiv 1 (\text{mod } 3)$,
$\pi_3(-3) = \overline{-3} = \overline{0}$ because $-3 \equiv 0 (\text{mod } 3)$,

and $\pi_3(-4) = \overline{-4} = \overline{2}$ because $-4 \equiv 2 (\text{mod } 3)$.

Note that the range of π_3 is all of $\mathbb{Z}_3$.

CHECK FOR UNDERSTANDING 8.12. Consider the map π_3 from Example 8.11. Calculate $\pi_3(107)$ and $\pi_3(-19)$.

8.2. Well-defined functions

HOW TO 8.13. **Show that a function is well-defined.**

Suppose that one is defining a function $f : A \to B$. To show that f is well-defined one must check the following.

Step 1. If $a \in A$, then $f(a) \in B$.

Step 2. For every $a_1, a_2 \in A$, if $a_1 = a_2$ then $f(a_1) = f(a_2)$. This step is particularly important when the elements of A can be expressed in more than one way.

EXAMPLE 8.14. Suppose that we want to define the function $f : \mathbb{Q} \to \mathbb{Q}$ given by the formula $f(a/b) = b/a$. Is f well-defined? No, because $0 = 0/1$ is in $\mathbb{Q}$ but $f(0/1) = 1/0$ is undefined. Hence f is not well-defined because it fails step one of How To 8.13.

EXAMPLE 8.15. Suppose that we want to define the function $f : \mathbb{Q} \to \mathbb{Q}$ given by the formula $f(a/b) = a$. For example, $f(2/5) = 2$. Is f well-defined? Certainly given $a/b \in \mathbb{Q}$ we have that $f(a/b) = a$ is an element of $\mathbb{Q}$. It seems like everything is fine. However, notice that each rational number can be written in an infinite number of ways and no matter which way we represent a fraction we must get the same output from f. This does not occur. For example, $2/5 = 4/10$, however $f(2/5) = 2$ and $f(4/10) = 4$, but $2 \neq 4$. This doesn't make any sense. Hence f is not a well-defined function.

CHECK FOR UNDERSTANDING 8.16.

(1) Is the function $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(a/b) = a - b$ well-defined?

(2) Is the function $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(a/b) = a^2/b^2$ well-defined?

EXAMPLE 8.17. Consider the function $f_3 : \mathbb{Z}_4 \to \mathbb{Z}_4$ given by the formula

$$f_3(\overline{x}) = \overline{3} \cdot \overline{x}.$$

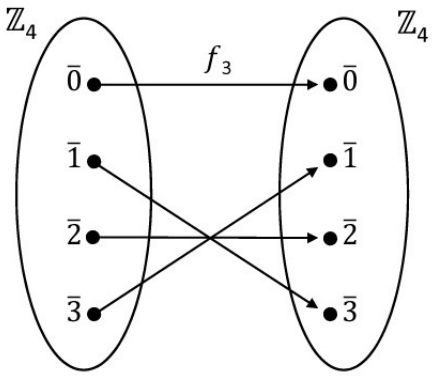


FIGURE 7. A picture of $f_3 : \mathbb{Z}_4 \to \mathbb{Z}_4$ from Example 8.17 . Recall that $f_3(\overline{x}) = \overline{3} \cdot \overline{x}$.

In Example 8.18 we will show that f_3 is a well-defined function. This example is to give the reader a feel for the function. Let us compute the values of f_3. We have that

$$\begin{aligned} f_3(\overline{0}) &= \overline{3} \cdot \overline{0} = \overline{0}, \\ f_3(\overline{1}) &= \overline{3} \cdot \overline{1} = \overline{3}, \\ f_3(\overline{2}) &= \overline{3} \cdot \overline{2} = \overline{6} = \overline{2}, \text{and} \\ f_3(\overline{3}) &= \overline{3} \cdot \overline{3} = \overline{9} = \overline{1}. \end{aligned}$$

See Figure 7 for a picture of f_3.

Note that in $\mathbb{Z}_4$ we have that $\overline{1} = \overline{9}$ since $1 \equiv 9 (\text{mod } 4)$. If f_3 is a well-defined function we must have that $f_3(\overline{1}) = f_3(\overline{9})$. Let us check this fact. From above we have that $f_3(\overline{1}) = \overline{3}$. This in fact equals

$$f_3(\overline{9}) = \overline{3} \cdot \overline{9} = \overline{27} = \overline{3}$$

since $27 \equiv 3 (\text{mod } 4)$. To show that f_3 is actually well-defined one has to give a more general argument. We do this in Example 8.18.

EXAMPLE 8.18. We now generalize Example 8.17. Let n be an integer with $n \geq 2$. Let a be an integer. Define $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ where

$$f_a(\overline{x}) = \overline{a} \cdot \overline{x}.$$

Then f_a is a well-defined function.

PROOF. Note that if $\overline{x} \in \mathbb{Z}_n$, then $f_a(\overline{x}) = \overline{a} \cdot \overline{x} = \overline{ax}$ is an element of $\mathbb{Z}_n$.
Hence step one of How To 8.13 is satisfied.

Suppose that $\overline{x_1} = \overline{x_2}$.
Then $f_a(x_1) = \overline{a} \cdot \overline{x_1} = \overline{a} \cdot \overline{x_2} = f_a(\overline{x_2})$ by Proposition 7.27.
Hence step two of How To 8.13 is satisfied.

Therefore f_a is a well-defined function. ■

CHECK FOR UNDERSTANDING 8.19. Let $n \geq 2$ be an integer. Consider the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f(\overline{x}) = \overline{x}^2$. Prove that f is a well-defined function.

8.3. One-to-one and Onto functions

We are about to give two very useful definitions involving functions. These are the "onto" and "one-to-one" properties that functions may or may not satisfy. These definitions are used throughout your future mathematics courses and are important to understand. We will give lots of examples in this section to illustrate the topic.

We begin with "one-to-one" functions. What is a one-to-one function? It is easier to define what a one-to-one function is not. A function $f : A \to B$ is NOT one-to-one if Figure 8 occurs with $a_1 \neq a_2$. That is, f is not one-to-one if there are two different elements of A that f maps to the same element of B. This is re-formulated in Definition 8.20.

DEFINITION 8.20. Let A and B be sets and $f : A \to B$. We say that f is **one-to-one**, or **injective**, if for every $a_1, a_2 \in A$ the following statement is true: If $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

EXAMPLE 8.21. See Figure 9. The function h in Figure 9 is not one-to-one because $11 \neq -1$ but $h(11) = h(-1)$. Another way of saying this is that there are two distinct elements from G, the numbers 11

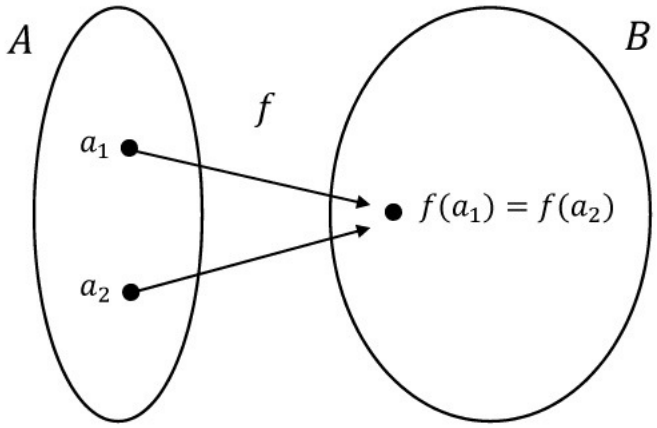
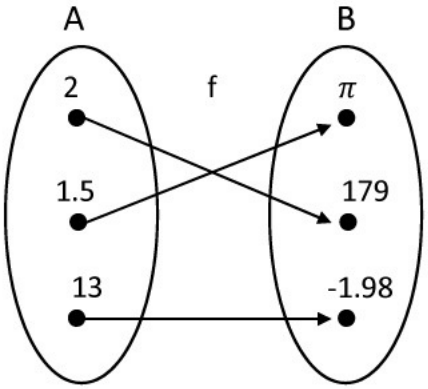


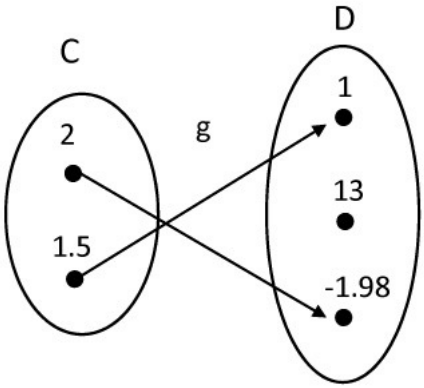
FIGURE 8. A diagram that illustrates how a function can FAIL to be a one-to-one function. Here we are assuming that $a_1 \neq a_2$.

and -1, that both go to 1.5 when they are plugged into the function h.

The function k in Figure 9 is not one-to-one because $-13 \neq -1$ but $k(-13) = h(-1)$. The function f in Figure 9 is one-to-one. The function g in Figure 9 is one-to-one.



f is one-to-one; f is onto



g is not onto; g is

TOO MUCH INFORMATION 8.22. The contrapositive of "If $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$" is "If $f(a_1) = f(a_2)$, then $a_1 = a_2$." We use this fact in How To 8.23.

HOW TO 8.23. **Show that a function $f : A \to B$ is one-to-one** Recall Remark 8.22. One technique to show that f is one-to-one is to use the following steps:

- Assume that $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$.
- Derive the fact that $a_1 = a_2$.

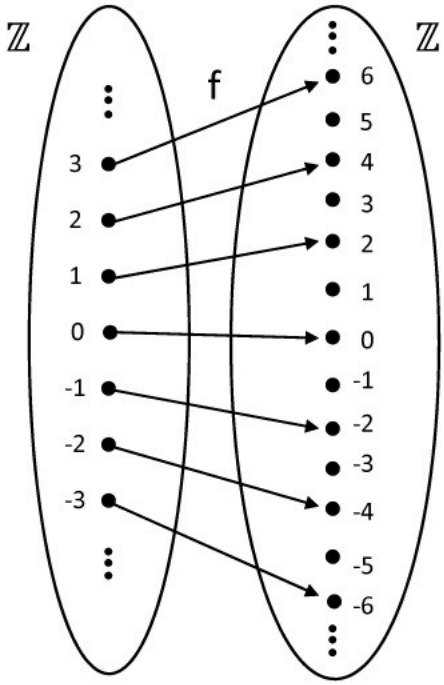


FIGURE 10. $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 2x$.

EXAMPLE 8.24. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ where f is given by the formula $f(x) = 2x$. A picture for f is given in Figure 10. We now show that f is one-to-one.

PROOF. Suppose that a_1 and a_2 are elements of $\mathbb{Z}$ with $f(a_1) = f(a_2)$.
This implies that $2a_1 = 2a_2$.
Dividing by 2 we see that $a_1 = a_2$.
Hence f is one-to-one. ■

HOW TO 8.25. **Show that a function $f : A \to B$ is NOT one-to-one**
Find two elements a_1 and a_2 from A where $a_1 \neq a_2$ and $f(a_1) = f(a_2)$.

Let's give an example a function that is not one-to-one and prove it.

EXAMPLE 8.26. Consider the function $f : \mathbb{Z}_7 \to \mathbb{Z}_7$ where $f(\overline{x}) = \overline{x}^2$. It is shown in Check for understanding 8.19 that f is a well-defined function. Note the following:

$$\begin{array}{lllllll} f(\overline{0}) & = & \overline{0} \cdot \overline{0} & = & \overline{0} & & \\ f(\overline{1}) & = & \overline{1} \cdot \overline{1} & = & \overline{1} & & \\ f(\overline{2}) & = & \overline{2} \cdot \overline{2} & = & \overline{4} & & \\ f(\overline{3}) & = & \overline{3} \cdot \overline{3} & = & \overline{9} & = & \overline{2} \\ f(\overline{4}) & = & \overline{4} \cdot \overline{4} & = & \overline{16} & = & \overline{2} \\ f(\overline{5}) & = & \overline{5} \cdot \overline{5} & = & \overline{25} & = & \overline{4} \\ f(\overline{6}) & = & \overline{6} \cdot \overline{6} & = & \overline{36} & = & \overline{1} \end{array}$$

See Figure 11 for a picture of f. Notice that f is not one-to-one since $f(\overline{1}) = f(\overline{6})$ but $\overline{1} \neq \overline{6}$. (We used the pair of numbers $\overline{1}$ and $\overline{6}$ to show that f is not one-to-one. We could have used the pair of numbers $\overline{3}$ and $\overline{4}$, or the pair of numbers $\overline{2}$ and $\overline{5}$.)

EXAMPLE 8.27. We now generalize Example 8.26. Let n be an integer where $n \geq 2$. Let $f : \mathbb{Z}_n \to \mathbb{Z}_n$ where $f(\overline{x}) = \overline{x}^2$. Then f is not one-to-one.

PROOF. Note that $\overline{1} \neq \overline{n-1}$ in $\mathbb{Z}_n$ by Proposition 7.21.
We have that $f(\overline{1}) = \overline{1}$.
Notice that $\overline{n-1} = \overline{-1}$ since $n - 1 \equiv -1 (\text{mod } n)$.
Thus $f(\overline{n-1}) = \overline{n-1} \cdot \overline{n-1} = \overline{-1} \cdot \overline{-1} = \overline{1}$.
Hence $f(\overline{n-1}) = f(\overline{1})$ but $\overline{n-1} \neq \overline{1}$.
Therefore f is not one-to-one. ■

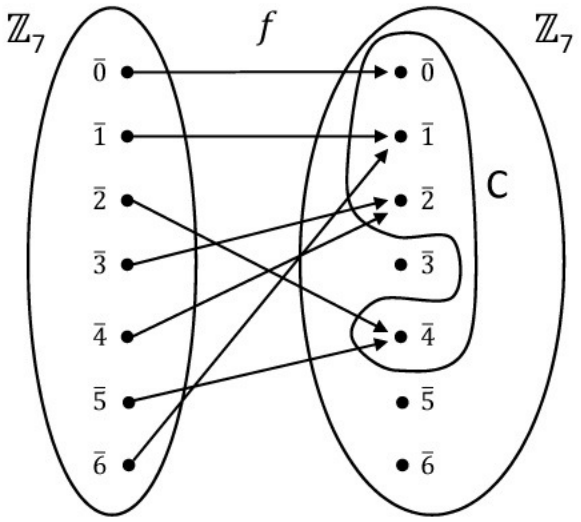


FIGURE 11. A picture of $f : \mathbb{Z}_7 \to \mathbb{Z}_7$ where $f(\overline{x}) = \overline{x}^2$. C is the range of f.

CHECK FOR UNDERSTANDING 8.28.

(1) Let $n = 6$. Consider $f_a : \mathbb{Z}_6 \to \mathbb{Z}_6$ where $f_a(\overline{x}) = \overline{a} \cdot \overline{x}$ as in Example 8.18. Draw a picture of f_2 and f_5. Is f_2 one-to-one? Is f_5 one-to-one?

(2) Consider the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = 2x - 5$. Is g one-to-one? Prove or disprove.

(3) Recall Example 8.11. Let $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ be given by $\pi_n(x) = \overline{x}$. Prove that π_n is not one-to-one.

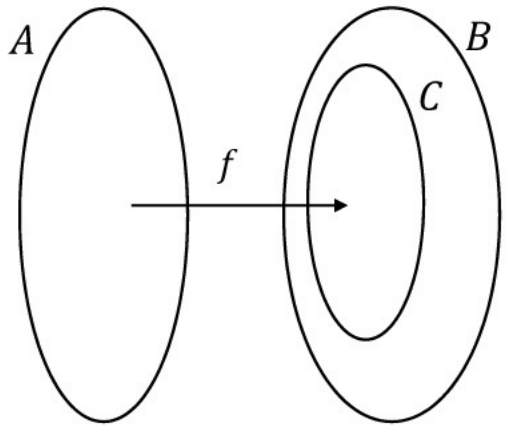


FIGURE 12. A function $f : A \to B$ with range C. We say that f is onto if and only if $C = B$.

We now discuss the property of being "onto" that a function may or may not possess.

DEFINITION 8.29. Let A and B be sets and $f : A \to B$. Let C be the range of f. We say that f is **onto**, or **surjective**, if $B = C$. See Figure 12.

EXAMPLE 8.30. The function f in Figure 9 is onto because the range of f is all of B.
The function g in Figure 9 is not onto because 12 is not in the range of g.
The function h in Figure 9 is onto because the range of h is all of F.
The function k in Figure 9 is not onto because -18 is not in the the range of k.

TOO MUCH INFORMATION 8.31. Let $f : A \to B$ be a function with range C. See Figure 12. To show that f is onto one must show that $C = B$. By the definition of a function we have that $C \subseteq B$, that is, the range of f is contained in B. Hence, to show that f is onto, one must show that $B \subseteq C$. That is, given any element $x \in B$ one must show that $x \in C$. This is formulated in How To 8.32.

HOW TO 8.32. **Show that a function $f : A \to B$ is onto**
- Let b be an arbitrary element of B.
- Show that there exists an element $a \in A$ with $f(a) = b$.

EXAMPLE 8.33. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = 2x - 5$. Then f is onto.

PROOF. Let $b \in \mathbb{R}$.
⟨*We must find $a \in \mathbb{R}$ with $f(a) = b$. This amounts to solving the equation $2a - 5 = b$ for a, which gives $a = (b+5)/2$. See Figure 13 for a picture illustrating this proof.*⟩
Let $a = (b + 5)/2$.
We have that $a \in \mathbb{R}$ since $b \in \mathbb{R}$.
Furthermore, $f(a) = f((b + 5)/2) = 2[(b + 5)/2] - 5 = b$.
Hence f is onto. ■

HOW TO 8.34. **Show that a function $f : A \to B$ is NOT onto**
Find an element $b \in B$ that is not in the range of f.

EXAMPLE 8.35. Consider the function $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ given by the formula $f(x) = x^2$. Then f is not onto.

PROOF. ⟨*We give a proof by contradiction. We will show that 2 is not in the range of f.*⟩
Suppose that the element 2 is in the range of f.
Then there exists $x \in \mathbb{Z}$ with $f(x) = 2$.
Hence $x^2 = 2$.
By Theorem 4.53 we know that this is not possible since the square

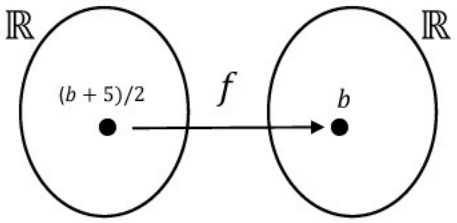


FIGURE 13. An illustration of the proof of Example 8.33

root of two is not an integer.
Hence 2 is not in the range of f.
Therefore f is not onto. ■

CHECK FOR UNDERSTANDING 8.36. (1) Recall Example 8.11. Let $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ be the reduction modulo n map given by the formula $\pi_n(x) = \overline{x}$. Is π_n is onto? Prove or disprove.
(2) Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = 2x$. Is f onto? Prove or disprove.

DEFINITION 8.37. Let A and B be sets and $f : A \to B$. We say that f is **bijective**, or f is a **bijection**, if f is both surjective and injective.

EXAMPLE 8.38. The function f in Figure 9 is bijective because f is both injective and surjective.
The function g in Figure 9 is not a bijection because it is not surjective.
The function h in Figure 9 is not a bijection because it is not injective.
The function k in Figure 9 is neither injective nor surjective, and hence k is not a bijection.

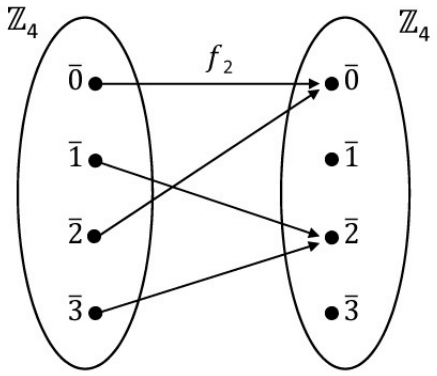


FIGURE 14. A picture of f_2 from Example 8.39

EXAMPLE 8.39. Recall Example 8.18. Let n be an integer with $n \geq 2$. Let a be an integer. Define the function $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ where

$f_a(\overline{x}) = \overline{a} \cdot \overline{x}$. When is f_a a bijection? We answer this question in Proposition 8.41, but first we give some examples.

In Example 8.17 we saw that $f_3 : \mathbb{Z}_4 \to \mathbb{Z}_4$ given by $f_3(\overline{x}) = \overline{3} \cdot \overline{x}$ is a bijection. Let's try another one. Let us keep $n = 4$ and compute the function f_2. We see that

$$\begin{aligned} f_2(\overline{0}) &= \overline{2} \cdot \overline{0} = \overline{0}, \\ f_2(\overline{1}) &= \overline{2} \cdot \overline{1} = \overline{2}, \\ f_2(\overline{2}) &= \overline{2} \cdot \overline{2} = \overline{4} = \overline{0}, \text{ and} \\ f_2(\overline{3}) &= \overline{2} \cdot \overline{3} = \overline{6} = \overline{2}. \end{aligned}$$

See Figure 14 for a picture of f_2. Notice that f_2 is not a bijection.

LEMMA 8.40. *Let n be an integer with $n \geq 2$. Let a be any integer. If $\gcd(a, n) = 1$, then there exists an element $\overline{b} \in \mathbb{Z}_n$ with*

$$\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b} = \overline{1}.$$

PROOF. By Theorem 4.63, there exist integers b and c such that $ba + cn = 1$ because $\gcd(a, n) = 1$.
Therefore $\overline{ba + cn} = \overline{1}$ in $\mathbb{Z}_n$.
Hence $\overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{n} = \overline{1}$ by Proposition 7.27.
It follows that $\overline{b} \cdot \overline{a} = \overline{1}$ because $\overline{n} = \overline{0}$ in $\mathbb{Z}_n$.
Furthermore, $\overline{b} \cdot \overline{a} = \overline{ba} = \overline{ab} = \overline{a} \cdot \overline{b}$ by the properties of the integers.
Therefore, $\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b} = \overline{1}$. ■

PROPOSITION 8.41. *Recall Example 8.18. Let n be an integer with $n \geq 2$. Let a be an integer. Define the function $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ where $f_a(\overline{x}) = \overline{a} \cdot \overline{x}$. If $\gcd(a, n) = 1$, then $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ is a bijection.*

PROOF. By Lemma 8.40 we have that there exists an element $\overline{b} \in \mathbb{Z}_n$ with

$$\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b} = \overline{1}$$

since $\gcd(a, n) = 1$.
⟨*We now show that f_a is a bijection. We start by showing that f_a is one-to-one.*⟩
Suppose that $f_a(\overline{x}) = f_a(\overline{y})$ for some $\overline{x}, \overline{y} \in \mathbb{Z}_n$.
Then $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y}$ by the definition of f_a.
Multiplying on the left by $\overline{b}$ gives us that $\overline{b} \cdot \overline{a} \cdot \overline{x} = \overline{b} \cdot \overline{a} \cdot \overline{y}$.
Thus $\overline{x} = \overline{y}$ since $\overline{b} \cdot \overline{a} = \overline{1}$.

Therefore f_a is one-to-one.

⟨*We now show that f_a is onto.*⟩
Let $\overline{y} \in \mathbb{Z}_n$.
Then $\overline{b} \cdot \overline{y} \in \mathbb{Z}_n$ and $f_a(\overline{b} \cdot \overline{y}) = \overline{a} \cdot \overline{b} \cdot \overline{y} = \overline{y}$ since $\overline{a} \cdot \overline{b} = \overline{1}$.
Therefore f_a is onto.

■

TOO MUCH INFORMATION 8.42. In Exercise 8 you will show that f_a is not a bijection if $\gcd(a, n) > 1$.

8.4. Composition of functions

DEFINITION 8.43. Let A, B, and C be sets. Let $f : A \to B$ and $g : B \to C$. The **composition of f and g**, denoted by $g \circ f$, is defined to be the function from A to C that satisfies the formula

$$(g \circ f)(x) = g(f(x)).$$

See Figure 15.

TOO MUCH INFORMATION 8.44. In set theoretic terms,

$$g \circ f = \{(a, g(f(a))) \mid a \in A\}.$$

We leave it as Exercise 1 to show that $g \circ f$ satisfies the properties of Definition 8.1.

EXAMPLE 8.45. Let $A = \{-1, 5, 3\}$, $B = \{7, 0, -3.2\}$, and $C = \{\pi, 4, -1\}$. Define the function $f : A \to B$ by $f(-1) = 7$, $f(5) = -3.2$, and $f(3) = 0$. Define the function $g : B \to C$ by $g(7) = 4$, $g(0) = -1$, and $g(-3.2) = \pi$. Then the function $g \circ f : A \to C$ is computed as follows:

$$\begin{array}{ccccccc} (g \circ f)(-1) & = & g(f(-1)) & = & g(7) & = & 4 \\ (g \circ f)(5) & = & g(f(5)) & = & g(-3.2) & = & \pi \\ (g \circ f)(3) & = & g(f(3)) & = & g(0) & = & -1 \end{array}$$

Pictorally, one can see the above computation in Figure 16. For example, to compute $(g \circ f)(5)$ follow the dotted arrows. These arrows match up with the computation given above. The function $g \circ f$ can be pictured in Figure 17.

EXAMPLE 8.46. Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be given by the formulas $f(x) = 2x - 1$ and $g(x) = x^2$. Then $g \circ f : \mathbb{R} \to \mathbb{R}$ is given by the formula $(g \circ f)(x) = g(f(x)) = g(2x-1) = (2x-1)^2 = 4x^2 - 4x + 1$.

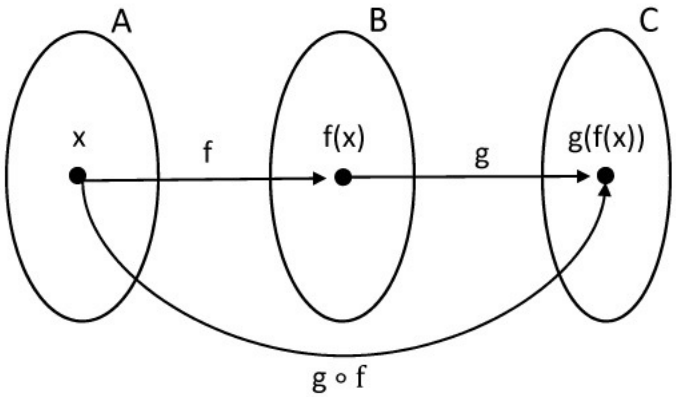


FIGURE 15. A diagram illustrating Definition 8.43.

PROPOSITION 8.47 (The composition of two onto functions is an onto function). *Let A, B, and C be sets. Suppose that $f : A \to B$ is an onto function and $g : B \to C$ is an onto function. Then $g \circ f : A \to C$ is an onto function.*

PROOF. ⟨*The proof ouline is as follows. To show that $g \circ f : A \to C$ is onto we use How To 8.32. That is, given $c \in C$ we need to find an $a \in A$ with $(g \circ f)(a) = c$. To do this, we start with an element $c \in C$.*

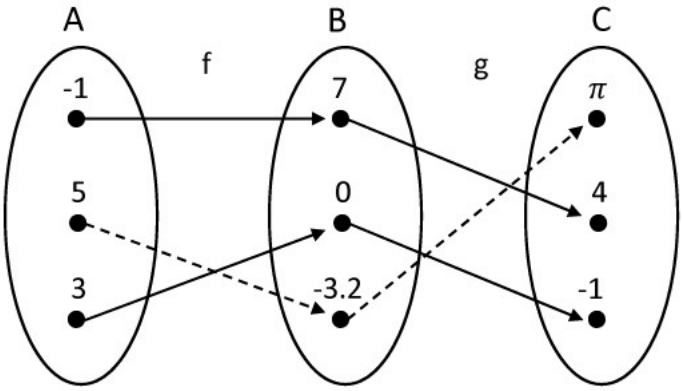


FIGURE 16. A picture of f and g from Example 8.45. The dotted lines illustrate the computation of $(g \circ f)(5)$.

We then use the fact that g is onto to "pull back" c to an element $b \in B$. We then use the fact that f is onto to "pull back" b to an element $a \in A$. See Figure 18 for a picture illustrating this proof.⟩
Let $c \in C$.
Since $g : B \to C$ is onto, there exists some $b \in B$ with $g(b) = c$.
Since $f : A \to B$ is onto, there exists some $a \in A$ with $f(a) = b$.
Thus $(g \circ f)(a) = g(f(a)) = g(b) = c$.
Therefore, for any $c \in C$, there exists $a \in A$ with $(g \circ f)(a) = c$.
This implies that $g \circ f$ is onto. ■

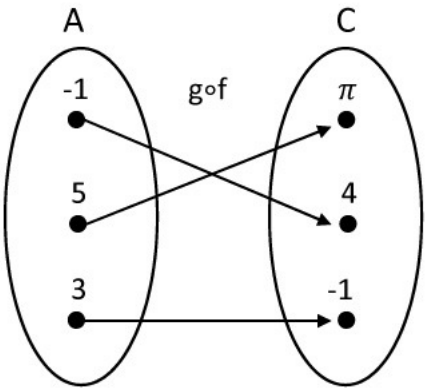


FIGURE 17. A picture of $g \circ f$ from Example 8.45

PROPOSITION 8.48 (The Composition of two one-to-one functions is a one-to-one function). *Let A, B, and C be sets. Suppose that $f : A \to B$ is a one-to-one function and $g : B \to C$ is a one-to-one function. Then $g \circ f : A \to C$ is a one-to-one function.*

PROOF. Let $a_1, a_2 \in A$ and suppose that $(g \circ f)(a_1) = (g \circ f)(a_2)$.
$\langle$*We must show that* $a_1 = a_2$.$\rangle$
We have that $g(f(a_1)) = g(f(a_2))$ by the definition of "composition".

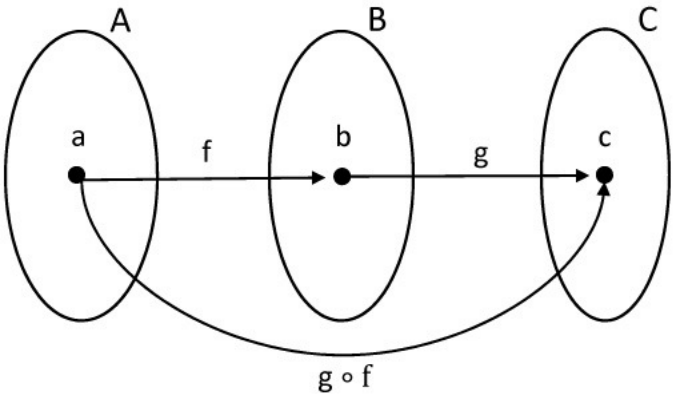


FIGURE 18. A picture illustrating the proof of Theorem 8.47

Therefore $f(a_1) = f(a_2)$ because g is one-to-one.
Therefore $a_1 = a_2$ because f is one-to-one.
This implies that $g \circ f$ is one-to-one. ■

COROLLARY 8.49 (The composition of two bijective functions is a bijective function). *Let A, B, and C be sets. Suppose that $f : A \to B$ is a bijection and $g : B \to C$ is a bijection. Then $g \circ f : A \to C$ is a bijection.*

PROOF. Both g and f are surjective by the definition of "bijection". Therefore $g \circ f$ is surjective by Proposition 8.47.
Both g and f are injective by the definition of "bijection".
Therefore $g \circ f$ is injective by Proposition 8.48.
Thus $g \circ f$ is bijective. ■

8.5. Inverse functions

DEFINITION 8.50. Let A and B be sets and $f : A \to B$ be a one-to-one function. Let C be the range of f. Define the function $f^{-1} : C \to A$ by $f^{-1}(c) = a$ if and only if $f(a) = c$. See Figure 19.

TOO MUCH INFORMATION 8.51. The definition of f^{-1} given in Definition 8.50 is a well-defined function. We leave the details of this fact to the reader in Exercise 1. The basic outline is as follows: Definition 8.50 is well-defined because f is one-to-one. That is, given an element c in the range of f there exists one and only one element a with $f(a) = c$. This allows us to define $f^{-1}(c) = a$.

EXAMPLE 8.52. Let $A = \{1, 7, -2, 10\}$ and $B = \{13, \pi, 1.5, 2.71, 1/2, 10\}$. Define the function $f : A \to B$ by the formula

$$f(a) = \begin{cases} \pi & , \text{ if } a = 1 \\ 13 & , \text{ if } a = 7 \\ 2.71 & , \text{ if } a = -2 \\ 1/2 & , \text{ if } a = 10 \end{cases}$$

Let C be the range of f. Then $C = \{13, \pi, 2.71, 1/2\}$. See Figure 20 for a picture of f.

Note that f is one-to-one. Thus we may construct $f^{-1} : C \to A$. We see that $f^{-1}(13) = 7$ because $f(7) = 13$, $f^{-1}(\pi) = 1$ because $f(1) = \pi$, $f^{-1}(2.71) = -2$ because $f(-2) = 2.71$, and $f^{-1}(1/2) = 10$ because $f(10) = 1/2$. See Figure 21 for a picture of f^{-1}. Note that f^{-1} is one-to-one and onto.

PROPOSITION 8.53. *Let $f : A \to B$ be a one-to-one function. Let C be the range of f. Let $f^{-1} : C \to A$ be the inverse function of f. Then*

(1) *The domain of f^{-1} equals the range of f.*

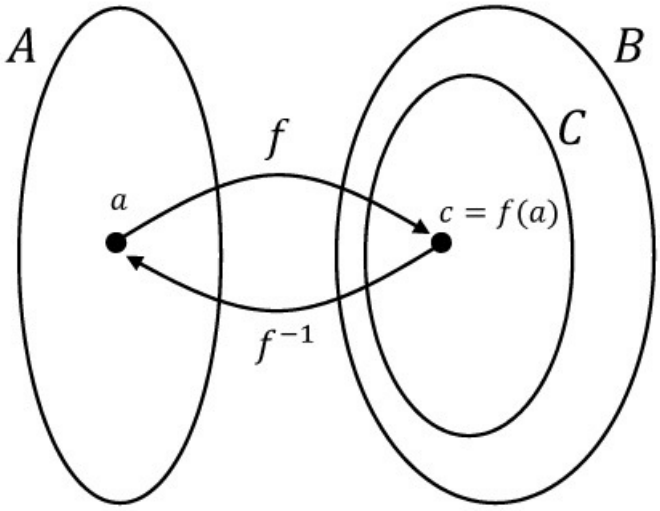


FIGURE 19. A figure illustrating Definition 8.50. Here $f : A \to B$ is a one-to-one function with range equal to C.

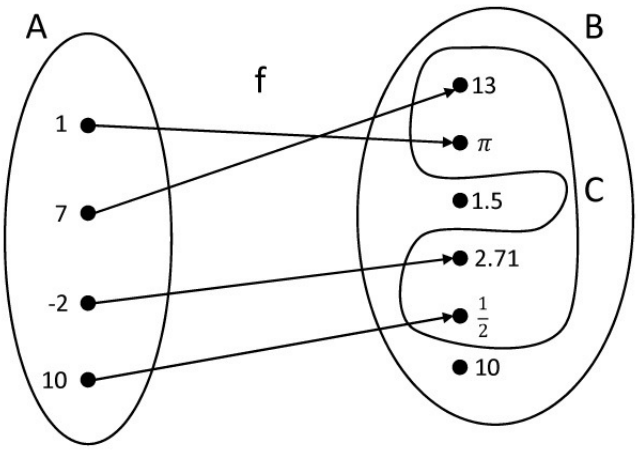


FIGURE 20. f from Example 8.52

(2) *The range of* f^{-1} *equals the domain of* f*. In particular,* f^{-1} *is onto* A*.*
(3) f^{-1} *is one-to-one.*
(4) $(f^{-1} \circ f)(a) = a$ *for all* $a \in A$*. That is,* $f^{-1} \circ f = i_A$*.*
(5) $(f \circ f^{-1})(c) = c$ *for all* $c \in C$*. That is,* $f^{-1} \circ f = i_C$*.*

PROOF. (1) This follows from the definition of f^{-1}.

(2) Let $a \in A$.
Then $f(a) = c$ for some $c \in C$.
Thus $f^{-1}(c) = a$ by the definition of f^{-1}.
Therefore f^{-1} is onto A.

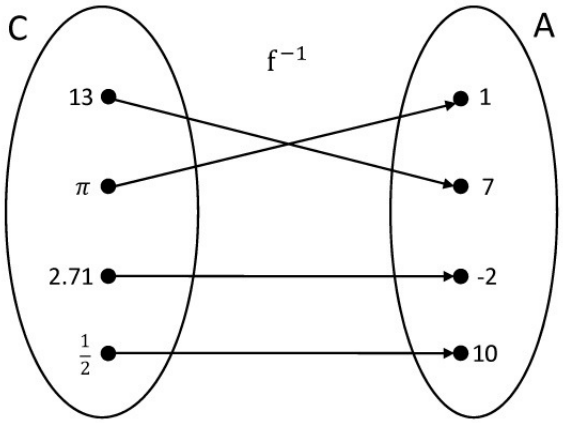


FIGURE 21. f^{-1} from Example 8.52

(3) Let c_1 and c_2 be elements of C and suppose that $f^{-1}(c_1) = a = f^{-1}(c_2)$ where $a \in A$.
Then $c_1 = f(a) = c_2$ by the definition of f^{-1}.
Hence f^{-1} is one-to-one.

(4) Let $a \in A$.
Applying f to a we get that $f(a) = c$ for some $c \in C$.
Applying f^{-1} to c we get that $f^{-1}(c) = a$ by the definition of f^{-1}.
Hence $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(c) = a$.

(5) Let $c \in C$.
There exists a unique element $a \in A$ such that $f(a) = c$ because C is the range of f and f is one-to-one.
Thus $f^{-1}(c) = a$ by the definition of f^{-1}.
Hence $(f \circ f^{-1})(c) = f(f^{-1}(c)) = f(a) = c$. ■

EXAMPLE 8.54. Let $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. If x is a real number then $(2x-1)/x$ is defined for all non-zero x. Hence we may define the function $f : \mathbb{R}^* \to \mathbb{R}$ given by the formula $f(x) = (2x-1)/x$. See Figure 22 for a picture of part of the graph of f.

What is the range of f? Let $y \in \mathbb{R}$. Note that y is in the range iff there exists an $x \in \mathbb{R}^*$ with $f(x) = (2x-1)/x = y$. Solving for x in this equation we see that $x = 1/(2-y)$. Therefore if y is a real number with $y \neq 2$ then

$$f\left(\frac{1}{2-y}\right) = \frac{2(\frac{1}{2-y}) - 1}{\frac{1}{2-y}} = y$$

giving that y is in the range of f. Thus the range of f is $\mathbb{R} \setminus \{2\}$.

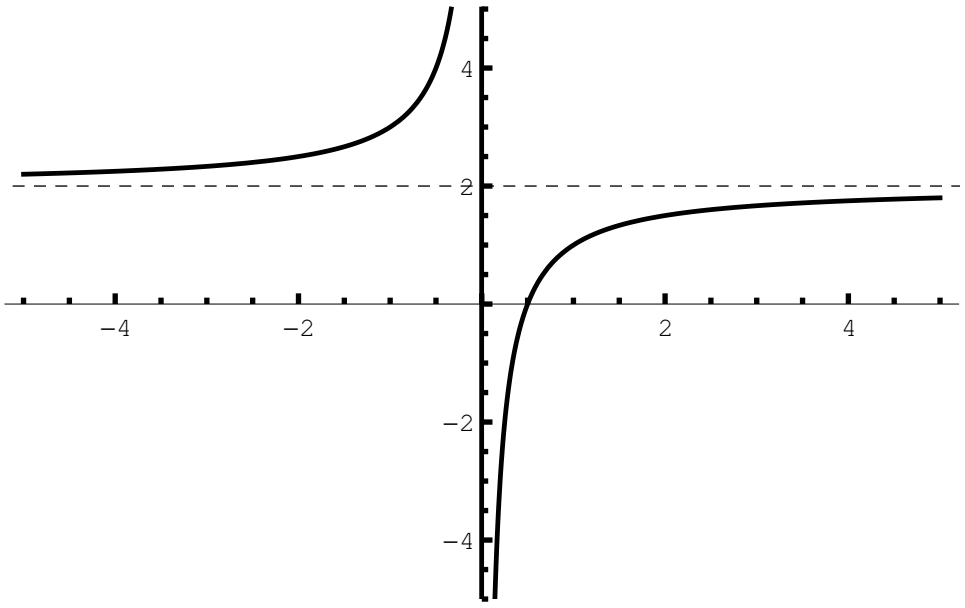


FIGURE 22. The graph of $f(x) = \dfrac{2x-1}{x}$

We now check that f is one-to-one. Suppose that $f(x_1) = f(x_2)$ for some $x_1, x_2 \in \mathbb{R}^*$. Then $(2x_1-1)/x_1 = (2x_2-1)/x_2$ which implies that $2x_1x_2 - x_2 = 2x_2x_1 - x_1$ which implies that $x_1 = x_2$. Therefore f is one-to-one.

Since f is one-to-one we may define the inverse function $f^{-1} : \mathbb{R} \setminus \{2\} \to \mathbb{R}^*$. Note that $f^{-1}(y) = x$ iff and only if $f(x) = y$. Hence to find a formula for the inverse of f we start with the formula $y = (2x-1)/x$ and solve for x. Solving for x we get that $x = 1/(2-y)$. Hence $f^{-1}(x) = 1/(2-x)$.

8.6. Image and pre-image of a function

DEFINITION 8.55. Let A and B be sets and let $f : A \to B$. Let $X \subseteq A$. The **image of X under f** is defined to be

$$f(X) = \{f(x) \mid x \in X\}.$$

EXAMPLE 8.56. Let $A = \{-1, 5, 10, \pi, 2.5, 17, 1, 13\}$ and $B = \{100, 21, 1.213, 6, 14, -1, 2\}$. Let $f : A \to B$ be defined as the function satisying $f(-1) = 100$, $f(5) = 21$, $f(10) = 14$, $f(\pi) = 14$, $f(2.5) = 1.213$, $f(17) = -1$, $f(1) = 2$, and $f(13) = -1$. Let $X = \{10, \pi, 2.5, 17\}$. Then

$$\begin{aligned} f(X) &= \{f(10), f(\pi), f(2.5), f(17)\} \\ &= \{14, 14, 1.213, -1\} \\ &= \{14, 1.213, -1\}. \end{aligned}$$

That is, we apply f to each element of X and see what we get. See Figure 23 for a picture of f and $f(X)$.

DEFINITION 8.57. Let A and B be sets and let $f : A \to B$. Let $Y \subseteq B$. The **inverse image of Y under f** is defined to be

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

EXAMPLE 8.58. Let A, B, and f be as in Example 8.56. Let $Y = \{6, -1, 2\}$. To calculate $f^{-1}(Y)$ one must find all $a \in A$ where $f(a) \in Y$. That is, follow the arrows backwards from Y. We see that $f(17)$, $f(1)$ and $f(13)$ are all in Y. Thus, $f^{-1}(Y) = \{17, 1, 13\}$. Note that no element of A maps to 6, which is in Y. See Figure 24 for a picture of f and $f^{-1}(Y)$.

PROPOSITION 8.59. *Suppose that X, Y, W, Z, A, B are sets. Let $f : X \to Y$, $W \subseteq X$, $Z \subseteq X$, $A \subseteq Y$, and $B \subseteq Y$. Then the following are true:*

(1) $f(W \cap Z) \subseteq f(W) \cap f(Z)$.
(2) $f(W \cup Z) = f(W) \cup f(Z)$.
(3) $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cup f^{-1}(B)$.

(4) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
(5) $X - f^{-1}(A) \subseteq f^{-1}(Y - A)$.
(6) $W \subseteq f^{-1}(f(W))$.

PROOF. Prove some of these and then leave the rest as exercises. See the exercises below and modify them to match up. ■

8.7. Application: Pythagorean triples

Consider a right triangle with sides x and y and hypotenuse z. See Figure 1. From the Pythagorean theorem, we know that triples of positive numbers (x, y, z) correspond to right triangles with sides x and y and hypotenuse z.

DEFINITION 8.60. We say that the triple (x, y, z) is a **Pythagorean triple** if x, y, and z are integers that satisfy the equation $x^2 + y^2 = z^2$ and where $z \neq 0$.

EXAMPLE 8.61. $(3, 4, 5)$ is a Pythagorean triple since $3^2 + 4^2 = 5^2$.
$(6, -8, 10)$ is a Pythagorean triple since $6^2 + (-8)^2 = 10^2$.
$(2, 1, 5)$ is not a Pythagorean triple since $2^2 + 1^2 \neq 5^2$.
$(1, 0, 1)$ is a Pythagorean triple since $1^2 + 0^2 = 1^2$. Note that the y coordinate of $(1, 0, 1)$ is zero.
$(0, 0, 0)$ is not a Pythagorean triple since the z-coordinate is zero.

TOO MUCH INFORMATION 8.62. Notice that there are "more" Pythagorean triples than there are right triangles with integer sides. For example, $(0, 1, 1)$ is a Pythagorean triple since $0^2 + 1^1 = 1^1$, even though there is no right triangle with side length 0. And $(-3, 4, -5)$ is a Pythagorean triple since $(-3)^2 + 4^1 = (-5)^1$, even though there is no right triangle with sides of negative length.

In this section we will answer the following questions.

QUESTIONS 8.63.
(1) How many Pythagorean triples are there? Are there an infinite number of them?
(2) If there are an infinite number of Pythagorean triples how do we generate all of them?

TOO MUCH INFORMATION 8.64. . Suppose that (x, y, z) is a Pythagorean triple. Then $x^2 + y^2 = z^2$. Let $\lambda \in \mathbb{Z}$ with $\lambda \neq 0$. Multiplying $x^2 + y^2 = z^2$ by λ^2 on both sides yields $(\lambda x)^2 + (\lambda y)^2 = (\lambda z)^2$. Hence $(\lambda x, \lambda y, \lambda z)$ is a Pythagorean triple.

EXAMPLE 8.65. The answer to Question 1 is that there are an infinite number of triples. Let us illustrate this fact with an example using the method of Remark 8.64. Let $(x, y, z) = (3, 4, 5)$. Multiplying $(3, 4, 5)$ by various values of λ gives the following:

$$\begin{array}{ccccc} & & \vdots & & \\ \lambda = -3 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (-9, -12, -15) \\ \lambda = -2 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (-6, -8, -10) \\ \lambda = -1 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (-3, -4, -5) \\ \lambda = 2 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (6, 8, 10) \\ \lambda = 3 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (9, 12, 15) \\ \lambda = 4 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (12, 16, 20) \\ & & \vdots & & \end{array}$$

We see that one can get an infinite number of solutions to $x^2 + y^2 = z^2$ given a starting solution. However, we can't get all the solutions starting with just $(3, 4, 5)$. We need more starting triples. For example, $(5, 12, 13)$ is a Pythagorean triple but it is not a multiple of $(3, 4, 5)$. Consider the triple $(297, 1620, 1647)$. Notice that 27 is a divisor of each of the numbers 297, 1620, and 1647. The triple $(297, 1620, 1647)$ comes from multiplying the triple $(11, 60, 61)$ by 27.

DEFINITION 8.66. Let x, y, and z be integers, not all zero. An integer d is a **common divisor** of x, y, and z if $d|x$, $d|y$, and $d|z$. We say that d is the **greatest common divisor** of x, y, and z if d is a positive common divisor of x, y, and z and $d \geq d'$ for every common divisor d' of x, y, and z. We write $d = \gcd(x, y, z)$ if d is the greatest common divisor of x, y, and z.

EXAMPLE 8.67. Let us calculate $\gcd(2, 4, 5)$. The divisors of 2 are 1 and 2. The divisors of 4 are 1, 2, and 4. The divisors of 5 are 1 and 5. There is only one common divisor of 2, 4, and 5. It is 1. Hence $1 = \gcd(2, 4, 5)$.

EXAMPLE 8.68. Let us calculate $\gcd(6, 12, 9)$. The divisors of 6 are 1, 2, 3, and 6. The divisors of 12 are 1, 2, 3, 6, and 12. The divisors

of 9 are 1, 3, and 9. The common divisors of 6, 12, and 9 are 1 and 3. Thus $\gcd(6, 12, 9) = 3$.

DEFINITION 8.69. Let (x, y, z) be a Pythagorean triple. We say that (x, y, z) is **primitive** if $\gcd(x, y, z) = 1$.

EXAMPLE 8.70. $(3, 4, 5)$ is primitive since $\gcd(3, 4, 5) = 1$.
$(297, 1620, 1647)$ is not primitive since $\gcd(297, 1620, 1647) = 27$.

LEMMA 8.71. *If (x, y, z) is a Pythagorean triple, then there exists a primitive Pythagorean triple (a, b, c) where $(x, y, z) = (\lambda \cdot a, \lambda \cdot b, \lambda \cdot c)$ for some integer λ. Moreover, $a = x/d$, $b = y/d$, and $c = z/d$ where $d = \gcd(a, b, c)$.*

PROOF. ⟨*We need to find a primitive triple that (x, y, z) is a multiple of. We do this by dividing x, y, and z by $\gcd(x, y, z)$*⟩
Let $d = \gcd(x, y, z)$.
Then $x = da$, $y = db$, and $z = dc$ for some integers a, b, c.
Note that $a = x/d$, $b = y/d$, and $c = z/d$.
Note that $x^2 + y^2 = z^2$ since (x, y, z) is a Pythagorean triple.
Therefore, $a^2 + b^2 = (x/d)^2 + (y/d)^2 = (z/d)^2 = c^2$.
Hence (a, b, c) is a Pythagorean triple.
⟨*We now show that (a, b, c) is primitive.*⟩
Suppose that k is a positive integer such that $k|a$, $k|b$, and $k|c$.
Hence $a = km$, $b = kn$, and $c = kr$ where m, n, r are integers.
So $x = (dk)m$, $y = (dk)n$, and $z = (dk)r$.
Thus $dk|x$, $dk|b$, and $dk|c$.
Hence dk is a common divisor of x, y, and z.
Therefore $d \geq dk$ since $d = \gcd(x, y, z)$.
On the other hand $dk \geq d$ since d and k are both positive integers.
We must have that $k = 1$.
Therefore $gcd(a, b, c) = 1$.
Hence (a, b, c) is a primitive Pythagorean triple. ■

TOO MUCH INFORMATION 8.72. Let (x, y, z) be a Pythagorean triple. We saw above that $(\lambda \cdot x, \lambda \cdot y, \lambda \cdot z)$ is a Pythagorean triple for any nonzero integer λ. Another way to generate triples from (x, y, z) is to multiply the components by -1. For example, $(3, 4, 5)$ generates the

triples $(3,4,5)$, $(3,4,-5)$, $(3,-4,5)$, $(3,-4,-5)$, $(-3,4,5)$, $(-3,4,-5)$, $(-3,-4,5)$, and $(-3,-4,-5)$.

EXAMPLE 8.73. $(30,-72,-78)$ is a Pythagorean triple.
Note that $(5,-12,-13)$ is a primitive Pythagorean triple and $(30,-72,-78) = (6\cdot 5, 6\cdot(-12), 6\cdot(-13))$.
Also, $(5,-12,-13)$ can be gotten by multiplying the second and third components of the positive triple $(5,12,13)$ by -1.
Hence, we may "generate" the triple $(30,-72,-78)$ from the positive primitive Pythagorean triple $(5,12,13)$.

TOO MUCH INFORMATION 8.74. The idea in Example 8.73 shows us that the problem of finding all Pythagorean triples boils down to the problem of finding all the positive, primitive Pythagorean triples. For let (x,y,z) be a Pythagorean triple. Then (x,y,z) is an integer multiple of a primitive Pythagorean triple (a,b,c) by Lemma 8.71. Multiplying the negative components of (a,b,c) by -1 gives us a positive, primitive Pythagorean triple.

Let Φ be the set of all non-negative, primitive Pythagorean triples. That is, let

$$\begin{aligned}\Phi &= \{(x,y,z) \mid x^2+y^2=z^2, x,y,z\in\mathbb{Z}, x\geq 0, y\geq 0, z>0, \gcd(x,y,z)=1\}\\ &= \{(1,0,1),(0,1,0),(3,4,5),(5,12,13),(7,24,25),(8,15,17),\ldots\}.\end{aligned}$$

Our goal is to find a formula that generates all of the elements of Φ. How will we accomplish this goal? We will use geometry! Consider the following set:

$$\widehat{U} = \{(r,s) \mid r^2+s^2=1, r\geq 0, s\geq 0, r,s\in\mathbb{Q}\}.$$

That is, $\widehat{U}$ is the set of rational points on the unit circle. See Figure 26 for a picture of $\widehat{U}$. See the note below the figure. For example $(3/5,4/5)$ is in $\widehat{U}$ since $3/5$ and $4/5$ are rational numbers and $(3/5)^2+(4/5)^2=1$. It turns out that there is a one-to-one correspondence between Φ and $\widehat{U}$. Consider the function

$$f:\Phi\to\widehat{U} \text{ given by } f(x,y,z)=(x/z,y/z). \tag{4}$$

For example, $(3,4,5)\in\Phi$ and $f(3,4,5)=(3/5,4/5)$. See Figure 27. Our goal is to show that f is a bijection. Once we have established this fact, we will give a formula to enumerate the elements of $\widehat{U}$. Then we will use the formula to give a formula for the elements of Φ.

We first show that f is one-to-one. We will need the following lemma.

LEMMA 8.75. *Let a, b, and c be integers with $a \neq 0$. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.*

PROOF. By Theorem 4.63 and the fact that $\gcd(a, b) = 1$, there exist integers x and y with $ax + by = 1$.
In addition we have that $bc = ak$ for some integer k since a divides bc.
Therefore, $acx + bcy = c$.
Hence $a(cx + by) = c$.
This gives that $a|c$. ■

PROPOSITION 8.76. *The function $f : \Phi \to \widehat{U}$ given by equation (4) is one-to-one.*

PROOF. Suppose that $(a, b, c), (x, y, z) \in \Phi$ with $x, y, z, a, b, c > 0$ and $f(x, y, z) = f(a, b, c)$.
⟨*We leave it to the reader to check the case where one of x, y, a, b are zero.*⟩
We have that $(x/z, y/z) = (a/c, b/c)$.
Hence $(a, b, c) = ((c/z) \cdot x, (c/z) \cdot y, (c/z) \cdot z)$.
By reducing the fraction c/z into lowest terms there exists $c'/z' \in \mathbb{Q}$ with $c'/z' = c/z$ and $\gcd(c', z') = 1$.
Hence $a = (c'/z') \cdot x$, $b = (c'/z') \cdot y$, and $c = (c'/z') \cdot z$.
Thus $az' = c'x$, $bz' = c'y$, and $cz' = c'z$.
So $z'|c'x$, $z'|c'y$, and $z'|c'z$.
By Lemma 8.75 and the fact that $\gcd(z', c') = 1$ we have that $z'|x$, $z'|y$, and $z'|z$.
Therefore $z' = 1$ since $\gcd(x, y, z) = 1$.
Similarly $c'|az'$, $c'|bz'$, and $c'|cz'$.
By Lemma 8.75 and the fact that $\gcd(z', c') = 1$ we have that $c'|a$, $c'|b$, and $c'|c$.
Therefore $c' = 1$ since $\gcd(a, b, c) = 1$.
This gives that $(a, b, c) = (x, y, z)$.
Hence f is one-to-one. ■

We now show that f is onto. As above, we need a lemma.

LEMMA 8.77. *Let a and b be integers, not both zero. Let $d = \gcd(a, b)$. Then $\gcd(a/d, b/d) = 1$.*

PROOF. We have that $a = dk$ and $b = dl$ for some integers k, l.
Suppose that m is a positive integer with $m|k$ and $m|l$.
Note that dm divides both a and b.
Hence dm is a common divisor of a and b.
Thus $d \geq dm$ because d is the greatest common divisor of a and b.
Therefore $m = 1$ since m is a positive integer.
Hence $\gcd(a/d, b/d) = \gcd(k, l) = 1$.

■

PROPOSITION 8.78. *The function $f : \Phi \to \widehat{U}$ given by equation (4) is onto.*

PROOF. Let $(x/y, w/z)$ be a rational point in $\widehat{U}$.
By reducing the fractions into lowest terms, we may assume that $\gcd(x, y) = 1$ and $\gcd(w, z) = 1$.
Let $d = \gcd(y, z)$.
We have that $(x/y)^2 + (w/z)^2 = 1$.
Hence $(xz)^2 + (wy)^2 = (yz)^2$.
Therefore $(xz/d)^2 + (wy/d)^2 = (yz/d)^2$.
Since $xy/d, wy/d$, and yz/d are integers, we have that $(xz/d, wy/d, yz/d)$ is a Pythagorean triple.
⟨*We now show that $(xz/d, wy/d, yz/d)$ is a primitive triple, which will complete the proof since $f(xy/d, wy/d, yz/d) = (x/y, w/z)$. We do this by contradiction.*⟩
Suppose that p is a prime with $p|(xz/d)$, $p|(wy/d)$, and $p|(yz/d)$.
Since $p|x \cdot (z/d)$, by Theorem 4.67, we have that $p|x$ or $p|(z/d)$.
Case 1: Suppose that $p|x$.
Since $p|w \cdot (y/d)$ we have that $p|w$ or $p|(y/d)$.
Note that p cannot divide y/d since if it did then p would divide y which can't happen since $\gcd(x, y) = 1$ and $p|x$ by assumption.
Suppose that p divides w.
Since $p|y \cdot (z/d)$ and p is prime, by Theorem 4.67, we have that $p|y$ or $p|z/d$.
Again p cannot divide y since $\gcd(x, y) = 1$.
Note that p cannot divide z/d since if it did then p would divide z

which can't happen since $\gcd(w, z) = 1$ and $p|w$ by assumption.
Hence p does not divide x.
Case 2: Suppose that $p|(z/d)$.
Hence $p|z$.
Since $p|w \cdot (y/d)$ we have that $p|w$ or $p|(y/d)$.
As above, p cannot divide w since $\gcd(z, w) = 1$ and $p|z$.
Note that p cannot divide y/d since $p|(z/d)$ and by Lemma 8.77 we have that $\gcd(y/d, z/d) = 1$.
Hence p does not divide z/d.

Therefore, there is no prime p with $p|(xz/d)$, $p|(wy/d)$, and $p|(yz/d)$.
Thus, $\gcd(xz/d, wy/d, yz/d) = 1$.
Hence, $(xz/d, wy/d, yz/d)$ is a primitive Pythagorean triple with $f(xz/d, wy/d, yz/d) = (x/y, w/z)$.
Therefore f is onto. ■

COROLLARY 8.79. *Let $(x/y, w/z)$ be a rational point in $\widehat{U}$ with $\gcd(x, y) = 1$ and $\gcd(w, z) = 1$. Let $d = \gcd(y, z)$. Then*

$$f^{-1}(x/y, w/z) = (xz/d, wy/d, yz/d)$$

PROOF. See the proof of Proposition 8.78. ■

EXAMPLE 8.80. $(8/17, 15/17) \in \widehat{U}$.
Set $x = 8$, $y = 17$, $w = 15$, $z = 17$, and $d = \gcd(17, 17) = 17$. Then by Corollary 8.79 we have that $f^{-1}(8/17, 15/17) = (8, 15, 17)$.

Define the function $g : \mathbb{Q} \cap [0, 1] \to \widehat{U}$ as follows: Let t be a rational number with $0 \leq t \leq 1$. Consider the line $y = tx + t$ that goes through the points $(-1, 0)$ and $(0, t)$. The line $y = tx + t$ intersects the unit circle $x^2 + y^2 = 1$ at two points. One of these points is $(-1, 0)$. Let $g(t)$ denote the other point. See Figure 28.

PROPOSITION 8.81.

$$g(t) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

PROOF. Suppose that $g(t) = (x, y)$.
Then $x^2 + y^2 = 1$ and $y = tx + t$.
Substituting $y = tx + t$ into $x^2 + y^2 = 1$ gives $x^2 + (tx + t)^2 = 1$.

This reduces to $(1+t^2)x^2 + (2t^2)x + (t^2-1) = 0$.
Using the quadratic formula we see that

$$\begin{aligned} x &= \frac{-2t^2 \pm \sqrt{(2t^2)^2 - 4(1+t^2)(t^2-1)}}{2(1+t^2)} \\ &= \frac{-2t^2 \pm 2}{2+2t^2} \\ &= \frac{1-t^2}{1+t^2} \text{ or } -1. \end{aligned}$$

Substituting $x = -1$ into $y = tx + t$ yields the point $(x, y) = (-1, 0)$.
Substituting $x = (1-t^2)(1+t^2)$ into $y = tx+t$ gives $y = 2t/(1+t^2)$. ■

EXAMPLE 8.82. See Figure 29 for a partial picture of the function g. As an example, $g(1/2) = ((1-(1/2)^2)/(1+(1/2)^2), 2(1/2)/(1+(1/2)^2) = (3/5, 4/5)$. The reader may wish to check that $g(0) = (1,0)$, $g(1/4) = (15/17, 8/17)$, and $g(3/4) = (7/25, 24/25)$.

PROPOSITION 8.83. *$g : \mathbb{Q} \cap [0,1] \to \widehat{U}$ is a well-defined bijection.*

PROOF. ⟨*We leave it to the reader to show that g is well-defined; see exercise* **??**.⟩
We first show that g is one-to-one.
Suppose that $g(t) = g(s)$ where s, t are rational numbers.
Then $g(t) = (x_1, tx_1 + t)$ and $g(s) = (x_2, sx_2 + s)$ for some real numbers x_1, x_2.
Thus $(x_1, tx_1 + t) = (x_2, sx_2 + s)$ since $g(t) = g(s)$.
Hence $x_1 = x_2$.
Substituting $x_1 = x_2$ into $tx_1 + t = sx_2 + s$ gives $t = s$.
Thus g is one-to-one.
We now show that g is onto.
Let $(a/b, c/d) \in \widehat{U}$.
Set $t = (c/d)/(a/b + 1)$.
Since $a/b + 1 \geq 1$ and $c/d \leq 1$, we see that $t = (c/d)/(a/b+1) \leq 1/1 = 1$.
Hence $t \in \mathbb{Q} \cap [0,1]$.
Using the facts that $a^2/b^2 + c^2/d^2 = 1$ and $-c^2/d^2 = a^2/b^2 - 1$ we have

that

$$\begin{aligned} g(t) &= \left(\frac{1-(c/d)^2/(a/b+1)^2}{1+(c/d)^2/(a/b+1)^2}, \frac{2((c/d)/(a/b+1))}{1+(c/d)^2/(a/b+1)^2}\right) \\ &= \left(\frac{(a/b+1)^2-(c/d)^2}{(a/b+1)^2+(c/d)^2}, \frac{2(c/d)(a/b+1)}{(a/b+1)^2+(c/d)^2}\right) \\ &= \left(\frac{a^2/b^2+2a/b+1-c^2/d^2}{a^2/b^2+2a/b+1+c^2/d^2}, \frac{2ac/bd+2c/d}{a^2/b^2+2a/b+1+c^2/d^2}\right) \\ &= \left(\frac{2a^2/b^2+2a/b}{2(a/b+1)}, \frac{(c/d)(2a/b+2)}{2(a/b+1)}\right) \\ &= (a/b, c/d). \end{aligned}$$

Hence g is onto. ■

EXAMPLE 8.84. The main idea now is to look at the function $f^{-1} \circ g : \mathbb{Q} \cap [0,1] \to \Phi$. We will see in Theorem 8.87 that $f^{-1} \circ g$ is a bijection. Hence we may enumerate the elements of Φ by plugging rational numbers in the interval $[0,1]$ into $f^{-1} \circ g$. For example, plugging $t = 2/3$ into $f^{-1} \circ g$ gives

$$\begin{aligned} f^{-1}(g(2/3)) &= f^{-1}(\big((3^2-2^2)/(3^2+2^2), (2\cdot 3\cdot 2)/(3^2+2^2)\big)) \\ &= f^{-1}((5/13, 12/13)) = (5,12,13). \end{aligned}$$

Similarly, plugging $t = 3/5$ into $f^{-1} \circ g$ gives

$$\begin{aligned} f^{-1}(g(3/5)) &= f^{-1}(\big((5^2-3^2)/(5^2+3^2), (2\cdot 5\cdot 3)/(5^2+3^2)\big)) \\ &= f^{-1}((8/17, 15/17)) = (8,15,17). \end{aligned}$$

See Figure 30 for a picture of the above computations.

TOO MUCH INFORMATION 8.85. In Theorem 8.87 we give a formula to enumerate all of the non-negative Pythagorean triples. There is one slight wrinkle that we wish to clarify before getting to the theorem. The formula for f^{-1} given in Corollary 8.79 says that $f^{-1}(x/y, w/z) = (xz/d, wy/d, yz/d)$ where $\gcd(x,y) = 1$ and $\gcd(w,z) = 1$ and $d = \gcd(y,z)$. We will be plugging $g(m/n) = ((n^2-m^2)/(n^2+m^2), 2mn/(n^2+m^2))$ into f^{-1}. The issue that we will confront is that we may have $\gcd((n^2-m^2)/(n^2+m^2)) \neq 1$ and/or $\gcd((2mn)/(n^2+m^2)) \neq 1$. However we will discover when this occurs and correct the problem. It turns out that we will just need to divide the numbers n^2-m^2, n^2+m^2, and $2mn$ by the number 2. We work this out in Lemma 8.86.

LEMMA 8.86. *Let m and n be integers with $n \geq m \geq 0$, $n \neq 0$, and* $\gcd(m, n) = 1$.

(1) *If m is odd and n is even, or if m is even and n is odd, then* $\gcd(n^2 - m^2, n^2 + m^2) = 1$ *and* $\gcd(2mn, n^2 + m^2) = 1$.
(2) *If m is odd and n is odd, then* $\gcd((n^2-m^2)/2, (n^2+m^2)/2) = 1$ *and* $\gcd(mn, (n^2 + m^2)/2) = 1$.

PROOF. (1) Suppose that m is odd and n is even, or m is even and n is odd.
Then $n^2 - m^2$ and $n^2 + m^2$ are both odd.
We will show that there is no odd prime p that is a common divisor of $n^2 - m^2$ and $n^2 + m^2$.
⟨*We may assume that p is odd since $n^2 - m^2$ and $n^2 + m^2$ are both odd.*⟩
Suppose that such a p exists.
Then p divides $(n^2 - m^2) + (n^2 + m^2) = 2n^2$ and $(n^2 + m^2) - (n^2 - m^2) = 2m^2$.
Since p is odd and $p|2n^2$, we have that $p|n$ by Theorem 4.67.
Similarly $p|m$.
But then $\gcd(m, n) \geq p$ which is a contradiction.
Thus, $\gcd(n^2 - m^2, n^2 + m^2) = 1$.
We now show that $\gcd(2mn, n^2 + m^2) = 1$.
Again suppose that p is a prime that is a common divisor of $2mn$ and $n^2 + m^2$.
Since $n^2 + m^2$ is odd we must have that p is odd.
Since p is odd and $p|2mn$ we must have that $p|m$ or $p|n$ by Theorem 4.67.
If $p|m$ then since $p|n^2 + m^2$ we must have that $p|n$.
This can't happen since $\gcd(m, n) = 1$.
Similarly if $p|n$ then since $p|n^2 + m^2$ we must have that $p|m$.
This can't happen since $\gcd(m, n) = 1$.
Thus, no such p exists.
Therefore, $\gcd(2mn, n^2 + m^2) = 1$.
(2) We leave this case to the reader. See Exercise 1.

■

THEOREM 8.87. *Let m and n be integers with $n \geq m \geq 0$, $n \neq 0$, and* $\gcd(m, n) = 1$.

(1) *If m is odd and n is even, or if m is even and n is odd, then $(n^2 - m^2, 2mn, m^2 + n^2)$ is a non-negative, primitive, Pythagorean triple.*
(2) *If m and n are both odd then $((n^2 - m^2)/2, mn, (m^2 + n^2)/2)$ is a non-negative, primitive, Pythagorean triple.*

Furthermore, all non-negative, primitive Pythagorean triples are of one of the above forms.

PROOF. By Proposition 8.83, $g : \mathbb{Q} \cap [0, 1] \to \widehat{U}$ is a bijection.
By Propositions 8.76 and 8.78, $f : \Phi \to \widehat{U}$ is a bijection.
By Proposition 8.53, $f^{-1} : \widehat{U} \to \Phi$ is a bijection.
By Corollary 8.49, $f^{-1} \circ g : \mathbb{Q} \cap [0, 1] \to \Phi$ is a bijection.
Let $t \in \mathbb{Q} \cap [0, 1]$.
Then $t = m/n$ where $n \geq m \geq 0$, $n \neq 0$, and $\gcd(m, n) = 1$.
By Proposition 8.81,

$$\begin{aligned} g(t) &= \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) \\ &= \left(\frac{1 - (m/n)^2}{1 + (m/n)^2}, \frac{2m/n}{1 + (m/n)^2}\right) \\ &= \left(\frac{n^2 - m^2}{n^2 + m^2}, \frac{2mn}{n^2 + m^2}\right) \end{aligned}$$

We now use Corollary 8.79 to compute the $f^{-1}(g(t))$.
We break this into two cases.
Case 1: Suppose that m is odd and n is even, or m is even and n is odd.
By Lemma 8.86 $\gcd(n^2 - m^2, n^2 + m^2) = 1$ and $\gcd(2mn, n^2 + m^2) = 1$.
Note that $\gcd(n^2 + m^2, n^2 + m^2) = n^2 + m^2$.
By Corollary 8.79 we have that

$$f^{-1}\left(\frac{n^2 - m^2}{n^2 + m^2}, \frac{2mn}{n^2 + m^2}\right) = (n^2 - m^2, 2mn, n^2 + m^2).$$

Case 2: Suppose that m is odd and n is odd.
By Lemma 8.86 $\gcd((n^2 - m^2)/2, (n^2 + m^2)/2) = 1$ and $\gcd(mn, (n^2 + m^2)/2) = 1$.
By Corollary 8.79 we have that

$$\begin{aligned} f^{-1}\left(\frac{n^2 - m^2}{n^2 + m^2}, \frac{2mn}{n^2 + m^2}\right) &= f^{-1}\left(\frac{(n^2 - m^2)/2}{(n^2 + m^2)/2}, \frac{mn}{(n^2 + m^2)/2}\right) \\ &= ((n^2 - m^2)/2, mn, (n^2 + m^2)/2). \end{aligned}$$

■

8.8. Exercises

8.8.1. Exercises for section 8.1.

(1) Recall Example 8.11. Consider the function $\pi_4 : \mathbb{Z} \to \mathbb{Z}_4$ given by $\pi_4(k) = \overline{k}$. Calculate $\pi_4(k)$ for all integers k with $-6 \leq k \leq 6$. Then draw a picture of π_4. What is the range of π_4?

8.8.2. Exercises for section 8.2.

(1) Let $n \geq 2$ be an integer. Let a and b be any integers. Let $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ be given by $f_a(\overline{x}) = \overline{a} \cdot \overline{x}$ as in Exercise 8.18.
   (a) Prove that $f_{ab} = f_{ba}$.
   (b) Prove: If $a \equiv b (\text{mod } n)$, then $f_a = f_b$.

(2) Let $f : \mathbb{Q} \to \mathbb{Z}$ be defined by $f(m/n) = m$. For example, $f(2/9) = 2$ and $f(5/10) = 5$. Is f a well-defined function? If so prove it. If not explain why not.

(3) Let n be an integer with $n \geq 2$. Let a and b be integers with $a \equiv b (\text{mod } n)$. Prove that $\gcd(a, n) = \gcd(b, n)$. Show that this implies that $f : \mathbb{Z}_n \to \mathbb{Z}$ defined by $f(\overline{x}) = \gcd(x, n)$ is a well-defined function.

(4) Let n and m be an integers with $n \geq 2$ and $m \geq 2$. Define the function $h : \mathbb{Z}_n \to \mathbb{Z}_m$ by the formula $h(\overline{x}) = \overline{x}$. For example, if $n = 6$ and $m = 3$ then $h(\overline{5}) = \overline{5} = \overline{2}$.
   (a) Consider $h : \mathbb{Z}_5 \to \mathbb{Z}_2$ defined as above. Show that h is not well-defined by considering $h(\overline{3})$ and $h(\overline{8})$.
   (b) Prove that h is well-defined if m divides n. That is, show that if $\overline{x} = \overline{y}$, then $h(\overline{x}) = h(\overline{y})$.

(5) Let $S = \mathbb{R} \times \mathbb{R}$. Define the relation $\sim$ where $(a, b) \sim (c, d)$ iff $a^2 + b^2 = c^2 + d^2$. Recall from Chapter 7, Exercise 2 that $\sim$ is an equivalence relation. Define the function $f(\overline{(a, b)}) = a^2 + b^2$. Prove that f is a well-defined function.

(6) Consider the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f(\overline{x}) = \overline{2} \cdot \overline{x} + \overline{1}$. Is f a well-defined function? Prove or disprove.

(7) Consider the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f(\overline{x}) = \overline{x}^2 + \overline{x}$. Is f a well-defined function? Prove or disprove.

8.8.3. Exercises for section 8.3.

(1) Consider the following functions. For each function f, (a) either prove that f is one-to-one or give an example to show

otherwise, and (b) either prove that f is onto, or give an example to show otherwise. You will need the following definition. Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices with entries from the real numbers. That is,

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

For example, $\begin{pmatrix} 1 & 0 \\ -10 & \pi \end{pmatrix}$ is an element of $M_2(\mathbb{R})$.

(a) Let $A = \{2n | n \in \mathbb{Z}\}$. This set is commonly referred to as $2\mathbb{Z}$. Let $f : \mathbb{Z} \to A$ given by $f(k) = 2k$. For example, $f(7) = 2 \cdot 7 = 14$.
(b) $f : \mathbb{Q} \to \mathbb{Q}$ where $f(x) = x^3$.
(c) $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$.
(d) $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = 2x$.
(e) $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^4 - 16$.
(f) $f : M_2(\mathbb{R}) \to \mathbb{R}$ where $f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d$.
(g) $f : M_2(\mathbb{R}) \to \mathbb{R}$ where $f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc$.

(2) Let $A = \{1, 2, 3, 4\}$ and $B = \{7, 8, -1, \pi, 1/2\}$.
   (a) Give an example of a function $f : A \to B$ that is one-to-one.
   (b) Give an example of a function $f : A \to B$ that is not one-to-one.
   (c) Give an example of a function $f : B \to A$ that is onto.
   (d) Give an example of a function $f : B \to A$ that is not onto.

(3) Suppose that $f : A \to B$ and $g : B \to C$. Prove: If f is not one-to-one, then $g \circ f$ is not one-to-one.

(4) Suppose that $f : A \to B$ and $g : B \to C$. Prove: If g is not onto, then $g \circ f$ is not onto.

(5) Give an example of $f : A \to B$ and $g : B \to C$ where the following are true:
   (a) f is not onto, but $g \circ f$ is onto.
   (b) g is not one-to-one, but $g \circ f$ is one-to-one.

(6) Consider the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f(\overline{x}) = \overline{x}^2$. Recall from Check for understanding 8.19 that f is a well-defined function. Recall from Example 8.27 that f is not one-to-one.
   (a) If n is even, show that the range of f equals the set

$$\left\{ \overline{x}^2 \mid \overline{x} = \overline{0}, \overline{1}, \ldots, \overline{n/2} \right\}$$

(b) If n is odd, show that the range of f equals the set

$$\left\{\overline{x}^2 \mid \overline{x} = \overline{0}, \overline{1}, \ldots, \overline{(n-1)/2}\right\}$$

(c) If $n > 2$, prove that f is not onto.

(7) Let n be an integer with $n \geq 2$. Let a be an integer. Define $g_a : \mathbb{Z}_n \to \mathbb{Z}_n$ by the formula $g_a(\overline{x}) = \overline{x} + \overline{a}$.
   (a) Prove that g_a is well-defined.
   (b) Draw a picture of g_3 and g_4 when $n = 4$.
   (c) Prove that g_a is one-to-one for general n.
   (d) Prove that g_a is onto for general n.

(8) Let $n \geq 2$ be an integer. Let a be any integer. Let $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ be given by $f_a(\overline{x}) = \overline{a} \cdot \overline{x}$ as in Exercise 8.18. Recall from Proposition 8.41 that if $\gcd(a, n) = 1$, then f_a is a bijection. Prove that if $\gcd(a, n) > 1$, then f_a is not a bijection. [Hint: Note that $f_a(\overline{0}) = \overline{0}$. Find $\overline{k} \neq \overline{0}$ with $f_a(\overline{k}) = \overline{0}$.]

(9) Let n and m be an integers with $n \geq 2$ and $m \geq 2$. Define the function $h : \mathbb{Z}_n \to \mathbb{Z}_m$ by the formula $h(\overline{x}) = \overline{x}$ as in Exercise 4.
   (a) Draw $h : \mathbb{Z}_6 \to \mathbb{Z}_3$.
   (b) If $m|n$ prove that $h : \mathbb{Z}_n \to \mathbb{Z}_m$ is onto but not one-to-one.

8.8.4. Exercises for section 8.4.

(1) Prove that $g \circ f$ defined in Definition 8.43 is actually a function. That is, show that $g \circ f$ satisfies the conditions of Definition 8.1.

(2) Let $n \geq 2$ be an integer. Let a and b be any integers. Let $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ be given by $f_a(\overline{x}) = \overline{a} \cdot \overline{x}$ as in Exercise 8.18. Prove that $f_a \circ f_b = f_{ab}$.

8.8.5. Exercises for section 8.5.

(1) Show that f^{-1} defined in Definition 8.50 is a well-defined function.

(2) Let $A = \{1, 2, 3, 4\}$. Let $i_A : A \to A$ be the identity function on A.
   (a) Let $f : A \to A$ where $f(1) = 3$, $f(2) = 1$, $f(3) = 2$, and $f(4) = 4$. Draw a picture of f. Draw a picture of f^{-1}. Show that $f \circ f^{-1} = i_A$ and $f^{-1} \circ f = i_A$.
   (b) Let $g : A \to A$ where $g(1) = 1$, $g(2) = 3$, $g(3) = 4$, and $g(4) = 2$. Draw a picture of g. Draw a picture of g^{-1}. Show that $g \circ g^{-1} = i_A$ and $g^{-1} \circ g = i_A$.

8.8.6. Exercises for section 8.6.

(1) Let $\pi_6 : \mathbb{Z} \to \mathbb{Z}_6$ be the reduction modulo 6 map defined by $\pi_6(n) = \overline{n}$. For example, $\pi_6(2) = \overline{2}$ and $\pi_6(18) = \overline{18} = \overline{0}$ since $18 \equiv 0 (\text{mod } 6)$.
   (a) Calculate $\pi_6(-1)$, $\pi_6(10)$, $\pi_6(7)$, and $\pi_6(-17)$. Draw a picture of the π_6 map.
   (b) Let $X = \{1, 17, -5, 102, -13\}$. Calculate $\pi_6(X)$.
   (c) Let $Y = \{\overline{0}\}$. Prove that $\pi_6^{-1}(Y) = \{6k | k \in \mathbb{Z}\}$. This set is commonly referred to as $6\mathbb{Z}$.
   (d) Let $Y = \{\overline{1}\}$. Prove that $\pi_6^{-1}(Y) = \{6k + 1 | k \in \mathbb{Z}\}$.
   (e) What is $\pi_6^{-1}(\{\overline{0}, \overline{3}\})$ equal to?

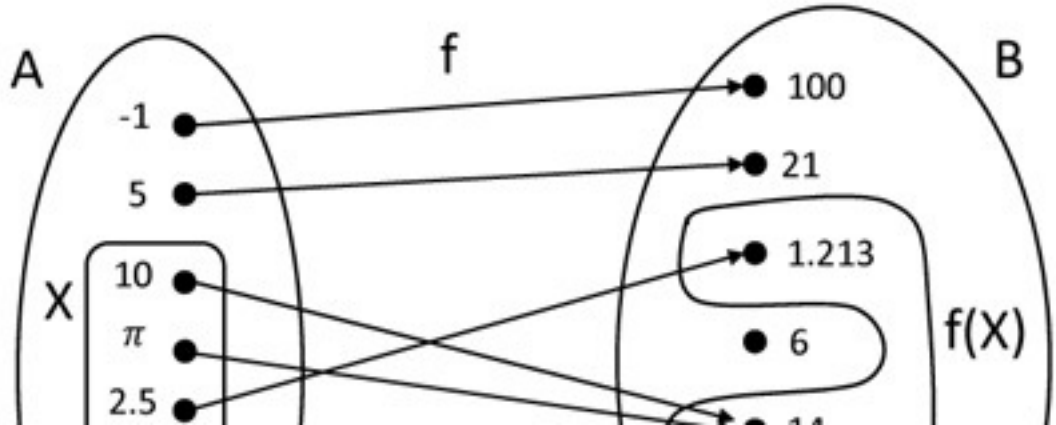
(2) Let $A = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots\}$. Let $f : A \times A \to A$ where $f((m, n)) = m^2 + n^2$.
   (a) Calculate $f(3, 5)$, $f(1, 1)$, and $f(2, 1)$.
   (b) Let $C = \{(0, 0), (1, 10), (2, 5)\}$. Calculate $f(C)$.
   (c) Let $B = \{1, 2, 3, 4\}$. Find $f^{-1}(B)$.
   (d) Show that f is not one-to-one.
   (e) Show that f is not onto.

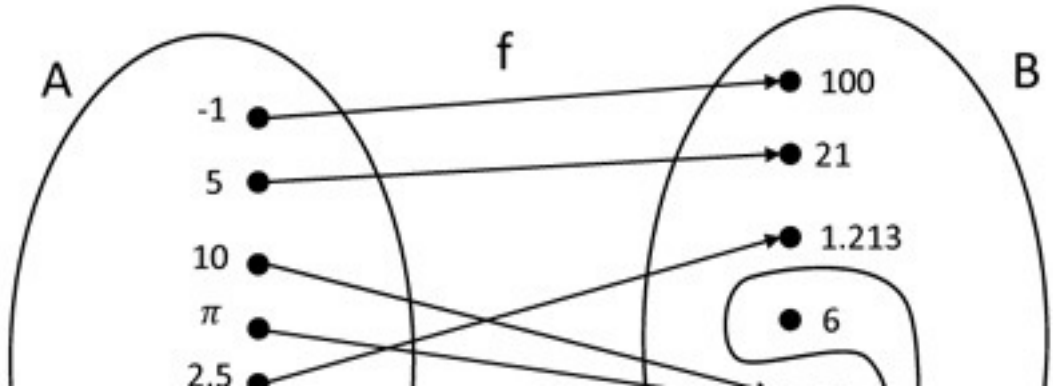
(3) Let $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2 - 2$.
   (a) $f^{-1}([0, 1))$
   (b) $f([0, 1])$
   (c) $f^{-1}([-3, -1))$

(4) Suppose that X, Y, W, Z, A, B are sets. Let $f : X \to Y$, $W \subseteq X$, $Z \subseteq X$, $A \subseteq Y$, and $B \subseteq Y$.
   (a) Prove that $f(W \cup Z) = f(W) \cup f(Z)$.
   (b) Prove that $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
   (c) Prove that $X - f^{-1}(A) \subseteq f^{-1}(Y - A)$.
   (d) Ptove that $W \subseteq f^{-1}(f(W))$.

8.8.7. Exercises for section 8.7.

(1) Prove part 2 of Lemma 8.86.


A
f
B
-1
5
X
10
π
2.5
100
21
1.213
6
f(X)


A
f
B
-1
5
10
π
2.5
100
21
1.213
6

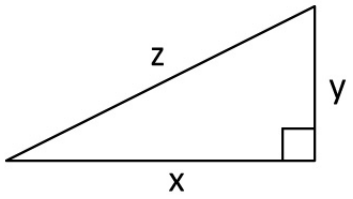


FIGURE 25. A right triangle

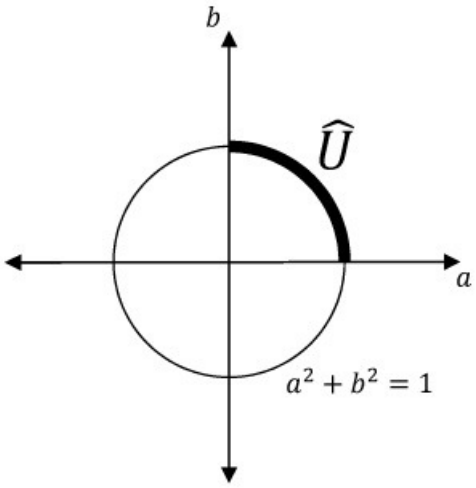


FIGURE 26. $\widehat{U}$ consists of the rational points in the first quadrant of the unit circle. We have drawn $\widehat{U}$ as a solid curve even though there are holes at the irrational points on the unit circle.

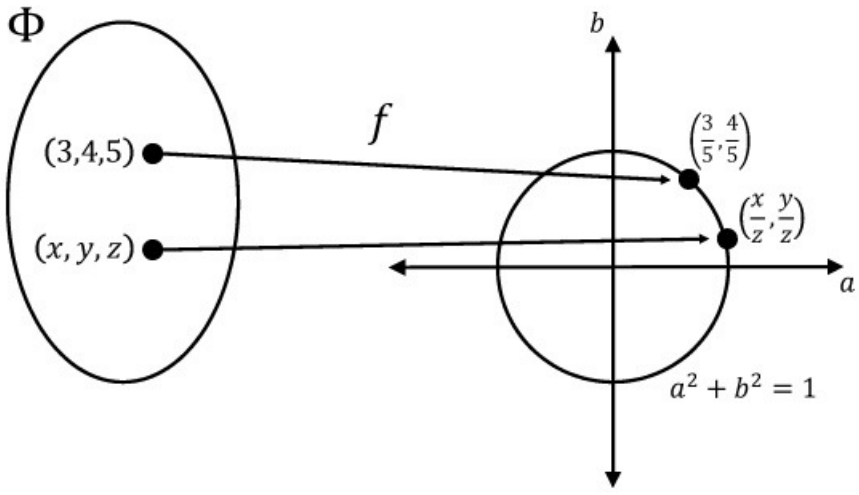

Φ
(3,4,5)
(x, y, z)
f
b
a
$\left(\frac{3}{5},\frac{4}{5}\right)$
$\left(\frac{x}{z},\frac{y}{z}\right)$
$a^2 + b^2 = 1$

FIGURE 27.

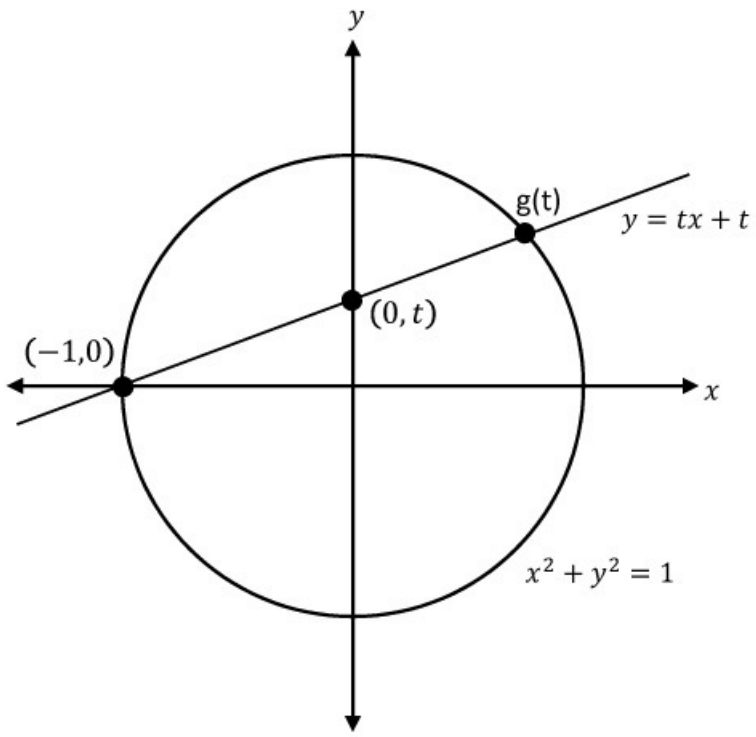


FIGURE 28.

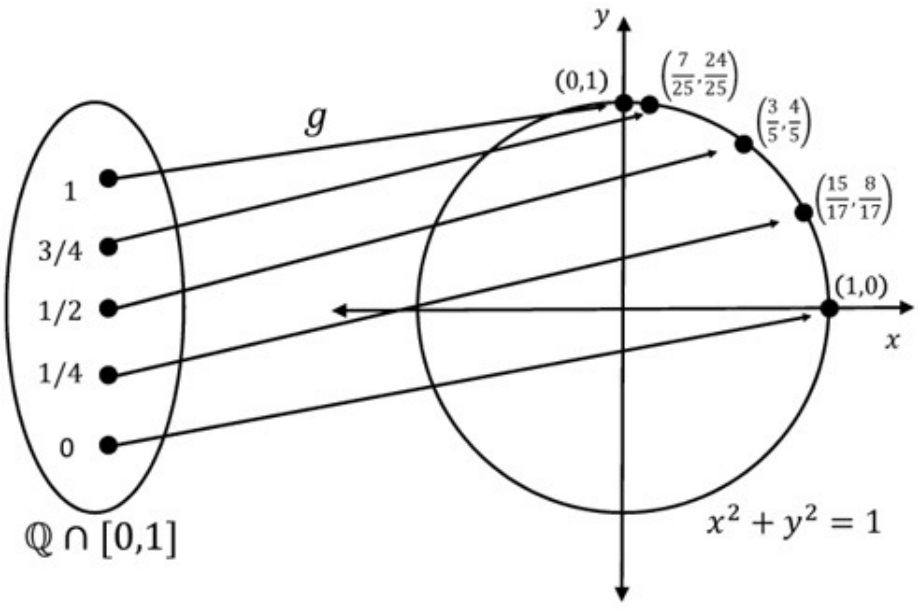


FIGURE 29. A partial picture of the function g

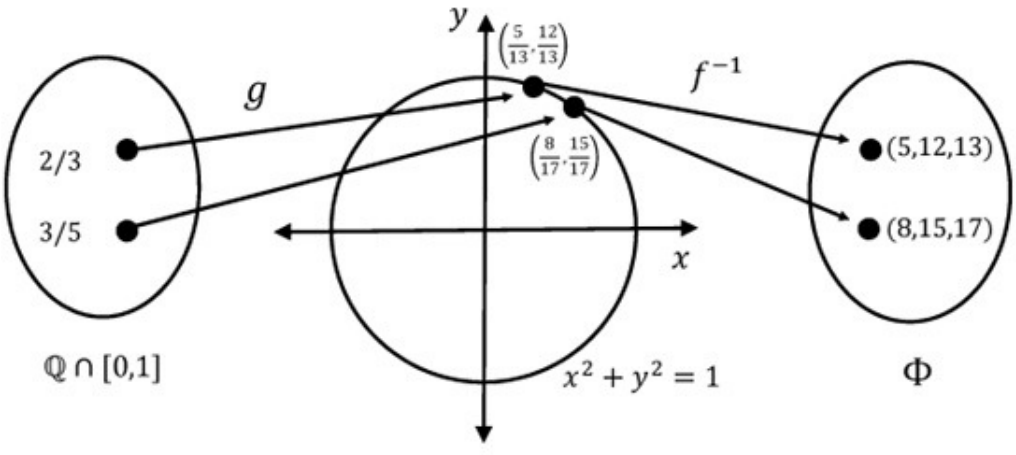


FIGURE 30. $f^{-1} \circ g : \mathbb{Q} \cap [0,1] \to \Phi$

m/n	$(f^{-1} \circ g)(m/n)$	m/n	$(f^{-1} \circ g)(m/n)$
0	$(1, 0, 1)$	4/5	$(9, 40, 41)$
1/2	$(3, 4, 5)$	1/6	$(35, 12, 37)$
1/3	$(4, 3, 5)$	5/6	$(11, 60, 61)$
2/3	$(5, 12, 13)$	1/7	$(24, 7, 25)$
1/4	$(15, 8, 17)$	2/7	$(45, 28, 53)$
3/4	$(7, 24, 25)$	3/7	$(20, 21, 29)$
1/5	$(12, 5, 13)$	4/7	$(33, 56, 65)$
2/5	$(21, 20, 29)$	5/7	$(12, 35, 37)$
3/5	$(8, 15, 17)$	6/7	$(13, 84, 85)$

FIGURE 31. Table of some values of $f^{-1} \circ g$.

Chapter 9

Cardinality

Infinity? That could take forever!

Jason Andrew Scally,
Mastermind

9.1. Cardinality of a set

In this chapter we define one notion of the "size" of a set. Consider the set $A = \{10, 5, -3, 4\}$ and the set $B = \{-100, \pi, \frac{1}{2}, 7\}$. Do A and B have the same size? You might think "Of course they do! They each have four elements." How did you figure that out? You counted the number of elements of A and then you counted the number of elements of B. Both times you got four. What if you couldn't count? How could you tell if two sets have the same size? One way to do this is to pair the elements in the sets. That is, make a correspondence between the two sets. See Figure 1. Since we are able to pair all of the elements of A with all of the elements of B in a one-to-one way, we may conclude that the two sets have the same size.

Now consider the sets $C = \{1, 4, -10\}$ and $D = \{3, 10, 5, 1\}$. Do these two sets have the same size? If we try to make a one-to-one correspondence between the sets C and D we see that we cannot do it. This is because we don't have enough elements in C. See Figure 2 for an attempt at making a correspondence.

How can we mathematically formulate a definition that embodies the above ideas? Do we have a mathematical object that is the same as a one-to-one correspondence between two sets? Yes! A bijection.

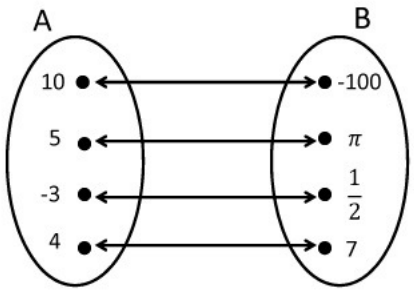


FIGURE 1. A correspondence between A and B

The next definition makes this precise. Note that instead of saying that A and B have the same "size" we say that A and B have the same "cardinality." This is because we will use this definition for infinite sets too and the word "size" has too much association with finite sets.

DEFINITION 9.1. Let A and B be sets. We say that A and B have the same **cardinality** if there exists a bijection $f : A \to B$. If this is the case, then we write $A \approx B$. Otherwise we write $A \not\approx B$.

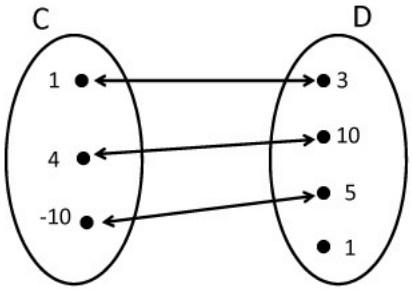


FIGURE 2. A failed attempt at a correspondence between C and D

TOO MUCH INFORMATION 9.2. Suppose that $f : A \to B$ is a bijection. Then f has a inverse function by ???? and $f^{-1} : B \to A$ is a bijection. Thus, $A \approx B$ if and only if $B \approx A$. So $\approx$ is well-defined; that is, the order of the sets does not matter in Definition 9.1.

9.2. Finite sets

THEOREM 9.3. *Let A be a finite set and $f : A \to A$. Then f is one-to-one if and only if f is onto.*

PROOF. put the easiest possible proof here. ■

Examples from number theory

Let us give an application of Theorem 9.3.

PROPOSITION 9.4. *Let $\overline{a} \in \mathbb{Z}_n$. Let $f : \mathbb{Z}_n \to \mathbb{Z}_n$ be defined by $f(\overline{k}) = \overline{a}\overline{k}$. If $\gcd(a, n) = 1$, then f is one-to-one and onto.*

PROOF. We will prove that f is one-to-one. By Theorem 9.3, this implies that f is onto. The main idea is to get an "inverse" for a. We do this as follows.

By Theorem 4.63, since $\gcd(a, n) = 1$ there exists integers x and y where $ax + ny = 1$. Therefore, by ?????? $\overline{a} \cdot \overline{x} + \overline{n} \cdot \overline{y} = \overline{1}$. Since $\overline{n} = \overline{0}$ we see that $\overline{a} \cdot \overline{x} = \overline{1}$.

Now suppose that $f(\overline{c}) = f(\overline{d})$. Then $\overline{a} \cdot \overline{c} = \overline{a} \cdot \overline{d}$. Multiplying both sides by $\overline{x}$ gives that $\overline{x} \cdot \overline{a} \cdot \overline{c} = \overline{x} \cdot \overline{a} \cdot \overline{d}$. Since $\overline{a} \cdot \overline{x} = \overline{1}$ we see that $\overline{c} = \overline{d}$. Therefore, f is one-to-one. ■

9.3. Countable sets

Infinite sets are rather strange objects. Let us begin with a journey to Hilbert's hotel.

One day, after much traveling, Tom arrived at a hotel. He was very tired, so he was excited to find a hotel. As Tom got closer to the hotel, he noticed some strange things. The hotel consisted of a hotel office and what appeared to be an infinite number of hotel bungalos numbered $1, 2, 3, 4, \ldots$. In fact, Tom could not see the end of the hotel bungalos. And what was worse, Tom noticed that the hotel office had the sign "no vacancies!" With so many hotel bungalos, Tom wondered how there could possibly be no vacancies. So he decided to walk up to the hotel office. As Tom approached the hotel office a man appeared. "Good afternoon. My name is Professor Hilbert," said Hilbert the hotel manager, "would you like a room?" Tom replied "Yes, I would. But I noticed that you have no vacancies." Hilbert replied "that is true, but I think something can be done. Please fill out these forms while

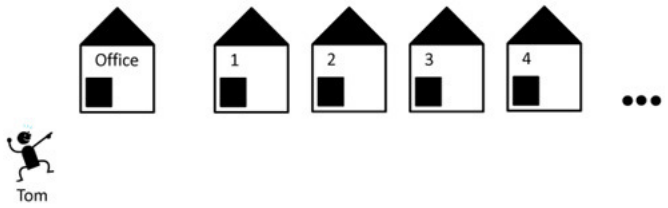


FIGURE 3.

I prepare your room." As Tom filled out the forms, he saw Hilbert walk over to the telephone and push a button that said "broadcast to all rooms." Hilbert pushed the button, picked up the phone, and said "Good afternoon hotel residents. I am sorry to disturb you. We must make room for another hotel guest. If you would be so kind. Could everyone please collect their belongings and in precisely ten minutes step out of their hotel rooms and move to the hotel room that is one number higher. Thank you for your understanding. A maid will be

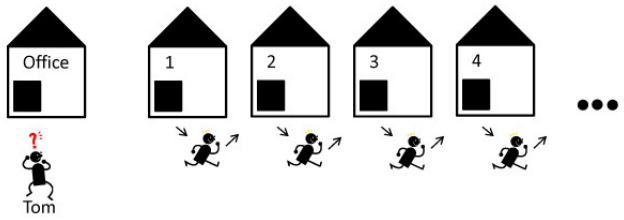


FIGURE 4.

in today to clean your rooms." When Hilbert returned to the desk, Tom said "Professor Hilbert, I don't understand. If all your rooms are occupied, how can there possibly be a room for me?" Professor Hilbert replied "My dear gentleman, I have an infinite number of hotel bungalos. If each person moves one bungalo over, then bungalo number one will be open and I can let you stay there for the evening." Tom seemed puzzled and replied "But what will happen to the person staying in the last bungalo? Where will they go?" Hilbert replied "there is no last bungalo. Just wait and see." After ten minutes Tom saw every bungalo door open and each person step out and move one bungalo

over. Hilbert then handed Tom the key for bungalo number 1 and said "Here you go Mr. Tom. Have a nice stay at my hotel."

You might be thinking to yourself "What went on in the above example?" Welcome to the land of infinite sets. We are going to notice that strange things happen in this land. We begin with countable sets.

Talk about countable sets.

9.4. Uncountable sets

Talk about uncountable sets.

9.5. Cantor-Schroeder-Bernstein Theorem

Talk about this theorem.

9.6. Exercises

(1) Find a bijection $f : \mathbb{N} \to A$ where
$$A = \{1, \frac{1}{3}, \frac{1}{9}, \frac{1}{27}, \frac{1}{81}, \ldots\}.$$
Prove that your answer is a bijection.
(2) Show that the set of odd integers O is countably infinite.
(3) Show that the set of even integers E is countably infinite.
(4) Find a bijection $f : (-1, 3) \to (0, 4)$. This shows that $(-1, 3) \simeq (0, 4)$.
(5) Let $n \geq 2$. Let $a \in \mathbb{Z}$. Prove that
$$\overline{a} = \{x \mid x \equiv a(\text{mod n})\}$$
is countably infinite.
(6) Suppose that A is countably infinite. Let x be some element of A. Prove that $A - \{x\}$ is countably infinite.
(7) Suppose that A and B are countably infinite. Show that $A \times B$ is countably infinite. [Hint: Start with $A = \{a_1, a_2, a_3, \ldots\}$ and $B = \{a_1, a_2, a_3, \ldots\}$. Find a bijection $f : \mathbb{N} \to A \times B$. Think about $\mathbb{Q}$.]

9.7. Fun math facts.

Talk about the continuum hypothesis.

Part 3

Extras

Chapter 10

Number Theory

10.1. Gaussian integers

Throughout this section let i denote the complex number where $i^2 = -1$.

DEFINITION 10.1. The set

$$\mathbb{Z}[i] = \{a + bi \mid a, b\mathbb{Z}\}$$

is called the set of **Gaussian integers**.

Given $a + bi$ and $c + di$ in $\mathbb{Z}[i]$. Recall that

$$\begin{aligned}
(a + bi) + (c + di) &= (a + c) + (b + d)i \\
(a + bi) - (c + di) &= (a + c) - (b + d)i \\
(a + bi)(c + di) &= (ac - bd) + (ad + bc)i \\
\frac{a + bi}{c + di} &= \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i
\end{aligned}$$

DEFINITION 10.2. Let $z = a + bi$ be a Gaussian integer. The **conjugate** of z is $\overline{z} = a - bi$. The **norm** of z is $N(z) = z\overline{z} = a^2 + b^2$. The **absolute value** of z is $|z| = \sqrt{a^2 + b^2}$.

PROPOSITION 10.3. *Let $z, w \in \mathbb{Z}[i]$. Then*

(1) $N(z)$ *is a real number and* $N(z) \geq 0$.
(2) $N(z) = 0$ *if and only if* $z = 0$.
(3) $N(zw) = N(z)N(w)$.

PROOF. ⟨*Parts (1) and (2) follow from the definition of* $N(z)$ *and are left to the reader. We prove part (3)*⟩

Let $z = a + bi$ and $w = c + di$ where $a, b, c, d \in \mathbb{Z}$.
Then

$$\begin{aligned} N(zw) &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(z)N(w). \end{aligned}$$

■

EXAMPLE 10.4. Note that $2 = (1 + i)(1 - i)$ and $N(2) = 4$, $N(1 + i) = 2$, and $N(1 - i) = 2$.

DEFINITION 10.5. Let $z \in \mathbb{Z}[i]$. We say that z is a **unit** if there exists $w \in \mathbb{Z}[i]$ with $zw = 1$. That is, z is a unit if $1/z$ is a Gaussian integer.

EXAMPLE 10.6. i and $-i$ are units since $i \cdot (-i) = 1$. 1 and -1 are units because $1 \cdot 1 = 1$ and $(-1)(-1) = 1$.

PROPOSITION 10.7. *Let* $z \in \mathbb{Z}[i]$. *Then* z *is a unit if and only if* $N(z) = 1$. *More specifically the units of* $\mathbb{Z}[i]$ *are* 1, -1, i, *and* $-i$.

PROOF. Suppose that the Gaussian integer z is unit.
Then there exists a Gaussian integer w with $zw = 1$.
By Proposition 10.3, $N(z)N(w) = 1$.
Thus $N(z) = 1$ since $N(z)$ is a non-negative integer.

Conversely, suppose that $z = a + bi$ is a Guassian integer with $N(z) = 1$.
Therefore $a^2 + b^2 = 1$.
Thus $(a, b) = (\pm 1, 0)$ or $(a, b) = (0, \pm 1)$.

We conclude that z must be one of 1, -1, i, or $-i$.
Each of the above elements are units in $\mathbb{Z}[i]$ by Example 10.6. ■

10.2. Division and primes

DEFINITION 10.8. Let $z, w \in \mathbb{Z}[i]$. We say that z **divides** w if there exists $u \in \mathbb{Z}[i]$ with $zu = w$. If z divides w then we say that z is a **divisor** of w and we write $z|w$.

EXAMPLE 10.9. $1 + i$ divides 2 since $2 = (1 + i)(1 - i)$.

EXAMPLE 10.10. In this example, we find all the divisors of 3. Note that $3 = (1) \cdot (3)$, $3 = (-1) \cdot (3)$, $3 = (i) \cdot (-3i)$, and $3 = (-i) \cdot (3i)$ are several factorizations of 3 into Gaussian integers. Hence 1, -1, i, $-i$, 3, -3, $3i$, and $-3i$ are divisors of 3. We now show that these are the only divisors of 3.

Suppose that $3 = zw$ with $z, w \in \mathbb{Z}[i]$. Therefore $9 = N(z)N(w)$. Thus $N(z)$ is 1, 3, or 9 because $N(z)$ is a non-negative integer. Let $z = a + bi$. If $N(z) = 1$, then z is one of 1, -1, i, or $-i$. Note that $N(z) = 3$ has no solutions since $a^2 + b^2 = 3$ has no solutions with $a, b \in \mathbb{Z}$. If $N(z) = 9$, then $a^2 + b^2 = 9$. So $(a, b) = (\pm 3, 0)$ or $(a, b) = (0, \pm 3)$. Hence z is one of 3, -3, $3i$, or $-3i$.

DEFINITION 10.11. Let $z \in \mathbb{Z}[i]$. The elements z, $-z$, iz, and $-iz$ are called the **associates** of z.

EXAMPLE 10.12. Let $z \in \mathbb{Z}[i]$. Note that $z = 1 \cdot z$, $z = (-1) \cdot (-z)$, $z = i \cdot (-iz)$, and $z = (-i) \cdot (iz)$. Hence, 1, -1, i, $-i$, z, $-z$, iz, and $-iz$ are divisors of z. Therefore, the units of $\mathbb{Z}[i]$ and the associates of z are divisors of z for any Gaussian integer z.

DEFINITION 10.13. Let $z \in \mathbb{Z}[i]$. We say that z is **prime** in $\mathbb{Z}[i]$ if z is not a unit and the only divisors of z are the units of $\mathbb{Z}[i]$ and the associates of z.

EXAMPLE 10.14. By Example 10.10, the only divisors of 3 are the units of $\mathbb{Z}[i]$ and the associates of 3. Hence 3 is prime in $\mathbb{Z}[i]$.

EXAMPLE 10.15. 2 is not prime since $2 = (1+i)(1-i)$. 5 is not prime since $5 = (2+i)(2-i)$.

EXAMPLE 10.16. In this example, we show that $1+i$ is prime. Suppose that $z = a+bi \in \mathbb{Z}[i]$ divides $1+i$. Then there exists $w \in \mathbb{Z}[i]$ with $1+i = zw$. Hence $2 = N(1+i) = N(z)N(w)$. Therefore $N(z) = 1$ or $N(z) = 2$. If $N(z) = 1$ then by Proposition 10.7 we have that z is a unit. If $N(z) = 2$, then $a^2 + b^2 = 2$. Hence $(a, b) = (\pm 1, \pm 1)$. So, z is one of $1+i$, $1-i = -i(1+i)$, $-1+i = i(1+i)$, $-1-i = -(1+i)$ which are the associates of $1+i$. Therefore $1+i$ is prime. By exercise 2 , we have that $1-i$ is also prime.

PROPOSITION 10.17 (Division Algorithm for the Gaussian Integers). *Let $z, w \in \mathbb{Z}[i]$ with $w \neq 0$, then there exist $q, r \in \mathbb{Z}[i]$ with $z = wq + r$ and $0 \leq N(r) < N(w)$.*

PROOF. Let $z = a + bi$ and $w = c + di$ where $a, b, c, d \in \mathbb{Z}$.
Let $A = \dfrac{ac+bd}{c^2+d^2}$ and $B = \dfrac{bc-ad}{c^2+d^2}$.
Then $z/w = A + Bi$.
Note that A and B are rational numbers.
Choose integers α and β that are as close to A and B as possible.
That is, let $\alpha, \beta \in \mathbb{Z}$ where $|A - \alpha| \leq 1/2$ and $|B - \beta| \leq 1/2$.
Let $q = \alpha + \beta i$ and $r = z - wq$.
Therefore $z = wq + r$.
In addition, we have that

$$\begin{aligned} |r| &= |z - wq| = |z - w(\alpha + \beta i)| = |w| \left| \frac{z}{w} - (\alpha + \beta i) \right| \\ &= |w||(A - \alpha) + i(B - \beta)| = |w| \sqrt{(A-\alpha)^2 + (B-\beta)^2} \\ &\leq |w| \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{|w|}{\sqrt{2}} < |w|. \end{aligned}$$

Hence, $N(r) = |r|^2 < |w|^2 = N(w)$. ■

EXAMPLE 10.18. This example will illustrate the procedure outlined in the proof of Proposition 10.17. Let $z = 10+2i$ and $w = 2-3i$. Then $z/w = (14/13) + (34/13)i$. Let $A = 14/13$ and $B = 34/13$. Choose $\alpha = 1$ and $\beta = 3$. Let $q = \alpha + \beta i = 1 + 3i$ and $r = z - wq = (10+2i) - (2-3i)(1+3i) = -1-i$. Note that $N(r) = 2 < 13 = N(w)$ and $z = (2-3i)(1+3i) + (-1-i)$.

PROPOSITION 10.19. *Let $z \in \mathbb{Z}[i]$ be prime and let $v, w \in \mathbb{Z}[i]$. If $z|vw$, then $z|v$ or $z|w$.*

PROOF. If z divides v then we are done.
For the remainder of the proof we assume that z does not divide v.
⟨*We begin by showing that z divides w.*⟩
By Proposition 10.17 there exist $q, r \in \mathbb{Z}[i]$ with

$$v = zq + r \text{ and } 0 \leq N(r) < N(z).$$

Note that $r \neq 0$ since z does not divide v.
Hence, by Proposition 10.3, we must have that $N(r) \neq 0$.
Therefore, $0 < N(r) < N(z)$.
Let $S = \{az + bv \mid a, b \in \mathbb{Z}[i]\}$ consist of all linear combinations of z and v.
Note that $r = (-q) \cdot z + 1 \cdot v \in S$ and $N(r) > 0$.
Hence S has an element of positive norm.
Let d be an element of S of minimum positive norm.
Suppose that $d = a_0 z + b_0 v$ where $a_o, b_0 \in \mathbb{Z}[i]$.
Then $N(d) \leq N(r) < N(z)$ by the definition of d and the fact that $r \in S$.
⟨*We now show that d divides z.*⟩
Dividing d into z gives

$$z = dq' + r' \text{ and } 0 \leq N(r') < N(d)$$

where $q', r' \in \mathbb{Z}[i]$.
Note that

$$r' = z - q'd = z - q'((-q)z + v) = (1 + q'q)z - q'v \in S.$$

This implies that $N(r') = 0$ since otherwise r' would be an element of S with smaller positive norm than d, which is impossible by the definition of d.
Therefore, $r' = 0$ by Proposition 10.3.
Therefore, $z = dq'$.
⟨*We now show that d is a unit.*⟩
Since z is a prime and $z = dq'$ then either d is a unit or q' is a unit.
If q' is a unit then by Proposition 10.7 we would have

$$N(z) = N(d)N(q') = N(d) \cdot 1 = N(d)$$

which cannot happen since $N(d) < N(z)$.
Therefore q' is not a unit and so d must be a unit.
⟨*We now show that w is a linear combination of z and v and use this*

fact to show that z divides w.⟩
Since d is a unit in $\mathbb{Z}[i]$ we know that $d^{-1} = 1/d \in \mathbb{Z}[i]$.
Multiplying $d = a_0 z + b_0 v$ by wd^{-1} we get that $w = (d^{-1}a_0 w)z + (d^{-1}b_0 w)v$.
Since z divides vw by assumption we have that $zk = vw$ for some $k \in \mathbb{Z}[i]$.
Hence $w = (d^{-1}a_0 w)z + (d^{-1}b_0 k)z = (d^{-1}a_0 w + d^{-1}b_0 k)z$.
Therefore z divides w. ■

10.3. Integers modulo a prime

Recall that addition and multiplication given by

$$\overline{a} + \overline{b} = \overline{a+b} \text{ and } \overline{a} \cdot \overline{b} = \overline{ab}$$

are well-defined in $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ by Proposition 7.27.

Too Much Information 10.20. By Proposition 7.15(3) and Example 7.16 we have that $\overline{a} = \overline{b}$ iff $a \equiv b (\text{mod } n)$. For example, in $\mathbb{Z}_5$ we have that $\overline{3} = \overline{8}$ since $3 \equiv 8 (\text{mod } 5)$. We make frequent use of this fact in this section and go back and forth between equations in $\mathbb{Z}_n$ and equations modulo n.

Definition 10.21. Let p be a prime. Define $\mathbb{Z}_p^\times = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$.

Lemma 10.22. *Let p be an odd prime. Let $\overline{a} \in \mathbb{Z}_p^\times$. Then there exists a unique $\overline{b} \in \mathbb{Z}_p^\times$ with $\overline{a} \cdot \overline{b} = \overline{1}$.*

Proof. ⟨*We first prove existence*⟩
We may assume that $1 \leq a \leq p-1$ since $\overline{a} \in \mathbb{Z}_p^\times$.
Thus $\gcd(a, p) = 1$.
There exist $b, c \in \mathbb{Z}$ with $ab + pc = 1$ by Theorem 4.63.
Therefore $\overline{ab + pc} = \overline{1}$.
Hence $\overline{a} \cdot \overline{b} + \overline{p} \cdot \overline{c} = \overline{1}$ by Definition 7.24.
Thus $\overline{a} \cdot \overline{b} = \overline{1}$ since $\overline{p} = \overline{0}$.
⟨*We now prove uniqueness.*⟩
Suppose that $\overline{a} \cdot \overline{b_1} = \overline{1}$ and $\overline{a} \cdot \overline{b_2} = \overline{1}$ where $\overline{b_1}, \overline{b_2} \in \mathbb{Z}_p^\times$.
Then $\overline{a} \cdot \overline{b_1} = \overline{a} \cdot \overline{b_2}$.
Multiplying on the left by $\overline{b_1}$ we get that $\overline{b_1} \cdot \overline{a} \cdot \overline{b_1} = \overline{b_1} \cdot \overline{a} \cdot \overline{b_2}$.
Therefore $\overline{b_1} = \overline{b_2}$ since $\overline{b_1} \cdot \overline{a} = \overline{1}$. ■

DEFINITION 10.23. We say that $\overline{x}, \overline{y} \in \mathbb{Z}_p^\times$ are **inverses** if $\overline{x} \cdot \overline{y} = \overline{1}$. If $\overline{x}$ and $\overline{y}$ are inverses then we write $\overline{x}^{\,-1} = \overline{y}$.

EXAMPLE 10.24. Consider

$$\mathbb{Z}_{13}^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}\}.$$

Notice that $\overline{2} \cdot \overline{7} = \overline{14} = \overline{1}$, $\overline{3} \cdot \overline{9} = \overline{27} = \overline{1}$, $\overline{4} \cdot \overline{10} = \overline{40} = \overline{1}$, $\overline{5} \cdot \overline{8} = \overline{40} = \overline{1}$, $\overline{6} \cdot \overline{11} = \overline{66} = \overline{1}$, and $\overline{12} \cdot \overline{12} = \overline{144} = \overline{1}$.

Therefore, $\overline{2}^{\,-1} = \overline{7}$, $\overline{3}^{\,-1} = \overline{9}$, $\overline{4}^{\,-1} = \overline{10}$, $\overline{5}^{\,-1} = \overline{8}$, $\overline{6}^{\,-1} = \overline{11}$, and $\overline{12}^{\,-1} = \overline{12}$.

LEMMA 10.25. *Let p be a prime. If $\overline{x} \in \mathbb{Z}_p^\times$ and $\overline{x}^2 = \overline{1}$, then $\overline{x} = \overline{1}$ or $\overline{x} = \overline{-1} = \overline{p-1}$. That is, the only elements of $\mathbb{Z}_p^\times$ that are their own inverses are the elements $\overline{1}$ and $\overline{p-1} = \overline{-1}$.*

PROOF. Suppose that $\overline{x}^2 = \overline{1}$.
Then $x^2 \equiv 1 (\text{mod } p)$.
So p divides $x^2 - 1 = (x-1)(x+1)$.
Therefore p divides $x - 1$ or p divides $x + 1$ by Theorem 4.67.
Hence $x \equiv 1 (\text{mod } p)$ or $x \equiv -1 (\text{mod } p)$.
Therefore $\overline{x} = \overline{1}$ or $\overline{x} = \overline{-1} = \overline{p-1}$. ■

EXAMPLE 10.26. In this example we illustrate the proof of Proposition 10.27 using $p = 13$. Consider

$$\mathbb{Z}_{13}^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}\}.$$

By Example 10.24 we have that

$$\begin{aligned}
\overline{12!} &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{7} \cdot \overline{8} \cdot \overline{9} \cdot \overline{10} \cdot \overline{11} \cdot \overline{12} \\
&= \overline{1} \cdot \overline{2} \cdot \overline{7} \cdot \overline{3} \cdot \overline{9} \cdot \overline{4} \cdot \overline{10} \cdot \overline{5} \cdot \overline{8} \cdot \overline{6} \cdot \overline{11} \cdot \overline{12} \\
&= \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{12} \\
&= \overline{12} \\
&= \overline{-1}.
\end{aligned}$$

PROPOSITION 10.27 (Wilson's Theorem). *Let p be a prime, then $\overline{(p-1)!} = \overline{-1}$ in $\mathbb{Z}_p^\times$.*

PROOF. If $p = 2$ then the result is true.
We now assume that p is odd.
Let $\overline{x} \in \mathbb{Z}_p^\times$ with $2 \leq x \leq p-2$.
By Lemmas 10.22 and 10.25 there exits a unique inverse $\overline{y} \in \mathbb{Z}_p^\times$ with $2 \leq y \leq p-2$ and $\overline{x} \cdot \overline{y} = \overline{1}$ in $\mathbb{Z}_p^\times$.
Note that $\overline{x} \neq \overline{y}$ since then we would have $\overline{x}^2 = \overline{1}$ which can't happen by Lemma 10.25 since $2 \leq x \leq p-2$.
Therefore, by pairing elements in the following product with their unique inverses we get that

$$\begin{aligned}\overline{(p-1)!} &\equiv \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{(p-2)} \cdot \overline{(p-1)} \\ &\equiv \overline{1} \cdot \overline{(1)^{(p-2)/2}} \cdot \overline{(p-1)} \\ &\equiv \overline{-1}.\end{aligned}$$

■

EXAMPLE 10.28. In Proposition 10.29 we will show that if p is an odd prime with $p \equiv 1 (\text{mod } 4)$ then there exists an element $\overline{x} \in \mathbb{Z}_p^\times$ with $\overline{x}^2 = \overline{-1}$. In this example we illustrate the proof of Proposition 10.29 using $p = 13 \equiv 1 (\text{mod } 4)$.

Let $\overline{x} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6}$ in $\mathbb{Z}_{13}^\times$. Note that there are an even number of terms in the product for x. Hence $\overline{x} = \overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdot \overline{-4} \cdot \overline{-5} \cdot \overline{-6}$ since the minus signs cancel each other. Note that $\overline{13-k} = \overline{13} + \overline{-k} = \overline{-k}$ for any integer k. Hence by Proposition 10.27 we have that

$$\begin{aligned}\overline{x}^2 &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdot \overline{-4} \cdot \overline{-5} \cdot \overline{-6} \\ &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{13-1} \cdot \overline{13-2} \cdot \overline{13-3} \cdot \overline{13-4} \cdot \overline{13-5} \cdot \overline{13-6} \\ &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{12} \cdot \overline{11} \cdot \overline{10} \cdot \overline{9} \cdot \overline{8} \cdot \overline{7} \\ &= \overline{(13-1)!} \\ &= \overline{-1}.\end{aligned}$$

PROPOSITION 10.29. *Let p be an odd prime with $p \equiv 1 (\text{mod } 4)$. There exists an element $\overline{x} \in \mathbb{Z}_p^\times$ with $\overline{x}^2 = \overline{-1}$.*

PROOF. ⟨*The reader may wish to read through Example 10.28 before reading this proof.*⟩
We have that $p - 1 = 4n$ for some integer n since $p \equiv 1 (\text{mod } 4)$.
Let

$$\overline{x} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{(p-1)/2}.$$

Note that there are an even number of terms in the product for $\overline{x}$ since $(p-1)/2 = 2n$ is even.
This gives us that

$$\overline{x} = \overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdots \overline{-(p-1)/2}.$$

since the minus signs cancel each other out.
Note that $\overline{p-k} = \overline{p} + \overline{-k} = \overline{-k}$ for every integer k.
Hence by Proposition 10.27

$$\begin{aligned}
\overline{x}^2 &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{(p-1)/2} \cdot \overline{-1} \cdot \overline{-2} \cdot \overline{-3} \cdots \overline{-(p-1)/2} \\
&= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{(p-1)/2} \cdot \overline{p-1} \cdot \overline{p-2} \cdot \overline{p-3} \cdots \overline{p-(p-1)/2} \\
&= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{(p-1)/2} \cdot \overline{(p+1)/2} \cdots \overline{p-3} \cdot \overline{p-2} \cdot \overline{p-1} \\
&= \overline{(p-1)!} \\
&= \overline{-1}.
\end{aligned}$$

■

10.4. Sums of squares

Let p be an odd prime. Then by Exercise 5, either $p \equiv 1 (\text{mod } 4)$ or $p \equiv 3 (\text{mod } 4)$. In this section we show that $p = x^2 + y^2$ for integers x and y if and only if $p \equiv 1 (\text{mod } 4)$.

DEFINITION 10.30. We say that an integer n is the **sum of two squares** if there exist integers x and y with $n = x^2 + y^2$. Otherwise we say that n is not the sum of two squares.

PROPOSITION 10.31. *Let p be an odd prime and suppose that $p \equiv 3 (\text{mod } 4)$. Then p is not the sum of two squares.*

PROOF. Let a be an integer.
By Table 1 we have that $\overline{a}^2 = \overline{0}$ or $\overline{a}^2 = \overline{1}$ in $\mathbb{Z}_4$.
Therefore, by Table 2, if x and y are integers, then $\overline{x}^2 + \overline{y}^2 \neq \overline{3}$ in $\mathbb{Z}_4$.
Hence there do not exist integers x and y with $p = x^2 + y^2$ since $\overline{p} = \overline{3}$ in $\mathbb{Z}_4$. ■

PROPOSITION 10.32. *Let p be an odd prime and suppose that $p \equiv 1 (\text{mod } 4)$. Then p is the sum of two squares.*

$\overline{a}$ in $\mathbb{Z}_4$	a^2 in $\mathbb{Z}_4$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{0}$
$\overline{3}$	$\overline{1}$

TABLE 1. Squares modulo four

$\overline{x}^2$ in $\mathbb{Z}_4$	$\overline{y}^2$ in $\mathbb{Z}_4$	$(\overline{x}^2 + \overline{y}^2)$ in $\mathbb{Z}_4$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{0}$	$\overline{1}$	$\overline{1}$
$\overline{1}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$

TABLE 2. Sums of squares modulo four

PROOF. ⟨*We begin by showing that p factors in* $\mathbb{Z}[i]$.⟩
By Proposition 10.29 there exists an integer x where $x^2 \equiv -1 (\text{mod } p)$.
Therefore $x^2 + 1 = pk$ for some integer k.
Factoring the above equation in $\mathbb{Z}[i]$ we have that $pk = (x + i)(x - i)$.
If p were prime in $\mathbb{Z}[i]$, then by Proposition 10.19, we would have that either p divides $x + i$ or p divides $x - i$.
Let $c + di \in \mathbb{Z}[i]$.
Note that $p(c+di) = pc+pdi \neq x+i$ and $p(c+di) = pc+pdi \neq x-i$, since $pd \neq \pm 1$.
Hence p does not divide $x + i$ and p does not divide $x - i$.
Therefore p is not prime in $\mathbb{Z}[i]$.
Hence $p = zw$ where $z, w \in \mathbb{Z}[i]$ and neither z nor w is a unit.
⟨*We now use the above factorization of p to show that p is the sum of two squares.*⟩
Thus $p^2 = N(p) = N(z)N(w)$.
By Proposition 10.7 we must have that $N(z) = N(w) = p$ since neither z nor w is a unit.
Let $z = a + bi$ where a and b are integers.
Then $p = N(z) = a^2 + b^2$.
Therefore p is the sum of two squares. ■

10.5. Exercises

(1) Let $z, w \in \mathbb{Z}[i]$. Prove that w divides z if and only if $\overline{w}$ divides $\overline{z}$.
(2) Let $z \in \mathbb{Z}[i]$. Prove that z is prime if and only if $\overline{z}$ is prime. [Hint: Use exercise 1.]
(3) Let $z \in \mathbb{Z}[i]$. Prove that if $N(z)$ is a prime in $\mathbb{Z}$, then z is prime in $\mathbb{Z}[i]$.
(4) Let $w, y, z \in \mathbb{Z}[i]$. Prove that if w is a unit and wz divides y, then z divides y.
(5) Let p be an odd prime in $\mathbb{Z}$. Prove that either $p \equiv 1 (\text{mod } 4)$ or $p \equiv 3 (\text{mod } 4)$.

Chapter 11

Real Analysis

11.1. Supremum of a set

DEFINITION 11.1. Let $S \subset \mathbb{R}$. We say that $x \in \mathbb{R}$ is an **upper bound** for S if $y \leq x$ for all $y \in S$. That is, x is an upper bound for S if x is bigger than every element of S.

If S has an upper bound then we say that S is **bounded from above**.

EXAMPLE 11.2. Let S be the interval $(-7.25, -1.5) \cup (0, 3]$. See Figure 1.

Then 4 is an upper bound of S since $x \leq 4$ for every x in S. Therefore S is bounded from above. Note that 3 and 5 are also upper bounds for S.

DEFINITION 11.3. Suppose that S is bounded from above and that x is an upper bound for S. We say that x is a **least upper bound** or **supremum** of S if $x \leq x'$ for every upper bound x' of S. If x is a supremum for S then we write $x = \sup(X)$.

EXAMPLE 11.4. Let S be the interval $(-7.25, -1.5) \cup (0, 3]$ be as in Example 11.2. See Figure 1.

The least upper bound for S is exactly what you think it is. It is the smallest number that is an upper bound for S. In this example,

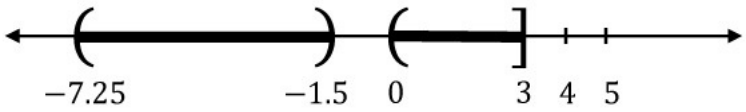


FIGURE 1. $S = (-7.25, -1.5) \cup (0, 3]$

is 4 the least upper bound for S? No, because 3.5 is a smaller upper bound for S. 3.12 is an even smaller upper bound for S. It is clear that 3 is the "least upper bound" from the picture of S. Let's show this with a short algebraic proof:

3 is an upper bound for S since $y \leq 3$ for every $y \in S$.
Suppose that x' is another upper bound for S.
Then $3 \leq x'$ since $3 \in S$.
Hence 3 is less than or equal to any other upper bound for S.
Hence $3 = \sup(S)$.

If you recall, the real numbers are the number system that satisfies Assumption 4.4. That is, the real numbers are *defined* to be "the" set that satisfies all of the properties given in Assumption 4.4. (We put "the" in quotes because there are actually many sets that satisfy the properties given in Assumption 4.4, however all of those sets are basically the same in some way. One of these sets is given in Chapter ?????)

The most important axiom that we will use for the real numbers is the completeness axiom. This is Axiom 17 from Assumption 4.4, which is repeated below for your convenience.

ASSUMPTION 11.5 (The completeness axiom for $\mathbb{R}$). *Let $S \subseteq \mathbb{R}$ that is bounded from above. Then there exists a supremum for S.*

TOO MUCH INFORMATION 11.6. Let S be a subset of $\mathbb{R}$ that is bounded from above. By the completeness axiom for $\mathbb{R}$ we know that a supremum for S exists. By exercise 1 we know that the supremum is unique. Hence the definition of supremum is well-defined.

PROPOSITION 11.7. *Let S be a non-empty subset of $\mathbb{R}$ that is bounded from above by an element $x \in \mathbb{R}$. Then $x = \sup(S)$ if and only if for every $\epsilon > 0$ there exists $y \in S$ with $x - \epsilon < y \leq x$*

PROOF. Let $\epsilon > 0$ be a real number.

Suppose that $x = \sup(S)$.
Note that $x - \epsilon$ is not an upper bound for S because $x - \epsilon < x$ and x is the least upper bound for S.
Therefore, there exists an element of $y \in S$ with $x - \epsilon < y \leq x$.

Conversely, suppose that for every $\epsilon > 0$ there exists $y \in S$ with $x - \epsilon < y \leq x$.
Suppose that x' is an upper bound for S.
⟨*Let's show that $x \leq x'$, which will show that $x = \sup(S)$. We show this via contradiction.*⟩
Suppose that $x' < x$.
⟨*See Figure 2 for an illustration of the rest of this proof.*⟩
Let $\epsilon = (x - x')/2$.
By our hypothesis on x, there exists $y \in S$ with $x - \epsilon < y < x$.
Note that

$$x - \epsilon = x - (x - x')/2 = x/2 + x'/2 > x'/2 + x'/2 = x'$$

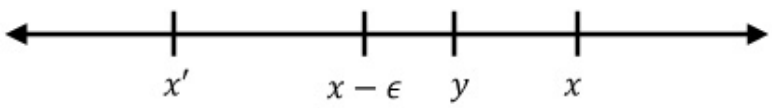


FIGURE 2. Illustration of the proof of Proposition 11.7

since $x > x'$.
Therefore $x' < x - \epsilon < y$.
This shows that x' is not an upper bound for S.
We conclude that $x' \geq x$. ■

EXAMPLE 11.8. Let

$$S = \left\{ 1 - \frac{1}{n} \;\middle|\; n = 1, 2, 3, 4, \ldots \right\} = \left\{ 0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \ldots \right\}.$$

In this example we use Proposition 11.7 to show that $1 = \sup(S)$. Let $\epsilon > 0$. Choose an integer n with $n > 1/\epsilon$. Let $y = 1 - 1/n$. Then $y \in S$ and $1 - \epsilon < y < 1$. Hence $y = \sup(S)$. See Figure 3.

11.2. Limits

DEFINITION 11.9. A **sequence of real numbers** is an ordered list of real numbers indexed by the natural numbers. If a_n is the nth term of a sequence then one writes $(a_n)_{n=1}^{\infty}$ or (a_n) to denote the sequence.

EXAMPLE 11.10. Consider the sequence given by $\left(\frac{1}{n}\right)_{n=1}^{\infty}$. The first term of the sequence is $1/1 = 1$. The second term of the sequence is $1/2$. The third term of the sequence is $1/3$. The 100th term of the sequence is $1/100$.

TOO MUCH INFORMATION 11.11. Consider Definition 11.9. What is an "ordered list of real numbers?" To make the definition of a sequence more precise one needs to use functions. One can define a sequence as a function $f : \mathbb{N} \to \mathbb{R}$. The nth term of the sequence is $a_n = f(n)$. For example, one can define the sequence in Example 11.10 as the function $f : \mathbb{N} \to \mathbb{R}$ where $f(n) = 1/n$.

TOO MUCH INFORMATION 11.12. Analysis loves absolute values. The absolute value function allows us to measure the distance between two points. From now on whenever you see $|a - b|$ you should think of it as the distance between a and b. Everytime. For example, $|3 - 10|$ gives the distance between 3 and 10. Or $|f(x) - L|$ gives the distance between the two numbers $f(x)$ and L.

EXAMPLE 11.13. Consider the sequence given in Example 11.10. As n gets larger and larger, $a_n = 1/n$ gets closer and closer to 0. For

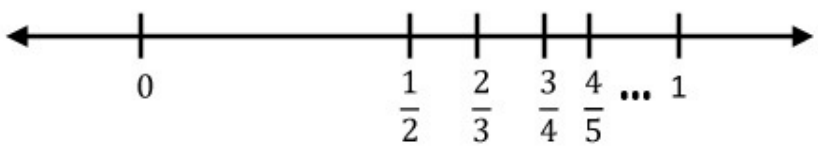


FIGURE 3. Illustration of Example 11.8

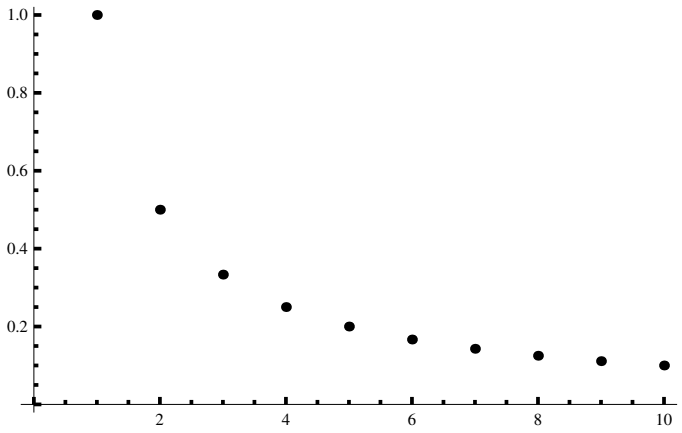


FIGURE 4. Illustration of Example 11.10

example, if $n \geq 1,000$, then $|a_n - 0| = 1/n \leq 0.001$. That is, after the 1000th term, every element in the sequence is within 0.001 of 0. Or if $n \geq 1,000,000$, then $|a_n - 0| = 1/n \leq 0.000001$. That is, after the $1,000,000$th term, every element of the sequence is within 0.000001 of 0. This is what we mean by "a_n gets closer and closer to 0 as n gets larger and larger." The reader may recall from Calculus that the limit of the sequence $a_n = 1/n$ is 0. We make the definition of limit precise in Definition 11.14.

DEFINITION 11.14. Let $(a_n)_{n=1}^{\infty}$ be a sequence of real numbers. We say that

$$\lim_{n\to\infty} a_n = L$$

if for every $\epsilon > 0$ there exists an integer $N > 0$ with $|a_n - L| < \epsilon$ for all $n > N$.

If such an L exists, then we say that $(a_n)_{n=1}^{\infty}$ **converges** to L. Otherwise we say that $(a_n)_{n=1}^{\infty}$ **does not converge**.

EXAMPLE 11.15. Recall Examples 11.10 and 11.13. We now show that $\lim_{n\to\infty} 1/n = 0$.

PROOF. Let $\epsilon > 0$.
Choose an integer N with $N > 1/\epsilon$.
If $n > N$, then $|1/n - 0| = 1/n < 1/N < \epsilon$.
Hence $\lim_{n\to\infty} 1/n = 0$. ■

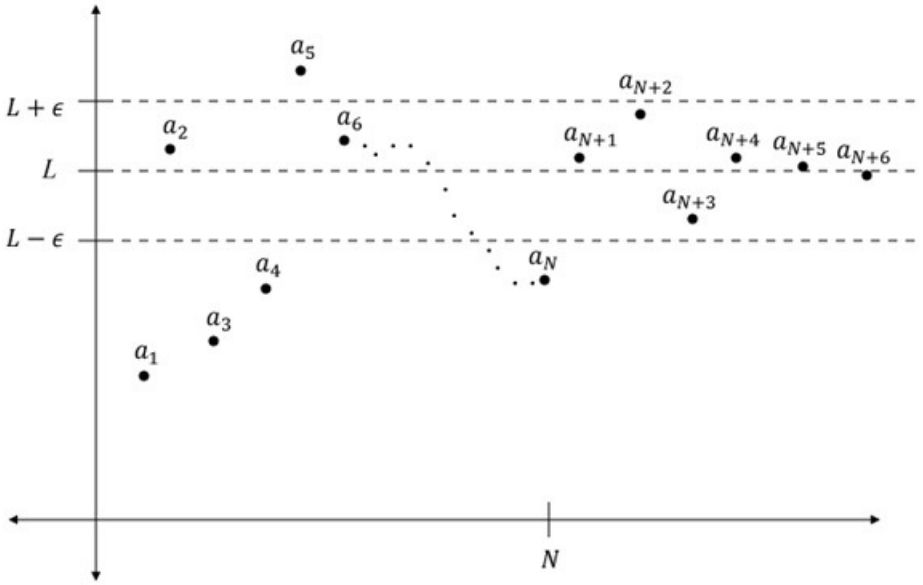


FIGURE 5. Illustration of Definition 11.14

TOO MUCH INFORMATION 11.16. By Exercise 3, we have that Definition 11.14 is well-defined, that is limits are unique.

EXAMPLE 11.17. Let c be a fixed real number. Then $\lim_{n\to\infty} c = c$.

PROOF. Let $\epsilon > 0$.
Pick $N = 1$.
If $n > N$, then $|c - c| = 0 < \epsilon$. ■

EXAMPLE 11.18. $((-1)^n)_{n=1}^{\infty}$ does not converge.

PROOF. Suppose that $\lim_{n\to\infty}(-1)^n = L$ for some real number L.
⟨*We break the proof into cases.*⟩
Suppose that L is a real number with $L = 1$.
Let $\epsilon = 1$.
Suppose that N is any positive integer.
Then there is an odd positive integer n_0 with $n_0 > N$.
Then $|(-1)^{n_0} - L| = |-1-1| = 2 > \epsilon$.
Hence $L = 1$ is not a limit for the sequence $((-1)^n)_{n=1}^{\infty}$.

Now suppose that L is a real number with $L \neq 1$.
Let $\epsilon = |L-1|/2$.
Let N be any positive integer.
Then there is an even positive integer n_0 with $n_0 > N$.
And $|(-1)^{n_0} - L| = |1 - L| = |L - 1| > |L-1|/2 = \epsilon$.
Hence L is not a limit for the sequence $((-1)^n)_{n=1}^{\infty}$.
We have shown that the sequence $((-1)^n)_{n=1}^{\infty}$ does not converge. ■

EXAMPLE 11.19 (Geometric sequence). Let x be a real number with $-1 \leq x \leq 1$. Consider the sequence $(x^n)_{n=1}^{\infty}$. Then $\lim_{n\to\infty} x^n = 0$.

PROOF. If $x = 0$, then $\lim_{n\to\infty} x^n = \lim_{n\to\infty} 0 = 0$ by Example 11.17.
Suppose for the remainder of the proof that $|x| < 1$ but $x \neq 0$.
Let $\epsilon > 0$.
Suppose that $\epsilon < 1$.
⟨*Note that the restriction that $\epsilon < 1$ is okay. For suppose that $\epsilon < \epsilon'$. If we show that $|x^n - 0| < \epsilon$, then we have shown that $|x^n - 0| < \epsilon'$.*⟩
Let N be a positive integer with $N > \log(\epsilon)/\log(|x|)$.
Note that $\log(\epsilon)$ and $\log(|x|)$ are both negative.
Therefore $N\log(|x|) < \log(\epsilon)$.
And so $\log(|x|^N) < \log(\epsilon)$.
It follows that $|x|^N < \epsilon$.
Suppose that n is an integer with $n > N$.
Then $|x - 0|^n = |x|^n < |x|^N < \epsilon$ since $|x| < 1$.
Hence $\lim_{n\to\infty} x^n = 0$. ■

PROPOSITION 11.20. *Let (a_n) and (b_n) be convergent sequences with $\lim a_n = L_a$ and $\lim b_n = L_b$. Let c be any real number. Then*

(1) $\lim ca_n = cL_a$.
(2) $\lim(a_n + b_n) = L_a + L_b$.
(3) $\lim(a_n - b_n) = L_a - L_b$.

PROOF. (1) If $c = 0$, then $\lim ca_n = \lim 0 = 0$ by Example 11.17.
Suppose that $c \neq 0$.
Let *epsilon* > 0.
Since $\lim a_n = L_a$ we know that there exists $N > 0$ where $|a_n - L_a| < \epsilon/|c|$ for all $n > N$.
Therefore if $n > N$ then

$$|ca_n - cL_a| = |c||a_n - L_a| < |c|(\epsilon/|c|) = \epsilon.$$

Hence $\lim ca_n = cL_a$.

(2) Let $\epsilon > 0$.
Since $\lim a_n = L_a$ we know that there exists $N_a > 0$ where $|a_n - L_a| < \epsilon/2$ for all $n > N_a$.
Since $\lim b_n = L_b$ we know that there exists $N_b > 0$ where $|b_n - L_b| < \epsilon/2$ for all $n > N_b$.
Let N be the maximum of N_a and N_b.
Then if $n > N$ we have that

$$\begin{aligned} |(a_n + b_n) - (L_a + L_b)| &= |(a_n - L_a) + (b_n - L_b)| \\ &\leq |(a_n - L_a)| + |(b_n - L_b)| \\ &< \epsilon/2 + \epsilon/2 = \epsilon \end{aligned}$$

by the triangle inequality ?????????????????? put a reference here ??????????????.
Hence $\lim(a_n + b_n) = L_a + L_b$.

(3) By part (1) we have that $-\lim b_n = \lim(-b_n)$.
Hence by part (2) we have that

$$\lim(a_n - b_n) = \lim(a_n + (-b_n)) = \lim a_n + \lim(-b_n) = \lim a_n - \lim b_n = L_a - L_b.$$

■

LEMMA 11.21. *Let (a_n) and (b_n) be convergent sequences with $\lim a_n = L_a$ and $\lim b_n = L_b$. If $a_n < b_n$ for all n, then $L_a \leq L_b$.*

PROOF. ⟨*We give a proof by contradiction.*⟩
Suppose that $L_a > L_b$.
Let $\epsilon = (L_a - L_b)/2$.
There exists N such that $|a_N - L_a| < \epsilon$ because (a_n) converges to L_a.
There exists M such that $|b_M - L_b| < \epsilon$ because (b_n) converges to L_b.
Then $b_M < L_b + \epsilon = L_a - \epsilon < a_N$.
This is a contradiction.
Hence $L_a \leq L_b$. ■

11.3. Infinite Sums

DEFINITION 11.22. Consider a sequence (a_n). The **N-th partial sum** of (a_n) is

$$s_N = a_0 + a_1 + \cdots a_N.$$

We say that the **infinite sum** or **series** $\sum_{n=0}^{\infty} a_n$ **converges** to L, and we write $\sum_{n=0}^{\infty} a_n = L$, if $L = \lim_{N\to\infty} s_N$. If $\lim_{N\to\infty} s_N$ does not exist then we say that the series $\sum_{n=0}^{\infty} a_n$ **diverges**.

EXAMPLE 11.23. Let x be a real number with $|x| < 1$. Then

$$\sum_{n=0}^{\infty} x^n = 1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}.$$

PROOF. By Example 5.3 we have that

$$s_N = 1 + x + x^2 + x^3 + \cdots + x^N = \frac{x^{N+1} - 1}{x - 1}.$$

If $|x| < 1$ then by Example 11.17, Example 11.19, and Proposition 11.20 we have that

$$\lim_{N\to\infty} \frac{x^{N+1} - 1}{x - 1} = \frac{1}{x-1}(\lim_{N\to\infty} x^{N+1} - \lim_{N\to\infty} 1) = \frac{1}{x-1}(0 - 1) = \frac{1}{1-x}.$$

■

EXAMPLE 11.24. By Example 11.23 we have that

$$\sum_{n=0}^{\infty} \left(\frac{1}{2}\right)^n = \frac{1}{1 - 1/2} = 2.$$

PROPOSITION 11.25. *Suppose that the infinite sums $\sum a_n$ and $\sum b_n$ converge. Let c be a real number. Then*

(1) $\sum(a_n + b_n) = \sum a_n + \sum b_n$
(2) $\sum(ca_n) = c\sum a_n$
(3) *If $a_n < b_n$ for all n, then $\sum a_n < b_n$*
(4) *If $a_n > 0$ for all n, then $\sum a_n > 0$.*

PROOF. Let s_N and s'_N be the N-th partial sums of $\sum a_n$ and $\sum b_n$ respectively.
(1) The N-th partial sum of $\sum(a_n + b_n)$ is $s_N + s'_N$.
Hence by Proposition 11.20 we have that

$$\sum(a_n + b_n) = \lim_{N\to\infty}(s_N + s'_N) = \lim_{N\to\infty} s_N + \lim_{N\to\infty} s'_N = \sum a_n + \sum b_n.$$

(2) The N-th partial sum of $\sum(ca_n)$ is cs_N.
Hence by Proposition 11.20 we have that

$$\sum(ca_n) = \lim_{N\to\infty}(cs_N) = c\lim_{N\to\infty} s_N = c\sum a_n.$$

(3) We have that $s_N < s'_N$ for all N since $a_n < b_n$ for all n.
Also, $s_N - a_0 < s'_N - b_0$ for all $N > 0$.
Hence, by Proposition 11.20 we have that

$$\begin{aligned}\sum a_n &= \lim s_N = \lim s_N - a_0 + a_0 = \lim(s_N - a_0) + a_0 \\ &\leq \lim(s'_N - b_0) + a_0 < \lim(s'_N - b_0) + b_0 = \lim s'_N - b_0 + b_0 \\ &= \lim s'_N = \sum b_n.\end{aligned}$$

(4) We have that $s_N > 0$ for all N since $a_n > 0$ for all n.
Also, $s_N - a_0 > 0$ for all $N > 0$.
Hence by Proposition 11.20 we have that

$$\begin{aligned}\sum a_n &= \lim s_N = \lim s_N - a_0 + a_0 \\ &= \lim(s_N - a_0) + a_0 \geq 0 + a_0 > 0.\end{aligned}$$

■

11.4. Bounded monotone convergence theorem and the irrationality of e

DEFINITION 11.26. A sequence (a_n) is called **monotone increasing** if $a_n \leq a_{n+1}$ for all n.

THEOREM 11.27 (Bounded monotone convergence theorem). *Let (a_n) be a monotone increasing sequence that is bounded above. Then (a_n) converges to $L = \sup(S)$ where $S = \{a_n \mid n = 1, 2, 3, \ldots\}$.*

PROOF. Note that $L = \sup(S)$ exists by the Completeness axiom (Assumption 11.5).
Let $\epsilon > 0$.
By Proposition 11.7, there exists a_N with $L - \epsilon < a_N \leq L$.
Since (a_n) is monotone increasing and $L = \sup(S)$ we have that $L - \epsilon < a_N \leq a_k \leq L$ for all $k \geq N$.
Hence $|a_k - L| < \epsilon$ for all $k \geq N$.
Therefore $\lim_{k\to\infty} a_k = L$. ■

TOO MUCH INFORMATION 11.28. The real number line has a special property that the rational numbers don't have. It has no "holes." Think about the following. Consider the set of rational numbers $\mathbb{Q}$. By Theoerem 4.53 we know that $\sqrt{2}$ is not in $\mathbb{Q}$. That is, there is a whole in the rational numbers. Indeed, let $A = \{r \in \mathbb{Q} \mid r \leq \sqrt{2}\}$ and $B = \{r \in \mathbb{Q} \mid \sqrt{2} \leq r\}$. Then $\mathbb{Q} = A \cup B$. In addition there is a number that sits between A and B and is not a rational number. It is $\sqrt{2}$. Of course there are rational numbers that get closer and closer to $\sqrt{2}$, but they never quite get there. Here are some of them: $1.41 = \frac{141}{100}$, $1.414 = \frac{1414}{1000}$, $1.4142 = \frac{14142}{10000}, \cdots$

The real numbers don't have this problem. The bounded montone convergence theorem (Theorem 11.27) guarantees this fact. For suppose (x_n) is a sequence of increasing

The completeness axiom takes care of this. In the list of numbers above we had a sequence of rational numbers that were getting bigger and bigger and were getting closer and closer to $\sqrt{2}$. This can't happen in the real number system. The Bounded monotone convergence theorem (Theorem 11.27) guarantees that if you have a list of increasing real numbers that get closer to and closer to a number x, then x has to be real. You don't have any "holes" in the real number system.

COROLLARY 11.29. *The infinite sum* $\sum_{n=0}^{\infty} \frac{1}{n!}$ *converges.*

PROOF. Let $s_N = \sum_{n=0}^{N} \frac{1}{n!}$.
$\langle$*We begin by showing that* (s_N) *is a bounded sequence.*$\rangle$
Note that $1 \cdot 2 \cdot 3 \cdots k \geq 2^{k-1}$ for all integers $k \geq 1$.
Hence $\frac{1}{k!} \leq \frac{1}{2^{k-1}}$ for all integers $k \geq 1$.
We have that

$$\begin{aligned} s_N &= \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{N!} \\ &\leq 1 + \frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \cdots + \frac{1}{2^{N-1}} \\ &= 1 + \frac{1 - \frac{1}{2}^N}{1 - \frac{1}{2}} \\ &\leq 1 + \frac{1}{1 - \frac{1}{2}} \\ &= 3. \end{aligned}$$

Therefore, (s_N) is a bounded sequence.
$\langle$*We now show that* (s_N) *is monotone.*$\rangle$
Note that $s_{N+1} = s_N + \frac{1}{(N+1)!} > s_N$.
Hence (s_N) is a monotone sequence.
By Theorem 11.27, we have that (s_N) converges. ■

DEFINITION 11.30. We define the number e to be equal to the infinite sum $\sum_{n=0}^{\infty} \frac{1}{n!}$.

EXAMPLE 11.31. e is irrational.

PROOF. $\langle$*We give a proof by contradition.*$\rangle$
Suppose that $e = a/b$ where $a, b \in \mathbb{Z}$ and $a > 0$ and $b > 0$.
Let $x = b! \left(e - \sum_{n=0}^{b} \frac{1}{n!} \right)$.
Note that

$$x = b! \left(\frac{a}{b} - \sum_{n=0}^{b} \frac{1}{n!} \right) = a(b-1)! - \sum_{n=0}^{b} \frac{b!}{n!}.$$

We see that x is an integer since $b!/n!$ is an integer for every $0 \leq n \leq b$.
We now show that $0 < x < 1$ which will be a contradiction.
By Proposition 11.25 we have that

$$x = b!\left(\sum_{n=0}^{\infty}\frac{1}{n!} - \sum_{n=0}^{b}\frac{1}{n!}\right) = \sum_{n=b+1}^{\infty}\frac{b!}{n!} > 0.$$

So $x > 0$.
If $n \geq b+2$, then

$$\begin{aligned}
\frac{b!}{n!} &= \frac{b(b-1)\cdots(2)(1)}{n(n-1)\cdots(b+1)(b)(b-1)\cdots(2)(1)} \\
&= \frac{1}{(b+1)(b+2)(b+3)\cdots(n-1)(n)} \\
&= \frac{1}{(b+1)(b+2)(b+3)\cdots(b+(n-(b+1)))(b+(n-b))} \\
&< \frac{1}{(b+1)^{n-b}}.
\end{aligned}$$

By Proposition 11.25 and Example 11.23 we have that

$$\begin{aligned}
x &= \sum_{n=b+1}^{\infty}\frac{b!}{n!} < \sum_{n=b+1}^{\infty}\frac{1}{(b+1)^{n-b}} \\
&= \sum_{k=1}^{\infty}\frac{1}{(b+1)^{k}} = \frac{1}{b+1}\sum_{k=0}^{\infty}\frac{1}{(b+1)^{k}} \\
&= \frac{1}{b+1}\left(\frac{1}{1-\frac{1}{b+1}}\right) = \frac{1}{b} \\
&\leq 1.
\end{aligned}$$

Therefore $x < 1$.
We have reached a contradiction since x is an integer and $0 < x < 1$.
Therefore e is not rational. ■

11.5. Exercises

(1) Let $S \subseteq \mathbb{R}$. Suppose that S is bounded from above. Prove that the supremum of S is unique.
(2) In this exercise we show that the set of rational numbers $\mathbb{Q}$ does not have the completeness property. Let

$$S = \{x \in \mathbb{Q} \mid x^2 < 2\}.$$

(a) Find a rational number that is an upper bound for S. This shows that S is bounded above in $\mathbb{Q}$.
(b) Suppose that $s = \sup(S)$ where s is a rational number. Show that both $s < \sqrt{2}$ and $s > \sqrt{2}$ are false. This will yield a contradiction since $\sqrt{2}$ is not rational. [Hint: If $s < \sqrt{2}$ then $s + 1/K < \sqrt{2}$ for every natural number K with $1/K < \sqrt{2} - s$. If $s > \sqrt{2}$ then $s - 1/M > \sqrt{2}$ for every natural number M with $1/M < s - \sqrt{2}$.]

(3) Let (a_n) be a convergent sequence. Suppose that $\lim a_n = L$ and $\lim a_n = L'$. Prove that $L = L'$.
(4) Suppose that (a_n) is a convergent sequence. Prove that (a_n) is bounded. That is, prove that there exists a real number $M > 0$ such that $|a_n| \leq M$ for all n.

Chapter 12

Group Theory

12.1. Definition of a group

Definition 12.1. A **group** is a set G with a binary operation $*$ defined on G such that the following statements are true:

(1) (closure) If $a, b \in G$, then $a * b \in G$.
(2) (associativity) If $a, b, c \in G$, then $(a * b) * c = a * (b * c)$.
(3) (identity) There exists $e \in G$ satisfying $e * a = a * e = a$ for all $a \in G$. The element e is called an **identity element** for G.
(4) (inverses) For each $a \in G$ there exists $b \in G$ with $a * b = b * a = e$. The element b is called an **inverse** for a.

Example 12.2. We now show that the set of integers $\mathbb{Z}$ is a group under the binary operation $+$. Let us check the four requirements of Definition 12.1.

(1) Let $a, b \in \mathbb{Z}$. Then by assumption ??? we have that $a + b \in \mathbb{Z}$.
(2) Let $a, b, c \in \mathbb{Z}$. Then by assumption ??? we have that $(a + b) + c = a + (b + c)$.
(3) Let $e = 0$.
Then $0 + a = a + 0 = a$ for every $a \in \mathbb{Z}$.
Hence 0 is an identity element for $\mathbb{Z}$ under addition.
(4) Let $a \in \mathbb{Z}$.
Let $b = -a$.
Then $b \in \mathbb{Z}$ and $a + b = 0 = b + a$.
Hence $b = -a$ is an inverse for a.

EXAMPLE 12.3. Consider the set of rational numbers $\mathbb{Q}$. We now show that $\mathbb{Q}$ is not a group under multiplication.

Consider Definition 12.1(3). The only element $e \in \mathbb{Q}$ with $e \cdot a = a \cdot e = a$ for all $a \in \mathbb{Q}$ is $e = 1$. Thus the only identity element for $\mathbb{Q}$ under multiplication is $e = 1$.

Now let $a = 0$ and $e = 1$ in part (4). Note that $0 \cdot b = b \cdot 0 = 1$ has no solutions. That is, 0 has no inverse under multiplication. Hence (4) is not true for $\mathbb{Q}$ under multiplication.

EXAMPLE 12.4. We now show that the set of non-zero rational numbers $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ is a group under multiplication. Let us check the four requirements of Definition 12.1.

(1) Let $a, b \in \mathbb{Q}^*$.
Then $a = m/n$ and $b = s/t$ where $m, n, s, t \in \mathbb{Q}$ and $m \neq 0$ and $s \neq 0$.
Hence $ab = ms/nt \in \mathbb{Q}^*$ since $ms \neq 0$.
(2) Let $a, b, c, \in \mathbb{Q}^*$.
Then $(ab)c = a(bc)$ by assumption ???.
(3) Let $e = 1$.
Then $a \cdot 1 = 1 \cdot a = a$ for all $a \in \mathbb{Q}^*$.
(4) Let $a \in \mathbb{Q}^*$.
Then $a = m/n$ where $m, n \in \mathbb{Z}$ and $m \neq 0$.
Hence $1/a = n/m \in \mathbb{Q}^*$ and $a(1/a) = (1/a)a = 1$.

PROPOSITION 12.5. *Let G be a group with binary operation $*$. Then the following are true:*

(1) *There is only one identity element for G.*
(2) *Given $a \in G$ there is only one inverse of a in G. We denote the unique inverse of a by a^{-1}.*

PROOF. (1) Suppose that e_1 and e_2 are both identity elements for G.
Then $e_1 * e_2 = e_2$ since e_1 is an identity element for G.
Similarly $e_1 * e_2 = e_1$ since e_2 is an identity element for G.
Hence $e_1 = e_2$.
(2) Let $a \in G$.
Let $e \in G$ be the identity element for G.
Suppose that x and y are inverses for a.
Then $a * x = x * a = e$ and $a * y = y * a = e$ by Definition 12.1(3).

Thus $a * x = a * y$.
Hence $y * (a * x) = y * (a * y)$.
Therefore $(y * a) * x = (y * a) * y$ by Definition 12.1(2).
Hence $e * x = e * y$.
Ergo $x = y$.

■

CHECK FOR UNDERSTANDING 12.6. (1) Consider the group of integers $\mathbb{Z}$ under addition. What is the identity element? Find the inverses of the following elements: 5, 0, -19.
(2) Consider the group $\mathbb{Q} \setminus \{0\}$ given in Example 12.4. What is the identity element? Find the inverses of the following elements: $2/3$, 5, 1, -1, $-10/3$.
(3) Is $\mathbb{R}$ a group under addition?
(4) Is $\mathbb{R}$ a group under the operation $a * b = a - b$?

Examples from number theory

EXAMPLE 12.7. Let $n \geq 2$. Then $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ is a group under addition.

PROOF. We go through the four requirements of a group.

(1) Let $\overline{a}, \overline{b} \in \mathbb{Z}_n$.
Then $\overline{a} + \overline{b} = \overline{a+b} \in \mathbb{Z}_n$ by Definition 7.24.
(2) Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$.
Since a, b, and c are integers we have that $(a+b)+c = a+(b+c)$ by assumption ???.
Thus by Definition 7.24 we have that

$$\begin{aligned}(\overline{a} + \overline{b}) + \overline{c} &= \overline{a+b} + \overline{c} = \overline{(a+b)+c} \\ &= \overline{a+(b+c)} = \overline{a} + \overline{b+c} \\ &= \overline{a} + (\overline{b} + \overline{c}).\end{aligned}$$

(3) Let $e = \overline{0}$. Let $\overline{a} \in \mathbb{Z}_n$.
Then $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$ and $\overline{0} + \overline{a} = \overline{0+a} = \overline{a}$.
Hence $\overline{0}$ is an identity element for $\mathbb{Z}_n$.

Let $\overline{a} \in \mathbb{Z}_n$.
Then $\overline{-a} \in \mathbb{Z}_n$.
Furthermore $\overline{a} + \overline{-a} = \overline{a-a} = \overline{0}$ and $\overline{-a} + \overline{a} = \overline{-a+a} = \overline{0}$.
Hence $\overline{-a}$ is an inverse for $\overline{a}$. ■

EXAMPLE 12.8. Consider $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Then $\overline{0}$ is the identity of $\mathbb{Z}_4$. Since $\overline{1} + \overline{3} = \overline{0}$ we have that $\overline{1}$ and $\overline{3}$ are inverses of each other. Since $\overline{2} + \overline{2} = \overline{0}$ we have that $\overline{2}$ is it's own inverse. Since $\overline{0} + \overline{0} = \overline{0}$ we have that $\overline{0}$ is it's own inverse.

12.2. The symmetric group

DEFINITION 12.9. Let G be a group with binary operation $*$. We say that G is **abelian** if $a * b = b * a$ for all $a, b \in G$.

EXAMPLE 12.10. The group $\mathbb{Z}$ under addition is abelian because $a + b = b + a$ for all integers a, b by assumption ???.

12.3. The group of Pythagorean triples

Consider a right triangle with sides x and y and hypotenuse z. See Figure 1. From the Pythagorean theorem, we know that triples of positive numbers (x, y, z) correspond to right triangles with sides x and y and hypotenuse z.

Number Theorists are interested in the properties of numbers. For example, they study the integers and the primes. A classic area that number theorists have studied for hundreds of years is the study of Pythagorean triples.

DEFINITION 12.11. We say that the triple (x, y, z) is a **Pythagorean triple** if x, y, and z are integers that satisfy the equation $x^2 + y^2 = z^2$ and where $z \neq 0$.

EXAMPLE 12.12. $(3, 4, 5)$ is a Pythagorean triple since $3^2 + 4^2 = 5^2$.
$(6, -8, 10)$ is a Pythagorean triple since $6^2 + (-8)^2 = 10^2$.
$(2, 1, 5)$ is not a Pythagorean triple since $2^2 + 1^2 \neq 5^2$.
$(1, 0, 1)$ is a Pythagorean triple since $1^2 + 0^2 = 1^2$. Note that the y coordinate of $(1, 0, 1)$ is zero. $(0, 0, 0)$ is not a Pythagorean triple since the z-coordinate is zero. Note that $(0, 0, 0)$ is the only triple that corresponds to $z \neq 0$.

TOO MUCH INFORMATION 12.13. Notice that there are "more" Pythagorean triples than there are right triangles with integer sides. For example, $(0, 1, 1)$ is a Pythagorean triple since $0^2 + 1^1 = 1^1$, even

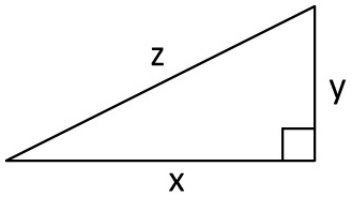


FIGURE 1. A right triangle

though there is no right triangle with side length 0. And $(-3, 4, -5)$ is a Pythagorean triple since $(-3)^2 + 4^1 = (-5)^1$, even though there is no right triangle with sides of negative length.

QUESTIONS 12.14. Number Theorists ask questions like the following:

(1) How many Pythagorean triples are there?
(2) If there are an infinite number of Pythagorean triples how do we generate all of them?
(3) Put Sierpinskis question here.

The answer to Question 1 is yes. There are an infinite number of triples. Let us illustrate this fact. Suppose that (x, y, z) is a Pythagorean triple. Then $x^2 + y^2 = z^2$. Let $\lambda \in \mathbb{Z}$ with $\lambda \neq 0$. Multiplying $x^2 + y^2 = z^2$ by λ^2 on both sides yields $(\lambda x)^2 + (\lambda y)^2 = (\lambda z)^2$. Hence $(\lambda x, \lambda y, \lambda z)$ is a Pythagorean triple.

For example, using $(x, y, z) = (3, 4, 5)$ we get the following Pythagorean triples for various values of λ:

$$\begin{array}{ccccc} & & \vdots & & \\ \lambda = -3 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (-9, -12, -15) \\ \lambda = -2 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (-6, -8, -10) \\ \lambda = -1 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (-3, -4, -5) \\ \lambda = 2 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (6, 8, 10) \\ \lambda = 3 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (9, 12, 15) \\ \lambda = 4 & \text{gives} & (3\lambda, 4\lambda, 5\lambda) & = & (12, 16, 20) \\ & & \vdots & & \end{array}$$

We see that one can get an infinite number of solutions to $x^2 + y^2 = z^2$ given a starting solution. However, we can't get all the solutions starting with just $(3, 4, 5)$. We need more starting triples. For example, $(5, 12, 13)$ is a Pythagorean triple but it is not a multiple of $(3, 4, 5)$.

Think about the following. We started with a triple $(3, 4, 5)$. This triple "generates" an infinite number of triples $(3\lambda, 4\lambda, 5\lambda)$. Here is another example, consider the triple $(297, 1620, 1647)$. Notice that 27 is a divisor of each of the numbers 297, 1620, and 1647. The triple $(297, 1620, 1647)$ comes from multiplying the triple $(11, 60, 61)$ by 27. We can multiply $(11, 60, 61)$ by any non-negative integer and get an infinite number of Pythagorean triples. These triples will differ from the ones gotten from $(3, 4, 5)$. In the following discussion we want to "group together" the triples that arise from a single triple. The way we will do this is with equivalence classes. We first define a relation on the Pythagorean triples.

DEFINITION 12.15. Let P denote the set of all Pythagorean triples. Let $(a, b, c), (x, y, z) \in P$. Define the relation $(a, b, c) \sim (x, y, z)$ iff there exists a non-zero rational number r with $(a, b, c) = (rx, ry, rz)$.

EXAMPLE 12.16. $(9, 12, 15) \sim (3, 4, 5)$ since $(9, 12, 15) = (3 \cdot 3, 3 \cdot 4, 3 \cdot 5)$.
$(-6, -8, -10) \sim (9, 12, 15)$ since $(-6, -8, -10) = ((-2/3) \cdot 9, (-2/3) \cdot 12, (-2/3) \cdot 15)$.

TOO MUCH INFORMATION 12.17. We needed rational numbers in Definition 12.15 because we want $(9, 12, 15)$ and $(-6, -8, -10)$ to be related because they come from the same "smallest" triple $(3, 4, 5)$.

PROPOSITION 12.18. *The relation $\sim$ defined in Definition 12.15 is an equivalence relation on P.*

PROOF. (1) Let $(x, y, z) \in P$.
Then $(x, y, z) = (1 \cdot x, 1 \cdot y, 1 \cdot z)$.
Hence $(x, y, z) \sim (x, y, z)$ since 1 is a non-zero rational number.
Therefore $\sim$ is reflexive.

(2) Let $(a, b, c), (x, y, z) \in P$.
Suppose that $(a, b, c) \sim (x, y, z)$.
Then $(a, b, c) = ((s/t) \cdot x, (s/t) \cdot y, (s/t) \cdot z)$ for some rational number s/t with $s \neq 0$.
Hence $((t/s) \cdot a, (t/s) \cdot b, (t/s) \cdot c) = (x, y, z)$ where t/s is a non-zero rational number.
So $(x, y, z) \sim (a, b, c)$.
Therefore $\sim$ is symmetric.

(3) Let $(a, b, c), (d, e, f), (g, h, i) \in P$.
Suppose that $(a, b, c) \sim (d, e, f)$ and $(d, e, f) \sim (g, h, i)$.
Then $(a, b, c) = (rd, re, rf)$ and $(d, e, f) = (sg, sh, si)$ for some non-zero rational numbers r and s.
Hence $(a, b, c) = (rsg, rsh, rsi)$ where rs is a nonzero rational number.
So $(a, b, c) \sim (g, h, i)$.
Therefore $\sim$ is transitive.

■

NOTATION 12.19. Let $(a, b, c) \in P$ and $\sim$ be as in Definition 12.15. Instead of denoting the equivalence class of (a, b, c) by $\overline{(a, b, c)}$ we will instead use $[(a, b, c)]$.

EXAMPLE 12.20. Consider the triple $(3, 4, 5)$. Some of the elements of $[(3, 4, 5)]$ are listed below.

$$\begin{aligned}[(3,4,5)] \;=\; &\{\ldots, (-12,-16,-20), (-9,-12,-15), (-6,-8,-10),\\ &(-3,-4,-5), (3,4,5), (6,8,10), (9,12,15), (12,16,20), \ldots\}\end{aligned}$$

What we have done is we have grouped together all the multiples of $(3, 4, 5)$ into a single equivalence class.

CHECK FOR UNDERSTANDING 12.21.
(1) List 10 elements in $[(5, 12, 13)]$.
(2) We say that $(x, y, z) \in P$ is **primitive** if the only positive common divisor of x,y, and z is 1. Give an example of a primitive Pythagorean triple. Give an example of a triple that is not primitive.
(3) Let $(a, b, c) \in P$. Show that there exists a primitive Pythagorean triple (x, y, z) with $[(x, y, z)] = [(a, b, c)]$.

DEFINITION 12.22. Let $\Psi = \{[(x, y, z)] \mid (x, y, z) \in P\}$ be the set of equivalence classes of Pythagorean triples.

EXAMPLE 12.23. Here we list a few elements from Ψ:

$$\Psi = \{[(3, 4, 5)], [(5, 12, 13)], [(7, 24, 25)], [(8, 15, 17)], \ldots\}$$

TOO MUCH INFORMATION 12.24. Is Ψ infinite? Yes. We answer this in ??????????????????????????????.

TOO MUCH INFORMATION 12.25. We want a method to generate new Pythagorean triples from ones that we know. Furthermore, we want this method to be better than just multiplying by a number. We want to "break out" of the equivalence class of a triple.
Suppose that we have two Pythagorean triples (a, b, c) and (d, e, f).
Then $a^2 + b^2 = c^2$ and $d^2 + e^2 = f^2$.
Thus $(a^2 + b^2)(d^2 + e^2) = (cf)^2$.
This implies that $(ad - be)^2 + (ae + bd)^2 = (cf)^2$.
Therefore $(ad - be, ae + bd, cf)$ is a Pythagorean triple.
This formula will allow us to generate a new Pythagorean triple from two that we already have. We formulate this in Definition 12.26.

DEFINITION 12.26. Let Ψ be as in Definition 12.22. Define addition on Ψ as follows:

$$[(a, b, c)] \oplus [(d, e, f)] = [(ad - be, ae + bd, cf)]$$

EXAMPLE 12.27. Consider the elements $(2, 3, 5), (5, 12, 13) \in \Psi$. Using Definition 12.26 we see that

$$[(3, 4, 5)] \oplus [(5, 12, 13)] = [(3 \cdot 5 - 4 \cdot 12, 3 \cdot 12 + 4 \cdot 5, 5 \cdot 13)] = [(-33, 56, 65)].$$

Note that $(-33)^2 + 56^2 = 65^2$. Hence $[(-33, 56, 65)] \in \Psi$.

TOO MUCH INFORMATION 12.28. The reader may be wondering why we are defining addition on the set Ψ. Why not just define addition on P? After all, P is a much simpler set. One can do this, however P is not a group under the above addition, while Ψ is. (You need equivalence classes to get an identity element for the group of Pythagorean triples. See Prop 12.30.)

TOO MUCH INFORMATION 12.29. The reader may be wondering if the addition defined in Definition 12.26 is well-defined. It is. We will prove this fact in Proposition 12.30. In this remark we want to remind the reader why we need to check this fact. Note that $[(3,4,5)] = [(6,8,10)]$ and $[(5,12,13)] = [(-10,-24,-26)]$. In fact $[(3,4,5)]$ can be written in an infinite number of ways. Same for $[(5,12,13)]$. However, the addition of $[(3,4,5)]$ and $[(5,12,13)]$ shouldn't be influenced by the way we represent the triples $[(3,4,5)]$ and $[(5,12,13)]$.

For example, we saw in Example 12.27 that $[(3,4,5)] \oplus [(5,12,13)] = [(-33,56,65)]$. If $\oplus$ is well-defined on Ψ then we should have that

$$[(6,8,10)] \oplus [(-10,-24,-26)] = [(3,4,5)] \oplus [(5,12,13)].$$

Indeed,

$$\begin{aligned}
[(6,8,10)] \oplus [(-10,-24,-26)] &= [(6\cdot(-10) - 8\cdot(-24), 6\cdot(-24) + 8\cdot(-10), 10\cdot(-26))] \\
&= [(132,-224,-260)] \\
&= [(4\cdot(-33), 4\cdot 56, 4\cdot 65)] \\
&= [(-33,56,65)] \\
&= [(3,4,5)] \oplus [(5,12,13)].
\end{aligned}$$

PROPOSITION 12.30. *Ψ is a group under the operation*

$$[(a,b,c)] \oplus [(d,e,f)] = [(ad-be, ae+bd, cf)].$$

The identity element is $[(1,0,1))]$. The inverse of $[(a,b,c]$ is $[(a,-b,c)]$.

PROOF. ⟨*We begin by checking that $\oplus$ is well-defined.*⟩
Suppose that (a,b,c) and (d,e,f) are Pythagorean triples.
Suppose that we have another representation $[(\lambda a, \lambda b, \lambda c)]$ of $[(a,b,c)]$ and another representation $[(\beta d, \beta e, \beta f)]$ of $[(d,e,f)]$ where λ and β are non-zero rational numbers.

Then

$$\begin{aligned}[(\lambda a, \lambda b, \lambda c)] \oplus [(\beta d, \beta e, \beta f)] &= [(\lambda\beta ad - \lambda\beta be, \lambda\beta ae + \lambda\beta bd, \lambda\beta cf)] \\ &= [(ad - be, ae + bd, cf)] \\ &= [(a, b, c)] \oplus [(d, e, f)].\end{aligned}$$

Hence $\oplus$ is well-defined.
⟨*We now check that the four group properties hold.*⟩

(1) Let (a, b, c) and (d, e, f) be Pythagorean triples.
Then $a^2 + b^2 = c^2$ and $d^2 + e^2 = f^2$.
By multiplying the two equations given in the line above, we have that $(ad - be)^2 + (ae + bd)^2 = (cf)^2$.
Hence $[(a, b, c)] \oplus [(d, e, f)] = [(ad - be, ae + bd, cf)]$ is in Ψ.

(2) Let (a, b, c), (d, e, f), and (g, h, i) be Pythagorean triples.
Then

$$\begin{aligned}([(a, b, c)] \oplus [(d, e, f)]) \oplus [(g, h, i)] &= [(ad - be, ae + bd, cf)] \oplus [(g, h, i)] \\ &= [(adg - beg - aeh - bdh, adh - beh + aeg + bdg, cfi)] \\ &= [(a, b, c)] \oplus [(dg - eh, dh + eg, fi)] \\ &= [(a, b, c)] \oplus ([(d, e, f)] \oplus [(g, h, i)])\end{aligned}$$

Hence $\oplus$ is associative.

(3) Let (a, b, c) be a Pythagorean triple.
Then

$$\begin{aligned}[(a, b, c)] \oplus [(1, 0, 1)] &= [(a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1, c \cdot 1)] \\ &= [(a, b, c)].\end{aligned}$$

and

$$\begin{aligned}[(1, 0, 1)] \oplus [(a, b, c)] &= [(1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a, 1 \cdot c)] \\ &= [(a, b, c)].\end{aligned}$$

Hence $[(1, 0, 1)]$ is an identity element for Ψ.

(4) Let (a, b, c) be a Pythagorean triple.
Then $(a, -b, c)$ is a Pythagorean triple.
Note that

$$\begin{aligned}[(a, b, c)] \oplus [(a, -b, c)] &= [(a^2 + b^2, -ab + ba, c^2)] \\ &= [(c^2, 0, c^2)] \\ &= [(1, 0, 1)]\end{aligned}$$

and

$$\begin{aligned}[(a,-b,c)] \oplus [(a,-b,c)] &= [(a^2+b^2, ab-ba, c^2)] \\ &= [(c^2,0,c^2)] \\ &= [(1,0,1)]\end{aligned}$$

Hence $[(a,-b,c)]$ is an inverse for $[(a,b,c)]$ in Ψ.

■

12.4. Exercises

(1) Consider the unit circle

$$U = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}.$$

Show the U is a group under the operation

$$(x_1,y_1) * (x_2,y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

The identity element is $(1,0)$. The inverse of (x,y) is $(x,-y)$.

(2) Consider the set

$$H = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x^2 - y^2 = 1\}.$$

Show that H is a group under the operation

$$(x_1,y_1) * (x_2,y_2) = (x_1x_2 + y_1y_2, x_1y_2 + x_2y_1).$$

The identity element is $(1,0)$ and the inverse of (x,y) is $(x,-y)$.

Chapter 13

The Standard Number Systems

Throughout this book, we've been working a great deal with some fairl y standard number systems: the natural numbers, the integers, the rational numbers, the real numbers, and the complex numbers. We've proved many statements about these sets: that every natural number can be factored into primes, that $\sqrt{2}$ is not rational, that the set of real numbers is uncountable, etc. Along the way, we've emphasized how important it is to carefully define all terms. And yet, we've been sloppy about what exactly numbers are. We have not given a rigorous definition of 47, for example. In this chapter, we begin to rectify that situation.

There is a problem with trying to define everything and prove everything. For example, we defined an integer to be even if it is divisible by 2. Well, what's the definition of 2? You could define 2 as 1 plus 1. But then you could ask, what's the definition of 1, and what's the definition of "plus"? And so on. Eventually, your definitions would either be circular, or they would never end.

We run into a similar problem if we try to prove every single statement we claim is true. Because no matter what statement you write as a justification, you can always ask, "How do you know that *that* statement is true?" Your reasoning will either become circular or will never end.

The solution to both problems is essentially the same: We begin with terms we do not attempt to define, and statements we do not attempt to prove. These undefined terms and assumptions serve as the starting point for all of mathematics. The assumptions will tell us what we can say about the undefined terms. While we will not prove

the assumptions, we will agree that they are true and deduce whatever we can from them.

We could take, say, Fermat's little theorem as one of our starting assumptions. But that would feel like cheating, because it's not at all obvious that p divides $a^p - a$ whenever p is prime and a is a natural number. So we should make as few assumptions as possible, and what little we do assume should be as self-evident as possible. One of our starting assumptions, for example, will be that 1 is a natural number. We will neither prove this fact nor define the terms "1" and "natural number." However, assuming that 1 is a natural number should not cause a great deal of controversy. It seems reasonable to agree to that fact without asking for a proof of it. That's exactly what we look for in an assumption.

Remarkably, all of the amazing theorems in this book and others follow from just a few basic assumptions about the natural numbers. We don't even need to make assumptions about the other standard number systems (integers, rationals, etc.), because once we have the natural numbers, we can *define* those other sets (and all the fun things that go with them, like addition, subtraction, and so on) and *prove* things about them. In this chapter, we take the standard approach, where we begin with $\mathbb{N}$, then use $\mathbb{N}$ to define $\mathbb{Z}$, then use $\mathbb{Z}$ to define $\mathbb{Q}$, then use $\mathbb{Q}$ to define $\mathbb{R}$, and then finally use $\mathbb{R}$ to define $\mathbb{C}$.

Too Much Information 13.1. All of these definitions will make use only of previously defined terms, and of the language of set theory (functions, Cartesian products, relations, etc.). For example, in the final step in our chain of constructions, we will define the complex numbers. By that point, we will have defined the real numbers. So we will want to define, for example, the imaginary number i. In other textbooks, you may have seen i defined as $\sqrt{-1}$. In this chapter, however, we will not allow such a definition. For one thing, we do not know that $\sqrt{-1}$ exists; for another, we must describe it using only real numbers and the language of set theory. Instead, we will define i to be the ordered pair $(0, 1)$. That's allowable, because all it uses are 0 and 1 (real numbers, previously defined) and an ordered pair (set theory concept). Now, how does $(0, 1)$ match up with our usual notion of i? And what about all the other numbers in the world, like 47 and -6 and $22/7$ and e and so on—how do we define them? To find out, read on.

13.1. The natural numbers

What are the most fundamental properties of the natural numbers? What distinguishes this collection of numbers from others? One element of $\mathbb{N}$ catches our attention right from the beginning, namely 1. We observe that every element has another element that comes "right after" it. For example, 33 comes right after 32. The number 1, however, does not come right after any other natural number. (It comes right after 0, but $0 \notin \mathbb{N}$.) We begin by making a definition along these lines to capture the essential nature of $\mathbb{N}$.

DEFINITION 13.2. Let N be a set, let $m \in N$, and let $q\colon N \to N$ be a function. We say (N, m, q) is a **natural number system** if:

(1) There does not exist $n \in N$ such that $q(n) = m$, and
(2) The function q is injective, and
(3) If A is a subset of N such that $m \in A$ and $q(n) \in A$ whenever $n \in A$, then $N = A$.

TOO MUCH INFORMATION 13.3. The various parts of Definition 13.2 are called the Peano axioms. They are named after Giuseppe Peano, the mathematician who first formulated them. The word "axiom" can mean either an assumption that we make, or a fundamental defining property of an object.

To get our heads around Definition 13.2, let's do some examples. For the sake of these examples, let's temporarily forget that we have not yet rigorously defined anything.

EXAMPLE 13.4. Define $P : \mathbb{Z} \to \mathbb{Z}$ by $S(n) = n + 1$. Is $(\mathbb{Z}, 1, P)$ a natural number system?

Answer: No, it is not, because $P(0) = 1$, so Axiom (1) fails. (Note that P takes the place of q, and 1 takes the place of m.)

EXAMPLE 13.5. Let $T = \{2, 4, 8, 16, \dots\}$ be the set of all powers of 2. Define $Q\colon T \to T$ by $Q(n) = 2n$. Is $(T, 2, Q)$ a natural number system?

Answer: Let's check every part of Definition 13.2, substituting T for N, 2 for m, and Q for q.

First note that T is a set, $2 \in T$, and $Q\colon T \to T$.

Axiom (1) holds, because there is no $n \in T$ such that $2n = 2$.

Axiom (2) holds, because if $2n = 2m$, then $n = m$.

Axiom (3) holds, because if A is a subset of T such that $2 \in A$ and $2n \in A$ whenever $n \in A$, then $T = A$. (Think about it this way: once you have $2 \in A$, then you get $4 \in A$, then $8 \in A$, and so on.)

Therefore, $(T, 2, Q)$ is a natural number system.

TOO MUCH INFORMATION 13.6. In Example 13.5, we are *not* saying that T is the set of natural numbers. It is not. Instead, T is a natural number *system*. We will see later that this simply means that is has the same basic structure as the natural number: a starting element followed by another element, then another, and so on.

EXAMPLE 13.7. Define $R\colon \mathbb{N} \to \mathbb{N}$ by $R(n) = n + 2$. Is $(\mathbb{N}, 1, R)$ a natural number system?

Answer: No, it is not, and here's why. Let A be the set of odd natural numbers. Note that $1 \in A$ and that $n + 2 \in A$ whenever $n \in A$. However, $\mathbb{N} \neq A$. So Axiom (3) fails.

TOO MUCH INFORMATION 13.8. In fact, in Example 13.7, every part of Definition 13.2 holds expect for Axiom (3). This shows that we really do want to include Axiom (3), because it cannot be proved from the others. In other words, Axiom (3) is independent of the other axioms. In Exercises 1 and 2, you will prove that Axioms (1) and (2) are also independent of the others.

CHECK FOR UNDERSTANDING 13.9.
(1) Let B be the set of negative integers. Define $f\colon B \to B$ by $f(n) = n - 1$. Is $(B, -1, f)$ a natural number system?
(2) Define $g\colon \mathbb{N} \to \mathbb{N}$ by $g(n) = n + 1$. Is $(\mathbb{N}, 2, g)$ a natural number system?

If we could, we would prove the following theorem: "Let $\mathbb{N}$ be the set of natural numbers, and define $S\colon \mathbb{N} \to \mathbb{N}$ by $S(n) = n + 1$. Then $(\mathbb{N}, 1, S)$ is a natural number system." However, we cannot prove that, because we don't have anywhere to start. So instead, we take $\mathbb{N}, 1$, and S to be undefined terms, and we simply assume that they form a natural number system.

<MAKE THE FOLLOWING ASSUMPTION STAND OUT, WITH LIKE RAYS OF SUNSHINE COMING OUT OF IT OR SOMETHING.>

ASSUMPTION 13.10. *There exists a natural number system* $(\mathbb{N}, 1, S)$.

DEFINITION 13.11. An element of $\mathbb{N}$ is a **natural number**.

TOO MUCH INFORMATION 13.12. Some authors include 0 as a natural number, in which case 0 takes the place of 1 in Assumption 13.10.

$(\mathbb{N}, 1, S)$	$1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto \cdots$
$(\{2, 4, 8, 16, \dots\}, 2, n \mapsto 2n)$	$2 \mapsto 4 \mapsto 8 \mapsto 16 \mapsto \cdots$
$(\{-1, -2, -3, -4, \dots\}, -1, n \mapsto n - 1)$	$-1 \mapsto -2 \mapsto -3 \mapsto -4 \mapsto \cdots$

TABLE 1. Three different natural number systems

Note that Definition 13.2 does not refer anywhere to addition, order, quantity, measurement, or counting. It is phrased entirely in the language of set theory: elements, functions, subsets, etc. So the concept of number can be expressed entirely in terms of sets and functions.

The letter S is often used for the function in Assumption 13.10. It stands for "successor," that is, the one that comes immediately afterwards. So intuitively, think of S as the function $S(n) = n+1$. But this is not a rigorous definition of S, because "+" has not yet been defined. In fact, we will later use S to define addition!

While 1 is an undefined term, we can now define the other natural numbers in terms of 1 and S. For example, the definition of 2 is $2 := S(1)$. Similarly, $3 := S(S(1))$, $7 := S(S(S(S(S(S(1))))))$, etc. We will use the usual decimal representation for natural numbers from now on, and trust that if pressed, you can convert them into expressions using only 1 and S.

Axiom (1) from Assumption 13.2 says that there is no natural number n such that $S(n) = 1$. (Intuitively, this means that there is no natural number n such that $n+1 = 1$.) Axiom (2) says that if $S(n) = S(m)$, then $n = m$. (Or intuitively, that $n+1 = m+1$ implies $n = m$.) Axiom (3) is the principle of mathematical induction.

While we can continue to think of $\mathbb{N}$ and 1 in the familiar ways we're used to, and think of S as the function $n \mapsto n + 1$, the only statements about them we can assume to be true without proving them are those spelled out in the definition of a natural number system. To justify any other claim about numbers, we must produce a chain of logic that ultimately begins with Assumption 13.10.

Between Example 13.5, Check for Understanding 13.9(1), and Assumption 13.10, we have three examples of natural number systems. Notice that all three have a similar structure. As illustrated by Table 1, each has a starting element; each element has an immediate successor; and for each element, there is a unique way to trace back to the starting element in finitely many steps.

DEFINITION 13.13. Let (N, m, S) be a natural number system. Let $a \in N$, and let $b = S(a)$. Then b is the **successor** of a, and a is the **predecessor** of b.

EXAMPLE 13.14. In the natural number system $(T, 2, Q)$ from Example 13.5, what is the successor of 4? What are the predecessor(s) of 64? Which elements of T do not have predecessors in T?

Answer: The successor of 4 is $Q(4) = 8$.

The predecessor of 64 is 32, because $Q(32) = 64$. There are no other predecessors of 64.

The element 2 does not have a predecessor in T, because there does not exist $a \in T$ such that $Q(a) = 2$.

CHECK FOR UNDERSTANDING 13.15. In the natural number system $(\mathbb{N}, 1, S)$, what is the successor of 4? What are the predecessor(s) of 1729? Which elements of $\mathbb{N}$ do not have predecessors in $\mathbb{N}$?

After studying Table 1 for a bit, and after considering Example 13.14 and Check for Understanding 13.15, we may conjecture that in a natural number system (N, m, q), the element m is the only one without a predecessor, and that every other element has exactly one predecessor. Our next lemma says precisely that.

LEMMA 13.16. *Let (N, m, q) be a natural number system. Let $b \in N$. If $b \neq m$, then b has a unique predecessor.*

PROOF. First, we will show that b has a predecessor.

We will prove this by contradiction.

Temporarily assume that b does not have a predecessor.

Let $A = N \setminus \{b\}$.

Then $m \in A$, because $m \neq b$.

We will show that $q(n) \in A$ whenever $n \in A$.

Let $n \in A$. We will show that $q(n) \in A$.

We know that $q(n) \neq b$, because $q(n)$ has a predecessor (namely, n), but b does not have a predecessor.

So $q(n) \in A$, because $q(n) \neq b$.

We have shown that $m \in A$ and $q(n) \in A$ whenever $n \in A$.

So by Definition 13.2(3), therefore $N = A$.

But $b \in N$ and $b \notin A$, so N cannot be a subset of A.
Contradiction.
Therefore, b has a predecessor.
Next, we will show that b has a unique predecessor.
Let a_1 and a_2 be predecessors of b.
We will show that $a_1 = a_2$.
By definition of predecessor, $q(a_1) = q(a_2) = b$.
By Definition 13.2, we know that q is injective.
By definition of injective, $a_1 = a_2$.
Therefore, b has a unique predecessor. ■

Consider the three natural numbers systems shown in Table 1. Observe that they each have the same structure: an initial element followed by its successor, then the successor of the successor, and so on. So it seems as if any two natural number systems are essentially the same. Let's formulate this conjecture more precisely. What do we mean by "essentially the same"? Suppose we have two natural number systems (N_1, m_1, q_1) and (N_2, m_2, q_2). There always appears to be a one-to-one correspondence between N_1 and N_2. In this correspondence, we should send the initial element to the initial element m_1 to m_2. And if a maps to b, then the successor of a should map to the successor of b. Figure 1 illustrates the sort of correspondence we wish to construct.

Our description of the correspondence we'd like tells us exactly how to construct it. First, map m_1 to m_2. Then map $q_1(m_1)$ to $q_2(m_2)$. Then map $q_1(q_1(m_1))$ to $q_2(q_2(m_2))$, and so on.

The proof of this theorem will illustrate a common technique at this stage the game. To prove a statement is true for all elements of a natural number system (N, m, q), often we let A be the set of all elements of N for which it is true. We then show that $m \in A$ and that $q(n) \in A$ whenever $n \in A$. So by Definition 13.2, $A = N$, and therefore the statement is true for all $n \in N$. Essentially, this is induction. We use it a lot at this point because there is very little else we know at this point!

$$\begin{array}{ccccccccc} 2 & \overset{Q}{\longmapsto} & 4 & \overset{Q}{\longmapsto} & 8 & \overset{Q}{\longmapsto} & 16 & \overset{Q}{\longmapsto} & \cdots \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\ -1 & \overset{B}{\longmapsto} & -2 & \overset{B}{\longmapsto} & -3 & \overset{B}{\longmapsto} & -4 & \overset{B}{\longmapsto} & \cdots \end{array}$$

FIGURE 1. A correspondence between two natural number systems

THEOREM 13.17. *Let (N_1, m_1, q_1) and (N_2, m_2, q_2) be natural number systems. Then there is a bijection $f\colon N_1 \to N_2$ such that $f(m_1) = m_2$ and $f(q_1(a)) = q_2(f(a))$ for all $a \in N_1$.*

PROOF. Define $f\colon N_1 \to N_2$ by

$$f(b) = \begin{cases} m_2 & \text{if } b = m_1 \\ q_2(f(a)) & \text{if } b = q_1(a). \end{cases}$$

Note that Lemma 13.16 guarantees that f is well-defined.

By definition of f, we have that $f(m_1) = m_2$.

So we must show that f is a bijection and that $f(q_1(a)) = q_2(f(a))$ for all $a \in N_1$.

First, we will show that f is a bijection.

To do so, we will show that f has an inverse function.

Define $g\colon N_2 \to N_1$ by

$$g(b) = \begin{cases} m_1 & \text{if } b = m_2 \\ q_1(f(a)) & \text{if } b = q_2(a). \end{cases}$$

Lemma 13.16 guarantees that g is well-defined.

We will show that g is the inverse of f.

First, we will show that $g \circ f = i_{N_1}$, where i_{N_1} is the identity function on N_1.

We will show that $(g \circ f)(b) = b$ for all $b \in N_1$.

Let $A = \{b \in N_1 \mid (g \circ f)(b) = b\}$.

Now, $(g \circ f)(m_1) = g(f(m_1)) = g(m_2) = m_1$.

So, $m_1 \in A$.

Now, suppose that $n \in A$. We will show that $q_1(n) \in A$.

The predecessor of $q_1(n)$ is n.

So by definition of f, we have that $f(q_1(n)) = q_2(f(n))$.

The predecessor of $q_2(f(n))$ is $f(n)$.

So by definition of g, we have that $g(q_2(f(n))) = q_1(g(f(n)))$.

So

$$\begin{aligned} (g \circ f)(q_1(n)) &= g(f(q_1(n))) \\ &= g(q_2(f(n))) \\ &= q_1(g(f(n))) \\ &= q_1((g \circ f)(n)) \\ &= q_1(n), \text{ because } n \in A. \end{aligned}$$

Therefore $q_1(n) \in A$, by definition of A.
So $m_1 \in A$ and $q_1(n) \in A$ whenever $n \in A$.
Hence, by Definition 13.2, $A = N_1$.
Therefore, $(g \circ f)(b) = b$ for all $b \in N_1$, by definition of A.
Therefore, $g \circ f = i_{N_1}$.
Similarly, we can prove that $f \circ g = i_{N_2}$.
Therefore, g is the inverse function of f.
Therefore, f is bijective.
Lastly, we must show that $f(q_1(a)) = q_2(f(a))$ for all $a \in N_1$. We will leave this part of the proof for you to do in Exercise 3. ■

Too Much Information 13.18. Theorem 13.17 shows that any two natural number systems have the same essential structure. The mathy way to say this is that they are *isomorphic*. The function f is an *isomorphism*. Isomorphisms appear in many branches of math. In Abstract Algebra class, you will encounter them when you study group theory; two groups are isomorphic if they are essentially the same. In topology, isomorphisms are called homeomorphisms, but it's the same concept. In all cases, the isomorphism acts like a dictionary that lets you "translate" elements of one set to the equivalent element in the other set. For example, in Figure 1, the element 16 in the top natural number system corresponds to the element -4 in the bottom one. Each is the fourth element in the list, so they play the same role in the natural number system.

The fact that any two natural number systems are isomorphic makes us feel better about Assumption 13.10, because it means that anything you prove about any one particular natural number system will automatically translate into a true statement about every natural number system.

13.1.1. Operations on natural numbers. A pretty basic thing we want to do with numbers is add them. How can we define addition, when we have only the symbols $\mathbb{N}$, 1, and S to play with? Recall that we intuitively think of S as the function $n \mapsto n + 1$. So we should *define* $n + 1$ to be $S(n)$. Now how to define $n + 2$? We want $n + 2 = (n + 1) + 1 = S(n + 1)$, which is legitimate, because $n + 1$ has already been defined. Then define $n + 3 = S(n + 2)$, and $n + 4 = S(n + 3)$, and so on. The phrase "and so on" suggests that we are using induction, so to be precise about it, we should make this a recursive definition.

DEFINITION 13.19 (Addition of natural numbers). We define the binary operation + on $\mathbb{N}$ by

$$n+m=\begin{cases} S(n) & \text{if } m=1 \\ S(n+a) & \text{if } m=S(a). \end{cases}$$

Lemma 13.16 guarantees that Definition 13.19 is well-defined.

EXAMPLE 13.20. Use Definition 13.19 to find $5+3$.

Answer: By Definition 13.19, we get $5+3=S(5+2)$, because $3=S(2)$.

By Definition 13.19, we get $5+2=S(5+1)$, because $2=S(1)$.

By Definition 13.19, we get $5+1=S(5)$.

So $5+3=S(5+2)=S(S(5+1))=S(S(S(5)))=S(S(6))=S(7)=8$.

CHECK FOR UNDERSTANDING 13.21. Use Definition 13.19 to find $12+4$.

TOO MUCH INFORMATION 13.22. Your friends will never believe it when you tell them that this is what you learned in math today.

Of course, you know that addition is commutative. For example, $5+3=3+5$, and $12+4=4+12$. In general, $a+b=b+a$. But now, we can prove it. To do so, as in our previous proofs, we will use induction. The catch is that there are two variables, so we will need to do two inductions, one for a, and one for b.

THEOREM 13.23 (Commutative property of addition for natural numbers). *We have that $a+b=b+a$ for all $a,b\in\mathbb{N}$.*

PROOF. Let $A=\{a\in\mathbb{N}\mid a+b=b+a \text{ for all } b\in\mathbb{N}\}$.

We will show that $\mathbb{N}=A$.

To do so, we will show that $1\in A$ and that $S(n)\in A$ whenever $n\in A$.

First, we will show that $1\in A$.

That is, we will show that $1+b=b+1$ for all $b\in\mathbb{N}$.

Let $B=\{b\in\mathbb{N}\mid 1+b=b+1\}$.

We will show that $\mathbb{N}=B$.

To do so, we will show that $1 \in B$ and that $S(n) \in B$ whenever $n \in B$.

We know that $1 \in B$, because $1 + 1 = 1 + 1$.

Now suppose that $n \in B$. We will show that $S(n) \in B$.

That is, we will show that $1 + S(n) = S(n) + 1$.

We have that

$$\begin{aligned} 1 + S(n) &= S(1 + n) && \text{by Definition 13.19} \\ &= S(n + 1) && \text{because } n \in B \\ &= S(S(n)) && \text{by Definition 13.19} \\ &= S(n) + 1 && \text{by Definition 13.19} \end{aligned}$$

So $S(n) \in B$.

We have shown that $1 \in B$ and $S(n) \in B$ whenever $n \in B$.

Therefore $\mathbb{N} = B$, by Definition 13.2.

So $1 + b = b + 1$ for all $b \in \mathbb{N}$, by definition of B.

Therefore $1 \in A$, by definition of A.

Now suppose that $n \in A$. We will show that $S(n) \in A$.

That is, we will show that $S(n) + b = b + S(n)$ for all $b \in \mathbb{N}$.

Let $C = \{b \in \mathbb{N} \mid S(n) + b = b + S(n)\}$.

We will show that C contains all natural numbers.

To do so, we will show that $1 \in C$ and that $S(x) \in C$ whenever $x \in C$.

First, we will show that $1 \in C$.

We know that $S(n) + 1 = 1 + S(n)$, because we have previously shown that $1 \in A$.

So $1 \in C$, by definition of C.

Now suppose that $x \in C$. We will show that $S(x) \in C$.

We must show that $S(n) + S(x) = S(x) + S(n)$.

We have that

$$\begin{aligned} S(n) + S(x) &= S(S(n) + x) && \text{by Definition 13.19} \\ &= S(x + S(n)) && \text{because } x \in C \\ &= S(S(x + n)) && \text{by Definition 13.19} \\ &= S(S(n + x)) && \text{because } n \in A \\ &= S(n + S(x)) && \text{by Definition 13.19} \\ &= S(S(x) + n) && \text{because } n \in A \\ &= S(x) + S(n) && \text{by Definition 13.19} \end{aligned}$$

So $S(x) \in C$, by definition of C.

We have shown that $1 \in C$ and that $S(x) \in C$ whenever $x \in C$.

Therefore $\mathbb{N} = C$, by Definition 13.2.
So $S(n) + b = b + S(n)$ for all $b \in \mathbb{N}$, by definition of C.
So $S(n) \in A$.
Therefore $S(n) \in A$ whenever $n \in A$.
We have shown that $1 \in A$ and that $S(n) \in A$ whenever $n \in A$.
So $\mathbb{N} = A$, by Definition 13.2.
Therefore, by definition of A, for all $a \in \mathbb{N}$, it is true that $a+b = b+a$ for all $b \in \mathbb{N}$.
In other words, $a + b = b + a$ for all $a, b \in \mathbb{N}$. ■

Too Much Information 13.24. You may be surprised that it takes so much work to prove such an obvious fact. Take a moment to marvel, though, at the fact that we have just proved infinitely many things. We have just proved that a googol plus a googolplex equals a googolplex plus a googol. We have just proved that my favorite number plus your favorite number equals your favorite number plus mine, without even knowing what those numbers are. In that light, maybe this proof wasn't so long after all. The fact that we can prove infinitely many things in a finite amount of time is quite remarkable.

Another basic fact about addition of natural numbers is the associative property, that is, the fact that $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{N}$. We will leave the proof of this fact for you as an exercise (Exercise 6). Be aware that because there are three variables, you should expect to have to do *three* inductions, one for each variable.

Now, let's define multiplication of natural numbers. This time, we have not only $\mathbb{N}$, 1, and S to work with, we also have addition, because we've defined it. Intuitively, multiplication is repeated addition, so our definition should capture that. We want $a \cdot 1 = a$ for all $a \in \mathbb{N}$. Then we want $a \cdot 2 = a \cdot (1 + 1) = a \cdot 1 + a \cdot 1$, which has meaning once $a \cdot 1$ is defined. Next we'll want $a \cdot 3 = a \cdot 2 + a \cdot 1$, which is legitimate so long as $a \cdot 2$ and $a \cdot 1$ have been defined. So first, we'll define $a \cdot 1$, and then $a \cdot 2$ in terms of $a \cdot 1$, then $a \cdot 3$ in terms of $a \cdot 2$ and $a \cdot 1$, and so on. As with addition, the phrase "and so on" suggests that a recursive definition is in order.

Definition 13.25 (Multiplication of natural numbers). We define the binary operation $\cdot$ on $\mathbb{N}$ by

$$n \cdot m = \begin{cases} n & \text{if } m = 1 \\ n \cdot a + n & \text{if } m = S(a). \end{cases}$$

Now we have two structures on $\mathbb{N}$, addition and multiplication. Having defined them, we want to establish how they relate to themselves and to each other. Some of the basic facts to establish along these lines are the identity, commutative, associative, and distributive properties. See Table 2 on page 298. In Theorem 13.28, we will prove the identity property of multiplication. In the exercises, you will be asked to prove the others, using nothing but facts we have established up to this point. After proving Theorem 13.28, we will make free use of the other addition and multiplication properties listed in Table 2 on page 298.

DEFINITION 13.26. Let $*$ be a binary operation on a set A, and let $e \in A$. We say that e is an **identity element** for A with respect to $*$ if for all $x \in A$, we have that $e * x = x * e = x$.

TOO MUCH INFORMATION 13.27. If you take an Abstract Algebra course in the future, be sure to remember this definition of an "identity element." In that class, you will study mathematical objects called groups, and the existence of an identity element is one of the defining axioms for a group.

THEOREM 13.28 (Identity property of multiplication for natural numbers). *For all $a \in \mathbb{N}$, we have that $1 \cdot a = a \cdot 1 = a$. In other words, 1 is an identity element for $\mathbb{N}$ with respect to multiplication.*

PROOF. By Definition 13.25, we know that $a \cdot 1 = a$ for all $a \in \mathbb{N}$.

So we will show that $1 \cdot a = a$ for all $a \in \mathbb{N}$.

Let $A = \{a \in \mathbb{N} \mid 1 \cdot a = a\}$.

We will show that $\mathbb{N} = A$.

To do so, we will show that $1 \in A$ and that $S(n) \in A$ whenever $n \in A$.

First, we will show that $1 \in A$.

We know that $1 \cdot 1 = 1$, by Def. 13.25.

So $1 \in A$, by definiton of A.

Now, let $n \in A$. We will show that $S(n) \in A$.

By definition of A, we know that

$$1 \cdot n = n. \tag{5}$$

We will show that $1 \cdot S(n) = S(n)$.

We know that

$$\begin{aligned} 1 \cdot S(n) &= 1 \cdot n + 1 && \text{by Definition 13.25} \\ &= n + 1 && \text{by equation (5)} \\ &= S(n). && \text{by Definition 13.19} \end{aligned}$$

We have shown that $1 \in A$ and that $S(n) \in A$ whenever $n \in A$. Therefore, by Definition 13.2, $\mathbb{N} = A$.

Therefore $1 \cdot a = a$ for all $a \in \mathbb{N}$. ■

Too Much Information 13.29. We sometimes abbreviate "1 is an identity element for $\mathbb{N}$ with respect to multiplication" by saying that 1 is a multiplicative identity for $\mathbb{N}$.

In fact, 1 is the only multiplicative identity for $\mathbb{N}$—see Exercise 7.

From now on, we will not hesitate to use other standard notations for multiplication, such as ab instead of $a \cdot b$, or $5(6)$ instead of $5 \cdot 6$, etc.

With the addition and multiplication properties from Table 2 on page 298 in hand, we can loop back around to some of the very first proofs we did way back in Chapter 4, but now we can prove every single step with complete rigor.

Example 13.30. Let $k, \ell \in \mathbb{N}$. Prove in minute detail that $\exists m \in \mathbb{N}$ such that $2k + (2\ell + 1) = 2m + 1$.

Proof. We know that

$$\begin{aligned} 2k + (2\ell + 1) &= (2k + 2\ell) + 1 && \text{by the associative property of addition} \\ &= 2(k + \ell) + 1 && \text{by the distributive property} \end{aligned}$$

Let $m = k + \ell$. Then $2k + (2\ell + 1) = 2m + 1$ by substitution. ■

Too Much Information 13.31. In Example 13.30, we have avoided saying, "Prove that an even natural number plus an odd natural number is odd," because the definitions of "even" and "odd" refer to the set of integers, which we have not yet defined.

Too Much Information 13.32. The first several proofs in this chapter were quite cumbersome, because we had virtually no tools to work with and so had to rely on the rather clunky axioms to make any progress. Once we have the properties listed in Table 2 on page 298, though, we can do proofs such as the one in Example 13.30 much more efficiently.

Check for Understanding 13.33. Let $k, \ell \in \mathbb{N}$. Prove in minute detail that $\exists m \in \mathbb{N}$ such that $(2k + 1) + (2\ell + 1) = 2m + 1$.

In Theorem 13.28, we proved that 1 is a multiplicative identity for the natural numbers. Is there an additive identity for $\mathbb{N}$? In other words, does there exist $n \in \mathbb{N}$ such that $x+n = n+x = x$ for all $x \in \mathbb{N}$? The only reasonable candidate is 0, but 0 is not a natural number. Our next lemma will establish that in $\mathbb{N}$, the equation $x + n = x$ can never hold.

LEMMA 13.34. *Let $x, n \in \mathbb{N}$. Then $x + n \neq x$.*

PROOF. Temporarily assume $x + n = x$.

Then $(x + n) + 1 = x + 1$.

So $[(x + n) + 1] + 1 = (x + 1) + 1$.

So $[x + (n + 1)] + 1 = (x + 1) + 1$, by the associative property of addition.

So $[x + (1 + n)] + 1 = (x + 1) + 1$, by the commutative property of addition.

So $[(x + 1) + n] + 1 = (x + 1) + 1$, by the associative property of addition.

So $(x + 1) + (n + 1) = (x + 1) + 1$, by the associative property of addition.

So $n + 1 = 1$, by the cancellation property of addition.

So $S(n) = 1$, by Definition 13.19.

But this contradicts Axiom (1) from Definition 13.2.

Therefore $x + n \neq x$. ■

QUESTION 13.35. In the proof of Lemma 13.34, we began by adding 1 to both sides of the equation twice. Why couldn't we have just done it once?

13.1.2. Ordering the natural numbers. So far, we have made an assumption about the natural numbers, defined addition and multiplication, and proved a few basic facts about them. We now want to define one more fundamental feature of $\mathbb{N}$, namely its ordering. That is, we will define the $<$ symbol. Our definition of $<$ should correspond to our usual notion of "less than." So $36 < 47$ should be true, for example, but $5 < 3$ should not. How can we explain why $36 < 47$ is true solely in terms of addition and multiplication in $\mathbb{N}$? Intuitively, 36 is less than 47 because you must increase 36 to get 47. Which previously defined concept captures the notion of "increasing"? Well, addition. We know $36 < 47$, because $36 + 11 = 47$, and $11 \in \mathbb{N}$. Adding two natural numbers produces a third that is larger than either.

DEFINITION 13.36. We define the relation $<$ on $\mathbb{N}$ by $x < y$ iff there exists $n \in \mathbb{N}$ such that $x + n = y$. We define the relation $\leq$ on $\mathbb{N}$ by $x \leq y$ iff $x < y$ or $x = y$.

TOO MUCH INFORMATION 13.37. Many other related notations derive from Definition 13.36. For example, $y > x$ means $x < y$, and $x \leq y < z$ means $x \leq y$ and $y < z$, and so forth. We will trust that you will find a way to correctly define any expression containing inequalities that you encounter in terms of Definition 13.36.

THEOREM 13.38. *The relation $\leq$ defines a linear ordering on $\mathbb{N}$.*

PROOF. Recall the definition of linear ordering. We must show that $\leq$ is reflexive, antisymmetric, and transitive.

First, note that Definition 13.36 immediately implies that $x \leq x$ for all $x \in \mathbb{N}$. Therefore $\leq$ is reflexive.

Next, we will show that $\leq$ is antisymmetric.

Let $x, y \in \mathbb{N}$ such that $x \leq y$ and $y \leq x$. We will show that $x = y$.

Temporarily assume that $x \neq y$.

Then by Definition 13.36, we have that $x < y$ and $y < x$.

So, by Definition 13.36, there exist $n, m \in \mathbb{N}$ such that $x + n = y$ and $y + m = x$.

So $(x + n) + m = x$, by substitution.

So $x + (n + m) = x$, by the associative property of addition.

But this contradicts Lemma 13.34, because $x, n + m \in \mathbb{N}$.

Therefore, $x = y$.

Finally, we will show that $\leq$ is transitive.

Let $x, y, z \in \mathbb{N}$ such that $x \leq y$ and $y \leq z$. We will show that $x \leq z$.

Case 1: $x = y$ or $y = z$. Then $x \leq z$ by substitution.

Case 2: $x \neq y$ and $y \neq z$.

Then $x < y$ and $y < z$, by Definition 13.36.

Therefore there exist $n, m \in \mathbb{N}$ such that $x + n = y$ and $y + m = z$, by Definition 13.36.

So $(x + n) + m = z$, by substitution.

So $x + (n + m) = z$, by the associative property of addition.

So $x < z$, by Definition 13.36.

So $x \leq z$, by Definition 13.36.

Therefore, $\leq$ is transitive.

Therefore, $\leq$ is a linear ordering on $\mathbb{N}$, by definition of linear ordering. ■

There are many basic properties that relate the linear ordering $\leq$ on $\mathbb{N}$ to the fundamental operations of addition and multiplication. Some of these are listed in Table 3 on page 298. In the exercises, you will be asked to prove them.

13.1.3. Strong induction and well-ordering. We now prove two fundamental properties of $\mathbb{N}$, which we used throughout Chapter 5. The first is the principle of strong induction.

THEOREM 13.39 (Principle of Strong Induction). *Let A be a subset of $\mathbb{N}$ such that for all $n \in \mathbb{N}$, we have that $n \in A$ whenever $k \in A$ for all natural numbers $k < n$. Then $\mathbb{N} = A$.*

PROOF. ⟨*We'd like to use induction here. In other words, we'd like to show that $1 \in A$, and then show that $S(n) \in A$ whenever $n \in A$. However, the given information does not allow us to go from $n \in A$ to $S(n) \in A$, because to get an element in A, we need* all *previous natural numbers in A, not just the immediate predecessor. So we introduce an auxiliary set B such that, for example, $5 \in B$ iff $1, 2, 3, 4, 5 \in A$, and $7 \in B$ iff $1, 2, 3, 4, 5, 6, 7 \in A$, and so on. Then we can apply usual induction on the set B, because we can get from one step to the next. For example, if $7 \in B$, then $1, 2, 3, 4, 5, 6, 7 \in A$, so $8 \in A$, so $1, 2, 3, 4, 5, 6, 7, 8 \in A$, so $8 \in B$.*⟩

Let $B = \{n \in \mathbb{N} \mid k \in A \text{ for all } k \in \mathbb{N} \text{ such that } k \leq n\}$.

We will show that $\mathbb{N} = B$.

First, we will show that $1 \in B$.

By Exercise 8, we know that there is no $k \in \mathbb{N}$ such that $k < 1$.

Therefore the statement "$k \in A$ for all natural numbers $k < n$" is vacuously true.

So by definition of A, we have that $1 \in A$.

Therefore, $k \in A$ for all $k \in \mathbb{N}$ such that $k \leq 1$. (Because the only such k is $k = 1$.)

So $1 \in B$, by definition of B.

Next, we will show that $S(n) \in B$ whenever $n \in B$.

Suppose that $n \in B$.

Then $k \in A$ for all $k \in \mathbb{N}$ such that $k \leq n$, by definition of B.

Therefore $k \in A$ for all $k \in \mathbb{N}$ such that $k < S(n)$. (Here we use Exercise 9.)

So $S(n) \in A$, from the given information about A.

So $k \in A$ for all $k \in \mathbb{N}$ such that $k \leq S(n)$.

Therefore, $S(n) \in B$, by definition of B.

We have shown that $1 \in B$ and that $S(n) \in B$ whenever $n \in B$.

Therefore, $\mathbb{N} = B$.

Notice that $B \subseteq A$, by definition of B.

So $\mathbb{N} \subseteq A$.

It was given that $A \subseteq \mathbb{N}$.

Therefore, $\mathbb{N} = A$. ■

Finally, we will prove the well-ordering principle.

THEOREM 13.40 (Well Ordering Principle). *Let A be a nonempty subset of $\mathbb{N}$. Then A contains a smallest element. In other words, there exists $n \in A$ such that $n \leq k$ for all $k \in A$.*

PROOF. ⟨*If $1 \in A$, then we're done—that's the smallest element. So imagine that $1 \notin A$. Then if $2 \in A$, we're done, similarly. So imagine that $1, 2 \notin A$. In that case, if $3 \in A$, we're done. And so on. At each stage, we imagine that $1, 2, ..., k \notin A$, then note that we're done if $k + 1 \in A$. Now this process has to stop at some point, because otherwise, A would be empty. The word "otherwise" tips us off that we're really doing a proof by contradiction. Something goes wrong if A does not have a smallest element. What goes wrong is that A winds up empty, because its complement is all of $\mathbb{N}$. To get every natural number in the complement, we're going from $1, 2, ..., k \notin A$ to $k + 1 \notin A$; in other words, we're using strong induction.*⟩

Temporarily assume that A does not contain a smallest element.

Let $B = \mathbb{N} \setminus A$. ⟨*That is, B is the complement of A.*⟩

We will show that $\mathbb{N} = B$.

We will show that $n \in B$ whenever $k \in B$ for all natural numbers $k < n$.

Suppose that $n \in \mathbb{N}$ and that $k \in B$ for all natural numbers $k < n$.

We will show that $n \in B$.

Temporarily assume that $n \notin B$.

Then $n \in A$, by definition of B.

Our given information about n tells us that if $k < n$, then $k \notin A$, by definition of B.

So by taking the contrapositive to get an equivalent statement, we get that if $k \in A$, then $n \leq k$. (Here we use that $\leq$ is a linear ordering on $\mathbb{N}$.)

So n is the smallest element of A.

This is a contradiction, because we assumed that A has no smallest element.

Therefore $n \in B$.

We have shown that $n \in B$ whenever $k \in B$ for all natural numbers $k < n$.

So by the Principle of Strong Induction, $\mathbb{N} = B$.

So $A = \emptyset$.

But this contradicts our assumption that A is nonempty.

Therefore A contains a smallest element. ■

Too Much Information 13.41. Recall that Axiom (3) of Definition 13.2 is essentially induction. In Theorem 13.39, we showed that induction implies strong induction. In Theorem 13.40, we showed that strong induction implies the well-ordering principle. In fact, it can be shown that the well-ordering principle implies induction. So these three statements (induction, strong induction, well-ordering) are equivalent. However, of the three, Axiom (3) of Definition 13.2 is perhaps the simplest to state, because it refers only to the symbols m and q; the other two statements refer to the ordering.

Answers to CFUs

13.1.4. Exercises for Section 13.1. For each of these exercises, when you are asked to prove something, you may assume that the previous exercises have already been proved, but not the later ones.

(1) Let $K = \{1\}$. Define $p\colon K \to K$ by $p(1) = 1$. Verify that $(K, 1, p)$ satisfies all parts of Definition 13.2 except Axiom (1). This shows that Axiom (1) is independent of the others.
(2) Let $K = \{1, 2\}$. Define $p\colon K \to K$ by $p(1) = p(2) = 2$. Verify that $(K, 1, p)$ satisfies all parts of Definition 13.2 except Axiom (2). This shows that Axiom (2) is independent of the others.
(3) Prove the last part of Theorem 13.17. Hint: Let $A = \{a \in N_1 \mid f(q_1(a)) = q_2(f(a))\}$.
(4) Prove the associative property of addition for natural numbers.
(5) Prove the commutative property of multiplication for natural numbers.
(6) Prove the associative property of multiplication for natural numbers.

(7) (a) Let A be a set with a binary operation $*$, and let $c, d \in A$. Prove that if c and d are identity elements for A with respect to $*$, then $c = d$. (This shows that identity elements are unique, if they exist.)
(b) Prove that 1 is the only multiplicative identity for $\mathbb{N}$.
(8) Prove that 1 is the smallest natural number. In other words, prove that for all $n \in \mathbb{N}$, we have that $1 \leq n$.
(9) Let $k, n \in \mathbb{N}$. Prove that if $k < S(n)$, then $k \leq n$.

13.2. The integers

Now that we have natural numbers to work with, how can we define the entire set of integers, including the negative numbers and zero? Consider -3, for example. How can we define it strictly in terms of positive integers, using only concepts we have defined up to this point?

We would like to think that $-3 = 2 - 5$, for example. We cannot, however, take that as a definition of -3, because we have not yet defined subtraction. At least, though, we can work with 2 and 5, because they live in $\mathbb{N}$. So we can think of -3 as being given somehow by the two natural numbers 2 and 5. Do we want to use the set $\{2, 5\}$ or the ordered pair $(2, 5)$? To answer that question, we ask ourselves: Does the order matter here? Yes, it does, because we want $2 - 5$ to be different than $5 - 2$. So we will think of -3 as the ordered pair $(2, 5)$.

However, $(2, 5)$ is not the only ordered pair of natural numbers that could represent -3; the way we're thinking about it, the ordered pair $(4, 7)$ would also represent -3, because $4 - 7 = -3$. So we have many ordered pairs of natural numbers that could potentially represent the same integer, and we want to think of them as essentially the same. What mathematical concept allows us to think of different things as "essentially the same"? The answer is equivalence relations. So we must define an equivalence relation so that $(2, 5)$ is equivalent to $(4, 7)$, and in general so that two ordered pairs are equivalent iff they represent the same integer. That is, we want (a, b) to be equivalent to (c, d) iff $a - b = c - d$. But we cannot use that as our definition, because we have only defined addition and multiplication in $\mathbb{N}$; we have not defined subtraction. No problem. The equation $a - b = c - d$ is equivalent to $a + d = b + c$. This latter definition can serve as our desired equivalence relation.

NOTATION 13.42. Throughout this section, we define the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by

$$(a, b) \sim (c, d) \text{ iff } a + d = b + c.$$

LEMMA 13.43. *The relation $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

PROOF. First, we will show that $\sim$ is reflexive.

Let $(a, b) \in \mathbb{N} \times \mathbb{N}$.

We know that $a+b = b+a$, by the commutative property of addition for natural numbers.

So $(a, b) \sim (a, b)$, by the definition of $\sim$.

Therefore, $\sim$ is reflexive.

Next, we will show that $\sim$ is symmetric.

Let $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ such that $(a, b) \sim (c, d)$.

We will show that $(c, d) \sim (a, b)$.

We know that $a + d = b + c$, by definition of $\sim$.

So $c + b = d + a$, by the commutative property of addition for natural numbers.

Therefore $(c, d) \sim (a, b)$, by definition of $\sim$.

So $\sim$ is symmetric.

Finally, we will show that $\sim$ is transitive.

Let $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$ such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$.

We will show that $(a, b) \sim (e, f)$.

By definition of $\sim$, we know that

$$a + d = b + c \tag{6}$$

and

$$c + f = d + e. \tag{7}$$

From (6) we get $(a + d) + e = (b + c) + e$.

So $a + (d + e) = (b + c) + e$, by the associative property of addition for natural numbers.

Substituting from (7), we get $a + (c + f) = (b + c) + e$.

Using a combination of commutativity, associativity, and cancellation, we can cancel the c from both sides to get $a + f = b + e$.

Therefore, $(a, b) \sim (e, f)$, by definition of $\sim$.

So $\sim$ is transitive.

Therefore, $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$, by definition of equivalence relation. ■

CHECK FOR UNDERSTANDING 13.44. In the proof of Lemma 13.43, why couldn't we have done the following to get transitivity, starting with equations (6) and (7)?
From (6) and (7), we get $a - c = b - d$ and $c - e = d - f$.
Add these two to get $a - e = b - f$.
Therefore $a + f = b + e$.

Recall that the equivalence class of an element x, denoted $[x]$, is the set of all elements equivalent to x.

EXAMPLE 13.45. Describe $[(7, 9)]$. Intuitively, what integer does it represent?

Answer: $[(7, 9)]$ is the set of all elements $(a, b) \in \mathbb{N} \times \mathbb{N}$ such that $a + 9 = b + 7$, or equivalently, such that $a + 2 = b$.

So $[(7, 9) = \{(1, 3), (2, 4), (3, 5), \dots\}$.

Intuitively, $[(7, 9)]$ represents the integer -2, because $7 - 9 = -2$.

CHECK FOR UNDERSTANDING 13.46.
(1) Describe $[(10, 4)]$. Intuitively, what integer does it represent?
(2) Describe $[(6, 6)]$. Intuitively, what integer does it represent?

DEFINITION 13.47. We define the set $\mathbb{Z}$ to be the set of all equivalence classes with respect to the relation $\sim$ from Notation 13.42. An element of $\mathbb{Z}$ is an **integer**.

That is, every integer *is* an equivalence class of ordered pairs of natural numbers.

13.2.1. Operations on the integers. Just as we did for the natural numbers, we now want to define the basic structures on the integers and establish their fundamental properties. Addition and mutliplication were the two most important operations on the natural numbers, and we will define them for the integers as well. The set $\mathbb{Z}$ possesses one other operation that $\mathbb{N}$ lacks, namely subtraction, so we want to define that, too. Like $\mathbb{N}$, the other basic structure on $\mathbb{Z}$ is its ordering. After making these definitions, we will then prove (or have you prove) the properties that describe how these structures interrelate with themselves and with each other.

How should we define addition of integers? In other words, suppose that $[(a,b)]$ and $[(c,d)]$ are two equivalence classes of ordered pairs of natural numbers; what equivalence class should represent $[(a,b)] + [(c,d)]$? Remember that intuitively, $[(a,b)]$ stands for the integer $a-b$, and $[(c,d)]$ stands for the integer $c-d$. So when we add them we should get $(a-b)+(c-d) = (a+c)-(b+d)$, which is represented by $[(a+c, b+d)]$. This is a legitimate definition, because $a,b,c,d \in \mathbb{N}$, and addition has already been defined for natural numbers.

Similar considerations lead to the definition of multiplication. We want $(a-b)(c-d) = ac - ad - bc + bd = (ac+bd) - (ad+bc)$. So we define $[(a,b)] \cdot [(c,d)]$ to be $[(ac+bd, ad+bc)]$.

DEFINITION 13.48. Let $[(a,b)], [(c,d)] \in \mathbb{Z}$. We define

$$[(a,b)] + [(c,d)] := [(a+c, b+d)]$$

and

$$[(a,b)] \cdot [(c,d)] := [(ac+bd, ad+bc)].$$

When inputs are equivalence classes, we must always be concerned with well-definedness. After all, $[(7,9)]$ and $[(12,14)]$ represent the same integer, as do $[(3,1)]$ and $[(5,3)]$, so we should get the same output when we add them, or when we multiply them.

In the following proof, and indeed from this point forward, we will freely invoke the properties of natural numbers listed in Section 13.6 without mentioning them each time we use them. Otherwise, our already lengthy and tedious proofs would become completely unwieldy.

LEMMA 13.49. *The operations $+$ and $\cdot$ on $\mathbb{Z}$ are well-defined.*

PROOF. We will prove that multiplication is well-defined; in the exercises, you will prove that addition is well-defined.

Suppose $[(a,b)] = [(x,y)]$ and $[(c,d)] = [(z,w)]$. We will show that $[(ac+bd, ad+bc)] = [(xz+yw, xw+yz)]$.

That is, we will show that

$$(ac + bd) + (xw + yz) = (ad + bc) + (xz + yw). \tag{8}$$

By definition of equivalence class, we know that $(a, b) \sim (x, y)$ and $(c, d) \sim (z, w)$.

By definition of $\sim$, then,

$$a + y = b + x \tag{9}$$

and

$$c + w = d + z \tag{10}$$

.

⟨*Somehow, we want to take advantage of the fact that we know (9) and (10) are true. But neither side of either equation appears anywhere in (8). So we add some "helpers" to force them to appear. For example, if we add the helper aw to both sides of (8), the left side becomes*

$$\begin{aligned} ac + bd + xw + yz + aw &= a(c + w) + bd + xw + yz \\ &= a(d + z) + bd + xw + yz, \end{aligned}$$

by (10). In all, we'll wind up needing four "helpers," one for each term on each side of (8).⟩

So

$$\begin{aligned} &(ac + bd + xw + yz) + (aw + bz + bw + az) \\ &\quad = a(c + w) + b(d + z) + w(b + x) + z(a + y) \\ &\quad = a(d + z) + b(c + w) + w(a + y) + z(b + x) \\ &\quad = (ad + bc + xz + yw) + (aw + bz + bw + az) \end{aligned}$$

By cancellation, we then get (8). ■

Table 2 on page 298 lists several addition and multiplication properties of $\mathbb{N}$. In fact, $\mathbb{Z}$ shares all of them. We will prove the distributive property and leave the others as exercises.

THEOREM 13.50 (Distributive property for the integers). *Let $x, y, z \in \mathbb{Z}$. Then*

$$x(y+z) = xy + xz.$$

PROOF. By Definition 13.47, we have that $x = [(a,b)], y = [(c,d)]$, and $z = [(e,f)]$ for some $a, b, c, d, e, f \in \mathbb{N}$.

By Definition 13.48, we have

$$\begin{aligned} x(y+z) &= [(a,b)]([(c,d)] + [(e,f)]) \\ &= [(a,b)] \cdot [(c+e, d+f)] \\ &= [(a(c+e) + b(d+f), a(d+f) + b(c+e))] \\ &= [((ac+bd) + (ae+bf), (ad+bc) + (af+be))] \\ &= [(ac+bd, ad+bc)] + [(ae+bf, af+be)] \\ &= [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)] \\ &= xy + xz. \end{aligned}$$

■

Does $\mathbb{Z}$ have any properties that $\mathbb{N}$ does not have? Earlier, we remarked that $\mathbb{N}$ does not have an additive identity, essentially because $0 \notin \mathbb{N}$. However, 0 is an integer, so $\mathbb{Z}$ should have an additive identity. Which equivalence class $[(a,b)]$ represents 0? We need $a - b = 0$, so anything with $a = b$ will do. The most convenient choice is $a = b = 1$.

DEFINITION 13.51. We define the integer $0 := [(1,1)]$.

We're *defining* zero! Can you believe that?

THEOREM 13.52. *For all $x \in \mathbb{Z}$, we have that $0 + x = x + 0 = x$.*

PROOF. Let $x \in \mathbb{Z}$.

By Definition 13.47, we have that $x = [(a, b)]$ for some $a, b \in \mathbb{N}$. So,

$$\begin{aligned} 0 + x &= [(1,1)] + [(a,b)] && \text{by Definition 13.51} \\ &= [(1+a, 1+b)] && \text{by Definition 13.48} \\ &= [(a,b)] && \text{because } (1+a, 1+b) \sim (a,b) \\ &= x \end{aligned}$$

The equation $x + 0 = x$ then follows from the commutative property of addition for integers. ■

TOO MUCH INFORMATION 13.53. Theorem 13.52 shows that 0 is an identity element for addition on $\mathbb{Z}$. More succinctly, we say that 0 is the **additive identity** for $\mathbb{Z}$. Recall that Exercise 7 shows that any identity element for any particular operation must be unique, so there are no other additive identities.

TOO MUCH INFORMATION 13.54. Recall our discussion of the term "isomorphic" in Remark 13.18. Theorem 13.52 gives us a property of $\mathbb{Z}$ that $\mathbb{N}$ does not have. This shows that $\mathbb{Z}$ and $\mathbb{N}$ are not isomorphic, at least as far as addition is concerned. For a more precise statement of this fact, see Exercise 3.

Is there a property of $\mathbb{N}$ that $\mathbb{Z}$ does not have? Yes—induction. More precisely, $(\mathbb{N}, 1, n \mapsto n + 1)$ is a natural number system, but there does not exist $a \in \mathbb{Z}$ such that $(\mathbb{Z}, a, n \mapsto n + a)$ is a natural number system.

Other than 0, what distinguishes $\mathbb{Z}$ from $\mathbb{N}$ is all those negative numbers. What's so special about -5, anyway? The point is that it cancels out 5. In other words, $-5+5 = 0$. We say that -5 and 5 are "additive inverses" of one another. Now let's be precise. What's the additive inverse of an integer $[(a, b)]$? We think of $[(a, b)]$ as $a - b$, so its opposite should be $b - a$, which we represent by $[(b, a)]$.

THEOREM 13.55. *Let $x \in \mathbb{Z}$. Then there exists a unique $y \in \mathbb{Z}$ such that $x + y = y + x = 0$.*

PROOF. We will prove existence; in Exercise 4, you will prove uniqueness.

By Definition 13.47, we have that $x = [(a, b)]$ for some $a, b \in \mathbb{N}$.

Let $y = [(b, a)]$.

Then

$$\begin{aligned} x + y &= [(a, b)] + [(b, a)] \\ &= [(a + b, b + a)] && \text{by Definition 13.48} \\ &= [(1, 1)] && \text{because } (a + b, b + a) \sim (1, 1) \\ &= 0 && \text{by Definition 13.51.} \end{aligned}$$

The fact that $y + x = 0$ now follows from the commutative property of addition for integers. ■

DEFINITION 13.56. Let $x \in \mathbb{Z}$. We define $-x$ to be the unique integer such that

$$x + (-x) = -x + x = 0.$$

We say that $-x$ is the **additive inverse** or **opposite** of x.

TOO MUCH INFORMATION 13.57. The proof of Theorem 13.55 shows that additive inverse of $[(a, b)]$ is $[(b, a)]$.

TOO MUCH INFORMATION 13.58. We sometimes refer to $-x$ as "negative x," but this can lead to confusion, as $-x$ might not be negative. For example, if $x = -3$, then $-x = 3$, which is positive.

EXAMPLE 13.59. Express $-[(5, 1)]$ in the form $[(a, b)]$.

Answer: We have that $-[(5,1)] = [(1,5)]$, because $[(5,1)]+[(1,5)] = [(1,5)] + [(5,1)] = [(6,6)] = [(1,1)] = 0$.

Next, we want to define subtraction. That is, given $x, y \in \mathbb{Z}$, we want to define the difference $x - y$. How can we express that in terms of previously defined concepts? Well, we want $x - y = x + (-y)$, and both addition and opposites have been defined for integers. So . . .

DEFINITION 13.60. Let $x, y \in \mathbb{Z}$. We define the **difference** of x and y by

$$x - y := x + (-y).$$

CHECK FOR UNDERSTANDING 13.61. Suppose we tried to define subtraction of integers as follows. Let $x, y \in \mathbb{Z}$, and take $x - y := [(x, y)]$. Would this be an acceptable definition? Why or why not?

13.2.2. Ordering the integers. Next, we define the usual ordering on $\mathbb{Z}$. We begin by defining positive and negative numbers. Then we use those concepts to define $<$ in general.

Should we consider the integer $[(20, 12)]$ to be positive? We think of it as $20 - 12 = 8$, so it should be positive. How could we tell that just from the numbers 20 and 12? A moment's thought shows that it's because $20 > 12$.

DEFINITION 13.62. Let $x = [(a, b)] \in \mathbb{Z}$. We say that x is **positive** if $a > b$. We say that x is **negative** if $a < b$.

In Exercise 7, you will show that this definition does not depend on the particular choice of ordered pair to represent x.

Now, how can we define $<$ for the integers in terms of previously defined concepts? We want $x < y$ iff $0 < y - x$ iff $y - x$ is positive. The latter formulation is perfect, because both "subtraction" and "positive" have been defined for $\mathbb{Z}$.

DEFINITION 13.63. We define the relation $<$ on $\mathbb{Z}$ by

$$x < y \text{ iff } y - x \text{ is positive.}$$

We define $\leq$ by $x \leq y$ iff $x < y$ or $x = y$.

TOO MUCH INFORMATION 13.64. As with $\mathbb{N}$, we'll trust that you can properly define related notations such as $x < y$ and $x < y \leq z$ and so on.

Tables 3 and 5 list several basic properties for the ordering on $\mathbb{Z}$. In the exercises, you will be asked to prove them.

13.2.3. Embedding the natural numbers in the integers. Perhaps by now you can see why we usually write an integer in the form, say, -47 instead of $[(6, 53)]$. The equivalence-class-of-ordered-pair-of-natural-numbers notation is rather cumbersome. Moreover, we think of $\mathbb{N}$ as a subset of $\mathbb{Z}$, but strictly speaking, a natural number is not the same thing as an integer $[(a, b)]$. So our next task will be to show that $\mathbb{N}$ really does sit inside $\mathbb{Z}$ in a "natural" way.

First, we need a systematic way to think of a natural number as an integer. We can represent 7, for example in many ways. It is $[(8, 1)] = [(9, 2)] = [(10, 3)] = \ldots$. The simplest one comes at the beginning, namely $[(8, 1)]$. Indeed, a natural number n can be represented by $[(n + 1, 1)]$. This defines a function, as in Figure 2.

Moreover, all of the structures we've defined on $\mathbb{N}$ (addition, multiplication, ordering) work exactly the same way in

$$
\begin{array}{ccc}
\underline{\mathbb{N}} & & \underline{\mathbb{Z}} \\
\vdots & \vdots & \vdots \\
n & \mapsto & [(n+1,1)] = n \\
\vdots & \vdots & \vdots \\
3 & \mapsto & [(4,1)] = 3 \\
2 & \mapsto & [(3,1)] = 2 \\
1 & \mapsto & [(2,1)] = 1 \\
 & & [(1,1)] = 0 \\
 & & [(1,2)] = -1 \\
 & & [(1,3)] = -2 \\
 & & \vdots
\end{array}
$$

FIGURE 2. An embedding of $\mathbb{N}$ into $\mathbb{Z}$

$\mathbb{N}$ as do their counterparts in $\mathbb{Z}$ under this correspondence. For example, in $\mathbb{N}$ you can use Definition 13.25 to find that $2 \cdot 3 = 6$. Denote the function in Figure 2 by f. Then $f(2) = [(3,1)]$, and $f(3) = [(4,1)]$, and $f(6) = [(7,1)]$. Well, whaddya know, using the definitions from this section, we find that $[(3,1)] \cdot [(4,1)] = [(13,7)] = [(7,1)]$. In other words, $f(2 \cdot 3) = f(2) \cdot f(3)$. If that works out for all natural numbers, then we say that the function "preserves multiplication."

THEOREM 13.65. *The set $\mathbb{N}$ embeds into $\mathbb{Z}$ in a way that preserves addition, multiplication, and ordering. In other words, there exists an injective function $f\colon \mathbb{N} \to \mathbb{Z}$ such that for all $a, b \in \mathbb{N}$,*

$$f(a+b) = f(a) + f(b), \text{ and}$$
$$f(a \cdot b) = f(a) \cdot f(b), \text{ and}$$
$$a < b \text{ iff } f(a) < f(b).$$

PROOF. Define $f\colon \mathbb{N} \to \mathbb{Z}$ by $f(n) = [(n+1, 1)]$.

First, we will show that f is injective.

Suppose $f(n) = f(m)$ for some $n, m \in \mathbb{N}$.

We will show that $n = m$.

By definition of f, we have that $[(n+1, 1)] = [(m+1, 1)]$.

So $(n+1, 1) \sim (m+1, 1)$, by definition of equivalence class.

So $n + 2 = m + 2$, by Notation 13.42.

So $n = m$, by cancellation.

Therefore, f is injective.

Next, we will show that $f(a+b) = f(a) + f(b)$ for all $a, b \in \mathbb{N}$.

Let $a, b \in \mathbb{N}$.

Then

$$\begin{aligned} f(a) + f(b) &= [(a+1, 1)] + [(b+1, 1)] && \text{by definition of } f \\ &= [(a+b+2, 2)] && \text{by Definition 13.48} \\ &= [(a+b+1, 1)] && \text{because } (a+b+2, 2) \sim (a+b+1, 1) \\ &= f(a+b) && \text{by definition of } f \end{aligned}$$

Next, we will show that $f(ab) = f(a) \cdot f(b)$ for all $a, b \in \mathbb{N}$.

Let $a, b \in \mathbb{N}$.

Then

$$\begin{aligned} f(a) \cdot f(b) &= [(a+1, 1)] \cdot [(b+1, 1)] && \text{by definition of } f \\ &= [((a+1)(b+1) + 1, (b+1) + (a+1))] && \text{by Definition 13.48} \\ &= [(ab + a + b + 2, a + b + 2)] \\ &= [(ab + 1, 1)] \\ &= f(ab). && \text{by definition of } f \end{aligned}$$

Note that in the next to last step, we used that $(ab + a + b + 2, a + b + 2) \sim (ab + 1, 1)$.

Finally, we will show that $a < b$ iff $f(a) < f(b)$ for all $a, b \in \mathbb{N}$.

This holds because

$$\begin{aligned}
f(a) < f(b) \text{ iff } & f(b) - f(a) \text{ is positive, by Definition 13.63} \\
\text{iff } & [(b+1,1)] - [(a+1,1)] \text{ is positive, by definition of } f \\
\text{iff } & [(b+1,1)] + (-[(a+1,1)]) \text{ is positive, by Definition 13.60} \\
\text{iff } & [(b+1,1)] + [(1,a+1)] \text{ is positive, by Remark 13.57} \\
\text{iff } & [(b+2,a+2)] \text{ is positive, by Definition 13.48} \\
\text{iff } & b+2 > a+2, \text{ by Definition 13.62} \\
\text{iff } & b > a, \text{ by cancellation.}
\end{aligned}$$

■

Theorem 13.65 shows that $\mathbb{Z}$ contains a "copy" of $\mathbb{N}$ sitting inside it, and that this copy behaves exactly like $\mathbb{N}$ in terms of addition, multiplication, and order. So from now on, we will make no distinction between $\mathbb{N}$ and its identical twin inside $\mathbb{Z}$. Instead of writing $[(22, 14)]$, for example, we'll simply call it by its usual name, that is, 8. This is only the first of several such embeddings we'll perform on our journey from $\mathbb{N}$ to $\mathbb{Z}$ to $\mathbb{Q}$ to $\mathbb{R}$ to $\mathbb{C}$.

Too Much Information 13.66. The proof of Theorem 13.65 would have been a bit simpler if we had allowed 0 as a natural number. Then the embedding is the map $n \mapsto [(n, 0)]$, and it's immediate to show that addition and multiplication are preserved.

Too Much Information 13.67. In this chapter, we started with natural numbers, then created a new set (the integers) via the equivalence relation $\sim$. What if we played the same game all over again, this time using integers in place of natural numbers? So we define two ordered pairs (a, b) and (c, d) of *integers* to be equivalent iff $a + d = b + c$. Then we form the set of all equivalence classes, and we

define addition, multiplication, and everything else just as we did before. Do we get an entirely new number system this way? The answer is no. Your "new" number system winds up being essentially the same as the integers. To see that, you can embed $\mathbb{Z}$ into the new set the same way we embedded $\mathbb{N}$ into $\mathbb{Z}$. This time, however, the embedding will be bijective, so a "copy" of $\mathbb{Z}$ will fill up the whole set.

More fundamentally, though, what's going on is this. The $[(a, b)]$ construction allows us to do what we could not do before: subtract. In other words, it guarantees that the equation $a = b + x$ always has a solution. Once those equations always have solutions, repeating the construction provides nothing new.

13.2.4. Exercises for Section 13.2. For each of these exercises, when you are asked to prove something, you may assume that the previous exercises have already been proved, but not the later ones.

(1) Prove that addition of integers is well-defined.
(2) Prove the other properties.
(3) Prove that there does not exist a bijective function $f : \mathbb{N} \to \mathbb{Z}$ such that $f(a + b) = f(a) + f(b)$ for all $a, b \in \mathbb{N}$.
(4) Finish the proof of Theorem 13.55 by proving uniqueness.
(5) In Definition 13.56, what kind of mathematical object is $-$? Is it a set, a function, an operation, an equivalence relation, or something else?
(6) In Definition 13.60, what kind of mathematical object is $-$? Is it a set, a function, an operation, an equivalence relation, or something else?
(7) Prove that Definition 13.62 is well-defined. That is, prove that if $[(a, b)] = [(c, d)]$, then $[(a, b)]$ is positive iff $[(c, d)]$ is positive, and $[(a, b)]$ is negative iff $[(c, d)]$ is negative.

13.3. The rationals

In $\mathbb{N}$, we could not always subtract, and so we constructed $\mathbb{Z}$ from $\mathbb{N}$. We now face a similar situation, for in $\mathbb{Z}$, we cannot divide. To solve that problem, we will construct $\mathbb{Q}$ from $\mathbb{Z}$.

In the previous section, we created a solution to the equation $a = b + x$ by forming the ordered pair (a, b), which we thought of as the integer $a - b$. To divide, we want solutions to the equation $n = mx$. We'll handle this the same way, by forming the ordered pair (n, m), which we think of as n/m. With integers, we wanted (a, b) and (c, d) to be effectively the same when $a - b = c - d$, so we declared those pairs equivalent iff $a + d = b + c$. We reframed the condition this way because addition, unlike subtraction, had already been defined for natural numbers. This time, we want (n, m) and (r, s) to be essentially the same iff $n/m = r/s$, which we rewrite as $ns = mr$, because multiplication of integers has been defined, whereas division has not. There's one catch: we do not want to allow division by zero. So in the ordered pair (n, m), we'll allow any $n, m \in \mathbb{Z}$ so long as $m \neq 0$.

NOTATION 13.68. Throughout this section, we define the relation $\sim$ on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by

$$(n, m) \sim (r, s) \text{ iff } ns = mr.$$

TOO MUCH INFORMATION 13.69. Obviously, this $\sim$ is not the same as the one from Notation 13.42. We're done with that one, so we are free to repurpose the $\sim$ symbol here.

THEOREM 13.70. *The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.*

PROOF. Exercise 1. ■

DEFINITION 13.71. We define $\mathbb{Q}$ to be the set of equivalence classes of the relation $\sim$ from Notation 13.68. Elements of $\mathbb{Q}$ are called **rational numbers**.

TOO MUCH INFORMATION 13.72. We write a rational number in the form $[(n, m)]$. We think of $[(n, m)]$ as representing the rational number n/m.

EXAMPLE 13.73.
(1) Find three elements of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ that are equivalent to $(-4, 6)$. Justify your answer.
(2) List three elements of the rational number $[(0, 5)]$. Justify your answer.
(3) Is $[(-2, 0)]$ a rational number? Why or why not?
(4) Intuitively, what rational number does $[(10, -2)]$ represent?

Answers:

(1) The ordered pair $(4, -6)$ is equivalent to $(-4, 6)$, because $4(6) = -6(-4)$.

The ordered pair $(-2, 3)$ is equivalent to $(-4, 6)$, because $-2(6) = 3(-4)$.

The ordered pair $(-12, 18)$ is equivalent to $(-4, 6)$, because $-12(6) = 18(-4)$.

(2) The ordered pair $(0, 5)$ is equivalent to $(0, 5)$ by the reflexive property. So $(0, 5)$ is an element of the equivalence class $[(0, 5)]$.

The ordered pair $(0, 1)$ is equivalent to $(0, 5)$, because $0(5) = 1(0)$. So $(0, 1)$ is an element of the equivalence class $[(0, 5)]$.

The ordered pair $(0, -47)$ is equivalent to $(0, 5)$, because $0(5) = -47(0)$. So $(0, -47)$ is an element of the equivalence class $[(0, 5)]$.

(3) No, $[(-2, 0)] \notin \mathbb{Q}$, because $0 \notin \mathbb{Z} \setminus \{0\}$.

(4) It represents $10/(-2) = -5$.

13.3.1. Operations on rational numbers. As with $\mathbb{Z}$, we now want to define the usual operations on $\mathbb{Q}$. How should we define $[(n, m)] + [(r, s)]$? We think of it as

$$\frac{n}{m} + \frac{r}{s} = \frac{ns + mr}{ms},$$

so we should define it to be $[(ns + mr, ms)]$. Note that this uses only the previously defined concepts of addition and multiplication of integers, so this definition is not circular. Similarly, for multiplication, we want $(n/m)(r/s) = nr/ms$, so we define $[(n, m)] \cdot [(r, s)] = [(nr, ms)]$.

DEFINITION 13.74. We define the binary operations $+$ and $\cdot$, called addition and multiplication, respectively, on $\mathbb{Q}$ by

$$[(n, m)] + [(r, s)] := [(ns + mr, ms)], \text{ and}$$

$$[(n, m)] \cdot [(r, s)] := [(nr, ms)].$$

THEOREM 13.75. *Addition and multiplication are well-defined on* $\mathbb{Q}$.

PROOF. Exercise 2. ■

Like the integers, the rational numbers have an additive identity.

DEFINITION 13.76. We define $0 := [(0, 1)]$.

In the exercises, you will be asked to prove that 0 is the unique additive identity for $\mathbb{Q}$, as well as to prove that $\mathbb{Q}$ possesses the properties listed in Tables 2, 4, and 6 in Section 13.6.

In particular, in Exercise 3, you will show that every rational number x has a unique additive inverse, which we denote $-x$. As in $\mathbb{Z}$, this allows us to define subtraction in $\mathbb{Q}$ by $x - y := x + (-y)$.

What distinguished $\mathbb{Q}$ from $\mathbb{Z}$ is the ability to divide. Just as additive inverses allow us to subtract, multiplicative inverses make division possible.

DEFINITION 13.77. We define $1 := [(1, 1)]$.

TOO MUCH INFORMATION 13.78. Definitions 13.76 and 13.77 may seem circular, because we define 0 in terms of 0 and 1 in terms of 1. However, the zero on the left in Definition 13.76 is the rational number 0, whereas the 0 on the right is the previously defined integer 0. It's similar for 1. Later, in Theorem 13.86, we will justify our recycling of the 0 and 1 symbols.

In Exercise 4, you will prove that 1 is the unique multiplicative identity element for $\mathbb{Q}$.

THEOREM 13.79. *Let $x \in \mathbb{Q}$ such that $x \neq 0$. Then $\exists! y \in \mathbb{Q}$ such that $xy = yx = 1$.*

PROOF. Let $x \in \mathbb{Q}$ such that $x \neq 0$.

Then by definition of $\mathbb{Q}$, we have that $x = [(n, m)]$ for some $n, m \in \mathbb{Z}$, where $m \neq 0$.

Moreover, because $x \neq 0$, we know that $n \neq 0$.

Let $y = [(m, n)]$.

Then $xy = [(n, m)] \cdot [(m, n)] = [(nm, nm)] = [(1, 1)] = 1$.

From this, we get that $yx = 1$ by commutativity.

Now, we prove uniqueness.

Suppose, $y, z \in \mathbb{Q}$ such that $xy = yx = 1$ and $xz = zx = 1$.

Then $y = y \cdot 1 = y(xz) = (yx)z = 1 \cdot z = z$. ■

TOO MUCH INFORMATION 13.80. Theorem 13.79 shows that $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$ with respect to multiplication, because it is true for $\mathbb{Q}$ but not for $\mathbb{Z}$. In fact, $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$ with respect to addition, either, and here's why. For all $x \in \mathbb{Q}$, there exists $y \in \mathbb{Q}$ such that $y + y = x$. But this statement becomes false when we change $\mathbb{Q}$ to $\mathbb{Z}$. Moreover, it is phrased entirely in terms of addition.

Theorem 13.79 tells us that every nonzero rational number has a unique multiplicative inverse. If $x \in \mathbb{Q}$ and $x \neq 0$, then we denote the unique multiplicative inverse of x by x^{-1}.

DEFINITION 13.81. Let $x, y \in \mathbb{Q}$. We define the **quotient** of x and y, denoted

$$x \div y := x \cdot y^{-1}$$

TOO MUCH INFORMATION 13.82. We will freely use other standard notations for division, such as x/y.

EXAMPLE 13.83. Use Definition 13.81 to compute $[(4, 6)] \div [(-10, 9)]$. Then rewrite your answer using standard fraction notation. (No need to reduce to lowest terms.)

Answer:

$$\begin{aligned}[(4,6)] \div [(-10,9)] &= [(4,6)] \cdot [(-10,9)]^{-1} \\ &= [(4,6)] \cdot [(9,-10)] \\ &= [(36,-60)].\end{aligned}$$

In standard fraction notation, we would write

$$\frac{4}{6} \div \frac{-10}{9} = \frac{4}{6} \cdot \frac{9}{-10} = \frac{36}{-60}.$$

13.3.2. Ordering the rationals. In $\mathbb{Z}$, we defined the ordering by first specifying which integers were positive, then declaring $n < m$ iff $m - n$ is positive. We now do the same for $\mathbb{Q}$. So which rational numbers (n, m) should be considered positive? Thinking of $[(n, m)]$ as n/m suggests that we should define $[(n, m)]$ to be positive when $n > 0$ and $m > 0$. But beware! We can represent $2/3$, for example, as $[(2, 3)]$ or as $[(-2, -3)]$, and we want to call it positive both ways. So we need to be careful about the wording.

DEFINITION 13.84. Let $x \in \mathbb{Q}$. We say x is **positive** if there exist positive integers n, m such that $x = [(n, m)]$.

EXAMPLE 13.85. Is $[(-2, -3)]$ positive? Why or why not?

Answer: Yes, $[(-2, -3)]$ is positive, because $[(-2, -3)] = [(2, 3)]$, and 2 and 3 are positive integers.

As with $\mathbb{Z}$, we define the relation $<$ on $\mathbb{Q}$ by $x < y$ iff $y - x$ is positive. Likewise, $x \leq y$ means that $x < y$ or $x = y$.

Tables 3, 5, and 7 in Section 13.6 list several properties of the ordering on $\mathbb{Q}$, and its relationship to addition and multiplication.

13.3.3. Embedding the integers in the rationals. In the previous section, we defined an embedding of $\mathbb{N}$ into $\mathbb{Z}$, so that we could think of $\mathbb{N}$ as a subset of $\mathbb{Z}$. Now, we will embed the integers into the rationals.

How do we think of, say, the integer 47 as a rational number? Easy—it's $47/1$, or more precisely, $[(47, 1)]$. This suggests that the desired map is $n \mapsto [(n, 1)]$, and indeed, that function does the trick.

THEOREM 13.86. *There exists a function* $f\colon \mathbb{Z} \to \mathbb{Q}$ *such that for all* $a, b \in \mathbb{Z}$,

$$f(a+b) = f(a) + f(b), \text{ and}$$
$$f(a \cdot b) = f(a) \cdot f(b), \text{ and}$$
$$a < b \text{ iff } f(a) < f(b).$$

PROOF. Exercise 5. ■

Having established Theorem 13.86, we now abandon the ordered pair notation for rational numbers. Instead, from this point forward, we will write the rational number $[(n, m)]$ in the usual n/m notation. Moreover, we will regard the integers as a subset of the rationals, in the usual way.

TOO MUCH INFORMATION 13.87. In Theorem

TOO MUCH INFORMATION 13.88. Why don't we also insist, in Theorem 13.86, that f also preserve subtraction? That is, why not also require that $f(a - b) = f(a) - f(b)$ for all $a, b \in \mathbb{Z}$? The reason is that subtraction comes for free. Once we know that f preserves addition, then it will necessarily preserve subtraction, too. See Exercise 6.

13.3.4. Exercises for Section 13.3. For each of these exercises, when you are asked to prove something, you

may assume that the previous exercises have already been proved, but not the later ones.

(1) Prove Theorem 13.70.
(2) Prove Theorem 13.75.
(3) Prove that every rational number has a unique additive inverse.
(4) Prove that 1 is the unique multiplicative identity element for $\mathbb{Q}$.
(5) Prove Theorem 13.86.
(6) Let f be as in Theorem 13.86. Prove that $f(a-b) = f(a) - f(b)$ for all $a, b \in \mathbb{Z}$.

13.4. The reals

We've now constructed a set, $\mathbb{Q}$, where we can subtract and divide. Is there anything we *can't* do in $\mathbb{Q}$? Yes: we can't always take limits when we'd like to. For example, consider the following sequence.

$$\begin{aligned} s_1 &= 1 + \frac{1}{1!} \\ s_2 &= 1 + \frac{1}{1!} + \frac{1}{2!} \\ s_3 &= 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} \\ &\vdots \\ s_n &= 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} \\ &\vdots \end{aligned} \tag{11}$$

Notice that each term in this sequence is a rational number. In Chapter 11, we showed that this sequence is bounded and monotonic, so it *should* have a limit. However, we called the limit of this sequence e, and we proved

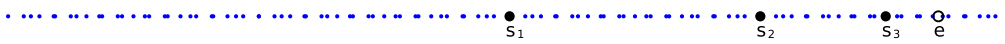


FIGURE 3. The sequence (s_n) converges to an irrational number

that $e \notin \mathbb{Q}$. Visually, it's as if $\mathbb{Q}$ has a "hole" in it where e is supposed to be—see Figure 3.

How in the world do we define a real number like e, when all we have to work with are rational numbers? The ordered pair construction we used to define $\mathbb{Z}$ and $\mathbb{Q}$ was helpful for creating inverse elements but is of no use to us here.

There are many approaches one can take. In this chapter, we use "Dedekind cuts" to define the real numbers. In Section 13.7, we present an alternate approach using "Cauchy sequences." In fact, it doesn't matter which one we use to define $\mathbb{R}$; the set of real numbers will have all the same properties eiether way.

We return now to the sequence (s_n) defined in equation (11). The rational numbers in (s_n) are less than e, yet somehow they lead all the way up to e. The mathematician Richard Dedekind (1831–1916) proposed the following: Why not consider the set of *all* rational numbers lass than e? The elements of this set are shown as solid dots in Figure 4.

Notice that this set communicates exactly what we have in mind—intuitively, we can think of its "right endpoint." In a similar way, we can specify any real number x, whether it be π, 47, or $-\sqrt{2}$, in terms of $\mathbb{Q}$ by taking the set of all rational numbers less than x.

One little problem: We can't yet refer to real numbers, because we have not yet constructed $\mathbb{R}$. So how do we characterize the sets we're talking about while making reference

FIGURE 4. A Dedekind cut

only to rationals? Look again at Figure 4. Notice that for any point s in the solid-dot set A, every rational number to the left of s is again in A. Also notice that some dots are solid, but some are not; that's because some rationals are less than e, but some are not. Finally, notice that A does not contain a maximum; given any solid dot, we can find another solid dot to its right. (Remember that there are infinitely many solid dots, so we can't show all of them.) These properties, it turns out, tell us exactly the kinds of sets we're looking for. See how each such set cuts the number line into two halves? For that reason, and in honor of their creator, we call them Dedekind cuts.

DEFINITION 13.89. Let $A \subseteq \mathbb{Q}$. We say that A is a **Dedekind cut** if:

(1) $A \neq \emptyset$, and
(2) $\mathbb{Q} \setminus A \neq \emptyset$, and
(3) For all $r, s \in \mathbb{Q}$, if $s \in A$ and $r < s$, then $r \in A$, and
(4) If $s \in A$, then $\exists t \in A$ such that $s < t$.

In words, (1) says that A is not empty; (2) says that the complement of A is not empty; (3) says that A is "downward closed"; and (4) says that A has no maximum.

TOO MUCH INFORMATION 13.90. In some other books, a Dedekind cut is defined as a pair (A, B), where A is as in Definition 13.89, and B is the complement of A.

EXAMPLE 13.91. Let $B = \{x \in \mathbb{Q} \mid x < 0\}$. (1) Is B a Dedekind cut? Prove that your answer is correct. (2) Intuitively, what real number does B represent?

Answers: (1) Yes, B is a Dedekind cut.

PROOF. First, notice that $-1 \in B$ and $1 \in \mathbb{Q} \setminus B$.

So $B \neq \emptyset$ and $\mathbb{Q} \setminus B \neq \emptyset$.

Next, let $r, s \in \mathbb{Q}$ such that $s \in B$ and $r < s$. We will show that $r \in B$.

We know that $s < 0$, by definition of B.

So $r < 0$, because $r < s$ and $s < 0$.

So $s \in B$, by definition of B.

Finally, let $s \in B$. We will show that $\exists t \in B$ such that $s < t$.

We know that $s < 0$, by definition of B.

So $s/2 < 0$.

Also, $s/2 \in \mathbb{Q}$, because $s \in \mathbb{Q}$.

So $s/2 \in B$, by definition of B.

Also, $s < s/2$, because $s < 0$.

Therefore, by Definition 13.89, we have that B is a Dedekind cut. ■

(2) When we draw a picture of B, we see that its "right endpoint" is at 0. So B represents the real number 0.

CHECK FOR UNDERSTANDING 13.92. Is $\{x \in \mathbb{Q} \mid x > 0\}$ a Dedekind cut? Why or why not?

EXAMPLE 13.93. Let $C = \{x \in \mathbb{Q} \mid x \leq 0\}$. Is C a Dedekind cut? Prove that your answer is correct.

Answer: No, C is not a Dedekind cut. Property (4) from Definition 13.89 fails. Specifically, let $s = 0$. Then there does not exist $t \in C$ such that $s < t$.

CHECK FOR UNDERSTANDING 13.94. Let $D = \{x \in \mathbb{Q} \mid x^2 < 2\}$. (1) Draw a picture of D. (2) Explain why D is not a Dedekind cut. (3) Without referring to any irrational numbers, how could you modify the definition of D to represent the real number $\sqrt{2}$?

EXAMPLE 13.95. Define the sequence (s_n) as in equation (11) on page 272. For each $n \in \mathbb{N}$, define $E_n = \{x \in \mathbb{Q} \mid x < s_n\}$. Let $E = \cup_{n\in\mathbb{N}} E_n$. Prove that E is a Dedekind cut.

Scratch work: Before going on, draw a picture of the sets E_n, so you can visualize what E looks like.

When we do a first attempt at this proof, we find that the hardest part is proving that $\mathbb{Q} \setminus E$ is not empty. In other words, we have to find an rational number that is greater than or equal to s_n for all n.

Each s_n is a sum of terms of the form $1/j!$.

So we look for numbers that are a little bigger than $1/j!$, but more manageable.

Because $j!$ is in the denominator, we can get a bigger number by replacing $j!$ with something *smaller*.

Note that $1 \cdot 2 \cdot 3 \cdots j \geq 2^{j-1}$ for all natural numbers j. Hence $\frac{1}{j!} \leq \frac{1}{2^{j-1}}$ for all natural numbers j.

So for all $N \in \mathbb{N}$,

$$\begin{aligned} s_n &= 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} \\ &\leq 1 + \frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}} \\ &= 1 + \frac{1 - \frac{1}{2}^n}{1 - \frac{1}{2}} \\ &\leq 1 + \frac{1}{1 - \frac{1}{2}} \\ &= 3. \end{aligned}$$

The powers of 2 gave us a geometric sum, which we could then add up. This is a common trick.

PROOF. First, we will show that $E \neq \emptyset$.
Note that $0 < 1 = s_1$.
Also, $0 \in \mathbb{Q}$.
So $0 \in E_1$, by definition of D_1.
So $0 \in E$, by definition of union.
So $E \neq \emptyset$.

Next, we will show that $\mathbb{Q} \setminus E \neq \emptyset$.
We will show that $3 \in \mathbb{Q} \setminus E \neq \emptyset$.
⟨*Remember the scratch work. That's where 3 is coming from here.*⟩
We will show that for all $\ell \in \mathbb{N}$, we have that $3 \notin E_\ell$.
Let $\ell \in \mathbb{N}$. We will show that $3 \notin E_\ell$.

We have that

$$\begin{aligned} s_\ell &= 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{\ell!} \\ &\leq 1 + \frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \cdots + \frac{1}{2^{\ell-1}} \\ &= 1 + \frac{1 - \frac{1}{2}^\ell}{1 - \frac{1}{2}} \\ &\leq 1 + \frac{1}{1 - \frac{1}{2}} \\ &= 3. \end{aligned}$$

So $s_\ell \leq 3$.

So $3 \notin E_\ell$, by definition of E_ℓ.

Now, we will show that $3 \notin E$.

Temporarily assume that $3 \in E$.

Then $3 \in E_n$ for some $n \in \mathbb{N}$.

But we just showed that $3 \notin E_\ell$ for all $\ell \in \mathbb{N}$, so this is a contradiction.

Therefore, $3 \notin E$.

We know that $3 \in \mathbb{Q}$.

So $3 \in \mathbb{Q} \setminus E$.

So $\mathbb{Q} \setminus E \neq \emptyset$.

Next, let $r, s \in \mathbb{Q}$ such that $s \in E$ and $r < s$. We will show that $r \in E$.

We know that $s \in E_n$ for some $n \in \mathbb{N}$, by definition of union.

So $s < s_n$, by definition of E_n.

So $r < s_n$, because $r < s$.

So $r \in E_n$, by definition of E_n.

Therefore $r \in E$, by definition of union.

Finally, let $s \in E$. We will show that $\exists t \in E$ such that $s < t$.

We know that $s \in E_n$ for some $n \in \mathbb{N}$, by definition of union.

So $s < s_n$, by definition of E_n.

Let $t = s_{n+1}$.

Then $t = s_n + 1/n! > s_n$.

So $s < t$.

We must show that $t \in E$.

We have that $s_{n+2} = s_{n+1} + 1/(n+1)! > s_{n+1} = t$.

So $t < s_{n+2}$.

So $t \in E_{n+2}$, by definition of E_{n+2}.

So $t \in E$, by definition of union.

Therefore $\exists t \in E$ such that $s < t$.

Therefore E is a Dedekind cut, by Definition 13.89. ■

DEFINITION 13.96. We define $\mathbb{R}$ to be the set of all Dedekind cuts. Elements of $\mathbb{R}$ are called **real numbers**.

13.4.1. Operations on real numbers. Just as we did for $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$, our next task is to define the basic operations and the ordering on $\mathbb{R}$. We begin, as usual, with addition. Given two real numbers (that is, two Dedekind cuts) A and B, how should we define $A + B$? For example, we want $2+3 = 5$. The cut reprsenting 2 is $\{x \in \mathbb{Q} \mid x < 2\}$. It contains all rational numbers less than 2, but the ones of most interest are those that lead right up to 2, such as $19/10 = 1.9$ and $1999/1000 = 1.999$. Similarly, the set representing 3 contains $2.9, 2.99999$, etc. Let's see what happens when we add those elements together.

$$1.9 + 2.9 = 4.8$$

$$1.999 + 2.99999 = 4.99899$$

Notice how the sums lead right up to 5? In fact, you can check that the resulting set is $\{x \in \mathbb{Q} \mid x < 5\}$, just what

we wanted. This suggests that we should define $A + B$ as the set of all sums $a + b$, where $a \in A, b \in B$. For this to be a valid operation on $\mathbb{R}$, first we must show that this new set is in fact a Dedekind cut. In Exercise 2 you will do just that, thereby justifying the following definition.

DEFINITION 13.97. We define the operation $+$ on $\mathbb{R}$ by

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

Like the integers and rationals, the set of real numbers has an additive identity.

DEFINITION 13.98. We define $0 := \{x \in \mathbb{Q} \mid x < 0\}$.

Recall that we showed in Example 13.91 that 0 is in fact a real number. In Exercise 3, you will show that 0 is an additive identity for $\mathbb{R}$.

As with $\mathbb{Z}$ and $\mathbb{Q}$, every element of $\mathbb{R}$ has an additive inverse. To justify this, we'll find a general formula for the additive inverse of a Dedekind cut. Given a real number A, it is tempting to define $-A$ as $\{-x \mid x \in A\}$. However, this set will be upward closed but not downward closed, so it is not a Dedekind cut. The problem is that negation reverses the order. To fix that problem, perhaps we should define $-A$ as the set of all negatives of rational numbers *not* in A? That almost works, but consider the case $A = \{x \in \mathbb{Q} \mid x < 2\}$. Then our proposed set $-A$ would be $\{x \in \mathbb{Q} \mid x \leq -2\}$, which contains a maximum and is therefore not a Dedekind cut. We can fix that by taking $-A$ to be the set of all rational numbers *strictly less than* the negative of some rational number not in A.

DEFINITION 13.99. Let A be a Dedekind cut. We define

$$-A := \{y \in \mathbb{Q} \mid y < -x \text{ for some } x \in \mathbb{Q} \setminus A\}.$$

In Exercise 4, you will prove that $-A$ is the unique additive inverse of A.

As usual, we define subtraction by $A - B := A + (-B)$.

Next, we define multiplication of Dedekind cuts. Your first guess, quite reasonably, might be to take $A \cdot B = \{ab; \mid a \in A, b \in B\}$, à la addition. Well, let's try it and see what happens. Suppose $A = \{x \in \mathbb{Q} \mid x < 2\}$ represents 2, and $B = \{x \in \mathbb{Q} \mid x < 3\}$ represents 3. If our definition works properly, then we should have that $A \cdot B$ is the Dedekind cut representing 6. Now, we have $(1.99)(2.99) = 5.9501$ and $(1.999)(2.99999) \approx 5.997$. So far, so good—these products seem to lead right up to 6. However, we also have $-4 \in A$ and $-5 \in B$, and $(-4)(-5) = 20$, which is greater than 6. Uh-oh.

The problem is that multiplying by a negative reverses the order. So let's try again. To avoid the same trouble, what if we multiply only the positive elements of A and B? That is, what if we define $A \cdot B$ to be $\{ab \mid a \in A, b \in B, a > 0, b > 0\}$? For our example of $2 \cdot 3$, we wind up with the set $\{x \in \mathbb{Q} \mid 0 < x < 6\}$. That's better, but there's still an issue—this set is not downward closed, so it's not a Dedekind cut.

This, too, is easily resolved. We can simply throw in all the missing elements. In other words, we can take the union of our previous set with the set of all nonnegative rationals. Now, for $2 \cdot 3$, we get $\{x \in \mathbb{Q} \mid x < 6\}$, which is exactly what we want.

So we have the right definition now? Slow down. It works great for positive numbers, but for negatives . . .

not so much. Consider $(-2)(-3)$, for example. This time, $A = \{x \in \mathbb{Q} \mid x < -2\}$ and $B = \{x \in \mathbb{Q} \mid x < -3\}$. So when we take all positive elements of A times all positive elements of B, we get the empty set, because A and B have no positive elements. Solution: we already know how to multiply positive reals, so simply define $(-2)(-3)$ to be $2 \cdot 3$.

The plan for defining multiplication of Dedekind cuts, then, will be the following. First, define the terms "positive" and "negative" for real numbers. Then define multiplication for positive real numbers. (In Exercise 5, you will prove that the definition we finally settled on above in fact yields a Dedekind cut.) Then define products involving negatives in terms of products of positives, using Definition 13.99.

DEFINITION 13.100. Let A be a Dedekind cut. We say that A is **positive** if $0 \in A$. We say that A is **negative** if $-A$ is positive.

LEMMA 13.101 (Law of Trichotomy). *Let A be a Dedekind cut. Then exactly one of the following three possibilities holds: A is positive, $A = 0$, or A is negative.*

PROOF. Exercise 6. ■

TOO MUCH INFORMATION 13.102. The word "trichotomy" means a splitting into three parts. Here, we split the set of real numbers into negatives, zero, and positives.

EXAMPLE 13.103. Let $A = \{x \in \mathbb{Q} \mid x^2 < 2 \text{ or } x < -1\}$. Is A positive, negative, or zero? (You may assume without proof that A is a Dedekind cut.)

Answer: Notice that $0 \in A$, because $0 \in \mathbb{Q}$ and $0^2 < 2$. So A is positive, by Definition 13.100. (By the way, A represents the real number $\sqrt{2}$.)

CHECK FOR UNDERSTANDING 13.104. For each statement below, say whether it is true or false, and justify your answer.

(1) Every positive Dedekind cut contains a positive rational number.
(2) Every negative Dedekind cut contains a positive rational number.
(3) No negative Dedekind cut contains a positive rational number.
(4) No negative Dedekind cut contains 0.
(5) Every negative Dedekind cut contains a negative rational number.
(6) Every positive Dedekind cut contains a negative rational number.

DEFINITION 13.105. We define the operation $\cdot$ on $\mathbb{R}$ by

$$A \cdot B := \begin{cases} \{ab \mid a \in A, b \in B, a > 0, b > 0\} \cup \{x \in \mathbb{Q} \mid x \leq 0\} \\ \qquad \text{if } A \text{ and } B \text{ are positive} \\ -(A \cdot (-B)) \text{ if } A \text{ is positive and } B \text{ is negative} \\ -((-A) \cdot B) \text{ if } A \text{ is negative and } B \text{ is positive} \\ (-A) \cdot (-B) \text{ if } A \text{ and } B \text{ are negative} \\ 0 \text{ if } A = 0 \text{ or } B = 0 \end{cases}$$

Lemma 13.101 assures us that this definition covers all possible cases without any overlapping.

All the usual properties of addition and multiplication, such as the commutative and distributive laws, hold for

$\mathbb{R}$ as well. Tables 2, 4, and 6 in Section 13.6 list several of these, and in the exercises, you will prove them. To demonstrate the flavor of these proofs, we now prove the distributive property for positive Dedekind cuts.

EXAMPLE 13.106. Let A, B, and C be positive real numbers (i.e., Dedekind cuts). Prove that $A \cdot (B + C) = A \cdot B + A \cdot C$.

Scratch work: The left- and right-hand sides of the equation are both Dedekind cuts, so they are *sets*. To prove two sets are equal to each other, we usually show the left is a subset of the right, then that the right is a subset of the left. Towards that end, when we choose an arbitrary element of the left-hand side, we want to use Definition 13.105. To do so, we need to know which case we're in. We know B and C are both positive, so we suspect that $B + C$ should also be positive, which puts us in the first case. But we need to justify that fact before using it. So that's how we'll begin.

PROOF. First, we will show that $A \cdot (B + C) \subseteq A \cdot B + A \cdot C$.

We are given that B and C are positive.

So $0 \in B$ and $0 \in C$, by Definition 13.100.

So $0 = 0 + 0 \in B + C$, by Definition 13.97.

So $B + C$ is positive, by Definition 13.100.

So $A \cdot (B + C) = \{ay \mid a \in A, y \in B + C, a > 0, b > 0\} \cup \{x \in \mathbb{Q} \mid x \leq 0\}$, by Definition 13.105.

Let $y \in A \cdot (B + C)$. We will show that $y \in A \cdot B + A \cdot C$.

Then $y \in \{ax \mid a \in A, x \in B + C, a > 0, x > 0\}$ or $y \in \{x \in \mathbb{Q} \mid x \leq 0\}$, by definition of union.

Case 1: $y \in \{ax \mid a \in A, x \in B + C, a > 0, x > 0\}$.

Then $y = ax$ for some $a \in A, x \in B + C$ such that $a > 0$ and $x > 0$.

Now, $B + C = \{b + c \mid b \in B, c \in C\}$, by Definition 13.97.

So $x = b + c$ for some $b \in B, c \in C$.

So $y = a(b + c) = ab + ac$, by the distributive property for rational numbers.

⟨*Careful to avoid falling into a trap at this point. We know that x is positive, but we don't know that b and c are positive!*⟩

We will now show that $ab \in A \cdot B$, whether $b > 0$ or $b \leq 0$.

If $b > 0$, then ab equals a positive element of A times a positive element of B, so $ab \in A \cdot B$, by Definition 13.105.

On the other hand, if $b \leq 0$, then $ab \leq 0$, because $a > 0$. In this case, $ab \in \{x \in \mathbb{Q} \mid x \leq 0\}$, so $ab \in A \cdot B$, by Definition 13.105.

Either way, we have that $ab \in A \cdot B$.

Similarly, $ac \in A \cdot C$.

So $y = ab + ac \in A \cdot B + A \cdot C$, by Definition 13.97.

Case 2: $y \in \{x \in \mathbb{Q} \mid x \leq 0\}$

Then y is a nonnegative rational number.

We know that A, B, and C are positive, so by Definition 13.105, both $A \cdot B$ and $A \cdot C$ contain every nonnegative rational number.

In particular, $y \in A \cdot B$, and $0 \in A \cdot B$.

So $y = y + 0 \in A \cdot B + A \cdot C$, by Definition 13.97.

In either case, we have $y \in A \cdot B + A \cdot C$.

Therefore, $A \cdot (B + C) \subseteq A \cdot B + A \cdot C$.

Next, we will show that $A \cdot B + A \cdot C \subseteq A \cdot (B + C)$.

Let $y \in A \cdot B + A \cdot C$. We will show that $y \in A \cdot (B + C)$.

By Definition 13.97, we know that $y = z + w$ for some $z \in A \cdot B$, $w \in A \cdot C$.

By Definition 13.105, we know that either $z = ab$ for some $a \in A, b \in B$ with $a > 0$ and $b > 0$, or else $z \leq 0$.

Similarly, we know that either $w = dc$ for some $d \in A, c \in C$ with $d > 0$ and $c > 0$, or else $w \leq 0$.

Case 1: $z = ab$ for some $a \in A, b \in B$ with $a > 0$ and $b > 0$, and $w = dc$ for some $d \in A, c \in C$ with $d > 0$ and $c > 0$

⟨*When we add $z + w$, we get $ab + dc$. It would be nice to apply the distributive property to factor out a, but we can't—we don't know that a and d are the same number. What we can do, though, is take advantage of the fact that Dedekind cuts are downward closed. If a is larger, for example, we can instead get that $ab+ac = a(b+c) \in A\cdot(B+C)$, then use downward closure.*⟩

WLOG assume that $d \leq a$.

Then $ab + dc \leq ab + ac = a(b + c) \in A \cdot (B + C)$, by the distributive property for rational numbers, and by Definition 13.105.

Therefore $z + w = ab + dc \in A \cdot (B + C)$ by Definition 13.89. (Specifically, we're using here the fact that $A\cdot(B+C)$ is a Dedekind cut and so is downward closed.)

Case 2: $z = ab$ for some $a \in A, b \in B$ with $a > 0$ and $b > 0$, and $w \leq 0$

By Definition 13.100, we know that $0 \in C$, because C is positive.

So $b = b + 0 \in B + C$, by Definition 13.97.

So $z = ab \in A \cdot (B + C)$, by Definition 13.105.

Now, $z + w \leq z$, because $w \leq 0$.

So $z+w \in A\cdot(B+C)$, by Definition 13.89. (Specifically, we're using here the fact that $A \cdot (B+C)$ is a Dedekind cut and so is downward closed.)

Case 3: $z \leq 0$, and $w = dc$ for some $d \in A, c \in C$ with $d > 0$ and $c > 0$

Similar to Case 2.

Case 4: $z \leq 0$ and $w \leq 0$

Then $z + w \leq 0$.

By Definition 13.105, we have that $0 \in A \cdot (B+C)$. (Here we use the fact that $B + C$ is positive, which we showed earlier.)

So $z+w \in A \cdot (B+C)$, by Definition 13.89. (Specifically, we're using here the fact that $A \cdot (B+C)$ is a Dedekind cut and so is downward closed.)

In every case, we have that $y = z + w \in A \cdot (B + C)$.

Therefore $A \cdot B + A \cdot C \subseteq A \cdot (B + C)$.

Therefore, $A \cdot (B+C) = A \cdot B + A \cdot C$, because $A \cdot (B+C) \subseteq A \cdot B + A \cdot C$ and $A \cdot B + A \cdot C \subseteq A \cdot (B + C)$. ■

Finally, we will define the standard ordering on $\mathbb{R}$. We could repeat our earlier trick: define $A < B$ iff $B - A$ is positive. That would give us exactly what we want. But there is another, more elegant way to define the ordering. Consider, for example, the two Dedekind cuts $A = \{x \in \mathbb{Q} \mid x < 2\}$ and $B = \{x \in \mathbb{Q} \mid x < 3\}$. Then A represents the real number 2, and B represents the real number 3. We want $A < B$. What can you say about the relationship of A to B, as sets? Well, A is a subset of B. In general, because of downward closure, Dedekind cuts representing larger numbers will contain those representing smaller numbers.

DEFINITION 13.107. We define a relation $\leq$ on $\mathbb{R}$ by $A \leq B$ iff $A \subseteq B$. We define $<$ by $A < B$ iff $A \leq B$ and $A \neq B$.

13.4.2. Ordering the reals. As before, we'll count on you to supply the correct definitions for all related notations.

CHECK FOR UNDERSTANDING 13.108. Prove that A is positive iff $A > 0$.

Tables 3, 5, 7, and 8 in Section **??** list several properties of the ordering on $\mathbb{R}$. In the exercises, you will be asked to prove them.

One order property of the real numbers deserves special attention. In the introduction to this chapter, we pointed out that in the rationals, we cannot always take limits when we ought to be able to. In Chapter 11, we saw that one order property of $\mathbb{R}$ in particular make limits work the way they're supposed to. That key feature of the reals is the *least upper bound property*. Before continuing, those of you who did not cover that chapter should go back right now and read Definitions 11.1 and 11.3. (And those of you who did cover that chapter should review those definitions!)

We will prove that $\mathbb{R}$ has the *least upper bound property*, also known as *Dedekind completeness*. This property states that if a nonempty set of real numbers has an upper bound, then it has a least upper bound. To understand this property, let's use a specific example to contrast the real to the rationals, which are not Dedekind complete. Define (s_n) by equation (11) on page 272, and let $S = \{s_n \mid n \in \mathbb{N}\}$. Figure 3 on page 273 shows a picture of S. Clearly, S is not not empty. Also, we showed in Example 13.95 that $s_n \leq 3$ for all $n \in \mathbb{N}$, so 3 is an upper bound for S. However, S does not have a least upper bound in $\mathbb{Q}$. The reason is that any such least upper bound must be the limit of the sequence (s_n), but (s_n) converges to e, which is not an element of $\mathbb{Q}$. In $\mathbb{R}$, however, no problem—the least upper bound of S is e.

For another example, let $T = \{x \in \mathbb{Q} \mid x^2 < 2\}$. The set T is not empty, because $1 \in T$. Also, $x \leq 5$ for all $x \in T$, so 5 is an upper bound for T. But T has no supremum in $\mathbb{Q}$; its least upper bound is $\sqrt{2}$, which is irrational.

Given a set S of real numbers (i.e., of Dedekind cuts), how do we find its least upper bound, if it has one? For

example, take $S = \{s_n \mid n \in \mathbb{N}\}$, as before. Figure **??** shows the Dedekind cuts corresponding to the real numbers s_1, s_2, and s_3; you can imagine the other elements of S. The smallest possible upper bound of S is e, as also shown in Figure **??**. How do we describe the *set* e in terms of the *sets* s_n? Figure **??** suggests an answer: take the union of the sets s_n.

THEOREM 13.109 (Least Upper Bound Property). *If a nonempty subset of* $\mathbb{R}$ *has an upper bound in* $\mathbb{R}$*, then it has a least upper bound in* $\mathbb{R}$*.*

PROOF. Suppose that S is a nonempty subset of $\mathbb{R}$, and that $U \in \mathbb{R}$ is an upper bound for S. We will show that S has a least upper bound in $\mathbb{R}$.

Let $L = \cup_{A \in S} A$.

First, we will show that L is a Dedekind cut, so $L \in \mathbb{R}$. Then, we will show that L is a least upper bound for S.

⟨*Recall Definition 13.89. To show L is a Dedekind cut, we have four things to show.*⟩

We know that $S \neq \emptyset$, so S contains at least one Dedekind cut B.

By Definition 13.89, $B \neq \emptyset$.

Therefore, $L \neq \emptyset$.

Next, we will show that $\mathbb{Q} \setminus L \neq \emptyset$.

We know that U is an upper bound for S.

So $A \leq U$ for all $A \in S$, by Definition 11.1.

So $A \subseteq U$ for all $A \in S$, by Definition 13.107.

So $L \subseteq U$, because $L = \cup_{A \in S} A$.

Now $U \in \mathbb{R}$, so U is a Dedekind cut, and so by Definition 13.89, we know that $\mathbb{Q} \setminus U \neq \emptyset$.

Therefore $\mathbb{Q} \setminus L \neq \emptyset$, because $L \subseteq U$.

Next, we will show that L is downward closed.

Let $r, s \in \mathbb{Q}$ such that $s \in L$ and $r < s$. We will show that $r \in L$.

By definition of union, $s \in B$ for some $B \in S$.

Now, B is a Dedekind cut, so Definition 13.89 tells us that B is downward closed.

So $r \in B$, by Definition 13.89.

Therefore $r \in L$, by definition of union.

Lastly, we will show that L has no maximum.

Temporarily assume that M is a maximum for L.

Then $M \in L$, and $x \leq M$ for all $x \in L$, by definition of maximum.

Now, $M \in L$, so $M \in B$ for some $B \in L$, by definition of union.

But then $M \in B$ and $x \leq M$ for all $x \in B$.

So M is a maximum for B.

But B is a Dedekind cut, so by Definition 13.89, B has no maximum.

Contradiction.

Therefore, L has no maximum.

So by Definition 13.89, we have that L is a Dedekind cut. In other words, $L \in \mathbb{R}$.

Next, we will show that L is a least upper bound for S.

⟨*Recall Definition 11.3. We must show two things.*⟩

First, we will show that L is an upper bound for S.

We know that $A \subseteq L$ for all $A \in S$, because $L = \cup_{A \in S} A$.

So $A \leq L$ for all $A \in S$, by Definition 13.107.

So L is an upper bound for S, by definition of upper bound (Definition 11.1).

Finally, let $K \in \mathbb{R}$ be any upper bound of S. We will show that $L \leq K$.

We know that $A \leq K$ for all $A \in S$, by definition of upper bound (Definition 11.1).

So $A \subseteq K$ for all $A \in S$, by Definition 13.107.
So $L \subseteq K$, because $L = \cup_{A \in S} A$.
So $L \leq K$, by Definition 13.107.

Therefore, by definition of least upper bound (Definition 11.3), L is a supremum for S. ■

Too Much Information 13.110. Now we know that $\mathbb{R}$ and $\mathbb{Q}$ cannot be isomorphic with respect to order, because by Theorem 13.109, the ordering on $\mathbb{R}$ is Dedekind complete, whereas we saw earlier that for $\mathbb{Q}$ it is not. In other words, there is no bijective function $f : \mathbb{Q} \to \mathbb{R}$ such that $a \leq b$ iff $f(a) \leq f(b)$. In fact, we proved in Chapter 9 that there is no bijective function whatsoever from $\mathbb{Q}$ to $\mathbb{R}$, because $\mathbb{Q}$ is countable, but $\mathbb{R}$ is not.

Too Much Information 13.111. Later on, in Theorem 13.122, we will see that Dedekind completeness is, in many ways, what makes the reals the reals.

13.4.3. Embedding the rationals in the reals. In earlier sections, we embedded $\mathbb{N}$ into $\mathbb{Z}$ and $\mathbb{Z}$ into $\mathbb{Q}$. It should come as no surprise that we will next embed $\mathbb{Q}$ into $\mathbb{R}$, so that we can think of rational numbers as real numbers. So given a rational number r, which real number (i.e., Dedekind cut) represents r? It's nothing new; several times throughout this section, we've used the Dedekind cut $\{x \in \mathbb{Q} \mid x < r\}$ to represent r. This gives us precisely the embedding we want. We state this fact in Theorem 13.112, whose proof we leave to you. In the proof of Theorem 13.112, there are several things to check: that $\{x \in \mathbb{Q} \mid x < r\}$ is in fact a Dedekind cut; that the map is injective; and that addition, multiplication, and order are preserved.

THEOREM 13.112. *Define* $f\colon \mathbb{Q} \to \mathbb{R}$ *by* $f(r) = \{x \in \mathbb{Q} \mid x < r\}$. *Then* f *is injective, and for all* $a, b \in \mathbb{Q}$,

$$f(a+b) = f(a) + f(b), \text{ and}$$
$$f(a \cdot b) = f(a) \cdot f(b), \text{ and}$$
$$a < b \text{ iff } f(a) < f(b).$$

PROOF. Exercise 7. ■

From now on, thanks to Theorem 13.112, we will regard $\mathbb{Q}$ as a subset of $\mathbb{R}$. For example, we may write $-2/3 \in \mathbb{R}$, where you should interpret $-2/3$ to mean the Dedekind cut $\{x \in \mathbb{Q} \mid x < -2/3\}$.

TOO MUCH INFORMATION 13.113. You may have wondered why, in Definition 13.89, we insisted that a Dedekind cut cannot have a maximum. Let's see what goes wrong if we eliminated (4) from that definition. Then both $\{x \in \mathbb{Q} \mid x < 2\}$ and $\{x \in \mathbb{Q} \mid x \leq 2\}$ would be distinct Dedekind cuts, for example. But they would both represent the number 2! In fact, every rational number would appear twice—once in the $<$ cut, and once in the $\leq$ cut. We prefer to have each rational number appear exactly once in $\mathbb{R}$, so we set up our definition accordingly.

TOO MUCH INFORMATION 13.114. Why don't we also insist, in Theorem 13.112, that f also preserve subtraction and division? That is, why not also require that $f(a-b) = f(a) - f(b)$ for all $a, b \in \mathbb{Q}$, and that $f(a/b) = f(a)/f(b)$ for all $a, b \in \mathbb{Q}$ such that $b \neq 0$? The reason is that subtraction and division come for free. Once we know that f preserves addition and multiplication, then it will necessarily preserve subtraction and division, too. See Exercise 8.

13.4.4. Exercises for Section 13.4. For each of these exercises, when you are asked to prove something, you may assume that the previous exercises have already been proved, but not the later ones.

(1) Define the sequence (p_n) by

$$p_n = \sum_{j=1}^{n} \frac{(-1)^{j+1}}{2j-1}.$$

For each $N \in \mathbb{N}$, define $P_n = \{x \in \mathbb{Q} \mid x < p_n\}$. Let $P = \cup_{n\in\mathbb{N}} P_n$. Prove that P is a Dedekind cut. (You may be interested to know that P represents the real number $\pi/4$.)

(2) Prove that if A and B are Dedekind cuts, then $\{a + b \mid a \in A, b \in B\}$ is a Dedekind cut.

(3) Prove that the real number 0 defined in Definition 13.98 is an additive identity for $\mathbb{R}$.

(4) Prove that the Dedekind cut $-A$ from Definition 13.99 is the unique additive inverse of the Dedekind cut A.

(5) Prove that if A and B are positive Dedekind cuts, then $\{ab \mid a \in A, b \in B, a > 0, b > 0\} \cup \{x \in \mathbb{Q} \mid x \leq 0\}$ is a Dedekind cut.

(6) Prove Lemma 13.101.

(7) Prove Theorem 13.112.

(8) Let f be as in Theorem 13.112. Prove that f preserves subtraction and division, too. In other words:
   (a) Prove that $f(a-b) = f(a)-f(b)$ for all $a, b \in \mathbb{Q}$.
   (b) Prove that $f(0) = 0$.
   (c) Prove that $f(a/b) = f(a)/f(b)$ for all $a, b \in \mathbb{Q}$ such that $b \neq 0$.

13.5. The complex numbers

At long last, we arrive at our final destination: the complex numbers. Having just constructed $\mathbb{R}$, our goal is to use

it to construct $\mathbb{C}$. We want to be able to write a complex number in the form $a + bi$, where $a, b \in \mathbb{R}$. The a and b are no problem. The question is, what exactly is i? Recall from Remark 13.1 that we will not allow $i = \sqrt{-1}$ as a definition. Instead, the answer is: don't worry about it. To specify $a + bi$, all we really need is the pair of numbers a and b. Should we use the set $\{a, b\}$ or the ordered pair (a, b)? To answer that question, we ask ourselves: does order matter? Well, yes. We need to know which one is the real part, and which goes with i. So we will define $\mathbb{C}$ as the set of all ordered pairs of real numbers. In other words, it will be the Cartesian product $\mathbb{R} \times \mathbb{R}$.

DEFINITION 13.115. We define

$$\mathbb{C} := \mathbb{R} \times \mathbb{R}.$$

An element of $\mathbb{C}$ is a **complex number**.

Technically, then, a complex number is an ordered pair (a, b), where $a, b \in \mathbb{R}$. We think of (a, b) as the complex number $a+bi$. Later, we will justify the use of this notation.

EXAMPLE 13.116.
(1) In the usual $a + bi$ notation, what complex number does $(2, -3)$ represent?
(2) Represent the complex number $\frac{1}{2}i - \frac{\sqrt{3}}{2}$ as an ordered pair.

(1) It represents $2 - 3i$.
(2) We have $\frac{1}{2}i - \frac{\sqrt{3}}{2} = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$, so we represent it as $(-\sqrt{3}/2, 1/2)$. (Note that we put the real part first—order matters.)

We now define addition and multiplication on $\mathbb{C}$. In the usual notation, we want to have

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \text{ and}$$

$$(a+bi)(c+di) = (ac-bd)+(bc+ad)i,$$

because we want $i^2 = -1$ to be true, along with the usual properties of addition and multiplication. These desired equations, then, lead to the following definition.

DEFINITION 13.117. We define the operations $+$ and $\cdot$ on $\mathbb{C}$ by

$$(a,b)+(c,d) := (a+c, b+d), \text{ and}$$
$$(a,b)\cdot(c,d) := (ac-bd, ad+bc).$$

In the exercises, you will verify that addition and multiplication of complex numbers satisfy the properties listed in Tables 2, 4, and 6. We define subtraction and division just as we did for $\mathbb{Q}$ and for $\mathbb{R}$.

We want to be able to write $i = 0+1\cdot i$, and so we make the following definition.

DEFINITION 13.118. We define the complex number i by

$$i := (0,1).$$

Also, we want to be able to think of $\mathbb{R}$ as a subset of $\mathbb{C}$. Another embedding theorem is in order. We want to represent a real number x as $x + 0 \cdot i$. This suggests the map $x \mapsto (x, 0)$.

THEOREM 13.119. *Define $f : \mathbb{R} \to \mathbb{C}$ by $f(x) = (x, 0)$. Then f embeds $\mathbb{R}$ into $\mathbb{C}$ in a way that preserves addition and multiplication. In other words, f is injective, and for all $a, b \in \mathbb{R}$,*

$$f(a+b) = f(a) + f(b), \text{ and}$$

$$f(ab) = f(a)f(b).$$

PROOF. Exercise **??**. ■

Thanks to Theorem 13.119, we will write real numbers in the usual way from now on. For example, instead of $(-47, 0)$, we will simply write -47. The notation $a + bi$, where $a, b \in \mathbb{R}$, really does mean (a, b), then, because

$$\begin{aligned} a + bi &= (a, 0) + (b, 0)(0, 1) && \text{by Definition 13.118} \\ &= (a, 0) + (0, b) && \text{by Definition 13.117} \\ &= (a, b) && \text{by Definition 13.117.} \end{aligned}$$

The special property of i is the equation $i^2 = -1$. This holds because

$$\begin{aligned} i^2 &= (0, 1) \cdot (0, 1) && \text{by Definition 13.118} \\ &= (-1, 0) && \text{by Definition 13.117} \\ &= -1. \end{aligned}$$

We previously defined orderings on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$, and proved in the exercise that they have the properties listed in Tables 3, 5, 7, and 8. However, there is no ordering on $\mathbb{C}$ that maintains these properties. Here's a quick sketch of the proof. Suppose that $\leq$ was such an ordering. Then $i \leq 0$ or $i \geq 0$. Either way, you get $i^2 \geq 0$, a contradiction.

Finally, we cannot leave this section without mentioning the most remarkable property of $\mathbb{C}$, at least insofaras addition and multiplication are concerned. This is the Fundamental Theorem of Algebra. (You know a theorem is significant when it's called "fundamental"!) The Fundamental Theorem of Algebra states that every nonconstant polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.

THEOREM 13.120. *[Fundamental Theorem of Algebra]Let $n \in \mathbb{N}$, and let $a_0, a_1, \ldots, a_n \in \mathbb{C}$ such that $a_n \neq 0$. Then there exists $x \in \mathbb{C}$ such that*

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0.$$

The proof of Theorem 13.120 is beyond the scope of this textbook, but not beyond the scope of your undergraduate career. As is often the case with a major result, there are many proofs of the Fundamental Theorem of Algebra. If you take a class in Complex Analysis, you will most likely see a proof of it, or perhaps several. You may see another proof in a Topology class. An Abstract Algebra class that covers Galois theory may present yet another proof.

TOO MUCH INFORMATION 13.121. Looking back over this entire chapter, you can see just how much work it took to define complex numbers. According to our formal definitions, a complex number *is* an ordered pair of real numbers, which are Dedekind cuts of rational numbers, which are equivalence classes of ordered pairs of integers, which are equivalence classes of ordered pairs of natural numbers, each of which can be expressed in terms of the undefined symbols S and 1. It would be quite a task to untangle all these definitions to write, say, $-(1/2) + (\sqrt{3}/2)i$ in terms of S and 1.

13.5.1. Exercises for Section 13.5. For each of these exercises, when you are asked to prove something, you may assume that the previous exercises have already been proved, but not the later ones.

(1) Prove properties in tables. For the appropriate exercise, recall as a hint the "multiply by the conjugate" trick for finding the multiplicative inverse of

Props	Props

TABLE 2. Table with addition and multiplication properties for N, Z, Q, R, C

Props	Props

TABLE 3. Table with order properties for N, Z, Q, R

Props	Props

TABLE 4. Table with addition and multiplication properties for Z, Q, R, C

a nonzero complex number:

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

(2) Prove Theorem **??**.

13.6. Properties of the number systems

In this section, we
Addition and Multiplication Props of N, Z, Q, R, C
Order Props of N, Z, Q, R
Addition and Multiplication Props of Z, Q, R, C
Order Props of Z, Q, R
Multiplication Prop of Q, R, C (inverses)
Order Prop of R (completeness)
Addition and Multiplication Prop of C: FTA
Remark that the proof of FTA is nontrivial.

Group, abelian group, ring, commutative ring, commutative ring with unity, field, ordered field, complete ordered field, algebraically complete field.

Props	Props

TABLE 5. Table with order properties for Z, Q, R

Props	Props

TABLE 6. Table with addition and multiplication properties for Q, R, C

Props	Props

TABLE 7. Table with order properties for Q, R

Props	Props

TABLE 8. Table with order properties for R

Note on which of N, Z, Q, R, C is which. Note that R is the unique complete ordered field.

above: include archimdean property

Above table: mult. inverses

Above table: intermediate value property

Above table: least upper bound property

THEOREM 13.122.

NOTE THAT Q IS AN ORDERED FIELD BUT NOT ISOM TO R. SO ORDERED FIELD AXIOMS ARE NOT ENOUGH TO CHARACTERIZE THE SET.

13.7. Cauchy sequences

Instead, we turn to a brilliant idea developed by several mathematicians throughout the 19th century. Namely, we use *the sequence* (s_n) *itself* to define e. So our first attempt at a definition of $\mathbb{R}$ is the set of all sequences of rational numbers that in some sense "should" converge.

We do not want every sequence to converge. For example, the sequence $1, 2, 3, \ldots$ should be divergent. How do we determine which sequence of rational numbers should converge, and which should not? The sequence (s_n) above, for example, should converge to e; perhaps we should use the definition of the limit of a sequence to say that (s_n) is convergent because for all $\epsilon > 0$, there exists $M \in \mathbb{N}$ such that if $k \geq M$, then $|s_k - e| < \epsilon$? Not so fast. We've constructed only rational numbers up to this point, so referring to e is illegal. Somehow, we must decide that (s_n) is convergent without mentioning anywhere what it converges to.

Towards that end, here comes the next brilliant idea. Rather than say that (s_n) converges if its terms eventually become arbitrarily close to some limit, we observe that it converges iff its terms eventually become arbitrarily close to *each other*.

DEFINITION 13.123. Let (a_n) be a sequence of rational numbers. We say that (a_n) is **Cauchy** if for all $\epsilon \in \mathbb{Q}$ such that $\epsilon > 0$, there exists $M \in \mathbb{N}$ such that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$.

Here's what Definition 13.123 says in words: To be a Cauchy sequence, we must have that for any given tolerance, there is a point in the sequence such that past that point, the distance between any two terms in the sequence is within the specified tolerance. The tolerance is ϵ. The point in the sequence we must go past in M. The distance between the two terms beyond that point is $|a_j - a_k|$.

TOO MUCH INFORMATION 13.124. Recall that a sequence of rational numbers is really a function from $\mathbb{N}$ to

$\mathbb{Q}$, and that both of these sets have now been constructed. So this is a valid definition.

TOO MUCH INFORMATION 13.125. In an Analysis class, you will learn that in the definition of a Cauchy sequence, we can take any $\epsilon > 0$, where $\epsilon \in \mathbb{R}$. However, we are in the process of defining $\mathbb{R}$, so we can not yet use $\mathbb{R}$ in any definitions. In fact, you will learn a much more general definition of Cauchy sequence.

TOO MUCH INFORMATION 13.126. INSERT A HISTORICAL NOTE ON AUGUSTIN CAUCHY HERE.

TOO MUCH INFORMATION 13.127. In the standard English pronunciation of the French name "Cauchy," the first syllable is "co" as in "code" or "commingle," and the second syllable is "she" as in "sheep" or the pronoun "she." When you say this word, you should not sound as if you are talking about a piece of furniture: please do not say "couchy"!

EXAMPLE 13.128. Define the sequence (a_n) by $a_n = n$. Is (a_n) a Cauchy sequence? Prove or disprove.

Scratch work: The terms of this sequence are $1, 2, 3, \ldots$ Given any tolerance, can we always find a point in the sequence so that from that point on, the distance between any two terms is within that tolerance? No, certainly not. The distance between any two distinct terms is never less than 1. So set the tolerance $\epsilon = 1/2$. Then no matter how far into the sequence you go, the distance between two consecutive terms is never less than ϵ.

Claim: The sequence (a_n) is not Cauchy.

PROOF. We will show that it is false that for all $\epsilon \in \mathbb{Q}$ such that $\epsilon > 0$, there exists $M \in \mathbb{N}$ such that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$.

We will show that $\epsilon = 1/2$ is a counterexample.

Note that $\epsilon \in \mathbb{Q}$ and $\epsilon > 0$.

We will show that there does not exist $M \in \mathbb{N}$ such that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$.

Temporarily assume that there exists $M \in \mathbb{N}$ such that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$.

Let $j = M$ and $k = M + 1$.

Then $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$.

So $|a_j - a_k| < \epsilon = 1/2$.

However, $|a_j - a_k| = |a_M - a_{M+1}| = |M - (M + 1)| = 1$.

We get $1 < 1/2$, which is a contradiction.

Therefore there does not exist $M \in \mathbb{N}$ such that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$.

Therefore $\epsilon = 1/2$ is a counterexample.

Therefore (a_n) is not Cauchy. ■

EXAMPLE 13.129. Define the sequence (a_n) by $a_n = 2^{-n+1}$.

(1) Let $\epsilon = 2/5$ and $M = 2$. Is it true that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$? Prove it or find a counterexample.
(2) Let $\epsilon = 2/5$ and $M = 3$. Is it true that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$? Prove it or find a counterexample.
(3) Let $\epsilon = 1/1000$. Prove that there exists $M \in \mathbb{N}$ such that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$.
(4) Is (a_n) a Cauchy sequence? Prove or disprove.

Answers:

(1) No, that is false. For example, let $j = 2$ and $k = 4$. Then $|a_j - a_k| = |1/2 - 1/16| = |7/16| = 0.4375$, which is not less that $2/5$.
(2) Scratch work: Let's start computing some examples to try to get the idea of whether this is true or not. We have $|a_3 - a_4| = |1/4 - 1/8| = 1/8 < 2/5$. We have $|a_4 - a_7| = |1/8 - 1/64| < 1/8 < 2/5$. We have

$|a_{10} - a_{12}| = |2^{-9} - 2^{-12}| < 2^{-9} < 2/5$. It looks as if this is true: we can bound $|a_j - a_k|$ by the larger term, which is no more than $1/4$ when $j, k \geq 3$.

PROOF. Let $j, k \in \mathbb{N}$ such that $j \geq M$ and $k \geq M$. We will show that $|a_j - a_k| < \epsilon$.
WLOG assume that $j \leq k$.
Then $a_j = 2^{-j+1} \geq 2^{-k+1} = a_k$.
Also, $a_j = 2^{-j+1} \leq 2^{-3+1} = 1/4$.
So $|a_j - a_k| = a_j - a_k \leq a_j \leq 1/4 < 2/5$. ■

(3) Scratch work: We must find a point in the sequence such that from that point on, the distance between any two terms of the sequence is less than $1/1000$. The previous part of this example gives us an idea: find a term in the sequence that's less than $1/1000$. (Warning: This trick works for this example, but it does not always work.) We have $2^{10} = 1024$, so $a_{11} = 1/1024 < 1/1000$. So take $M = 11$.

PROOF. Let $M = 11$.
Let $j, k \in \mathbb{N}$ such that $j \geq M$ and $k \geq M$. We will show that $|a_j - a_k| < \epsilon$.
WLOG assume that $j \leq k$.
Then $a_j = 2^{-j+1} \geq 2^{-k+1} = a_k$.
Also, $a_j = 2^{-j+1} \leq 2^{-11+1} = 1/1024$.
So $|a_j - a_k| = a_j - a_k \leq a_j \leq 1/1024 < \epsilon$. ■

(4) Scratch work: Intuitively, (a_n) is a Cauchy sequence, because it is convergent. (It converges to 0.)

Now, let's figure out how to prove that. Given a rational number $\epsilon > 0$, we must find a point in the sequence such that from that point on, the distance between any two terms of the sequence is less than ϵ. The previous part of this example gives us an idea: find a term in the sequence that's less than ϵ. So choose M to be large enough such that $a_M < \epsilon$.

In other words, we need $2^{-M+1} < \epsilon$. That is, we need $2^{M-1} > 1/\epsilon$. It is straightforward to show by induction that $2^{M-1} \geq M$ for all $M \in \mathbb{N}$. So we can just choose $M > 1/\epsilon$.

Claim: The sequence (a_n) is Cauchy.

PROOF. Let $\epsilon \in \mathbb{Q}$ such that $\epsilon > 0$.

We will show that there exists $M \in \mathbb{N}$ such that if $j, k \in \mathbb{N}$ and $j \geq M$ and $k \geq M$, then $|a_j - a_k| < \epsilon$.

Choose $M \in \mathbb{N}$ such that $M > 1/\epsilon$. (This is possible by the Archimedean property—see Table 3.)

Then $2^{M-1} \geq M > 1/\epsilon$, so $a_M = 2^{-M+1} < \epsilon$.

Let $j, k \in \mathbb{N}$ such that $j \geq M$ and $k \geq M$. We will show that $|a_j - a_k| < \epsilon$.

WLOG assume that $j \leq k$.

Then $a_j = 2^{-j+1} \geq 2^{-k+1} = a_k$.

Also, $a_j = 2^{-j+1} \leq 2^{-M+1} < \epsilon$.

So $|a_j - a_k| = a_j - a_k \leq a_j < \epsilon$. ■

POINT OUT THAT BY Theorem 13.122, CAUCHY SEQUENCES GIVE US A COMPLETE ORDERED FIELD AND SO ARE EQUIVALENT TO DEDEKIND CUTS. REMARK THAT THEY GENERALIZE IN DIFFERENT WAYS.

13.8. Fun math facts

Axioms for set theory. Mention ZFC. State informal version of Lawvere's axioms, refer to the "Rethinking Set Theory" article. Mention independence of choice, CH (Godel, Cohen).

Comment on how the axiomatic method works in general, undefined terms, axioms. Note connection to Euclidean geometry: point, line, plane, etc. History (independence of parallel postulate, Hilbert's work). Hilbert quote.

Other number systems: quaternions, octonions, sedonions, etc. See Which Numbers are Real? book for more examples.

What's the point of having these number systems? Arise naturally from solving problems, are convenient. Need R for geometry—Pythagoras shows Q is not good enough. C arises naturally from solving polynomials, note history of cubic.

Apparently Dedekind came up with a definition of the reals in the process of preparing for a Calculus class. He was trying to prove everything rigorously but got stuck at the Intermediate Value Theorem because the reals had not been properly defined.